

---

Doctoral

Science

---

2019

## Modelling Anti-Phishing Authentication Ceremonies

Edina Hatunic-Webster

*Technological University Dublin*, [edina.hatunicwebster@tudublin.ie](mailto:edina.hatunicwebster@tudublin.ie)

Follow this and additional works at: <https://arrow.tudublin.ie/sciendoc>

---

### Recommended Citation

Hatunic-Webster,E. (2019) *Modelling Anti-Phishing Authentication Ceremonies*. Doctoral thesis, 2019.  
DOI:10.21427/repy-b403

This Theses, Ph.D is brought to you for free and open access by the Science at ARROW@TU Dublin. It has been accepted for inclusion in Doctoral by an authorized administrator of ARROW@TU Dublin. For more information, please contact [arrow.admin@tudublin.ie](mailto:arrow.admin@tudublin.ie), [aisling.coyne@tudublin.ie](mailto:aisling.coyne@tudublin.ie), [vera.kilshaw@tudublin.ie](mailto:vera.kilshaw@tudublin.ie).



# Modelling Anti-Phishing Authentication Ceremonies

**Edina Hatunić-Webster MSc. BSc.**

A thesis submitted to the Technological University Dublin  
for the degree of Doctor of Philosophy

Supervised by:

Dr. Fredrick Mtenzi

Prof. Sarah Jane Delany

School of Computer Science

Technological University Dublin

February 2019

# Abstract

This dissertation explores the use of security ceremonies as a way of extending the reach of current methods for social, technological and contextual analysis of web authentication schemes and the reasons they do not protect effectively against phishing. A security ceremony extends the concept of security protocol to include both user interface and human-protocol interaction. This thesis enhances the understanding of security ceremonies and their importance in the analysis of web authentication schemes. The modelling of the human elements of a ceremony is an active research area. Our focus is the modelling of human communication processing in authentication ceremonies.

Phishing is a form of electronic fraud that tries to steal users' authentication credentials by spoofing the login page of a legitimate, trusted website. Various anti-phishing authentication schemes are being proposed to help users resist attacks. The threat analysis and security proofs of these schemes rarely specifically take into account the human user limitations as a potential threat. When authentication protocols are implemented and used by humans, the underlying assumptions about human-protocol interactions are often susceptible to social engineering attacks such as phishing. Incorrect human trust decisions, i.e. human factors, play a big role in phishing.

In this thesis we present the Human Factors in Anti-Phishing Authentication Ceremonies (HF-APAC) Framework as a way to analyse the communication pro-

cessing performed by human users in authentication ceremonies.

We demonstrate a usage of the HF-APAC Framework by designing a Model for Analysing HF-APAC. The model examines how users process authentication tasks and how these tasks impact the user’s decision-making and consequently their detection of spoofed login prompts. The model proposes communication processing principles that can be used as part of the design process of authentication ceremonies.

To demonstrate how these principles can be applied to provide enhanced anti-phishing resistance we designed a new authentication ceremony, MultiStep Mutual Authentication (MSMA). The graphical part of the MSMA ceremony is a Human Perceptible Authenticator (HPA) that helps the user establish the legitimacy of the website and mitigate phishing attacks. We found evidence that MSMA helped users resist attacks.

We evaluated MSMA, the Model, and in turn the Framework, with a user study. Our findings suggest how communication processing affects decision making; we found that increasing the number of recall and recognise communication processing tasks improves the phishing resistance of a ceremony.

# Declaration

I certify that this thesis which I now submit for examination for the award of Doctor of Philosophy, is entirely my own work and has not been taken from the work of others save and to the extent that such work has been cited and acknowledged within the text of my work.

This thesis was prepared according to the regulations for graduate study by research of the Technological University Dublin and has not been submitted in whole or in part for another award in any other third level institution.

The work reported on in this thesis conforms to the principles and requirements of the TU Dublin's guidelines for ethics in research.

TU Dublin has permission to keep, lend or copy this thesis in whole or in part, on condition that any such use of the material of the thesis be duly acknowledged.

Signature \_\_\_\_\_

Date \_\_\_\_\_

# Acknowledgements

I would like to express my gratitude to my supervisors, Dr. Fred Mtenzi, for his support and advice and Prof. Sarah Jane Delany, for stepping forward to join the supervisory team at the last, but very important stage. They helped me to overcome the many challenges associated with part-time research study.

I would like to thank Prof. Brendan O'Shea for his time as a supervisor and for his support and encouragement, that continued even after his retirement. I would also like to thank Prof. Kenny Paterson for his time and help as an advisory supervisor.

Many thanks to all of the participants who took part in my study, and who allowed me to take up their valuable time. Thanks to the School of Computer Science lecturers for helping with running the study; Andrea Curley, Denis Manley, Ciaran O'Leary, Prof. John Kelleher, Dr. Art Sloane and Dr. Paul Doyle in particular. Thanks to Dr. John Gilligan for taking the time to review this thesis. I would also like to thank Prof. Robert Biddle for his help with the study.

Finally, I owe a debt of gratitude to my family who have supported me throughout the process. Thanks to my parents, especially to my mother who encouraged me to persevere with my research ambitions; my children for their patience while their mother worked too many hours, especially my daughter for trying to understand what a PhD is all about; and to my husband for his support to allow me to see this research through to completion.

# Abbreviations

<b>AIN</b>	Anonymous Identification Number
<b>APAC</b>	Anti-Phishing Authentication Ceremonies
<b>APWG</b>	Anti-Phishing Working Group
<b>HF-APAC</b>	Human Factors in APAC
<b>HPA</b>	Human Perceptible Authenticator
<b>MSMA</b>	MultiStep Mutual Authentication

# Contents

<b>List of Figures</b>	<b>xi</b>
<b>List of Tables</b>	<b>xiv</b>
<b>Chapter 1 Introduction</b>	<b>1</b>
1.1 Research Problem . . . . .	1
1.2 Research Methodology . . . . .	4
1.3 Contributions . . . . .	7
1.4 Thesis Overview . . . . .	8
<b>Chapter 2 Background and Related Work</b>	<b>10</b>
2.1 Introduction . . . . .	10
2.2 Phishing . . . . .	10
2.2.1 Anatomy of Phishing Attacks . . . . .	12
2.2.2 Persistence of Phishing . . . . .	14
2.2.3 Phishing Countermeasures . . . . .	18
2.3 Anti-Phishing Authentication . . . . .	23
2.3.1 User Authentication . . . . .	24
2.3.2 Server Authentication . . . . .	28
2.3.3 Human Perceptible Authenticators . . . . .	28
2.3.4 User Studies of Authentication and Phishing . . . . .	34
2.4 Security Ceremonies . . . . .	37



2.5	Human Communication Processing . . . . .	43
2.5.1	The C-HIP Model . . . . .	44
2.5.2	Human-in-the-Loop Security Framework . . . . .	46
2.5.3	Decision Making and Deception Detection . . . . .	47
2.6	Conclusion . . . . .	51
<b>Chapter 3 Communication Processing in Authentication Ceremonies</b>		<b>55</b>
3.1	Introduction . . . . .	55
3.2	Ceremony Analysis and Phishing . . . . .	55
3.3	Communication Processing . . . . .	58
3.3.1	Analysis of Sample Authentication Ceremonies . . . . .	59
3.3.2	Assumptions and Related Issues . . . . .	60
3.3.3	Influencing Factors . . . . .	62
3.4	Conclusion . . . . .	66
<b>Chapter 4 Human Factors in Anti-Phishing Authentication Ceremonies (HF-APAC) Framework</b>		<b>67</b>
4.1	Introduction . . . . .	67
4.2	HF-APAC Framework in Ceremony Analysis . . . . .	69
4.3	The Framework . . . . .	70
4.3.1	Components . . . . .	73
4.4	Applying the Framework . . . . .	80
4.4.1	Design and Analysis Process of an Existing Ceremony . . . . .	80
4.4.2	New Ceremony Design Process . . . . .	81
4.5	Conclusion . . . . .	82
<b>Chapter 5 Model for Analysing HF-APAC</b>		<b>84</b>
5.1	Introduction . . . . .	84
5.2	The Model Elements . . . . .	85

5.3	Evaluation Methodology . . . . .	88
5.3.1	Hypotheses Development . . . . .	89
5.4	Human Communication Processing . . . . .	94
5.5	Conclusion . . . . .	95
<b>Chapter 6 MultiStep Mutual Authentication (MSMA) Ceremony</b>		<b>96</b>
6.1	Introduction . . . . .	96
6.2	Design Goals . . . . .	97
6.3	Ceremony Analysis Approach and Notation . . . . .	100
6.4	MSMA Setup . . . . .	103
6.4.1	User Training . . . . .	106
6.5	MSMA Operation . . . . .	106
6.6	Security Analysis . . . . .	111
6.6.1	Password Strength . . . . .	111
6.6.2	Assumptions . . . . .	112
6.6.3	Attacks and Countermeasures . . . . .	114
6.6.4	Experimental Evaluation . . . . .	117
6.7	Conclusion . . . . .	120
<b>Chapter 7 User Study for Evaluation of MSMA and the Model</b>		<b>121</b>
7.1	Introduction . . . . .	121
7.2	Design Considerations . . . . .	122
7.3	User Study Design . . . . .	123
7.3.1	Conditions . . . . .	125
7.3.2	Methodology . . . . .	132
7.3.3	Simulated Attack . . . . .	138
7.3.4	Measures . . . . .	141
7.3.5	Statistical Tests . . . . .	144

7.4	Conclusion . . . . .	146
<b>Chapter 8 Evaluation Results</b>		<b>147</b>
8.1	Introduction . . . . .	147
8.2	Study Overview . . . . .	148
8.3	Data Preparation . . . . .	148
8.4	Descriptive Outcomes . . . . .	150
8.4.1	Demographics . . . . .	150
8.4.2	Data Overview . . . . .	153
8.5	MSMA Evaluation Results . . . . .	157
8.6	The Model Evaluation Results . . . . .	160
8.6.1	Reliability of Constructs . . . . .	161
8.6.2	Hypotheses Testing . . . . .	161
8.6.3	Summary of Results . . . . .	171
8.7	Discussion . . . . .	172
8.7.1	MSMA Effectiveness . . . . .	172
8.7.2	Human Communication Processing Principles . . . . .	173
8.7.3	Limitations . . . . .	176
8.8	Conclusion . . . . .	179
<b>Chapter 9 Conclusions</b>		<b>180</b>
9.1	Thesis Summary . . . . .	180
9.2	Contributions . . . . .	183
9.3	Future Research Directions . . . . .	185
<b>Bibliography</b>		<b>186</b>
<b>Appendix A User Study Materials</b>		<b>214</b>

# List of Figures

1.1	Research methodology . . . . .	6
2.1	Phishing email . . . . .	12
2.2	Phishing attack vectors . . . . .	13
2.3	Phishing attack cycle . . . . .	14
2.4	Spear phishing sample [155, 97] . . . . .	17
2.5	Phishing countermeasures . . . . .	19
2.6	Examples of authentication with DSS [55] . . . . .	30
2.7	The Passfaces login screen [174] . . . . .	30
2.8	Security image on a banking website . . . . .	31
2.9	BBMA login screen [86] . . . . .	32
2.10	TwoStep login screen [216] . . . . .	33
2.11	Protocol and ceremony association . . . . .	38
2.12	Human-protocol interaction layers [38] . . . . .	42
2.13	Communication-Human Information Processing (C-HIP) Model [222] . . . . .	45
2.14	The Human-in-the-Loop Security Framework [47] . . . . .	46
2.15	The Theory of Deception fraud detection method [131, 95] . . . . .	49
3.1	A degenerate web authentication ceremony . . . . .	57
4.1	HF-APAC Framework in Ceremony Analysis . . . . .	70
4.2	HF-APAC Framework . . . . .	72

4.3	Design and analysis process of human communication factors in authentication ceremonies with the HF-APAC Framework . . . . .	81
4.4	New ceremony design and analysis process with the HF-APAC Framework . . . . .	82
5.1	The Model evaluation methodology . . . . .	89
5.2	Model for Analysing HF-APAC and hypotheses . . . . .	90
6.1	MSMA ceremony analysis . . . . .	103
6.2	MSMA Setup . . . . .	104
6.3	MSMA Operation . . . . .	108
6.4	Login with MSMA: Step 1 . . . . .	118
6.5	Login with MSMA: subsequent Steps . . . . .	119
6.6	Login with MSMA: the last Step . . . . .	119
7.1	User study overview . . . . .	123
7.2	Login prompt for Ceremony One . . . . .	129
7.3	Login prompt for Ceremony Two . . . . .	130
7.4	Login prompt for Ceremony Three: Step 1. . . . .	132
7.5	Login prompt for Ceremony Three: the first of subsequent Steps. . .	132
7.6	User Study website . . . . .	134
7.7	Simulated attack against Ceremony One: a wrong image is displayed in the attack login screen. . . . .	140
7.8	Simulated attack against Ceremony Two: a set of distractor images shown in the attack login screen does not contain the correct image. . .	140
7.9	Simulated attack against Ceremony Three: a set of distractor images shown in the attack login screen does not contain the correct image. . .	141
8.1	Age and gender count . . . . .	151
8.2	Area and occupation count . . . . .	152

8.3	Frequencies for survey constructs . . . . .	154
8.4	Recall times for ceremonies . . . . .	155
8.5	Recognise times for ceremonies . . . . .	156
8.6	Success rates of the attack per ceremony . . . . .	158
8.7	Differences between ceremonies in detecting the simulated attack . . . . .	159
8.8	H1: Cochran-Armitage association between the Number of login Communication factors and Behaviour . . . . .	162
8.9	H4: Association between Motivation and Elaboration . . . . .	169
8.10	Count of participants and the attack outcome per ceremony . . . . .	174
A.1	Emails sent to recruit participants . . . . .	215
A.2	Notice for bulletin boards to recruit participants . . . . .	216
A.3	User Study Information Sheet 1 . . . . .	217
A.4	User Study Information Sheet 2 . . . . .	218
A.5	Consent form . . . . .	219
A.6	Study home page . . . . .	220
A.7	Study page - Website Tasks . . . . .	221
A.8	Study page - Survey Tasks . . . . .	222
A.9	Help with registering and login screen . . . . .	223
A.10	Registering screen . . . . .	224

# List of Tables

3.1	Behaviour assumptions and related issues . . . . .	61
3.2	Communication processing issues and influencing factors . . . . .	63
4.1	The components of the HF-APAC Framework . . . . .	74
6.1	Logical notation . . . . .	100
6.2	Notation used in describing MSMA ceremony . . . . .	101
7.1	Study conditions . . . . .	126
7.2	Password configurations of the ceremonies used in the study . . . . .	128
7.3	Motivation items . . . . .	143
7.4	Capabilities items . . . . .	144
7.5	Elaboration items . . . . .	145
8.1	Age percentages . . . . .	150
8.2	Gender percentages . . . . .	150
8.3	Area percentages . . . . .	151
8.4	Occupation percentages . . . . .	151
8.5	Survey construct statistics . . . . .	153
8.6	Recall time statistics (milliseconds) . . . . .	155
8.7	Recognise time statistics (milliseconds) . . . . .	156
8.8	Differences between ceremonies in detecting the simulated attack . . . . .	158

8.9	Summary of survey construct measurements and reliability . . . . .	161
8.10	H1: Results of logistic regression predicting being phished by login communication factors . . . . .	163
8.11	H2a: Results of logistic regression predicting Elaboration level . . . . .	166
8.12	H4: Association between Motivation and Elaboration . . . . .	168
8.13	Summary of the Model for Analysing HF-APAC hypotheses results . . . . .	171
8.14	Percentages of participants who entered their password without the right image being displayed . . . . .	173
8.15	Summary of the communication factors and phishing detection rate . . . . .	176



# Associated Publications

Part of the contents of this thesis presents revised and updated versions of the work published in the following papers:

1. Edina Hatunic-Webster. *Anti-phishing models: Main challenges*. In Proceedings of the 3rd International Conference on Internet Technology and Secured Transactions (ICITST-2008), Dublin, Ireland, June 2008.

This paper reviewed and presented the main challenges in tackling the phishing problem (Chapter 2).

2. Edina Hatunic-Webster, Fred Mtenzi and Brendan O'Shea. *Poster: Towards a Model for Analysing Anti-Phishing Authentication Ceremonies*, the 9th Symposium on Usable Privacy and Security (SOUPS). 2013: Newcastle, UK, July 2013.

This poster outlined the Human Factors in APAC Framework (Chapter 4) and introduced the Model for Analysing APAC (Chapter 5).

3. Edina Hatunic-Webster, Fred Mtenzi and Brendan O'Shea. *Model for Analysing Anti-Phishing Authentication Ceremonies*, in Proceedings of 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014), IEEE, London, UK, December 2014.

This paper outlined human communication processing issues within authentication ceremonies (Chapter 3) and presented the Human Factors in APAC

Framework and the Model for Analysing APAC (Chapters 4 and 5).

4. Edina Hatunic-Webster, Fred Mtenzi and Brendan O'Shea. Evaluation of the Model for Analysing Anti-Phishing Authentication Ceremonies. *International Journal for Information Security Research (IJISR)*, 5(1):529-537, 2015.

This journal paper outlined the design of a user study for experimental evaluation of the Model for Analysing APAC (Chapter 7) and MSMA ceremony (Chapter 6).

In addition, an extended abstract was presented at the first annual APWG eCrime Researchers Sync-Up [15] (Chapter 2):

- Edina Hatunic-Webster, Fred Mtenzi and Brendan O'Shea. *Password-Based Authentication and Phishing*, (Extended Abstract), APWG eCrime Researchers Sync-Up. 2011: Dublin, Ireland, March 2011.

# Chapter 1

## Introduction

### 1.1 Research Problem

The focus of this thesis is on the use of security ceremonies as a way of extending the reach of current methods for social, technological and contextual analysis of web authentication schemes and why they do not protect effectively against social engineering threats such as phishing.

Phishing is a form of electronic fraud [128] whose purpose is to obtain confidential information from a victim. Attackers, also known as phishers, use email or other types of communication (e.g. messaging service on social media sites) that trick users into taking an action, which is usually to click on a link to a spoofed website. Phishing attacks spoof the login page of a legitimate, trusted website to steal authentication credentials. In spite of significant legal and technical approaches to fight it, phishing remains one of the main forms of electronic fraud [9, 115] and the number of phishing attacks is still high. According to the Anti-Phishing Working Group (APWG) [11], the total number of reported phishing attacks in 2016 was 1,220,523; and already, up to September 2017, reached 710,350 [10, 13]. As countermeasures are deployed, phishers are modifying their techniques as well.

Human factors, incorrect human trust decisions, play a big role in phishing.

Different to other computer security threats, phishing takes advantage of the way humans interact with computers or interpret messages. Phishers exploit the fact that most computer users do not possess understanding of how computer systems work; they do not pay attention to security indicators or notice the absence of security indicators [57].

The majority of the websites that are spoofed require that users authenticate themselves. Therefore, phishing attacks usually involve spoofing a login webpage and the authentication method used by the service provider. Phishers target the human users and their usage and interpretation of authentication schemes that fools them to make mistakes.

The most common mechanism for online authentication is username and password. Its weaknesses are well researched, but the alternatives offered have drawbacks that means that username/password authentication will stay in use for some time [85]. In the rest of thesis we use the term *password* as any secret knowledge, that may be either character, PIN, graphical, one-time password or their combination. We use the term *text password* to mean a traditional short character string, as used in username/password authentication. In an obvious context, we only use the term password to mean text password.

Security researchers have proposed many alternative anti-phishing authentication schemes that suggest using images for authentication [54, 173, 205, 40]; using digital objects as passwords [148] or sending one-time password (OTP) tokens out-of-band to the user [189, 90]. However, authentication schemes that are more secure require more effort than traditional username/password authentication, both on behalf of the user and the service provider. If security impedes a user's primary task, the user will probably try to avoid the security measures [7].

Although researched extensively, existing and newly proposed anti-phishing authentication schemes still do not adequately protect users against phishing attacks.

When protocols are implemented and used by humans, the underlying assumptions about human-protocol interactions are often susceptible to social engineering attacks such as phishing [57, 123]. The threat analysis and security proofs for these authentication schemes mostly have a technical focus and rarely specifically take into account the human user limitations as a potential threat.

In this thesis, we explore methods to analyse web authentication schemes not only with a technical focus but including the human into the analysis. In particular, we explore the methods to analyse the tasks that users need to perform as part of authentication; how the users process these additional authentication tasks; and how these tasks impact the human decision-making process and decision outcome in determining whether a website login prompt is spoofed or not.

We explore the use of *security ceremonies* as a way of extending the reach of current methods for social, technological and contextual analysis of web authentication schemes. A security ceremony, as described by Ellison [68] is an extension of the concept of network security protocol that includes user interface, human-to-human communication and transfers of physical objects that carry data. It is similar to the conventional notion of a protocol, except that a ceremony explicitly includes human participants as nodes in the network and network links are not limited to traditional communications channels. Radke [182] defines a security ceremony as a protocol in its context of use. Any technique used for network protocol design can be used for ceremony design. A technique for verification of ceremonies is not an agreed and a straightforward process. What is important for anti-phishing research is that a secure ceremony is secure against both normal and social engineering attacks [68]. As phishing is a type of social engineering attack researching the security of ceremonies seems a plausible approach to try to analyse why phishing still works.

The complexity of defining a ceremony comes with modelling a '*human node*' [68], i.e. a user. The modelling of the of the memory and processing performed by human

nodes of a ceremony is an active research area [68, 183, 23, 152, 38]. This thesis fills this gap in the ceremony analysis research with an approach for analysis of the communication processing performed by human users in authentication ceremonies.

The main research questions this thesis explores are:

1. Why current web authentication schemes do not protect effectively against phishing? This question aims at assessing the effectiveness of current anti-phishing schemes through identification of their weaknesses specifically taking into account human factors.
2. How can we use research on ceremonies to improve design of anti-phishing authentication schemes?
3. How to model human communication processing in authentication ceremonies?
4. How to evaluate human communication processing in authentication ceremonies?

## 1.2 Research Methodology

In our approach we use the concept of ceremony to improve analysis of the anti-phishing security of web authentication schemes.

In order to analyse the communication processing performed by users in authentication ceremonies we developed a framework of human factors affecting security of Anti-Phishing Authentication Ceremonies (APAC). The framework, we call *Human Factors in APAC (HF-APAC) Framework*, is aimed to provide insights into human behaviour in the context of web authentication and as a help in the designing authentication schemes with improved phishing resistance. Our review of existing anti-phishing authentication ceremonies and identification of factors affecting human communication processing was a main base for the development of the

Framework components and the relationships between them. By *human communication* we mean human-device (i.e. user interface) communication, as opposed to human-to-human communication, e.g. speech. The framework builds on previous research from the communication processing of security communications and warnings science literature, specifically Cranor’s Human-in-the-Loop security framework [47] and Wogalter’s Communication-Human Information Processing (C-HIP) Model [222]. However, our HF-APAC Framework includes the influence of elaboration which neither the C-HIP model nor the Human-in-the-Loop framework did. Elaboration can be defined as a cognitive process of making conscious connections between the cues observed and prior knowledge, and is important part of deception detection [218, 217, 71, 177].

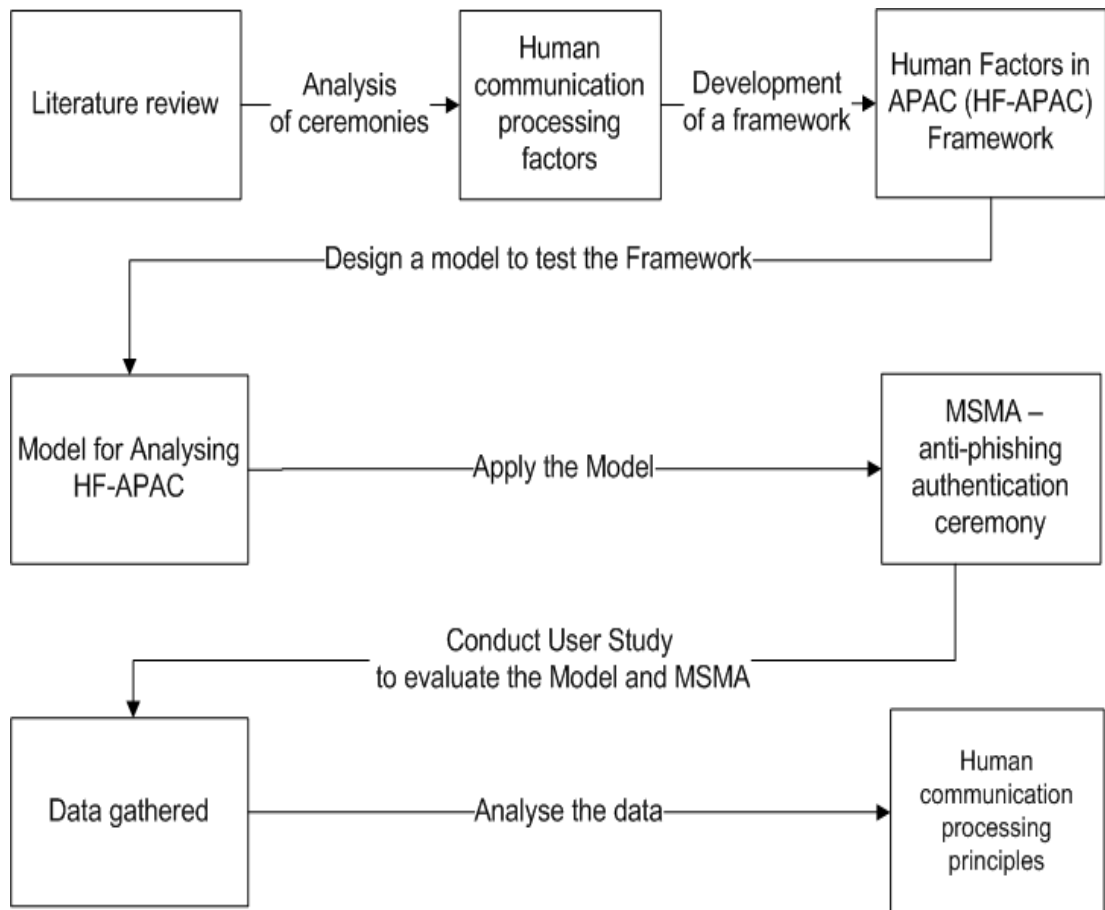
We then designed the *Model for Analysing HF-APAC* that tests the Framework and demonstrates how the Framework can be used. The Model for Analysing HF-APAC is a communication processing model that makes specific assumptions about the components of the HF-APAC Framework and explores to what extent they influence each other. In particular, the Model examines how users process authentication communication tasks and how these tasks impact the user’s decision-making and consequently their phishing detection.

We then applied the Model as part of the design process of a novel anti-phishing authentication ceremony called *MultiStep Mutual Authentication (MSMA)*.

MSMA prototype and the Model for Analysing HF-APAC was experimentally evaluated by a user study we designed, developed and conducted.

The methodology is depicted in Figure 1.1 and summarised as follows:

1. Review existing authentication schemes with regard to human-protocol communication processing affecting their anti-phishing security.
  - Result: Framework of Human Factors affecting security of Anti-Phishing Authentication Ceremonies (APAC)



**Figure 1.1:** Research methodology

2. Apply the HF-APAC Framework

- Result: Model for Analysing HF-APAC proposing human node communication processing principles for improving phishing resistance of authentication ceremonies.

3. Apply the Model

- Result: MultiStep Mutual Authentication (MSMA) anti-phishing authentication ceremony.

4. Evaluate the Model and the Ceremony

- Revise the human node communication processing principles.



## 1.3 Contributions

The contributions of this thesis investigate how the concept of ceremony and human communication processing can be used to improve the anti-phishing security of current authentication schemes. We also contributed to the understanding, design and analysis of security ceremonies by providing a way to model communication processing performed by human nodes. We used a multidisciplinary approach where we make use of concepts and ideas from different areas such as phishing, web authentication, human factors in authentication, information processing and decision making; and combine it with ceremony research.

The main contributions of this thesis are the following:

1. *An exploration into the use of security ceremonies in addressing the phishing problem.* We enhance the understanding of security ceremonies by demonstrating modelling of communication processing performed by human nodes in authentication ceremonies with a framework and a model.
2. *Design and analysis process of human communication factors in authentication ceremonies and its demonstration.* The suggested process comprises a framework, a model, a novel anti-phishing authentication ceremony, and a user study.
3. *A framework of human factors in anti-phishing authentication ceremonies.* We contributed the Human Factors in Anti-Phishing Authentication Ceremonies (HF-APAC) Framework that can be used by authentication scheme designers to address human factors affecting anti-phishing security of authentication ceremonies [105, 106].
4. *A model that proposes human communication processing principles in authentication ceremonies and demonstrates the usage of the HF-APAC Framework.*

We contributed the Model for Analysing HF-APAC [106, 107], a model of human communication processing in authentication ceremonies. The Model proposes human communication processing principles that can be used to improve the phishing resistance of authentication ceremonies.

5. *An anti-phishing authentication ceremony.* We contributed the MultiStep Mutual Authentication (MSMA) [107] ceremony that uses a HPA to allow a user to verify that the website that he/she is accessing is legitimate, helping to mitigate phishing attacks.

A user study [107] was conducted to evaluate the Model for Analysing HF-APAC and MSMA. We find that the principle of increasing the number of recall and recognise communication factors, as used in MSMA, improves the phishing resistance of a ceremony.

## 1.4 Thesis Overview

The first person plural voice (we) is used in this thesis to reflect the fact that the research was conducted by me under the supervision of my thesis advisers. The rest of the thesis is organized as follows:

- Chapter 2 provides background and related work for the topics covered in the thesis. These include phishing and anti-phishing countermeasures, web authentication solutions, ceremonies, human factors in authentication and information processing and decision making.
- Chapter 3 provides an understanding of ceremony design and analysis. It also explores assumptions and related issues about behaviour of humans who are expected to process and react to security-related communication in online authentication protocols.

- Chapter 4 presents the Human Factors in Anti-Phishing Authentication Ceremonies (HF-APAC) Framework. It also presents design and analysis process of human communication factors as a way of applying the Framework.
- Chapter 5 presents the Model for Analysing HF-APAC that demonstrates the usage of the Human Factors in APAC framework by a ceremony designer and suggests human communication processing principles for improving phishing resistance of authentication ceremonies.
- Chapter 6 presents the MultiStep Mutual Authentication (MSMA) Anti-Phishing Ceremony. We designed MSMA to show how the Model can be applied.
- Chapter 7 presents the design of a user study conducted to evaluate the Model for Analysing HF-APAC and MSMA ceremony.
- Chapter 8 describes data analysis and presents the results of the user study.
- Chapter 9 contains summary, conclusions and future research directions.

# Chapter 2

## Background and Related Work

### 2.1 Introduction

The research in this thesis investigates the use of security ceremonies as a way of extending the reach of current methods for social, technological and contextual analysis of web authentication schemes and why they do not protect effectively against social engineering threats such as phishing. The research builds upon the results of multiple research areas: phishing and phishing countermeasures; anti-phishing authentication; security ceremonies and human communication processing and decision making. In this chapter we review notable examples from each area.

### 2.2 Phishing

The security of the web is proving difficult to achieve, as the human user is not able to effectively establish the legitimacy of the server with which his/her browser is interacting [232]. Felten et al. [74] introduced the term 'web spoofing' as far back as 1997 and showed how a malicious site could forge many of the browser security indicators that humans use to determine a website's identity. Phishing, often referred to as *web spoofing*, became a real problem nearly a decade later and

still remains one of the main forms of Internet fraud [9, 115].

Nowadays, the term phishing pertains to not only obtaining user account details, but also obtaining access to personal and financial data of any web user by actively impersonating an online e-commerce, financial or social media institution. Phishers try to obtain credit-card numbers, national identification numbers, account details, for the purpose of identity and money theft and fraud, and also for corporate espionage and similar criminal activities. Phishing attacks target both organisations and their customers.

The estimate of financial losses stemming from phishing attacks vary [108, 154, 188] and are not easy to quantify. According to the 2016 Financial Fraud Action UK report [79] online banking fraud increased to £133.5 million (64% increase on 2015) and could be attributed to criminals using social engineering scams such as phishing and vishing in combination with malware attacks.

Phishing has spread beyond financial institutions to other areas, retailers and service-oriented companies such as cloud organizations, travel, insurance, government [9, 187], web-based email providers, social media sites [160, 9], and even massively multiplayer games [200]. As a result of the growing problem of phishing and email spoofing an Anti-Phishing Working Group (APWG) was formed. APWG is a global industry, law enforcement, and government coalition focused on unifying the global response to cyber crime [12].

The number of attacks is still high. In the 1st half of 2017, the APWG estimated over 590,000 unique phishing emails and over 291,000 unique phishing websites. The European Union Agency for Network and Information Security, that provides recommendations for cyber security in Europe, also reported concerns on the further rise of phishing in 2017 [70].

## 2.2.1 Anatomy of Phishing Attacks

Phishing emails are only a small part of the overall phishing economy and the only aspect seen by most people. The Figure 2.1 shows a sample of a phishing email.

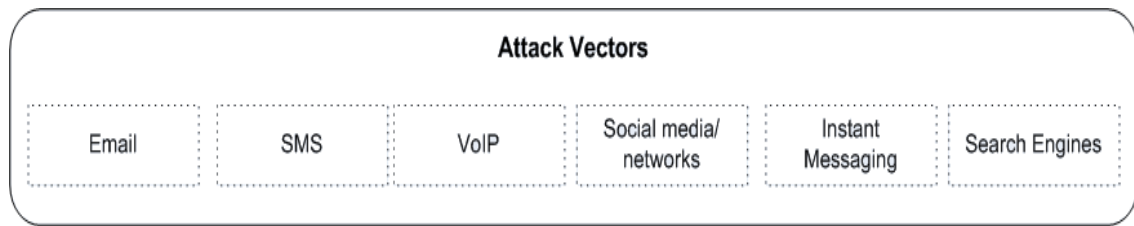


Figure 2.1: Phishing email

Instant messaging (IM), Voice over Internet Protocol (VoIP), Short Message Service (SMS), search engines, social networks and other ways of communicating are also used for sending attacks, as shown in Figure 2.2. In the rest of the thesis we only refer to emails as a communication used to trick people into visiting spoofed websites.

All phishing attacks fit into the same general information flow. Hence, a typical phishing attack can be divided into three major stages [115], depicted in Figure 2.3:

1. Preparation and delivery of phishing attack



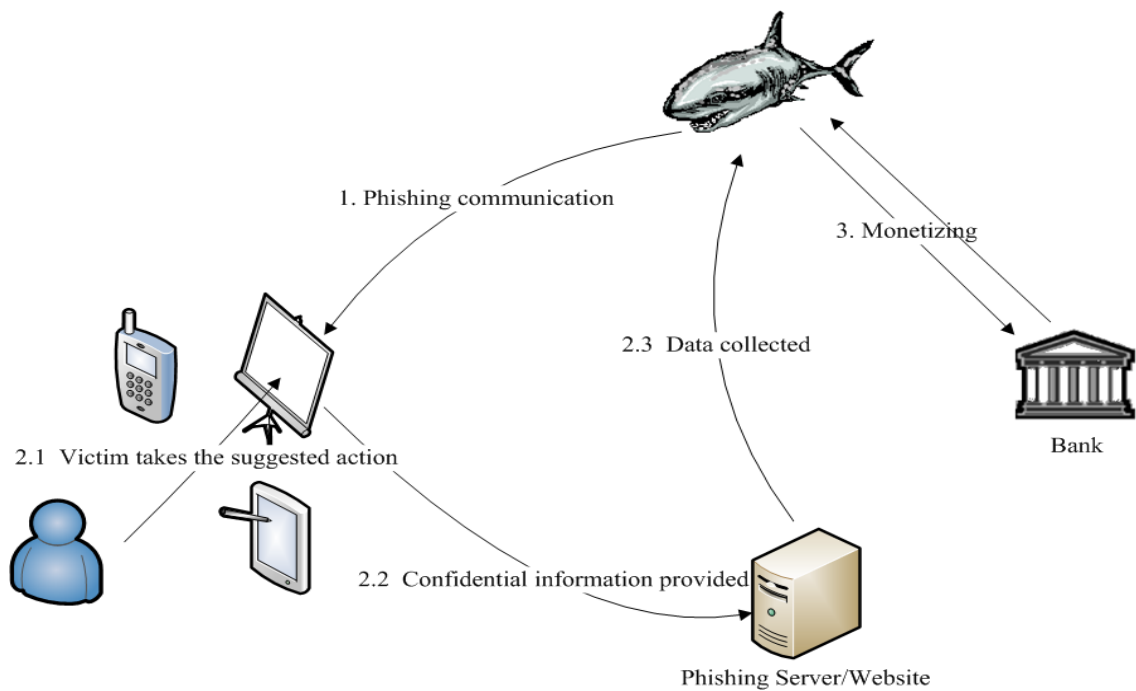
**Figure 2.2:** Phishing attack vectors

2. Victim taking the action suggested in the phishing communication
3. Monetizing stolen information

**Preparation and delivery of phishing attack.** The first stage involves the preparation of infrastructure, e.g. fake website, used to perform the attack and collect stolen information; and the preparation of attack communication e.g. email, voice, text, attachment. A phisher does not need specialized knowledge to send out the emails or create fake websites. He/she only needs to acquire the right tool to perform the mass communication. The toolkits that create a copy of legitimate websites and collect stolen credentials are available to buy within the phishers community. They can create a complete phishing site ready to be deployed on a public web server [46]. If corrections are needed, skilled web designers who advertise on fraud-related forums are available for hire. Abad [1] defines the phishing marketplace as a loosely-connected group of forums where participants can trade goods, services and money. The key goods in the phishing market place are credentials.

**Victim taking the suggested action.** In the second stage, the user - becoming a victim, takes the action suggested in the phishing communication and provides confidential information to the phisher. Typically, the email directs the user to a fake website where credentials are entered on spoofed login web pages (i.e. server) on behalf of the attacker. The stolen data is collected or sent to an attacker quickly, to avoid the phishing site being taken down. The average uptime of phishing sites has reduced to about 24 hours [16].

**Monetizing stolen information.** In the last stage, phishers make use of collected information, i.e. cash or monetize it. The cashing is done by withdrawing money online, taking out cash advances, or making purchases of goods and services on the accounts. In other cases, the cashing is further masked by stealing credentials for online games or social networking sites. For example, for online games, criminals might transfer all of a victim’s virtual gold to an accomplice and then sell the stolen gold to other players for real money. On social networks it may involve notifying the victim’s friends that that person is in trouble and needs money fast.



**Figure 2.3:** Phishing attack cycle

### 2.2.2 Persistence of Phishing

As technical countermeasures were deployed in response to phishing, the criminals began introducing new techniques as well, and the arms race is still ongoing. The problem is that most phishing attacks also use social techniques to attack people using technology, rather than attacking technology itself. For example, users accept



to fill out a survey for a bank in return for a small amount of money; and at the end of the survey they need to give their account number to deposit funds into [115].

Phishing is adapting to new technologies and the way we use them and the attacks are becoming more pervasive. Phishing through *social media* has been reported as well [160, 96, 99].

*Vishing* is a type of attack that exploits the proliferation of VoIP [213, 206]. Phishers either use a voice call to lure users to divulge confidential information or a fraudulent phone number, sent in an email or other communication. Upon dialling the provided phone number the user's personal data is taken.

In *SMiShing* [146] the attack is delivered via text messages requesting the recipient to click on a link or provide credentials in a text message reply. The text may inform the user that his or her bank account has been compromised or credit card has been deactivated. The user is directed to call a number or go to a spoofed website to reactivate the card. The reactivating card is then performed on the site, or through an automated phone system, where the victim is asked for card, account and PIN numbers.

*Malware based phishing* tricks users in different ways to install malware on their computers. Regarding their use in phishing, Gupta [126] divides malware programs into two categories: those that reside on the victim's computer to extract sensitive information (spyware, adware, keyloggers, trojans); and those that help to propagate the first category of malware on behalf of the phishers (worms and viruses). Malware-based phishing attacks can be performed either using deceptive email attachments (e.g. greeting card or screen saver) or by social engineering where people are lured to download a file from a fake website. Apart from the advertised functionality, the attachment contains an executable program that intercepts future communications between the victim's computer and a legitimate institution.

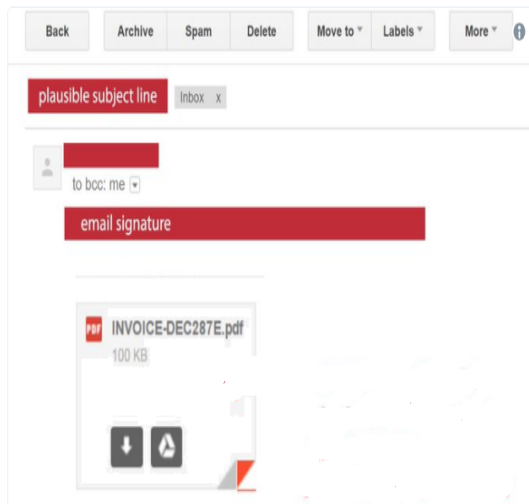
*Pharming* attacks [203] redirect users to phishing websites by compromising the

Domain Name System (DNS) infrastructure so that DNS queries for the victim site's domain return a phisher-controlled IP address. In this attack the browser's Uniform Resource Locator (URL) displays the domain name of the website the user wanted to visit.

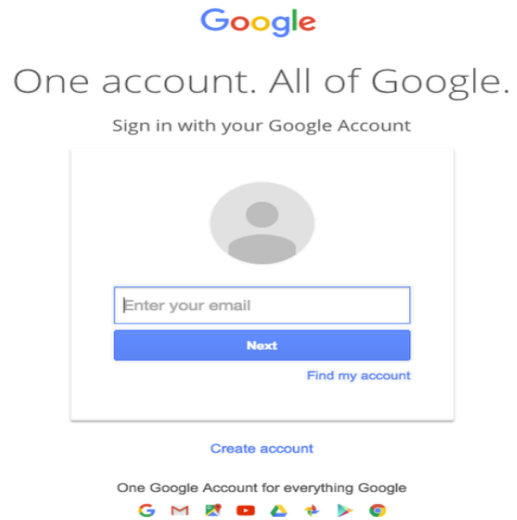
*Search engines* can also be used to deliver phishing attacks [126]. Phishers create web pages for fake products, or advertise fake banks offering an interest rate slightly higher than any real bank. When the user 'discovers' these attractive banks via a search engine, he/she will be asked to enter their bank account credentials for 'balance transfer' to the new 'account'.

*Context aware phishing.* Criminals are increasingly using more sophisticated, *context aware* [122] or *spear-phishing* [120, 115, 28] attacks, which targets a specific user and their organisation with knowledge of his or her information. In the latest version of context aware attacks an attacker sends an email appearing to come from a trusted sender containing an attachment, a PDF document (Figure 2.4a). This attachment is really an embedded image that has been crafted to look like a PDF document. When clicked on, instead of revealing a preview of the document the embedded image links to a fake Google login page [97, 155]. The user may think he/she needs to provide credentials to read a confidential document. The Figure 2.4b shows a spoofed Gmail login page displayed to a user that clicked on an embedded email attachment. The page looks the same as the Google login page at the time of the attacks, apart from a difference in URL. *Whaling* is a special form of spear-phishing that focuses on senior management in companies or government representatives or corporations, or of high net-worth individuals [8].

These types of context-aware phishing attacks are getting easier to launch with so many data security breaches reported in various organisations [96, 78, 196]. According to Symantec [207], at the end of 2015, the total publicly reported number of exposed records was 191 million and 429 million of exposed identities. Unfortu-



(a) Phishing email with an image link, disguised as a PDF attachment



(b) Spoofed Gmail login page

**Figure 2.4:** Spear phishing sample [155, 97]

nately, companies are not reporting the full extent of their data breaches. Symantec estimates that the real number of exposed records is more than half a billion [207].

### 2.2.2.1 Visual Deception

Phishers use visual deception to spoof websites, mimic legitimate emails, windows, text, images or security indicators [57, 56, 126, 74]. Even experienced users can be tricked by visually deceptive text used in URLs (i.e. URL obfuscation [143]); windows and text masking underlying web pages and producing deceptive look and feel [52, 220, 226]; or looking the same as a 'secure login' page [127]. Examples of phishing techniques that has been recorded to directly exploit visual deception [52] are described bellow.

**Windows masking underlying windows.** During this attacks phishers place an illegitimate browser window on top of a legitimate window, or near it. If the windows have the same look and feel, users may be tricked to believe that both

windows are from the same website [52]. A variation of this technique is so called picture-in-picture phishing attacks, that can place an image of a web browser in the content area of a web browser [119, 57].

**Similar name attack [143, 226, 57, 115].** Homograph attacks exploit the visual similarity of characters. For example, a website that is hosted at 'bankofthevest.com' with two 'v's instead of a 'w' in the domain name [57]. Even simpler schemes are used successfully by the phishers, e.g. attackers can use a hostname that bears a superficial similarity to the imitated website's hostname, for example 'paypal.com.mysite.com' [226].

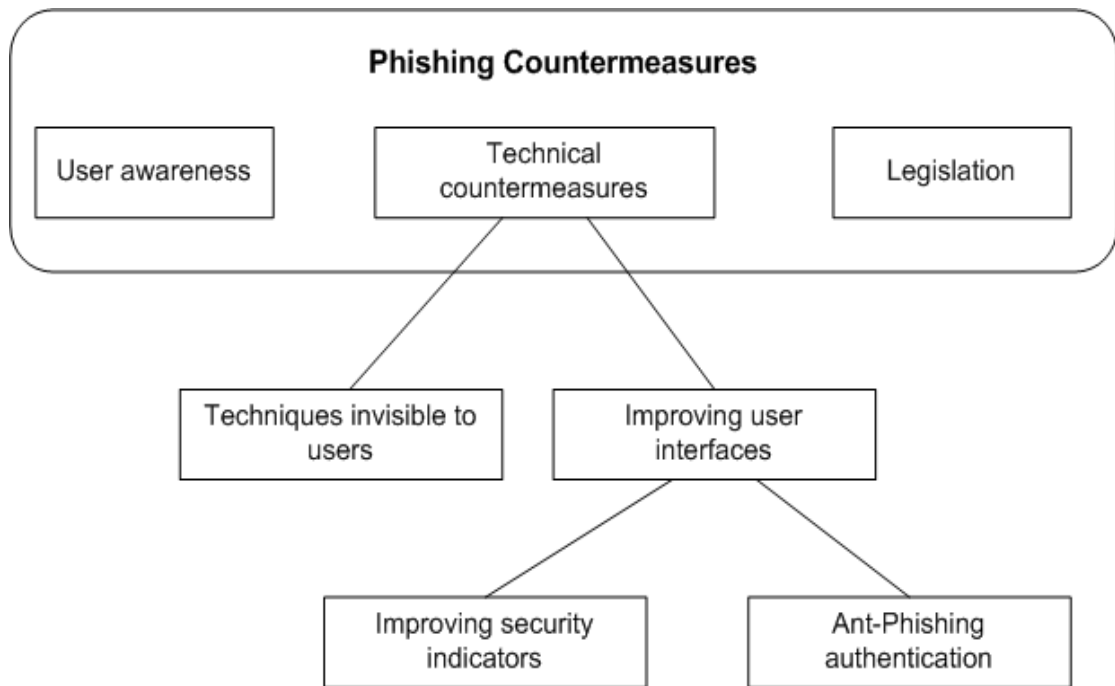
**Deceptive look and feel.** Phishers can create phishing websites that look like legitimate websites, with logos, images and look and feel identical to the legitimate website. [52, 74, 126]

**Images mimicking browser chrome.** Many people cannot differentiate between the browser chrome, which can usually be trusted, and the browser content, where attackers can show anything [115]. This has been exploited to spoof login prompt web pages. As the spoofed image looks exactly like a real login prompt, a user can be tricked to submit login credentials to a spoofed website [52, 144, 110].

### 2.2.3 Phishing Countermeasures

Current capabilities to investigate phishing, identify perpetrators, present evidence and convict criminals are still inadequate. An integrated approach on multiple levels is needed to mitigate phishing effects. Technical and non-technical measures need to be combined to reduce the success rate of phishing attacks [103]. Therefore, research of phishing problem spans into diverse areas such as social psychology, human computer interaction, machine learning, economics, public policies and law enforcement and user training [115].

The countermeasures can be broadly categorised as follows, depicted in Figure



**Figure 2.5:** Phishing countermeasures

2.5:

1. User awareness
2. Legislation
3. Technical countermeasures

### 2.2.3.1 User Awareness

Training users to enhance their awareness of phishing attacks is an important strategy for phishing protection. Most security experts agree that user awareness about Internet and general computer security, not just phishing, should be improved. There is disagreement among researchers on whose responsibility this should be, i.e. whether it is the operating system manufacturer's, product producer's or the institution's whose websites are used, or if the user himself should be responsible for it. Some, like Lininger [145], argue that it is unrealistic to expect users to teach

themselves something that they are not interested in. For most users, the Internet is just a tool to play a game or to access the bank.

Most websites, companies and government agencies provide guidelines and security advice on phishing and other online safety rules [84, 214, 3, 19]. For example, both eBay and Amazon specifically advise their customers how to recognise if their respective website (or email) is spoofed [62, 6]. Previous studies [141] found that this way of educating users is good if you can get users to read the training material. This can be difficult to achieve as security is never the users' primary goal [221].

Notable examples of specific training tools developed are: PhishGuru [141, 140] that uses simulated phishing attacks to train users; Anti-Phishing Phil [199], an online game that teaches users to identify phishing web sites; 'Smells Phishy?' [20], an educational board game that raises users' awareness of online phishing scams.

APWG was formed to raise awareness about cybercrime and phishing in particular and it also provides educational material. The APWG landing page [14] teaches consumers online safety when they have just accessed a link in a phishing communication.

### **2.2.3.2 Legislation**

Phishing is a multinational crime. According to APWG [10] the top ten phishing sites hosting countries in the first half of 2017 were: United States, Brazil, Ireland, Canada, Germany, France, Czech Republic, Argentina, Netherlands and the Virgin Islands. The phishing victims are not necessarily based in the same country as the attackers. In order to prosecute and stop the phishers international cooperation must be achieved, and that makes the law enforcement task even more complex.

In response to blacklisting and takedowns anti-phishing techniques, the criminals adapt their techniques as well. Phishers move fake websites from one server to another, perhaps in a different country, very quickly. Some use a large number of

proxies and domain names to hide their true location [159, 156].

There is no shortage of laws applicable to phishing [215, 169, 212, 102] but the number of phishing prosecutions is very low. Some of the reasons are [161]:

- Many victims of phishing are slow to discover that their information has been compromised. By the time they discovered it, the perpetrators/phishing website, has been moved.
- Phishing is a multinational crime. Most of the countries impose constraints on information sharing.
- Not enough resources. Investigators need to keep up to date with the evolving phishing techniques. Sufficient funding is still lacking in both the public and the private sector for the continuous training, hardware and software, and other tools necessary to keep up with the phishers.
- Number of people involved in phishing. Different people may be involved in different phishing phases and they even may be located in different countries. Differences in language, laws, and legal procedures make it very difficult to conduct criminal investigation, especially as most countries pick and choose legislation they want, and are concerned of too much information sharing.

### **2.2.3.3 Technical Countermeasures**

As our focus is on human factors in phishing, we categorise technical countermeasures from the user's point of view as follows:

1. Automated phishing detection techniques - invisible to users.
2. User interface improvement - offering more protection or helping users make better security decisions [115].

Improving user interfaces spans the following areas:

- Security warnings
- Indicators for verifying legitimacy of websites
- Anti-phishing authentication

Since the anti-phishing approach we propose in this thesis falls in the *improving authentication techniques*, we will focus on that in Section 2.3. We will now only give a brief overview of other technical countermeasures.

### **Detecting phishing via automatic techniques**

In order to prevent the phishing email ever reaching the intended recipient specific anti-spam phishing filters are deployed at email servers. Heuristic solutions look for specific techniques used by phishers, such as encoding the name of a financial institution in the local part of a URL and using IP addresses as the host part of the URL. Heuristic schemes perform quite well against phishing, especially if the solutions are specifically designed to detect phishing attacks [77]. Fingerprinting schemes work by comparing known samples of phishing messages against incoming email [147].

PhishTank [179] is a collaborative anti-phishing site that allows to submit, view or confirm phishing URLs. Microsoft and Google also operate anti-phishing that blacklists URLs manually verified as phish. Once verified and blacklisted, phishing websites can be taken down. Finding the actual server hosting the phishing site needs to be done fast, as phishers move their websites from one server to another very quickly. Moore and Clayton [159] showed that phishers are improving their phish sites architecture to allow them to be moved very quickly.

### **Improving user interfaces**

Users rely on indicators used in the non-digital world, i.e. the logo, and familiar look and feel to decide if a website is legitimate. To make the problem even worse,



users are not aware how easy is to create a webpage that looks nearly the same as the legitimate webpage. As a help, most browsers nowadays include blacklists based phishing warnings; Internet Explorer with Microsofts blacklist; Firefox and Chrome integrates Google’s blacklist and safe browsing [91]. Users only need to notice and interpret the warnings.

Browser indicators such as location bar information and certificate information, also tell the user whether to trust a server and identify what site they are on. Empirical studies have been performed to examine effectiveness of these security indicators. These studies have shown that many users ignore security warnings [65, 236, 57, 226]. Even if the user pays attention to these indicators, Ye et al. [231] showed how easily they can be forged.

Extended Validation (EV) certificates were introduced to indicate that the company purchasing the certificate is legitimate. They use colour-coding of the browser’s address bar. Green browser navigation window indicates an authentically validated site. The brand name of the organization that owns the Transport Layer Security (TLS) protocol certificate and the issuing authority are also shown. It turns red for an untrustworthy site. However, Jackson et al. [119] found that EV certificates were not effective in protecting users against picture-in-picture or the homograph phishing attacks.

## **2.3 Anti-Phishing Authentication**

Improving the authentication mechanisms is another approach to the phishing problem, complementary to improving phishing indicators and warnings.

In this section we mention notable examples of knowledge-based web anti-phishing authentication schemes relevant to our research, but do not attempt to survey the entire field. As our newly proposed ceremony combines text, PIN and graphical

passwords, we will review them in more detail than other authentication techniques.

Our focus is on knowledge-based authentication (KBA). Knowledge-based authentication can be defined as a process in which a human entity authenticates itself by proving the knowledge of some secret that was previously shared with the party requesting the authentication [48]. In this definition we include all authentication systems that require users to remember a secret; the user may choose to rely on writing the secret down or remembering said secrets. Our research excludes the biometric [121], token-based [167] and key-based authentication systems where secret keys are not stored or memorised by a human.

We specifically concentrate on text and graphical password authentication schemes. We also review in more details the schemes that were used as a base for the implementation of ceremonies used in our user study (Chapter 7): Browser-Based User-Aware Mutual Authentication [86] and TwoStep [216]. As our proposed MSMA ceremony is based on Delayed Password Disclosure (DPD) [127] we describe it in more detail as well.

### **2.3.1 User Authentication**

The most common mechanism for user authentication is a username and text password. In most cases, the user's password is sent after the secure, encrypted connection to the server is established via TLS. TLS is an updated version of Secure Sockets Layer (SSL). TLS uses Public Key Infrastructure (PKI) certificates to authenticate the server, i.e. websites, by installing trusted certificates on client's browsers. The weaknesses of text password authentication are well researched, but the alternatives offered have weaknesses that mean that username and password authentication will stay in use for some time [85, 109].

Another widely used and persisting type of authentication are Personal Identification Numbers (PINs). PINs are passwords that consist of only digits and were

initially used for systems with mainly numeric input, e.g. at Automatic Teller Machines (ATMs). In spite of well known weaknesses, small password space and memorability problems [7], they also continue to be used. They have also been widely adopted as a password choice for mobile phones and chip and PIN credit card transactions.

Alternative authentication schemes suggest using two-factor authentication; sending one-time password (OTP) tokens out-of-band to the user [158, 90]; introducing variations of Password Authenticated Key Exchange (PAKE) protocols [118, 176]; or using graphical passwords [40, 205, 216].

**Two-factor authentication.** For two-factor authentication, the user is required to satisfy two criteria in order to prove its identity. As phishers normally hold only a password as a means to impersonate a user (as one criteria), as long as the second criteria/token is safe, the phisher will not be able to impersonate the user. Most two-factor authentication schemes use shared secrets, tokens (USB token devices, smart cards, or password-generating tokens) [189, 90] or biometrics. Shared secrets are questions that are asked during the authentication process, which a fraudster would be unlikely to be able to answer. The most widely used form of two-factor authentication is when withdrawing money using an ATM, where the user must present both an ATM card (something the person has) and a password or PIN (something the person knows).[73]

Another widely deployed second-factor authentication mechanism is the use of one-time password (OTP) tokens.

**One-time passwords.** In response to phishing, banks, governments, and other institutions are deploying one-time passwords (OTP), i.e. passwords that are valid for only one login session or transaction. Using OTP as a second factor has been suggested and adopted by many commercial institutions (RSA SecurID [189]). OTP tokens can be sent out-of-band to the user, for example as an SMS to the user's

phone, e.g. Google Gmail [92]; in the form of transaction numbers (TANs) - adopted by various banks, or quite recently, combining with graphical passwords [45]. OTP tokens are devices that generate random passwords that are only valid for a single use, hence limiting the amount of damage should the password be intercepted by a phisher. Also, for time-based tokens, the generated OTP is only valid for a limited, short time period, requiring a phisher to act immediately. In organised phishing schemes, where collected passwords are sold to other parties, use of OTPs would protect the user.

Paterson in [176] considers the use of one time passwords in the context of PAKE, which allows for mutual authentication, session key agreement, and resistance to phishing attacks.

**Password Authenticated Key Exchange (PAKE).** PAKE research explores an alternative approach to protecting passwords without relying on a PKI. PAKE schemes only require that a human memorable secret password is shared between the participants. Using PAKE by itself does not protect against phishing, as keyloggers can record the password. Also, if PAKE is to be used for web authentication both server and client side need to be changed and must participate in the PAKE protocol. Some of the PAKE anti-phishing protocols employ zero-knowledge authentication, which is a practical application of the concept of a zero-knowledge proof (ZKP). In a zero-knowledge proof, one party can confirm whether or not a statement is true without revealing any other property about the statement. Others combine it with TLS. The deployment problem with these schemes is the high computation cost. [104]

**Graphical passwords.** Graphical passwords is another notable user authentication type that has been researched as an alternative to text passwords. Graphical passwords can be defined as knowledge-based authentication mechanisms where images or sketches are used as a pre-defined secret between the user and the server

[30]. Graphical authentication schemes usually ask users to perform some kind of image-based task to login. The main advantages of using graphical schemes as an alternative to textual passwords are as follows:

- Increased memorability - they utilise the psychological finding that the human's ability of remembering images is far superior than remembering text [171].
- Easier to use on smaller or touch screen devices.

Graphical schemes can be classified into three categories [30]:

1. *Recognition-based*: In recognition-based graphical passwords, users need to recognise and then select a set of correct images from a larger set, e.g. [173].
2. *Cued-recall*: In cued-recall, the images cue the user, for example, to click a set of points on an image, e.g. [205, 40].
3. *Recall-based*: In recall-based, users are required to recall a password without any cues, such as drawing a doodle in Draw-A-Secret (DAS) [130, 209].

A number of graphical authentication schemes have been proposed [148, 41, 205, 101, 54]. Everitt et al. [72] studied multiple graphical passwords in a real usage situation, i.e. where users have multiple graphical passwords and they use them infrequently. Their study shows that the time required to authenticate can be significantly impacted by frequency, interference, and training even when the failure rate is not. They suggest that the design of systems that utilise graphical passwords in applications needs to take into account realistic estimates of the time that will be required to authenticate using a particular graphical password system. However, Stobert and Biddle [205] found that authentication schemes leveraging both recall and recognition memory have good memorability and also that login times were faster than in schemes utilising only recognition-based graphical password.

### 2.3.2 Server Authentication

The success of phishing can be attributed to the user's inability to authenticate a website. i.e web server. Most e-commerce financial institutions use TLS certificates for server authentication and rely on trusted third parties to authenticate certificates. In spite of this, phishers succeed in taking users to the spoofed websites, as certificates can be acquired by any party including phishers. Tan and Teo [208] and Clayton [43] pointed to the limitations/weaknesses of the current SSL protocol and its inefficiencies against phishing attacks. TLS weaknesses have been reported as well [201, 138].

### 2.3.3 Human Perceptible Authenticators

In this section we review authentication schemes that provide mutual authentication between a user and a server using a Human Perceptible Authenticator (HPA); a HPA allows the human user to authenticate the server. Mutual authentication refers to a process or technology in which both the server and the client authenticate each other.

Gajek et al. [86] introduced the term HPA as an item the user has to recognise to identify the server. The HPA can be anything, e.g. an image, video, or audio sequence, such as voice recording; a piece of music or excerpt from a book. Unlike certificates, authentication with HPA is more familiar to users as a way of identification in the physical world where identities are provided in an easy, human recognizable form.

A *trusted path* is a protected channel that provides the secrecy and authenticity of communication between the user and the program with which the user intended to communicate. A trusted path between a browser and a server is in general established via TLS and PKI. Jakobsson [126] pointed out that the notion of trusted path is very relevant to defend against phishing and an effective way of combating

phishing must involve establishing a trusted path between a user and a server.

The establishment of trusted path usually involves extra shared secrets between the user and the server. The problem is that while using more complex shared secrets increases security, it decreases usability of the resulting interface [113].

A number of systems have been proposed that address the phishing problem by creating a trusted path between the *user interface* and the *user* by using mobile phones, being variations of the original proposal by Parno et al. [172]. There have also been a number of investigations to determine how to establish a trusted path between the *user* and the *browser* [232, 69, 86].

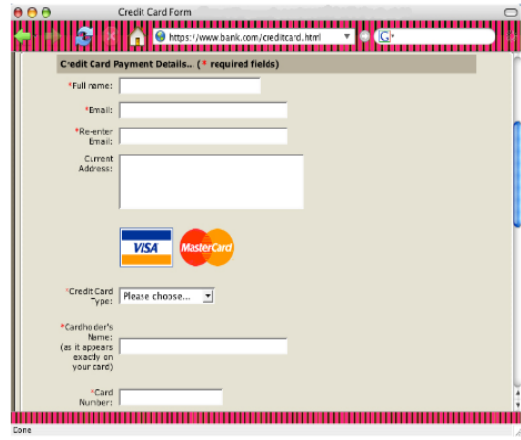
Our focus is on authentication schemes that provide a trusted path between the user and the server using images as a type of HPAs. Dhamija proposed Dynamic Security Skins (DSS) [55], a scheme that allows establishment of a trusted path between the *user* and the *password window* with the user recognising a photographic image only known to the user. DSS use a randomly generated visual hash to customize the browser window to indicate the successfully authenticated sites. Examples of authentication with DSS where the trusted password window displays the randomly generated image; and the image as a border around the authenticated website, are shown in Figure 2.6.

Passfaces [174] is a commercial recognition-based system that assigns each user a set of three faces. To log in, users are shown a different arrays of nine faces multiple times, as shown in Figure 2.7. The user must select the face that is part of their assigned password. To improve security and reduce predictability, Passfaces assigns a random set of faces as a password. A study by Hlywa [111] found that using either houses or other objects instead of faces in schemes equivalent to Passfaces increased the memorability.

**Security images.** Security images are a type of graphical authentication scheme that has been used by internet banking and other websites as a part of the login

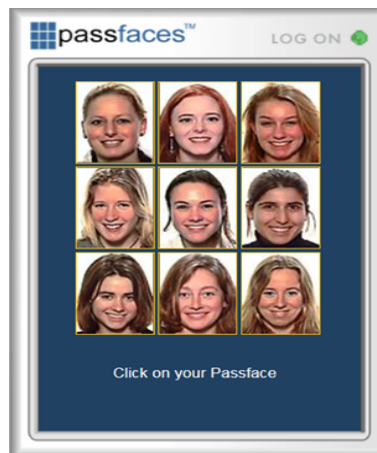


(a) Password window



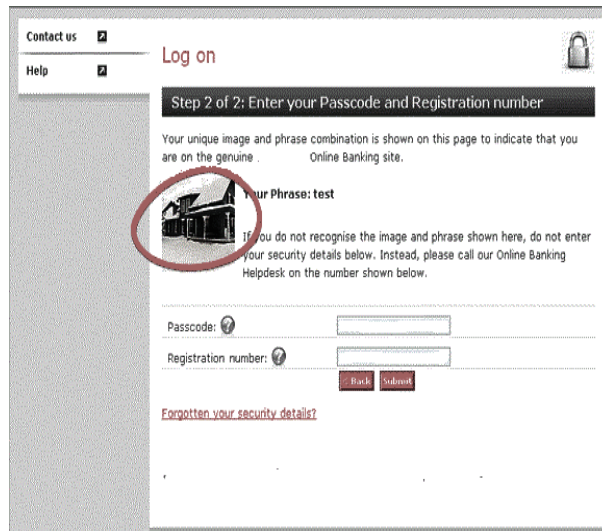
(b) Authenticated website

**Figure 2.6:** Examples of authentication with DSS [55]



**Figure 2.7:** The Passfaces login screen [174]





**Figure 2.8:** Security image on a banking website

process as a help to prevent phishing attacks [18, 192, 180, 192, 228]. Security images are usually combined with a phrase or caption as shown in Figure 2.8. They are used for server authentication, rather than user authentication. In order to prove its identity to the user on logins, the server displays the security image chosen at the time of registration. Some studies have shown that website authentication security images are not very effective in protecting users, prompting some well-known banks to remove them [234, 149, 181]. Schechter et al. [194] have shown that 92% of users entered their account passwords even though their site-authentication images were absent, in spite of being instructed not to do so. Lee et al. [144] got quite similar results exploring whether users will login when the security image was replaced with an 'under maintenance' image.

### **Browser-Based User-Aware Mutual Authentication**

Gajek's et al. proposed Provably Secure Browser-Based User-Aware Mutual Authentication (BBMA) over TLS [86]. BBMA specifically considers the user and the browser as protocol participants, and tie the user's authentication to the TLS secure channel. The server identifies the browser on the basis of client certificates, ensuring that the server establishes a secure channel to the browser. However, it does not au-

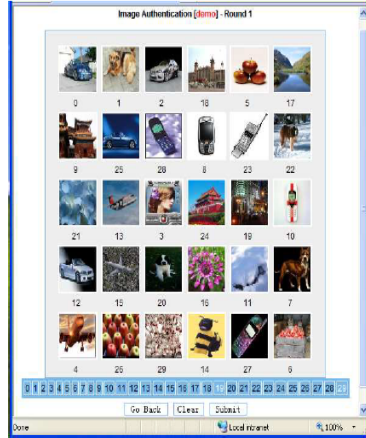


**Figure 2.9:** BBMA login screen [86]

thenticate the user. In order to prove its identity to the user, the server sends a HPA [86, 185], e.g. a personal picture or a voice recording (Figure 2.9) that was chosen during the registration. The user has to recognise the authenticator at the login. Verification of server certificates (and the underlying public key infrastructure) and any security indicator (e.g. URL, padlock) is irrelevant. The user is authenticated to the server via a text password.

### **TwoStep Authentication**

TwoStep [216] is a hybrid user authentication scheme that combines text passwords and recognition-based graphical passwords in a two-step process. In *step one*, a user is asked to supply the username and text password. After this, even if the username/password combination is not correct, in *step two*, the user is presented with an image portfolio, an example of which is shown in Figure 2.10. The user must correctly select the images previously selected at the time of registration in each round of graphical password verification. If the selection is not correct, access is denied despite a valid text password. Both the text password and all graphical passwords must be correct for a successful login. The TwoStep scheme may be implemented in different ways according to a specific graphical password policy with regard to: number of rounds of verification; display layout; number of images to be selected in each round; an ordered or unordered image selection.



**Figure 2.10:** TwoStep login screen [216]

### Delayed Password Disclosure

Jakobsson and Myers introduced Delayed Password Disclosure (DPD) [127] as an attempt to make PAKE protocols more immune to phishing/spoofing attacks [126]. DPD is built on top of Oblivious Transfer (OT) and PAKE [25]. The aim of DPD design is to allow a user interface that provides users with visual character-by-character feedback as they enter their passwords into a login form and permit the user to stop entering their password if the feedback is not correct. Jakobsson and Myers point out that there are many ways in which the interface to such a protocol could be implemented, but their goal is to provide a secure protocol on which such interfaces can be built upon [127].

DPD is aimed at promiscuous users, using devices that may not have been used before. Hence, there are no pre-established secrets between user's machines and target sites.

The gradual feedback is not well received in the cryptographic community, i.e. processing secret credentials little by little, because of the design principle that one should maximise the entropy of the distribution from which secret credentials are drawn. For example, if a design allows a server to verify password character by character as entered, and stops if an incorrect character is seen, that could help the

attacker to determine the password by repeating an attack multiple times. Jakobsson and Myers address the gradual feedback problem by placing two requirements [127] on their solution: (1) The server does not obtain any partial credentials during the execution of the protocol, but only after the user has approved all gradual feedback. (2) Each feedback item depends on the most recent prefix on all the characters that have been entered. They solved the contradiction between these two requirements by Oblivious Transfer techniques that allow the client to index a database of feedback items that is unique to the specific user. The indexing is done using the entered credential prefix. DPD also introduces an important blinding technique that is used to reduce the costs of communication and computation of the OT component.

### **2.3.4 User Studies of Authentication and Phishing**

Security researchers have conducted a number of studies [57, 55, 110, 226, 119, 101, 80, 129, 75, 144, 194] that tried to evaluate how well individuals can identify phishing web pages.

A particular concern in any user study, and especially phishing studies, is how to realistically simulate experiences users have in the real world, perform it in an ethical manner and yet employ an element of deception [80, 125, 66]. A form of deception is a necessity in many phishing research studies [80]. Using deception in phishing studies means that researchers intentionally withhold some of the research procedures from the participants, aiming to hide from the participants that they are participating in a phishing experiment. [66]

There are three main approaches in phishing user studies. The first involves using questionnaires, in the form of survey, interviews or polls relating to recent corruptions of systems and credentials. A disadvantage of this approach is that it may underestimate the damages, as many victims may be unaware that they have been attacked. On the other hand, surveys may overestimate the risks, given the

limited understanding of phishing among the public. A laboratory experimental approach involves recruiting subjects to participate in a study of online behaviour, often conducted in a university setting, and using an element of deception by not fully informing participants that some of their online interactions are spoofed. A third approach is to perform experiments outside of the laboratory environment and try to simulate a real phishing attack in such a way that participants can not distinguish the study from reality. [80]

A number of phishing studies have been performed in laboratory environments where the users were either told the true purpose of the experiment or asked to role-play a fictitious identity [194, 110, 110, 226]. Some of them have employed deception, or an element of deception.

Wu et al. [226] conducted a study to analyse how participants use anti-phishing toolbars to detect fake phishing websites. They created dummy accounts at various e-commerce websites. The participants were asked to play the role of a personal assistant that processes email messages of the (dummy) account holder, and to protect his passwords. They found that participants were fooled 34% of the time. When webpages looked similar enough, participants ignored toolbars though they had been asked to focus on the toolbars.

Schechter et al. [194] conducted a laboratory based study to evaluate website authentication measures designed to protect users from man-in-the-middle, 'phishing', and other website spoofing attacks. Their consent form notified participants that they would be observing their actions, but to obscure the purpose of the study, they did not detail that they were specifically observing password behaviour.

Dhamija et al. [57] performed a laboratory based user study in which participants were asked to distinguish legitimate websites from spoofed phishing websites. Participants were asked to imagine that they clicked on a link in email to see if it is a legitimate website or a 'spoof'. They informed participants that a website may be

legitimate or not, independent of what they previously saw. Despite the heightened security awareness, the study found that some phishing websites were not noticed by a large fraction of participants.

Herzberg and Margulies [110] conducted a long-term user study of authentication mechanisms which forced users to log in safely. Authentication mechanisms were different combinations of bookmarks, 'non working' links and images. They found that interactive site-identifying images received 70% detection rates. They also found that login bookmarks, when used together with 'non-working' links, doubled the prevention rates of reaching spoofed login pages. Also, when several images were displayed in the login page, the best detection rates (82%) and overall resistance rates (93%) were achieved. This study used an online exercise submission system used by courses at the computer science department of a university. Participants were students at the computer science department, which were given up to 5 bonus points for correctly detecting attacks. This might have been a significant incentive for students who wanted to do well in the course. Also, they did not use deception as participants were warned that an attack could happen.

Karlof et al. [135] conducted a non-laboratory based study to evaluate their email based authentication ceremony. They compared the security of their email registration to the security of registration using challenge questions. The study simulated man-in-the-middle (MITM) social engineering attacks against users of each of the ceremonies. They employed deception to hide the study's true purpose.

Hart et al. conducted a non-laboratory based study to measure the success of phishing attacks against PhorceField, their newly proposed authentication scheme [101]. In their study, participant were told that they were conducting an experiment to evaluate the usability of graphical passwords. They acknowledged that knowing that the study was about passwords may have had some security priming. However, they pointed out that prior research [194] has found that such subtle security priming

did not cause participants to behave more cautiously.

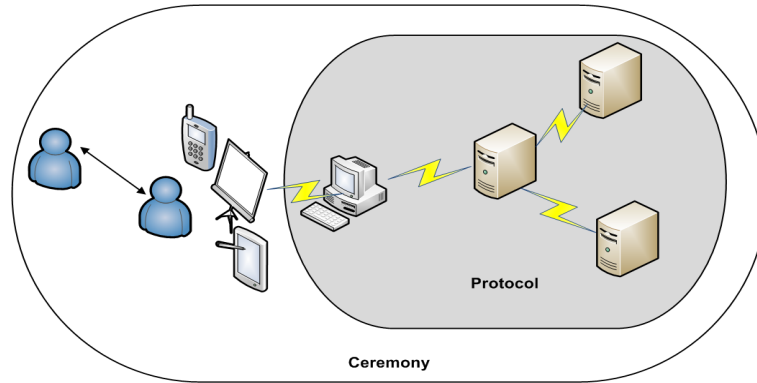
Lee and Bauer [144] conducted an online study that attempted to clarify to what extent users notice and react to the absence of security images. Security images are used as part of the login process on some internet banking websites, with the aim of foiling phishing attacks. In their study, 73% participants entered their password even when the security image was removed. Also, the condition in which participants were security primed, i.e not fully deceived, did not show a significant difference in the effectiveness of security images.

A number of the these studies [57, 110, 226] have shown that is possible to get meaningful results without fully deceiving participants.

## 2.4 Security Ceremonies

The concept of *ceremony* was introduced in 2003 [67] and further developed in 2007 by Ellison [68]. Ellison acknowledged Jesse Walker of Intel Corporation as the first person who defined the term 'ceremony' for such a purpose. Ellison argued that a better way for examining the security of a protocol was to consider a security ceremony. He defined it with regard to network protocols, but it can be extended to any group of protocols. As defined by Ellison, a ceremony is an extension of the concept of network protocols that includes user interface (i.e. human-device communication), human-to-human communication and transfers of physical objects that carry data. Figure 2.11 depicts the association between protocol and ceremony.

Different to the traditional protocol analysis approach, the idea behind the ceremony approach is to deal with a human factor explicitly, treating humans as separate entities from their machines, and assuming that they are being subject to social and psychological influences or tendencies. It is an attempt to answer an open question as how to model human behaviour in a network protocol. Human participants are



**Figure 2.11:** Protocol and ceremony association

modelled as nodes in the network, separate from the computers and devices they use. For example, typical password authentication using HyperText Transfer Protocol Secure (HTTPS) on the Internet is a ceremony where *a human user* needs to type in a *username* and *password* to login to an account; or use a physically protected personal device as out-of-band channels.

Many security decisions that cause the success of phishing are based on trust, such as trust in a brand, rather than the strength of the underlying security protocol. Therefore, ceremony analysis provides a more complete understanding of the security threats surrounding the use of a protocol by a human, than analysing the protocol alone.

A ceremony allows more detailed analysis of a security protocol. In 1978 Needham and Schroeder [162] introduced the idea of an active attacker who could modify messages, copy messages, replay messages or create messages. Dolev and Yao [59] extended the attacker model, by adding that the attacker has complete control of the communication channels. Nowadays, the Dolev-Yao threat model is the most widely accepted model to analyse security protocols. Security ceremonies are a superset of security protocols. However, to guarantee that a ceremony is secure against a Dolev-Yao attacker, a complex model of user’s behaviour should be considered. Importantly, we also need to consider the fact that the user is likely to try



to circumvent the security mechanisms in order to accomplish his/her tasks.

The modelling of the memory, state machines and processing performed by human nodes is yet to be accomplished [68]. The complexity of designing a ceremony comes with modelling a human node.

**Formal modelling.** Areas where ceremony analysis has been directly utilised are in formal methods [152, 151], authentication in computer-security systems [135, 184] and e-voting systems [137]. Formal modelling was one of the techniques mentioned by Ellison, that could be used for security protocol analysis. Martina et al. supported this idea [150] as they further developed it in the context of PKI [152] building on previous work by Rukšėnas [190]. To declare a ceremony secure and trusted requires a large number of states and conditions to be covered.

Radke defines a security ceremony as a protocol in its context of use [182]. Radke [184] extends the concept of ceremony to a higher level protocol which uses the underlying protocol as a cryptographic primitive or building block [183]. Radke builds on practice-oriented-provable security (POPS) by Bellare and Rogaway. A basic idea of POPS [24] is that at no point should a protocol be able to be broken without breaking the underlying cryptographic primitive, and hence the protocol should not be weaker than the underlying primitive. That means the way to break the protocol is to break the cryptographic building block, and as long as the building block remains secure, the protocol remains secure. Radke focuses on mutual authentication, using *browser-based* protocols, defined by Gajek as protocols realizable within the constraints of commodity web browsers [86].

Gajek's et al. [86] used Bellare and Rogaway's concept of practice oriented provable security for specification of their Provably Secure Browser-Based User-Aware Mutual Authentication (BBMA) over TLS [86]. They did not explicitly use the term ceremony, but theirs was the first model that proved a protocol including a human to be secure. Gajek added formal actions *render* and *recognise* to a security

model. *Render* is the process of a web browser rendering an HTML page, and presenting that page to the user. The ceremony specifically considers the user and the browser as protocol participants, and ties the user's authentication to the TLS secure channel. In order to prove its identity to the user the server sends a digital artefact, a HPA [86]. A HPA can be an image, video, or audio sequence, such as voice recording.

**Condition-safe ceremonies.** More specific use of ceremony analysis is taken by Karlof et al. [135], who show that security can be achieved by regulating human node behaviour via use of *forcing functions*. Karlof et al. [135] proposed a concept of *conditioned-safe ceremony* which is a ceremony that deliberately conditions users to automatically take actions that protect them from attacks. They found that we should not rely on humans to figure out the attack situation, but we should design an authentication protocol in such a way that it makes users safe even in the presence of an adversary. Their results suggest that conditioned-safe ceremonies may be useful in building ceremonies which resist social engineering attacks. Forcing functions were used by Karlof et al. [135] as user behaviour constraints, helping to achieve a conditioned-safe ceremony, a ceremony that forces users to take actions that are safe for them. Karlof pointed out that conditioned-safe ceremonies are based on lessons learnt from human factors and human reliability areas: forcing functions, defence in depth, and the use of human psychological tendencies, such as rule-based decision making [136].

A *forcing function* is a type of behaviour constraint designed to prevent human error. Forcing functions usually work by preventing a user from progressing in a task until the user performs a specific action whose omission would result in a failure or accident. As users must take this action during every instance of the task, the forcing function trains them to always perform this action, and after a short experience it will become automatic.

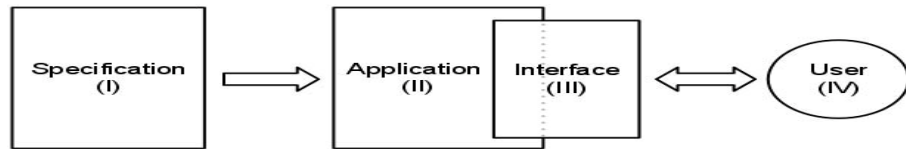
Karlof [135] argues that to resist social engineering attacks, condition-safe ceremonies need *defence in depth*, i.e. that conditioned-safe ceremonies should have (at least) two levels of protection: an attack should succeed only if a user *both* omits the conditioned action required by a forcing function *and* makes an action not normally used in the ceremony.

Psychology research shows that humans tend to prefer rule-based decision making over more tedious analytical approaches [42]. This means that users tend to apply problem-solving rules of the form "if (situation) then (action)" for frequently encountered situations. This tendency helps us go through our daily lives, reserving our time and energy for tasks requiring more detailed analysis. Unfortunately, adversaries can exploit rule-based decision making in social engineering attacks. For example, the majority of websites require a user to log in before he can do a task, many users have developed a rule of the form "if (login form) then (enter username/password)" and will apply it when they encounter login prompts on webpages which look familiar, genuine, or trustworthy [136].

Hart et al. suggested PhorceField [101], a password ceremony that uses user laziness rather than vigilance in the fight against phishing. In PhorceField the user chooses a number of images during registration. These images are stored in a secret file on the user's device that only the legitimate website has access to. When the users try to log in, they need to click on images among a set of others that are not part of the password.

### **Ceremony analysis**

Radke et al. [183] showed that ceremony analysis is a powerful tool for capturing flaws in a protocol otherwise proven to be secure. Significantly, Radke also pointed out the weakness of current ceremony analysis, which is that 'a different context, even for the same set of protocols, is a different ceremony'. This means that if the context, i.e application of the set of protocols is changed, then what was secure may



**Figure 2.12:** Human-protocol interaction layers [38]

no longer be secure.

Bella and Colles-Kemp [22] also observed that it is a big challenge to develop methodologies for the analysis of general ceremonies. They extend the ceremony analysis by proposing a layered model for integrated technical and technology practice analysis. Their approach is somewhat similar to human-protocol interaction layers defined by Carlos [38]. According to Carlos, the ceremony analysis goes through all the layers of system security, as shown in Figure 2.12. The specification layer is the protocol specification; the application layer is the implementation of the specified protocol in an application; the interface represents interaction between the application and the user.

While analysing the causes of attacks on systems against the non-cryptographic components, such as the human interaction with the system, Carlos et al. [38] have shown that there are many factors that should be taken into account when considering human-protocol interaction. They proposed a taxonomy of human-protocol interaction weaknesses.

Ceremony analysis should include the analysis of the user communication processing, i.e. processing of messages that the user inputs, receives or provides to the user interface. It should also include the analysis of human interaction errors. This involves identifying potential causes of security failures that can be attributed to, so called 'human error'.

## 2.5 Human Communication Processing

The importance and challenge of the relationship between human users and security mechanisms had been recognised long before the term 'user-centred security' was introduced in 1996. Back in 1975 Saltzer and Schroeder [191] recognised the importance of the human interface being designed for ease of use, so that users can automatically apply the security mechanisms in the correct way.

The design of user interaction for security applications, and user authentication systems in particular, has very specific non-functional requirements that sets them apart from ordinary computer applications, such as follows:

- In performing tasks, security is almost never the main goal of the user [221]. If security impedes a user's primary task, the user will probably try to avoid the security measures [7].
- Apart from ordinary, legitimate users, there are malicious users, cybercriminals, who may try to attack the system.
- Users do not understand how to interpret security indicators [57].

The importance of better understanding how users perceive security mechanisms as a way of improving security, has long been recognised. For example, Dhamija and Tyger [55] suggested design changes that could provide users with guidance to make better security decisions. Carlos et al. [38] built a set of recommendations to assist designers in the task of minimizing security threats from user interaction. Their recommendations are based on a thorough study of the existing work, among different areas, to learn and understand the most common characteristics and behavioural patterns of human-protocol interaction. Unlike Cranor, they do not suggest a definite process as how to apply their recommendations.

In the next sections, we examine the two most relevant communication processing models for evaluating secure systems used by humans.

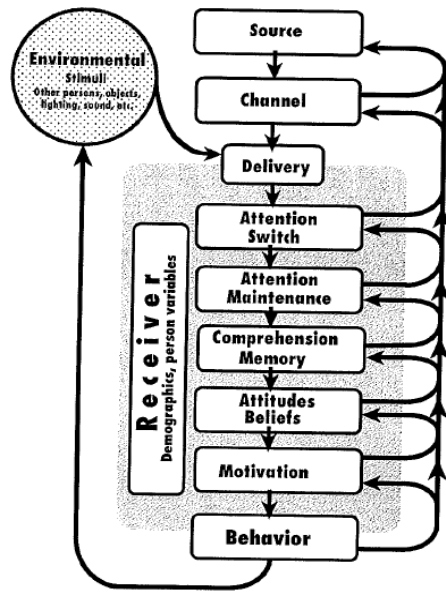
### 2.5.1 The C-HIP Model

Wogalter proposed the Communication-Human Information Processing (C-HIP) Model as part of warnings science research. C-HIP is recommended to be used to identify reasons why a particular warning is ineffective [222]. The C-HIP model begins with a *source* delivering a warning to a receiver through a *channel*. The receiver goes through a number of information processing stages that determine whether the warning results in any change in receiver's behaviour, that protects the receiver from harm. Each stage is a necessary condition for the steps that follow.

The stages of the model, shown in Figure 2.13, are as follows:

1. *Attention switch*: A warning attracts the receiver's attention.
2. *Attention maintenance*: Attention must be maintained on the warning for a certain amount of time to be properly processed.
3. *Comprehension, Memory*: Comprehension concerns understanding the intended meaning of the warning.
4. *Attitudes, Beliefs*: The receiver decides if the warning is applicable to him/her.
5. *Motivation*: The receiver judges importance of warning information and whether to take an action (if required).
6. *Behaviour*: Resulting warning compliant safe behaviour.

The C-HIP model has been applied to many applications in the physical world to improve safety warning indicators. Cranor was one of the first to use the C-HIP model in the computer *security* communications, as part of the Human-in-the-Loop framework [47]. The Human-in-the-Loop framework adapts and extends the C-HIP model for computer security scenarios. It distinguishes five types of communications as being relevant to security functions: warnings, notices, status indicators, training, and policies.

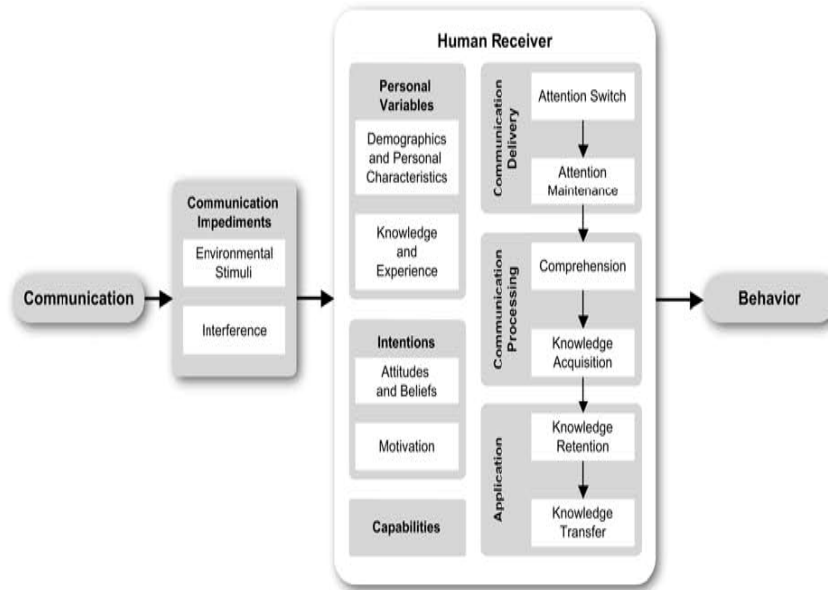


**Figure 2.13:** Communication-Human Information Processing (C-HIP) Model [222]

Bravo-Lillo [34] used both the C-HIP model and the Human-in-the-Loop framework to produce a theoretical framework for analysing the different stages that occur whenever a person faces a computer security dialog.

Egelman has also applied the C-HIP model to qualitatively examine computer security warnings, specifically indicators alerting users to phishing websites and SSL/TLS errors [64].

In the context of web authentication, we distinguish the authentication communication that is displayed via login prompts. The receiver is the user of the application. The user needs to notice the login communication, accept it, and act on it appropriately. The flow of login communication processing may or may not result in an appropriate communication response, i.e. behaviour. Using the C-HIP model and the Human-in-the-Loop framework as a theoretical base, allowed us to analyse the influence on communication processing that occurs whenever a user faces an authentication communication, as a type of computer security communication.



**Figure 2.14:** The Human-in-the-Loop Security Framework [47]

## 2.5.2 Human-in-the-Loop Security Framework

Cranor proposed the Human-in-the-Loop Security Framework [47] that can be used by security system designers to identify problem areas and address these deficiencies before the system is built, hence reducing opportunities for human security failures. She emphasizes the importance of designing secure systems in such a way that human computer interactions should be kept to the minimum required, hence the potential cause of human failure will be minimised. The Human-in-the-Loop framework builds on Wogalter’s C-HIP [222] model, adapting it to better fit computer security scenarios. The Human-in-the-Loop framework, shown in Figure 2.14, can help understand the behaviour of humans expected to perform security critical functions. The framework is a communication processing model in which a communication receiver is a human user. The communication sent triggers some behaviour that depends on the outcome of several information processing steps taken by the receiver, the personal characteristics of the receiver and the possible communication impediments.



The Human-in-the-Loop is not a precise model of human information processing, but it provides a systematic approach for identifying potential causes for human failure. It was designed to be used as a part of a four-step iterative process. This human threat identification and mitigation process can be conducted at the design phase or after a system has been implemented and deployed. Either way, the goal is to identify and proactively reduce opportunities for human security failures. As there are limits of security automation [63], a possible approach may be to determine how humans might be better supported in performing these tasks.

Masone [153] applied the Human-in-the-Loop framework to evaluate his Attribute-Based, Usefully Secure Email (ABUSE) system. Kaında [134] used it as a base to design a framework for understanding and reasoning about different factors that are important in developing or choosing secure empirical channels in *ad hoc* mobile device interactions. In his thesis, Bravo-Lillo [34] used it to analyse computer security dialogs.

In this thesis, we use the Human-in-the-Loop [47] framework and the C-HIP [222] Model as a basis for our framework.

### 2.5.3 Decision Making and Deception Detection

In this section we give an overview of human information-processing models for identifying weaknesses in users' decision-making. Deception is a crucial part of phishing attacks. Therefore, prior research in cognitive processing and deception detection is important for identifying weaknesses in users' decision making that can lead them to fall for phishing attacks [202, 123].

Johnson [131] defines a deception as a cognitive interaction between a deceiver and a victim under conflict of interest. The deceiver manipulates the environment of the victim in order to achieve a desired action [95]. The Internet is a very convenient medium for deception as it makes it easy to falsify an identity and difficult

to authenticate. Various forms of deception are on the rise on the Internet [124], including phishing.

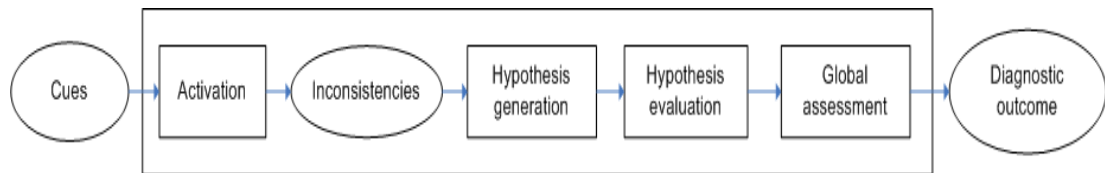
We examined two main decision-making models, the Theory of Deception [132, 131] and the Elaboration Likelihood Model (ELM) [178]. These were chosen because they were used in prior research to identify areas of weakness in users' decision-making with regard to phishing [95, 217, 218, 4, 100].

Theories and models place values on some of the variables identified as important in a framework [195, 168]. Frameworks only organize information but do not themselves provide explanations for, or predictions of behaviour and outcomes. By placing values on some of the variables identified as important in a framework explanation and prediction is performed by theories and models [195].

**Theory of Deception.** The Theory of Deception [132, 131] proposes an information processing model in which individuals recognise deception by noticing and interpreting the inconsistencies between the deceptive event and their past experiences. The Theory of Deception [132] provides a process model of how potential victims evaluate the deceptiveness of information provided to them, but does not explain how that determination fits in the overall decision making; for example, if the login page is authentic or fraudulent. It has provided a theoretical underpinning of research on internet deception [94, 95] and processing of phishing emails [217, 218, 4]. It was originally proposed to understand information processing involved in fraud detection.

The process of recognizing deception is composed of four steps [95, 131], as shown in Figure 2.15:

1. *Activation.* The target of deception pays attention to inconsistencies between what is observed and what is expected. This process may require more detailed evaluation.
2. *Deception hypothesis generation.* Users either ignore inconsistencies or use



**Figure 2.15:** The Theory of Deception fraud detection method [131, 95]

prior knowledge to generate interpretative hypothesis to explain the difference between expectations and observed cues.

3. *Hypothesis evaluation.* Once a hypothesis is generated, it is evaluated by comparing against some criteria.
4. *Global assessment stage.* The last step is to reach the conclusion, where the information is combined to form a single, synthetic assessment of deceptiveness. The assessment of deception can be the result of either a single hypothesis or it can be the result of several, less strong ones.

The Theory of Deception is recognised to be appropriate to analyse how individuals detect deception in information-intensive environments such as email-based phishing or e-commerce [95, 218, 217].

**The Elaboration Likelihood Model (ELM).** Researchers have used Petty and Cacioppo’s [178] Elaboration Likelihood Model to explore how cognitive processing influences deception (e.g. Vishwanath et al. [217], Workman [224]). ELM explores how consumers respond and process communication such as persuasive advertising messages. ELM is a dual-process model that suggests that users process message information via two main routes: the central route and the peripheral route. The central route involves diligent consideration of the information presented using comparisons and prior experience and consists of two sub-processes known as *attention* and *elaboration*. Attention is the first stage in information processing and is determined by the amount of mental focus given to specific elements of the message [177, 71]. The elaboration sub-process that follows happens when individuals make

connections between the elements and their prior experience. ELM defines elaboration as the extent to which a person thinks about the issue-relevant arguments contained in a message [178]. The ELM notion of attention is similar to the concept of activation in the Theory of Deception, but in the Theory of Deception activation consists of allocating attention to cues based on the presence of discrepancies between what is observed and what is expected [93] and it potentially may require more detailed evaluation, i.e. individuals need to *elaborate* on the cues.

The peripheral route does not consider all elements of the communication and only relies on simple cues, such as its overall appearance to make a decision regarding communication. This tendency to process information in different ways could affect users' behaviour and decision-making towards a particular message and result in different levels of susceptibility to the persuasive advertising material [178]. Prior phishing research suggests that phishing emails are peripherally processed [223] and that users who fall victim to phishing emails are those who use the peripheral route [217]. The process of elaboration, used during central information processing, is also recognised as important to deception detection in other models of mediated information processing such as the cognitive mediation models [71].

ELM provides a useful theoretical framework for understanding the communication processing during phishing attacks as it allows a concurrent examination of how attention to phishing communication and elaboration of communication can result in either resisting or succumbing to a phishing attack [100].

An *integrated information processing model of phishing susceptibility* proposed by Vishwanath et al. [217] is based on the Theory of Deception [132, 131], ELM [178] and research on mediated cognitions [71]. Vishwanath et al. [217] examined how individuals process a phishing email and decide whether to respond to it, i.e. how the users detect deception. Their model structured the information processing activities leading to deception detection into two sub-processes: *attention* and *elaboration*,

based on Eveland's et al [71] research in mediated cognitions and learning from the news.

The reviewed models suggest the information processing that underpins the users' decision making of the legitimacy of a communication messages. The Theory of Deception provides a process model of how potential users evaluate the deceptiveness of information provided to them, it does not suggest how the evaluation of deceptiveness happens [95]. Paying attention to the communication message is a necessary but not sufficient condition for detecting deception. Individuals need to make conscious connections between the cues they observe and their prior knowledge, i.e. they need to elaborate on the cues [177, 218].

## 2.6 Conclusion

Online security is proving difficult to achieve, as users are not able to effectively establish the legitimacy of the server with which their browser is interacting. Phishing is a social engineering attack that is a main threat to web authentication.

Various anti-phishing techniques are being proposed, and can be broadly categorised into: user awareness, legislation and technical countermeasures. From the user's point of view technical countermeasures can be categorised into those that are invisible to users, that use automated phishing detection techniques; and those that provide user interface improvement by offering more protection against visual deception attacks or helping users make better security decisions. Improving user interfaces spans the following areas: security warnings, indicators for verifying legitimacy of websites; and improving the authentication mechanisms by using stronger authentication protocols than just username and password.

Common to the reviewed alternative authentication schemes [86, 216, 135, 55, 101, 127, 176, 41, 174, 172, 158, 90, 32] is that, as part of the authentication pro-

cess users are expected to perform a greater number of tasks than in the traditional username/text-based schemes. Additional tasks are often more complex cognitive tasks than simply remembering and typing a password. For example, users may be expected to recall and recognise some credentials, read/write a value from an out-of-bound device, perform a comparison, and then provide it to the authentication scheme. These additional tasks are usually necessary because to provide anti-phishing resistance, these schemes often include not only a protocol to authenticate the user but also a protocol to authenticate the server [127, 86]. This additional part of the protocol is designed for the user to verify that the website that he/she is accessing is legitimate.

Graphical passwords are a notable user authentication type that have been used as an alternative to text based password schemes. They utilise the psychological finding that the human's ability of remembering images is far superior than remembering text; and we explore this possibility in Chapter 6.

Security researchers have conducted a number of studies trying to evaluate how well individuals can identify spoofed web pages, and spoofed authentication, i.e. login pages in particular. A number of reviewed phishing studies have shown that it is possible to get meaningful results without fully deceiving participants, as described in Section 2.3.4. Notable examples are as follows. In the study by Dhamija, Tygar and Hearst [57, 55] participants were aware that they were part of a security study and that spoofed websites would be present in the study. In the study by Herzberg and Margulies [110], students participants were specifically warned that an attack could happen. In the study by Wu, Miller and Garfinkel [226, 225] subjects were given a consent form to read that explained that the purpose of the study was to test web browser security indicators that detect fake web pages that look like pages from legitimate websites; and that the purpose of these fake websites is to trick people into making dangerous decisions or actions.

The success of phishing can be attributed to the user's inability to authenticate websites. i.e web server. Some authentication schemes provide mutual authentication between a user and a server using a Human Perceptible Authenticator (HPA); a HPA allows the human user to authenticate the server. Authentication with a HPA is more similar to identification in the physical world and more familiar to users. Our focus is on authentication schemes that use graphical passwords as a type of HPA.

Social engineering attacks target human users and their usage and interpretation of authentication schemes that leads them to make mistakes. There is a need for research that would investigate human processing of phishing attacks and expand the understanding of this form of social engineering attacks. Ceremony analysis provides a more complete understanding of the security threats surrounding the use of a protocol by a human, than analysing the protocol alone. We use the concept of ceremony to analyse authentication schemes and why they do not protect effectively against phishing.

The review of decision making and deception detection models [132, 131, 178, 95, 177, 218, 71, 100] points to attention and elaboration as being the main information processing activities that underpin the users' evaluation of deceptiveness. Both the C-HIP model [222] and Human-in-the-Loop framework [47] include attention to the communication and a form of communication judgement, as an important step in communication processing that helps identifying weaknesses in users' decision-making. We combine the Human-in-the-Loop [47] framework and the C-HIP [222] model for evaluating secure systems used by humans, with the research in information processing and decision making [132, 71, 95, 178, 218, 217], to explore the factors influencing user's behaviour in authentication ceremonies and to develop a framework of human factors in anti-phishing authentication ceremonies (Chapter 4).

Models place values on variables identified as important in a framework and can provide explanation and prediction. The model we develop in Chapter 5 places specific values on the variables of our framework, that we identified as important in authentication ceremonies.

In the next chapter, Chapter 3 we explore the issues that may arise due to the user's behaviour assumptions.



# Chapter 3

## Communication Processing in Authentication Ceremonies

### 3.1 Introduction

In this chapter we explore the behaviour of humans who are expected to process and react to security-related communication as part of web authentication ceremonies. We describe the issues that may arise due to these behaviour assumptions. Recognising these issues may help to discover additional vulnerabilities that attackers exploit.

This was the starting point of our research, which led us to identify human factors that should be considered during the threat analysis of anti-phishing authentication ceremonies. The work presented in this chapter was published in [106].

### 3.2 Ceremony Analysis and Phishing

The advantages of extending protocol design and analysis to ceremonies are supported by previous research [37, 182, 68]. Some of the advantages are as follows: more realistic protocol analysis, improved usability, earlier problem detection, re-

ducing the gap between protocol and HCI communities; prediction of the impacts of user misbehaviour [37]. A particularly important analysis to phishing research is the analysis of, so called, user misbehaviour. These misbehaviours are in fact flawed system design assumptions as to how a human user processes the communication from an authentication protocol. These assumptions can compromise security of the authentication protocols. Many protocol security design specifications do not hold once they are implemented and deployed in the real world and used by people.

The notion of a ceremony indicates that the classical protocol description must be expanded with a representation of humans as nodes in the network and the extra communication between the humans and the other nodes, that can be either human or computer nodes. Human node communication in ceremonies may involve communication of a human node to user interface, human-to-human communication or the transfers of physical objects that carry data.

Any design process that we use for network protocol can be followed for ceremony design [68]. Analogue to a computer protocol node, a human node receives and sends messages, sometimes through human computer interfaces, sometimes by human-to-human communication or peripheral devices (e.g. using a smartcard or an USB token). Unfortunately, human input and output messages are often subject to errors, that are quite regularly treated as arbitrary faults by some of the protocols' correctness models. These errors happen mainly because users, i.e. 'human nodes', have different capabilities from ordinary computer nodes. The importance of modelling the memory and processing performed by human nodes is recognised and is yet to be accomplished. [68, 37, 182]

Ceremony design needs to explicitly specify the user interaction, e.g. messages that the user inputs, receives or provides. It should also include a design of processing human interaction errors. This involves identifying potential causes of security failures that can be attributed to human error. In the case of phishing attacks



**Figure 3.1:** A degenerate web authentication ceremony

these human errors may be partially caused by protocol specification that does not model human communication processing sufficiently. As a basic example, in traditional username/password authentication, users are conditioned to type in their username and password when they see a login form on the legitimately looking website. But, phishers can redirect users to a website that seemingly looks the same as the legitimate website and causes users to reveal their credentials. As part of the ceremony design process every human interaction should be considered and defined. It is proving to be a complex research task and is being undertaken by a number of researchers [37, 182, 23, 151, 136].

Our focus is on the communication between a human node and a computer user interface, i.e. computer nodes, that convey messages to or from the protocol’s technological nodes as represented in Figure 3.1. As such, we focus on the representation of web authentication ceremonies as a degenerate ceremony [68] of two nodes: a computer application and a human user. The application is in most cases a service provider’s website accessed via a web browser. We will refer to it as *the application* throughout the thesis, only sometimes as a website or service provider. We do not explore the other parts of ceremonies that involve protocols between computer nodes or between human nodes.

In our ceremony analysis we assume that the authentication protocol specifying communication between computer nodes in ceremony is working as required. We ignore it as it is part of protocol specification and security analysis in traditional sense. We concentrate on the main design assumptions about the human node to computer node communication part of the authentication ceremonies. That com-

munication is normally referred to as *human-computer interaction (HCI)*. We then identify those that can compromise ceremony security.

Users are often advised to verify a web page’s domain and TLS certificate before entering their credentials, but the research shows that users largely ignore these security indicators [65, 194, 57, 60, 226]. Therefore, we do not take into consideration the influence of browser security indicators.

### 3.3 Communication Processing

As a result of security limitations of the traditional text-based passwords researchers have proposed a number of different anti-phishing authentication ceremonies [86, 216, 135, 55, 101, 127, 176, 41, 174]. In order to provide anti-phishing resistance, these ceremonies include not only a protocol to authenticate the user but also a protocol to authenticate a server. This additional part of the protocol is designed for the user to verify that the website that he/she is accessing is legitimate. Some ceremonies offer a choice of images, some a piece of music [88], instead of, or in addition to text, as part of the *server authentication*.

For anti-phishing ceremonies, as part of the login process, the user may be expected to recall some credentials, read/write a value from an out-of-bound device, perform a comparison, and then provide it to the authentication ceremony. Therefore, users (i.e. human nodes) in a ceremony are often required to make decisions that demand significant human abilities and knowledge. Variation of the behaviour of human nodes, such as limited memory, probabilistic memory access, fuzzy comparisons, etc. introduces additional flaws in a ceremony. Research shows that recognising these flaws could lead to improved ceremony design [184].

There are a few variations of these newly proposed ceremonies, where the server sends digital artefacts (an image, voice, music) in order to prove its identity to the

user, i.e. HPA. Examples of ceremonies are: Déjà Vu [54], Provably Secure Browser-Based User-Aware Mutual Authentication over TLS [86], TwoStep [216], Delayed Password Disclosure (DPD) [127], PhorceField [101], Passfaces [174].

### 3.3.1 Analysis of Sample Authentication Ceremonies

We focused on ceremonies in which a server sends and presents a graphical feedback (i.e. a HPA) to the user as proof of its identity. For most of these ceremonies the graphical feedback is in the form of images. These types of ceremonies can be broadly classified as recognition-based graphical passwords. They harness the ability of the human memory to recognise events or stimuli that have been previously seen when authenticated. This ability is far superior to the recall ability. Previous research shows that images are remembered better than words in tests of item recognition and recall [163, 114]. While most of the ceremonies are implemented as prototypes, some are available for deployment [45, 173] or variations of them. In these ceremonies, as part of the login process the user will:

- Type 1: Recognise an image. The main examples is BBMA [86] and its variations, often used on internet banking websites [18, 180, 192].
- Type 2: Select images from a larger challenge set. Examples are: TwoStep [216], Passfaces [174], Confident ImageShield [45], PhorceField [101].

For Type 1, security image ceremonies, we specifically analysed Gajek’s et al. Provably Secure Browser-Based User-Aware Mutual Authentication over TLS [86] and commercial variations similar to BBMA, such as Sign-in Seal [228]. Some of the commercial variations were [18], or still are being used by major Internet banking websites [192, 180]. As part of BBMA, in order to prove its identity to the user, the server sends a HPA. A HPA can be an image, video, or a voice recording. The HPA

is chosen during the registration phase and the user has to recognise it at the login phase. The user authenticates himself/herself to the server using a text password.

For Type 2 ceremonies we analysed TwoStep [216], PhorceField [101], Passfaces [175]. In these ceremonies, as part of the website login the user is presented with an image set. The user must correctly select the secret images previously selected at the time of registration. As phishers do not have access to the secret images, it would not be easy to present victims with the set of images containing the right ones.

The focus of our analysis was the communication between the human and computer node in these ceremonies. Radke et al. [184] have also researched human computer interaction issues that can arise due to implementation variation of handling a HPA in Gajek et al. BBMA [86] protocol. Exploration of related research findings, such as Radke et al. [184] and our own investigation of Type 1 and Type 2 ceremonies reveals a number of issues arising from assumptions as to how a human is supposed to use these ceremonies as well as the ceremony implementation.

### 3.3.2 Assumptions and Related Issues

The main assumptions made about how human nodes behave while processing communication from the computer nodes in the reviewed ceremonies and related issues, are summarized in Table 3.1 and described in detail below.

- *The user will expect a HPA as part of the authentication ceremony.* This assumption implies that a user is familiar with the ceremony steps and will find it strange to be asked to enter a password without a HPA being displayed.  
*Issue.* The login webpage may be spoofed; a phisher may trick a user to enter a password in a non-secure manner, so that the secure protocol that is using HPAs is never used [176].

Behaviour Assumptions	Issues
The user will expect a HPA	Spoofed login, secure protocol never used
The user will wait for a HPA	Delay in displaying the HPA Skipping security step
The user will notice a HPA	User busy with primary task
The user is able to recognise a HPA	Not able to recognise the right HPA
The HPA is human distinguishable	User interface design - usable security

**Table 3.1:** Behaviour assumptions and related issues

- *The user will wait for a HPA.* Implementing a display of HPA may slow down the execution of ceremony steps. For example, a user may be offered a set of images to choose their HPA from, and their downloading may be very slow. It is assumed that the user will not skip these tasks that potentially slow down his/her primary task offered by a service provider after the login.

*Issue.* Research shows that users are prone to skip a security step if it slows down the primary task [184].

- *The user will notice a HPA.* Most ceremonies assume that users will notice the HPA being presented to them, but the HPA may be obscured by some other computer applications or stimuli around the user.

*Issue.* The user may be concentrating on the primary task to be accomplished on the website and not pay enough attention to notice the HPA [57, 60]. To make things worse, some implementations of the website login pages contain service provider's advertisements (e.g. Yahoo's [229]) which may further distract a busy user.

- *The user is able to recognise a HPA.* It is assumed that the user will switch

attention to the right HPA being presented and have the capability to distinguish the correct one. This is in the case of multiple HPAs being presented and only the right one being chosen.

*Issue.* The user may not have capability to recognise the right HPA.

- *The interface will make the HPA human distinguishable.* It is assumed that the implementation of website login forms will make HPAs human distinguishable and memorable.

*Issue.* This assumption highly depends on the user interface design and implementation. Also, the user senses can be affected if displayed just after some other computer applications or a stimuli around her.

Each of the above assumptions and issues will also be affected by the type of the input and output medium that can make it easier or harder to receive a HPA [83]. For example, small screens on phones make it more difficult to type a password. On the other hand, the phones are the easiest medium to send/receive an one-time-passwords used in some ceremonies.

### **3.3.3 Influencing Factors**

The issues identified in the previous section may be exacerbated by different factors in different ways. Some of the factors that may influence the user's communication processing and can cause these issues are described in this sections and summarised in Table 3.2.

- *Spoofed login, so secure ceremony is never used.* An essential precondition to security is getting users to use the security protocol. If a phisher tricks a user into entering their password in a spoofed web page, so that the secure protocol is never used, then the cryptographic countermeasures are bypassed



<b>Issue</b>	<b>Influencing Factors</b>	<b>Supportive literature</b>
Spoofer login, secure ceremony never used	Knowledge of the ceremony Interference, delivery channel Format, font size, length	([176], [38], [57], [47], [83])
Delay in displaying a HPA	Technology failures, deficiencies Interference, delivery channel Format, font size, length	([47], [184], [83])
User skipping security step	Distraction from primary task Doing more interesting things Motivation, habituation	([47], [184], [135], [47], [222], [34])
User busy with primary task	Distraction from primary task Interference, delivery channel Format, font size, length Habituation	([226], [38], [202], [221], [47], [83], [57], [60])
Not able to recognise the HPA	Cognitive or physical skills Memorability Interference, delivery channel Format, font size, length	([193], [68], [47], [38], [83])
User interface design	Cognitive or physical skills Delivery channel Format, font size, length	[47], [38], [186], [83])

**Table 3.2:** Communication processing issues and influencing factors

[176]. *Knowledge* of the ceremony with user training, and user interface features such as format, font size, length and type of delivery channel are the main influencing factors to consider for this issue. Interference with the login prompt by an attacker or other related and unrelated communications such as advertisements may also contribute to the user not *switching attention* as to whether the login prompt is correct or if the HPA is presented. [57, 47, 38, 83]

- *Delay in displaying HPA*. If there is a delay in displaying HPA due to technology failures, deficiencies or interference, in some ceremony implementations the user can still enter their login and password and proceed with login without checking the HPA. [184, 47] Format, font size, length and type of delivery channel could make this problem better or worse. [83] There is no guarantee that the user's *attention* will be *switched* to or *maintained* if there is a considerable delay in presenting the HPA.
- *User skipping security step*. Research shows that if security tasks are not required actions (i.e. acting on security warnings, checking security indicators), then users routinely skip them as usually there are no immediate visible consequences of not doing so [194, 144]. Users may not be *motivated* to perform security steps properly, as they require extra time and effort [57].

According to Karlof [135], human psychological tendency to develop automatic responses to frequently encountered situations is one of the main contributors to success of the phishing attacks. Some researchers define this tendency as habituation [47, 222, 34]. This notion of habituation seems to be the same as what the psychologist Cialdini [42] refers to as human *click-whirr responses*. Habituation or click-whirr responses means that the user automatically enters his/her username/password on any login page which looks familiar and legitimate. Especially as they will usually be doing something more interesting on

a website after they complete the login.

- *User busy with primary task.* When logging in to a website, security is almost never the main goal of the user [38, 221, 226, 202]. Hence, users may not *switch attention* to the HPA, or notice that it is missing or that is different. Habituation and predictability is an important influencing factor as a busy user may over time ignore a HPA that they observe frequently and they are usually correct [57, 60]. Characteristics of the HPA and user interface design such as format, font size, length, delivery channel will strongly influence this issue [47, 83]. If they switch the attention to the HPA, it is not guaranteed that they will examine in detail and *elaborate* on the security communication presented to them.
- *Not able to recognise the right HPA.* A wide range of people with mixed *capabilities* use authentication ceremonies, including different cognitive and technical abilities. Depending on the type of communication, i.e. whether the user needs to *recall*, *recognise* or *compare* as part of the authentication, specific *capabilities*, knowledge, *attention* or memory may be necessary to complete the login. [47, 38, 83] Overloading humans' memory by requiring them to remember large amount of data has become a big problem of online authentication. Even more so as many password policies force users to choose a random data as a password. [68, 193]
- *User interface design.* The importance of usable security is widely accepted and recognised as one of the factors that can compromise the protocol security [48, 233]. It is essential that the human interface be designed for ease of use, so that users apply the security mechanisms correctly without too much effort [191]. Therefore, the design of *input/output* communication, i.e. login prompt, will affect the ceremony's security level and should be taken into account

during the user interface design. Also, it is important that user interface design (format, font size, length, delivery channel) is able to cater for people with mixed cognitive and physical skills to allow successful completion of security tasks. [47, 83, 38, 186]

## 3.4 Conclusion

In this chapter, we have shown how the assumptions about the behaviour of humans in authentication ceremonies can affect its anti-phishing security. We described related issues that can arise due to these assumptions as to how humans process communication within authentication protocols. We presented the main factors that may influence these issues in different ways.

We have shown that there is no guarantee that a user will switch to, pay enough attention to, or examine in detail the authentication login prompt presented to them. The user also may not be motivated enough to perform additional security tasks. In addition, some users may not have cognitive or technical abilities to perform them correctly.

Recognising these assumptions, issues and influencing factors (presented in Sections 3.3.2 and 3.3.3, and summarised in Table 3.2) helped us to identify the components of the framework described in Chapter 4.

# Chapter 4

## Human Factors in Anti-Phishing Authentication Ceremonies (HF-APAC) Framework

### 4.1 Introduction

This chapter presents the *Human Factors in Anti-Phishing Authentication Ceremonies (HF-APAC) Framework* that is designed to help authentication ceremony designers to analyse security threats and improve the design to alleviate them. Depending on the context, we may refer to it only as *HF-APAC Framework*; or *Human Factors in APAC Framework*; or *the Framework*.

The focus of the Framework is on helping to analyse the communication processing performed by human users in authentication ceremonies. That in turn should help to adapt the ceremony design to better resist social engineering threats such as phishing.

The base of the Framework is the exploration of existing research on human-protocol interactions [68, 37, 182, 42, 47, 222] and findings of various phishing user

studies [57, 136, 194, 144, 110, 123]. The Framework specifically builds on Cranor’s [47] The Human-in-the-Loop Security Framework and Wogalter’s Communication-Human Information Processing Model (C-HIP) model [222]. It incorporates aspects of these frameworks and combines it with the ceremony research.

The main source of development of the HF-APAC Framework components and the relationships between them was a review of existing anti-phishing authentication ceremonies and identification of issues and factors affecting human communication processing as presented in Chapter 3 and summarised in Table 3.2. Identified issues and factors influencing them pointed out which components of C-HIP model and the Human-in-the-Loop framework should be incorporated into the HF-APAC Framework.

The rationale behind developing a new framework is that neither the C-HIP model nor the Human-in-the-Loop framework considered the influence of *elaboration*. In information-processing science, elaboration is defined as the process of making conscious connections between the cues observed and prior knowledge [218]. Elaboration in this thesis means the process through which a human connects the authentication communication they observe and their prior knowledge and experience of these communication elements. The importance of elaboration in deception detection is supported by prior phishing research [57, 123, 217, 218]. Significantly, it has been recognised that deception, visual deception in particular, is at the core of the social-engineering attacks, such as phishing [52, 225, 202, 95].

The rest of the chapter proceeds as follows. We first present the place of the HF-APAC Framework in broader ceremony analysis, followed by a detailed description of its components. We then propose a design and analysis process of human communication factors in authentication ceremonies and describe how the HF-APAC Framework can be applied either to improve an existing ceremony or design a new ceremony. The work presented in this chapter was published in [105, 106].

## 4.2 HF-APAC Framework in Ceremony Analysis

Security protocol analysis is a well researched area, a notable example is Needham and Schroeder's modelling of an active attacker [162], further extended by Dolev and Yao [59] and further developed by many [24, 25]. Recent research [136, 22, 182, 37, 152] advocates analysing a protocol in context to cater for a more realistic threat model applicable to the concept of a ceremony.

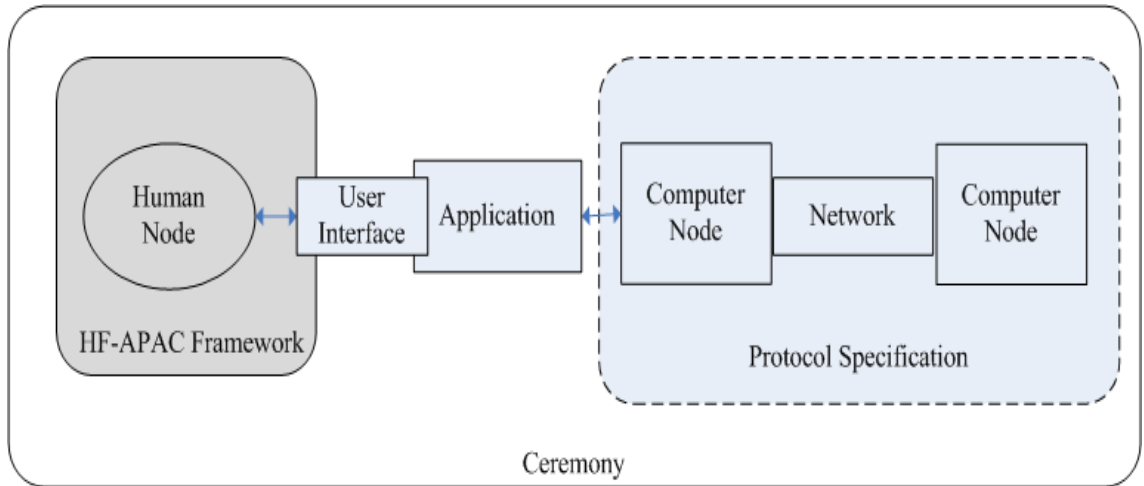
A security ceremony expands a security protocol with the out-of-band communication, which in ceremony can be human-computer (via user interface), human-human (face-to-face, phone calls, etc.) or physical (e.g. use of a smartcard or USB token). In a protocol design and specification any out-of-band communication is generally part of the design assumptions and left open for arbitrary people to satisfy in arbitrary ways. [68] Some of these assumptions turn out to be security issues, as we have shown in Chapter 3.

The modelling of processing performed by human nodes in ceremonies is yet to be accomplished. Our Framework is aimed at helping the analysis of the communication processing performed by human users in authentication ceremonies.

Both Carlos and Price [38] and Bella and Coles-Kemp [23] suggest a layered approach to ceremony analysis. As our Framework is designed to be used at the human application interaction points, we adopt the human-protocol interaction layers similar to those suggested by Carlos and Price [38], shown in Figure 2.12.

The layers underlying our ceremony analysis approach and the place of HF-APAC Framework, shown in Figure 4.1, are as follows:

- Protocol Specification - is a 'traditional' protocol specification between computer nodes;
- Application - is the implementation of the protocol;
- User Interface - is the point of interaction between the application and human



**Figure 4.1:** HF-APAC Framework in Ceremony Analysis

node; and

- Human Node - represents a user of the application.

The HF-APAC Framework design takes into consideration the application implementation as users may exhibit different behaviour with different services. For example, a user may be better motivated to consider security indicators while interacting with an online banking site than when browsing a discussion forum.

The Framework, presented in Figure 4.2 is described in detail in the rest of the chapter. We also discuss how the Framework can be applied. The foundations of the components were the issues and factors affecting human communication processing identified in Sections 3.3.2, 3.3.3 and summarised in Table 3.2.

### 4.3 The Framework

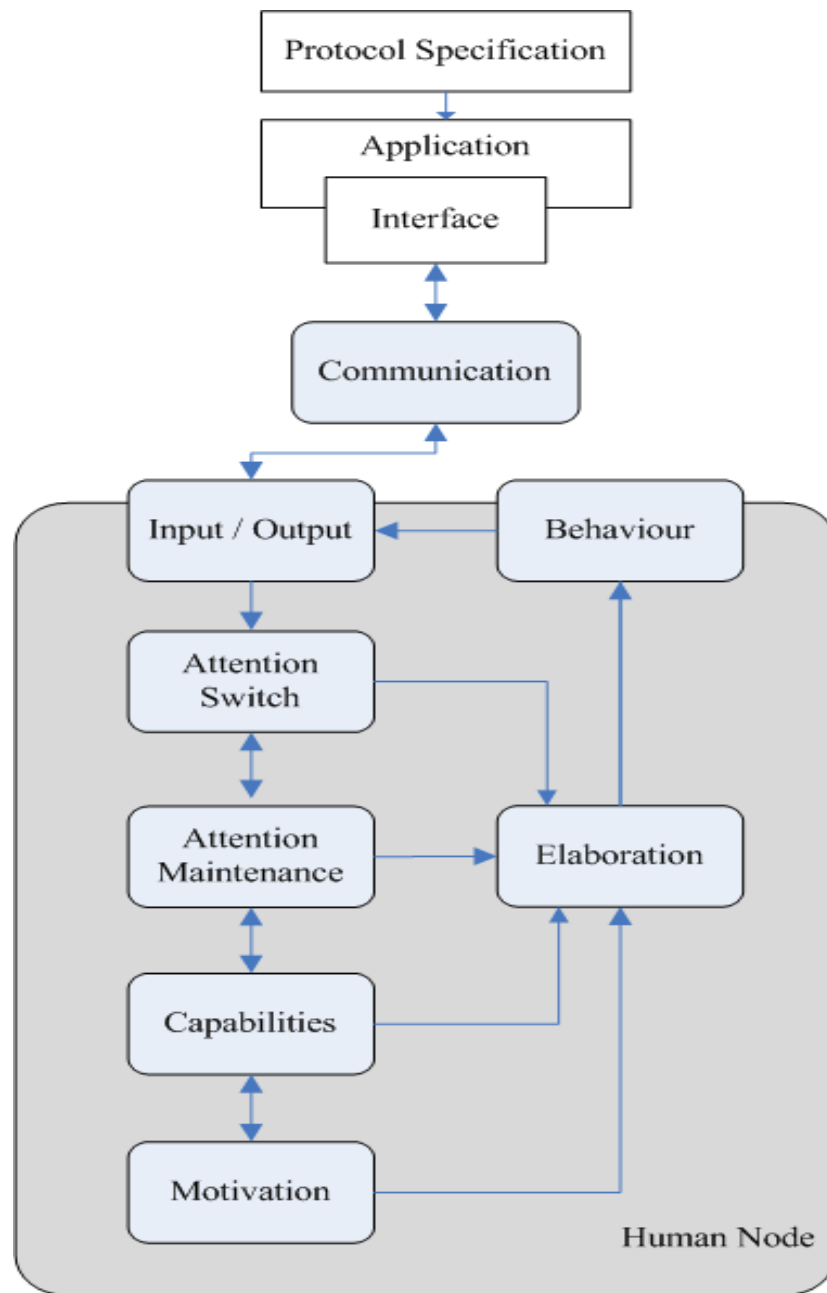
Our Framework builds on The Human-in-the-Loop Security Framework [47] and Communication-Human Information Processing Model (C-HIP) model [222]. The Human-in-the-Loop framework is not a precise model of human information processing, but it provides a systematic approach for identifying potential causes of human



security failure in a wide context of computer security. Different to the Human-in-the-Loop, our Framework considers the different factors specific to the anti-phishing authentication ceremonies context and indicates more precisely the temporal flow between the components. This temporal flow builds on the C-HIP model [222], adapted to fit to web authentication ceremonies. The C-HIP model comes from psychology literature and is recommended to be used to identify reasons why a particular warning is ineffective [222]. The C-HIP model analysis consists of going through a number of information processing steps, which determine whether the warning results in any change in receiver's behaviour. Similar to the C-HIP model, in the HF-APAC Framework communication goes through several processing steps affecting the outcome of user's behaviour.

A review of existing anti-phishing authentication ceremonies and identification of issues and factors affecting human communication processing presented in Chapter 3, particularly in Sections 3.3.2 and 3.3.3, and summarised in Table 3.2, helped us in identifying the Framework components.

The HF-APAC Framework is based on C-HIP and the Human-in-the-Loop communication processing models, in which a communication is sent to a human node triggering some behaviour, as shown in Figure 4.2. Figure 4.2 depicts a temporal flow of authentication communication delivered through input/output and processed through the Framework components, described in Section 4.3.1 and presented in Table 4.1. The flow between the components should not be interpreted as a linear process but one that can go back and forward between them. One of the goals of this research is to give more insight as to how this communication and processing flows and how it influences the security of the authentication.



**Figure 4.2:** HF-APAC Framework

### 4.3.1 Components

This section describes the components of the HF-APAC Framework in detail, Table 4.1 gives an overview of the components. The foundations of the components were the issues and factors affecting human communication processing identified in Sections 3.3.2, 3.3.3 and summarised in Table 3.2. The components were identified by reviewing existing anti-phishing authentication ceremonies and identification of issues and factors affecting human communication processing (Sections 3.3.2 and 3.3.3, Table 3.2).

#### 4.3.1.1 Communication

The first component of the Framework is the communication to the human node, which should trigger an appropriate behaviour in an authentication ceremony. The Human-in-the-Loop framework [47] distinguishes five types of communications as being relevant to security functions: warnings, notices, status indicators, training, and policies. We distinguish three types of communications that are relevant to authentication ceremonies: *recall*, *recognise*, and *compare*. They may be combined in an authentication ceremony. *Recall* communications are those that require a user to memorise and recall a specific authentication credential, e.g. recalling a password (and username) in a typical username/password authentication. *Recognise* communications are used in graphical password schemes, e.g. where the user has to recognise a previously seen image. *Compare* communication is mainly used in one-time password schemes, where a user is supposed to read/write a value from an out-of-bound device, perform a comparison, and then provide the resulting outcome to the ceremony. There are specific issues that may arise from each, most notable being a huge demand on users' memory [193]. For example, humans tend to perform fuzzy comparisons [68], which means ignoring comparisons that cannot be completed because information is lacking or because some other factors suggest a different

<b>Component</b>	<b>Factors to Consider</b>	<b>Source</b>
Communication	Recognise	([47], [68], [193])
	Recall	
	Comparison	
Input and Output	Keyboard, Mouse, Touch	([83], [47], [233], [191, 186])
	Visual, Auditory	
	Out-of-Band Devices	
Attention Switch	Format, Font, Size	([222], [47], [83], [177], [71], [218])
	Motion, Sound	
Attention Maintenance	Format, Font, Size	([222], [47], [83], [57], [42], [34], [60], [177], [71])
	Length, Habituation	
Capabilities	Memory, Comprehension	([222], [47], [68], [193], [83])
	Knowledge	
	Specific Cognitive or Physical Skills	
Motivation	Distraction from primary task	([222], [47], [221], [219], [202])
	Convenience, Risk perception	
	Incentives/Disincentives	
Elaboration	Automatic responding	([178], [71], [131], [217], [218], [135])
	Cognitive effort	
Behaviour	Skip a required step	([222], [47], [184], [186], [35], [173])
	Predictable	
	Perform an action incorrectly	

**Table 4.1:** The components of the HF-APAC Framework

outcome.

How the user inputs authentication credentials and receives feedback (i.e output) from the ceremony, can affect communications processing [47]. It can as well affect security and vulnerability of the authentication process and influence a number of issues as described in Section 3.3.3. Hence, input/output is the next component of the Framework.

#### **4.3.1.2 Input/Output**

Many anti-phishing authentication ceremonies use methods other than the standard keyboard or keypad to enter credentials. Examples are mouse, touch, visual, auditory, combining with out-of-band devices. The format, font, size or length and type of input affects usability and the level of user's acceptance of the ceremony [83, 191, 233] and hence the anti-phishing security. We have shown (Sections 3.3.2 and 3.3.3, Table 3.2) that these factors may influence a number of communication-processing issues.

The human decision-making process is not linear, i.e. does not follow a direct path from communication to the response (i.e. *behaviour*) [217]. The delivery of a communication consists of two phases: attention switch and attention maintenance, and they are the important components of the HF-APAC Framework. Attention indicates the amount of mental focus given to specific elements of an event or object. [177, 71, 218].

#### **4.3.1.3 Attention Switch**

In traditional protocol analysis it has been easy to overlook a failed delivery as a source of design error. The assumption was that the communication was sent as per protocol specification. However, the successful sending of a communication does not mean that it was successfully received [57]. For example, a picture used to

authenticate a server to the user, may not get displayed/downloaded successfully before the user enters his password, or the download may be delayed. Hence, it is not guaranteed that the user switched attention to the communication. As shown in Section 3.3.3, this can cause a number of security issues. Ceremony security analysis needs to make sure that the human node has indeed received the intended communication. The main factors to consider are: *format, font, size, motion and sound*.

#### 4.3.1.4 Attention Maintenance

Once the communication has attracted the user's attention, it needs to keep his/her focus *long* enough to be understood. [177, 71] The length of attention kept may not correspond to the effort necessary to complete a necessary authentication task. The user may get frustrated and try to avoid the task if possible - or provide any input only to move to the next step. This component is vulnerable to *habituation*, the tendency for users to pay less attention to stimuli they experience frequently. For example, entering username and password in the username/password fields without considering other authentication factors [135]. Another common behaviour is the user who skips a security step, as he/she is *rushing* to finish a primary task provided by a service provider [184]. The type of input/output will have an influence as well as format, font, size.

#### 4.3.1.5 Capabilities

An important aspect of any authentication is how newly created authentication credentials are remembered and later retrieved at login. The user's long term memory abilities is a well recognised issue that influences users to create passwords that are easy to remember, but not strong and are easily guessed by attackers [204]. More and more of the general population are using online services and are required to re-

member dozens of passwords. Hence, more users with mixed capabilities, including cognitive and technical abilities are required to accomplish login tasks. Depending on what the user needs to remember or recognise as part of the authentication, specific knowledge, memory or comprehension may be necessary to complete the login. This is becoming a bigger issue as the general population is being encouraged more and more to use online services for day-to-day business, not only by financial institutions but also by government service providers, such as revenue, social protection sites and health providers. [38, 83, 68, 193] We distinguish the following capability types that affect the communication process in authentication ceremonies: *memory*, *comprehension*, *knowledge* or some other *cognitive or physical skill*.

#### 4.3.1.6 Motivation

Motivation plays an important role in how users decide what action they are willing to take. Research shows that users are not good at recognizing risky or dangerous situations. Users are prone to believe they are not important or rich enough to be a target of an attack and that the likelihood of being targeted personally is seen as small [219]. This is often supported by a human tendency to only take into account confirming evidence for one's belief and ignore disconfirming evidence. This aspect of human reasoning is known as *confirmation bias*. [164] Also, users who are by nature risk averse take less risks in the digital world compared to those who are not. Risk perception is also determined by the perceived financial or other importance of a particular website to a user and also how busy the user is with the primary task. [202]

In general, authentication to a website is an extra task that creates an overhead for the user, who is required to use it as a tool to achieve a primary, real-world task [219]. As the compliant ceremony security behaviour often slows down the receiver's primary task, incentive can be difficult to provide [221]. As the benefit of

completing the authentication task quicker (i.e doing something more interesting) is more certain than the probability of being a target of an attack, there is a strong incentive for the user to proceed with security steps even if they do not look right. The convenience of an authentication ceremony will influence the user's motivation to accomplish all the tasks with enough attention.

Hence, *risk perception, distraction from primary task and convenience* are the factors that influence motivation.

#### **4.3.1.7 Elaboration**

Phishers use deception to trick users to submit their login credentials to fake websites. Present research on phishing explores various factors that influence this form of deception [217, 218, 100]. Also, previous researchers [223] have explored how cognitive processing such as elaboration influences deception in social engineering attacks such as phishing.

The importance of elaboration in deception detection has its roots in the human psychological tendency to apply rule-based decision making and develop *automatic responses* to situations that are encountered more than once [42]. We tend to classify a communication according to a few key features, and if one or more features match what we have encountered in the past, we may respond mindlessly with the action that we learned was most appropriate. For example, many users will automatically enter their login credentials on any page which looks familiar and legitimate. This is an important and generally positive feature, otherwise we would spend a considerable amount of time analysing everyday situations [136]. Unfortunately, the phishers have learnt to exploit this predictability of human behaviour.

Elaboration in this thesis means the extent to which a user thinks about the authentication factors they observe and make connections between these factors and their prior knowledge and experience. This definition is based on research



in deception detection and mediated cognitions [177, 178, 132, 71, 131, 217, 218] Attention to authentication factors is a necessary but not sufficient condition for detecting phishing. In addition, users need to elaborate on the security cues. [123, 223, 217, 100] Therefore, elaboration is a very important component of the HF-APAC Framework.

#### 4.3.1.8 Behaviour

The Generic Error-Modelling System (GEMS) was developed by James Reason for understanding human errors during decision making and problem solving [186]. Researchers have also used it to model human errors which can lead to security failures [35, 47]. Reason categorizes behavioural errors according to the performance level at which they occur. *Mistakes* are errors at the rule-based and knowledge-based levels. Humans make them due to picking an inappropriate/deficient rule or incomplete/inaccurate understanding of the system. *Slips* are errors at skill-based level. They are execution failures, in which the user decides on an action, but the result is not what was intended. For example, selecting a wrong item on a menu.

As we have shown in Section 3.3.3 behavioural errors in authentication ceremonies may result in a protocol step not achieving the desired goal, users skipping a required step or performing an action incorrectly. [194, 144, 135] For example, the user may not pay enough attention to a website login prompt or examine it in detail to notice that it does not look correct before submitting his/her password. Karlof et al. [135] and Herzberg and Margulies [110] show that security can be achieved by regulating human node behaviour via use of forcing functions. A forcing function is a type of behaviour constraint designed to prevent human error by preventing a user from progressing in a task until the user performs a specific action, i.e. a forcing function prevents the user skipping a required step.

An important consideration in our research was also to consider the fact that the

user is likely to try to circumvent the excessive security demands in order to accomplish his/her primary task. The *predictability* of behaviour is also very important, as phishers may exploit it. For example, a choice of passwords depending on gender or race [173].

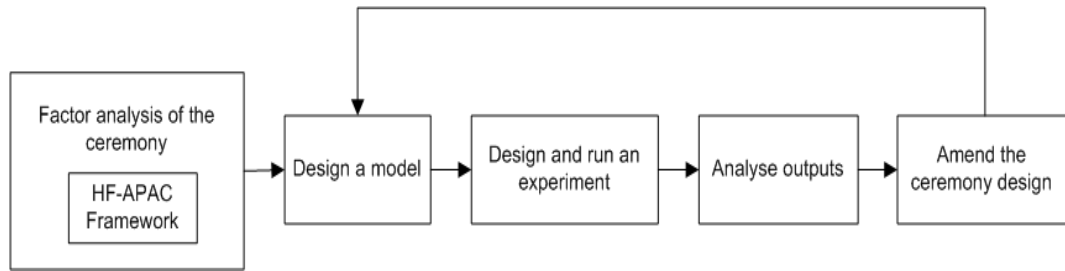
## 4.4 Applying the Framework

The HF-APAC Framework was designed as a constructive way of analysis of human communication factors affecting anti-phishing security of authentication ceremonies. The Framework helps in extending the ceremony's threat model by specifically taking into account issues and factors affecting processing of authentication communication by human users, that can affect their phishing detection.

The next sections describe how it can be applied to improve the design of either an existing, or a new ceremony.

### 4.4.1 Design and Analysis Process of an Existing Ceremony

The Framework can be used by designers of authentication ceremonies at the threat analysis phase to improve the human interface weak points of a ceremony and reduce the success of phishing attacks. In the factor analysis phase a designer analyses the components and factors of the Framework that pertain to the authentication ceremony being designed. In general, models place values on some of the variables identified as important in a framework, present relationships among the variables, and make predictions about likely outcomes [168, 195]. A model that places a specific value on the components of the HF-APAC Framework identified as important in the ceremony is then designed. An experiment is then designed and conducted to evaluate the model hypotheses and provide empirical evidence as to which factors improve or reduce phishing resistance. After the data analysis phase, the ceremony



**Figure 4.3:** Design and analysis process of human communication factors in authentication ceremonies with the HF-APAC Framework

design can be amended if needed. The model can be modified accordingly, and the experiment re-run.

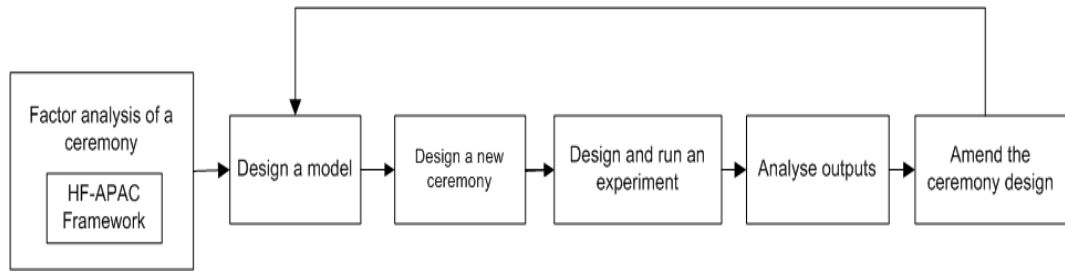
The application of the HF-APAC Framework in ceremony analysis, shown in Figure 4.3, can be summarised as follows:

1. Identify the components and factors of the HF-APAC Framework that are important for the context in which an authentication ceremony is being used.
2. Design a model that places values on the identified components of the HF-APAC Framework.
3. Design and run an experiment to evaluate the factors.
4. Analyse outputs.
5. Amend the ceremony design if necessary.

This process can be modified for a design of a new ceremony (Figure 4.4).

#### 4.4.2 New Ceremony Design Process

Ceremony design and analysis process with the HF-APAC Framework for a new ceremony is shown in Figure 4.4 and can be summarised as follows:



**Figure 4.4:** New ceremony design and analysis process with the HF-APAC Framework

1. Identify the components and factors of the HF-APAC Framework that are important for the context in which an authentication ceremony is being used.
2. Design a model that places values on the identified components of the HF-APAC Framework.
3. Design a new ceremony according to design principles suggested by a model.
4. Design and run an experiment to evaluate the factors.
5. Analyse outputs.
6. Amend the ceremony design if necessary.

We demonstrate this usage of the Framework with the Model for Analysing HF-APAC, described in Chapter 5 and a new, MSMA, ceremony (Chapter 6).

## 4.5 Conclusion

In this chapter, we presented the Human Factors in Anti-Phishing Authentication Ceremonies (HF-APAC) Framework that can help in security analysis of authentication ceremonies. The Framework helps in extending the ceremony's threat analysis by taking into account issues and factors affecting processing of authentication communication by human users, that in turn can influence their phishing detection. A

review of existing anti-phishing authentication ceremonies and identification of issues and factors affecting human communication processing presented in Chapter 3, particularly Sections 3.3.2 and 3.3.3, helped us in identifying the components of the Framework.

We described the place of the HF-APAC Framework in a broader ceremony analysis followed by a detailed description of its components. We proposed a design and analysis process of human communication factors in authentication ceremonies with the HF-APAC Framework and described how it can be applied either to improve the design of an existing ceremony or when designing a new one.

Chapter 5 presents the Model for Analysing HF-APAC that demonstrates how the HF-APAC Framework can be used as part of the proposed ceremony analysis process.

# Chapter 5

## Model for Analysing HF-APAC

### 5.1 Introduction

This chapter presents the *Model for Analysing HF-APAC* that demonstrates the usage of the HF-APAC Framework by a ceremony designer. Sometimes we refer to it only as *the Model*. Most of the work presented in this chapter was published in [106].

Models place values on some of the variables identified as important in a framework [195, 168]. The Model for Analysing HF-APAC places values on the components of the HF-APAC Framework identified as important in anti-phishing ceremonies that use HPAs as part of the authentication process. It explores to what extent the identified components influence each other.

The main purpose of the Model is to explore how users process authentication communication conveyed through a website login prompt and what influences their decision-making process and behaviour, that can ultimately result in an error of submitting login credentials to a phishing website.

This chapter is organized as follows. The next section presents the Model elements. After that we present the development of hypotheses. We then present the human communication processing assumptions proposed by the Model.

## 5.2 The Model Elements

In this section we describe the elements of the Model and how they correspond to the specific factors of the components of the HF-APAC Framework.

Models place values on some of the variables identified as important in a framework [195, 168]. The Model for Analysing HF-APAC considers and tests specific factors of some of the components of the HF-APAC Framework, described in Section 4.3.1 and summarised in Table 4.1.

The Model for Analysing HF-APAC is grounded in the prior research in information processing and decision making [132, 131, 95, 71, 177, 71, 217, 218], the most important were reviewed in Section 2.5.3. The review points to attention and elaboration as being the main information processing activities that underpin the users' evaluation of deceptiveness.

The human information processing activities are structured into two main separate sub-processes: *attention* and *elaboration* [71]. Attention to phishing indicators, or a fake login prompt, is a necessary but not sufficient condition for detecting phishing deception. Users also need to elaborate on the indicators. During elaboration, users make conscious connections between the elements they observe and their prior knowledge. [217] The *attention* to the ceremony communication and the *elaboration* on discrepancies between what is observed and what is expected are important components in HF-APAC Framework and also important elements of the Model.

### Communication via Input/Output

The model classifies authentication ceremonies with regard to a specific communication type (i.e. tasks) that the user is required to perform. Many authentication ceremonies consist of either recall or recognise or their combination. Specific issues may arise from each communication type, most notable, the demand on users' memory [193]. Other issues that may arise are described in Sections 4.3.1 and 3.3.3.

Hence, the types of communication and their combinations that the Model considers are:

- Recall. Typically used in traditional username/password authentication.
- Recognition. In a typical login procedure for recognition-based, graphical passwords ceremonies, the user would see an image and must recognise it. Examples are: Passfaces [174], Dynamic Security Skins [55], PhorceField [101].
- Combination of recognition and recall. In the simplest form, it is provided as a combination of a security image and caption [228, 192].

The communication is an authentication ceremony login prompt webpage. It is conveyed to the user via input/output elements, directly corresponding to the communication and the input/output components of the HF-APAC Framework. The login page may be spoofed. If used in phishing attacks it perhaps contains at least some false content which may or may not be noticed by the user. We assume that the security mechanisms for detecting phishing webpages are in place, but may or may not be noticed by a user. The ceremony relies on the human to perform authentication steps bound to the login webpage and to decide whether to proceed giving their credentials; essentially deciding if the webpage is legitimate or not.

### **Attention**

Attention is the first stage in communication processing [178, 222] and in our model it is the attention given to either a recall or recognise authentication task. We assume that an attention switch has happened - as the user is prompted with a login page. The *format* and the *size* of the HPA will influence the switch, as described in Sections 4.3.1 and 3.3.3. Different authentication ceremonies will influence the *length* that attention is maintained, and appropriate factors are considered. Hence, the attention element in the Model comprises the attention switch and attention maintenance of the HF-APAC Framework (Section 4.3.1).



## **Capabilities**

The HF-APAC Framework distinguishes the following capabilities that can affect the communication process in authentication ceremonies: *memory, comprehension, knowledge* or some other *cognitive or physical skill* (Table 4.1). The capabilities element of the Model considers the knowledge of the ceremony and web security factors. That is, users knowing what credentials are expected to be sent/received to/from a server and having a knowledge about web security. Users' knowledge, or rather the lack of it, has been exploited by attackers [38, 57, 226].

## **Motivation**

The motivation element considers risk perception and distraction from primary task as factors of the corresponding motivation component of the HF-APAC Framework. Risk perception is assessed by the perceived importance of a particular website to the user and also how busy the user is with the primary task. (Section 4.3.1, [202])

## **Elaboration**

Users need to make conscious connections between the communication they observe and their prior knowledge, i.e. they need to elaborate on the communication to detect phishing. Previous research in communication processing of phishing emails suggest that users who do not attend to the emails upon receipt would neglect to elaborate on the information received, increasing the likelihood of making a wrong decision. [218, 123, 223, 217, 100] The elaboration element considers the cognitive effort the user puts into assessing the authentication communication they observe and make connections between the presented communication and their prior knowledge and experience.

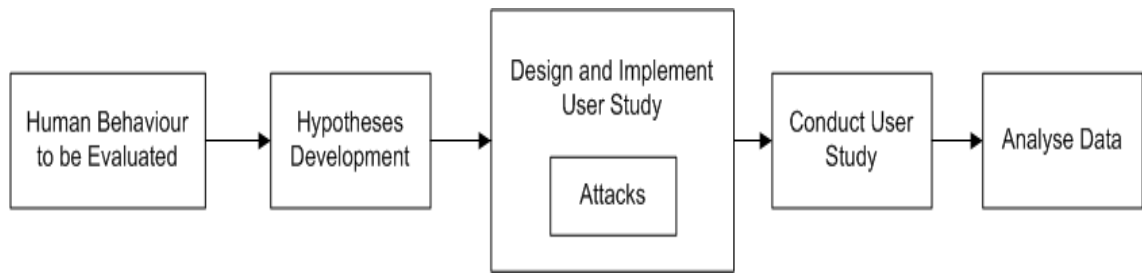
## Behaviour

The specific human behaviour that the Model evaluates is whether the user performs an action incorrectly. In this case the action is to *notice* if the login prompt is spoofed; or to make an error and get phished. The model tests how users process communication messages in authentication ceremonies and determine if they are genuine or not. Specifically, how the number and combinations of recall and recognise communication types influences the user’s decision-making processes and consequently their decision outcomes, regarding submitting the credentials to the website.

## 5.3 Evaluation Methodology

We used *the hypothetico-deductive* method from empirical social sciences research [89, 76] to test the Model. The hypothetico-deductive experimental method is generic enough to be applied in the design and implementation of user related experiments for socio-technical systems (systems that depend on how human use technical ‘parts’). It starts with the definition of the research questions to be explored. It is followed by developing hypotheses to answer the research question. The process continues with the definition of the most appropriate research methodology (e.g. user studies, surveys, laboratory experiments, interviews, surveys) to test the hypotheses. The next step is to design and implement the selected methodology. After that the experiment is run and output data is collected, analysed and interpreted. What is important for our research is that the hypothetico-deductive method can be adapted to different socio-technical scenarios and that different research methodologies can be combined to collect empirical data in order to evaluate the hypotheses [76].

We applied the hypothetico-deductive method as follows (shown in Figure 5.1).



**Figure 5.1:** The Model evaluation methodology

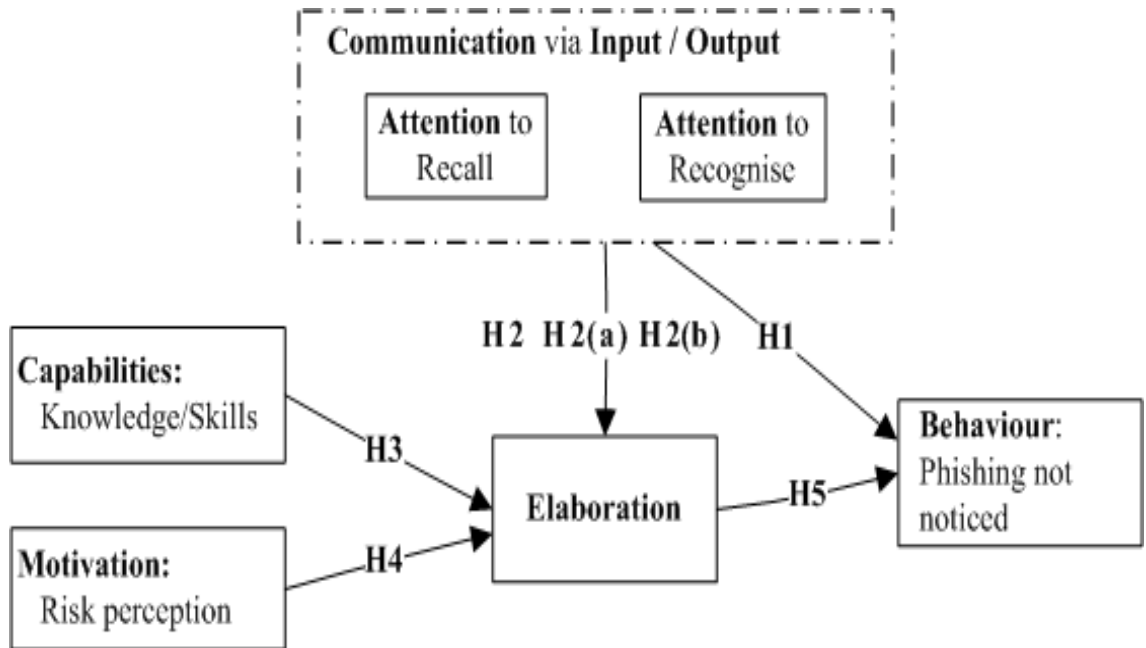
The research question was specified in the human behaviour to be evaluated. Once the hypotheses were developed, they needed to be evaluated. As the Model for Analysing HF-APAC involves research constructs, such as attention, motivation, and capabilities, we needed to use quantitative data to test the Model hypotheses. We collected empirical data by performing a *user study* in order to evaluate the hypotheses. The user study design is presented in Chapter 7. Data analysis and results of the user study are described in Chapter 8.

### **Human Behaviour to be Evaluated**

The specific behaviour to be evaluated is whether the user will *notice* if the login prompt is spoofed, or to make an error and get phished; and what and how influences their decision-making process, that can ultimately result in an error of submitting login credentials to a phishing website.

#### **5.3.1 Hypotheses Development**

The Model for Analysing HF-APAC, with suggested hypotheses, is presented in Figure 5.2 and detailed below in terms of the key constructs laid out in previous sections.



**Figure 5.2:** Model for Analysing HF-APAC and hypotheses

### 5.3.1.1 Communication Processing Activities

Attention is the first stage in communication processing and indicates the amount of mental focus given to a specific element of communication presented via input/output. The attention paid to each communication component might have a distinctly different influence on the user’s likelihood to detect a fake login page. Apart from paying attention to the communication, users need to elaborate on the details, in our case on the credentials needed to be entered or evaluated. Research shows that users who elaborate on communication details are more likely to understand, learn, retain and recall the information than users who merely pay attention to them [42].

*Recall and Recognition.* Many anti-phishing ceremonies suggest a challenge-response mechanism where the user is supposed to verify a website by a set of pre-agreed credentials. Current practices involve using challenge questions or graphical passwords. Graphical passwords schemes generally expect a user to recognise a

previously registered image. Seeing a login prompt that does not include a familiar image allows a legitimate user to immediately realize that she entered an invalid text or graphical password (and then go back to re-enter it). It prevents an attacker from knowing that the text or graphical password tried is invalid.

During a normal login, users must perform an image recognition task, which is relatively easy for humans. During a phishing attack the right image(s) may not be present, therefore the user will not be performing a recognition task, but the recall of trying to remember the right image(s), i.e. during a recall phase.

Recall requires that a user remembers information without cueing. It is generally accepted that recall is substantially harder, and will require an extra cognitive effort during elaboration phase, which otherwise may be used to notice phishing indicators. Human ability for recognition far exceeds that for recall. Stobert [205] showed that it is easier to memorise recognition-based graphical passwords, but their usability was limited by slow login times. A graphical password scheme that utilised recognition and recall memory was most successful at combining memorability and usability. Stobert's explanation is as follows: recognition memory involves making a binary decision for each image while traversing the entire image set (on offer). Using this decision-making process to recognise an entire password can be very slow. In contrast, recall memory involves fewer but more complex tasks. The user is less likely to successfully complete these tasks, but when successful, the process is faster, as it can often be typed from muscle memory [32]. Hence, time to login should be longer during a phishing attack, i.e. during a recall phase.

Recent studies explored whether users will login in spite of the security image being absent or replaced with a static 'under maintenance' image [144, 194]. They have shown that single site-authentication security images are generally not very effective. Therefore, we wanted to explore whether requiring participants to interact with multiple site-authentication images in combination with text passwords

improves effectiveness of using images as part of authentication process.

We assume that a login prompt to recall a password, enter it and/or recognise an image(s), forces a user to pay the attention to it. We seek to explore how much the user elaborated on these additional communication factors and whether it lowered the likelihood of the user getting phished. Hence:

**H1:** Increased Number of recall and recognise Communication factors of the authentication ceremony will result in a lower likelihood of a user making an error during the authentication process, i.e. getting phished.

**H2:** Increased Number of recall and recognise Communication factors of the authentication ceremony will lead to increased Elaboration of the authentication login prompt.

The model distinguishes between the specific communication component types and how they may influence human behaviour. The attention paid to each of these components might have a distinctly different influence on the user's behaviour. Hence we posited the following hypotheses:

**H2(a):** The level of Attention given to the Recall communication factor of the authentication ceremony will be negatively related to the level of Elaboration.

**H2(b):** The level of Attention given to the Recognise communication factor of the authentication ceremony will be positively related to the level of Elaboration.

### 5.3.1.2 Impact of Capabilities

A user's knowledge of the ceremony steps is considered an important factor that affects elaboration. It ties in with a user awareness and training approach for reducing user phishing susceptibility. Consistent with this approach, we expect increased ceremony knowledge to influence user phishing likelihood indirectly, by influencing the user ability to effectively elaborate and find anomalous or deceptive information.

**H3:** Increased Capabilities will lead to increased Elaboration of the authentication login prompt.

#### **5.3.1.3 Impact of Motivation**

The concept of motivation is important in understanding human information processing. We define motivation as the perceived relevance of a particular website to a user. Generally, information processing is more likely to occur when the user finds the services offered by a website sensitive to his/her needs and is thereby motivated to consciously evaluate website credibility. Also, the motivation to elaborate will be hampered by the need or urgency of the primary task, to be completed after the login to the website. Hence:

**H4:** Increased Motivation will lead to increased Elaboration of the authentication login prompt.

#### **5.3.1.4 Impact of Elaboration on Phishing Detection**

The influence of elaboration in phishing detection is supported by prior research [57, 123]. We posit that users are more likely to fall victim to a phishing login webpage because they fail to elaborate on additional credentials, thereby failing to make connections between what they are presented with and the knowledge stored in their memory.

**H5:** Increased Elaboration will result in a lower likelihood of the user making an error during the authentication process, i.e. getting phished.

## 5.4 Human Communication Processing

The human communication processing assumptions proposed by the Model hypotheses can be summarised as follows:

1. Increasing the number of recall and recognise communication factors results in a higher phishing detection rate.
2. Increasing the number of recall and recognise communication factors results in increased elaboration.
3. Increased elaboration will result in a lower likelihood of the user making an error during the authentication process, i.e. getting phished.
4. Increased attention to recall communication factors of the authentication ceremony results in less elaboration.
5. Increased attention to recognition communication factors of the authentication ceremony results in more elaboration.
6. Increased user's motivation leads to increased elaboration.
7. Increased user's knowledge of the ceremony and online security leads to increased elaboration.

The assumptions 1 to 5 can be used by *ceremony designers* when designing (or evaluating) authentication ceremonies to improve anti-phishing resistance. We specifically applied the assumption 1 as part of the design of MSMA, a novel authentication ceremony, presented in Chapter 6.

The assumptions 6 and 7 could also be used by *system designers* to choose the most appropriate authentication ceremony for the particular user profile (e.g. technical knowledge) or the application context (e.g. if used in e-commerce or less security demanding environment).



## 5.5 Conclusion

The Model for Analysing HF-APAC is a communication processing model that demonstrates how the Human Factors in APAC Framework can be used as part of the design process of authentication ceremonies described in Section 4.4. The Model considers and tests specific factors of some of the components of the HF-APAC Framework, described in Section 4.3.1 and summarised in Table 4.1. The Model examines how users process authentication communication tasks and how these tasks impact the users decision-making and consequently their phishing detection.

The Model proposes human communication processing assumptions that can be used during the design of authentication ceremonies. In Chapter 6 we show how these assumptions can be used as part of the design of a novel ceremony called MultiStep Mutual Authentication (MSMA).

We evaluate the Model experimentally by performing a user study described in Chapters 7 and 8.

# Chapter 6

## MultiStep Mutual Authentication (MSMA) Ceremony

### 6.1 Introduction

This chapter presents a novel MultiStep Mutual Authentication (MSMA) anti-phishing ceremony. MSMA demonstrates how the HF-APAC Framework can be applied during the design and analysis process of a new authentication ceremony, as described in Section 4.4.

The aim of MSMA is to make it more effective for the user to establish the legitimacy of a website, i.e. provide mutual authentication, and mitigate a phishing attack. MSMA combines PIN, text passwords and recognition-based graphical passwords in a multi-step process. The graphical part of MSMA authentication is a HPA and enables the user to verify that the website, he/she is accessing, is legitimate. The HPA provides server authentication to the user.

This chapter provides a detailed description of the MSMA protocol used between the user and the user interface. We also outline a secure protocol between the client and server upon which the MSMA ceremony can be built. In particular, how

MSMA can be built on an adaptation of the Delayed Password Disclosure (DPD) [127] protocol developed by Jakobsson and Mayers.

The MSMA design was published in [107].

## 6.2 Design Goals

The MSMA ceremony design is a result of the research described in previous chapters and is built to satisfy the following requirements. We aimed to show how to apply some of the human communication processing assumptions developed as part of Model for Analysing HF-APAC, described in Section 5.4 and also discussed in Chapter 3. The specific assumption we applied was that increasing the number of recall and recognise communication factors would achieve higher phishing detection rates. This demonstrates the application of the HF-APAC Framework during the design and analysis of a new authentication ceremony (Figure 4.4). Another aim was to mitigate phishing attacks by creating a HPA based trusted path between the user and a server, via the user interface (i.e. website login prompt).

In this section we describe how these requirements are met and also how they are combined with other anti-phishing design principles.

### Human Perceptible Authenticator

A number of ceremonies have been proposed that address the phishing problem by creating a trusted path between the *user interface* (normally via a browser) and the *user* [55, 18, 45, 230]. Some of them use a variation of graphical passwords to create a trusted path using a HPA, for example BBMA [86] or PhorceField [101]. What is similar among these approaches is that images are used as a HPA for the user to verify that the website the user is accessing is legitimate. The same images may or may not be used as part of the user authentication to the server.

To establish a *trusted path* from the user to the server, our aim was to create

a ceremony in such a way that an attacker can not easily present a credible login prompt to their victims. MSMA satisfies this requirement by presenting users with feedback as they enter their passwords. This feedback is a HPA [86] that authenticates the server to the user. This, HPA enabled, trusted path provides *mutual* authentication between the user and the server, as the server authenticates itself via HPA providing the user with assurance that the login prompt is legitimate. The HPA is created during the registration phase and is stored at the server and memorised by the user.

The HPA can be anything, but we have chosen a visual HPA, to be provided in the form of images, rather than a piece of music or excerpt from a book. This was to leverage the picture superiority effect [171]. The picture superiority effect is a human psychological trait that postulates that humans have better memory for images than words. It is attributed to the brain's dual coding feature. According to dual coding theory [170], the human brain encodes visual information in two ways: a visual form corresponding to the image, and also in a verbal descriptive form. This dual encoding makes it easier to remember an item than if it was coded one way. The choice of images for visual feedback is also in line with our human communication processing assumptions suggested in Section 5.4. Using images as a feedback should lead to an increase in attention given to recognition communication factors and a higher detection of visual deception attacks.

For the visual feedback, i.e. image to be recognised, a cognometric graphical password scheme is used. Cognometric schemes present users with a set of distractor images and request that the user recognise and identify images belonging to their set of password images. The MSMA user is presented with a grid of images, where one image belongs to a known set of password images, and the other images are distractors.

## Distractor images

Distractor images were added to the design as they exploit strengths of human memory that helps in resisting phishing attacks. They leverage the strengths of recognition memory in the presence of the right image being displayed [171, 173, 205, 30]. The phisher would have difficulties to present image sets to the user containing the images belonging to the user's set of password images. Therefore, during a phishing attack users would experience memory interference while looking through distractor images without recognising their own image. [101] The user would then use a recall memory, as the right image would not be displayed to be recognised. Recall memory requires more effort and would cause errors or suspicions which may cause a user to give up login. This behaviour should help foil a phishing attack.

## Forcing functions

The user may ignore the fact that his/her image is not present among the set of distractor images displayed, and start entering the text password. In order to safeguard against this type of behaviour we introduced a *forcing function*.

Forcing functions are constraints used by designers in the human reliability area to help prevent human errors in safety-critical environments [165]. They were also shown to be a useful tool in regulating human node behaviour in security ceremonies [135, 110, 38]. They are designed to prevent the user from progressing in a task until they perform an action which must be taken to avoid a failure. The user is prevented from skipping a required step, as skipping the step may result in a security failure, as we described in Sections 3.3.3 and 4.3.1.

We introduced a forcing function to prevent the user skipping a task of recognising the right HPA, i.e. an image, among the displayed distractor images. This forcing function prevents an MSMA user from entering a part of the text password without first selecting an image from the set of distractor images. This should help

Symbol	Logical context	Reads as
$\wedge$	conjunction	'and'
$\vee$	disjunction	'or'
$=$	equality	'is equal to'
$\in$	set membership	'is in'
$\notin$	negation of set membership	'is not in'

**Table 6.1:** Logical notation

the user to foil a phishing attack in which a set of the distractor HPAs not containing the right HPA is presented.

### Communication factors

The decision to have PIN, text password and images as part of the user authentication was based on the following.

First, most users are now using tablets or smartphones and are used to entering PINs as part of authentication. Therefore, using PIN and text password largely preserves the existing user sign-in experience, given their resilience and persistence [109].

The second reason was the application of our human communication processing assumptions proposed by the Model for Analysing HF-APAC (presented in Section 5.4); specifically, that increasing the number of recall and recognise communication factors should result in a higher phishing detection rates. The PIN, text password and images are MSMA communication factors

## 6.3 Ceremony Analysis Approach and Notation

This chapter contains logical expressions. In Table 6.1 we present the logical symbols used, followed by how they are read in English.

<b>Symbol</b>	<b>Explanation</b>
$U, u, UI$	User, username, user interface
$C$	Client - application
$S$	Server
Password	Text password
$C/S$ Protocol	Authentication protocol between client and server
PIN	Personal Identification Number
$\Sigma$	The alphabet for text password
$l$	The length of the password in characters; and The number of images in a set for HPA
$T = (t_0, \dots, t_{l-1}) \in \Sigma^l$	Text password
$A$	Set (database) of images for HPA
$\overrightarrow{HPA} = (a_0, \dots, a_{l-1}) \in A$	HPA - vector of images corresponding to password T
$\vec{\alpha} = (\alpha_0, \dots, \alpha_{v-2}) \in A$	Vector of distractor images
$F = (u, PIN, T, \overrightarrow{HPA})$	Pseudo - random function
$m = (a'_0, \dots, a'_{v-1})$	Visualisation message with distractor images
$v$	The number of images in visualisation message
$pw$	User's credentials

**Table 6.2:** Notation used in describing MSMA ceremony

The notation we use for protocol description is presented in Table 6.2 and described below. An apostrophe (') symbol beside a variable indicates the value of the variable selected or entered by the user via the user interface during the MSMA login, rather than the pre-registered variable value, without an apostrophe.

We developed the notation specifically to present human interaction, i.e. the user to user interface (UI) part of MSMA. That should help to formalise a threat analysis that specifically takes into account the human user limitations as a potential threat.

We define functions **select** and **enter** as a generic user input/output communication without considering a medium to be used, e.g. it can be achieved via a mouse click, keyboard, touch, vocal, visual, or using eye gaze (e.g. with an eye tracker).

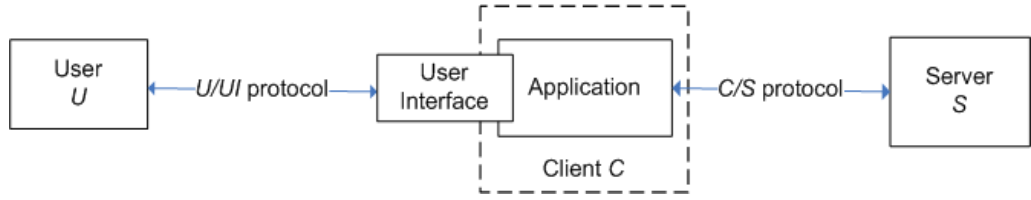
We define the following functions analogue to Gajek’s usage in BBMA protocol [87]. To model the communication from the user to user interface, we define functions **render** and **recognise**. Visualization message  $m$  contains the login communication factors and is created by the user interface function **render**. The human perception function **recognise** denotes processing of this visualization message  $m$ , i.e. login communication factors and tasks required to be accomplished. Upon receiving a visualization message  $m$  from the user interface, the user calls the function **recognise** which takes as input the protocol message  $m$  and the rendered HPA and returns the appropriate output.

MSMA considers the following participants:

- User - human users or human node.
- User Interface - includes user interface of the application (i.e. service provider’s login prompt displayed by a browser).
- Client - non-user interface application processing; includes user interface and the client side of the application (i.e. service provider’s website).
- Server - Includes all protocol specification, together with the interaction of server with client side of application, which we refer to as *client/server (C/S) protocol*.

The MSMA ceremony is used to demonstrate how the HF-APAC Framework can be applied during the design and analysis process of a new authentication ceremony, as described in Section 4.4 and presented in Figure 4.4. The MSMA ceremony analysis is illustrated in Figure 6.1. It builds on our ceremony analysis approach and the place of the HF-APAC Framework in it, depicted in Figure 4.1. The User





**Figure 6.1:** MSMA ceremony analysis

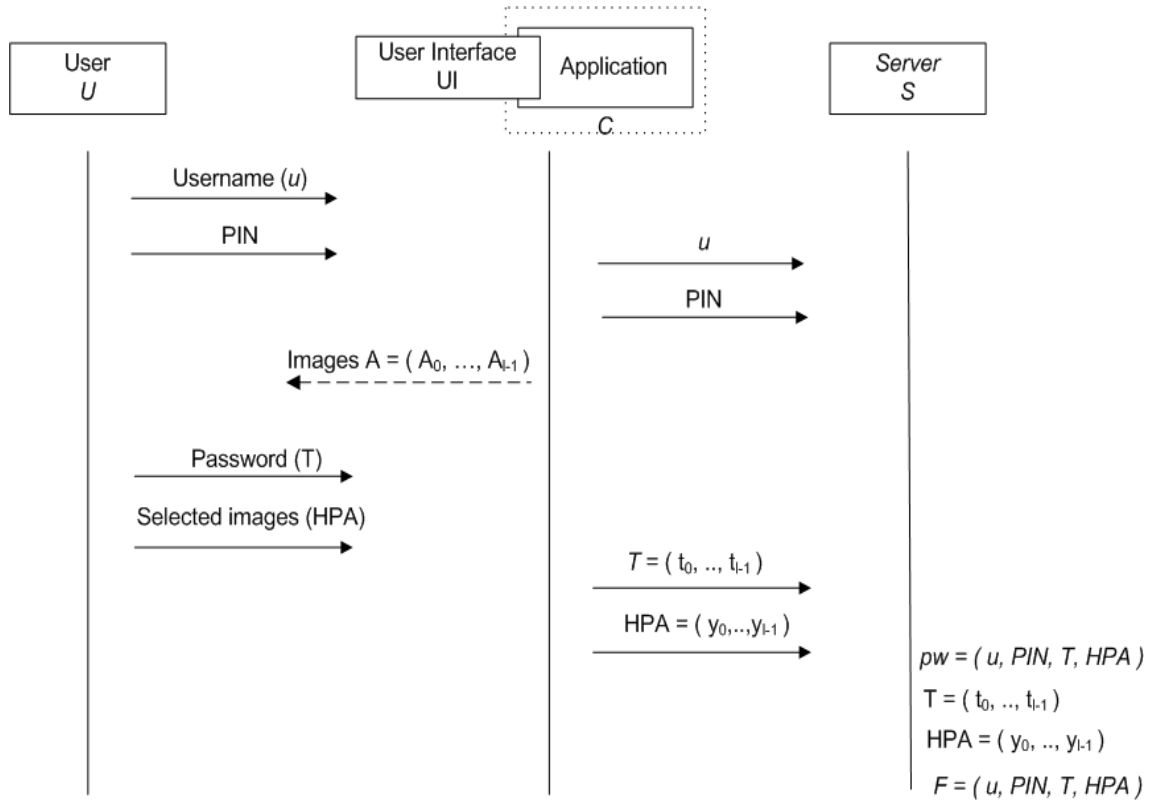
(Figure 6.1) corresponding to the Human Node (Figure 4.1); the User Interface, delivered using U/UI protocol (Figure 6.1), corresponding to the Communication and Input/Output components of the HF-APAC Framework (Figures 4.1 and 4.2).

As our research focus is on modelling and analysing the communication processing performed by human users in ceremonies, we give the detailed description of the protocol between the user and the user interface (*U/UI* protocol). The protocol between client and server (*C/S* protocol) is described in less detail. This protocol can be realised in different ways. The description of *C/S* protocol we present is largely based on Jakobsson’s DPD protocol [127] which was chosen as the most appropriate to build the MSMA upon. In our description we refer to where the DPD protocol can be directly incorporated or suggest an alternative approach. DPD is built on top of Oblivious Transfer (OT) and PAKE [25]. DPD also introduces an important blinding technique that is used to reduce the costs of communication and computation of the OT component. A high level description of DPD was given in Chapter 2.

We describe the setup and the operation of MSMA ceremony in next sections, illustrated in Figures 6.2 and 6.3, using notation presented in Tables 6.1 and 6.2.

## 6.4 MSMA Setup

Before MSMA can be executed, a setup, or registration phase, is necessary to establish shared secrets between the user and the target website, i.e server. No shared



**Figure 6.2:** MSMA Setup

secrets between the user machine and the target website are pre-established. As part of the registration, the user specifies a username, a PIN, a text password and a number of images. To prevent, so called, birthday-based guessing attacks, it is recommended to have a PIN randomly assigned [33].

The text password is divided into parts; each part corresponds to one of the chosen images, e.g. the first character of the text password corresponds to the first image; the second character corresponds to the second image; and so on.

The HPA provides server authentication to the user. From the protocol's point of view, the HPA is a vector of images  $\overrightarrow{HPA} = (a_0, \dots, a_{l-1})$  that corresponds to each user's username, PIN and text password. From the user's point of view, the HPA images correspond to the characters of the text password. The user only needs to be able to associate the first character of the text password to the first image of HPA;

the second character corresponds to the second image and so on.

MSMA setup proceeds as follows. The user is prompted to choose a username and PIN. The uniqueness of the username is checked. If satisfied - the user is prompted to enter characters of the text password and associate images with it. The images presented are the images from a database of images  $A$ . The images are offered sequentially for the user to choose in size and format defined as  $A = (A_0, \dots, A_{l-1})$ .

MSMA allows the database of images to be stored either on the user's device or the server. Those design decisions can vary depending on the details of the protocol between the client and a server. During the operation of the protocol it may be slow to transfer a large number of images from server to the client. One approach, as suggested by Jakobsson and Mayers [127] is for the server to have a database of indexes to images (instead of a database of images). The client then uses the index to generate the images from a local database. This solution would not be feasible in cases of users that use a large number of semi-trusted devices or public terminals.

$\Sigma$  is the alphabet over which the password is chosen,  $l$  is the length of the password in characters, which also determines number of HPA images, and the number of *rounds* of HPA verification. We refer to HPA verification steps, i.e repeated server authentication, as *rounds*. The image set in round  $n$  is pseudo-randomly generated from a seed value derived from the entered username and PIN in Round 0, and from the images selected in previous rounds, up to Round  $n - 1$ , when  $n \geq 1$ .

Therefore, the password used for server authentication consists of a vector of images  $\overrightarrow{HPA} = (a_0, \dots, a_{l-1})$  associated with text password  $T = (t_0, \dots, t_{l-1}) \in \Sigma^l$ . The PIN and text password are used for user authentication to the server.

At the end of the setup phase, the user's credentials  $pw$  consist of username, PIN, text password and a HPA - images corresponding to each of the characters in the text password, as shown below and in Figure 6.2:

$$pw = (u, PIN, T = (t_0, \dots, t_{l-1}), \overrightarrow{HPA} = (a_0, \dots, a_{l-1}))$$

The server then creates a function  $F$ , a pseudo-random function (PRF), that is associated with user's credentials. This function can be used as part of client/server protocol to check the matching between each  $t_i$  character entered and the value of the matching image  $F(a_1, \dots, a_j)$ . This function can then be used to compute an additional pseudo-random function to be used for a protocol between the client and the server.

An example PRF is provided as part of the DPD [127] protocol. Another use of PRFs is in verifier-based protocols between client and the server, such as Secure Remote Password Protocol (SRP) [227], where a PRF can be used as a verifier that the user recognised an image displayed and entered the right portion of the text password, without revealing neither the image nor the text password to the server.

#### **6.4.1 User Training**

As part the setup phase, a short user training session is used to improve memorability of the HPA, i.e. images corresponding to the text password parts. The setup and the training should be conducted in a secure environment, where no other person can see the image sets, to avoid shoulder-surfing attack.

### **6.5 MSMA Operation**

As part of the MSMA operation (i.e. login phase), the username and PIN are used in step one. In subsequent steps, a combination of a graphical and a text password is used. The HPA, set of distractor images together with the correct one, are presented after the user enters his username and PIN and provide visual server authentication. The user enters the text password in parts: each part may consist of a number of characters/digits. Each of the text parts is augmented by one HPA (i.e. an image).

MSMA can be adapted to have fewer or more steps, depending how many seg-

ments the text password is divided into. The segment size can vary. Further on, we assume that each segment of the text password consists of *one* character.

If the user is presented with an HPA that does not contain the image corresponding to the next part of text password, the user should halt entering the text password to avoid disclosing all parts to a spoofed website.

If either the PIN or the image selected by the user in a previous round is incorrect, the image set presented to the user will not contain the image corresponding to the next part of the text password. The same incorrect images are displayed, no matter how many times the protocol is invoked to prevent a variation of a dictionary attack. The example attack would be as follows: an attacker would guess the first character of the password, and look at the images displayed [127]. By repeating the login attempt with the same first character, the attacker would establish if this was the correct first character of the password, and then for the next character, etc.

If the username, the PIN and the image selected by the user in the previous step are correct, the presented image set will contain the corresponding image as defined during the registration phase. All authentication credentials: the PIN, the set of images and the text password must be correct for a successful login.

To be able to enter a part of the text password, the user must first select an image from the presented HPA image set. This step was introduced as a *forcing function* so that the user would not ignore the HPA and proceed entering passwords without checking if the correct image is displayed. It is modelled as the human perception function `recognise` as follows; upon receiving a visualization message  $m$  from user interface, the user calls the function `recognise` which takes as input the message  $m$  and the rendered HPA, and outputs `true`, when the message contains the right corresponding HPA (i.e. an image) from the  $\overrightarrow{HPA}$ . Otherwise, `recognise` outputs false.

Figure 6.3 illustrates MSMA interaction between user  $U$ , user interface (UI),

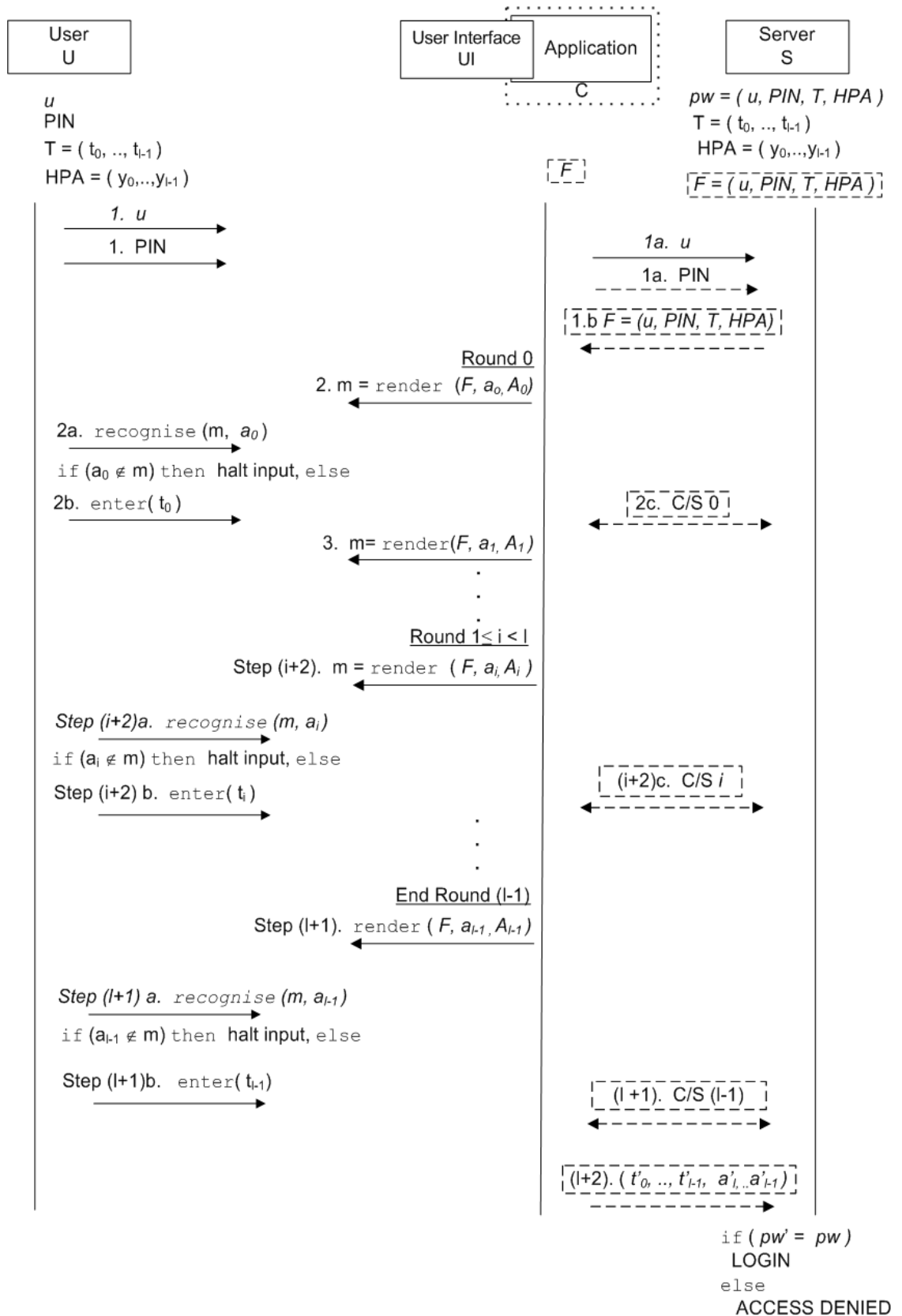


Figure 6.3: MSMA Operation

client  $C$  (i.e. application) and server  $S$ . Boxed messages denote a protocol between the client and the server. The interaction steps are described below.

**1.** The user  $U$  initiates the ceremony by communicating the server's URL to the client's application ( $C$ ) and enters username  $u$  and PIN in the user interface  $UI$ .

**1a.** The client  $C$  sends the username  $u$  and PIN to the server  $S$ .

**1b.** The server  $S$  sends user specific pseudo random function

$F = (u, PIN, T, \overrightarrow{HPA})$  to the client  $C$ .  $F$  is used by the visualization function **render** to form the login prompt.

**2.** The user interface (UI) presents the message  $m = \mathbf{render}(F, a_0, \overrightarrow{A_0})$  to the user. If the PIN and username match, then the distractor image set  $\overrightarrow{A_0}$  will contain the right  $a_0$ , otherwise not.

**2a.** If the user does not recognise the HPA, (i.e.  $\mathbf{recognise}(m, a_0 \notin m)$ ) then stop input of text password. Otherwise, proceed:

**2b.** User  $U$  selects  $\mathbf{select}(a'_0 \in m)$  and enters  $\mathbf{enter}(t_0)$ .

**2c.** C/S protocol Round 0 HPA verification is performed.

**3.** If the entered part of the text password is correct and the selected image is correct, i.e.  $(t'_0 = t_0) \wedge (a'_0 = a_0)$ , UI presents to the user visualization message  $m = \mathbf{render}(F, a_1, \overrightarrow{A_1})$ .

If the entered part of the text password differs from the pre-registered one, i.e.  $(t'_0 \neq t_0)$ , the visualization message  $\mathbf{render}(F, a'_1, \overrightarrow{A'_1})$  with the same incorrect distractor images is displayed for each round.

Steps 3a, 3b and 3c analogue to 2a, 2b and 2c are then performed.

For  $3 < i < l$  rounds of HPA verification are analogue to steps 3, 3a, 3b and 3c.

**Step (i+2).** Message  $m = \text{render}(F, a_i, \vec{A}_i)$  is presented to the user.

**(i+2)a.** If the user does not recognise the HPA, (i.e.  $\text{recognise}(m, a_i \notin m)$ ) then stop input of text password. Otherwise, proceed.

**(i+2)b.** User U selects  $\text{select}(a'_i \in m)$  and enters the  $i$  part of the text password,  $t_i$ .

**(i+2)c.** C/S protocol Round  $i$  HPA verification is performed.

Repeated steps until the End Round (l-1).

**Step (l+1).** Message  $\text{render}(F, a_{l-1}, \vec{A}_{l-1})$  is presented to the user. If  $(t'_l \neq t_l)$  the incorrect images are displayed.

**(l+1)a.** If the user does not recognise the HPA (i.e.  $\text{recognise}(m, a_{l-1} \notin m)$ ) then stop input of text password. Otherwise, proceed.

**(l+1)b.** User U selects  $\text{select}(a'_{l-1} \in m)$  and enters the  $(l - 1)$  part of the text password,  $t_{l-1}$ .

**(l+1)c.** C/S protocol End Round (l-1) HPA verification is performed.

**Step (l+2)** Client sends all  $(t_0, \dots, t_{l-1})$  to the server.

If all the username, PIN, the text password and all HPA images are correct, i.e.  $\text{if } (pw' = pw)$ , the login is successful. Otherwise, access to the account is denied.



## 6.6 Security Analysis

In this section we identify a number of possible attacks on MSMA that serve to impersonate the user and the server. We also discuss the main threats in the context of phishing attacks . An experimental evaluation of MSMA is described in Chapters 7 and 8.

### 6.6.1 Password Strength

The strength or randomness of passwords is often referred to as *entropy*. It is a measure of the amount of uncertainty that an attacker faces to determine the value of a secret and is usually stated in bits [36].

For text passwords entropy is measured as follows: a password of length  $l$  characters has entropy of  $l \times \log_2 t$  where the characters are selected randomly from a character set of  $t$  characters. For example, a 7 character password that is randomly generated from case sensitive Latin alphabet has  $7 \times \log_2 52 = 39.9$  bits of entropy. Character sets can also be digits only, hence the calculation also applies to PIN passwords. As the PIN is one part of the MSMA user authentication it should be acceptable to have 4 digit, randomly assigned PIN, which translates to 13 bits of entropy. Depending on the ceremony context, this can be increased to more digits.

Additional MSMA password strength is achieved with the text password and HPA. In reality, password space is usually much smaller than the theoretical password space [31]. Nevertheless, Florêncio and Herley [81] suggest that 20 bits of security is sufficient password strength for everyday computing, which translates to a 6 digit PIN approximately.

As the MSMA user password is formed from all three parts, the PIN, the text password and the HPA images, it improves the security of the password against both guessing and password capture attacks. Guessing entropy helps to determine

targeted, online password guessing attacks. Therefore, it is considered an important measure of the strength of an authentication system [36]. This added security from the HPA helps to strengthen the password against single or multiple account attacks. For the HPA password, one image is chosen in each round of HPA verification, i.e. the entropy for  $r$  rounds would be  $r \times \log_2 v$ , where  $v$  is the number of images in the visualisation message. For example, if there are 9 images in the visualisation message, each round represents  $\approx 3.17$  bits of entropy. It is recommended to have at least 3 rounds of verification which brings minimum entropy to 9.3 [36].

As the HPA (graphical part) is only used for server authentication, having 6 or 7 rounds would increase the entropy to 19 and 22.1 respectively which brings it to the recommended 20 bits of security for user's authentication [81]. Adding extra rounds would increase security, but also will affect usability as the length of the text password will be increased as well. This would increase user's memory demand and the effort which would inevitably affect overall ceremony usability [204].

### 6.6.2 Assumptions

As our focus is on the human part of the ceremony we do not analyse the security of the MSMA client/server protocol in the threat model. The security models of formally proven security protocols evolved to not only consider a passive attacker but also an active attacker as defined by Needham and Schroeder [162], which was further extended by Dolev and Yao [59]. Dolev and Yao [59] extended the attacker model, by adding that the attacker has complete control of the communication channels. Bellare and Rogaway's security model [27] concentrated on authentication and key distribution protocols. The most widely used security model for PAKE is the one suggested by Bellare, Pointcheval, and Rogaway [26]. In most of them heavy assumptions are placed on the human communication processing part of the protocols, which may cause a protocol to fail when implemented and used in real

world, as discussed in Chapter 3.

Our intention is that our *user to user interface* threat modelling may be used to complement the existing, well analysed security protocol models, to form more complete *ceremony threat modelling*.

#### 6.6.2.1 Attacker

We make the following assumptions regarding the underlying, i.e. network client/server, security protocol features and the attacker:

1. There is no attacker who intercepts the registration phase, i.e. setup of credentials.
2. The attacker is unable to corrupt the server. We do not consider malware attacks against the server, such as stealing the ephemeral and long term secrets stored inside the server.
3. The attacker is unable to corrupt the client. We do not consider malware attacks against the client, such as stealing the ephemeral and long-term secrets stored inside the client, i.e. a browser.
4. The main attacker is a remote, networked phisher with the following abilities:
  - Is able to eavesdrop, i.e. passively intercept communication between the server and client.
  - Is able to control the domain name resolution, and can mount phishing and pharming attacks.
  - Is able to direct selected victims from a target website to a website controlled by the attacker, i.e. mount a phishing attack at the user interface level.

### 6.6.2.2 User

Since the focus of ceremonies is not only on the client server communication, we need to explicitly define the set of premises for user communication.

1. The user is capable of performing basic information recall, such as remembering a low-entropy password.
2. The user is able to recognise the high-entropy HPA (i.e images).
3. The user does not understand the meaning of public key infrastructures, i.e. not able to identify servers based on certificates.
4. The user operates from a number of unsupervised client devices, such as personal computer; some of which may not have been used before.

## 6.6.3 Attacks and Countermeasures

### 6.6.3.1 Guessing Attacks

A guessing attack is an attack on the user's account where the attacker knows the username and tries to guess the rest of the password. Guessing entropy is an important measure of the resistance to targeted, online password guessing attacks [36]. Florêncio, Herley, and van Oorschots suggested [82] that 20 bits of entropy should be sufficient to protect against online guessing attacks. The password space, or the set of all possible passwords, of MSMA that spans PIN, text password and HPA images increases its resistance to this type of attacks. An adversary may attempt to impersonate the user by picking random images in the HPA distractor set, hoping that they contain the user's HPA. The user should recognise that the right HPA is not present even after one attempt. However, to prevent brute-force attacks, systems generally deny access after a small number of attempts. In the case of MSMA, the attacker must mount an attack on username, PIN, the text password

and all HPA images as the ceremony operation is not stopped if, for example, the PIN does not match the username. The HPA password guessing attacks must be done while interacting with the server (e.g. via real-time MITM attack) which makes it more costly than guessing only the PIN or text password without real-time interaction with the server.

### **6.6.3.2 Shoulder-Surfing**

Shoulder-surfing is considered as the HPA is recognition based, and an attacker can record or observe the images selected by users during login and also the PIN and the text password. Shoulder surfing by using a video camera is a realistic threat for ceremonies in some environments. It would be very easy to do if, for example, user interface implementation highlights an image border upon user selection of image. Fortunately, the problem of shoulder-surfing is now a well publicised and understood threat in the context of ATM machines, and chip and PIN card use, that users are getting better in protecting themselves. Randomised position of distractor images would better protect it against casual shoulder-surfing attack. To improve resistance against camera based attack, MSMA can be implemented to use gaze-based [139] selection of HPA.

### **6.6.3.3 Phishing Attacks**

#### **Classic phishing attack**

In a classic phishing attack a spoofed email containing a link to a spoofed login page of a legitimate website is sent to the user. If a user clicks on the link he/she will be asked to enter credentials into this fraudulent login prompt. With MSMA, a legitimate password login prompt has access to a secret set of images that enables it to create a password prompt. Phishers can not gain access in an easy way to the secret images and hence must present potential victims with a fundamentally

different and more difficult login interface. Users cannot ignore the differences, especially being required to enter a part of text password after recognising the image. This should eliminate user conditioning or click-whirr responses [42, 135, 101], where users automatically enter their credentials or perform a required security step without enough consideration.

The limitation of the MSMA is that there is no mechanism to protect username and PIN and they can still be stolen by phishing. However, obtaining the HPA parts, i.e. images, is more difficult: without knowledge of users' image profiles, the phisher does not know what images to present in order to extract a graphical password.

As we described earlier on, MSMA can be adapted to use a different protocol between client and a server. Depending on the context in which MSMA will be deployed, if an additional level of security is required, PIN password can be protected by choosing a verifier-based client/server protocol such as SRP in Step 1. The verifier can be derived from a pseudo-random function established during the setup phase.

### **HPA missing**

In the case that the HPA (i.e. images) are not being presented at all during the login, the whole password will not be revealed as the images will not be there to form the password. Hence, the phisher will not be able to gain access to the service offered by the website. In this case, the phisher will be able to capture the PIN and the username, but the rest of the login tasks will be so profoundly different that the user should notice the difference.

### **Real-time MITM attack**

We do not consider the much more adversarial model in which a phisher is able to mount real-time (i.e. an active) man-in-the-middle (MITM) attack. This type of phisher has the additional power to establish one connection to the user's prover and simultaneously another connection to the user's verifier and impersonate each one

at the level that cryptographers are concerned with. It is difficult to prevent this active MITM attack and using SSL cannot mitigate this attack [74]. To make things worse, many websites home and login pages are not even protected by SSL/TLS and can be spoofed by a MITM attack that targets the site’s home page.

## 6.6.4 Experimental Evaluation

We collected empirical data by performing a user study in order to evaluate the ceremony against a phishing attack. We implemented an MSMA prototype for the study. The study measured the success rate of a phishing attack against the MSMA ceremony in comparison to the security image and password, and the multiple images and password ceremonies. We did not attempt to measure the usability of the MSMA or the memorability of graphical passwords – those topics have been explored elsewhere [205, 32, 233, 112, 53]. The user study is described in Chapters 7 and 8.

### 6.6.4.1 Prototype

For our proof-of-concept MSMA realisation we divided the text password into three segments: each segment consisting of one character and corresponding to one image from a graphical feedback password. The prototype is used in the user study described in Chapters 7 and 8. A  $3 \times 3$  display layout was used for presenting the HPA image set containing the corresponding image and the distractor images. The PIN, text password and images were randomly pre-assigned.

The MSMA login process from the user’s point of view is as follows:

- *Step 1*: The user enters username and PIN.
- *Step 2*: The first set of images is presented to the user.

The user clicks on the recognised image and then enters the 1st part of the text password.

- *Step 3*: The second set of images is presented to the user.

The user clicks on the recognised image and then enters the 2nd part of the text password.

- *Step 4*: The third set of images is presented to the user.

The user clicks on the recognised image and then enters the 3rd part of the text password.

- *Step 5*: The user submits the text password, that is concatenated from the three parts.

The policy applied gives the following password strength for MSMA, measured by entropy in bits. The entropy for PIN part is 13 bits; for the HPA part is 9.3 and for the text part is  $3 \times \log_2 52 = 17.7$ , which brings the overall MSMA password entropy to 40. That is well above the suggested strength of 20 bits [81] for everyday computing.

The prototype of the login page with the MSMA is shown in Figures 6.4, 6.5 and 6.6.

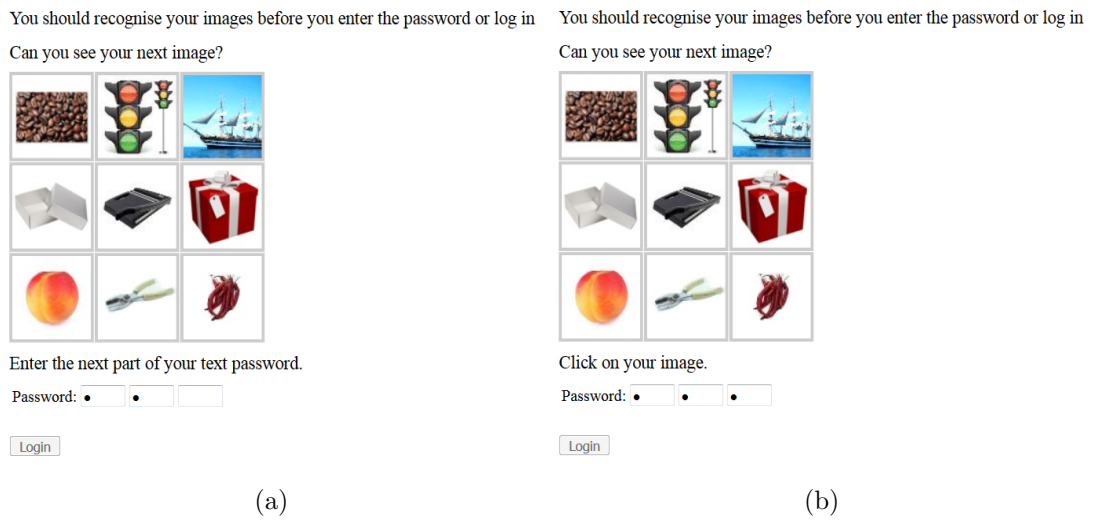
**Enter 4 digit PIN:**

PIN:

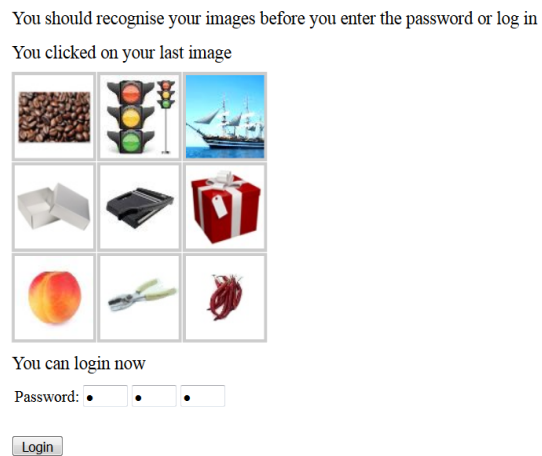
1	2	3
4	5	6
7	8	9
	0	

**Figure 6.4:** Login with MSMA: Step 1





**Figure 6.5:** Login with MSMA: subsequent Steps



**Figure 6.6:** Login with MSMA: the last Step

## 6.7 Conclusion

The MSMA ceremony is a mutual authentication ceremony that combines PIN, text password and recognition-based graphical passwords in multiple steps. The graphical part of MSMA ceremony is a Human Perceptible Authenticator (HPA) and enables the user to verify that the website, he/she is accessing, is legitimate, helping to mitigate phishing attacks. The HPA can be anything, but we have chosen a visual HPA, to be provided in the form of images, rather than a piece of music or excerpt from a book.

MSMA design applies some of the human communication processing assumptions proposed by the Model for Analysing HF-APAC (presented in Section 5.4) and demonstrates the new ceremony design and analysis process using the HF-APAC Framework (presented in Section 4.4). The specific assumption applied was that increasing the number of recall and recognise communication factors will result in higher phishing detection rates.

Experimental evaluation of the MSMA is described in Chapter 7 and data analysis and the results are presented in Chapter 8.

# Chapter 7

## User Study for Evaluation of MSMA and the Model

### 7.1 Introduction

In this chapter we present the design of a user study we conducted to evaluate the Model for Analysing HF-APAC and the MultiStep Mutual Authentication (MSMA) ceremony.

The user study is a part of the Model evaluation methodology, shown in Figure 5.1 and a part of demonstration of the usage of the HF-APAC Framework during the design and analysis process of a new authentication ceremony, shown in Figure 4.4.

Our study compares three authentication ceremonies with regard to their impact on the user's ability to distinguish between legitimate and spoofed website login prompts. The study simulates a phishing attack at the user interface level against users of each of the ceremonies. The study design was published in [107].

Data analysis and the results of the study are presented in Chapter 8.

## 7.2 Design Considerations

An ongoing concern in any user study, and especially phishing studies, is *ecological validity*. Ecological validity of phishing studies concerns how to realistically simulate experiences users have in the real world, conduct it in an ethical manner and yet to employ an element of deception [80, 125, 66]. This was one of the main design considerations we needed to take into account.

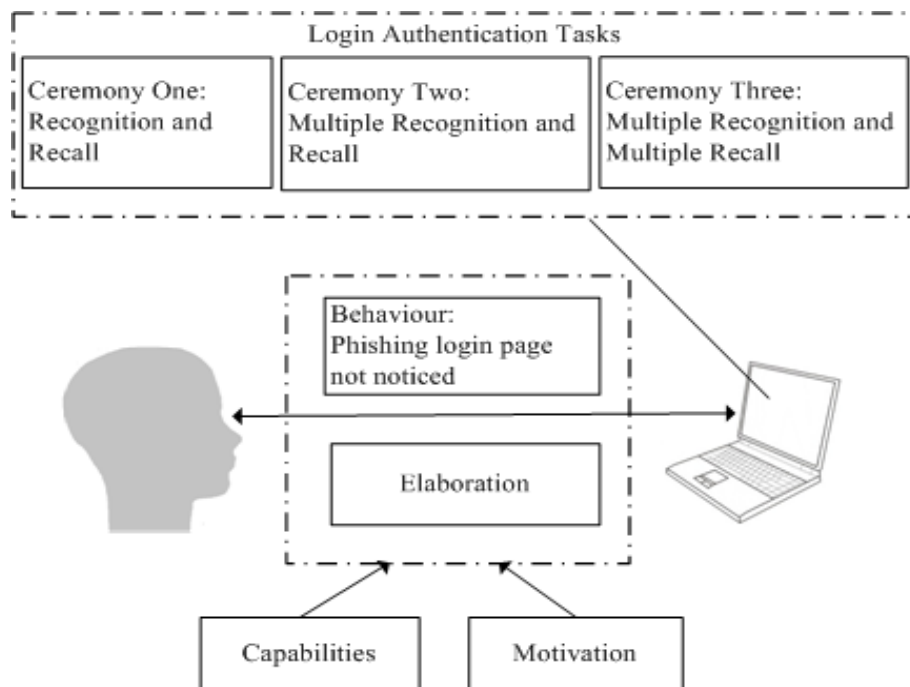
Other mechanisms were put in place in an effort to elicit realistic behaviour and achieve external validity to allow us to draw conclusions that extend beyond the laboratory environment. Even without having phishing considerations it can be very difficult to run studies that are both controlled (i.e. performed in laboratory settings) and ecologically valid [30, 116]. We considered the profile of the participants and their recruitment, scenario and procedure, tasks (described in Sections 7.3.2, 7.3.2.1, 7.3.2.3, 7.3.2.4). As participants were recruited from an education institution, we could anticipate a high percent of students in the study. We did not limit their numbers, as previous research shows that students are users who are very vulnerable to phishing attacks as they tend to engage in more online behaviours [141, 198, 217, 4]. This was aimed at ensuring that an experiment closely represents a real world scenario and that obtained results are valid in the real world as much as they are in the laboratory.

Another challenge we needed to consider was how to directly compare the ceremonies, as the spoofing techniques are different for each ceremony. Even without the spoofing problem, any security comparison of authentication schemes needs to be carefully considered and is not easy to achieve [52, 21, 39, 83, 204].

### 7.3 User Study Design

We designed the study to compare the effect of the communication presented to the user in the login prompt on the user’s behaviour - likelihood of being phished. We selected three authentication ceremonies covering the two main communication types and their combination from our Model for Analysing HF-APAC: *recall* and *recognise* (Figure 5.2). All three ceremonies in the study used images as a type of a HPA. The HPA allowed a user to visually authenticate a server.

The study overview is shown in Figure 7.1. The materials used in this study can be found in Appendix A.



**Figure 7.1:** User study overview

The study was approved and received ethical clearance by the Dublin Institute of Technology (DIT) Research Ethics Committee (*Ethical Clearance Ref:15-02*). The study was conducted in DIT Kevin Street laboratories. There was no risk to user’s personal data during the duration of the study as users were assigned new, temporary credentials. To address the issue of risk to participants, participants’ usernames were

pre-assigned. Since these usernames have no value outside the scope of the study, this limits the potential risk to users. There was no risk to any other of the user's data being compromised.

In order to simulate experiences users have in the real world, i.e. ecological validity, participants were asked to perform a task in a context. This raised a number of challenges. It is difficult to simulate the experience of risk for users without crossing ethical boundaries. Also, the users evaluate risk differently during the lab studies than they would otherwise [80].

In order to motivate the user to make an effort to safeguard their login credentials and introduce a level of risk in case the credentials are stolen, we tried to increase the importance of the account for the website, i.e. the value of the username/password used during the study. To achieve this, a number of *prizes* were awarded to randomly selected participants providing they accomplish *all* required tasks in the study. Part of each website task was to post at least one comment on the website page. In the first line of each comment they needed to enter the Anonymous Identification Number (AIN) corresponding to the participant's username, that was given to each participant at the beginning of the study (see Section 7.3.2.3). The AIN number was then put into the raffle for the prizes. The prize was a random draw to win one of five €10 gift cards.

The main reason that most studies in phishing, authentication and usability area offer incentives to participants, is to ensure that users sufficiently care about the task to be performed and protect their password as they would if it were their real banking or email account password. Some examples are [135, 101, 197, 133, 61]. Other reasons for the incentive are to encourage participation and avoid a high dropout rate, as is often the case in user studies, especially where students are involved. Because of high demands on students' time, non-participation and study dropout remain big challenges for researchers [50].

The prize eligibility, that could be lost if the account was compromised, was put in place to increase the value of their account used during the study, and introduce a level of risk. The awarding of the prizes also served as an incentive to participants to complete all study tasks (described in Section 7.3.2.4).

To introduce an element of deception and avoid priming, we did not inform participants about the study true purpose, i.e. that we were researching phishing. Participants were told that the main focus of the study was security usability of graphical authentication methods, i.e. using images for authentication; and how easy and secure it is to use them. The information sheet they were given to read before signing the consent form also mentioned that the purpose of the study was to compare the schemes regarding their help in distinguishing between legitimate and altered login pages. The information sheets were taken away together with the consent forms before the participants started the study tasks. The study website only referred to 'Usability Study'; there was never any mention of security during the experiment. We never mentioned word phishing or web spoofing.

The study scenario and procedure is described Section 7.3.2.3.

### **7.3.1 Conditions**

The study design was between-subjects, where participants were randomly assigned to one of three conditions, the three different authentication ceremonies, as shown in Figure 7.1. We chose the between-subject design for several reasons. First, we needed to preserve a level of deception. Experiments employing any form of deception cannot be done within subjects, as participants should not become aware of the purpose of the experiment. Users could have learned to notice the spoofed login prompt easier when using a subsequent authentication ceremony. Also, as we sought to determine the effect of the login tasks in ceremonies, a between-subject study design was the most appropriate choice. To adequately compare authentica-

Condition	Login communication	Number of communication tasks
One	Recognition and Recall	2
Two	Multiple Recognition and One Recall	4
Three	Multiple Recognition and Multiple Recall	7

**Table 7.1:** Study conditions

tion ceremonies, the tasks that the users needed to perform needed to be exactly the same apart from the login task. Another reason was that it was simpler for the user. It would have taken extra effort for our participants to learn three different password schemes that they do not normally use.

In order to compare the communication presented to the user in login pages and its effect on his/her behaviour we selected authentication ceremonies that utilised the two main communication message types and their combinations, *recall* and *recognise*, as referred to in Figure 5.2. The combination of recognition and recall in the ceremonies is defined as follows, and shown in Table 7.1:

1. *Recognition and Recall.* The user needs to recognise an image and then recall a text password. In some figures, we refer to this condition as *Single image + text*.
2. *Multiple Recognition and One Recall.* The user needs to recognise multiple images and recall a text password. In some figures, we refer to this condition as *Multiple images + text*.
3. *Multiple Recognition and Multiple Recall.* The user needs to recognise multiple images and recall a PIN and multiple segments of a text password. In some figures, we refer to this condition as *Multiple images + multiple text*.

For our study, all three ceremonies were using images as a type of a HPA. The



HPA allowed a user to authenticate a server. For ceremonies One and Two we implemented the user interaction for password registration and login broadly matching the original BBMA [86] and TwoStep [216] ceremony specifications. For MSMA, the Ceremony Three, we implemented it as specified in Chapter 6. We omitted the exact protocol implementation for the client/server interaction as that is not the main focus of our research. For our study it was sufficient to only exactly implement parts of ceremonies that the user interacts with, i.e. images and text passwords.

A standard text-based password mechanism was used, in which users can enter alphanumeric and special characters. Text passwords were hidden when typed by the users. For graphical password parts all three ceremonies were implemented using images of everyday objects.

#### **7.3.1.1 Password Parameters Settings**

Each user created an account and setup the password for the ceremony they were assigned to. As we were not comparing memorability or usability of ceremonies, having equal theoretical password security for each condition was not crucially important. Nevertheless, we set the parameters of the ceremonies passwords so that they were as close as possible. As a guideline for the security setting in the study, we used Florêncio and Herley [81] suggestion that 20 bits of security is sufficient for everyday computing. All ceremonies had more than 20 bits. The number of items users needed to remember, was between 8 and 10, consisting of characters, digits and images.

Table 7.2 shows the password configuration for the ceremonies used in the studies.

Ceremony	Password configuration
One	62 characters, length 7 1 × 1 grid, 1 image
Two	62 characters, length 7 3 × 3 grid, 1 image, 3 rounds
Three	10 digits, length 4 52 characters, length 3 3 × 3 grid, 1 image, 3 rounds

**Table 7.2:** Password configurations of the ceremonies used in the study

### 7.3.1.2 Condition One - Ceremony One: Recognition and Recall

As a representative of 'Recognition and Recall' ceremony, Ceremony One, we implemented an adaptation of BBMA [86]. The high level description of BBMA was presented in Section 2.3.3. Ceremony One login consisted of a single image (i.e. the HPA) and a text based password. The user had to recognise the image and then authenticate herself to the server, using a username and a text password. The text passwords needed to be exactly *seven* characters long including digits, a mixture of lower and upper-case letters and special characters.

Hence, the communication types, as described in Chapters 4 and 5, utilised in Ceremony One were:

- Recognition: Single image.
- Recall: One text password.

The login prompt with the Ceremony One is shown in Figure 7.2

You should recognise your image before you log in



Username: user001  
Password:

Login

**Figure 7.2:** Login prompt for Ceremony One

### 7.3.1.3 Condition Two - Ceremony Two: Multiple Recognition and One Recall

As a representative of the 'Multiple Recognition and One Recall' ceremony, Ceremony Two, we implemented an adaptation of *TwoStep* authentication scheme [216]. *TwoStep* high level description was described in Section 2.3.3. Ceremony Two uses text passwords and multiple images in a two-step process. In *step one*, a user is asked to supply her user name and text password. After this, even if the user-name/password combination is not correct, in *step two*, the user is presented with an image set in multiple rounds. In each round, the user must correctly select the images previously selected at the time of registration. Both the text password and the graphical password must be correct for a successful login.

*TwoStep* [216] authentication can be implemented in different ways according to a specific security policy with regard to the number of rounds of image verification; display layout or number of images to be selected in each round. We implemented it with a policy to represent the second condition for our study, i.e. multiple recognition and one recall: 3 rounds of verification; a  $3 \times 3$  display layout. In each round, one image to be selected from an image set of 9 distractor images containing the correct

## Step 2: Image Selection

You should recognise your images before you log in

### Step 1: Enter Password

Username: user002

Password:

Next

(a) Step 1



Click on your 1st image

Login

(b) Step 2

**Figure 7.3:** Login prompt for Ceremony Two

image.

Therefore, the communication types, as described in Chapters 4 and 5, utilised in Ceremony Two were:

- Recognition: Multiple images.
- Recall: One text password.

The login prompt with the Ceremony Two is shown in Figure 7.3.

### 7.3.1.4 Condition Three - Ceremony Three: Multiple Recognition and Multiple Recall

The third, 'Multiple Recognition and Multiple Recall' ceremony, is our newly proposed ceremony MSMA ceremony, described in detail in Chapter 6.

MSMA can be adapted to have fewer or more steps, depending on how many segments are in the text password. The size of the segments that the text password is divided into can vary, or it can be just one character. The length of the PIN can also vary. In order to enable comparison with the other two ceremonies, MSMA was implemented as follows. We divided a text password into three segments: each segment consisting of one character and corresponding to *one image* from a graphical feedback password, which is in fact a HPA. An image set of 9 distractor images containing the correct one (as described in Chapter 6), were used for visual feedback. We chose to use  $3 \times 3$  display with 9 images for immediate memory limits, as HCI research shows that an average human can handle maximum 'seven plus or minus two' items at once [157]. We used 4 digit randomly assigned PINs.

Therefore, the summary of the MSMA policy applied is as follows: 3 rounds of verification; text password divided into 3 segments - each 1 character;  $3 \times 3$  display layout; 1 image to be to be recognised and selected in each round; 4-digit PIN.

The communication types, as described in Chapters 4 and 5, utilised in Ceremony Three were:

- Recognition: Multiple images.
- Recall: Multiple text and a PIN.

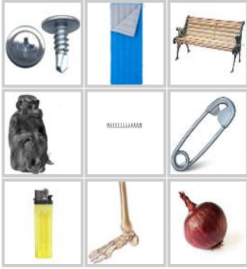

The login prompt for Ceremony Three is shown in Figures 7.4 and 7.5.

**Enter 4 digit PIN:**

PIN:

1	2	3
4	5	6
7	8	9
	0	

**Figure 7.4:** Login prompt for Ceremony Three: Step 1.

<p>You should recognise your images before you enter the password or log in</p> <p>Can you see your 1st image?</p>  <p>Enter the 1st part of your text password.</p> <p>Password: <input type="text"/> <input type="text"/> <input type="text"/></p> <p><input type="button" value="Login"/></p>	<p>You should recognise your images before you enter the password or log in</p> <p>Can you see your 1st image?</p>  <p>Click on your image.</p> <p>Password: <input type="text" value="•"/> <input type="text"/> <input type="text"/></p> <p><input type="button" value="Login"/></p>
--	--

(a) (b)

**Figure 7.5:** Login prompt for Ceremony Three: the first of subsequent Steps.

### 7.3.2 Methodology

This section describes our study methodology, starting with recruitment process, experiment implementation, scenario, finishing with the description of the study tasks.

#### 7.3.2.1 Recruitment

Participants were recruited from the Dublin Institute of Technology (DIT), Kevin Street Campus, and included students, academic, technical and administrative staff.

Teddlie and Yu [211] describe convenience sampling as sampling that involves drawing samples that are both easily accessible and willing to participate in a study. Our participants only needed to be able to browse the web and use websites that require a username and password to gain access. The majority of the general population uses various websites where they need to login providing credentials. DIT students and staff met these criteria.

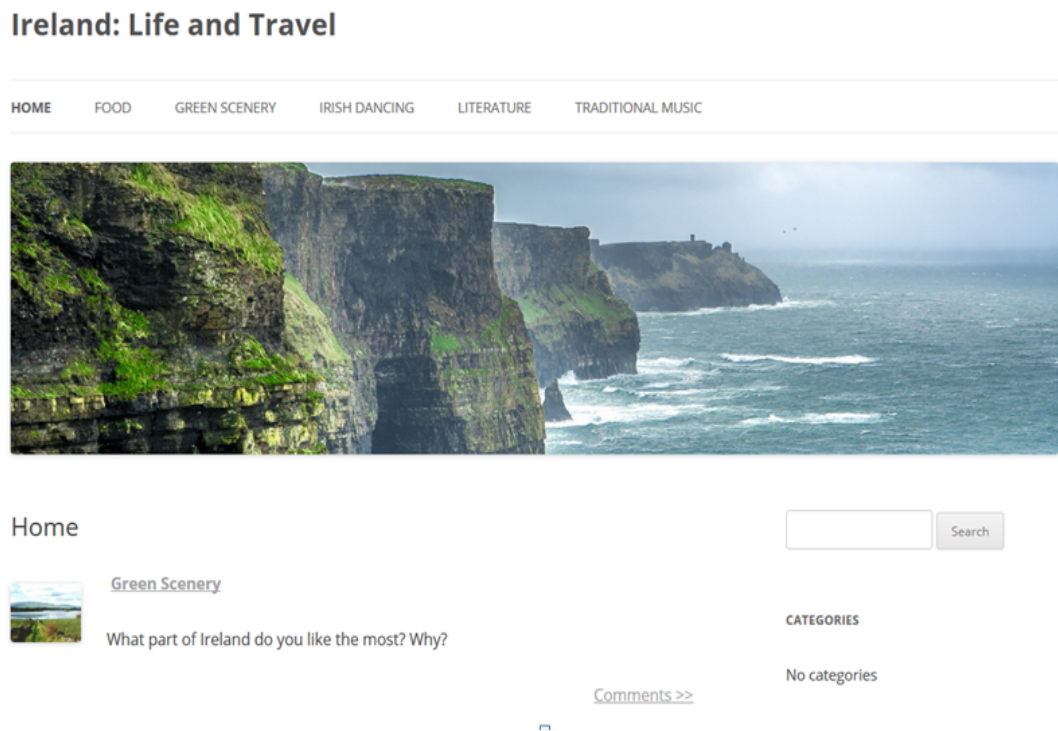
Participants for the study were recruited in three ways: (1) invitation to staff and students through e-mail; (2) interaction by phone and in person and by (3) posting a notice on DIT bulletin boards. Selection of participants was based on those *students* and *staff* who identified themselves as willing to participate in the study. They needed to be at least 18 years old. The information given during the recruiting process was that we are conducting a user study on security usability of web authentication schemes that use images as part of the login process (presented in Appendix A, Figures A.1 and A.2). Our target population was primarily composed of university students and staff. We recognise that the general population is much more diverse, but it is adequate for a comparative study like this [116, 112, 141, 136, 204].

We aimed to recruit about 140 participants, taking into account the recognised study dropout problem [50]. As we planned to analyse the data using non-parametric tests, this sample size would have exceeded the recommended sample size of at least 30 for an analysis using non-parametric statistics [58].

Participants were *excluded* from the data analysis if they failed to complete the tasks required by the user study. Participants that refused to sign the consent form were also excluded.

### 7.3.2.2 Implementation

A fully functioning website called 'Ireland: Life and Travel' was created, hosted, and maintained for the study, hereafter referred as *User Study website*. Figure 7.6 shows the home page of the website.



**Figure 7.6:** User Study website

The 'Ireland: Life and Travel' website was implemented in such a way to allow participants to authenticate with one of the three authentication ceremonies, i.e. conditions (Section 7.3.1). Thus, participants were tested under identical conditions, only differing in the type of authentication being used.

Surveys were designed and implemented and data was collected using a DIT created account at an online survey tool.

We created an online study page and all the tasks including surveys were accessed from the links from that page (Appendix A).



### 7.3.2.3 Scenario and Procedure

At the beginning of the study participants were given a consent form and the study information sheets to read. The materials used can be found in Appendix A. The consent form was a generic DIT research form that pointed out to participants that they were free to withdraw from the study at any time, without giving a reason for withdrawing and without affecting their future relationship with DIT. The first information sheet had a brief overview of the study, task, duration and anonymity. It also mentioned that the purpose of the study was to evaluate the security usability of three web login schemes; that we were trying to determine how easy and secure it is for people to use these schemes; and that we were comparing login schemes regarding their impact on the user's ability to distinguish between legitimate and altered website login pages. The second information sheet outlined the website and survey tasks to be performed as part of the study; and explained that they need to sign the consent form if they are willing to proceed with the study. It also had the URL of the study website from which to perform the study (Appendix A, Figure A.6). If participants had any questions, the researcher reviewed the consent form and information sheets with them.

Neither the consent form nor information sheets mentioned the word *phishing* or *spoofing*.

Participants that signed the consent form were given an envelope containing their predefined account details: username, email address, AIN, username and password for accessing the study website and surveys. The consent form and the information sheets were then taken away from the participants.

Upon receiving the account details participants were given the opportunity to ask questions. However, after this step, the participants were asked to continue with the tasks without asking questions, as if they were accessing the website from home. and the session could begin.

Users performed all tasks by clicking on the links from the web page, hereafter referred to as the *Study page*, as shown in Appendix A, Figure A.7. Each session lasted between 30-40 minutes. Participants were offered chocolate at the end of the session, as they were leaving the laboratory, and also they were then debriefed about the true nature of the study. We followed Jakobsson's [80] guidelines suggesting that debriefing in a laboratory phishing study is appropriate. The aim of debriefing is to heal any negative feedback and the breach of trust and the face-to-face conversation between the participant and the researcher is proper in the circumstances.

#### **7.3.2.4 Study Tasks**

The study tasks were accessed from the links on the Study page (Appendix A) and grouped as follows:

1. Registering
2. Website tasks
3. Post Study survey
4. Demographics survey

Participants were asked to first register for the User Study website and then perform the tasks in order.

#### **Registration procedures**

After signing the consent form, each participant was given an envelope containing a paper strip with the following predefined details: username, email address, AIN, username and password for accessing the study surveys. The username details determined which condition of the user study will the user be in. Before registering, participants were directed to familiarise themselves with the assigned authentication ceremony.

*Tutorials.* Short tutorials for using each ceremony were developed and links to them were provided. Participants were also provided a link to their assigned ceremony registration screen from the study page. Each user then created an account on the User Study website, with the given username. The participants were advised that they could use their AIN or the survey password as a text password. Both were 7 digits/characters long.

### **Website tasks**

The website tasks consisted of logging in to the 'Ireland: Life and Travel' website at least 5 times, using a newly created password. During each login, they needed to post a short comment on the topic of the specific website page and then log out. Topics of the pages were: Food, Green Scenery, Irish Dancing, Literature and Traditional music. Participants needed to add their AIN to comments in order to be eligible for the raffle.

The adding comments task served multiple purposes. First, it ensured that the users login to the pages. Second, it was added to increase the experience of risk by giving users password-protected accounts where participants needed to add their AIN to comments in order to enter the raffle for the prizes. The third aim was to distract the users between login attempts to clear their working memory. It was used instead of using a specific mental rotation tasks (MRT), often used in laboratory studies [197, 41].

### **Survey tasks**

After completing the website tasks participants were instructed to complete two surveys, a Post Study and a brief Demographics survey.

The Post Study survey contained questions used to measure Elaboration, Motivation and Capabilities components of our Model. Their measurement is described in Section 7.3.4.

The Demographics survey collected basic information about participants including age, gender and occupation. It was intended to give a better understanding of the user study sample.

The questionnaires, as administered to participants, can be found in Appendix A with the other user study materials.

### **7.3.3 Simulated Attack**

The choice of attacks to perform was determined by a couple of factors. First, it is a recognised difficulty in comparing authentication schemes that the spoofing techniques are very different for each scheme [52]. To adequately compare the effect of a phishing attack, it needs to be possible to perform it for each ceremony in a very similar way and also make the attack plausible. Another consideration we needed to keep in mind was that if an attack was fundamentally changing the login prompt, we could assume that the user would refuse to interact with it. That narrowed a choice of phishing attacks. As we intended to evaluate the impact of differences in the number of communication tasks in ceremonies, launching, for example, a missing security images attack, was not plausible for all ceremonies. We also would not have a difference in the number of communication tasks in ceremonies which we needed to assess.

The attack we launched was applicable for all three ceremonies and is a recognised type of phishing attack [144]. During this attack a secure login page was spoofed, with the user interface providing all the interaction and functionalities with the user in the same way as a legitimate login page would, but without the interaction with the real server provider, making the user believe that he/she is interacting with the intended target website. This is a type of a man-in-the-middle (MITM) attack, the attacker is only interacting with the victim at the interface level, and not at the network level, as in real-time man-in-the-middle attack. We did not consider

real-time man-in-the-middle attack, which is more difficult to launch for attackers as well. In a real MITM attack, the phisher poses both as a service provider and as a user and can obtain access to any transmitted information in the process, and can control all network traffic.

Based on the above consideration we decided to simulate a phishing attack where we prompt the user with an invalid HPA - graphical part of the login prompt; i.e. image(s) that are not part of the user's password. In a real phishing attack the user would have been redirected to the spoofed site and the phisher would then try to present with a login prompt in order to get the user to enter the password into it. We assumed that the user does not notice a slight difference in the URL, or lack of other security indicators. These issues have been explored elsewhere and it has been shown that security indicators do not adequately protect against phishing attacks [57, 65, 194]. Many real world phishing attacks do not even attempt to alter the destination site, as they rely on peoples lack of understanding of URLs [115].

The main website tasks of the study involved logging in five times to the user study website and post a short comment each time. After the user logged in *three* times, we simulated an attack on the *fourth* login attempt.

As part of the attack, we prompted the user with an invalid graphical part of the password prompt. For Ceremony One, a wrong image was displayed; for Ceremonies Two and Three a set of distractor images not containing the right image. We measured if participants noticed that the correct image is not displayed or present in the set, and if they would submit their credentials in spite of that.

The spoofed login prompt would be presented one more time. The subsequent login attempts would have the correct login prompt restored and the users could continue with the rest of the study tasks.

As our primary goal was to evaluate human behaviour, rather than the strength of the security protocol, the user was allowed to enter all segments of the text

You should recognise your image before you log in



Username: user001  
Password:

Login

(a) Login

You should recognise your image before you log in



Username: user001  
Password:

Login

(b) Attack login

**Figure 7.7:** Simulated attack against Ceremony One: a wrong image is displayed in the attack login screen.

**Step 2: Image Selection**

You should recognise your images before you log in



Click on your 1st image

Login

(a) Login

**Step 2: Image Selection**

You should recognise your images before you log in



Click on your 1st image

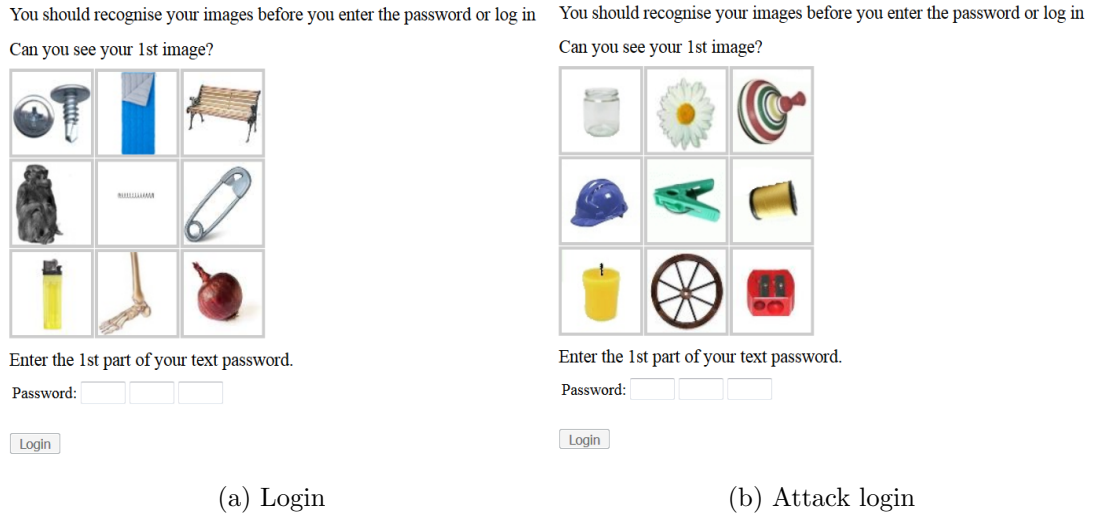
Login

(b) Attack login

**Figure 7.8:** Simulated attack against Ceremony Two: a set of distractor images shown in the attack login screen does not contain the correct image.

password even if they had clicked/chosen the wrong images of the graphical part of the password.

The same attack was employed against users of all *three* ceremonies. We show screenshots of the attack login pages in Figures 7.7, 7.8 and 7.9.



**Figure 7.9:** Simulated attack against Ceremony Three: a set of distractor images shown in the attack login screen does not contain the correct image.

### 7.3.3.1 Attack Success Metrics

The attack was considered to be successful if the user submitted the password in spite of the wrong images presented. The attack was considered to be a failure if the user did not submit the password or abandoned the page. After launching the attack we continued the experiment. We designed the attack in such a way that on the second login attempt after the attack launch, the participants were presented with the correct images and could login to the website again. This is in line with the real life attacks where users do not realise they have been subjected to an attack until they notice the misuse of the stolen credentials. Some participants reported it as: 'I am not sure why my images were different at one stage.'

### 7.3.4 Measures

We conducted two surveys: the first one was the Post Study survey and the second was the Demographic survey. The questionnaires were approved by the DIT Research Ethics Committee, and the full questionnaires can be seen in Appendix A.

Both surveys and data from the experiment were designed to be anonymous.

The Post Study survey consisted of 15 questions divided into three sections, the sections either measuring Elaboration, Motivation or Capabilities constructs. We designed the Post Study survey based on the elements of our Model for Analysing HF-APAC. For the most part, measures used for Elaboration, Motivation and Capabilities were based on prior validated measures developed in communication processing [217, 71, 235] and extended and adapted for our research model.

**Communication Factors.** Recall and recognition communication factors was measured as the total number of recall and recognition tasks in the ceremony. We also referred to it as *Number of Communication factors*.

**Attention to Recall.** Attention to Recall communication was measured as the overall time span between when the text and/or PIN part of the password login part appeared for the first time on a participant's screen and when the participant responded to it. It was measured in *milliseconds*.

**Attention to Recognise.** Attention to Recognise communication was measured as the overall time span between when the image(s) to be recognised or selected appeared for the first time on a participant's screen and when the participant responded to it. It was measured in *milliseconds*.

**Behaviour.** Behaviour measured the attack success, i.e. whether a participant submitted his/her credentials in spite of correct image not being displayed or present in the set.

**Motivation.** Motivation was measured using the values of *seven* items based on prior research in information processing of phishing emails [217] and adapted and extended for our research model. Sample items, 5-point scale, read: 'The informa-



Item	Description
Q1	The information in the User Study Website was essential.
Q2	The information in the User Study Website was trivial.
Q3	The information in the User Study Website was significant.
Q4	The information in the User Study Website was important.
Q5	The information in the User Study Website was relevant to you.
Q6	The information in the User Study Website was of concern to you.
Q7	The information in the User Study Website matters to you.

**Table 7.3:** Motivation items

tion in the User Study Website was essential.’ The items were questions 1 to 7 in the Post Study survey, shown in Table 7.3 and Appendix A.

Each item response was scored as follows: 1 = ‘Strongly Disagree’, 2 = ‘Somewhat disagree’, 3 = ‘Neither agree nor disagree’, 4 = ‘Somewhat agree’, 5 = ‘Strongly Agree’. The items were combined by using the *median* value.

**Capabilities.** Capabilities was measured using the values of *three* items, which were derived from prior research in web security and information processing of phishing emails [136, 217] and adapted and extended for our research model. Sample items, 5-point scales, read: ‘How would you rate your knowledge about Web security in general?’ The items were questions 8 to 10 in the Post Study survey, shown in Table 7.4 and Appendix A.

Each item response was scored as follows: 1 = ‘Not at all Knowledgeable’, 2 = ‘Slightly Knowledgeable’, 3 = ‘Moderately Knowledgeable’, 4 = ‘Very Knowledgeable’, 5 = ‘Extremely Knowledgeable’. The items were combined by using the *median* value.

**Elaboration.** Elaboration was measured using *five* items derived from prior re-

Item	Description
Q8	How would you rate your knowledge about Web security in general?
Q9	How would you rate your knowledge of the authentication scheme used in the User Study Website?
Q10	How would you rate you knowledge about Web based scams?

**Table 7.4:** Capabilities items

search in information processing of phishing emails [217] and adapted and extended for our research model. Sample items, 5-point scale, read: 'After trying to login to the User Study Website you thought about the type of authenticators you previously used for this website.' The items were questions 11 to 15 in the Post Study survey, shown in Table 7.5 and Appendix A.

Each item response was scored as follows: 1 = 'Strongly Disagree', 2 = 'Somewhat disagree', 3 = 'Neither agree nor disagree', 4 = 'Somewhat agree', 5 = 'Strongly Agree'. The items were combined by using the *median* value.

### 7.3.5 Statistical Tests

For our analyses we used a number of different statistical tests as we tested the *seven* Model for Analysing HF-APAC hypotheses, developed in Section 5.3.1. For MSMA evaluation we tested the differences between the three ceremonies regarding the user's likelihood of being phished. The choice of the tests for each of the hypotheses was determined by the nature and number of the independent and dependent variables, the between-subject study design and the particular question to be answered by the hypothesis [142, 2].

Logistic regression was conducted to test the prediction in hypotheses where the dependent variable was a binary categorical variable. To test an association between variables we performed Cochran-Armitage test of trend, Somers' delta and Fisher's

Item	Description
Q11	After trying to login to the User Study Website you thought about the type of authenticators you previously used for this website.
Q12	After trying to login to the User Study Website you thought about the login page and compared it to your previous login experience.
Q13	After trying to login to the User Study Website you thought about the login page look and feel and compared it to your previous login experience.
Q14	After trying to login to the User Study Website you thought about the security of your passwords.
Q15	After trying to login to the User Study Website you thought about whether the website was secure.

**Table 7.5:** Elaboration items

exact test. For differences between three conditions we conducted Chi-square test of homogeneity.

*Logistic regression.* A binomial (or binary) logistic regression is usually referred to as logistic regression. It is a form of regression analysis when the dependent variable is binary (i.e. dichotomous) and the independents can be categorical and/or continuous. It is used when we have a binary outcome (dependent variable) and wish to carry some kind of prediction, make an estimate of the probability of a certain event occurring.

*Cochran-Armitage test of trend.* The Cochran-Armitage test of trend is used in categorical data analysis when the aim is to assess for the presence of an association between an ordinal independent variable (IV) and a dichotomous dependent variable (DV).

*Somers' delta.* Somers' delta (or Somers'  $D$ ) measures associations between independent variables (IVs) and dependent variables (DVs) in terms of differences between

proportions. It is a non-parametric test of the strength and direction of association between an ordinal dependent variable and an ordinal independent variable.

*Fisher's exact test.* Fisher's exact test can be used to determine if there is an association between two dichotomous variables. Fisher's exact test does not make a distinction between an independent variable and a dependent variable.

*Chi-square test of homogeneity.* The chi-square test of homogeneity is used to determine if a difference exists between two or more independent groups on a dichotomous dependent variable. It is used to determine whether the proportions are statistically significantly different in the different groups. If there are statistically significant differences, a post hoc test can be run to determine where the differences between these groups lie.

## 7.4 Conclusion

This chapter presented the design of the user study used to experimentally evaluate the MSMA ceremony and the Model for Analysing HF-APAC. The user study compares three authentication ceremonies with regard to their impact on the user's ability to distinguish between legitimate and spoofed website login prompts.

The goal of the study was to explore the impact of the number and types of login communications (recall and recognition) on the user's likelihood of detecting a spoofed login page; to explore the influence of attention and elaboration on users making an error during the authentication process, i.e. getting phished; and also to explore the influence of users' motivation and capabilities. The second goal of the study was to experimentally evaluate the MSMA ceremony resistance to phishing.

Data analysis and the study results are presented in the next chapter, Chapter 8.

# Chapter 8

## Evaluation Results

### 8.1 Introduction

In this chapter we present the results of the user study we conducted to evaluate the Model for Analysing HF-APAC and the MSMA ceremony. The study design was described in Chapter 7.

The study compared three authentication ceremonies with regard to their impact on the user's ability to distinguish between legitimate and spoofed website login prompts. The study simulated a phishing attack at the user interface level against users of each of the ceremonies. As part of the attack, we prompted the user with an invalid graphical part of the password prompt. For Condition One (Section 7.3.1.2), a wrong image was displayed; for Condition Two (Section 7.3.1.3) and Condition Three (Section 7.3.1.4), a set of distractor images not containing the right image was displayed. We measured if participants noticed that the correct image was not displayed or present in the set, and if the users would submit their credentials in spite of that. The attack is described in detail in Section 7.3.3.

The rest of the chapter proceeds as follows. We first present the data analysis, followed by MSMA evaluation results. Next, we present the results of the Model evaluation. Finally, we discuss the implications of the results.

## 8.2 Study Overview

A total of 135 participants were initially recruited for the study. The study was conducted in April and May 2016 and 113 participants completed all the task of the study.

One participant refused to sign the consent form and that precluded him of continuing with the study. Due to unforeseen WiFi issues, 19 participants did not complete the Website Tasks and dropped out of the study. All participants also needed to complete a Post Study and a Demographics survey. Out of 115 participants that completed the Website Tasks, 1 did not do any of the two surveys and 1 did not complete the Demographic survey. These two sets of data were excluded from the analysis. Therefore, only the results of 113 participants that completed all the tasks were included in the analysis.

The data from the phished and non-phished participants composed one continuous data set. Out of 113 participants that completed all part of the study: 38 were in Condition One, 38 in Condition Two and 37 in Condition Three. Conditions One, Two and Three were described in Sections 7.3.1.2, Section 7.3.1.3 and 7.3.1.4 respectively.

## 8.3 Data Preparation

The data gathered by the study needed to be prepared for analysis. The data comprised of data gathered by the users participating in the website experiment and data gathered via surveys after the users completed the experiment part of the study.

All the experiment and survey data was conducted online, and the data were entered electronically. The data preparation involved retrieving relevant data from the experiment and the survey databases, cleaning unrelated entries such as logs

that were not included in the analysis and finding missing values. The data from participants who did not complete or submit all the required questions in the two surveys were considered incomplete and needed to be removed from the dataset.

Raw data were first exported into comma separated values (CSV) files and then imported to SPSS statistical software [117]. All data analyses and data manipulations were conducted using SPSS versions 23 and 24 [117]. We used a significance level of  $\alpha = 0.05$  for all analyses.

### **Data Coding**

*Communication Factors.* Recall and recognition communication factors, or the Number of Communication factors was coded as: 2, 4 and 7; for Ceremony One, Two and Three respectively.

*Attention to Recall.* Attention to Recall communication was measured in *milliseconds* and coded as a continuous variable.

*Attention to Recognise.* Attention to Recognise communication was measured in *milliseconds* and coded as a continuous variable.

*Behaviour.* Behaviour was coded as a binary categorical variable indicating whether the participants submitted password to the spoofed login page, i.e. was phished. The attack success was coded as 1, and 0 if failed.

*Motivation.* The Motivation was coded as an ordinal variable on the scale 1 to 5.

*Capabilities.* The Capabilities was coded as an ordinal variable on the scale 1 to 5.

*Elaboration.* The Elaboration was coded as an ordinal variable on the scale 1 to 5. We also coded Elaboration as a dichotomous variable. The scores 1-3 as a low Elaboration level, equal to 0; and 4-5 as a high Elaboration level, equal to 1.

## 8.4 Descriptive Outcomes

This section summarises the descriptive data, beginning with the demographics.

### 8.4.1 Demographics

Our participants spanned a range of age groups. 51 (45.1%) participants reported themselves to be in the 18-25 age range, 33 (29.2%) in the 26-35 range, 16 (14.2%) in the 36-45 range, 11 (9.7%) 46-55 and 2 (1.8%) in the 56-65 range. No participant was in the 65 and up range, as depicted in Table 8.1 and Figure 8.1.

27 (23.9%) of participants reported themselves as female, 86 (76.1%) reported themselves as male, as depicted in Table 8.2 and Figure 8.1.

Age	Percent
18-25	45.1%
26-35	29.2%
36-45	14.2%
46-55	9.7%
56-65	1.8%

**Table 8.1:** Age percentages

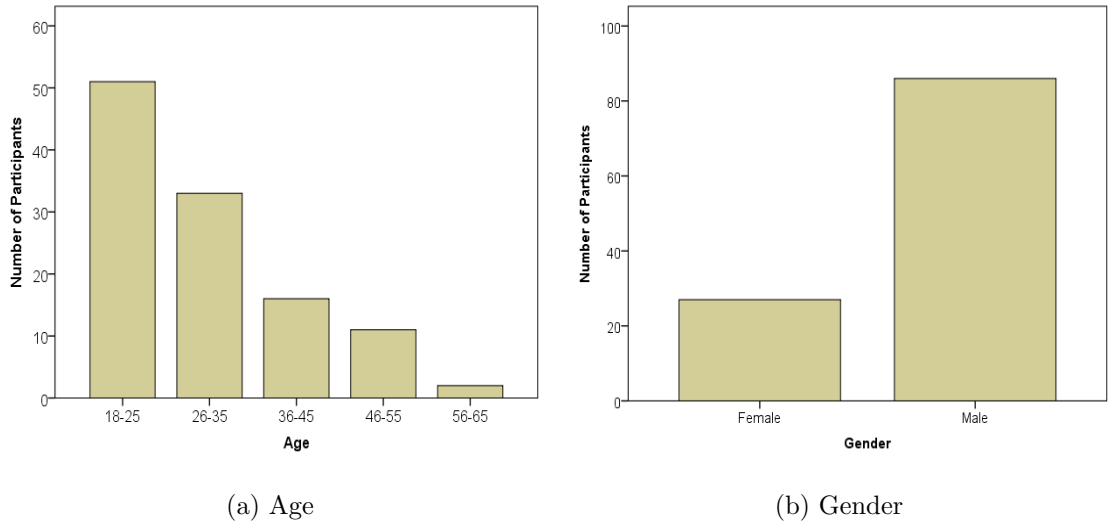
Gender	Percent
Female	23.9%
Male	76.1%

**Table 8.2:** Gender percentages

86 (76.1%) of participants reported that their area is computer science, business and engineering 7 (6.2%) each, 5 (4.4%) science, mathematics and social science 2 (1.8%) each (Table 8.3 and Figure 8.2). The remaining 3.5% reported their area as education, history, law and physical theatre.

53 (46.9) reported themselves as undergraduate students, 15 (13.3%) as PhD students, 11 (9.7%) as masters students and 7 (6.2%) as trade school or apprenticeship students (Table 8.4 and Figure 8.2). 23 (23.9%) were reported as being lab technicians, lecturers, technical officers, apprentices and HDip students.





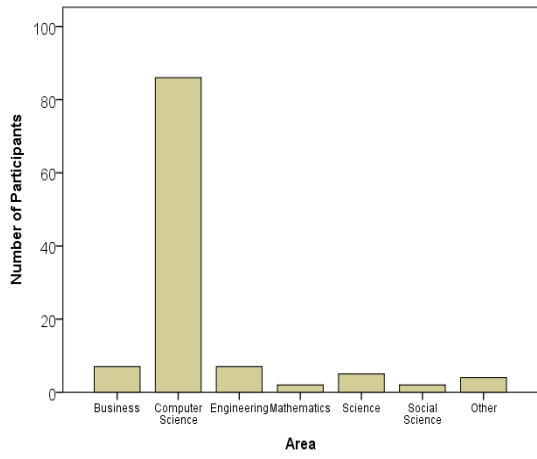
**Figure 8.1:** Age and gender count

Area	Percent
Computer Science	76.1%
Business	6.2%
Engineering	6.2%
Science	4.4%
Mathematics	1.8%
Social Science	1.8%
Other	3.5%

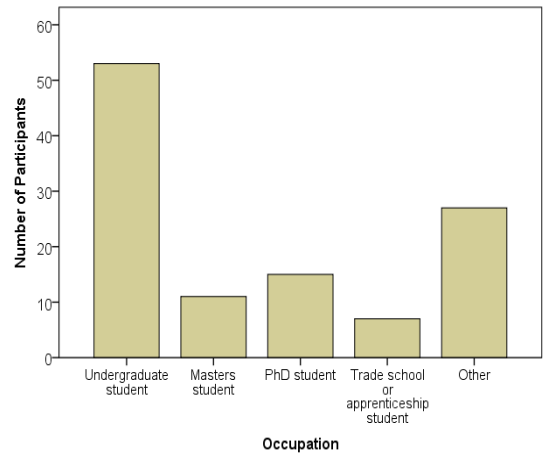
**Table 8.3:** Area percentages

Occupation	Percent
Undergraduate student	46.9%
PhD student	13.3%
Masters student	9.7%
Trade school or apprenticeship student	6.2%
Other	23.9%

**Table 8.4:** Occupation percentages



(a) Area



(b) Occupation

**Figure 8.2:** Area and occupation count

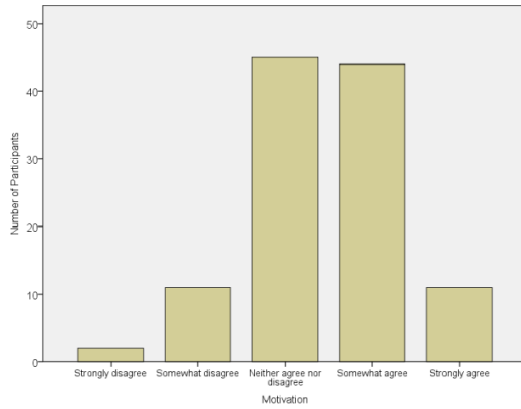
<b>Construct</b>	<b>Median</b>	<b>Mode</b>
Motivation	3.00	3.00
Capabilities	3.00	3.00
Elaboration	4.00	4.00

**Table 8.5:** Survey construct statistics

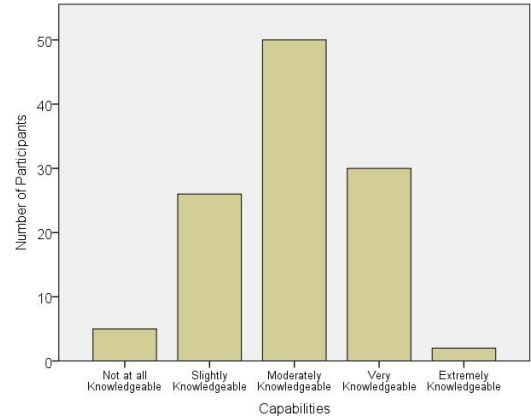
## 8.4.2 Data Overview

Table 8.5 shows median and mode values for survey construct measures. The median value for Motivation and Capabilities was 3, for Elaboration was 4 (Table 8.5). The frequencies for survey constructs are shown in Figure 8.3. For Motivation, 45 (39.8%) of participants were undecided about the importance of the User Study website, closely followed by 44 of those that 'Somewhat agreed' to the importance statements (38.9%). For Capability construct, 26 (23%) participants rated themselves as 'Slightly Knowledgeable', 50 (44.2%) as 'Moderately Knowledgeable'; and 30 (26.5%) as 'Very Knowledgeable', in the area of authentication and web security in general. However, for Elaboration, the majority of participants (69, i.e. 61.1%) 'Somewhat agreed' about thinking and considering User Study website communication.

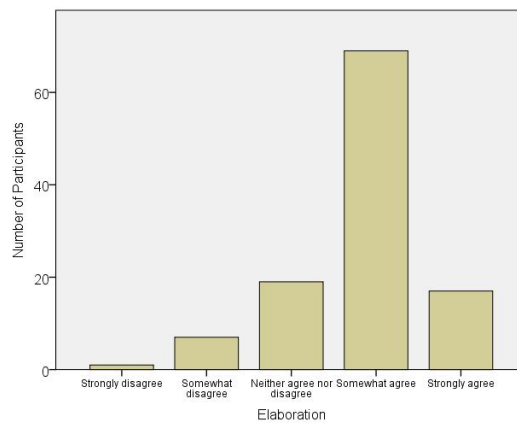
Tables 8.6 and 8.7 show the descriptive statistics of recall and recognise times for each study condition. For Condition One (Section 7.3.1.2) Ceremony One was used; for Condition Two (Section 7.3.1.3) Ceremony Two was used; and for Condition Three (Section 7.3.1.4) Ceremony Three was used. Recall and recognition times in ceremonies was measured in milliseconds. Mean recall time was the lowest for Ceremony Two, which can be attributed to recall task being more distinct from recognition task in Ceremony Two. Mean recognition time was the lowest for Ceremony One and the highest for Ceremony Three. This is due to users having to recognise 3 images in Ceremonies Two and Three, rather than 1 in Ceremony One.



(a) Motivation



(b) Capabilities



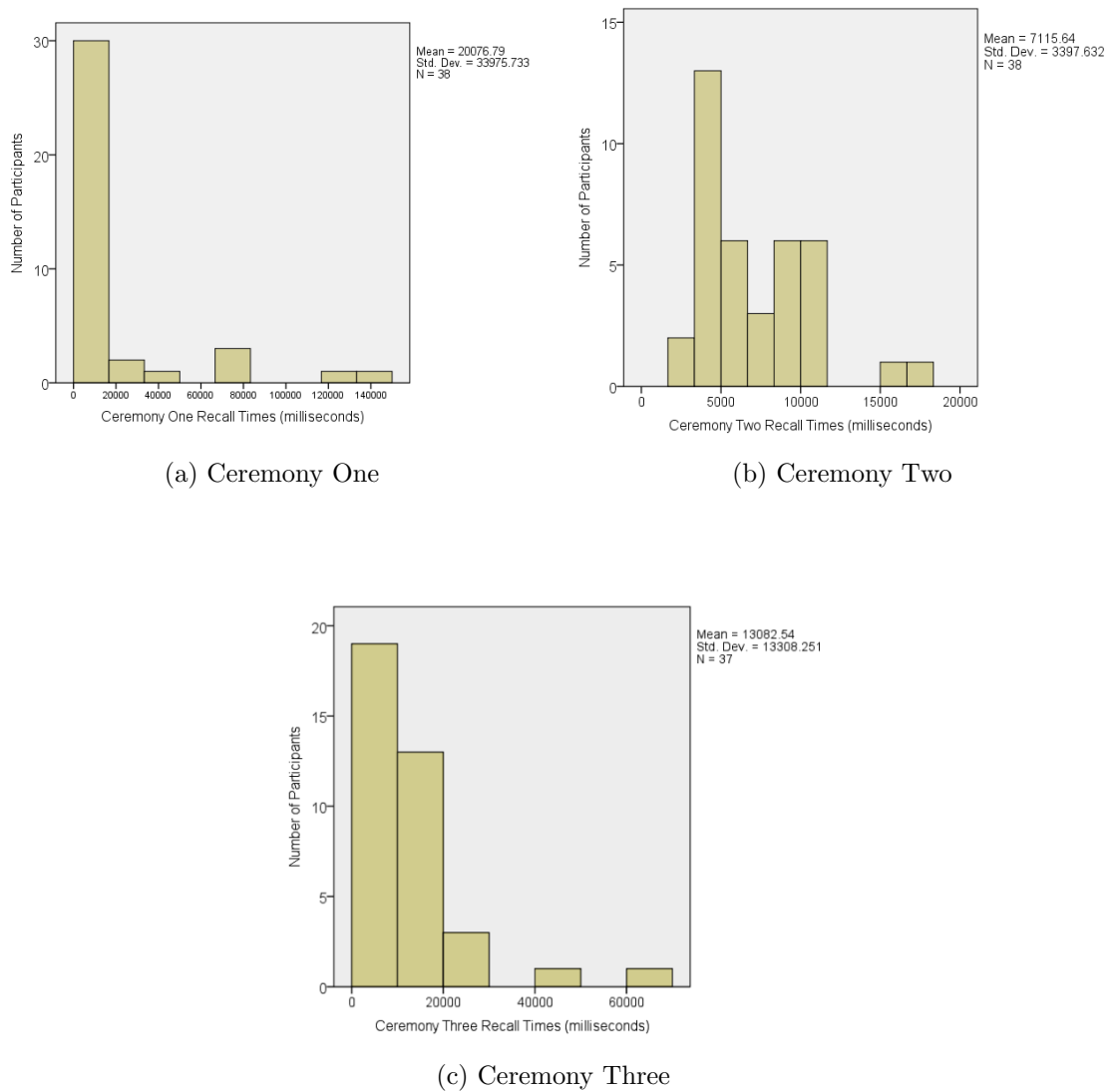
(c) Elaboration

**Figure 8.3:** Frequencies for survey constructs

The difference between Ceremony Three and Ceremony Two recognition time can be attributed to Ceremony Three users being required to switch between recognition and recall tasks, i.e. recognise an image and recall part of text password; while Ceremony Two recognition tasks were performed consecutively. Figures 8.4 and 8.5 show distributions of recall and recognition times by number of participants for each study condition. We used histograms to graphically summarize and display the distribution of recall and recognition times.

Ceremony	Mean	SD	Median	Skewness	Kurtosis
One	20076.79	20076.79	6687.35	2.42	5.29
Two	7115.64	3397.63	5868.50	0.99	0.62
Three	13082.54	13308.25	7753.00	0.38	8.75

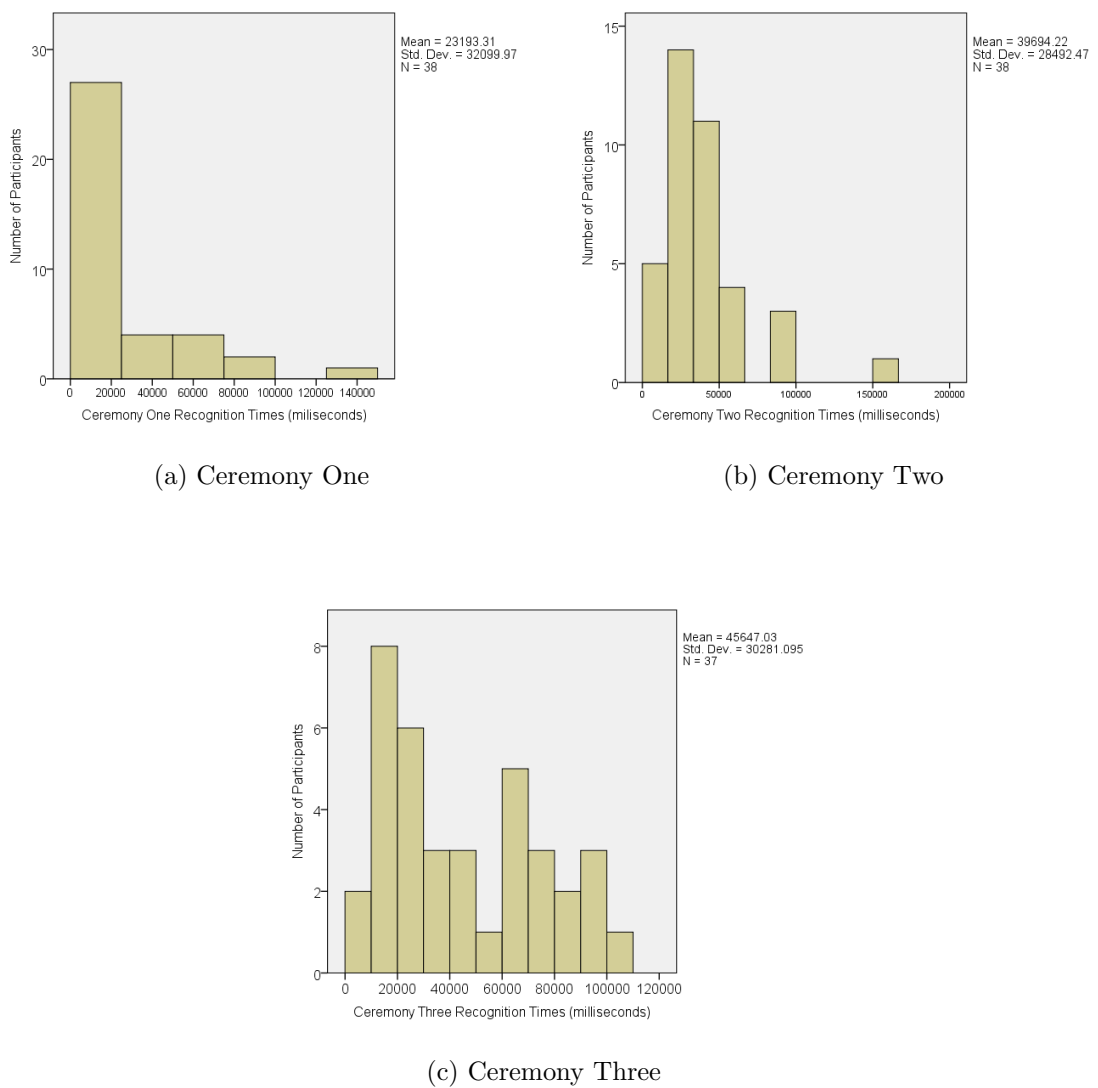
**Table 8.6:** Recall time statistics (milliseconds)



**Figure 8.4:** Recall times for ceremonies

Ceremony	Mean	SD	Median	Skewness	Kurtosis
One	23193.31	32099.97	7289.00	1.93	3.76
Two	39694.22	28492.47	33687.60	2.00	5.53
Three	45647.03	30281.09	35459.00	0.44	-1.19

**Table 8.7:** Recognise time statistics (milliseconds)



**Figure 8.5:** Recognise times for ceremonies

## 8.5 MSMA Evaluation Results

Our study evaluated the MSMA ceremony in comparison to a single security image and password, and multiple images and password authentication ceremonies. We did not attempt to evaluate the usability of the MSMA prompt or the memorability of graphical passwords - those topics have been explored elsewhere [205, 53].

The following hypothesis was formulated for the purpose of the study:

### **Hypothesis: Behaviour Difference**

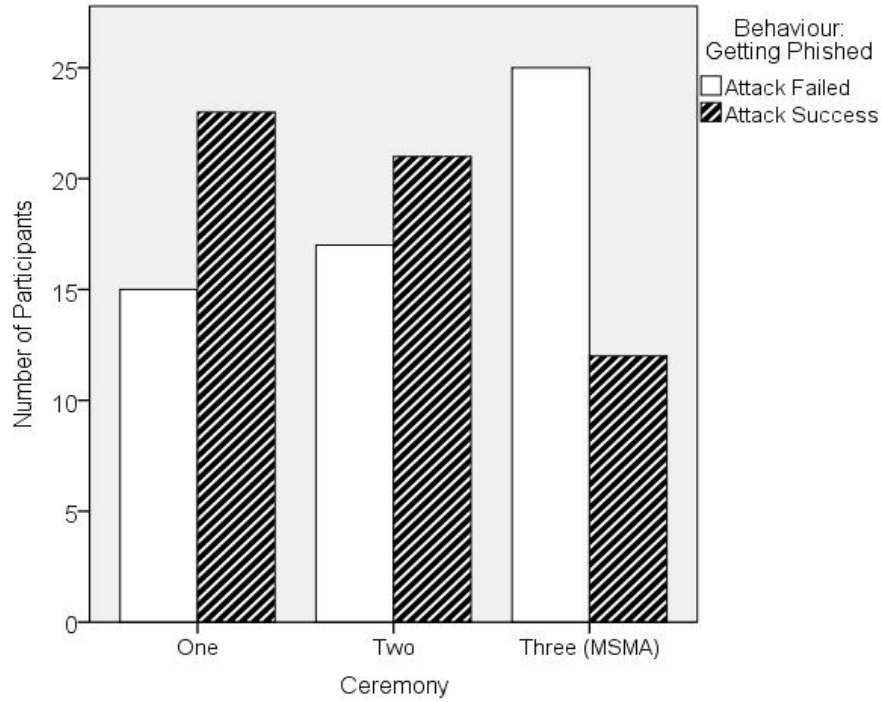
*H* : There would be significant difference among the three ceremonies regarding the user's likelihood of being phished.

We performed chi-square test of homogeneity to look for differences between the three conditions, i.e. ceremonies, on the user's likelihood to fall for the attack. A significant difference ( $\chi^2(2) = 6.665, p = 0.036$ ) between the ceremonies was seen.

Post hoc analysis involved pairwise comparisons using the z-test of two proportions with a Bonferroni correction. It showed that the only significant difference ( $p < 0.05$ ) in falling for the attack was between Condition One and Condition Three (MSMA ceremony). There was no statistically significant difference in proportions, neither between Ceremony One and Ceremony Two conditions, nor Ceremony Two and Ceremony Three (MSMA ceremony) conditions.

In Ceremony One condition, 23 out of 38 participants (60.53%) submitted their passwords in spite of different image being presented at the login; in Ceremony Two condition, 21 out of 38 (55.26%); while in Ceremony Three condition (MSMAC ceremony) 12 out of 37 participants submitted it (32.43%). Results of the attack success by condition are shown in Table 8.8; and Figures 8.7 and 8.6.

Significantly more MSMA users resisted the simulated attack (described in Section 7.3.3) than in the ceremony where only a single image and text password were used,



**Figure 8.6:** Success rates of the attack per ceremony

Ceremony	%Attack successful	%Attack success /%participants	<i>p</i>
One	60.53%	23/38	
Two	55.26%	21/38	
Three (MSMA)	32.43%	12/37	<b>0.036*</b>

**Notes:**

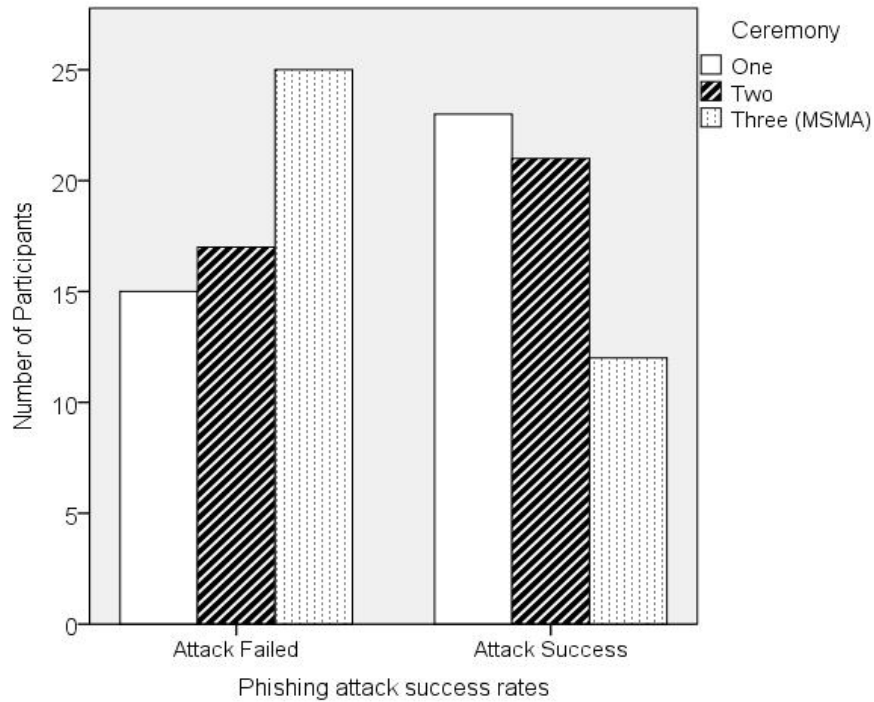
Pearson Chi-Square  $\chi^2 (2) = 6.665$

Significance is indicated by \* $p < 0.05$

**Table 8.8:** Differences between ceremonies in detecting the simulated attack as depicted in Figure 8.7. It gives an indication of increased anti-phishing resistance of our proposed MSMA ceremony.

Of the pool of 113 participants in all conditions of our experiment 56 submitted





**Figure 8.7:** Differences between ceremonies in detecting the simulated attack

passwords into a spoofed login window, i.e. got phished.

The participants using MSMA ceremony were significantly better in resisting the simulated attack than the participants using the Ceremony One, where only a single image and text password was used. The Ceremony One closely mimicked commercial variations of security images authentication often used on internet banking websites [18, 180, 192].

The combination of images and text password as used in MSMA, with multiple image choices combined with text passwords seem to make users significantly less likely to succumb to the simulated phishing attack.

## 8.6 The Model Evaluation Results

We used *the hypothetico-deductive* methodology to evaluate the Model for Analysing HF-APAC, presented in Section 5.3 and Figure 5.1. The hypotheses 1 to 5 were developed as part of that method and were used to test the Model. The testing of the hypotheses, we present in Section 8.6.2, was the evaluation of the Model. The hypotheses development was described in Section 5.3.1, and hypotheses are summarised here for clarity:

1. **H1:** Increased Number of recall and recognise Communication factors of the authentication ceremony will result in a lower likelihood of a user making an error during the authentication process, i.e. getting phished.
2. **H2:** Increased Number of recall and recognise Communication factors of the authentication ceremony will lead to increased Elaboration of the authentication login prompt.
3. **H2(a):** The level of Attention given to the Recall communication factor of the authentication ceremony will be negatively related to the level of Elaboration.
4. **H2(b):** The level of Attention given to the Recognise communication factor of the authentication ceremony will be positively related to the level of Elaboration.
5. **H3:** Increased Capabilities will lead to increased Elaboration of the authentication login prompt.
6. **H4:** Increased Motivation will lead to increased Elaboration of the authentication login prompt.
7. **H5:** Increased Elaboration will result in a lower likelihood of the user making an error during the authentication process, i.e. getting phished.

<b>Construct</b>	<b>Description</b>	<b>Cronbach <math>\alpha</math></b>
Motivation	7 items; 5 point scale	0.728
Capabilities	3 items; 5 point scale	0.745
Elaboration	5 items; 5 point scale	0.696

**Table 8.9:** Summary of survey construct measurements and reliability

### 8.6.1 Reliability of Constructs

The measurement reliability of variables that were captured via survey questions as response scales was assessed using Cronbach’s alpha. Cronbach’s alpha is a measure of the internal consistency, or reliability, of model constructs. It is most commonly used for multiple Likert questions in a survey that form a scale. It is computed in terms of the average intercorrelation among the items measuring the concept. Cronbach’s alpha measures how closely related a set of items are as a group. It is expressed as a number between 0 and 1. It is generally accepted that values above 0.70 are preferred [166, 210]. However, others [98, 51] suggest that alpha reliability between 0.65 and 0.70 are also sufficient to insure internal consistency of the scale. Elaboration, Motivation or Capabilities constructs exhibited moderate to good internal reliability, ranging from 0.696 to 0.745 as shown in Table 8.9.

Table 8.9 shows a summary of survey construct measurements along with their alpha reliabilities.

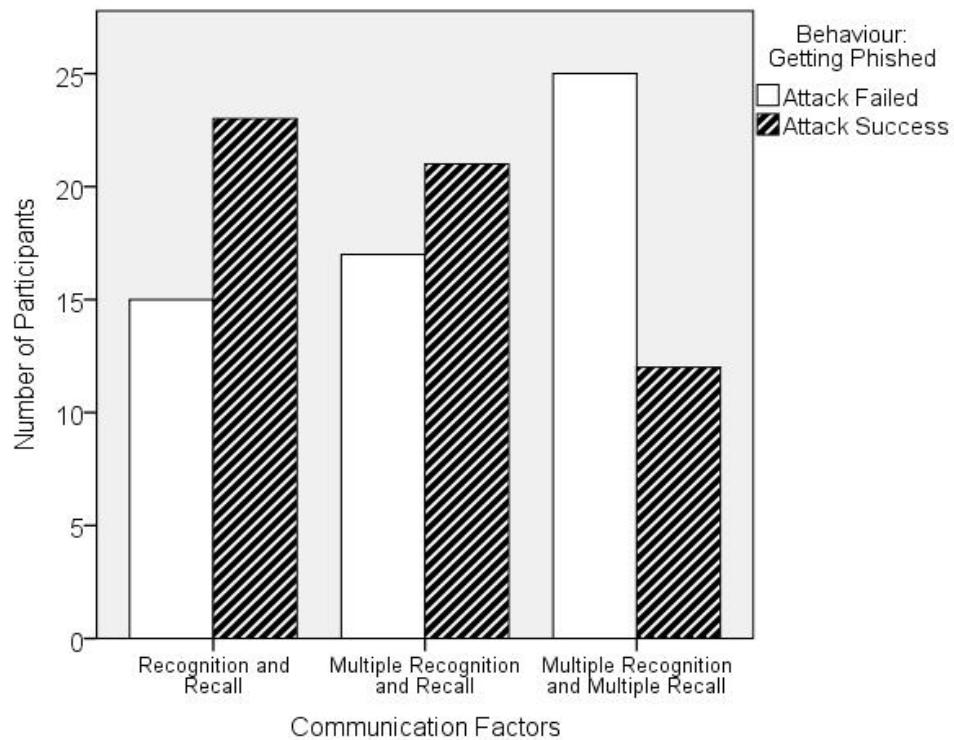
### 8.6.2 Hypotheses Testing

#### 8.6.2.1 Hypothesis H1: Communication Factors to Behaviour

*H1:* Increased Number of recall and recognise authentication Communication factors of the ceremony will result in a lower likelihood of a user getting phished.

A *Cochran-Armitage trend test* for association was run to determine whether a linear trend exists between the number of recall and recognition Communication tasks and the Behaviour - proportion of users who fell for the simulated attack.

The Cochran-Armitage test of trend showed a statistically significant linear trend ( $p = 0.015$ ), with adding more communication factors resulting in a higher proportion of users resisting the attack. The number of communication factors were 2 (Ceremony One), 4 (Ceremony Two) and 7 (Ceremony Three), and the proportion of users that resisted attack was as follows: 26.3%, 29.8% and 43.9%, as displayed in Figure 8.8.



**Figure 8.8:** H1: Cochran-Armitage association between the Number of login Communication factors and Behaviour

In order to ascertain the effects of the number of login communication tasks on the likelihood of being phished, a *logistic regression* was performed. The dependent

Predictors	B	S.E.	Wald	df	p	Exp(B)
Communication Factors:						
Recognition + Recall (Base)			6.446	2	<b>0.040*</b>	
Multi. Recognition + One Recall	-0.216	0.465	0.216	1	0.642	0.806
Multi. Recognition + Multi. Recall	-1.161	0.483	5.777	1	<b>0.016*</b>	0.313
Constant	0.427	0.332	1.659	1	0.198	1.533
Nagelkerke $R^2$ 0.078%						
Chi-square 6.776, df = 2, $p = 0.034^*$						
<b>Notes:</b> Multi. = Multiple; Significance is indicated by * $p < 0.05$ , B - regression coefficient; S.E. - standard errors; Wald - Wald chi-square value; df - degrees of freedom; $p$ - statistical significance; Exp(B) - odds ratios for the predictors.						

**Table 8.10:** H1: Results of logistic regression predicting being phished by login communication factors

variable was Behaviour - indicating attack success or failure; and independent variable was the Number of login Communication factors - a categorical variable with three categories. The logistic regression model was statistically significant ( $\chi^2(2) = 6.776, p = 0.034$ ). No outliers were found. The model explained 7.8% (Nagelkerke  $R^2$ ) of the variance in behaviour and correctly classified 61.1% of cases.

Login communication had statistically significant overall effect (Wald = 6.446, df = 2,  $p = 0.040$ ), as shown in Table 8.10. The Wald statistic test is used to determine statistical significance for each of the independent variables. In logistic regression, the B coefficient indicates the increase in the log odds (or logits) of the outcome for a unit increase of the independent variable. The B coefficient for MSMA was negative and significant (B = -1.161,  $p = 0.016$ ), indicating that having Multiple Recall and Multiple Recognition communication is associated with decreased odds of falling for the attack (Table 8.10).

The  $\text{Exp}(B)$  value presents change in the odds for each unit increase of the independent variable. Values less than 1.000 indicate decreased odds for an increase in one unit of the independent variable. The  $\text{Exp}(B)$  for Ceremony Three (MSMA) was equal to 0.313. What this means is that the odds of noticing a phishing attack was 0.313 times lower for users in Ceremony One than in Ceremony Three. For clarity, the odds ratio is sometimes inverted, i.e.  $1 \div 0.313 = 3.194$ . Therefore, we can say that the participants using Multiple Recognition and Multiple Recall (Ceremony Three) had 3.194 higher odds to notice a phishing attack than the participants using Recognition and Recall ceremony (Ceremony One).

Hence, hypothesis H1 was supported by the data. Increased Number of recall and recognition login Communication factors reduces the likelihood of the user getting phished.

### 8.6.2.2 Hypothesis H2: Communication Factors to Elaboration

*H2*: Increased Number of recall and recognise authentication Communication factors of the ceremony will lead to increased Elaboration of the login prompt.

A *Cochran-Armitage trend test for association* [44, 17] was run to determine whether there is a linear trend in binomial proportions of Elaboration across the number of communication factors.

The Elaboration was operationalised as a dichotomous (low and high) variable. The scores 1-3 were operationalised as a low Elaboration level (= 0); and 4 and 5 as a high Elaboration level (= 1).

The number of communication factors were 2 (Ceremony One), 4 (Ceremony 2) and 7 (Ceremony Three). The proportion of users with high elaboration was 65.8%, 81.6% and 81.1% respectively. The Cochran-Armitage test of trend did not show a statistically significant linear trend between the number of communication factors and the Elaboration level ( $p = 0.119$ ).

We performed *logistic regression* to examine whether the number of Recall and Recognise communication factors predicts level of Elaboration. The Elaboration was operationalised as a dichotomous (low and high) variable.

The number of communication factors were 2 (Ceremony One), 4 (Ceremony 2) and 7 (Ceremony Three). However, the omnibus model was not statistically significant ( $p = 0.198$ ) to establish prediction between login communication factors and Elaboration.

Overall, there was no support by the data for hypothesis H2.

### **8.6.2.3 Hypothesis H2(a): Attention to Recall**

*H2(a)*: The level of Attention given to the *Recall* communication factor of the authentication ceremony will be *negatively* related to the level of Elaboration.

Only data from Ceremony Two and Three were used to test this hypothesis as they differed in number of recall communication factors.

We performed a *logistic regression* to ascertain the effects of the recall time and ceremony condition on the Elaboration level. The Attention to Recall and ceremony condition were independent variables. The Attention to Recall was measured as the overall time a participant spent on considering and entering the text and/or PIN part of the password and ceremony was coded as a categorical variable. The Elaboration was a dichotomous, dependent variable. The Elaboration scores 1-3 were operationalised as a low Elaboration level (= 0); and 4 and 5 as a high Elaboration level (= 1).

Linearity of the Recall time with respect to the Elaboration was assessed via the Box-Tidwell procedure. A Bonferroni adjustment was applied, resulting in statistical significance being accepted when  $p < 0.0125$ . Based on this assessment, the continuous Recall time variable was found to be linearly related to the logit of the

Predictors	B	S.E.	Wald	df	p	Exp(B)
Ceremony	0.580	0.692	0.703	1	0.402	1.787
Attention to Recall	-0.000078	0.000	4.414	1	<b>0.035*</b>	0.99985
Constant	2.63	0.508	16.517	1	0.000	7.868

Nagelkerke  $R^2$  0.136%

Chi-square 6.578, df = 2,  $p = \mathbf{0.037^*}$

**Notes:** Ceremony is for Ceremony Two compared to Ceremony Three; Significance is indicated by  $*p < 0.05$ , B - regression coefficient; S.E. - standard errors; Wald - Wald chi-square value; df - degrees of freedom;  $p$  - statistical significance; Exp(B) - odds ratios for the predictors.

**Table 8.11:** H2a: Results of logistic regression predicting Elaboration level

Elaboration. There were two residuals with a value of 3.023 and 2.774 standard deviations, which were kept in the analysis. No outliers were found. The logistic regression model was statistically significant,  $\chi^2(2) = 6.578$ ,  $p = 0.037$ . The model explained 13.6% (Nagelkerke  $R^2$ ) of the variance in Elaboration and correctly classified 84% of cases.

Attention to Recall had statistically significant overall effect (Wald = 4.414, df = 1,  $p = 0.035$ ). The B coefficient for attention to Recall was negative and significant ( $B = -0.000078$ ,  $p = 0.035$ ), indicating that increased Attention to Recall is associated with decreased odds of high Elaboration. The Exp(B) for Attention to Recall was equal to 0.99985. For clarity, the odds ratio is inverted, i.e.  $1 \div 0.99985 = 1.00015$ . Therefore, for each *millisecond* increase in Attention to Recall, the odds of high Elaboration decreases by a factor of 1.00015. See Table 8.11.

Hence, hypothesis H2(a) was supported by the data. Increased Attention to Recall is negatively related to the level of Elaboration.



#### 8.6.2.4 Hypothesis H2(b): Attention to Recognise

*H2(b)*: The level of Attention given to the *Recognise* communication factor of the authentication ceremony will be *positively* related to the level of Elaboration.

Only data from Ceremony One and Two were used as they differed in number of recognise communication factors. The Elaboration was the dependent variable, measured as a dichotomous (low and high) variable. The Attention to Recognise was the independent variable, measured as the overall time spent on recognising/choosing images.

We performed logistic regression to ascertain the effects of ceremony condition and the recognition time on Elaboration, but this model was not statistically significant ( $\chi^2(2) = 2.484, p = 0.289$ ).

Hence, we could not find support of hypothesis H2(b) from the data.

#### 8.6.2.5 Hypothesis H3: Capabilities to Elaboration

*H3*: Increased Capabilities will lead to increased Elaboration of the authentication login prompt.

For this test the Elaboration was operationalised as a dichotomous, low (= 0) and high (= 1) variable.

We performed *Cochran-Armitage trend test for association*. The Capability level was measured on the scale 1 to 5, and the proportion of users with increased Elaboration was 40.0%, 76.9%, 78.0%, 76.7% and 100.0%, respectively. The Cochran-Armitage test of trend did not show a statistically significant linear trend between Capability and the Elaboration,  $p = 0.247$ .

Hypothesis 3 was also tested using *Somers' delta* (or Somers' *D*) to determine the association between user's Capabilities level and the level of Elaboration of the authentication login prompt. Both Capabilities and Elaboration were operationalized

as ordinal variables, on the scale of 1 to 5. There was a strong, positive association between Capability and the Elaboration level, but it was not statistically significant ( $D = 0.601$ ,  $p = 0.439$ ). Therefore, the data were only in support of the direction of hypothesis 3.

Hence, we could not find support of hypothesis H3 from the data.

#### 8.6.2.6 Hypothesis H4: Motivation to Elaboration

$H_4$ : Increased Motivation will lead to increased Elaboration of the authentication login prompt.

Hypothesis 4 was tested using *Somers' D* measure examining the strength and direction of association between users Motivation level and the level of Elaboration of the authentication login prompt. There was a positive association between the Motivation and the Elaboration levels, and it was statistically significant ( $D = 0.178$ ,  $p = 0.041$ ), as shown in Table 8.12.

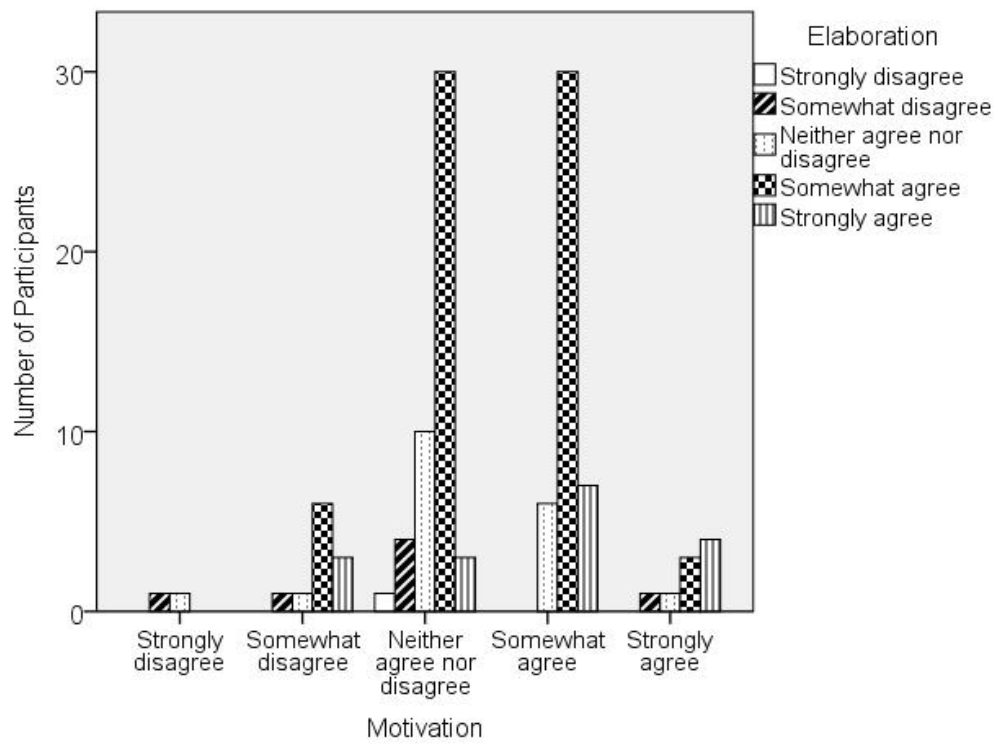
	<b>Somers' <math>D</math></b>	<b><math>p</math></b>
Motivation to Elaboration	0.178	<b>0.041*</b>

**Notes:** Significance is indicated by \* $p < 0.05$

**Table 8.12:** H4: Association between Motivation and Elaboration

As Somers'  $D$  is positive, it means that as the user's Motivation increases so does the Elaboration (Figure 8.9).

Hence, hypothesis 4 was supported by the data.



**Figure 8.9:** H4: Association between Motivation and Elaboration

### 8.6.2.7 Hypothesis H5: Elaboration to Behaviour

*H5*: Increased Elaboration will result in a lower likelihood of the user making an error during the authentication process, i.e. getting phished.

We performed *Cochran-Armitage trend test for association* to determine if there is a linear relationship, association, between the Elaboration and the Behaviour. The test was run to determine whether a linear trend exists between the Elaboration level and the proportion of users who submitted their password on the spoofed login page.

The Elaboration level was measured on the scale 1 to 5 (high elaboration), and the proportion of users where attack failed was 0.0, 42.9, 42.1, 53.6 and 52.9, respectively. The Cochran-Armitage test of trend did not show a statistically significant linear trend between Elaboration and the Behaviour of users who submitted their password on the spoofed login page,  $p = 0.272$ .

We also ran *Fisher's exact test* treating the Elaboration as a dichotomous variable. The Elaboration was operationalised as a dichotomous (low and high) variable. Elaboration scores 1-3 were operationalised as a low Elaboration level ( $= 0$ ); and 4 and 5 as a high Elaboration level, ( $= 1$ ).

The difference between the two independent binomial proportions was not statistically significant ( $p > 0.05$ ). Hence, we could not find evidence of association between Elaboration and Behaviour.

Hence, there was no support for hypothesis H5 by the data.

Hypotheses	Overall conclusion
H1	Supported Increased Number of login Communication factors results in a lower likelihood of getting phished.
H2	Not supported
H2(a)	Supported Increased Attention to Recall communication results in a lower Elaboration level.
H2(b)	Not supported
H3	Direction as hypothesized, but not significant A strong, positive association between Capabilities and Elaboration level.
H4	Supported As the user's Motivation increases so does the Elaboration.
H5	Not supported

**Table 8.13:** Summary of the Model for Analysing HF-APAC hypotheses results

### 8.6.3 Summary of Results

Results of the hypotheses evaluation of our Model for Analysing HF-APAC are summarised as follows and depicted in Table 8.13.

- Increasing the number of communication factors did not influence how much users elaborated on the login prompt.
- The number of communication factors was a significant predictor of whether an individual was phished or not.
- The elaboration level was not associated with a phishing detection rate.
- Increased user's motivation was associated with increased elaboration.

- Increased attention to recall communication resulted in a lower elaboration level.
- There was a positive association between the capabilities and the elaboration level, but not statistically significant.
- The attention to recognise communication was not associated with the elaboration level.

## 8.7 Discussion

### 8.7.1 MSMA Effectiveness

The evaluation of our newly proposed MSMA ceremony involved exploring whether the HPA using multiple authentication images in combination with text passwords improves effectiveness of using security images as part of authentication.

Our study results showed a statistically significant difference between MSMA and the ceremony with a single image and text password (i.e. Ceremony One condition, Section 7.3.1.2) in resisting simulated phishing attack. In the single image and text password condition, 23 out of 38 (60.53%) of participants entered their password in spite of different security images displayed. Only 12 out of 37 (32.43%) of MSMA participants entered their password, showing a significant improvement to the single security image condition (Figure 8.10). Significantly more MSMA users resisted the attack (Table 8.14) and that should imply an increased anti-phishing resistance in comparison to single security image authentication – similar to commercial variations often used on internet banking websites [18, 180, 192]. This shows that improvements could be made in the way that the security images are currently used which could result in greater anti-phishing resistance.

<b>Ceremony</b>	<b>Attack Successful</b>	<b><i>p</i></b>
Single image + text	60.53%	
Multiple images + text	55.36%	
MSMA (Multiple images + multiple text)	32.43%	<b>0.036*</b>

Significance is indicated by \* $p < 0.05$

**Table 8.14:** Percentages of participants who entered their password without the right image being displayed

The participants using multiple images and a text password ceremony (i.e. Ceremony Two condition, 7.3.1.3) were not significantly more effective at noticing that different images were displayed; 21 out of 38 (55.36%) of them logged in anyway. Surprisingly, the difference was not significant when compared to MSMA or the Ceremony One (i.e. single security image).

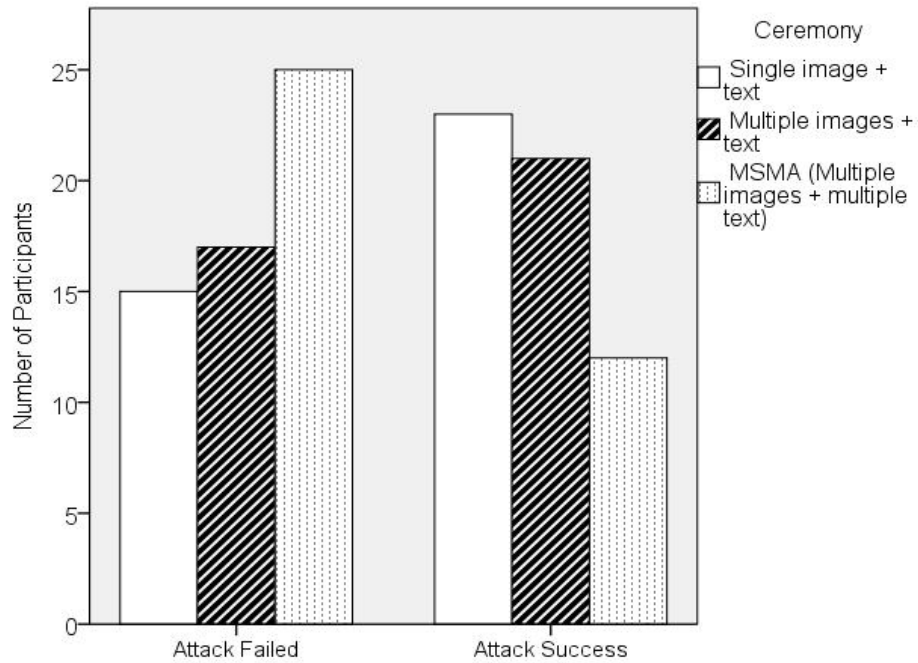
Only the HPA as used in MSMA, with multiple image choices combined with text passwords seem to make users significantly less likely to succumb to the phishing attack.

## 8.7.2 Human Communication Processing Principles

The Model hypotheses H1 to H5 testing was the evaluation of the human communication guidelines suggested in Section 5.4. Overall, the results showed support for about half of them.

Our findings show that the attention to recall communication (i.e. text and/or PIN password) significantly influence elaboration, which is an important step in deception detection. Decreased attention to recall communication factors results in higher elaboration.

The results show that neither the number of communication factors nor attention



**Figure 8.10:** Count of participants and the attack outcome per ceremony

to recognise communication (i.e. images) influenced the extent of elaboration. As elaboration is defined as the process of making conscious connections between the cues observed and the prior knowledge, this means that the type of communication tasks needed to be performed affected overall cognitive effort during authentication.

However, user's motivation was found to significantly influence elaboration, with increased motivation the elaboration was increased as well.

Another important implication of our study is the lack of significant support for the effect of prior security awareness and knowledge on elaboration. Our results showed a strong, positive association between capabilities (measuring web security and the ceremony knowledge) and elaboration, but not statistically significant.

The results also show that performing additional communication tasks to log in was a significant predictor of whether an individual was phished or not, leading to significantly greater effectiveness in detecting the simulated attack. An increase in



communication factors have shown significant increases in the phishing detection rate which is depicted in Table 8.15. Surprisingly, elaboration expended in processing a login communication was not significantly related to the likelihood of a user getting phished. Hence, we could not find the evidence that those who more closely attend to login communication end up making the right choice.

Therefore, the human communication processing principles, proposed by the Model can be summarised as follows:

1. Increasing the number of recall and recognise communication factors results in a higher phishing detection rate.
2. Increasing the number of communication factors does not influence how much users elaborate on the login prompt.
3. The elaboration level is not associated with a phishing detection rate.
4. Increased user's motivation is associated with increased elaboration.
5. Increased attention to recall communication results in a lower elaboration level.
6. Increased user's knowledge of the ceremony and online security can lead to increased elaboration.
7. The attention to recognise communication is not associated with the elaboration level nor a higher phishing detection rate.

<b>Communication factor</b>	<b>Phishing detection rate</b>
Recognition and recall	39.47%
Multiple recognition and recall	44.64%
Multiple recognition and multiple recall	67.57%

**Table 8.15:** Summary of the communication factors and phishing detection rate

### 8.7.3 Limitations

As with other studies, our study had a number of possible limitations, which we discuss in this section.

Even though we attempt to emphasize ecological validity in our study, it can be very difficult to run phishing studies that are ecologically valid. The study results were most likely influenced by participants lack of experience with the ceremonies used, and the fact that they were still establishing mental models for how these ceremonies work. Our study did not evaluate usability differences between the ceremonies, especially if the increased phishing resistance of MSMA affected its usability.

While the findings of the study shed light on the communication process influencing detection of spoofed login prompt, arguments could be made that the percentage of the students among participants (76.1%) was high. It is possible that students are more computer-literate than the general population and that could influence the level of detection. However, students are a relevant sample population for authentication and phishing as they tend to engage in more online behaviours [217]. Students were used as the main participant sample in previous important phishing studies [194, 110, 217].

Another limitation was that we did not use the TLS certificate for the domain name that we used for the study, as normally used in commercial websites. While previous research has shown that HTTPS security indicators are generally not effective [57, 194], some users might have realized that the website they were accessing

was not via a HTTPS connection and could have behaved differently. One participant pointed out that the login page is not a secure connection, which is what one would normally expect on a sensitive websites.

Our user study was conducted in a laboratory setting, as were a number of previous important phishing studies [57, 110, 194]. Countermeasures were taken to ensure ecological validity, but it can be very difficult to run phishing studies that are ecologically valid, especially in laboratory settings. Laboratory environment can also influence a higher detection rate than in real world conditions [80, 144]. A future study carried entirely online, not in a laboratory environment, could add a different insights into user's behaviour and it would allow the comparison of results. Also, using an online micro-working platform such as Crowdfunder [49], or Amazon's Mechanical Turk [5] would give access to a large and more diverse participants' sample [29]. However, some argue that perhaps the population of workers on Mechanical Turk are more computer-literate than the general population [204].

The Ceremony One prototype used in our study closely mimicked the implementation of security images authentication as used by some websites [192, 180]. We could not find any other study that performed the same type of attack to directly compare our results with. However, in one study [144] the authors considered performing it, but due to no definitive understanding of the most effective way to trick users they have chosen to use absence of a security image attack instead. Therefore, the closest comparison we could do was with the studies that explored the ability of users to notice missing security images. These studies largely evaluated if participants would enter their password even in the absence of a security image with somewhat differing results. The results ranged from 92% [194], 73% [144], to 40% [110] of participants entering their passwords without their security image being displayed. The differences between the results of those studies can partly be attributed to the laboratory [194] vs. online [144] settings; or a combination of online settings

used as part of an university submission system [110]. In our Ceremony One (i.e security image) condition, 60.53% of participants (Table 8.14) entered their password in spite of different security images displayed which was consistent with other studies using simulated phishing attacks.

As we mentioned security in the study information sheets given to participant to read before signing the consent form (described in Section 7.3.2.3), arguments can be made that participants were not deceived. However, security was never mentioned on the website page (Figure A.6) from which participants conducted the study. Neither phishing nor spoofing was ever mentioned in information sheets given, or the website from which the study was conducted, on which the participants were given other tasks to attend (Section 7.3.2.4). Also, a number of previous important phishing studies have shown that it is possible to get meaningful results without fully deceiving participants. For example, the study by Dhamija, Tygar and Hearst [57, 55], where participants were aware that they were part of a security study and that spoofed websites would be present in the study. In the study by Herzberg and Margulies [110], students participants were specifically warned that an attack could happen. In the study by Wu, Miller and Garfinkel [226, 225] subjects were given a consent form to read that explained that the purpose of the study was to test web browser security indicators that detect fake web pages that look like pages from legitimate websites; and that the purpose of these fake websites is to trick people into making dangerous decisions or actions.

It is likely that mentioning security in our study information sheets decreased the attack success rates. Therefore, we would expect participants to detect spoofed login prompt at a higher rate than in real world conditions. However, if our participants were fooled, real-world users are likely to also be fooled. We have also shown that our result are consistent with other studies [194, 144, 110] that simulated phishing attacks.

## 8.8 Conclusion

The aim of the study was to experimentally evaluate the MSMA ceremony. The results showed that significantly more MSMA users resisted simulated attack in comparison to a security image ceremony, similar to commercial variations often used on internet banking websites. The HPA, consisting of multiple images combined with text passwords, as used in MSMA, makes users more resistant to phishing.

The evaluation of the Model for Analysing HF-APAC involved assessing the impact of the number and types of login communications (recall and recognition) on a user's likelihood of getting phished; the influence of attention and elaboration on phishing and how motivation and capabilities influence elaboration.

The study results showed that an increase in the number of communication factors have improved detection rate of spoofed login prompt, but it did not influence how much users elaborated on the login prompt. Increased attention to recall communication resulted in a lower elaboration level, but not the recognise communication. Increased user's motivation was associated with increased elaboration. Also, the level of elaboration on the login prompt was not associated with the phishing detection rate.

# Chapter 9

## Conclusions

### 9.1 Thesis Summary

For more than a decade, phishing has been one of the main social engineering attacks on the Internet. As new legal and technical approaches are being put in place to fight it, phishers are modifying their techniques as well, and the number of phishing attacks is not abating. The majority of the websites that are being spoofed require that the users authenticate themselves. Therefore, phishing attacks usually involve spoofing a login webpage and the authentication method used by the service provider. Phishers target the human users and their usage and interpretation of authentication schemes that fools them to make mistakes.

The goal of this thesis was to explore why current web authentication schemes do not protect effectively against phishing. We investigated the use of security ceremonies as a way of extending the reach of current methods for social, technological and contextual analysis of web authentication schemes. A security ceremony extends a concept of security protocol and includes the human node (i.e. user component) explicitly. Ceremony research stems from the recognition that information security is much more than a technical issue. The challenge of defining and analysing ceremonies is significant, especially the modelling of the communication process-

ing performed by humans. The focus of this thesis was the modelling of human communication processing in authentication ceremonies that can help to mitigate phishing.

Multifaceted aspects of phishing was the reason that this thesis involves multiple lines of research: phishing and anti-phishing countermeasures; anti-phishing authentication schemes; security ceremonies; security communication processing and decision making. The analysis of the research in these areas was provided in Chapter 2. It led us to approach the phishing problem by exploring why existing web authentication schemes, built on security protocols proven to be secure in theory, are not as secure when they are deployed in real world and used by humans.

In Chapter 3 we explored assumptions about the behaviour of humans who are expected to process and react to security-related communication as part of web authentication ceremonies. We have shown how these assumptions can affect its security. We described related issues that can arise due to these assumptions and presented the main factors that may influence these issues in different ways. Recognising these assumptions, issues and influencing factors helped us to identify the components of the Human Factors in Anti-Phishing Authentication Ceremonies (HF-APAC) Framework described in Chapter 4.

The Human Factors in APAC Framework was designed to be used by designers of authentication ceremonies at the design phase to improve the human interface weak points of a ceremony and reduce the success of phishing attacks. The Framework can help to extend a ceremony threat model by taking into account issues and factors affecting processing of authentication communication by human users and consequently their phishing detection. We described how the HF-APAC Framework fits in broader ceremony analysis and gave a detailed description of its components and overview of the possible application of the Framework.

We proposed a design and analysis process of human communication factors

in authentication ceremonies and described how the HF-APAC Framework can be applied either to improve the design of a new, or an existing ceremony.

We developed a model that demonstrates how the HF-APAC Framework can be used by a designer in ceremony analysis. The Model for Analysing HF-APAC, presented in Chapter 5, is a communication processing model that makes specific assumptions about the components of the HF-APAC Framework and explores in what extent they influence each other. The Model explores how users process authentication communication conveyed through a website login prompt and what, and to what extent, influences their decision-making processes and behaviour, that can ultimately result in an error of submitting login credentials to a phishing website.

In the Model we have proposed communication processing principles that can be used as part of the design process of authentication ceremonies. In Chapter 6 we demonstrated how these principles can be applied as part of the design of an authentication ceremony to provide enhanced anti-phishing resistance: we designed a new MultiStep Mutual Authentication (MSMA) ceremony. The MSMA ceremony is a mutual, hybrid authentication ceremony that combines PIN, recognition-based graphical and text password in multiple steps. The graphical part of the MSMA ceremony is a HPA that enables the user to verify that the website, he/she is accessing, is legitimate. The HPA can be anything, but we have chosen a visual HPA, to be provided in the form of images, rather than a piece of music or excerpt from a book.

Chapter 7 presented the user study we designed and performed to experimentally evaluate the Model for Analysing HF-APAC and the MSMA ceremony. The goal of the study was to explore the impact of number and types of login communications (recall and recognition) on user's likelihood of getting phished; to explore the influence of attention and elaboration on phishing; and also to explore the influence of users' motivation and capabilities. The second goal of the study was to



experimentally evaluate MSMA resistance to phishing.

The data analysis and the results of the study were presented in Chapter 8. The results show that significantly more MSMA users resisted the simulated phishing attack in comparison to users of a security image ceremony similar to commercial variations often used on internet banking websites [18, 180, 192].

## 9.2 Contributions

We summarise the contributions of this thesis as follows:

1. We further developed and enhanced the understanding of security ceremonies and their importance in analysis of social engineering threats such as phishing. We demonstrated modelling of communication processing performed by human nodes in authentication ceremonies with the HF-APAC Framework and the Model for Analysing HF-APAC.
2. We proposed and demonstrated the design and analysis process of human communication factors in authentication ceremonies with the HF-APAC Framework, the Model for Analysing HF-APAC, MSMA ceremony and the user study.

The process we demonstrated fills the research gap of modelling of processing performed by human nodes in the ceremony analysis.

3. We developed the Human Factors in Anti-Phishing Authentication Ceremonies Framework that is used as part of the proposed ceremony design and analysis process.

The particular focus of the Framework is on helping to analyse the communication processing performed by human users in authentication ceremonies.

That in turn should help to adapt the ceremony design to better resist social engineering threats such as phishing.

4. We designed the Model for Analysing HF-APAC as a communication processing model that demonstrates a usage of the HF-APAC Framework. The Model examines how users process authentication communication tasks and how these tasks impact the user's decision-making and consequently their phishing detection.

The human communication processing principles proposed and evaluated by the Model can be taken into account by designers when designing new authentication ceremonies or adapting existing ones. Taking into account these principles can improve the anti-phishing resistance of the ceremony.

5. We developed the MultiStep Mutual Authentication (MSMA) anti-phishing ceremony. The MSMA ceremony is a mutual authentication ceremony that combines PIN, text password and recognition-based graphical passwords in multiple steps. The graphical part of the MSMA ceremony is a HPA that helps the user verify that the website, he/she is accessing, is legitimate, helping to mitigate phishing attacks.

We found evidence that the HPA, consisting of multiple images combined with text passwords, as used in MSMA, improves user's ability to distinguish between legitimate and spoofed website login prompts.

We conducted a user study to experimentally evaluate the Model and MSMA. The Model evaluation results show how processing of authentication communication factors impacts the user's decision-making and consequently their phishing detection. We found that the principle of increasing the number of recall and recognise communication factors, as used in MSMA, improves the phishing resistance of a ceremony.

### 9.3 Future Research Directions

There are several potential improvements and further extensions of our thesis work that would be interesting to investigate further.

We designed the HF-APAC Framework as a way in extending threat model of authentication ceremonies and suggested its place in broader ceremony analysis. The Framework contributes to ceremony research by the modelling of processing performed by human nodes in ceremonies. An interesting avenue of research would be to investigate if and how the Framework can be used in a formal methods approach of security ceremonies analysis.

The components of our Framework consider issues and factors affecting communication processing in knowledge-based anti-phishing authentication ceremonies. For our next phase of research, we will examine factors specific to biometric, token or other types of authentication ceremonies that could be added into the Framework and that would further enhance its applicability.

Another avenue of research would be the design of a new MSMA prototype using other types of HPAs, instead of images, examples of which would be implementation of an audible HPA (e.g. a piece of music).

# Bibliography

- [1] C. Abad. The economy of phishing: A survey of the operations of the phishing market. *First Monday*, 10(9), September 2005.
- [2] A. Agresti. *An Introduction to Categorical Data Analysis*. John Wiley and Sons, Inc., 2nd edition, 2007.
- [3] Allied Irish Banks. Common frauds and threats, 2017. <https://aib.ie/investorrelations/security-centre/common-frauds-and-threats>, Accessed December 2017.
- [4] I.M. Alseadoon. *The impact of users' characteristics on their ability to detect phishing emails*. PhD thesis, Science and Engineering Faculty, Queensland University of Technology, Brisbane, Australia, 2014.
- [5] Amazon Mechanical Turk. Human intelligence through an API, 2017. <https://www.mturk.com/>, Accessed December 2017.
- [6] Amazon.com. About identifying whether an e-mail or webpage is from Amazon, 2017. Accessed December 2017.
- [7] R.J. Anderson. Why cryptosystems fail. *Communications of the ACM*, 37(11):32–40, November 1994.
- [8] Anti-Phishing Working Group. Phishing activity trends report, 4th quarter 2009. Technical report, Anti-Phishing Working Group, Inc., 2009.

- [9] Anti-Phishing Working Group. Phishing activity trends report, 1st half 2017. Technical report, Anti-Phishing Working Group, October 2017. Accessed December 2017.
- [10] Anti-Phishing Working Group. Phishing activity trends report, 1st half 2017. Technical report, Anti-Phishing Working Group Inc., October 2017. Accessed December 2017.
- [11] Anti-Phishing Working Group. Phishing activity trends report, 4th quarter 2016. Technical report, Anti-Phishing Working Group Inc., February 2017. Accessed August 2017.
- [12] Anti-Phishing Working Group. Unifying the global response to cybercrime, 2017. <https://www.antiphishing.org>, Accessed August 2017.
- [13] Anti-Phishing Working Group. Phishing activity trends report, 3rd quarter 2017. Technical report, Anti-Phishing Working Group Inc., February 2018. Accessed March 2018.
- [14] APWG. APWG/CMU phishing education landing page program, 2008. <http://education.apwg.org>, Accessed December 2017.
- [15] APWG. APWG ecrime researchers sync-up, March 2011. <http://docs.apwg.org/ecrimeresearch/2011syncup/cfp.html>.
- [16] APWG. Global phishing survey: Trends and domain name use in 1H2012, October 2012. Accessed January 2017.
- [17] P. Armitage. Tests for linear trends in proportions and frequencies. *Biometrics*, (11):375–386, 1955.
- [18] Bank of America. SiteKey authentication, 2013.

<https://www.bankofamerica.com/privacy/online-mobile-banking-privacy/sitekey.go>, Accessed March 2013.

- [19] Bank of Ireland Group plc. Day-to-day safety, 2017. <https://www.bankofireland.com/security-zone/personal/safety-online>, Accessed December 2017.
- [20] S. Baslyman and S. Chiasson. "Smells Phishy?": An educational game about online phishing scams. In *2016 APWG Symposium on Electronic Crime Research (eCrime)*, pages 1–11, June 2016.
- [21] A. Beutement and M.A. Sasse. Gathering realistic authentication performance data through field trials. In *The 6th Symposium on Usable Privacy and Security, SOUPS '10*, Redmond, WA, USA, July 2010.
- [22] G. Bella and L. Coles-Kemp. Seeing the full picture: the case for extending security ceremony analysis. In *9th Australian Information Security Management Conference*, Edith Cowan University, Perth Western Australia, December 2011.
- [23] G. Bella and L. Coles-Kemp. Layered analysis of security ceremonies. In *Information Security and Privacy Research*, volume 376, pages 273–286. Springer, 2012.
- [24] M. Bellare. Practice-oriented provable-security. In *Proceedings of the 1997 Information Security Workshop (ISW)*, Tokyo, Japan, September 1997.
- [25] M. Bellare, D. Pointcheval, and P. Rogaway. Authenticated key exchange secure against dictionary attacks. In *Proceedings of the 19th International Conference on Theory and Application of Cryptographic Techniques, EURO-CRYPT'00*, pages 139–155, Berlin, Heidelberg, 2000. Springer-Verlag.

- [26] M. Bellare, D. Pointcheval, and P. Rogaway. Authenticated key exchange secure against dictionary attacks. In *Proceedings of the 19th International Conference on Theory and Application of Cryptographic Techniques, EURO-CRYPT'00*, pages 139–155, Berlin, Heidelberg, 2000. Springer-Verlag.
- [27] M. Bellare and P. Rogaway. Entity authentication and key distribution. In *Proceedings of the 13th Annual International Cryptology Conference on Advances in Cryptology, CRYPTO '93*, pages 232–249, New York, NY, USA, 1994. Springer-Verlag New York, Inc.
- [28] Z. Benenson, F. Gassmann, and R. Landwirth. Unpacking spear phishing susceptibility. In *Financial Cryptography and Data Security 2017*, Lecture Notes in Computer Science. Springer International Publishing, April 2017.
- [29] A.J. Berinsky, G.A. Huber, and G.S. Lenz. Evaluating online labor markets for experimental research: Amazon.com’s Mechanical Turk. *Political Analysis*, 20(03):351–368, 2012.
- [30] R. Biddle, S. Chiasson, and P.C. Van Oorschot. Graphical passwords: Learning from the first twelve years. *ACM Computing Surveys*, 44(4):19:1–19:41, September 2012.
- [31] J. Bonneau. The science of guessing: Analyzing an anonymized corpus of 70 million passwords. In *Proceedings of the 2012 IEEE Symposium on Security and Privacy*, pages 538–552, Washington, DC, USA, 2012. IEEE Computer Society.
- [32] J. Bonneau, C. Herley, P.C. van Oorschot, and F. Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *Proceedings of the 2012 IEEE Symposium on Security and Privacy, SP '12*, pages 553–567, Washington, DC, USA, 2012. IEEE Computer Society.

- [33] J. Bonneau, S. Preibusch, and R.S. Anderson. A birthday present every eleven wallets? The security of customer-chosen banking PINs. In *The 16th International Conference on Financial Cryptography and Data Security, FC 12*, pages 25–40. Springer-Verlag, 2012.
- [34] C.A. Bravo-Lillo. *Improving Computer Security Dialogs: An Exploration of Attention and Habituation*. PhD thesis, Carnegie Mellon University, Pittsburgh, PA, May 2014.
- [35] S. Brostoff and M. A. Sasse. Safe and sound: A safety-critical approach to security. In *Proceedings of the 2001 Workshop on New Security Paradigms, NSPW '01*, pages 41–50, New York, NY, USA, 2001. ACM.
- [36] W.E. Burr, D.F. Dodson, and W.T. Polk. Electronic authentication guideline. Technical report, NIST, August 2013.
- [37] M.C. Carlos. *Towards a Multidisciplinary Framework for the Design and Analysis of Security Ceremonies*. PhD thesis, Royal Holloway, University of London, 2014.
- [38] M.C. Carlos and G. Price. Understanding the weaknesses of human-protocol interaction. In *Workshop on Usable Security at 16th International Conference on Financial Cryptography and Data Security*, March 2012.
- [39] S. Chiasson, C. Deschamps, E. Stobert, M. Hlywa, B. Freitas Machado, A. Forget, N. Wright, G. Chan, and R. Biddle. [paper] the MVP web-based authentication framework. In *International Conference on Financial Cryptography and Data Security (FC)*, pages 16–24. Springer Berlin/Heidelberg, 2012.
- [40] S. Chiasson, Stobert E., A. Forget, R. Biddle, and P.C. Van Oorschot. Persuasive Cued Click-Points: Design, implementation, and evaluation of a



- knowledge-based authentication mechanism. *IEEE Transactions on Dependable and Secure Computing*, 9(2):222–235, March 2012.
- [41] S. Chiasson, P. C. van Oorschot, and R. Biddle. Graphical password authentication using Cued Click Points. In *Computer Security – ESORICS 2007: 12th European Symposium On Research In Computer Security*, Dresden, Germany, September 2007.
- [42] R.B. Cialdini. *Influence: Science and Practice*. Pearson Education, Inc., 5th edition, 2009.
- [43] R. Clayton. Insecure real-world authentication protocols (or why phishing is so profitable). In *Thirteenth Cambridge Protocols Workshop, Sidney Sussex, 2005*, Sydney, Sussex, 2005.
- [44] W. G. Cochran. Some methods for strengthening the common chi-squared tests. *Biometrics*, (10):417–451, 1955.
- [45] Confident Technologies. Confident ImageShield, 2017. <http://confidenttechnologies.com/confident-imageshield/>, Accessed July 2017.
- [46] M. Cova, C. Kruegel, and G. Vigna. There is no free phish: An analysis of ”free” and live phishing kits. In *Proceedings of the 2Nd Conference on USENIX Workshop on Offensive Technologies, WOOT’08*, pages 4:1–4:8, Berkeley, CA, USA, 2008. USENIX Association.
- [47] L.F. Cranor. A Framework for Reasoning About the Human in the Loop. Technical Report CMU-CyLab-08-001, Carnegie Mellon University, 2008.
- [48] L.F. Cranor and S. Garfinkel. *Security and Usability: Designing Systems that People Can Use*. O’Reilly Media, first edition, 2005.

- [49] CrowdFlower. Making AI work in the real world, 2017. Accessed December 2017.
- [50] D. Cyr, R. Childs, and S. Elgie. Recruiting students for research in post-secondary education: A guide. Technical report, Toronto: Higher Education Quality Council of Ontario, 2013.
- [51] R.F. DeVellis. *Scale development: Theory and applications, Third Edition*. Sage Publications, 2012.
- [52] R. Dhamija. *Authentication for Humans: The Design and Evaluation of Usable Security Systems*. PhD thesis, University of California, Berkeley, Fall 2005.
- [53] R. Dhamija and L. Dusseault. The seven flaws of identity management: Usability and security challenges. *IEEE Security and Privacy*, 6(2):24–29, March 2008.
- [54] R. Dhamija and P. Perrig. Déjà Vu: A user study using images for authentication. In *USENIX Security Symposium*, August 2000.
- [55] R. Dhamija and D. Tygar. The battle against phishing: Dynamic Security Skins. In *Symposium on Usable Privacy and Security (SOUPS) 2005*, Pittsburgh, PA, USA, July 2005. ACM.
- [56] R. Dhamija and J.D. Tygar. Phish and HIPs: Human interactive proofs to detect phishing attacks. In *Human Interactive Proofs, Second International Workshop, HIP 2005*, Bethlehem, PA, USA, May 2005.
- [57] R. Dhamija, J.D. Tygar, and M. Hearst. Why phishing works. In *CHI Conference on Human Factors in Computing Systems*, Montreal, Quibec, Canada, April 2006.

- [58] A. Diamantopoulos and B.B. Schlegelmilch. *Taking the Fear Out of Data Analysis: A Step-by-step Approach*. Dryden Press, 1997.
- [59] D. Dolev and A.C. Yao. On the security of public key protocols. *IEEE Transactions on Information Theory*, 29(2):198–208, 1983.
- [60] J.S. Downs, M.B. Holbrook, and L.F. Cranor. Decision strategies and susceptibility to phishing. Technical report, Carnegie Mellon University, Institute for Software Research, Pittsburgh, PA, USA, January 2006.
- [61] J.S. Downs, M.B. Holbrook, and L.F. Cranor. Behavioral response to phishing risk. In *APWG eCrime Researchers Summit*, Pittsburgh, PA, USA, October 2007.
- [62] eBay. Recognizing spoof (fake) eBay websites, 2017. <http://pages.ebay.com/help/account/recognizing-spoof.html>, Accessed December 2017.
- [63] W.K. Edwards, E.S. Poole, and J Stoll. Security automation considered harmful? In *IEEE New Security Paradigms Workshop (NSPW 2007)*, White Mountain, New Hampshire, September 2007.
- [64] S. Egelman. *Trust Me: Design Patterns for Constructing Trustworthy Trust Indicators*. PhD thesis, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA 15213, April 2009.
- [65] S. Egelman, R. Dhamija, and J. Hong. You have been warned: An empirical study of the effectiveness of web browser phishing warnings. In *CHI Conference on Human Factors in Computing Systems, CHI 2008*, Florence, Italy, April 2008. ACM.

- [66] R.S. El-din. To deceive or not to deceive! Ethical questions in phishing research. In *BCS HCI 2012 Workshops: HCI Research in Sensitive Contexts: Ethical Considerations*, Birmingham, UK, September 2012.
- [67] C. Ellison. UPnP security ceremonies design document. Technical report, UPnP Forum, October 2003.
- [68] C. Ellison. Ceremony design and analysis. Technical Report 2007/399, Cryptology ePrint Archive, 2007.
- [69] A. Emigh. Online identity theft: Phishing technology, chokepoints and countermeasures. Technical report, Radix Labs, October 2005.
- [70] European Union Agency for Network and Information Security. Phishing on the rise, October 2017. <https://www.enisa.europa.eu/publications/info-notes/phishing-on-the-rise>, Accessed December 2017.
- [71] W.P.Jr. Eveland, D.V. Shah, and N. Kwak. Assessing causality in the cognitive mediation model. *Communication Research*, 30(4):359–386, 2003.
- [72] K. Everitt, T. Bragin, J. Fogarty, and T. Kohno. A global look at authentication. In *ACM Conference on Human Factors in Computing Systems (CHI)*. ACM, April 2009.
- [73] FDIC. Putting an end to account-hijacking identity theft. Technical report, Federal Deposit Insurance Corporation (FDIC), Division of Supervision and Consumer Protection, Technology Supervision Branch, December 2004.
- [74] E.W. Felten, D. Balfanz, D. Dean, and D.S. Wallach. Web spoofing: An internet con game. Technical report, Department of Computer Science, Princeton University, February 1997. Available at: <http://sip.cs.princeton.edu/pub/spoofing.pdf>.

- [75] A.J. Ferguson. Fostering e-mail security awareness: The West Point Car-ronade. *EDUCASE Quarterly*, (1), 2005.
- [76] A. Ferreira, J.-L. Huynen, V. Koenig, and G. Lenzini. A conceptual framework to study socio-technical security. Crete, Greece, June 2014. Springer.
- [77] I. Fette, N. Sadeh, and A. Tomasic. Learning to detect phishing emails. In *Proceedings of the 16th International Conference on World Wide Web, WWW '07*, pages 649–656, New York, NY, USA, 2007. ACM.
- [78] S. Fiegerman. Yahoo says 500 million accounts stolen, September 2016. <http://money.cnn.com/2016/09/22/technology/yahoo-data-breach/>, Accessed December 2017.
- [79] Financial Fraud Action UK Ltd. Fraud the facts 2016, 2016. <https://www.financialfraudaction.org.uk/wp-content/uploads/2016/07/Fraud-the-Facts-A5-final.pdf>, Accessed September 2017.
- [80] P. Finn and M. Jakobsson. Designing and conducting phishing experiments. In *In IEEE Technology and Society Magazine, Special Issue on Usability and Security*. IEEE, 2007.
- [81] D. Florêncio and C. Herley. Where do security policies come from? In *The 6th Symposium on Usable Privacy and Security, SOUPS '10*, Redmond, WA, USA, July 2010.
- [82] D. Florêncio, C. Herley, and P.C. Van Oorschot. Password portfolios and the finite-effort user: Sustainably managing large numbers of accounts. In *Proceedings of the 23rd USENIX Conference on Security Symposium, SEC'14*, pages 575–590, Berkeley, CA, USA, 2014. USENIX Association.

- [83] A. Forget. *A World With Many Authentication Schemes*. PhD thesis, Carleton University, Ottawa, Ontario, November 2012.
- [84] The Federal Trade Commission (FTC). Consumer information, phishing, July 2017. <https://www.consumer.ftc.gov/articles/0003-phishing>, Accessed December 2017.
- [85] S. Furnell and L. Zekri. Replacing passwords: in search of the secret remedy. *Network Security*, January 2006.
- [86] S. Gajek, M. Manulis, A.R. Sadeghi, and J. Schwenk. Provably secure browser-based user-aware mutual authentication over TLS. In *ACM Symposium on Information, Computer and Communications Security (ASIACCS'08)*, pages 300–311, Tokyo, Japan, March 2008. ACM.
- [87] S. Gajek, M. Manulis, and J. Schwenk. User-aware provably secure protocols for browser-based mutual authentication. *International Journal of Applied Cryptography (IJACT)*, 1(4):290–308, 2009.
- [88] M. Gibson, K. Renaud, M. Conrad, and C. Maple. Musipass: Authenticating me softly with "My" song. In *Proceedings of the 2009 Workshop on New Security Paradigms Workshop, NSPW '09*, pages 85–100, New York, NY, USA, 2009. ACM.
- [89] P. Godfrey-Smith. *Theory and reality: an introduction to the philosophy of science*. Science and its conceptual foundations. The University of Chicago Press, 2003.
- [90] Google. Google 2-step verification. <http://www.google.com/landing/2step>, Accessed December 2017.
- [91] Google. Google safe browsing. <https://developers.google.com/safe-browsing/>, Accessed December 2017.

- [92] Google. Stronger security for your Google account, 2013. <http://www.google.com/landing/2step>, Accessed April 2013.
- [93] S. Grazioli. Where did they go wrong? An analysis of the failure of knowledgeable internet consumers to detect deception over the internet. 13:149–172, March 2004.
- [94] S. Grazioli and S. L. Jarvenpaa. Perils of internet fraud: An empirical investigation of deception and trust with experienced internet consumers. *Trans. Sys. Man Cyber. Part A*, 30(4):395–410, July 2000.
- [95] S. Grazioli and A. Wang. Looking without seeing: Understanding unsophisticated consumers’ success and failure to detect internet deception. In *ICIS*, pages 193–204. Association for Information Systems, 2001.
- [96] Guardian. Hacker advertises details of 117 million LinkedIn users on darknet, May 2016. <https://www.theguardian.com/technology/2016/may/18/hacker-advertises-details-of-117-million-linkedin-users-on-darknet>, Accessed December 2017.
- [97] R. Hackett. Everyone is falling for this frighteningly effective gmail scam, January 2017. Accessed December 2017.
- [98] J. Hair, R. Anderson, B. Black, and B. Babin. *Multivariate Data Analysis*. Pearson Education, 2016.
- [99] J. Hamada. Phishing: The easy way to compromise Twitter accounts, February 2013. Symantec Official Blog, Accessed December 2017.
- [100] B. Harrison, E. Svetieva, and A. Vishwanath. Individual processing of phishing emails: How attention and elaboration protect against phishing. *Online Information Review*, 40(2):265–281, 2016.

- [101] M. Hart, C. Castille, M. Harpalani, J. Toohill, and R. Johnson. PhorceField: A phish-proof password ceremony. In *The 27th Annual Computer Security Applications Conference (ACSAC 2011)*, Orlando, Florida, USA, December 2011.
- [102] W.K. Haskins. California passes nation’s first antiphishing law, 2005. Accessed October 2007.
- [103] E. Hatunic-Webster. Anti-phishing models: Main challenges. In *Proceedings of the 3rd International Conference on Internet Technology and Secured Transactions (ICITST-2008)*, pages 91–95, Dublin, Ireland, June 2008.
- [104] E. Hatunic-Webster, F. Mtenzi, and B. O’Shea. Password-based authentication and phishing (Extended Abstract). Dublin, Ireland, March 2011. APWG eCrime Researchers Sync-Up. <http://docs.apwg.org/ecrimeresearch/2011syncup/cfp.html>.
- [105] E. Hatunic-Webster, F. Mtenzi, and B. O’Shea. Poster: Towards a Model for Analysing Anti-Phishing Authentication Ceremonies. In *9th Symposium on Usable Privacy and Security (SOUPS)*, Newcastle, UK, July 2013.
- [106] E. Hatunic-Webster, F. Mtenzi, and B. O’Shea. Model for Analysing Anti-Phishing Authentication Ceremonies. In *Proceedings of 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014)*, London, UK, December 2014. IEEE.
- [107] E. Hatunic-Webster, F. Mtenzi, and B. O’Shea. Evaluation of the Model for Analysing Anti-Phishing Authentication Ceremonies. *International Journal for Information Security Research*, 5(1):529–537, 2015.
- [108] C. Herley and D. Florêncio. A profitless endeavor: Phishing as tragedy of the commons. pages 59–70, September 2008.



- [109] C. Herley and P.C. Van Oorschot. A research agenda acknowledging the persistence of passwords. *IEEE Security Privacy*, 10(1):28–36, Jan 2012.
- [110] A. Herzberg and R. Margulies. Forcing Johnny to login safely - long-term user study of forcing and training login mechanisms. In *Computer Security - ESORICS 2011 - 16th European Symposium on Research in Computer Security, Leuven, Belgium, September 12-14, 2011. Proceedings*, pages 452–471, September 2011.
- [111] M. Hlywa, R. Biddle, and S.P. Andrew. Facing the facts about image type in recognition-based graphical passwords. In *Proceedings of the 27th Annual Computer Security Applications Conference, ACSAC '11*, pages 149–158, New York, NY, USA, 2011. ACM.
- [112] M. Hlywa, R. Biddle, and A.S. Patrick. Facing the facts about image type in recognition-based graphical passwords. In *Proceedings of the 27th Annual Computer Security Applications Conference, ACSAC '11*, pages 149–158, New York, NY, USA, 2011. ACM.
- [113] B. Hoanca and K. Mock. A theoretical framework for assessing eavesdropping-resistant authentication interfaces. In *2009 42nd Hawaii International Conference on System Sciences*, pages 1–10, January 2009.
- [114] W.E. Hockley. The picture superiority effect in associative recognition. *Memory and cognition*, 36:1351–9, November 2008.
- [115] J. Hong. The state of phishing attacks. *Communications of the ACM*, 55(1):74–81, January 2012.
- [116] K. Hornbæk. Some whys and hows of experiments in human–computer interaction. *Foundations and Trends in Human Computer Interaction*, 5(4):299–373, Jun 2011.

- [117] IBM. SPSS statistics. <https://www.ibm.com/support/knowledgecenter/en/SSLVMB>.
- [118] C. Jackson, D. Boneh, and M. Mitchell. Spyware resistant web authentication using virtual machines. Technical report, Stanford University, 2006.
- [119] C. Jackson, D.R. Simon, D.S. Tan, and A. Barth. An evaluation of extended validation and picture-in-picture phishing attacks. In *Proceedings of the 11th International Conference on Financial Cryptography and 1st International Conference on Usable Security, FC'07/USEC'07*, pages 281–293, Berlin, Heidelberg, 2007. Springer-Verlag.
- [120] T.N. Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer. Social phishing. *Commun. ACM*, 50(10):94–100, 2007.
- [121] A.K. Jain, A. Ross, and S. Pankanti. Biometrics: A tool for information security. *IEEE Transactions on Information Forensics and Security*, 1(2):125–143, 2006.
- [122] M. Jakobsson. Modeling and preventing phishing attacks. In *Phishing Panel in Financial Cryptography '05*, February 2005.
- [123] M. Jakobsson. The human factor in phishing. In *Privacy and Security of Consumer Information '07*, 2007.
- [124] M. Jakobsson. User trust assessment: a new approach to combat deception. In *Socio-Technical Aspects in Security and Trust (STAST '16)*, Los Angeles, CA, USA, December 2016. ACM.
- [125] M. Jakobsson, N. Johnson, and P. Finn. Why and how to perform fraud experiments. *IEEE Security and Privacy*, 6(2):66–68, 2008.
- [126] M. Jakobsson and S. Myers. *Phishing and Countermeasures: Understanding*

- the Increasing Problem of Electronic Identity Theft*. John Willey and Sons, Inc., 2007.
- [127] M. Jakobsson and S. Myers. Delayed Password Disclosure. *Int. J. Applied Cryptography*, 1(1):47–59, 2008.
- [128] M. Jakobsson and Z. Ramzan. *Crimeware: Understanding New Attacks and Defenses*. Symantec Press. Pearson Education, 2008.
- [129] M. Jakobsson and J. Ratkiewicz. Designing ethical phishing experiments: A study of (ROT13) rOnl query features. In *Proceedings of the 15th International Conference on World Wide Web, WWW '06*, pages 513–522, New York, NY, USA, 2006. ACM.
- [130] I. Jermyn, A. Mayer, F. Monroe, M.K. Reiter, and A.D. Rubin. The design and analysis of graphical passwords. In *8th USENIX Security Symposium*, Washington, DC, USA, August 1999.
- [131] P.E. Johnson, S. Grazioli, K. Jamal, and R.G. Berryman. Detecting deception: adversarial problem solving in a low base-rate world. *Cognitive Science*, 25(3):355–392, 2001.
- [132] P.E. Johnson, S. Grazioli, K. Jamal, and I.A. Zualkernan. Success and failure in expert reasoning. *Organizational Behavior and Human Decision Processes*, 53(2):173–203, 1992.
- [133] M. Just and D. Aspinall. Personal choice and challenge questions: A security and usability assessment. In *Symposium on Usable Privacy and Security (SOUPS)*, Mountain View, CA USA, July 2009.
- [134] R. Kainda. *Usability and Security of Human-Interactive Security Protocols*. PhD thesis, St. Cross College, University of Oxford, Trinity Term 2011.

- [135] C. Karlof, J.D. Tygar, and D. Wagner. Conditioned-safe ceremonies and a user study of an application to web authentication. In *The 5th Symposium on Usable Privacy and Security, SOUPS '09*, Mountain View, CA, USA, July 2009.
- [136] C.K. Karlof. *Human Factors in Web Authentication*. PhD thesis, Electrical Engineering and Computer Sciences, University of California, Berkeley, February 2009.
- [137] A. Kiayias, T. Zacharias, and B. Zhang. Ceremonies for end-to-end verifiable elections. In *Proceedings, Part II, 20th IACR International Conference on Public-Key Cryptography — PKC 2017*, pages 305–334, New York, NY, USA, 2017. Springer-Verlag New York, Inc.
- [138] H. Krawczyk, K.G. Paterson, and H. Wee. On the security of the TLS protocol: A systematic analysis. In *Advances in Cryptology – CRYPTO 2013*, pages 429–448, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.
- [139] M. Kumar, T. Garfinkel, D. Boneh, and T. Winograd. Reducing shoulder-surfing by using gaze-based password entry. In *Proceedings of the 3rd Symposium on Usable Privacy and Security, SOUPS '07*, pages 13–19, New York, NY, USA, 2007. ACM.
- [140] P. Kumaraguru, J. Cranshaw, A. Acquisti, L.F. Cranor, J. Hong, M.A. Blair, and T. Pham. School of phish: A real-world evaluation of anti-phishing training. In *Proceedings of the 5th Symposium on Usable Privacy and Security, SOUPS '09*, pages 3:1–3:12, New York, NY, USA, 2009. ACM.
- [141] P. Kumaraguru, S. Sheng, A. Acquisti, L. F. Cranor, and J. Hong. Teaching Johnny not to fall for phish. *ACM Trans. Internet Technol.*, 10(2):7:1–7:31, Jun 2010.

- [142] Laerd Statistics. Statistical tutorials and software guides., 2015. <https://statistics.laerd.com/>.
- [143] J. Lance. *Phishing Exposed*. SYNGRESS, 2005.
- [144] J. Lee and L. Bauer. Studying the effectiveness of security images in Internet banking. In *Web 2.0 Security and Privacy (W2SP) Workshop*, May 2014.
- [145] R. Lininger and R.D. Vines. *Phishing: Cutting the Identity Theft Line*. Wiley Publishing, Inc., 2005.
- [146] McAfee LLC. Protect yourself from SMiShing, February 2012. Accessed December 2017.
- [147] MAAWG and APWG. Anti-phishing best practices for ISPs and mailbox providers. Technical report, Messaging Anti-Abuse Working Group (MAAWG), Anti-phishing Working Group (APWG), July 2006.
- [148] M. Mannan and P.C. van Oorschot. Digital objects as passwords. In *3rd USENIX Workshop on Hot Topics in Security*, San Jose, CA, USA, July 2008.
- [149] Z. Martin. BofA, Chase adding authentication mechanisms, June 2015. <https://www.secureidnews.com/news-item/bofa-chase-adding-authentication-mechanisms>, Accessed January 2018.
- [150] J.E. Martina and M.C. Carlos. Why should we analyse security ceremonies? In *Applications of Logic in Computer Security. The 15th International Conference on Logic for Programming, Artificial Intelligence and Reasoning*, 2008.
- [151] J.E. Martina, T.C.S. de Souza, and R.F Custodio. Ceremonies design for PKI's hardware security modules. In *SBSEG 2009:9th Brazilian Symposium on Information and Computer System Security (2009)*, Campinas, Sao Paulo, Brazil, September 2009.

- [152] J.E. Martina, T.C.S. de Souza, and R.F Custodio. Ceremonies formal analysis in PKI's context. In *PASSAT 2009: The 2009 IEEE International Conference on Information Privacy, Security, Risk and Trust*, Vancouver, Canada, August 2009.
- [153] C.P. Masone. *Attribute-Based, Usefully Secure Email*. PhD thesis, Dartmouth College, Hanover, New Hampshire, August 2008.
- [154] L. Mathews. Phishing scams cost american businesses half a billion dollars a year, May 2017. <https://www.forbes.com/sites/leemathews/2017/05/05/phishing-scams-cost-american-businesses-half-a-billion-dollars-a-year>, Accessed January 2018.
- [155] M. Maunder. Wide impact: Highly effective gmail phishing technique being exploited, January 2017. <https://www.wordfence.com/blog/2017/01/gmail-phishing-data-uri>, Accessed December 2017.
- [156] D.K. McGrath, A. Kalafut, and M. Gupta. Phishing infrastructure fluxes all the way. *IEEE Security Privacy*, 7(5):21–28, Sept 2009.
- [157] G.A. Miller. The magical number seven, plus or minus two: Some limits on our capacity for processing information. *Psychological Review*, 63(2):81–97, 1956.
- [158] Mobile-OTP Project. Mobile one time passwords: Mobile-OTP, 2013. <http://motp.sourceforge.net>, Accessed April 2013.
- [159] T. Moore and R. Clayton. Examining the impact of website take-down on phishing. In *APWG eCrime Researchers Summit*, Pittsburgh, PA, USA, October 2007.

- [160] I. Naor. Facebook phishing attacks claim 10,000 victims in two days, December 2017. <http://www.informationsecuritybuzz.com/articles/facebook-phishing-attacks-claim-10000-victims-in-two-days/>, Accessed 31 December 2017.
- [161] National Consumers League. A call for action: Report from the national consumers league anti-phishing retreat. Technical report, National Consumers League, Washington, DC, March 2006.
- [162] R.M. Needham and M.D. Schroeder. Using encryption for authentication in large networks of computers. *Communications of ACM*, 21(12):993–999, 1978.
- [163] D.L. Nelson, V.S. Reed, and J.R. Walling. Pictorial superiority effect. *Journal of experimental psychology. Human learning and memory*, 2:523–8, October 1976.
- [164] R. Nickerson. Confirmation bias: A ubiquitous phenomenon in many guises. 2:175–220, June 1998.
- [165] D.A. Norman. *The Design of Everyday Things*. Basic Books, Inc., New York, NY, USA, 2002.
- [166] J.C. Nunnally. *Psychometric theory*. McGraw-Hill series in psychology. McGraw-Hill, 1978.
- [167] L. O’Gorman. Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE*, 91(12):2021–2040, Dec 2003.
- [168] E. Ostrom. Institutional rational choice: An assessment of the institutional analysis and development framework. In *Theories of the Policy Process*, pages 21–64. Sabatier, P.A. (Ed.), Westview Press, 2007.
- [169] OUT-LAW.COM. Prison terms for phishing fraudsters, November 2006. Accessed October 2007.

- [170] A. Paivio. *Imagery and verbal processes*. Hillsdale, N.J.: Lawrence Erlbaum Associates, 1979.
- [171] A. Paivio, T. B. Rogers, and P. C. Smythe. Why are pictures easier to recall than words? *Psychonomic Science*, 11(4):137–138, Apr 1968.
- [172] B. Parno, C. Kuo, and A. Perrig. Phoolproof phishing prevention. In *Financial Cryptography and Data Security, 10th International Conference, FC 2006, Anguilla, British West Indies, February 27-March 2, 2006, Revised Selected Papers*, pages 1–19, 2006.
- [173] Passfaces Corporation. Passfaces: Two factor authentication for the enterprise, 2017. <http://www.passfaces.com>, Accessed September 2017.
- [174] Passfaces Corporation. The science behind Passfaces, 2017. <http://www.passfaces.com>, Accessed August 2017.
- [175] Passfaces Corporation. Welcome to the Passfaces demonstration, 2017. <http://www.passfaces.com/demo>, Accessed August 2017.
- [176] K.G. Paterson and D. Stebila. One-time-password-authenticated key exchange. In *1th Australasian Conference on Information Security and Privacy (ACISP)*, volume 6168. Springer, 2010.
- [177] E. Perse. Audience selectivity and involvement in the newer media environment. 17:675–697, October 1990.
- [178] R. Petty and J. Cacioppo. The elaboration likelihood model of persuasion. 19:123–205, December 1986.
- [179] PhishTank. PhishTank. <http://www.phishtank.com/>, Accessed December 2017.



- [180] PNC Inc. An added layer of security, 2018. <https://www.pnc.com/en/security-privacy/added-layer-security.html>, Accessed January 2018.
- [181] PNC Inc. Online and mobile banking, 2018. <https://www.pnc.com/en/customer-service/update-center/sign-on-changes.html>, Accessed January 2018.
- [182] K. Radke. *Security Ceremonies Including Humans in Cryptographic Protocols*. PhD thesis, Science and Engineering Faculty Queensland University of Technology, October 2013.
- [183] K. Radke, C. Boyd, J.G. Nieto, and M. Brereton. Ceremony analysis: Strengths and weaknesses. In *The 26th IFIP TC-11 International Information Security Conference (IFIP SEC2011)*, Lucerne, Switzerland, June 2011.
- [184] K. Radke, C. Boyd, J.G. Nieto, and M. Brereton. Towards a secure human-and-computer mutual authentication protocol. In *Australasian Information Security Conference (AISC) 2012*, RMIT University, Melbourne, Australia, 30 Jan - 3 Feb 2012.
- [185] K. Radke, C. Boyd, J.G. Nieto, M. Manulis, and D. Stebila. Formalising human recognition: a fundamental building block for security proofs. In *Australasian Information Security Conference (ACSW-AISC 2014)*, Auckland, New Zealand, January 2014.
- [186] J. Reason. *Human Error*. Cambridge University Press, 1990.
- [187] Revenue Irish Tax and Customs. Warning: Latest email and SMS (text message) scam, 2018. <https://www.revenue.ie/en/news/articles/email-scam.aspx>, Accessed January 2018.
- [188] K. Richards, R. LaSalle, M. Devost, F. van den Dool, and J. Kennedy-White.

- Cost of cybercrime study. Report, Ponemon Institute LLC and Accenture, 2017.
- [189] RSA Security. Protecting against phishing by implementing strong two-factor authentication. Technical report, RSA Security, 2004.
- [190] R. Rukšėnas, P. Curzon, and A. Blandford. Detecting cognitive causes of confidentiality leaks. *Electronic Notes in Theoretical Computer Science*, 183(183):21–38, 2007.
- [191] J. Saltzer and M. M. Schroeder. The protection of information in computer systems. *Proceedings of the IEEE*, 63(9):1278–1308, September 1975.
- [192] Santander UK plc. Santander online banking - choose your image and phrase to help you log on securely, 2017. <http://www.santander.co.uk/info/videohub/helping-you-understand-online-banking/santander-online-banking-choose-your-image-and-phrase-to-help-you-log-on-securely/xegmgk2wJOE>, Accessed September 2017.
- [193] M. A. Sasse, S. Brostoff, and D. Weirich. Transforming the 'Weakest Link': a human-computer interaction approach to usable and effective security. *BT Technology Journal*, 19(3):122–131, July 2001.
- [194] S.E. Schechter, R. Dhamija, A. Ozment, and I. Fischer. The emperor's new security indicators: An evaluation of website authentication and the effect of role playing on usability studies. In *The 2007 IEEE Symposium on Security and Privacy*, Oakland, California, May 2007.
- [195] E. Schlager. A comparison of frameworks, theories, and models of policy processes. In *Theories of the Policy Process*, pages 293–319. Sabatier, P.A. (Ed.), Westview Press, 2007.

- [196] B. Schneier. On the Equifax data breach, September 2017. <https://www.schneier.com/blog/archives/2017/09>, Accessed December 2017.
- [197] F. Shaub, M. Walch, B. Knings, and M. Weber. Exploring the design space of graphical passwords on smartphones. In *Symposium on Usable Privacy and Security (SOUPS)*, Newcastle, UK, July 2013.
- [198] S. Sheng, M. Holbrook, P. Kumaraguru, L.F. Cranor, and J. Downs. Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI '10*, pages 373–382, New York, NY, USA, 2010. ACM.
- [199] S. Sheng, B. Magnien, P. Kumaraguru, A. Acquisti, L.F. Cranor, J. Hong, and E. Nunge. Anti-Phishing Phil: The design and evaluation of a game that teaches people not to fall for phish. In *Proceedings of the 3rd Symposium on Usable Privacy and Security, SOUPS '07*, pages 88–99, New York, NY, USA, 2007. ACM.
- [200] Sophos Ltd. Phishing in a world of Warcraft, January 2011. <https://nakedsecurity.sophos.com/2011/01/20/phishing-in-a-world-of-warcraft/>, Accessed 31 December 2017.
- [201] I. Staedman. 'Serious weaknesses' found in security protocol for web banking, Facebook, February 2013. <http://www.wired.co.uk/article/weakness-in-tsl-protocol>.
- [202] F. Stajano and P. Wilson. Understanding scam victims: seven principles for systems security. 54:70–75, January 2011.

- [203] S. Stamm, Z. Ramzan, and M. Jakobsson. Drive-by pharming. In *Information and Communications Security: 9th International Conference, ICICS 2007*, pages 495–506, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg.
- [204] E. Stobert. *Graphical Passwords and Practical Password Management*. PhD thesis, Carleton University, Ottawa, Ontario, Canada, 2015.
- [205] E. Stobert and R. Biddle. Memory retrieval and graphical passwords. In *Symposium on Usable Privacy and Security (SOUPS)*, Newcastle, UK, July 2013.
- [206] Symantec Corporation. Security 1:1 - Part 3 - various types of network attacks, December 2013. <https://www.symantec.com/connect/blogs/beware-vishers>, Accessed December 2017.
- [207] Symantec Corporation. 2016 Internet Security Threat Report. Technical report, Symantec Corporation, April 2016.
- [208] C.H. Tan and J.C.M. Teo. Protection against web-based password phishing. In *International Conference on Information Technology (ITNG'07)*. IEEE Computer Society, 2007.
- [209] H. Tao and C. Adams. PassGo: A proposal to improve the usability of graphical passwords. 7(2):273–292, September 2008.
- [210] M. Tavakol and R. Dennick. Making sense of Cronbach’s alpha. *International Journal of Medical Education*, 2:53–55, 2011.
- [211] C. Teddlie and F. Yu. Mixed methods sampling: A typology with examples. 1:77–100, 01 2007.
- [212] UK Office of Public Sector Information. The privacy and electronic commu-

- nications (EC Directive) Regulations 2003. Technical Report 2003 No. 2426, 2003. Accessed October 2007.
- [213] M. Urban. The evolution of phishing. *ISSA Journal*, pages 1–53, September 2006.
- [214] US-CERT. Avoiding social engineering and phishing attacks, January 2017. <https://www.us-cert.gov/ncas/tips/ST04-014>, Accessed December 2017.
- [215] U.S. Copyright Office. The digital millennium copyright act of 1998: U.S. copyright office summary. Technical report, 1998. Accessed October 2007.
- [216] P.C. van Oorschot and T. Wan. TwoStep: An authentication method combining text and graphical passwords. In *4th MCETECH Conference on eTechnologies*, May 2009.
- [217] A. Vishwanath, T. Herath, R. Chen, J. Wang, and H.R. Rao. Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems*, 51:576–586, 2011.
- [218] J. Wang, H. Tejaswini, R. Chen, A. Vishwanath, and H.R. Rao. Phishing susceptibility: An investigation into the processing of a targeted spear phishing email. *IEEE Transactions on Professional Communication*, 55(4):345–362, 2012.
- [219] D. Weirich and M.A. Sasse. Pretty good persuasion: A first step towards effective password security in the real world. In *Proceedings of the 2001 Workshop on New Security Paradigms*, NSPW '01, pages 137–143, New York, NY, USA, 2001. ACM.
- [220] L. Wenyin, G. Huang, L. Xiaoyue, Z. Min, and X. Deng. Detection of phishing

- webpages based on visual similarity. In *14th international conference on World Wide Web*, Chiba, Japan, May 2005.
- [221] A. Whitten and J. Tygar. Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In *8th USENIX Security Symposium*, Washington, D.C., USA, August 1999.
- [222] M.S. Wogalter. *Communication-Human Information Processing (C-HIP) Model*. Lawrence Erlbaum Associates, 2006. In *Handbook of Warnings*, Edited by Michael S. Wogalter.
- [223] M. Workman. A test of interventions for security threats from social engineering. *Information Management & Computer Security*, 16(5):463–483, 2008.
- [224] M. Workman. Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *J. Am. Soc. Inf. Sci. Technol.*, 59(4):662–674, February 2008.
- [225] M. Wu. *Fighting Phishing at the User Interface*. PhD thesis, Massachusetts Institute of Technology, August 2006.
- [226] M. Wu, R.C. Miller, and S.L. Garfinkel. Do security toolbars actually prevent phishing attacks? In *CHI*, Montreal, Quabec, Canada, April 2006. ACM.
- [227] T. Wu. The Secure Remote Password protocol. In *Proceedings of the 1998 Internet Society Network and Distributed System Security Symposium*, pages 97–111, 1998.
- [228] Yahoo! Give password scams the boot with personalized Sign-in Seals., 2013. Accessed April 2013.
- [229] Yahoo! Yahoo! UK and Ireland, 2014. Accessed June 2014.

- [230] Yahoo! Security Center. What is a Sign-in Seal?, 2010. <http://security.yahoo.com/article.html?aid=2006102507>, Accessed December 2010.
- [231] E.Z. Ye, Y. Yuan, and S. Smith. Web spoofing revisited: SSL and beyond. Technical Report TR2002-417, Department of Computer Science, Dartmouth College, February 2002.
- [232] Z.E. Ye, S. Smith, and D. Anthony. Trusted paths for browsers. *ACM Transactions on Information and System Security (TISSEC)*, 8(2):153–186, May 2005.
- [233] K-P. Yee. Aligning security and usability. *IEEE Security and Privacy*, 2(5):48–55, September 2004.
- [234] J. Youll. Fraud vulnerabilities in SiteKey security at Bank of America. July 2006.
- [235] J. L. Zaichkowsky. Measuring the involvement construct. *Journal of Consumer Research*, 12(3):341–352, 1985.
- [236] Y. Zhang, S. Egelman, L.F. Cranor, and J. Hong. Phinding phish: Evaluating anti-phishing tools. In *14th Annual Network and Distributed System Security Symposium*, volume 2007, San Diego, CA, February/March 2007.

# Appendix A

## User Study Materials

This appendix contains the materials used for the user study described in Chapter 7:

1. Emails sent to recruit participants.
2. Notice for bulletin boards to recruit participants.
3. Study information sheets given to participants to read before signing the consent form.
4. Consent form given to participants to read and sign.
5. Screenshots of the user study main web page - allowing users to complete all tasks of the study.
6. Post Study and Demographic questionnaires.



Subject: User Study - Web Authentication Schemes

Dear \_\_\_\_\_,

My name is Edina Hatunic-Webster and I am currently undertaking research towards a PhD with the School of Computing in Dublin Institute of Technology. I am a lecturer in Computer Science in DIT.

I am conducting a user study on security usability of web authentication schemes that use security images as part of the login process.

The goal is to determine how easy and secure it is for people to use these schemes.

I am inviting volunteers to take part in the study. Participants should be able to browse the web and use websites that require a username and password to gain access.

All information submitted as part of this study will be used only for this research project. At no point will any individual respondent be identified by name. You will not be required to use your own username or passwords for the study.

A number of prizes will be awarded to randomly selected participants that complete the study.

The study should take around 35-40 minutes to complete.

The study will primarily take place at a DIT Kevin Street laboratory during April and May 2016.

If you are willing to participate in this project, please contact me at:

Edina.Hatunic-Webster@dit.ie or (01) 4024696

Kind Regards

Figure A.1: Emails sent to recruit participants

## USABILITY STUDY

- We are conducting a user study on security usability of web authentication schemes that use images as part of the login process.
- We are inviting volunteers to take part in the study.
- It should take around 35-40 minutes to complete.
- If you are willing to participate, please contact me at:
  - [Edina.Hatunic-Webster@dit.ie](mailto:Edina.Hatunic-Webster@dit.ie) , or
  - “mobile num x”

**Note: A number of small prizes will be awarded to randomly selected participants**

Figure A.2: Notice for bulletin boards to recruit participants

## **Information Sheet 1: Security Usability Study of Web Authentication Schemes**

Thank you for expressing an interest in participating in research I am undertaking towards a postgraduate qualification with the School of Computing in Dublin Institute of Technology. I am a lecturer in the School of Computing in Dublin Institute of Technology. This research is being undertaken as part of my role as a student.

Please read this information carefully before signing the Consent Form.

This user study is anonymous. Do not submit your name or other identifying information during the study.

If you are a DIT student: This experiment is NOT a requirement of your class and is entirely voluntary.

### *Study Purpose*

The purpose of this user study is to evaluate the security usability of three web login schemes. We are trying to determine how easy and secure it is for people to use these schemes. We will compare login schemes regarding their impact on the user's ability to distinguish between legitimate and altered website login pages.

### *Task Requirements*

We will ask you to complete a series of tasks that involve web login procedures, e.g., entering your username and text-based and graphical passwords; and entering a simple set of data. We will ask that you fill out short questionnaires, and at the conclusion of the user study session you will be asked to provide us with any suggestions you might have to improve the software.

### *Duration and Locale*

The study session should take less than 1 hour. The study will primarily take place at a DIT Kevin Street laboratory. A number of small prizes will be awarded to randomly selected participants providing you accomplish all required tasks in the study.

### *Potential Risk/Discomfort*

There will be no psychological or physical risk.

### *Anonymity/Confidentiality*

All data that is collected will be held completely confidential. Data will be coded for identification purposes. You will not be required to use your own accounts or passwords for the study.

### *Right to Withdraw*

You have the right to withdraw at any time, without any explanation as to the reason for withdrawing from the study.

If you have any further questions, please contact me on:

(01) 402 4696 or [edina.hatsunic-webster@dit.ie](mailto:edina.hatsunic-webster@dit.ie)

Figure A.3: User Study Information Sheet 1

## Information Sheet 2: Tasks Details

### Security Usability Study of Web Authentication Schemes

#### *Website Tasks*

This first stage of the experiment requires that you register for the UserStudy website. To be able to register you will be given a **Username** and **Email** address. The Email address is not real.

After that you will be required to log into the Study Website page **multiple** times and post a **short** comment on the topic of the page. The comments are **private**, i.e. visible only to you and the Researcher. The content of the comment is NOT important.

You need to post at least **one comment** on each page. In the **1st line** of each comment you should enter the Anonymous Identification Number (AIN) that you will be given. The number will then be put into the **raffle** for the prizes. You will need your username to claim the prize.

#### *Surveys*

You will then be asked to complete two short surveys.

The Post Study Survey will ask questions related to the authentication scheme used in the User Study Website.

The Demographics survey will ask questions about your demographics and your computer usage habits.

To be able to do surveys you will be given a **Survey Username** and **Survey Password**.

#### *If you are willing to proceed*

1. Sign the Consent Form
2. You will then be given: Website Username, Email address, Anonymous Identification Number (AIN), Survey Username and Survey Password
3. Go to the following URL: <http://ehwa.nightsky.ie/userstudy/>  
Follow the step by step instruction on this webpage. This is your main UsabilityStudy page to go back to during the study.

If you have any issues, contact me, Edina Hatunic-Webster, on:

'mobile num' or aacerlab.help@gmail.com

Figure A.4: User Study Information Sheet 2

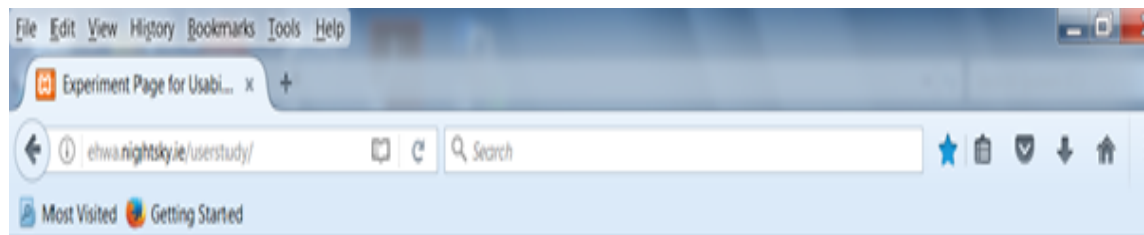
## CONSENT FORM

<b>Researcher's Name:</b> EDINA HATUNIC-WEBSTER	<b>Title:</b> MS.
<b>Faculty/School/Department:</b> SCHOOL OF COMPUTING, COLLEGE OF SCIENCES AND HEALTH, DUBLIN INSTITUTE OF TECHNOLOGY	
<b>Title of Study:</b> SECURITY USABILITY STUDY OF WEB AUTHENTICATION SCHEMES	
3.1 Have you been fully informed/read the information sheet about this study?	YES/NO
3.2 Have you had an opportunity to ask questions and discuss this study?	YES/NO
3.3. Have you received satisfactory answers to all your questions?	YES/NO
3.4 Have you received enough information about this study and any associated health and safety implications if applicable?	YES/NO
3.5 Do you understand that you are free to withdraw from this study?	
<ul style="list-style-type: none"> <li>• at any time</li> <li>• without giving a reason for withdrawing</li> <li>• without affecting your future relationship with the Institute</li> </ul>	YES/NO
3.6 Do you agree to take part in this study the results of which are likely to be published?	YES/NO
3.7 Have you been informed that this consent form shall be kept in the confidence of the researcher?	YES/NO
Signed _____	Date _____
Name in Block Letters _____	
Signature of Researcher _____	Date _____

**Please note:**

- For persons under 18 years of age the consent of the parents or guardians must be obtained or an explanation given to the Research Ethics Committee and the assent of the child/young person should be obtained to the degree possible dependent on the age of the child/young person. **Please complete the Consent Form (section 4) for Research Involving 'Less Powerful' Subjects or Those Under 18 Yrs.**
- In some studies, witnessed consent may be appropriate.
- The researcher concerned must sign the consent form after having explained the project to the subject and after having answered his/her questions about the project.

Figure A.5: Consent form



Thank you in advance for your participation, and please remember the following:

- This study is anonymous; DO NOT submit your name, or other identifying information.
- This experiment is NOT a requirement of your class and is entirely voluntary.
- A number of small prizes will be awarded to randomly selected participants that complete **All Stages 1-4** of the experiment.

Please proceed to Stage 1 below.

---

### Stage 1: Registering

This first stage of the experiment requires that you register for the User Study website. It should take approximately 5 minutes.

1. You first need to familiarise yourself with the authentication scheme you will need to use. Please read your authentication scheme [Tutorial](#).
  2. [Register](#) for the Ireland: Life and Travel website.
- 

Figure A.6: Study home page

## Stage 2: Website Tasks

This second stage of the experiment should take approximately 20 minutes to complete. The tasks comprise of logging into the **Ireland: Life and Travel** User Study Website page and posting a **short** comment on the topic of the page. The comments are **private**, i.e. visible only to you and the Researcher.

The content of the comment is NOT important. You need to post at least **one comment** on each page. In the **1st line** of each comment you should enter the Anonymous Identification Number that you received. The number will then be put into the **raffle** for the prizes.

**Note:** You must **log out** from the website at the end of each task.

### Tasks:

1. Log in to the [Ireland: Life and Travel](#) website
  - o Click on the **Food** page
  - o Post a comment on Food
  - o **Log out**
  
2. Log in to the [Ireland: Life and Travel](#) website
  - o Click on the **Green Scenery** page
  - o Post a comment on Green Scenery
  - o **Log out**
  
3. Log in to the [Ireland: Life and Travel](#) website
  - o Click on the **Irish Dancing** page
  - o Post a comment on Irish Dancing
  - o **Log out**
  
4. Log in to the [Ireland: Life and Travel](#) website
  - o Click on the **Literature** page
  - o Post a comment on Literature
  - o **Log out**
  
5. Log in to the [Ireland: Life and Travel](#) website
  - o Click on the **Traditional music** page
  - o Post a comment on Traditional music
  - o **Log out**
  
6. Go **back** to the main Usability Study page (<http://ehwa.nightsky.ie/userstudy/>).

Figure A.7: Study page - Website Tasks

### **Stage 3: Take the Post Study survey**

The questionnaire asks questions related to the authentication scheme used in Ireland: Life and Travel website. The survey should take approximately 5 minutes.

Go **back** to the main Usability Study page (<http://ehwa.nightsky.ie/userstudy/>).

Click on the Post Study Survey link.

- [Post Study Survey](#)
- 

### **Stage 4: Take the Demographics survey**

This questionnaire asks questions about your demographics and your computer usage habits. The survey should take approximately 5 minutes.

Go **back** to the main Usability Study page (<http://ehwa.nightsky.ie/userstudy/>).

Click on the Demographics Survey link.

- [Demographics Survey](#)
- 

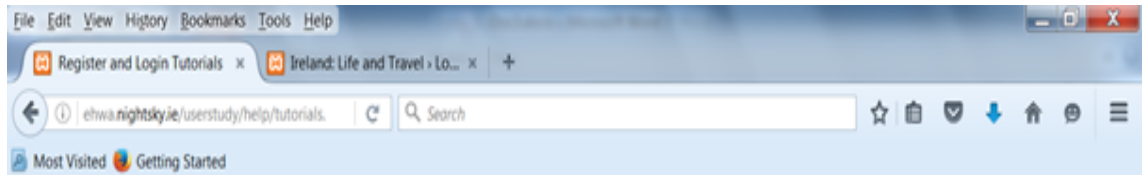
### **Questions or Issues?**

Should you have any questions related to the study, or issues with performing the study, you can email [aacerlab.help@gmail.com](mailto:aacerlab.help@gmail.com).

[Help page](#)

**Figure A.8:** Study page - Survey Tasks





## Usability Study: Help with Registering and Login

If your **username** starts with: 'B' or 'b' then click:

- [Secure Image Help](#)

If your **username** starts with: 'T' or 't' then click:

- [Two Step Authentication Help](#)

If your **username** starts with: 'M' or 'm' then click:

- [Multi Step Authentication Help](#)

Back to [Usability Study](#) page

**Figure A.9:** Help with registering and login screen

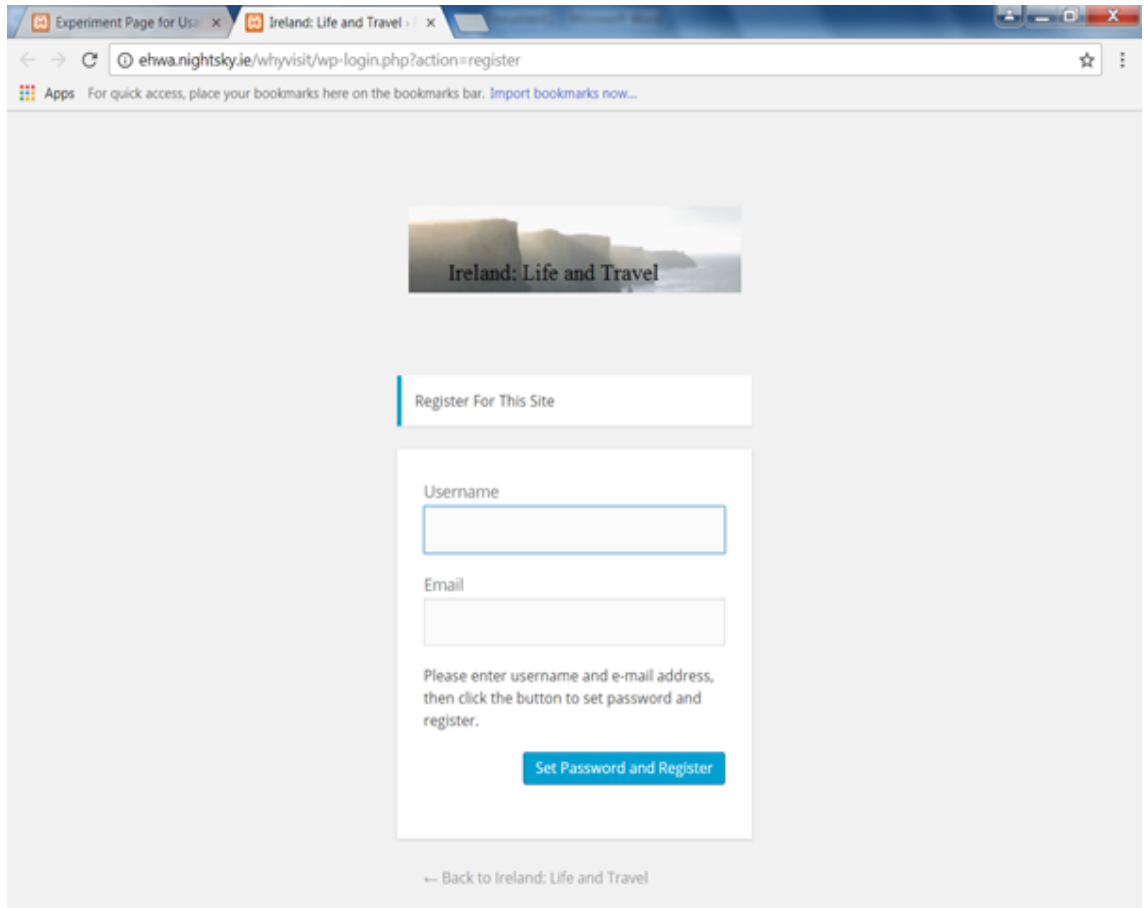


Figure A.10: Registering screen

# User Study Questionnaire

---

## Page 1: Post User Study Questionnaire

The questionnaire asks questions related to the authentication scheme used in **Ireland: Life and Travel** User Study Website (i.e. the User Study Website).

This survey is anonymous. This information will be held completely confidential.

1 The information in the User Study Website was essential.

- Strongly disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Strongly agree

2 The information in the User Study Website was trivial.

- Strongly disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Strongly agree

3 The information in the User Study Website was significant.

- Strongly disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Strongly agree

4 The information in the User Study Website was important.

- Strongly disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Strongly agree

5 The information in the User Study Website was relevant to you.

- Strongly disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Strongly agree

6 The information in the User Study Website was of concern to you.

- Strongly disagree

- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Strongly agree

7 The information in the User Study Website matters to you.

- Strongly disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Strongly agree

## Page 2: Post User Study Questionnaire

8 How would you rate your knowledge about Web security in general?

- Not at all Knowledgeable
- Slightly Knowledgeable
- Moderately Knowledgeable
- Very Knowledgeable
- Extremely Knowledgeable

9 How would you rate your knowledge of the authentication scheme used in the User Study Website?

- Not at all Knowledgeable
- Slightly Knowledgeable
- Moderately Knowledgeable
- Very Knowledgeable
- Extremely Knowledgeable

10 How would you rate you knowledge about Web based scams?

- Not at all Knowledgeable
- Slightly Knowledgeable
- Moderately Knowledgeable
- Very Knowledgeable
- Extremely Knowledgeable

## Page 3: Post User Study Questionnaire

11 After trying to login to the User Study Website you thought about the type of authenticators you previously used for this website.

- Strongly disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Strongly agree

12 After trying to login to the User Study Website you thought about the login page and compared it to your previous login experience

- Strongly disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Strongly agree

13 After trying to login to the User Study Website you thought about the login page 'look and feel' and compared it to your previous login experience

- Strongly disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Strongly agree

14 After trying to login to the User Study Website you thought about the security of your passwords.

- Strongly disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Strongly agree

15 After trying to login to the User Study Website you thought about whether the website was secure.

- Strongly disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Strongly agree



# Usability Study: Demographics

---

## Page 1: Participant Profile

This questionnaire asks questions about your demographics and your computer usage habits. The survey is anonymous. This information will be held completely confidential.

1 What is your gender?

- Female
- Male

2 What is your age group?

- 18-25
- 26-35
- 36-45
- 46-55
- 56-65
- 66+

3 Please choose one of the following:

- Undergraduate student

- Masters student
- PhD student
- Trade school or apprenticeship student
- Other

3.a If you selected Other, please specify:

4 What is your highest level of completed education:

- Secondary school
- Undergraduate degree
- Apprenticeship
- Masters
- PhD
- Other

4.a If you selected Other, please specify:

5 Please identify your area

- Art
- Business
- Computer Science
- Engineering

- Languages
- Mathematics
- Music
- Science
- Social Science
- Other

5.a If you selected Other, please specify:

6 What operating system do you primarily use?

- Windows
- Linux
- Mac OS
- Other

6.a If you selected Other, please specify:

## Page 2: Page 2: Participant Information

7 What Web browser do you primarily use?

- Internet Explorer
- Firefox
- Chrome
- Safari
- Opera
- Other

7.a If you selected Other, please specify:

8 How many hours a week do you use a Web browser?

- 0-5
- 6-10
- 11-20
- 20+

9 Approximately, how many online accounts that require a username and password do you have in total? E.g.: for Emails, Forums, Social networks, School, Gaming, Pictures, Cloud storage, Banks.

- 0-5
- 6-10
- 10+