2019

A new network model for cyber threat intelligence sharing using blockchain technology

Daire Homan

Ian Shiel

Christina Thorpe

A New Network Model for Cyber Threat Intelligence Sharing Using Blockchain Technology

Daire Homan
Technological University Dublin
Blanchardstown, Ireland
dairehoman@gmail.com

Ian Shiel
Technological University Dublin
Blanchardstown, Ireland
ian.shiel@itb.ie

Christina Thorpe
Technological University Dublin
Blanchardstown, Ireland
christina.thorpe@itb.ie

***Abstract*—The aim of this research is to propose a new blockchain network model that facilitates the secure dissemination of Cyber Threat Intelligence (CTI) data. The primary motivations for this study are based around the recent changes to information security legislation in the European Union and the challenges that Computer Security and Incident Response Teams (CSIRT) face when trying to share actionable and highly sensitive data within systems where participants do not always share the same interests or motivations. We discuss the common problems within the domain of CTI sharing and we propose a new model, that leverages the security properties of blockchain. Our model provides a more effective and efficient framework for a CTI sharing network that has the potential to overcome the trust barriers and data privacy issues inherent in this domain. We implemented a testbed using Hyperledger Fabric and the STIX 2.0 protocol and validated the efficacy of the segmentation, implemented using smart contracts and Fabric channels.**

***Index Terms*—Blockchain, cyber threat intelligence, security, trust, privacy**

I. Introduction

Cyber Threat Intelligence (CTI) sharing [13] involves the dissemination of useful information to other external organisations that could potentially be affected by a security incident. A key driver behind CTI sharing is the Directive on Security of Network and Information Systems (NIS directive), adopted by the EU in 2016, which aims to implement a legal framework where various different entities in the European Union can collaborate and share CTI with each other (e.g., Computer Security Incident Response Teams (CSIRTs), critical infrastructure operators, and private organisations).

Sharing intelligence information is challenging: CTI is highly sensitive in nature and the target participants of these sharing networks operate within different trust boundaries. If CTI is handled incorrectly or leaked, it could have a detrimental impact on the organisation at the source of the intelligence; they could be exposed to further exploitation from attackers and their reputation could be damaged, leading to loss of revenue. Moreover, the inherent trust barriers that exist between the individual and/or groups of participants can inhibit sharing and discourage network participation. Finally, although some work is ongoing [4], currently the CTI sharing process is under-standardised, and often CTI is shared on an ad-hoc basis using insecure methods, such as telephone and email, that require resource-intensive processing.

Blockchain technology has the potential to disrupt traditional financial and commercial processes and aims to bring about new ways of transacting data and providing a higher level of provenance to data assets via cryptographic protocols, consensus mechanisms and an added layer of non-repudiation and immutability - security properties that lend the technology to a CTI sharing application.

Given the challenges involved in CTI sharing and the architecture and security properties of blockchain, the two objectives of this work are:

1) Determine whether blockchain technology is a suitable candidate for effectively sharing and disseminating CTI.
2) Develop a prototype network that can be used as a test platform for future research into enhancing CTI sharing using blockchain technology.

We investigated the common issues within the area of CTI sharing in order to define the requirements for the system. We also evaluated the various tools available to implement a prototype CTI sharing blockchain network, which could be used as a testbed to validate future proposals. We designed the network to be compliant with the STIX 2.0 standard - a structured language for CTI sharing [4]. Moreover, this project achieves the 'partitioning' of the network into 'channels' whereby information can be disclosed within private communities/partnerships. This is achieved through a mechanism that still provides participants with the benefits of smart contract capabilities, auditability, and the data provenance properties inherent in a blockchain system.

II. Literature Review

CTI sharing has the potential to be an effective process that allows organisations to respond quickly to malicious activity that could threaten their networks [7]. Although, several vendors and organisations are developing products to support CTI sharing, significant problems are still present in this domain. For example, an unresolved issue is the inherent trust boundaries that exist between the different organisations that must participate in these sharing networks. Moreover, the sharing process is under standardised, with no formal automated methods for processing information, thus resulting in an inefficient, resource intensive, process that requires considerable manual intervention [1].

978-1-7281-1542-9/19/$31.00 ©2019 IEEE

The activation of the NIS directive in Europe in May 2018 means that CSIRT's of each member state and some private organisations are required to implement protocols to effectively share CTI. This is a far-reaching directive, spanning different jurisdictions and countries, and has led to the publication of several studies into the state of the art in CTI sharing prior to the activation of the NIS directive. Two prominent themes in the literature are trust and privacy [12], [16], [17], [19]. Trust remains a very human element in an exchange of information in a CTI sharing context; however, there have been proposals to automate the trust element with computation [19], [8]. Although, some work to enable trusted information sharing has been published, there are still significant obstacles that prevent the delivery of trust in a complete way. The distribution of the participating organisations means that trust building is not straightforward and there is still more work to be completed if a network is to be set up for different European member states to exchange CTI [11].

CTI information is highly sensitive and has the potential to harm an organisations reputation, if leaked. Moreover, it may also inadvertently advertise a vulnerability that may be present in the organisation's infrastructure [18], [10]. This issue will have a negative effect when it comes to member states effectively building a collaborative information-sharing network. Privacy remains a serious concern for entities participating in a CTI sharing network. Anonymisation of the participant sharing the information has also been proposed, however, this introduces a situation where the data will lack credibility if its origin cannot be confirmed [8], a solution that provides both anonymisation and data provenance is critical.

Mattila et al. [14] conducted a study to determine how blockchains could provide some essential properties of privacy; a key finding was that the through the use of smart contracts and distributed consensus mechanisms, blockchains were an interesting and relevant approach to solve the issue of privacy. The authors in [14] approached the issue from a high-level context and did not give any examples of how these systems have been applied to a CTI use case.

There are many open challenges in the domain of CTI and works published in the literature on blockchain technologies make several claims about addressing trust and privacy [23], [9], [21]. However, to the best of our knowledge, there are no examples of blockchain technology within the literature that apply the technology to the domain of CTI sharing, thus making the proposal in this paper a novel and interesting approach.

III. Use Case

A. Cyber Threat Intelligence Sharing

Currently, CTI is frequently shared in an ad-hoc manner, with many organisations disseminating important CTI information through emails and phone calls. Trust, collaboration, and participation in a distributed CTI sharing network that spans across borders and different jurisdictions, are all challenges in this context.

1) Typical CSIRT Responsibilities: CSIRTs have a comprehensive range of duties in order to effectively protect/respond to events within their constituents network. A typical CSIRT will provide [5]: reactive services (alerts and warnings, incident handling, incident analysis, etc.); proactive services (security-related information dissemination, intrusion detection services, etc.); and security quality management (risk analysis, business continuity and disaster recovery, etc.). This research will focus primarily on the methods used to carry out the 'security-related information dissemination' operation.

2) CSIRT Tooling and Infrastructure: Typically, CSIRTs will utilise a Security, Information and Event Management (SIEM) system. There are a vast array of these particular systems available, both open-source and commercially developed. SIEM systems are crucial to the successful operation of an incident response team. They provide a useful means to accessing data at all layers of the network. Furthermore, it is a useful tool for accessing external intelligence data that has not originated from within their constituents network. However, not every CSIRT will use the same SIEM system, therefore different CSIRTs will have access to different external threat intelligence data, creating silos of information and information that is only available to the users of that particular system [19].

3) CTI Sharing Standards: There are many efforts being taken to standardise the the protocols that are used to share CTI. The domain of CTI sharing is lacking when it comes to a universal standard and the process of sharing data in a human-readable and machine interpretable format is still an area that requires further development. One organisation looking to tackle this issue is the OASIS organisation with the Structured Threat Information Exchange (STIX) standard. STIX is a JSON specification that enables the dissemination of actionable CTI whereby it can be consumed by humans and machines to enable them to carry out their security duties [3]. STIX has been coined as the best-path forward in the efforts for standardisation by ENISA [15], hence, it was selected for this work.

B. Blockchain Technology

A blockchain is a distributed database technology that maintains a continuously growing list of data records. These data records are also known as a 'ledger' in many circumstances. For each new record added to the ledger, a consensus must be reached whereby each new record appended to the ledger is validated by each/some participant(s) in the network [22]. Blockchain utilises a peer-to-peer architecture with public-private key cryptographic mechanisms to identify valid participants in the network. Essentially, it is a *shared record* amongst participating parties, each party has a copy of the record, each party *verifies* new inputs to the record and each party sees the same up-to-date version of the record.

A common characteristic that drives participation in a blockchain network, both public and private, is the incentive for actors to participate. There must be some common benefit from participating in a blockchain network, whether it's a

monetary/financial gain or the need for a fully traceable and auditable ledger of events.

Public networks have clear incentives for participation, especially when referring to a cryptocurrency-based network - potential financial gain and security by-design. The incentive to participate in a private blockchain network is significantly different. These networks are modelled around business/enterprise networks and the incentive is typically not monetary gain. This particular research focuses on a consortium of organisations that transact assets (both tangible and intangible) amongst each other and build proprietary blockchain networks to facilitate these transactions. Several pertinent issues arise in this context:

A clear incentive in a CTI sharing use case is the requirement for an immutable and audit-able log of all transactions, which is desirable in any enterprise network (regardless of how it is achieved). It rules out any costly/timely reconciliation mechanisms between different authorities/organisations. A blockchain provides this by-design.

It is feasible to store an immutable log in a centralised system, where a neutral authority manages and maintains it. For example, database engineers could employ 'UPDATE-only' mechanisms and a hash-linked blockchain data structure within a standard database. Therefore, we can state that blockchain networks are *only* useful when the participating actors/entities do no trust each other and have differing economic/political motivations. Furthermore, if the volume of participants scales up, a centralised service and the rules that govern it, become a complex system to maintain. Consequently, it becomes increasingly complex for this neutral party to ensure that the data-protection and security needs are met for every organisation in the network.

The neutrality of a centralised authority may become an issue. If a system has multiple participants, spanning across borders and jurisdictions, the issue of what lawful jurisdiction the neutral party is resident in, arises. Thus, the element of trust now comes back under scrutiny. Many participants may not agree on the central party's neutrality and thus, boundaries must created for participation.

The subject of cost when provisioning a centralised system may also be an issue, particularly for smaller enterprises with limited means. In a distributed blockchain network, every participant covers the cost of provisioning their network node only. This creates a situation where every participant has a stake in the overall infrastructure of the network.

The issue of who governs the rules within the network can be addressed, firstly, by deciding to use an open-source blockchain implementation. A base-level of trust can be established on how every organisation's network-nodes will behave. Secondly, an agreement on what consensus protocol to employ can be reached. This aspect will govern how fault-tolerance and malicious behaviour should be handled within the enterprise network.

Participants	
Org	**Description**
CSIRT-IE	Representing the national incident response team for Ireland.
CSIRT-UK	Representing the national incident response team for the United Kingdom.
CSIRT-BE	Representing the national incident response team for the Belgium.
PRIV-ORG	Representing a private commercial entity within the network.

TABLE I
NETWORK PARTICIPANTS

IV. SYSTEM DESIGN & IMPLEMENTATION

This section presents the requirements and testbed design, including details of the segmentation using chaincodes and Fabric channels.

A. Testbed Requirements

Based on the literature review, the following requirements were defined for the sharing network:

- The network must have access control. A public blockchain system is not suited for sharing highly sensitive CTI data amongst organisations. Due to the requirement of a private/permissioned network, and the fact the application domain is inherently a commercial/enterprise setting, this study will use the Hyperledger Project [6]. Fabric has a plug-and-play styled architecture and is a good fit for this work, providing flexibility to the development phase [2].
- The block data must be structured around a CTI standard - the *STIX 2.0* standard was selected. The blockchain ledger and client applications must be able to persist and transact STIX 2.0 data.
- The Traffic Light Protocol (TLP) [20], commonly used within CTI sharing communities, can be enforced by means of Smart Contracts. This will allow participating organisations to ensure that they are only sharing relevant CTI data with the intended authorities/organisations, and not leaking sensitive data to organisations that don't have the adequate permissions to view the it.
- There must be client applications to simulate different actors within the network that possess different interests.

B. CTI Network Definition

First, the relevant participants within the network are defined in table I. Next, given the definition of the participating entities, the concept of Fabric 'channels' can be explored. In this particular test network there are 4 channels, as defined in table II. A description of the 'chaincodes' that are deployed to these channels is detailed below. These chaincodes govern the rules on which CTI information is disseminated on these channels, and they are based on TLP.

All-Chan (tlp-green) If a STIX data object contains TLP:green, that information is permitted to be shared freely. The 'tlp:green' parameter indicates that information is free to be shared to all participants.

Channels		
Channel	**Participants**	**Description**
All-Chan	CSIRT-IE, CSIRT-UK, CSIRT-BE, PRIV-ORG	All participants have access.
CSIRT-Chan	CSIRT-IE, CSIRT-UK, CSIRT-BE	All Incident response teams have access.
EU-Chan	CSIRT-IE, CSIRT-BE	All European entities have access (for demonstration purposes CSIRT-UK will be omitted from this channel).
Priv-Chan	CSIRT-IE, PRIV-ORG	Private channel between a private organisation and another public organisation they are in partnership with.

TABLE II
NETWORK CHANNELS

CSIRT-Chan (tlp-amber) If a STIX data object contains TLP:amber, that information is permitted to be shared on this channel only. The 'tlp:amber' parameter indicates that information is only to be shared with authorised individuals within a certain channel.

EU-Chan (tlp-amber) If a STIX data object contains TLP:amber, that information is permitted to be shared on this channel only. The 'tlp:amber' parameter indicates that information is only to be shared with authorised individuals within a certain channel.

Priv-Chan (tlp-red) If a STIX data object contains TLP:red, that information is permitted to be shared on this channel. The 'tlp:red' parameter indicates that the information is of high sensitivity and is only to be shared with authorised/trusted entities.

C. CTI Client Definition

Each participant in the network has their own client application. These applications allow end-users from those organisations to interface with the network and submit transaction events.

D. CTI Network Architecture and Design

This section presents the physical components and environments that form the network.

1) Orderer: This component is required for the entire network to function. The 'Orderer' provides a consensus layer to the network and ensures that each Peer maintains a valid 'ordering-of-events' within their copy of the blockchain/ledger. Also, the Orderer holds other essential components such as the channel configuration blocks.

It is worth noting that, although this testbed only utilises one Orderer node, this is not recommended in a production network as it introduces a single-point-of-failure within the system. Moreover, the Orderer in our network model uses the Solo consensus mechanism, which is not appropriate for a real-world deployment.

2) Peers: Two Peer nodes are deployed for each participant. This simulates a network that more accurately resembles a real-life deployment. For example, one Peer node may represent 'Headquarters' and another may represent 'Branch' for a given organisation. The Peer acts as the interface to the Client and it physically maintains a copy of the blockchain/ledger.

3) Certificate Authority (CA): Each organisation runs an instance of the Hyperledger Fabric CA server. This component disseminates certificates to participants in the network to authenticate their identity. The CA instances in this test network disseminate generated cryptographic material for simulation purposes. In a real-world deployment, Fabric is designed around being interoperable with real-life certificate authorities.

4) Chaincode: These components host the chaincode, which is installed on selected Peer(s). The appropriate number of chaincode components that must be installed depends on the number of chaincodes and the number of chaincodes deployed per channel. These environments remain idle until an 'INVOKE' event/transaction activates them.

5) API: This provides an API to interact with the Peer nodes from the Client.

6) Client: This container hosts an instance of the client application for the given organisation.

7) CLI: This is a tool that Fabric provides to run commands on different Fabric components during setup/testing.

Figure 1 represents the network topology. All of these environments can be initialised on a single machine for testing, however, in a real-world deployment, each component can be deployed to different environments/physical machines. Clustering can also be applied to provide fault-tolerance and high-availability. These distributed components were configured using docker - the entire set of congurations and execution scripts for the testbed is available here: http://tinyurl.com/blockchain-cti-network.

E. Client Application

The client application for this network must support a number of use cases to demonstrate the networks functionality. However, since the focus of this work is the network itself, providing a feature-rich application that demonstrates the entire functional capabilities of a standard CTI sharing product is out of scope. The core functionality that must be included in order to demonstrate how an end-user can share CTI effectively is detailed below in the form of Agile 'User Stories'.

- As a User, I want to share non-sensitive STIX data to all participants in the network and select a smart contract that enforces a check on the data before it's shared.
- As a User, I want to share sensitive STIX data within my trusted community in the network and select a smart contract that enforces a check on the data before it's shared.
- As a User, I want to share highly-sensitive STIX data with one of my trusted partners in the network and select a smart contract that enforces a check on the data before it's shared.

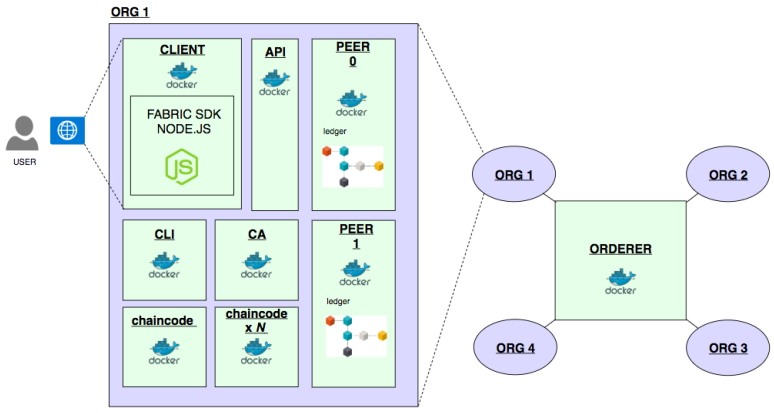

Fig. 1. Network Architecture

- As a User, I want to be able to query specific STIX data that I am authorised to access.

The test network contains four participating organisations, thus four client applications are required. Again, these applications are hosted within their own Docker environments. Furthermore, four instances of a REST interface are required in order for the client applications to transact with the network. The priorities with the client are to: implement the Node.js Fabric SDK; provide some basic functionality to the end-user; and build and push a Docker image of the client application and the REST API to DockerHub so the images can be loaded into the organisations' congurations during network-startup.

The user-facing application is a simple Node.js web application that utilises the functionality and endpoints provided by the REST API. It has two views and two forms that the user can interact with. The user can also see the blockchain/STIX data specific to the channel(s) their organisation participates in. The application passes events from the UI, to the Node.js runtime, which then dispatches that data to the REST API. Finally, the API communicates that information to the relevant Peer in the network and a transaction event is initiated in the network.

V. Testing and Evaluation

In order to test certain functional properties within the network, the relevant Fabric components within the network must be initialised and running.

A. Sample Development Network

A development network was created for this work; its design is based entirely on https://github.com/hyperledger/fabric-samples/tree/release-1.1/chaincode-docker-devmode. This is a small test network that is useful for provisioning a subset of the required components and developing chaincode. The test methodology is as follows: (i) determine Fabric requirements; (ii) test basic chaincode functionality without calling Fabric's API; (iii) configure docker environments as per requirements; (iv) run the network; (v) execute 'INSTALL', 'INIT', 'INVOKE', and 'QUERY' operations from the CLI.

B. Feature Evaluation

This section aims to evaluate the feature-set in the prototype application and demonstrate whether components function as they were intended.

1) User Story 1: As a User, I want to share non-sensitive STIX data to all participants in the network and select a smart contract that enforces a check on the tlp:green property on the data before it's shared.

Outcome must demonstrate: An Indicator of Compromise (IOC) has been shared amongst the entire blockchain network on 'all-chan' and each participant has access to that STIX data in their ledger (see fig 2).

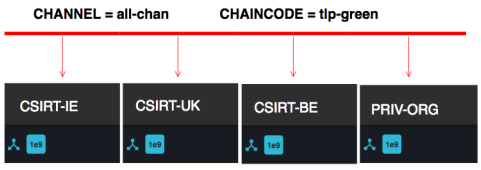

Fig. 2. Block-data with hash beginning '1e9' available to all participants.

2) User Story 2: As a User, I want to share sensitive STIX data within my trusted community in the network and select a smart contract that enforces a check on the data before it's shared.

Outcome must demonstrate: An IOC has been shared amongst a trusted community within the blockchain network on 'csirt-chan' and each participant that is part of 'csirt-chan' access to that STIX data in their ledger. Moreover, organisations that are not participants in this channel ('Priv-Org') cannot query/see this block data (see fig 3).

3) User Story 3: As a User, I want to share highly-sensitive STIX data with one of my trusted partners in the network and select a smart contract that enforces a check on the data before it's shared.

Outcome must demonstrate: An IOC has been shared amongst two trusted entities that are in partnership within

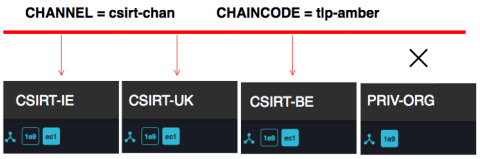

Fig. 3. Block-data with hash beginning 'ec1' only available to participants of 'csirt-chan'.

the blockchain network on 'priv-chan' and both participants of 'priv-chan' have access to that STIX data in their ledger. Moreover, organisations that are not participants in this channel('CSIRT-UK' and 'CSIRT-BE') cannot query/see this block data (see fig 4).

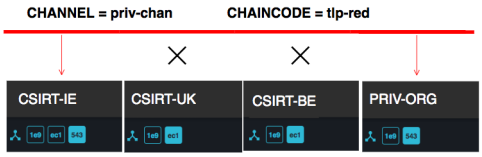

Fig. 4. Block-data with hash beginning '543' only available to participants of 'priv-chan'.

VI. Conclusions

This work focused on prototyping a CTI sharing Blockchain network. The literature review revealed that the subject of trust within existing CTI sharing networks was a difficult concept to quantify and that heavy-automation within these networks may create more problems than it solves. Blockchain emerged as a trustless mechanism where non-trusting entities could share and transact data within a network. We designed a new model for threat intelligence sharing and implemented it using the Hyperledger Fabric open-source Blockchain specification and tools. The prototype demonstrated successfully how STIX 2.0 security data could be disseminated within a network whilst utilising the constructs that Blockchain technology provides. Furthermore, this project achieved a successful partitioning of the network by utilising Fabric's channel capabilities, which allow trusted communities/partnerships to disseminate highly sensitive data in a privatised manner, whilst still participating in the overall network. TLP was enforced by utilising Fabric's chaincodes/smart contracts to enforce sharing rules within the network. This serves to protect participants from sharing highly-sensitive data with unintended parties. Future work will look at the performance and security aspects of a CTI Blockchain network with the view of designing a practical and secure application for use in the real-world.

References

[1] NH Ab Rahman, GC Kessler, and K-KR Choo. Implications of emerging technologies to incident handling and digital forensic strategies: A routine activity theory. pages 131–146, 2017.

[2] Elli Androulaki, Artem Barger, Vita Bortnikov, Christian Cachin, Konstantinos Christidis, Angelo De Caro, David Enyeart, Christopher Ferris, Gennady Laventman, Yacov Manevich, et al. Hyperledger fabric: a distributed operating system for permissioned blockchains. In *Proceedings of the Thirteenth EuroSys Conference*, page 30. ACM, 2018.

[3] S Barnum. Standardizing cyber threat intelligence information with the structured threat information expression (stix)[white paper]. *Retrieved July*, 20:2015, 2014.

[4] Sean Barnum. Standardizing cyber threat intelligence information with the structured threat information expression (stix). *Mitre Corporation*, 11:1–22, 2012.

[5] Henk Bronk, Marco Thorbruegge, and Mehis Hakkaja. A step-by-step approach on how to set up a csirt. *ENISA*, page 86, 2006.

[6] Christian Cachin. Architecture of the hyperledger blockchain fabric. In *Workshop on distributed cryptocurrencies and consensus ledgers*, volume 310, 2016.

[7] Paul Cichonski, Tom Millar, Tim Grance, and Karen Scarfone. Computer security incident handling guide. *NIST Special Publication*, 800(61):1–147, 2012.

[8] George Danezis, Josep Domingo-Ferrer, Marit Hansen, Jaap-Henk Hoepman, Daniel Le Metayer, Rodica Tirtea, and Stefan Schiffner. Privacy and data protection by design-from policy to engineering. *arXiv preprint arXiv:1501.03726*, 2015.

[9] Ali Dorri, Salil S Kanhere, Raja Jurdak, and Praveen Gauravaram. Blockchain for iot security and privacy: The case study of a smart home. In *2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops)*. IEEE, 2017.

[10] Cristin Goodwin, J Paul Nicholas, J Bryant, K Ciglic, A Kleiner, C Kutterer, A Massagli, A Mckay, P Mckitrick, J Neutze, et al. A framework for cybersecurity information sharing and risk reduction. Technical report, Technical report, Microsoft Corporation, 2015.

[11] John Haller, Samuel A Merrell, Matthew J Butkovic, and Bradford J Willke. Best practices for national cyber security: Building a national computer security incident management capability. Technical report, Carnegie-Mellon University PittsBurgh PA Software Eng Inst, 2010.

[12] Otto Hellwig, Gerald Quirchmayr, Edith Huber, Gernot Goluch, Franz Vock, and Bettina Pospisil. Major challenges in structuring and institutionalizing cert-communication. pages 661–667, 2016.

[13] Christopher Johnson, Mark Badger, David Waltermire, Julie Snyder, and Clem Skorupka. Guide to cyber threat information sharing. Technical report, National Institute of Standards and Technology, 2016.

[14] Juri Mattila et al. The blockchain phenomenon–the disruptive potential of distributed consensus architectures. 2016.

[15] Clemens Sauerwein, Christian Sillaber, Andrea Mussmann, and Ruth Breu. Threat intelligence sharing platforms: An exploratory study of software vendors and research perspectives. 2017.

[16] Florian Skopik. *Collaborative Cyber Threat Intelligence: Detecting and Responding to Advanced Cyber Attacks at the National Level*. CRC Press, 2017.

[17] Florian Skopik, Giuseppe Settanni, and Roman Fiedler. A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers & Security*, 60:154–176, 2016.

[18] Václav Stupka, Martin Horák, and Martin Husák. Protection of personal data in security alert sharing platforms. In *Proceedings of the 12th International Conference on Availability, Reliability and Security*, page 65. ACM, 2017.

[19] Clare Sullivan and Eric Burger. The privacy implications of international business-to-business sharing of cyber-threat intelligence. *Computer Law & Security Review*, 33(1):14–29, 2017.

[20] US-CERT, 2016.

[21] QI Xia, Emmanuel Boateng Sifah, Kwame Omono Asamoah, Jianbin Gao, Xiaojiang Du, and Mohsen Guizani. Medshare: Trust-less medical data sharing among cloud service providers via blockchain. *IEEE Access*, 5:14757–14767, 2017.

[22] Jesse Yli-Huumo, Deokyoon Ko, Sujin Choi, Sooyong Park, and Kari Smolander. Where is current research on blockchain technology?a systematic review. *PloS one*, 11(10):e0163477, 2016.

[23] Guy Zyskind, Oz Nathan, et al. Decentralizing privacy: Using blockchain to protect personal data. In *2015 IEEE Security and Privacy Workshops*, pages 180–184. IEEE, 2015.