A System Architecture of Cybersecurity Information Exchange with Privacy (CYBEX-P)

Farhan Sadique
Dept. of Computer Science and Engineering
University of Nevada, Reno
NV, USA
fsadique@nevada.unr.edu

Khalid Bakhshaliyev
Dept. of Computer Science and Engineering
University of Nevada, Reno
NV, USA
khalidb@nevada.unr.edu

Jeff Springer
Office of Information Technology
University of Nevada, Reno
NV, USA
jeffs@unr.edu

Shamik Sengupta
Dept. of Computer Science and Engineering
University of Nevada, Reno
NV, USA
ssengupta@unr.edu

Abstract—**Rapid evolution of cyber threats and recent trends in the increasing number of cyber-attacks call for adopting robust and agile cybersecurity techniques. Cybersecurity information sharing is expected to play an effective role in detecting and defending against new attacks. However, reservations and organizational policies centering the privacy of shared data have become major setbacks in large-scale collaboration in cyber defense. The situation is worsened by the fact that the benefits of cyber-information exchange are not realized unless many actors participate. In this paper, we argue that privacy preservation of shared threat data will motivate entities to share threat data. Accordingly, we propose a framework called CYBersecurity information EXchange with Privacy (CYBEX-P) to achieve this. CYBEX-P is a structured information sharing platform with integrating privacy-preserving mechanisms. We propose a complete system architecture for CYBEX-P that guarantees maximum security and privacy of data. CYBEX-P outlines the details of a cybersecurity information sharing platform. The adoption of blind processing, privacy preservation, and trusted computing paradigms make CYBEX-P a versatile and secure information exchange platform.**

Index Terms—**CYBEX-P, cybersecurity, information sharing, privacy preservation, information exchange, STIX**

I. Introduction

Modern cyberspace is beleaguered with an increasing number of advanced cyber-attacks rendering conventional cybersecurity measures practically useless. This is evident from the tenfold increase in the number of data breaches over the past 12 years- from about 160 in 2005 to about 1600 in 2017 [1]. Furthermore, the Center for Strategic and International Studies estimates the current global cost of cybercrime to be $600 billion (0.8% of global GDP) seeing an increase of $100 billion from 2014 [2]. These data show the need for adoption of agile cybersecurity measures by organizations.

It is envisioned that collaborative cybersecurity information sharing can protect firms more effectively from these advanced cyber-attacks. The benefits of cybersecurity information sharing are twofold: 1) new threats are detected faster, owing to collaborative intelligence 2) the corresponding signatures are distributed faster due to real-time sharing. Moreover, cyber threat intelligence sharing allows for investigating the latest trends in evolution of threats. As such, a cybersecurity information exchange platform is instrumental for assessing the contemporary threat landscape.

In this context, it should be noted that, an information sharing platform would be ineffective without an adequate amount of data. Which means, an effective management of such a broad spectrum of threats requires the widespread participation by public and private entities alike.

Unfortunately, despite the long-term advantages of collaboration, widespread adoption of an information sharing platform is affected by a number of challenges. The limitations of sharing security-related information are:

1) It may reveal vulnerabilities in the system attracting more targeted attacks.
2) Competitors may acquire significant underlying intelligence from the data.
3) It can compromise the privacy of the users.
4) It may violate companies' regulations and data policy.

All the above challenges stem from the issue of data privacy. Thus, an effective information sharing mechanism must address the privacy preservation of the shared data. The mechanism must achieve this for a variety of situations covering diverse conditions. Also, the mechanism must achieve this data privacy without any compromise.

The primary objective of our work is to develop a versatile information sharing framework for cybersecurity enhancement. Our design goal is to achieve this without sacrificing the security and privacy of the shared data. In this paper, we propose a novel framework called CYBersecurity information EXchange with Privacy (CYBEX-P) to tackle the above challenges.

CYBEX-P is a structured information sharing platform with a robust operational and administration structure. This platform addresses the inefficiency in dealing with cybersecurity problems by an individual entity. Real-time exchange of threat data helps organizations analyze current threats to predict and prevent future cyber-attacks. It also disrupts the rapid and extensive spreading of new threats and malware.

This research is supported by the National Science Foundation (NSF), USA, Award #1739032.

978-1-7281-0554-3/19/$31.00 ©2019 IEEE

CYBEX-P uses trusted computing paradigms, blind processing, and a two-step privacy handling mechanism. Besides, the platform includes a flexible governance framework that caters to the policies of any organization. These features make CYBEX-P a versatile and robust information sharing framework suitable for all types of organizations, small or big, public or private.

The rest of the paper is organized as follows: section II discusses the related literature and compares them with our work. Section III explains the basic functionalities of CYBEX-P and provides the detailed system architecture for implementation. Section IV presents a detailed analysis of CYBEX-P from a security and privacy perspective. Finally, section V concludes the paper with a discussion of its impact on the cybersecurity community.

II. Related Work

Plenty of research has been done on cybersecurity information sharing [4], [5]. Various protocols and specifications such as TAXII, STIX, OpenIOC, VERIS, MAEC, SCAP, and IODEF have also been developed to provide a common platform for sharing cybersecurity information [6]–[8]. Authors in [3], [9] analyze a game theoretic incentive model for information sharing and numerically verify it's effectiveness. Authors in [4] discuss the effectiveness of cybersecurity information sharing and formulate it as a risk-based decision-making model with a directed graph.

Bryant et al. discuss different models and methods of information exchange in [10]. SKALD [11] has been developed and presented as a framework for real-time information sharing. Authors in [12] propose a collaborative information sharing framework. However, none of these consider privacy preservation of shared information to motivate actors.

Security and privacy challenges in cybersecurity information sharing have also been studied extensively [5], [13]–[15]. Privacy-preserving data publication for log analysis has been studied in [13]. PRACIS [14] has been introduced as a privacy-preserving data analytics system. Its operations are however limited to generating some summary statistics by aggregating encrypted values.

A cryptographic privacy-preserving framework based on group signature scheme for sharing cybersecurity information has been presented in [15]. An attribute-based cybersecurity information exchange platform using attribute-based encryption has been introduced in [16]. Authors in [17] have investigated the trade-off between sharing cybersecurity information and privacy cost in a dynamic 3-way game model between attacker, organizations, and cybersecurity information sharing platform. The integrated privacy preservation has been discussed in [18]. Nevertheless, none of the above works propose a complete system architecture with integrated privacy preservation mechanism.

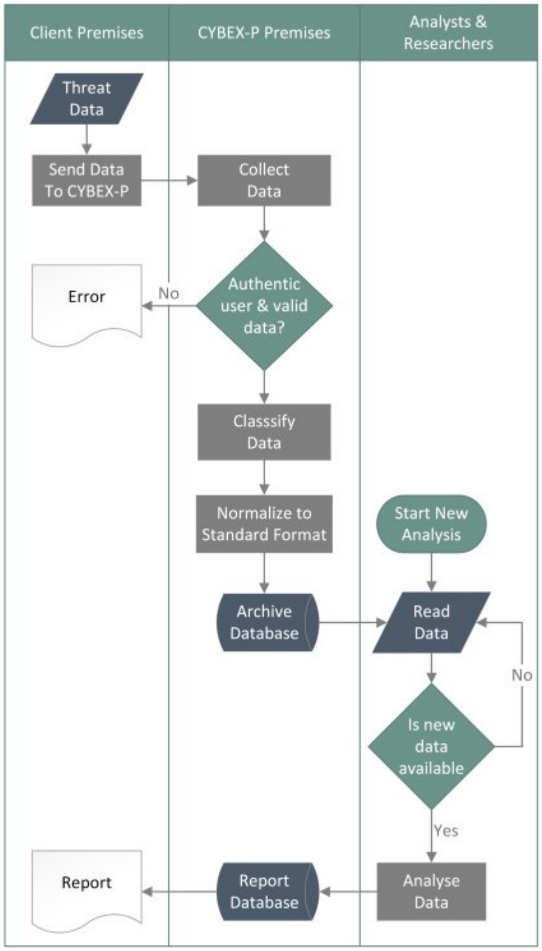

Fig. 1. The functional diagram of CYBEX-P

III. CYBEX-P Framework

A. CYBEX-P Process Overview

Figure 1 shows the functional diagram of CYBEX-P system with data flow among all the key processes. There are three separate parties involved throughout the complete lifecycle of the threat data: 1) Client organization 2) CYBEX-P 3) Analysts and Researchers.

The client organization acts as the source of threat data. It can be any external or internal threat data source willing to share threat data with others. CYBEX-P acts as the intermediary between all organizations and data analysts. There are two categories of data analysts participating in analyzing the data, namely professional cybersecurity analysts and cybersecurity researchers. They create static or dynamic rules to analyze the data to draw valuable inferences in the form of report data. These report data are shared with organizations as alerts or warnings.

The input to the process is threat data. Examples of threat data are firewall and IDS/IPS logs, system logs, emails, malware signatures, suspicious URLs, incident reports, list of malicious IP addresses, etc. These threat data may be machine generated or curated by a security specialist. Machines automatically generate data as a direct or indirect consequence of an event containing relevant information to that event. As an illustration, a firewall generates a packet log message when it receives a network packet.

Organizations send the threat data to the data collector in CYBEX-P. The data collector first authenticates the sending organization and validates the data. Afterward, it sends the data to the classifier.

At first, the classifier identifies the type of threat data. The second task of the classifier is to identify the formatting of the data later required for parsing. It is required because the same type of data can be represented in different formats depending on the particular software, operating system, device or vendor. This is demonstrated by the apparent dissimilarity in the logs of two different firewalls which nevertheless contain the same information.

The classified data is then normalized and converted to a standardized format. To represent the data uniformly we consider the standardized format Structured Threat Information Expression (STIX) [19]. STIX is a language and serialization format that enables organizations to exchange CTI in a consistent and machine readable manner These normalized data are stored in the archive database. The data analysts work on this archived threat data.

Data analysis is a continuous process. A new report is generated when an analyst decides to get some information out of the data. Additionally, old reports are updated as new data reaches the archive database. The information obtained from data analysis are stored as reports in the report database. Finally, the reports are sent to the client organizations on demand.

B. System Architecture Overview

Figure 2 shows our proposed design for CYBEX-P. The design is described in detail in the following sections:

1) Firewall Zones: There are three zones from the perspective of the CYBEX-P firewall: the outside zone, the demilitarized zone (DMZ), and the inside zone. All data originating from outside CYBEX-P premises are considered to be in the outside zone. The DMZ contains the services which communicate with other services outside CYBEX-P over public internet. Finally, the services in the inside zone have no access to the internet and can communicate only between themselves or with those in the DMZ.

2) Public Key Infrastructure: CYBEX-P maintains its own public key infrastructure (PKI). The corresponding certificate authority (CA) is shown in figure 2. This CA issues certificate to all the other components in the system to verify the authenticity of the source and the data.

C. Operation & Data Flow

The operation of the different modules along with the associated data flow are described below:

1) Raw Threat Data or CTI: Raw threat data are collected from client organizations. Examples of threat data are logs, malware signatures, spam emails, cyber threat intelligence data (CTI) etc.

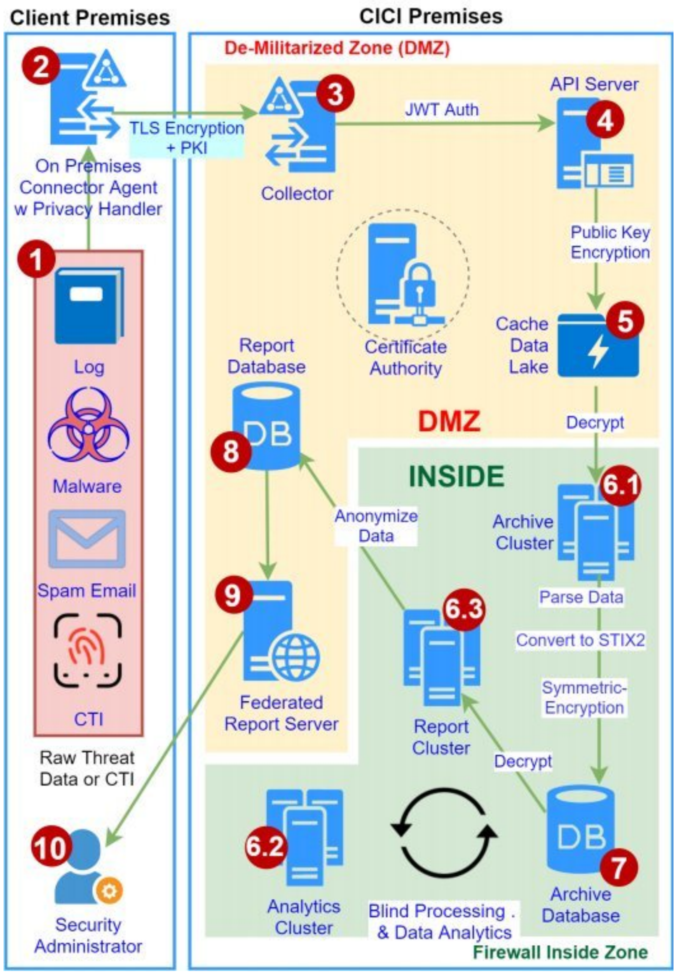

Fig. 2. Proposed Design for CYBEX-P

2) On-Premises Connector Agent with Privacy Handler: This agent acts as a real-time data shipper on client premises. It acts as a central hub to collect various types of threat data and relays them to the collector server in CICI premises. The first privacy handler is incorporated into this connector. It has provisions for modifying input data according to the specific requirement of the client. This connector agent is managed by the client organization.

The key feature of this connector is that it performs the necessary privacy-handling at the source before the data leaves their network. This makes it easier for organizations to integrate to CYBEX-P without violating their policies and regulations.

The public key infrastructure (PKI) described in section III-B2 is used to encrypt and sign the data.

3) Collector: The collector resides in the CICI premises. It negotiates with the connector agent to receive threat data from the client. The collector verifies the integrity of the data using the PKI.

4) API Server: The API server acts a medium for posting data into the cache data lake. It uses a token-based authentication method to authenticate the source of data. The data is encrypted with the public key of the processing server making it inaccessible to others. This is discussed in detail in section III-C6.

5) Cache Data Lake: The cache data lake stores the threat data as received from the client. The data in the data lake are unprocessed and stored in the exact format as received from the source. Even though the data lake lies in the demilitarized zone of the network the data is secured because they are encrypted with the public key of the processing server. So, only the processing server can decrypt these data.

6) Processing Server & TPM: The processing server is the only server that can decrypt threat data. It resides in the trusted zone of the firewall. This means no outside process can initiate communication to this server.

The encryption keys are stored in the trusted platform module (TPM). The integrity of the software and hardware are also verified by the TPM. Any alterations would automatically lock down the system. This makes the data secure even if the processing server is infected by a malware. There are three parts to the processing server:

6.1 Archive Cluster: The archive cluster reads the threat data from the cache data lake and decrypts it using the processing servers private key. It then parses the data into STIX 2.0 format and adds metadata. Finally, it re-encrypts the data using a symmetric key and stores the data in the archive database.

6.2 Analytics Cluster: The analytics cluster works continuously on the data stored in the archive database to come up with intelligent reports. It decrypts the data using the aforementioned symmetric key, performs the required analysis on the data, then re-encrypts it with the same symmetric key and stores the data back in the archive database.

6.3 Report Cluster: The report cluster decrypts the report data in the archive database, anonymizes the data and sends them to the report database. It has a privacy handler in it that removes all user-related information from the data to make it completely anonymous. This is done because the data in the report cluster is not encrypted and available to the subscribers of CYBEX-P. So, any organization specific data can be used for reconnaissance by malicious parties.

7) Archive Database: The archive database serves as the storage for all the threat data. It contains both unprocessed data and report data. All data in the archive database are encrypted using a symmetric key. The symmetric key is secured in the TPM of the processing server and no other processes have access to it.

8) Report Database: The report database contains categorized and analyzed report data. It serves these data to the clients. Since it communicates over the public internet it resides in the DMZ.

The data in here are not encrypted because they carry no information regarding the source user. Some of the reports contain aggregate data and need no anonymization. The others are anonymized before presenting. Thus, they pose no risk to any individual organization.

9) Federated Report Server: The report server is simple web front end where the users login to get access to the reports prepared by CYBEX-P.

10) Security Administrator: The reports are accessed by the security administrators from different organizations. These reports guide administrators to secure their environment with different priorities.

IV. CYBEX-P from a Security Perspective

A. CYBEX-P Features

The CYBEX-P incorporates a number of features to ensure maximum security and privacy of shared data. These features are discussed in detail below:

1) Data Encryption: CYBEX-P protects client data, both in transport and in storage, with state-of-the-art encryption schemes. The data in transit over the internet (or other public media) are encrypted on the transport layer using the Transport Layer Security (TLS) 1.3 [20]. TLSv1.3 is a major rewrite of the TLS protocol that boosts performance, security, and privacy.

There are two major data storages in CYBEX-P: the cache data lake and the archive database. The data in the cache data lake are encrypted using the public key of the processing server. This is done as soon as the data reaches the CYBEX-P premises. Therefore, no other entity can decrypt these data. This is desirable because the cache data lake lives in the DMZ whereas the processing server is in the more secured inside zone of CYBEX-P network.

On the other hand, the data in the archive database are encrypted using advanced encryption standard (AES) [21]. These data are encrypted using a symmetric key because no component other than the processing server will have access to the decrypted data.

Furthermore, the keys of the processing server are secured using Trusted Platform Module (TPM) [22] as described in IV-A3.

2) Data Integrity, Authenticity, Nonrepudiation: CYBEX-P has it's on PKI that issues certificates to all the components in the system including the connector in the connector premises. For the data received from a particular client, the PKI authenticates the source, verifies data integrity and ensures nonrepudiation. This means that CYBEX-P can trace an organization which tries to intentionally inject garbage data and corrupt the reports.

The PKI also does the same for all the communication inside the CYBEX-P premises. This added level of security keeps the data secure even if a certain component of CYBEX-P gets hacked.

3) Trusted Platform Module (TPM): The processing server in CYBEX-P has a TPM. The TPM verifies the integrity of the software and hardware running in the processing server. The TPM also acts as the secured storage for the private key and the symmetric key of the processing server.

The system shuts itself down if it detects any change in any software or hardware component. This assures that only trusted processes have access to the keys and the unencrypted data. Thus, the data is secured in case the processing server itself gets compromised or gets infected by a malware.

As discussed earlier, no component other than the processing server can access the unencrypted data in CYBEX-P. Therefore, our design makes the data inaccessible to any malicious party.

4) Privacy Preservation: An on-premise privacy handler performs privacy preservation before the data even leaves the client premises and reaches CYBEX-P premises. As the threat data may convey private information, it is not always possible to share such information in a raw format. Thus, we need a mechanism to protect the sensitive information before sharing. To this end, we classify the data into four categories based on sensitivity:

Level 0. These data are not sensitive and are transferred without encryption. Examples are a virus file, a malicious IP address, and a malicious URL. Fuzzy Hashing[1] is used to check the homologies of larger data like files/emails. Fuzzy Hashing reduces the dimensionality of high-dimensional data and hashes input items so that similar items map to the same *buckets* with high probability.

Level 1. These data have sensitive information about the source organization which might be exploited by the attacker for reconnaissance. For instance, consider that the source wants to share information about a new attack on its database server, however sharing the detailed information about the server network configuration, version and the model of the database server helps an attacker to have a better understating of the victims underlying network infrastructure. Thus, the source applies masking or generalization techniques (such as k-anonymity [23]) to hide the underlying sensitive information.

For instance, instead of reporting *The Oracle database server 11g with IP address 192.168.1.1*, source shares *Database server in the local network*.

Level 2. For this set of data, encryption is used to hide information for access control. In this case, only subscribers who have access to the key can decrypt the message. For instance, consider a new unpatched vulnerability has been detected, and such information should not be shared with the public.

Level 3. By sharing such information the subscribers are only able to find out if the other party has received the same message or not and no more information can be inferred. Private Set Intersection (PSI) [24] protocols are applied for this purpose. For instance, consider that an organization has received an unknown email which it cannot classify as SPAM or benign. As the email might be a normal message, the organization cannot share the message with other organizations. Hence, organizations initiate the PSI protocol to know if the message has been received by any other organization.

5) Blind Processing: CYBEX-P performs blind processing on all threat data. Organizational policies, constraints and trust boundaries are respected by performing blind processing on data. This is achieved by sharing only the structure of threat data and the output reports with the analysts. Since, CYBEX-P stores all data in STIX format, the structure is unambiguous and clearly dictated.

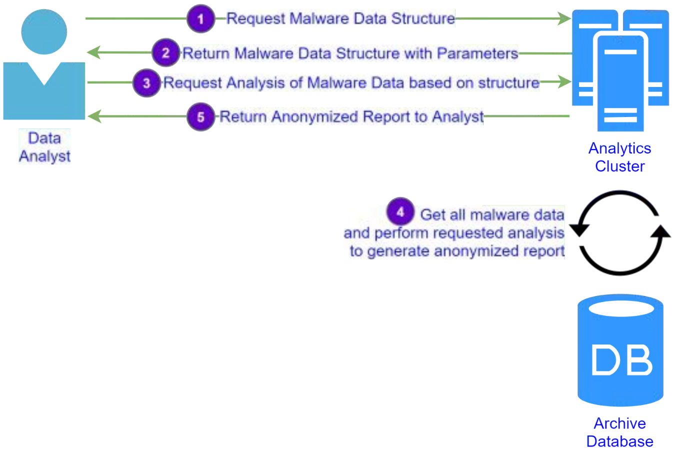
Data Analyst
1 Request Malware Data Structure
2 Return Malware Data Structure with Parameters
3 Request Analysis of Malware Data based on structure
5 Return Anonymized Report to Analyst
Analytics Cluster
4 Get all malware data and perform requested analysis to generate anonymized report
DB
Archive Database

Fig. 3. Blind Processing of Data in CYBEX-P

Figure 3 shows the process of blind processing in CYBEX-P with a simple test case. Suppose an analyst wants to perform some analysis on all malware data stored in CYBEX-P. He first requests the structure of the data to the analytics server. The analytics server returns the STIX structure of the malware data stored in its database with examples. It also returns the detail of each parameter from STIX specification.

The analyst then requests certain manipulation of the data to the processing server in the form of a script. The processing server fetches all malware data from the archive database, performs the requested manipulation of the data and generates an anonymous report based on the analysis. This report contains no organization-specific information and can be shared with the analyst. The analyst can repeat the process based on their requirement.

6) Data Anonymization: The second privacy handler guarantees complete privacy of client data by sharing only anonymized data with interested parties. It removes all information related to the source organization from the report.

7) Data Governance: CYBEX-P implements a flexible governance framework for compliance and regulatory requirements.

V. Conclusion & Future Work

The system architecture and implementation details of CYBEX-P has been presented in this paper. Future work related to this project will include analysis of the architecture with test cases and from a performance perspective. Our final goal is to make the architecture horizontally scalable and suitable for large-scale implementation.

CYBEX-P will contribute to the advancement of cybersecurity in two major ways. Firstly, it will play a central role in defense against new threats. The instantaneous sharing of threat indicators will cripple a new attack at its onset. This will render the process of painstakingly devising a new attack pattern economically infeasible. Secondly, the large information

[1] https://ssdeep-project.github.io/ssdeep/index.html

base will promote and incubate cybersecurity research in machine learning. Recent researches demonstrate that machine-generated rules outperform their human-generated counterparts in detecting zero-day attacks. However, the outcome of a machine learning algorithm is only as good as the training dataset. CYBEX-P will bolster such research endeavors by providing a rich, diverse and sizable dataset.

References

[1] "Annual number of data breaches and exposed records in the united states from 2005 to 2018 (in millions)," https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/, 2018.

[2] J. Lewis, "Economic impact of cybercrime-no slowing down," *Santa Clara: McAfee & CSI (Center for Strategic and International Studies)*, 2018.

[3] D. K. Tosh, S. Sengupta, S. Mukhopadhyay, C. A. Kamhoua, and K. A. Kwiat, "Game theoretic modeling to enforce security information sharing among firms," in *Cyber Security and Cloud Computing (CSCloud), 2015 IEEE 2nd International Conference on*. IEEE, 2015, pp. 7–12.

[4] J. L. Hernandez-Ardieta, J. E. Tapiador, and G. Suarez-Tangil, "Information sharing models for cooperative cyber defence," in *Cyber Conflict (CyCon), 2013 5th International Conference on*. IEEE, 2013, pp. 1–28.

[5] I. Vakilinia, S. Cheung, and S. Sengupta, "Sharing susceptible passwords as cyber threat intelligence feed," in *Military Communications Conference (MILCOM), MILCOM 2018-2018 IEEE*. IEEE, 2018.

[6] "Standards and tools for exchange and processing of actionable information," https://www.enisa.europa.eu/publications/standards-and-tools-for-exchange-and-processing-of-actionable-information/.

[7] J. Steinberger, A. Sperotto, M. Golling, and H. Baier, "How to exchange security events? overview and evaluation of formats and protocols," in *Integrated Network Management (IM), 2015 IFIP/IEEE International Symposium on*. IEEE, 2015, pp. 261–269.

[8] P. Kampanakis, "Security automation and threat information-sharing options," *IEEE Security & Privacy*, vol. 12, no. 5, pp. 42–51, 2014.

[9] D. Tosh, S. Sengupta, C. Kamhoua, K. Kwiat, and A. Martin, "An evolutionary game-theoretic framework for cyber-threat information sharing," in *Communications (ICC), 2015 IEEE International Conference on*. IEEE, 2015, pp. 7341–7346.

[10] C. Goodwin, J. P. 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," *Microsoft*, 2015.

[11] G. D. Webster, Z. D. Hanif, A. L. Ludwig, T. K. Lengyel, A. Zarras, and C. Eckert, "Skald: a scalable architecture for feature extraction, multi-user analysis, and real-time information sharing," in *International Conference on Information Security*. Springer, 2016, pp. 231–249.

[12] W. Zhao and G. White, "A collaborative information sharing framework for community cyber security," in *Homeland Security (HST), 2012 IEEE Conference on Technologies for*. IEEE, 2012, pp. 457–462.

[13] M. E. DeYoung, P. Kobezak, D. Raymond, R. Marchany, and J. Tront, "Privacy preserving network security data analytics: Architectures and system design," in *51st Hawaii International Conference on System Sciences, 2018*. University of Hawaii at Manoa, 2018.

[14] J. M. de Fuentes, L. González-Manzano, J. Tapiador, and P. Peris-Lopez, "Pracis: privacy-preserving and aggregatable cybersecurity information sharing," *Computers & Security*, vol. 69, pp. 127–141, 2017.

[15] I. Vakilinia, D. K. Tosh, and S. Sengupta, "Privacy-preserving cybersecurity information exchange mechanism," in *Performance Evaluation of Computer and Telecommunication Systems (SPECTS), 2017 International Symposium on*. IEEE, 2017.

[16] I. Vakilina, D. K. Tosh, and S. Sengupta, "Attribute based sharing in cybersecurity information exchange framework," in *Performance Evaluation of Computer and Telecommunication Systems (SPECTS), 2017 International Symposium on*. IEEE, 2017.

[17] I. Vakilinia, D. K. Tosh, and S. Sengupta, "3-way game model for privacy-preserving cybersecurity information exchange framework," in *Military Communications Conference (MILCOM), MILCOM 2017-2017 IEEE*. IEEE, 2017, pp. 829–834.

[18] F. Sadique, S. Cheung, I. Vakilinia, S. Badsha, and S. Sengupta, "Automated structured threat information expression (STIX) document generation with privacy preservation," in *2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON) (IEEE UEMCON 2018)*, 2018.

[19] S. Barnum, "Standardizing cyber threat intelligence information with the structured threat information expression (stix)," *MITRE Corporation*, vol. 11, pp. 1–22, 2012.

[20] E. Rescorla, "The transport layer security (tls) protocol version 1.3," Tech. Rep., 2018.

[21] P. Chown, "Advanced encryption standard (aes) ciphersuites for transport layer security (tls)," Tech. Rep., 2002.

[22] T. Morris, "Trusted platform module," in *Encyclopedia of cryptography and security*. Springer, 2011, pp. 1332–1335.

[23] L. Sweeney, "k-anonymity: A model for protecting privacy," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 10, no. 05, pp. 557–570, 2002.

[24] B. Pinkas, T. Schneider, and M. Zohner, "Faster private set intersection based on ot extension." in *USENIX Security Symposium*, vol. 14.