Trustworthy Incident Information Sharing in Social Cyber Defense Alliances

Florian Skopik
Safety and Security Department
AIT Austrian Institute of Technology, Austria
florian.skopik@ait.ac.at

Qin Li
School of Computer Engineering
Nanyang Technological University, Singapore
qin.li@ntu.edu.sg

***Abstract*—The Internet threat landscape is fundamentally changing today. A major shift away from hobby hacking towards well-organized cyber crimes can be observed. The aim of these criminal organizations is the commercial exploitation of vulnerabilities in ICT infrastructures. Since attacks become more and more coordinated, we argue that counter measures must be properly coordinated too. Additionally, networks have grown to a scale and complexity, and have reached a degree of interconnectedness, that their protection can often only be guaranteed and financed as shared efforts. In this paper, we therefore introduce the concept of social cyber defense alliances. These alliances are shaped by social networks which connect information security stakeholders from various domains and facilitate the sharing of incident information. Some primary challenges include: 1) how to encourage participating stakeholders to contribute, and 2) how to ensure the quality and reliability of shared incident information. Here, we discuss an incentive model, which encourages information security stakeholders to share incident information. Furthermore, we highlight an architectural blueprint which is able to support the establishment of our proposed social cyber defense alliances in a real world context, and evaluate its applicability using agent-based simulations.**

***Keywords*-security incident sharing architecture, information exchange format, cyber alliances, incentive model**

I. Introduction

The Internet has emerged as the main driver and factor of growth for today's economy. Enterprises become increasingly interconnected to enable flexible collaboration across organizational boundaries, to harness synergies of shared resources and to allow novel and innovative forms of businesses. As a consequence, our society becomes more and more dependent on ICT. For instance, today most critical infrastructures, including energy supply, banking and transportation, are controlled by complex ICT systems to deliver unmatched service quality at low costs. While these systems were mostly operated in isolation from each other in the last decades, nowadays they are being connected to the Internet in order to enable remote monitoring and cost-efficient maintenance. Furthermore, ICT has become pervasive, using new computing paradigms, such as mobile computing and cloud computing. Due to this rapid interconnection, commercial forms of cyber attacks and cyber terrorism [1] have recently arisen. A recent study conducted by RSA revealed the vast extent of potential exposure to malware and data loss within some of the world's largest organizations [2]. RSA concluded that among the Fortune 500, 88 percent demonstrated botnet activity associated with their domains and 60 percent had e-mail addresses compromised by malware. Currently more than 60 million different malware variants are indexed from which one third came up only in the last year. This exponential growth rate, mainly resulting from customized malware created with dedicated toolkits, impressively demonstrates that there is an urgent need for novel countermeasure approaches.

We argue that since attacks become increasingly sophisticated, customized and coordinated, we also need to employ targeted and coordinated counter measures. Typical COTS virus scanner and firewall systems do not seem to sufficiently protect against advanced persistent threats (APTs) [3]. The rapidly growing complexity of today's networks, vast emergence of zero day exploit markets [4] and often underestimated vulnerabilities, e.g., due to outdated software or policies, lead to novel attacks every day. Thus, numerous information security platforms and knwoledge basis have emerged on the Web. From there, people can retrieve valuable information about identified threats, new malware and spreading viruses, along with information how to protect (e.g., see national CERTs [5]). However, these information is usually quite generic, not shaped to particular industries and lacks in depth knowledge. We are convinced that, in order to make such platforms more effective, personalized views along with rich information and experience reports are required to provide an added value to professional users.

In this paper, we thus motivate the need for cyber alliances, where organizations can form strong partnerships to collaboratively notify about novel threats and protect against corresponding attacks. While many works have focused on sophisticated technical means to set up effective protection mechanisms for today's large-scale networks (beginning from high performance event logging, over new data correlation and reasoning algorithms, to distributed anomaly detection approaches), we argue that much more emphasis must be placed on the actual sharing of incident-related information among partners. In particular, a cyber alliance requires: (i) to provide a strong incentive to partners to join such an alliance, and (ii) to encourage partners to actually share information. Tackling both aspects, besides

others, are of paramount importance when it comes to sharing of potentially sensitive and company-internal information. A federated trust and reputation model helps to dispel reservations. However, since such trust relations can hardly be technically enforced, we employ a social network that personally connects chief information security officers (CISOs) and their staff and enables them to exchange incident information with trustworthy partners around the globe. Traditionally, information sharing on a peer-to-peer basis was mostly informative, e.g., through phone calls or free-text e-mail messages. However, in the proposed cyber alliances, a formal approach is required to concurrently deal with many information sources in order to avoid overloads. Moreover, the exchange of sensitive information is usually shaped by social trust relations [6], for instance, people know each other from university or recent professional workshops. Our concept of social cyber defense alliances aims at transferring these fundamental pillars to the cyber space on a large scale.

In this work, we discuss the following contributions:

- *Motivation for Cyber Defense Alliance Setups.* First, we thoroughly motivate the need for social cyber defense alliances, and discuss concrete challenges to be addressed, including the stimulation of the incentive of potential partners to contribute.
- *Architectural Blueprint of a Resilient Framework.* Second, we define requirements on an architecture that realizes the technical basis for cyber defense alliances. Here, we also outline the basic building blocks and show the overall solution.
- *Solutions and Discussions.* Third, we discuss major solutions and their applicability. In detail, we present an incentive mechanism, which is important for the platform to gain momentum, and evaluate the approach using agent-based simulations.

The remainder of the paper is organized as follows. Related work is covered by Section II. Section III shows challenges and the problem statement. Section IV highlights the sharing incentive model. Then, Section V introduces an architectural blueprint which covers the outlined requirements. Section VI deals with the applicability of the proposed solutions. Finally, Section VII concludes the paper.

II. Background and Related Work

As ICT systems are being applied in a greater number of critical areas, cyber attacks are becoming more frequent and have an increasing impact. Situational awareness plays an important role in the defense and survival of ICT infrastructures amid a cyber attack. Attack detection relies on cyber sensors, such as intrusion detection systems (IDS), log file sensors, anti-virus systems, malware detectors, and firewalls [7]. Since many of the attack detection tasks are performed at a local level, within a single organization, such as an Internet Service Providers (ISP), cross-domain security information sharing is a crucial step to correctly understanding ongoing situations and to warn others against current threats. However, in practice, security information sharing is usually accomplished via ad-hoc and informal relationships [8]. Often, national Computer Emergency Response Teams (CERTs) assume the role of national contact points for coordinating and aggregating security incidence reports via communication channels such as email, instant messaging, file exchange/storage, VoIP, IRC and the Web [9]. Internet forums such as the Internet Storm Center from SANS [10] collect and provide data about malicious activities on the Internet. Commercial service providers, such as Arbor Networks [11], offer network-wide threat information updates and analysis services. However, we argue that there is a crucial tradeoff to be considered: Since information needs to be verified at higher level (in order to avoid hoaxes), the speed of distribution suffers – which is indeed the most important factor to protect against aggressive attackers and zero-day exploits. Thus, we argue that a direct sharing model between trustworthy partners is an additional means to allow efficient information sharing.

Social trust and reputation models have been widely studied in context of online collaboration platforms [12]. Since eventually, social cyber defense alliances and online collaboration platforms have many things in common, the application of these mechanisms are also beneficial in this context. The major aim of social trust models is to personalize online interactions and to prioritize collaboration with trustworthy individuals. Trust relations can be defined manually by users, e.g., by declaring 'friend'-relations, or can be determined automatically through mining of interactions [6]. We argue that the application of trust models is essential in environments where highly sensitive data is exchanged. Here, we do not suggest the artificial construction of relations, but the explicit modeling of networks that exist in reality anyway. We conclude, that while trust relations are a useful means to control the degree of information sharing [13], reputation is a crucial means to verify the credibility of information circulating in the network. The actual implementation of trust models is out of scope of this paper but have been extensively studied in [6], [13].

III. Challenges and Problem Statement

In reality there are several factors that discourage organisations from sharing information about incidents that they have experienced. These factors include:

- *Competition*. An organization is often reluctant to share incident information with its competitors, due to their conflict of interest.
- *Reputation*. Public disclosure of incident information such as security breaches often damage the reputation of an organization, especially commercial organizations such as financial institutes. This significantly deters them from sharing incident information with others.

- *Privacy*. Some description of an incident contains sensitive information about the victim. Sometimes the more detailed description of the incident is, the more sensitive information is revealed. This privacy concern discourages organizations from sharing the incident information.
- *Reliability*. An organization may be reluctant to utilize incident information received from organizations if the reliability of the incident information is not guaranteed.
- *Applicability*. An organization may not be interested in receiving incident information that does not apply to its information system.

The ultimate goal is to design a framework under which organizations are willing to share their incident information and the extent of incident information sharing among organizations is maximized, while the above-mentioned concerns and discouraging factors are sufficiently respected and taken into consideration.

IV. Sharing Incentive Model

We take a closer look on incentive engineering aspects in a simplified scenario in which only two parties v_i and v_j share information with each other – as pointed out in detail in [14]. Here, we recapitulate the basics which are essential in our whole framework. However, in contrast to the original work by Gordon et al. [14], we propose a few extensions to make this model fit for a social network context:

- *Customized Sharing Along Individual Relations:* An organization's security representative (e.g., a CISO) might not want to share the same amount of information with everyone in the alliance, but based on reciprocal behavior and personal trust, decides to share more with well reputed partners and less with, for instance, newcomers or parties with bad reputation.
- *Transitive Sharing Over Multiple Hops:* Once a party shares a portion of information with another party, it is not able to control the dissemination level of this information any longer. Therefore, we need mechanisms that ensure the partner that information is (i) strictly private, i.e., is not allowed to be shared with 3rd parties, (ii) can be shared with trusted partners on a need-to-know basis, e.g., if a service recovery procedure requires deeper knowledge in partner companies, (iii) public, i.e., can be shared with everyone within the alliance.

The incentive model describes how single parties benefit from being part of a social cyber defense alliance. The first notable property is the probability of a breach in party v_i, denoted as P^i. This probability directly relates to the amount of spent money for information security m_i. Notice that through v_j's sharing of valuable security-relevant information, v_i also benefits from v_j's investment. This propagated investment $m_i^{j\to i}$ depends on v_j's amount of spent money and portion of shared information (Eq. 1). The portion of shared information Θ_j can either be set from an external source (e.g., through national policies and/or legislative frameworks) or individually determined.

$$m_j^{j\to i} \equiv m_j \Theta_j^{j\to i} \tag{1}$$

The above definition covers the sharing procedure between only two partners v_i and v_j. Now, we introduce a third party v_k who is connected to v_i but not v_j. The question here is if and how much information is indirectly shared between v_j and v_k over the transitive relation $v_j \to v_i \to v_k$. The positive effect of v_j sharing information with v_i and the subsequent spillover to v_k is described by $m_j^{i\to k}$ (Eq. 2). This variable is determined by the expenditures of v_j (m_j), the portion of shared information $\Theta_j^{j\to i}$ (here: with v_i), and the portion of this information passed on by v_i to v_k ($\Theta_j^{i\to k}$).

$$m_j^{i\to k} \equiv m_j \Theta_j^{j\to i} \Theta_j^{i\to k} \tag{2}$$

Apart from the additional spillover effect from transitively connected parties (i.e., with one intermediate hop), and the personalization of shared information portions, the original sharing model for two parties v_i and v_j is applicable as described in [14]. For the sake of clarity, we stick to this simple case. So, v_i's security breach probability function $P^i(m_i, m_j^{j\to i})$ in Eq. 3 does not only depend on v_i's own security expenditures, but also on v_j's. In other words, the more money v_i and v_j spend *together* on security solutions and information collection, the less is the probability of a security breach at v_i (and subsequently, if sharing is bidirectional, also at v_j).

$$P^i(m_i, m_j^{j\to i}) = \Phi^i(m_i + m_j^{j\to i}) \tag{3}$$

As outlined in detail in [14], P^i is a continuously twice differentiable function from the set of non-negative real numbers to (0,1) such that the first derivation is smaller than zero and the second derivation is greater than zero (i.e., an increased investment m results in lower probabilities for breaches (typically at decreasing rates)). The effect is that for this class Φ^i of functions we can rewrite Eq. 3 as Eq. 4. Studying Eq. 4, investments – under dedicated assumptions such as the application of the special class of probability breach functions – in parties v_i and v_j simply add up.

$$P^i(m_i, m_j^{j\to i}) = P^i(m_i + m_j^{j\to i}, 0) = P^i(m_i + m_j \Theta_j^{j\to i}, 0) \tag{4}$$

In a sharing alliance consisting of n parties, this means, that any investment m_v at any company $1...n$ will have positive effects on each single partner and is thus highly beneficial to significantly reduce expenditures from a global point of view. Each organization's challenge here is to discover its best level of investments m to reach the highest net benefit. This problem is the same as minimizing the

Table I
DESCRIPTION OF SYMBOLS.

symbol	*description*
P^i	probability of a breach in party v_i
m_i	invested money of v_i for security
$\overline{m_i}$	optimal investment to gain highest net benefit
m_i^*	optimal investment if no sharing
$m_j^{i \to k}$	part of v_j's investment spilled over from v_i to v_k
L_i	loss of money of v_i in case of a breach
$\Theta_j^{i \to k}$	portion of info originating from v_j shared by v_i with v_k

total expected costs. In the worst case of a security breach (causing loss L_i), this challenge can be written as Eq. 5.

$$min_{m_i}(\Phi^i(m_i + m_j^{j \to i})L_i + m_i) \tag{5}$$

Calculating the first derivative reveals the first order conditions Eq. 6 and Eq. 7, which describe the optimal investment $\overline{m_i}$. The latter describes the optimal investment m_i^* in case of no sharing, i.e., $\Theta_j^{j \to i} = 0$ and/or $m_j = 0$.

$$-\Phi^i(\overline{m_i} + m_j^{j \to i})L_i = 1 \tag{6}$$

$$-\Phi^i(m_i^*)L_i = 1 \tag{7}$$

A *reaction curve* $\overline{m_i}(v_j)$ describes v_i's expenditure behavior based on v_j's behavior. Comparing Eq. 6 and 7 and since $m_i, m_j \geq 0$, we can determine $\overline{m_i}(m_j)$ as Eq. 8.

$$\overline{m_i}(v_j) = max\{m_i^* - \Theta_j^{j \to i} m_j, 0\} \tag{8}$$

The point where – for this two-party case – the reaction curves of v_i and v_j intersect, is the *Nash equilibrium* in expenditure levels in a non-cooperative game. In this game, each party independently sets its expenditures to a level so that the cost saving factor through sharing is maximized.

For the general case of n organizations in the alliance, a single party v_i will react[1] to the expenditure levels of its direct partners, i.e., connected neighbors $V_i \subseteq V$ of the social graph $G = (V, E)$. This is formulated in Eq. 9.

$$\overline{m_i}(V_i) = max\{m_i^* - \sum_{j=1}^{|V_i|} \Theta_j^{j \to i} m_j, 0\} \tag{9}$$

V. INCIDENT INFORMATION SHARING ARCHITECTURE

Requirements: We categorize the basic requirements of the platform into: 1) incentivizing incident information sharing, 2) allowing diverse and dynamic configuration of incident sharing policies, 3) applying an appropriate incident information format for a structured classification of incidents and description of detection and mitigation strategies, 4) ensuring the reliability of received incident information, 5) providing privacy protection for sharing peers, 6) supporting development of trust among sharing partners, and 7) proving an efficient, scalable, and fault-tolerant incident sharing platform.

Architectural Blueprint: Overall, we employ a hybrid model (aka semi-distributed model). This allows the individual peers to share their incident information in a distributed manner, and make their individual decisions for each incident information on 1) the recipients, 2) the richness of the incident information with respect to each recipient, and 3) the channel to share the incident information with each recipient and the security of the channel. This hybrid model also includes a centralized identity management system combined with a public key infrastructure (PKI) and a reputation system. The whole approach is depicted in Figure 1. Notice that sensitive and confidential incident information is shared directly between peers, while a centralized entity is used to implement a reputation system and key management facilities. This model is a trade-off to enable fast and confidential sharing on the one side, and keeping the whole infrastructure efficiently manageable on the other side.

The operation for disseminating incident information can be conceptually described as follows. First, incident information is entered into the system, formatted and registered as incident report in the local database. Then this new report is encrypted using the public keys of the alliance partners (buddies) of the sending peer, and the encrypted report is sent directly to the corresponding buddies. Upon receiving the encrypted report, if the receiving peer considers the sending peer its buddy then the encrypted report is decrypted, stored in the local database, and visualized. If the sending peer is unknown to the receiving peer, then the receiving peer may retrieve the reputation of the sending peer from the centralized reputation system. The incident report may be accepted if the reputation score of the sending peer is sufficiently good. The receiving peer at a later time may report the centralized reputation server about the reliability of the received incident report. The centralized reputation server periodically updates the reputation score of the sending peer based on received feedback. A peer periodically updates its list of buddies based on its own sharing policy.

Information Formats: A few applicable formats exist to exchange information across organizations, e.g., x-arf[15] or Incident Object Description Exchange Format (IODEF)[16]. In this work, we particularly focus on the IODEF format. The major advantage is that this format is already well described in an RFC and going to be implemented in a wide variety of products, thus, offering supporting technologies for the future system implementation. As explained in [16], IODEF is a format for representing computer security information commonly exchanged between Computer Security Incident Response Teams (CSIRTs). It provides

[1]Notice that this formula will be used to let the system in the next section autonomously decide to what degree information is shared to reach an optimal expenditure level. However this system decisions need to be balanced out carefully with company policies about information sharing.

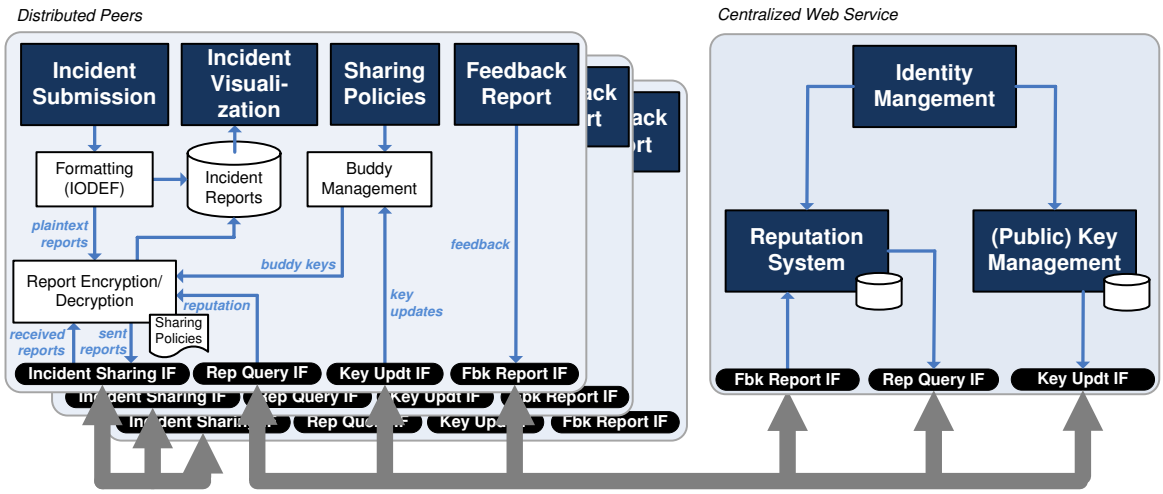


Figure 1. Semi-distributed incident information sharing architecture.

an XML representation for conveying incident information across administrative domains between parties that have an operational responsibility of remediation or a watch-and-warning over a defined constituency. The data model encodes information about (i) hosts, networks, and the services running on these systems; (ii) attack methodology and associated forensic evidence; (iii) impact of the activity; and (iv) limited approaches for documenting workflow.

The purpose of the IODEF is to enhance the operational capabilities of CSIRTs. Community adoption of the IODEF provides an improved ability to resolve incidents and convey situational awareness by simplifying collaboration and data sharing. The structured IODEF format allows for:

- increased automation in processing of incident data, since the resources of security analysts to parse free-form textual documents will be reduced;
- decreased effort in normalizing similar data (even when highly structured) from different sources; and
- a common format on which to build interoperable tools for incident handling and subsequent analysis, specifically when data comes from multiple constituencies.

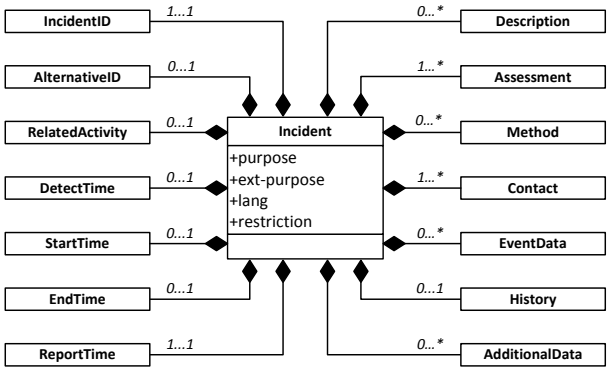


Figure 2. Incident structure defined as IODEF [16].

These properties make the IODEF format the ideal choice to exchange information in social cyber defense alliances. The most important attributes (see overview in Figure 2) to make this model fit to the opportunistic information sharing approach described before, are:

- `Purpose`: Multiple reasons exist why an incident report has been generated. Of particular interest is the `report` class, used to warn other parties about current threats, and the `mitigation` class, used to request mutual aid and support in solving a problem.
- `Restriction`: As outlines earlier, sharing takes place along social relations, potentially even over multiple hops. Thus, the restriction attribute describes the conditions for further sharing. Here, we distinguish at least between `private` which means sharing is just allowed with direct neighbors, `need-to-know` which permits transitive sharing over one intermediate hop, and `public`, which allows sharing with all partners in the alliance.
- `Contact`: This is typically the disseminating party, or any 3rd party from where this incident is originating from (in case of transitively shared reports).
- `EventData`: Sharing policies [13] (via configurable Θ) determine what incidents and how much data is shared (e.g., log file snippets or IDS signatures).

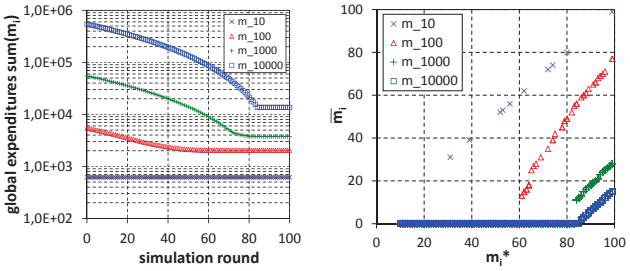
VI. Evaluation and Discussions

The main issue regarding a sophisticated evaluation of our concepts is that the system is not running yet and we therefore lack experience with its applicability. Therefore, we run a combined approach, consisting of a simplified agent-based simulation to study the basic capabilities of our model and the configuration options in a real-world context.

Experiment Setup: We neglect the bootstrapping problem (e.g., covered in [17]) and look at a synthetic social network which would emerge under realistic conditions. For

that purpose, we employ the preferential attachment model [18] to create a graph with power-law distributed node degrees. We then randomly distribute optimal security expenditure levels $m^* = \{10...100\}$ over nodes, combined with random information sharing levels $\Theta = \{0...100\%\}$. For the round-based agent simulation, we initialize $\overline{m} \leftarrow m^*$, and apply varying environmental conditions as described in the following experiments. Essentially, in each simulation round an agent v_i changes its m_i by only ± 1 in order to avoid oscillating behavior due to fast changes of security expenditures.

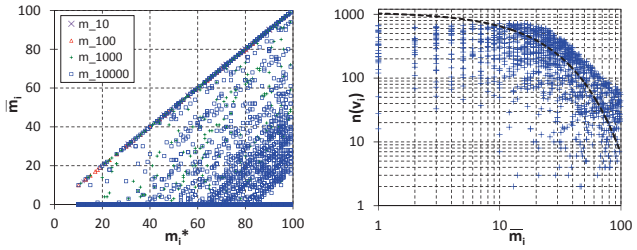
Simple Scenario with Static Sharing Levels: The first experiment ignores the social network and simply distributes shared information to everyone in the alliance (similar to a Web repository). We create alliances of 10, 100, 1000, and 10 000 members. Figure 3(a) shows the evaluation of the global expenditures in the whole alliance over time. Here, Eq. 9 is evaluated once in each simulation round. From a global perspective significant cost reduction can be achieved if everyone has access to everyone else's incident information. Figure 3(b) compares for each single node v_i its individual expenditures if no sharing takes place (m_i^*) and if integrated in the alliance ($\overline{m_i}$). Obviously, the more partners are part of the alliance, the higher is also the potential for individual savings.



(a) $\sum_V \overline{m}$ over time. (b) $\overline{m_i}$ compared to m_i^* for each v_i.

Figure 3. Simple sharing scenario.

Network-based Scenario with Static Sharing Levels: We create alliances of different size again, however connect these members with a scale-free social network, i.e., a graph with power-law distributed node degrees. Sharing takes place only along these links. The experiment is run as before. Figure 4(a) now shows that due to the power-law distribution of node degrees, there are a considerable amount of members who highly benefit ($\overline{m_i} << m_i^*$ along the x-axis) and those who do not benefit at all compared to no sharing (along the first median – since these nodes are simply not well integrated in the network). Figure 4(b) shows the correlation of optimal security expenditures $\overline{m_i}$ (after the simulation run) and their node degrees (i.e., the number of connected neighbors). For the given experiment, we calculated a Pearson correlation coefficient of -0,312, which is not as high as expected, but nevertheless shows a considerable dependency. So we conclude that both figures demonstrate that it is essential for nodes to bring themselves in beneficiary positions within the social network.



(a) $\overline{m_i}$ compared to m_i^* for each v_i. (b) degree of v_i compared to $\overline{m_i}$

Figure 4. Network-based sharing scenario.

Applicability of the Sharing Model in a Real-World Context: We foresee basically two ways to make organizations part of the proposed sharing alliances. First, if there is a legal framework that forces organizations, which provide critical services to the public, to report cyber incidents – similar to reporting obligations of data security breaches in many countries. Second, and from our perspective the more promising way, is to offer them some clear advantage and thus motivate them to participate voluntarily. Today's profit-oriented economy is fundamentally shaped by opportunistic behavior. While it might be comparatively easy to encourage governmental organizations and NPOs to become part of a social cyber defense alliances, there must be clear advantages for business-oriented companies to participate. Examples for such advantages are:

- *Cut Security Expenditures.* Being part of a cyber alliance means that participants receive early warnings from partners about current threats, open vulnerabilities of widely applied COTS, and recently exploited weaknesses in ICT infrastructures. Furthermore, mutual aid and assistance in surviving an attack can be granted among partners. If carefully planned and set up, this will allow for a cut of security expenditures without significantly impacting the security level.
- *Improve Resilience of Business Services.* Even in case a company does not want to decrease security expenditures, active information sharing will lead to an increased situational awareness, thus allow the timely identification of vulnerabilities, and eventually cause more resilient business services. Furthermore, if a company is reliant on partner services being under attack, it might get earlier informed about expected service downtimes, allowing for timely reaction to critical service losses and suffering quality.

While the further detailed mathematical description – apart from the previous section – is given in [14], here we like to discuss the application of this model in the social cyber defense alliance context:

Measurement of Θ*:* One fundamental question is, if the amount of shared information Θ is absolutely measured and compared or relative to the organization's capabilities. For instance, a smaller organization might decide to share all security-related information and can still not contribute as much as a large-scale organization which decided to share only a small portion. The aspect, if parties should know to what extend their partners share information deals with the question if other companies are aware of partner capabilities and their theoretical maximum Θ. In the end, it will not be easy to determine the theoretical maximum amount of shareable information.

Configuration of Θ*:* The described model is well applicable under the assumption that Θ_i is an exogenously assigned (static) factor (e.g., set by governmental policies or laws). One main question however is, what if we let single companies control their respective Θ? For instance if i increases Θ_i due to increasing trust levels, this clearly means for v_j that it could reduce m_j and still keeping P^j at the same level. However, if this happens $m_j^{j \to i}$ will decrease and thus v_i will suffer from a reduced spillover effect. In other words if a party increases the portion of shared information it will eventually suffer from reduced security investments of allied companies.

Network Stability: As long as v_i does not apply an – unlikely – altruistic behavior, we need an efficient mechanism to compensate aforementioned negative effect which would harm the whole alliance. One applicable concept, besides policies, regulations and law, is reciprocity, where v_i and v_j agree on an equal level of sharing in order to maintain a trustworthy business relation. Reciprocity prevents one actor from suddenly changing its Θ and thus, leads to more stable network alliances reflected by the balanced trust relations.

VII. Conclusion and Future Work

In this paper, we described the concept of social cyber defense alliances. The overall aim of this approach is to increase the efficiency with which critical information on security incidents is shared among parties. Here, information sharing is crucial to warn alliance members about ongoing attacks, new malware and detected vulnerabilities. We argue that compared to common manual sharing on open Web platforms, direct and policy-based (semi-)automatic sharing is more efficient because of 1) increased timeleness of reports, i.e., certain types of data can be shared immediately without cross-checking, because personalized relations and a reputation system will effectively avoid hoaxes and spam; 2) personalized sharing allows for the dissemination of sensitive data, such as system log files and company-internal configuration details. We further demonstrated a model that shows how single parties will eventually benefit from this approach and should thus be encouraged to join alliances. A sophisticated technical architecture is required to ensure confidentiality and privacy preservation. For that purpose, our proposed architecture uses a public-key infrastructure with a standardized encryption scheme, and a customized feedback and reputation system.

Future work includes the application of the implemented system in a small-scale real-world pilot case. Here, Austrian SMEs will evaluate the practical usage of incident information sharing and prove its usefulness in daily businesses.

Acknowledgements

This work was partly funded by the Austrian FFG research program KIRAS in course of the project CAIS.

References

[1] G. Ollmann, "The evolution of commercial malware development kits and colour-by-numbers custom malware," *Computer Fraud & Security*, vol. 2008, no. 9, pp. 4–7, 2008.

[2] RSA, "Cybercrime trends report: The current state of cybercrime and what to expect in 2011," Tech. Rep., 2011.

[3] C. Tankard, "Advanced persistent threats and how to monitor and deter them," *Network security*, vol. 2011, no. 8, pp. 16–19, 2011.

[4] C. Miller, "The legitimate vulnerability market: the secretive world of 0-day exploit sales," in *Proceedings of the Workshop on the Economics of Information Security (WEIS)*, 2007, pp. 1–10.

[5] Computer Emergency Response Team (CERT), http://www.cert.org/, December 2012.

[6] F. Skopik, D. Schall, and S. Dustdar, "Modeling and mining of dynamic trust in complex service-oriented systems," *Information Systems*, vol. 35, no. 7, pp. 735–757, 2010.

[7] S. Jajodia, P. Liu, V. Swarup, and C. Wang, *Cyber Situational Awareness: Issues and Research*. Springer, 2009.

[8] U.S. Homeland Security Cyber Security R&D Center, "A roadmap for cybersecurity research," November 2009.

[9] ENISA, "Practical guide/roadmap for a suitable channel for secure communication:secure communication with the CERTs & other stakeholders," December 2011.

[10] Internet Storm Center, http://isc.sans.org/, December 2012.

[11] Arbor Networks, http://www.arbornetworks.com/, December 2012.

[12] A. Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," *Decision Support Systems*, vol. 43, no. 2, pp. 618–644, 2007.

[13] F. Skopik, D. Schall, and S. Dustdar, "Trusted information sharing using soa-based social overlay networks," *International Journal of Computer Science and Applications*, vol. 9, no. 1, pp. 116–151, 2012.

[14] L. A. Gordon, M. P. Loeb, and W. Lucyshyn, "Sharing information on computer systems security: An economic analysis," *Journal of Accounting and Public Policy*, vol. 22, no. 6, pp. 461–485, 2003.

[15] x-arf, http://www.x-arf.org/, December 2012.

[16] R. Danyliw, J. Meijer, and Y. Demchenko, "RFC 5070: Incident Object Description Exchange Format (IODEF)," http://www.ietf.org/rfc/rfc5070.txt, December 2012.

[17] C. Burnett, T. J. Norman, and K. P. Sycara, "Bootstrapping trust evaluations through stereotypes." in *Proceedings of 9th International Conference on Autonomous Agents and Multiagent Systems (AAMAS)*, 2010, pp. 241–248.

[18] A. Reka and Barabási, "Statistical mechanics of complex networks," *Review of Modern Physics*, vol. 74, pp. 47–97, 2002.