Hindawi
Security and Communication Networks
Volume 2018, Article ID 9634507, 11 pages
https://doi.org/10.1155/2018/9634507

Research Article

A Novel Trust Taxonomy for Shared Cyber Threat Intelligence

Thomas D. Wagner, Esther Palomar, Khaled Mahbub, and Ali E. Abdallah

Birmingham City University, Curzon Street, Birmingham, B4 7XG, UK

Correspondence should be addressed to Thomas D. Wagner; thomas.wagner@bcu.ac.uk

Received 29 December 2017; Revised 28 March 2018; Accepted 30 April 2018; Published 5 June 2018

Academic Editor: Emmanouil Vasilomanolakis

Cyber threat intelligence sharing has become a focal point for many organizations to improve resilience against cyberattacks. The objective lies in sharing relevant information achieved through automating as many processes as possible without losing control or compromising security. The intelligence may be crowdsourced from decentralized stakeholders to collect and enrich existing information. Trust is an attribute of actionable cyber threat intelligence that has to be established between stakeholders. Sharing information about vulnerabilities requires a high level of trust because of the sensitive information. Some threat intelligence platforms/providers support trust establishment through internal vetting processes; others rely on stakeholders to manually build up trust. The latter may reduce the amount of intelligence sources. This work presents a novel trust taxonomy to establish a trusted threat sharing environment. 30 popular threat intelligence platforms/providers were analyzed and compared regarding trust functionalities. Trust taxonomies were analyzed and compared. Illustrative case studies were developed and analyzed applying our trust taxonomy.

1. Introduction

Cyber intelligence is of high value when it comes to mitigating threats and, if shared, can contribute to thwarting repeated attacks. To accelerate the process of system hardening, cyber intelligence has to be actionable; i.e., it has to be complete, timely, accurate, relevant [1], and trustworthy to stakeholders. There are two types of cyber threat intelligence (CTI): strategic and tactical [2]. Actionable cyber intelligence should not need further analysis; it contains all information needed to understand the vulnerability and to take immediate action. Many organizations are ready to share their threat intelligence but insufficient threat sharing models and collaboration platforms hinder the process [3]. Yet, small organizations are especially incapable of analyzing and producing good enough quality CTI. Current industry-focused collaborations such as the Financial Sector (FS-ISAC: https://www.fsisac.com), the Retail Sector (R-CISC: https://r-cisc.org), the Electricity Sector (E-ISAC: https://www.eisac.com), and the recently established Automotive Sector (AUTO-ISAC: https://www.automotiveisac.com) are sharing cyber threat intelligence mainly in a manual and supervised fashion [4, 5]. In particular, FS-ISAC represents a community of trust that continually collects, analyzes, vets, and disseminates relevant threat intelligence to its participating members around the globe. Upon user authentication, the Critical Infrastructure Notification System (CINS) allows the FS-ISAC to distribute security threats and alerts to multiple recipients. This is manually done through a web portal on a "pull" basis. Furthermore, FS-ISAC does not allow to share received information with stakeholders outside the community. The detection of such a breach could result in being fined and dismissed from the community.

Furthermore, Internet of Things (IoT) vulnerabilities are a new challenge in the sharing environment where information about products, i.e., hardware, is exchanged additionally to traditional IT infrastructure vulnerabilities. The sharing in this domain is still very low and few sources provide information about such vulnerabilities. One of the reasons may be the recent emergence of connected cars, household items, or medical devices to the Internet and the therefore resulting low sources of threat intelligence. Moreover, the complexity of the components and its attributes render it challenging for companies to provide relevant inventory lists. These are required to know which information is relevant.

Crowd and supply chain sourcing models are also bringing in environments where trust naturally emerges. TripAdvisor and Wikipedia are perhaps the crowdsourcing industry's best known names. Crowdsourcing models are also supporting risk management strategies, e.g., by enabling companies to communicate transportation timelines, severe weather, and manufacturing interruptions, for instance, and allowing real-time collaboration between suppliers and other stakeholders [6–8]. The Synack Crowd Security Intelligence (https://www.synack.com) provides a hacker powered security platform with focus on crowdsourced penetration testing, vulnerability orchestration, analytics, and risk reporting. The solution was launched in May 2013 and provides a network of hundreds of vetted and trusted cyber security researchers and engineers who are made available for ongoing security testing at scale to clients for vulnerability remediation on an ongoing subscription.

In the case of supply chain based trusted environments, the information and know-how sharing between the partners certainly enhances the chain performance [7, 9]. Furthermore, collaborative data management and analytics tools have come a long way in helping data fit into data warehouses and business intelligence environments as well as providing a full range of collaboration features [10]. Indeed, collaborative cloud-based solutions not only have the potential to enable better teamwork, stakeholder engagement, and productivity, but also come up with powerful file storing and sharing capabilities and customized dashboards for better visibility into the entire supply chain management, for example.

This paper is organized as follows. Section 2 discusses the related work. Section 3 presents a comparison of threat intelligence platforms focusing on trust. Section 4 presents, discusses, and compares the trust taxonomy. Section 5 presents, analyzes, and evaluates our case studies. Section 6 concludes our work.

2. Related Work

Different suggestions of what threat intelligence is have been published. That is, a survey from the Ponemon Institute revealed that timeliness, ability to prioritize, implementation, and trust in source were amongst the most important attributes of actionable cyber threat intelligence to participants [11]. The European Network and Information Security Agency (ENISA) suggests actionability as accuracy, ingestibility, completeness, relevance, trustworthiness, and timeliness [12]. According to these two sources, trust establishment in CTI sharing is a crucial attribute to build long-lasting relationships amongst stakeholders. Sharing threat intelligence may include revealing that an organization was breached [13]. Reference [14] defines trust as one of the most crucial obstacles to share CTI amongst stakeholders. Trust in cyber threat intelligence sharing has been addressed by the Mitre group with its sharing protocol Trusted Automated eXchange of Indicator Information (TAXII: https://oasis-open.github.io/cti-documentation/taxii/intro). TAXII, based on HTTPS, shares indicators and uses the Structured Threat Information Exchange (STIX: https://oasis-open.github.io/cti-documentation/stix/intro), inter alia, to share CTI. The producing stakeholder (TAXII client) shares his threat intelligence over a TAXII server with other TAXII clients. STIX has become the forefront runner for the description of cyber threat intelligence in the past few years; nevertheless, it has been found to be challenging to implement and use by practitioners. The Malware Information Sharing Platform (MISP: https://github.com/MISP/MISP) provides another format to describe indicators and offers a plug-in for cyber threat intelligence in the STIX format. The Vocabulary for Event Recording and Incident Sharing Framework (VERIS: http://veriscommunity.net, https://github.com/vz-risk/veris) is a language to describe security incidents in a structured form. Reference [15] presents a threat intelligence framework that aims to create situational awareness amongst cyber security teams. The work includes a detailed analysis about trust in cyber threat intelligence sharing, such as the different trust models, i.e., "Validated Trust", "Direct Historical Trust", "Mediated Trust", "Mandated Trust", and "Hybrid Trust". Trust is related to the transmission between stakeholders, i.e., that the sharing and consuming stakeholders are the intended participants. Moreover, the authors define another trust attribute as "confidence" in threat intelligence. Reference [12] describes trust related not only to the sharing stakeholder, but also to where the threat intelligence is coming from. This requires a continuous path of transparency. Reference [16] published a threat taxonomy where one attribute describes the threat to information sharing with unauthorized stakeholders. This may have negative outcomes, depending on the secrecy labeling of the information. For instance, sharing groups may expel the stakeholder or fines may be issued. Reference [17] advises stakeholders in the preparation of enabling a trust mechanism for information sharing, such as nondisclosure agreements, Traffic Light Protocol (TLP) (TLP is defined into four colors, namely, white (no restrictions), green (sharing with peers and partners, not publicly), amber (sharing only inside own organization on who-need-to-know basis), and red (no sharing)), and antitrust rules.

According to the literature, trust is one of the most challenging attributes of cyber threat intelligence sharing. Without it, decentralized cyber threat intelligence sharing would be unthinkable. According to the Oxford Dictionary, trust is defined as "a firm belief in the reliability, truth, ability, or strength of someone or something." We define trust as an assurance that stakeholders are treating received CTI with confidentiality, if applicable, and not using it for malicious purposes. Furthermore, stakeholders are sharing true and correct CTI without the intending to badmouth or harm another peer in any way.

3. Analysis of Threat Intelligence Platforms regarding Trust

The process of aiding stakeholders to establish trust manually or automatically through trust taxonomies, or other support, is limited in the analyzed threat intelligence platform/providers. The focus mainly lies in sharing indicators and visualizing them in a graphical interface. The majority of the platforms provide an internal vetting process which leaves the responsibility to the provider. Hence, the provider

Table 1: Threat intelligence platforms: [1]denotes direct access; [2]denotes white/gray literature.

Threat Intelligence Platforms	Trust	Links
Malware Information Sharing Platform (MISP)[1]	T_2	https://github.com/MISP/MISP
NC4 CTX/Soltra Edge[1]	T_2	http://nc4.com/Pages/default.aspx
ThreatConnect[1]	T_1	https://www.threatconnect.com
Microsoft Interflow[2]	T_2	https://cloudblogs.microsoft.com/microsoftsecure/2014/06/23/microsoft-interflow-a-new-security-and-threat-information-exchange-platform/
HP Threat Central[2]	T_1	https://software.microfocus.com/en-us/solutions/enterprise-security
Facebook Threat Exchange[2]	T_1	https://github.com/facebook/ThreatExchange
IBM X-Force Exchange[1]	T_2	https://exchange.xforce.ibmcloud.com
Alien Vault Open Threat Exchange (OTX)[1]	T_2	https://www.alienvault.com
Anomali Threat Stream (STAXX)[2]	T_2	https://www.anomali.com/platform/threatstream
LookingGlass Scout Prime (Cyveillance)[2]	T_1, T_2	https://www.lookingglasscyber.com
Cisco Talos[2]	T_1	https://www.talosintelligence.com
Crowd Strike Falcon Platform[2]	T_1	https://www.crowdstrike.com
Norm Shield[2]	T_1	https://www.normshield.com
ServiceNow-Bright Point Security[2]	T_1	https://www.servicenow.com
NECOMAtter (NECOMAtome)[2]	T_2	https://github.com/necoma/NECOMAtte
Recorded Future[1]	T_1	https://www.recordedfuture.com
CyberConnector[2]	T_1	https://cyberconnector.eu/welcome
Last Quarter Mile Toolset (LQMT)[2]	T_1	https://cfm.gss.anl.gov/lqmt/
Health Information Trust Alliance - Cyber Threat XChange (CTX)[2]	T_1	https://hitrustalliance.net/cyber-threat-xchange/
Defense Security Information Exchange[2]	T_1	https://www.dsie.org
Retail Cyber Intelligence Sharing Center (R-CISC) Intelligence Sharing Portal[2]	T_2	https://r-cisc.org
Accenture Cyber Intelligence Platform[2]	T_1	https://www.accenture.com/gb-en/service-cyber-defense-solutions
Anubis Networks Cyberfeed[2]	T_1	https://www.anubisnetworks.com
Comilion[2]	T_2	http://comilion.com
McAfee Threat Intelligence Exchange[2]	T_1	https://www.mcafee.com/uk/products/threat-intelligence-exchange.aspx
ThreatQuotient[2]	T_1, T_2	https://www.threatq.com
ThreatTrack ThreatIQ[2]	T_1, T_2	https://www.threattrack.com
Eclectic IQ[2]	T_1, T_2	https://www.eclecticiq.com
Infoblox Threat Intelligence Data Exchange[2]	T_1	https://www.infoblox.com
Cyber-security Information Sharing Partnership[1]	T_1	https://www.ncsc.gov.uk/cisp

and its vetting processes have to be fully understood and trusted. This does not leave any room to establish circles of trust with decentralized peers. For instance, threat intelligence may be very limited if it is only shared in small circles. Therefore, a wide range of connected stakeholders is desirable. This enables participants to use threat sensors globally; i.e., each stakeholder enables threat monitoring and detection systems; the results are automatically consumed by all members. Table 1 provides an analysis of 30 threat intelligence platforms/providers which have been evaluated according to trust functionalities. The evaluation methods consisted of testing the platforms (direct access) and the analysis of white/gray literature. Platform testing was conducted by installing the newest version on virtual boxes or signing up with the web applications where possible. The white/gray literature consisted of academic papers, reports, and manuals provided online. Platforms labeled with T_1 establish trust internally for the stakeholder. Platforms labeled with T_2 provide no previously established trust environment and have to be initiated manually. Some platforms are labeled with both T_1 and T_2 and provide a trusted environment for stakeholders but also allow manual connections to other peers and repositories outside the trusted environment.

21 service providers establish trust for stakeholders (T_1) through vetting processes and closed environments such as hidden groups or sharing only with specific stakeholders. Some platforms provide intelligence to the stakeholder without having to reciprocate or connect to other stakeholders

Table 2: Threat intelligence platform matrix.

Threat Intelligence Platform	Own CTI	External Sources	Vetting Process	Same Industry	No Stakeholder contact
Malware Information Sharing Platform (MISP)		•			
NC4 CTX/Soltra Edge		•			
ThreatConnect		•			
Microsoft Interflow		•			
HP Threat Central		•			
Facebook Threat Exchange			•		
IBM X-Force Exchange		•			
Alien Vault Open Threat Exchange (OTX)		•			
Anomali Threat Stream (STAXX)		•			
LookingGlass Scout Prime (Cyveillance)	•	•			
Cisco Talos	•				•
Crowd Strike Falcon Platform	•				•
Norm Shield	•				•
ServiceNow-Bright Point Security	•				•
NECOMAtter (NECOMAtome)		•			
Recorded Future	•				•
CyberConnector	•		•		
Last Quarter Mile Toolset (LQMT)	•				•
Health Information Trust Alliance - Cyber Threat XChange (CTX)			•	•	
Defense Security Information Exchange			•		
Retail Cyber Intelligence Sharing Center (R-CISC) Intelligence Sharing Portal		•		•	
Accenture Cyber Intelligence Platform	•				•
Anubis Networks Cyberfeed	•				•
Comilion		•			
McAfee Threat Intelligence Exchange	•				•
ThreatQuotient	•	•	•		
ThreatTrack ThreatIQ	•	•		•	
Eclectic IQ	•	•	•		
Infoblox Threat Intelligence Data Exchange	•				•
Cyber-security Information Sharing Partnership			•		

through the platform. Nine platforms require the stakeholder to manually establish trust with other peers or groups (T_2). There is no identified mechanism that supports automated trust establishment in any of the analyzed threat intelligence platforms. Four platforms enable both (T_1, T_2) a trusted environment and manual connections to other stakeholders and cyber threat intelligence feeds.

Table 2 provides an overview of which platforms produce their own CTI, whether they allow external sources to flow into the TIP, if an internal vetting process is in place, whether they only share inside the same industry, and whether collaboration with other stakeholders is allowed.

3.1. Summary. This research has shown that various platforms enable internal vetting processes to establish a trusted environment, but they do not allow external connections. This creates a limitation of cyber threat intelligence sources. The trend as seen in Figure 1 shows that most of the tested threat intelligence platforms chose to provide cyber threat intelligence directly to their stakeholders without enabling direct contact to others. Roughly a third of the tested platforms decided to only provide manual trust establishment. That is, stakeholders have to develop trust relationships manually. Only 4 platforms enabled the manual connections between stakeholders or to external threat intelligence feeds alongside their vetted cyber threat intelligence. The used processes to establish trust are mostly vetting processes which are not transparent for users to see. Hence, stakeholders have to fully trust the threat intelligence provider with its processes.

Threat intelligence platforms should provide a more rigorous trust evaluation model, in particular, when the

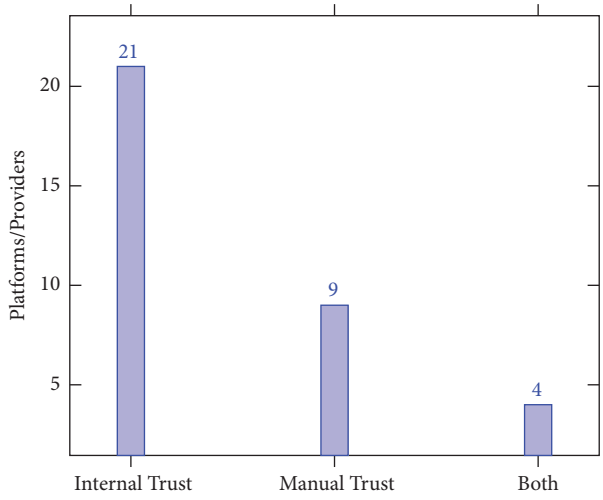


Figure 1: Trust establishment.

platform enables stakeholder interaction. Free platforms, such as AlienVault and IBM X-Force Exchange, allow participation with a valid e-mail and password. These vetting processes are not sufficient when sharing information about vulnerabilities. Malicious peers may create profiles to monitor current threat intelligence discussions which could tip off an adversary's attack. Moreover, a malicious peer could feed false information into the cyber threat intelligence ecosystem which could occupy stakeholders with the verification of the fake information. This may be used to distract stakeholders from real threats.

4. Trust Taxonomy

Trust plays a critical role in sharing cyber threat intelligence. Trusted relationships foster confidence for stakeholders that the provided information will be acted upon as intended, for instance, that stakeholders do no harm with the knowledge of vulnerabilities, especially if they have not been remedied yet and, furthermore, that stakeholders have appropriate protection measures in place and share the information as indicated. In this regard, understanding the value each actor contributes to the exchange is key. Identifying the membership criteria for any information sharing effort helps to build transparency and trust from day one.

Trust taxonomies have been widely investigated, such as for P2P systems, for instance [18–21], to establish both centralized and decentralized secure environments. Moreover, the 5x5x5 scheme (the 5x5x5 scheme evaluates intelligence in 3 areas: source, data validity, and sensitivity; each evaluation has 5 possible types of grading) and Admiralty Code (the Admiralty Code evaluates the reliability of the source and the confidence in the information) have appeared in recent platforms to evaluate intelligence. Section 4.3 presents a comparison of the aforementioned trust taxonomies and our trust taxonomy.

Figure 2 depicts our trust taxonomy processes to establish a trusted environment between centralized and decentralized stakeholders. Every stakeholder has its own profile which shows the sharing activity, peer ratings from poor to excellent, Mitre's Common Vulnerabilities and Exposures (CVE: https://cve.mitre.org/index.html) number, the source, and the industry group. Mitre's CVE is a dictionary of publicly known cyber security vulnerabilities that can also be used to correlate new indicators with historic events. Stakeholders can submit new potential security vulnerabilities which are then listed on the CVE website. The approval process is overseen by the CVE board. To elaborate further on the profile attribute sharing, we set our parameter to very active = 10 or more; active = 1–9; inactive = 0 shared threat records per month. Even though the activity does not automatically reflect good quality CTI, it is nevertheless a trust attribute.

The stakeholder rating borrows its functionality from eBay and Amazon's peer review after purchase. Buyers can rate sellers after purchase and vice versa. In our model, the stakeholders are rated manually from poor to excellent and the rating is based on the quality, or actionability, of threat intelligence (relevance, completeness, and timeliness). The threat intelligence and source define the type and origin, for example, whether the sharer is also the producer (1), someone else (2), or unknown (3). The industry column shows the affiliated industry group, if any, and can contribute to the trust level by being part of a respected group. For instance, organization A is part of the Financial Sector (FS-ISAC).

The trust balance chart shows how much value each column has. Our system's parameters are set to have sharing activity as 9%, stakeholder rating as 36%, same source 18%, and same industry as 37% weight. The reasoning behind the values is shown in Table 3.

We combine these inputs to help decentralized stakeholders to establish incipient trust. The parameters (sharing activity, stakeholder rating, same source, and same industry) are adjustable to stakeholder preferences. The rating value depicts the amount of each rating attribute pertaining to our trust balance. An organization must score at least 70% (this threshold is defined by our personal acceptance level and may be modified to suit individual stakeholders) to be considered trusted according to our personal trust acceptance level.

(i) **Scenario 1:** Organization A is very active (9%) and has an excellent stakeholder rating (36%); the industry is the same (37%); nevertheless, the shared cyber threat intelligence source is unknown (5.94%). According to our personalized trust balance parameters, the organization has a complete score of 87.94% and is thus accepted.

(ii) **Scenario 2:** Organization B is active (4.5%) but has a poor stakeholder rating (7.2%); the source of the threat intelligence is the sharing stakeholder itself (18%), and it is the same industry (37%). The organization has a final score of 47.7% and is therefore rejected.

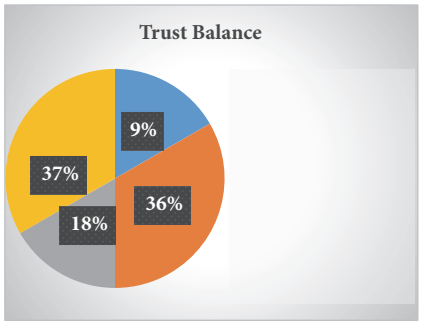
4.1. Trust Analysis. Trust in threat intelligence platforms (TIPs) is mostly established through a vetting process conducted by the CTI vendor. Some platforms use a recommendation system where a trusted peer may recommend another one as seen in the UK based Cyber Security Information Sharing Partnership (CiSP: https://www.ncsc.gov.uk/cisp).

Table 3: Attribute reasoning.

Attribute	Value	Reasoning
Sharing Activity	9%	The number of CTI contributions may not be a direct indicator for trust. Nevertheless, the activity may signal the stakeholder whether someone is a free-rider or actively interested in a collaboration.
Stakeholder Rating	36%	The rating of the stakeholder received a higher contribution to the overall trust because other stakeholders may evaluate the peer's trustworthiness based on the quality of the information and the conduct after receiving the information, i.e., whether the stakeholder conformed to secrecy labeling.
Same Source	18%	Transparency regarding where the intelligence comes from is a valuable contribution to the overall trust result, for instance, whether the sharing stakeholder also produced the intelligence or forwarded it from another unknown source.
Same Industry	37%	The same industry parameter received the highest value of all four attributes. Being inside the same industry sector, i.e., finance, retail, or manufacturing, automatically increases the trust amongst stakeholders.

Stakeholder	Sharing	Stakeholder Rating	Threat Intelligence and Source	Industry
Organization A	Very Active	Excellent ∗∗∗∗∗	CVE-XXXX-XXX / Unknown (3)	Finance
Organization B	Active	Poor ∗	CVE-XXXX-XXX / Stakeholder (1)	Retail
Organization C	Active	Good ∗∗∗	CVE-XXXX-XXX / Organization F (2)	N/A
Organization D	Active	Very Good ∗∗∗∗	CVE-XXXX-XXX / Organization X (2)	Industrial
Organization E	Inactive	Bad ∗∗	CVE-XXXX-XXX / Stakeholder (1)	N/A

Stakeholder Profiles



Trust Balance

- Sharing Activity
- Stakeholder Rating
- Same Source
- Same Industry

Activity	Inactive = 0% Active = 4.5% Very Active = 9%
Rating	∗ = 7.2%; ∗∗ = 14.4%; ∗∗∗ = 21.6%; ∗∗∗∗ = 28.8%; ∗∗∗∗∗ = 36%
Source	Unknown (3) = 5.94% Different Source (2) = 11.88% Same Source (1) = 18%
Industry	Other Industry = 18.5% Same Industry = 37%

Rating Value

Organization	Score
Organization A	87.94%
Organization B	47.7%
Organization C	56.4%
Organization D	63.18%
Organization E	43.7%

Stakeholder Trust Score

Figure 2: Trust taxonomy.

Nevertheless, the stakeholder is still vetted by the platforms administrators. Open-source platforms, such as the Malware Information Sharing Platform (MISP), rely on traditional trust establishment in manual form, i.e., through personal meetings or by being a member of a trusted circle. The limitations of such trust processes are that cyber threat intelligence is mostly shared behind closed doors. Therefore, stakeholders may not get the maximum value out of the information because of the limited circle of stakeholders. Trust functionalities in threat intelligence platforms may increase the participation and the shared information.

4.2. System Model. This subsection presents the system model of the trust taxonomy accompanied by Figure 3.

The first attribute of the trust taxonomy is the trust level in the source. This requires transparency pertaining to the generation of the CTI, i.e., the whole life cycle of the intelligence so far (Table 4).

The second attribute is the stakeholder rating. Stakeholders may be rated by other stakeholders who received CTI. The attributes may differ depending on the importance to the rating stakeholder. These attributes may comprise quality, timeliness, or communication (Table 5).

The third attribute is the sharing activity which may reveal free riders (Table 6).

The fourth attribute is the industry sector of the sharing stakeholder (Table 7).

4.3. Trust Taxonomies Comparison. This section presents a comparison of the mentioned trust taxonomies in Section 4. The papers and schemes have been selected due to their

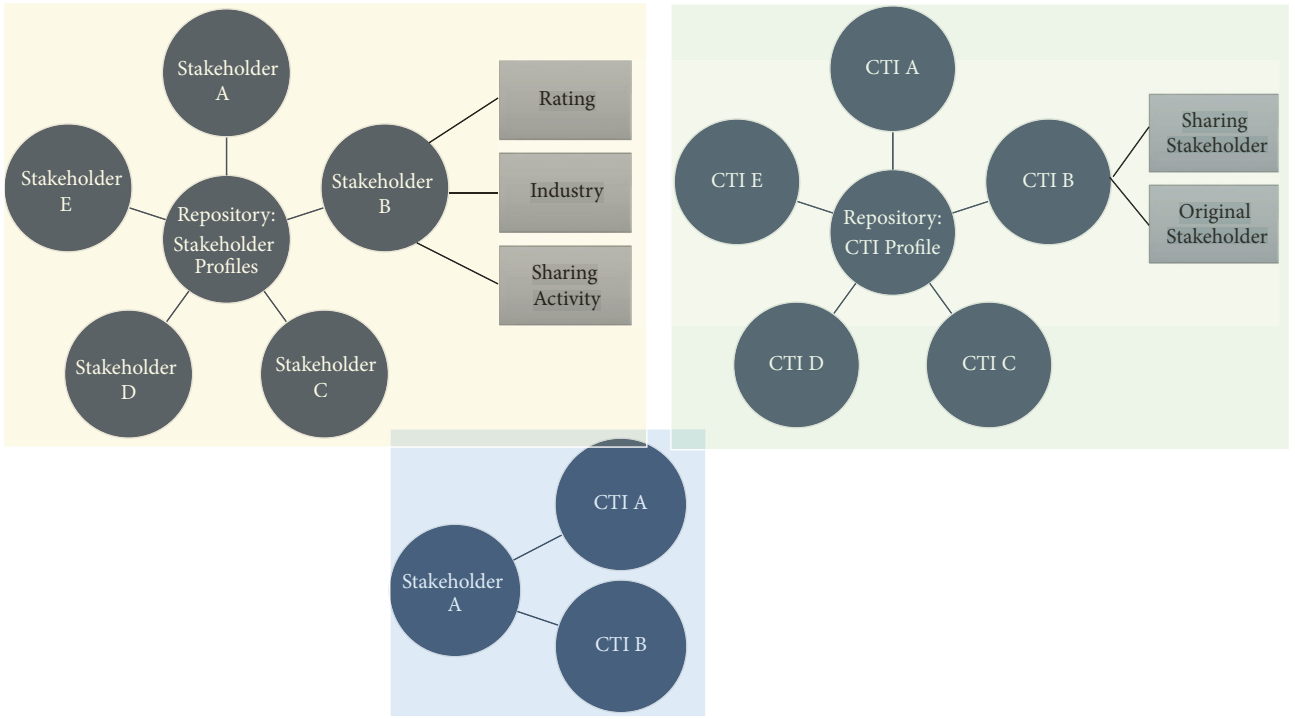


Figure 3: Trust taxonomy system model.

Table 4: Trust in source.

Trust Level	Trust Description
1	Very High Trust
2	High Trust
3	Medium Trust
4	Low Trust
5	Very Low Trust

Table 5: Stakeholder rating.

Rating	Description
1 *	Poor
2 **	Bad
3 * * *	Moderate
4 * * **	Good
5 * * * * *	Excellent

Table 6: Stakeholder sharing activity.

Activity	Description
Very Active	Shared CTI in the past 7 days
Active	Shared CTI in the past 30 days
Inactive	Shared CTI more than 30 days ago

possible capability of being implemented in a cyber threat intelligence sharing environment to establish or contribute to a trusted environment. We summarized and compared the taxonomies below.

Table 7: Industry sectors.

ID	Industry
1	Finance
2	Retail
3	Academia
4	Automotive
5	Electricity

A recommendation and authentication model was presented in "Research of P2P Network Trust Model (2013)" [20]. The model is based on trust and access control. It contributes to the identification of nodes with malicious intent, such as free riders. The nodes reputation is identified according to the node's malicious feedback behavior. The historical experience attribute of the trust model is similar to our stakeholder rating attribute of the trust taxonomy. The model evaluates whether the transaction was satisfactory and is then added to the peers profile. In our model, the stakeholders may rate another peer after a CTI record was shared. The missing control of the authenticity of the rating is a limitation in our model.

A taxonomy was presented in "A Taxonomy for Securely Sharing Information among Others in a Trusted Domain" (2013) [21]. The taxonomy presents a decentralized trusted environment for information sharing. It intends to prevent the leakage of information and proving the foundation for secure information sharing. The components to establish the trusted domain are assets, policy, controls, roles, evidence, and actions. The proposed trust domain has similar functions compared to our stakeholder trust score where the

stakeholder's trust is evaluated through different attributes. In CTI sharing, similar attributes may be relevant, fine-tuned with our proposed set of attributes to establish a trust score, i.e., sharing activity, stakeholder rating, same source, and same industry. A reputation model was presented in "A Taxonomy to Express Open Challenges in Trust and Reputation Systems" (2012) [19]. The paper examines the techniques used in reputation models and provides an overview of problem areas and possible solutions. The authors propose solutions for the lack of portability between systems, lack of categorization and the ability to filter and search, and explicit feedback, i.e., initialization, cold start, and subjectivity. The paper's overview of challenges in trust and reputation systems is still present. The paper outlines the initial phase of decentralized trust establishment. This issue is reflected in our trust taxonomy when new participants join the sharing groups and have to "earn" their trust.

A reputation model was presented in "Taxonomy of Trust: Categorizing P2P Reputation Systems" (2006) [18]. The authors present various trust and reputation models to build a trust taxonomy. A reputation scoring and ranking model is presented which describes "inputs", "outputs", and "peer selection". Furthermore, incentives for encouragement and punishments for malicious peers are presented. The reputation scoring and ranking model defines "inputs" which may be compared to the sharing activity attribute. Furthermore, it is discussed whether quality and quantity should influence the trust score. Our model provides a sharing activity attribute which reflects the quantity. The quality of the CTI is evaluated through the stakeholder rating attribute. "Output" comprises a scale from 1 to 10 and may be compared to the stakeholder rating. The authors discuss that different functions may be applied to different trust situations.

4.4. Trust Taxonomy Threat Model. Our trust taxonomy has been shown to be vulnerable against the following attacks.

(i) **Collusion Attacks:** stakeholders may form a group of adversaries to rate each other positively or increase the sharing activity to gain the trust of others. The adversaries may use this vulnerability to decrease the stakeholder reputation by giving poor ratings. For instance, malicious stakeholders A, B, C, and D join a cyber threat intelligence sharing community. The peers share and consume intelligence without any negative occurrences in the first few months. At the beginning, all stakeholders have low trust scores which increase, decrease, or stay the same over time. The incentive is that stakeholders with high trust scores have access to highly critical information which may be labeled with green or amber TLP. The previously mentioned peers start giving each other high stakeholder ratings which contribute positively to the trust score. The malicious peers had therefore access to critical intelligence and use the information to start exploiting unfixed vulnerabilities. Another scenario may involve the attack of specific stakeholders to decrease their reputation by giving bad stakeholder ratings. This may result in access loss to critical threat intelligence or complete loss of consumption. Hence, the stakeholder would only be able to share his own threat intelligence until the reputation is restored.

Possible solution: behavior monitoring may be able to pick up certain anomalies in stakeholder behavior and alert administrators to check suspicious stakeholders.

(ii) **Sybil:** a malicious stakeholder may create false identities to increase his own reputation. The incentive would be to obtain access to higher classified cyber threat intelligence for malicious purposes. For example, stakeholder XYZ joined a threat intelligence community which uses our trust taxonomy. The adversary uses several disposable e-mail addresses to create fake users which allowed him to rate himself higher. He then gained the trust of real stakeholders to receive permission to access higher classified cyber threat intelligence.

Possible solution: reference [22] developed a Sybil attack prevention mechanism which focuses on the social network domain. The mechanism is based on pairing based cryptography which includes a challenge and a response mechanism to join a group. This approach may be borrowed and implemented into the cyber threat sharing environment to protect the proposed trust taxonomy.

5. Case Studies

The presented trust taxonomy is tested through different illustrative use case studies. Case studies 1 and 2 discuss a fixed trust level. Case studies 3 and 4 discuss a dynamic trust environment and how trust is managed. The threat sharing community is called "X1", contains currently 12,536 stakeholders from various industries, and uses the presented trust taxonomy to enable a trusted environment. The repository is not industry-specific, but circles of trust were created supporting specific industries.

(i) **Case Study 1:** the organization "CFCyberX" has recently joined the threat sharing community X1. Therefore, stakeholder ratings are very low and comprise currently 3 reviews. The represented industry is the Automobile Sector. The actionability of the submitted CTI fulfilled all attributes to satisfaction. For example, the intelligence was submitted to the repository in less than 1 hour of discovery; the Course of Action (CoA) was accurately described for other stakeholders to directly implement the remedy. Five different types of information have been shared since registration 2 weeks ago. Therefore, the sharing activity is set to active. CFCyberX ensured transparency regarding where the intelligence was generated. Four different CTIs were shared as self-generated and 1 CTI was shared from another source.

This case study presents an ideal functioning state of incipient trust where the organization CFCyberX has already earned the limited trust of other stakeholders.

The identified risks with this case study are as follows: due to its recent registration and few contributions, the stakeholder may use this account to increase the rating of another account. For example, good quality CTI is shared to make other stakeholders believe in its good intentions. The trust level may indicate that confidential CTI is shared with the new stakeholder. If the stakeholder has malicious intentions, then the shared information could be used against the sharing peer, particularly if the vulnerability has not been remedied yet.

(ii) **Case Study 2:** this case study presents the financial organization "QuickExchange" which sells and buys various currencies. The organization joined X1 7 months ago and has received moderate to negative ratings. 63 different types of CTI have been shared with the community. For example, the negative feedback is a result of poor communication after sharing CTI and poor overall quality regarding timeliness. The negative reviews from the community had the effect that "QuickExchange" only has access to low risk CTI.

This case study demonstrates that trust may deteriorate over time if negative feedback is continuously received. Moreover, the continuation of low feedback may result in being removed from the trust circle or will only be allowed to provide CTI.

(iii) **Case Study 3:** the organization "CyberWhiteGoods" produces electronic appliances which are connected to the Internet. The sharing community X1 provides a trusted circle of stakeholders that share specific IoT threats. The products are very system specific and unique, and hence most vulnerabilities are discovered in-house or by external penetration testers. A bounty by "CyberWhiteGoods" is paid to white hat hackers for every discovered vulnerability. Nevertheless, data transfer is over traditional TCP/IP and data is stored on servers in the cloud. Ergo, some traditional CTI, such as information about server vulnerabilities and DDoS attacks, is applicable. The organization has shared various CTIs over the last 2 years since registration. The stakeholder's trust level is currently at 85% derived from criteria such as activity, ratings, and industry sector. The reputation deteriorated below an acceptable trust level because the account was temporarily hacked by an adversary. The adversary tried to misuse the consumed CTI to attack stakeholders at vulnerable points. Stakeholders raised their concern that they were attacked directly after critical information was shared with "X1". This had the effect that the organization was only allowed to share but not consume CTI. After a thorough investigation, the account was restored and permission given back to "CyberWhiteGoods". The trust level was restored to before the attack. This cases study shows that if an account was hijacked, access to critical information is given to the adversary. Therefore, system critical information can be exploited to attack unfixed vulnerabilities. It may also decrease the stakeholder's reputation even if the trust level is restored. The stakeholder may not be trusted any more with critical CTI because they may not be able to keep the shared information safe.

(iv) **Case Study 4:** the UK based water supplier "WaterPlus" joined "X1" 5 years ago and is part of the sharing circle specific for threats to the water supply chain. The stakeholders in the sharing circle represent different organizations nationally and internationally. Information is shared about cyber vulnerabilities but also about tangible attacks, such as planned attacks on pipes or contamination of the water supply. The sharing circle is highly interested in threats from the dark web where cyber terrorists collude and may reveal attacking details. The stakeholder has received positive reviews and is a very active participant pertaining to its amount of shared CTI. Nevertheless, it shares also third-party intelligence from outside the sharing circle. This has a negative impact on the trust level because the intelligence source is unknown or not trusted. Moreover, the organization has shared CTI with a nonmember which was discovered by another stakeholder of the sharing circle. This led to a warning from the repository administration. Further breaches would lead to a dismissal from the community.

This case study has shown sharing activities between stakeholders of critical infrastructure systems. Not following sharing policies such as sharing with third parties may be detrimental to trust levels. Stakeholders may decide not to share with "WaterPlus" if it shares CTI with peers outside the trusted community.

5.1. Case Studies Evaluation. Four case studies were presented and the evaluation is based on each case study. At first, we analyze key problems within each case study and why they exist. Then, we analyze the impact on the stakeholders and finally whether the proposed trust taxonomy is able to aid the trust establishment.

(i) **Case Study 1:** the key problem with case study 1 is that the stakeholder is a new peer in the trusted circle and has little history of sharing. It may be challenging for new peers to establish a trusted relationship at the beginning. This is a common problem in information sharing frameworks where trust has to be slowly created. This is not the case if a vetting process is conducted before sharing commences. The impact in this scenario may be that the company "CFCyberX" may not receive valuable threat intelligence that has a high security label, such as TLP red or amber. This case study may benefit from our proposed trust taxonomy by using the rating system for the CTI sharing attributes. It can help aid new stakeholders to establish trust after a few sets of threat intelligence were shared. The positive rating of the stakeholder may enable other trusted peers to share more critical threat intelligence with the stakeholder.

(ii) **Case Study 2:** the key problem with case study 2 is that "QuickExchange" has shared poor quality threat intelligence, did not communicate efficiently, and hence received negative reviews from other peers. The reason for this behavior may have 2 different reasons: deliberate or accidental. Deliberately sharing low quality threat intelligence and not communicating with other peers may reveal the intention of free riding, where CTI is consumed but not shared, or like in this case, only low quality CTI is shared. Accidental may include that in the sharers opinion the quality was sufficient. Furthermore, the stakeholder may not have the time and capacity to provide high quality threat intelligence and communicate adequately with other peers. The impact may be that the stakeholder only receives low quality threat intelligence in return and may be excluded from receiving CTI at all until its ratings go up. The benefit of the trust taxonomy for this case study is that free riders may be located. Moreover, it may also aid in deciding which threat intelligence is shared.

(iii) **Case Study 3:** the key problem with case study 3 differs from the previous 2 case studies where, in this case, the account of "CyberWhiteGoods" was hacked. Therefore, the user did not have control over the account and its actions. The account suffered from a loss of trust during the hijack and it took some time to prove that the attack really happened.

Furthermore, it took the stakeholder some time to readjust their trust level back to normal. Accounts may be hacked at any time and attackers may deteriorate a stakeholder's trust level. The impact of this case study is that the stakeholder did not have full access to critical threat intelligence during the time of the attack and recovery. This may have been damaging towards the proactive defense of the system. Therefore, breaches that could have been prevented through threat intelligence may have been successful. This case study benefited from the trust taxonomy until the account hijack. The trust taxonomy was unable to differentiate between the real stakeholder and the hijacker. Therefore, the trust taxonomy would profit from safety implemented to identify whether the real stakeholder is in control.

(iv) **Case Study 4:** the key problem with this case study is that "WaterPlus" shared third-party threat intelligence without revealing where it emanated from. Moreover, the stakeholder was caught sharing threat intelligence from the sharing circle with a nonmember. This deteriorated the trust level and a warning was issued. The reason for sharing outside the trusted circle may be accidental or deliberate. The accidental scenario would involve that the stakeholder may not be well organized. The threat intelligence may have been shared with a stakeholder outside the trusted circle, because it was not clear where it originated from. A deliberate scenario would involve that the stakeholder knew that it was against the policy to share outside the trusted circle but shared it anyway. The impact of such a behavior may result in not receiving classified threat intelligence due to the stakeholder's misbehavior. The trust taxonomy can aid the sharing stakeholders in the process to quickly identify another peer's trust level and hence decide which threat intelligence to share. The trust taxonomy may not aid the stakeholders in detecting anomalies that would cause trust deterioration. This would have to be fed manually into the trust taxonomy.

6. Conclusion and Future Work

Trust relationships between sharing stakeholders are imperative to share cyber threat intelligence. Nevertheless, it is challenging to find the right ingredients to establish a trusted environment. 30 threat intelligence platforms/providers were analyzed pertaining to trust functionalities. The trust taxonomy presented in this work demonstrates a way to establish trust for decentralized stakeholders. A threat model described vulnerabilities in our trust taxonomy and possible solutions to mitigate attacks. Illustrative case studies that reflect real-world scenarios were developed and analyzed to produce a testing environment for our trust taxonomy.

Future work includes the implementation with other components of actionable cyber threat intelligence sharing, for instance, threat intelligence relevance filtering for consumption. Moreover, the implementation in a live environment may provide our trust taxonomy with interesting challenges and further insights.

Disclosure

This article does not contain any studies with human participants or animals performed by any of the authors.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

[1] C. Ciobanu, Luc Dandurand, M. Grobauer et al., "Actionable Information for Security Incident Response," Tech. Rep., ENISA, Heraklion, Greece, 2014.

[2] G. Farnham and K. Leune, *Tools and Standards for Cyber Threat Intelligence Projects*, SANS Institute, USA, 2013.

[3] D. F. Vazquez, O. P. Acosta, C. Spirito, S. Brown, and E. Reid, "Conceptual Framework for Cyber Defense Information Sharing within Trust Relationships," in *Proceedings of the in. 4th International Conference on Cyber Conflict, CyCon*, p. 17, Tallinn , Estonia, 2012.

[4] K. M. Moriarty, "Transforming Expectations for Threat-Intelligence Sharing," 2013.

[5] C. Z. Liu, H. Zafar, and Y. A. Au, "Rethinking FS-ISAC: An IT security information sharing network model for the financial services sector," *Communications of the Association for Information Systems*, vol. 34, no. 1, pp. 15–36, 2014.

[6] G. Inverarity and S. Moseley, "50th anniversary of Numerical Weather Prediction (NWP) in the UK," *Weather*, vol. 71, no. 7, pp. 162-162, 2016.

[7] C. Forlines, S. Miller, L. Guelcher, and R. Bruzzi, "Crowdsourcing the future: Predictions made with a social network," in *Proceedings of the 32nd Annual ACM Conference on Human Factors in Computing Systems, CHI 2014*, pp. 3655–3664, can, May 2014.

[8] R. Prikladnicki, L. Machado, E. Carmel, and C. R. B. De Souza, "Brazil software crowdsourcing: A first step in a multi-year study," in *Proceedings of the 1st International Workshop on CrowdSourcing in Software Engineering, CSI-SE 2014*, pp. 1–4, ind.

[9] M. Migliardi and E. Riccomagno, "Some security considerations on crowd-sourcing an ontology," in *Proceedings of the 2013 36th International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2013*, pp. 953–958, hrv, May 2013.

[10] F. Kerschbaum, A. Schroepfer, A. Zilli et al., "Secure collaborative supply-chain management," *The Computer Journal*, vol. 44, no. 9, pp. 38–43, 2011.

[11] P. I. LLC, *Exchanging Cyber Threat Intelligence: There Has to Be a Better Way Sponsored by IID Independently conducted by Ponemon Institute LLC*, Exchanging Cyber Threat Intelligence, There Has to Be a Better Way Sponsored by IID Independently conducted by Ponemon Institute LLC, 2014.

[12] A. Abimbola, "Information security incident response," *Network Security*, vol. 2007, no. 12, pp. 10–13, 2007.

[13] D. Chismon and M. Ruks, *Threat intelligence: Collecting, analysing, evaluating. MWR InfoSecurity Ltd*, Threat intelligence, Collecting, 2015.

[14] ENISA, *SHARE, Protect-Solutions for Improving Threat Data Exchange among CERTs*, ENISA, Heraklion, Greece, 2013.

[15] H. Programme, "D5.1 Threat Intelligence Sharing: State of the Art and Requirements," *Proactive Risk Management through Improved Cyber Situational Awareness*, 2016.

[16] L. Marinos, *Enisa threat taxonomy: A tool for structuring threat information. ENISA, Heraklion*, Enisa threat taxonomy, A tool for structuring threat information. ENISA, 2016.

[17] ENISA, *NCSS Good Practice Guide Designing and Implementing National Cyber Security Strategies*, ENISA, Heraklion, Greece, 2016.

[18] S. Marti and H. Garcia-Molina, "Taxonomy of trust: categorizing P2P reputation systems," *Computer Networks*, vol. 50, no. 4, pp. 472–484, 2006.

[19] M. Tavakolifard and K. C. Almeroth, "A taxonomy to express open challenges in trust and reputation systems," *Journal of Communications*, vol. 7, no. 7, pp. 538–551, 2012.

[20] J. Wang, X. Li, and Y. Zhang, "Research of P2P Network Trust Model," in *Proceedings of the 2013 5th International Conference on Intelligent Human-Machine Systems and Cybernetics (IHMSC)*, pp. 70–73, Hangzhou, China, August 2013.

[21] N. A. G. Arachchilage, C. Namiluko, and A. Martin, "A taxonomy for securely sharing information among others in a trust domain," in *Proceedings of the 2013 8th International Conference for Internet Technology and Secured Transactions, ICITST 2013*, pp. 296–304, chn, March 2013.

[22] M. Alrubaian, M. Al-Qurishi, S. M. M. Rahman, and A. Alamri, "A novel prevention mechanism for Sybil attack in online social network," in *Proceedings of the 2015 2nd World Symposium on Web Applications and Networking, WSWAN 2015*, tun, March 2015.