2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering

Towards Trustworthy Information Sharing by Creating Cyber Security Alliances

1st Ameneh Deljoo
Informatics Institute, Faculty of Science
University of Amsterdam
Amsterdam, the Netherlands
a.deljoo@uva.nl

2nd Tom van Engers
Leibniz Center for Law
University of Amsterdam
Amsterdam, the Netherlands
vanengers@uva.nl

3rd Ralph koning
Informatics Institute, Faculty of Science
University of Amsterdam
Amsterdam, the Netherlands
r.koning@uva.nl

4th Leon Gommans
AirFrance-KLM
Amsterdam, the Netherlands
leon.gommans@klm.com

5th Cees de Laat
Informatics Institute, Faculty of Science
University of Amsterdam
Amsterdam, the Netherlands
delaat@uva.nl

***Abstract*—As attacks are becoming more and more organized, collaboration amongst network domain owners is required next to arranging technical counter measures. Sharing cyber intelligence amongst network domain owners is, therefore, becoming increasingly important. Additionally, networks have grown scale, complexity, and degree of inter-connectedness, such that their protection can often only be guaranteed and financed as a shared effort. In this paper, we introduce the concept of cyber security alliance shaped by different organizations that facilitate the sharing of incident information across them. Creating a cyber security alliance highlights requirements such as:**

1) **creates and manages trust among the members,**
2) **introduces a federated governance model, creating common policies, standards for alliance's members, and**
3) **provides a strong incentive to partners to join an alliance by introducing a common benefit.**

This paper discusses ongoing research on a social trust model, which helps the members to select the right partner to perform joint tasks, and encourages sharing of incident information. Furthermore, we use the service provider group framework as a way to arrange the establishment of our proposed cyber security alliance that coordinates activities across the alliance to establish trust. We present our social computational trust model and its antecedents.

***Index Terms*—Computational trust, alliances, cyber security, information sharing, service provider group**

I. Introduction

Sharing information across network domain owners and operating IT infrastructures is becoming essential in cyber security. Information sharing helps such organizations in many aspects such as improving individual and collective decision making processes to select optimal cyber defense tactics. Another benefit is the reduction of the uncertainties with regards to the performance and service availability of an individual organization, a whole critical sector, and/or service chain spanning multiple organizations [1]. It is abundantly clear that no organization can address the full spectrum of its cyber security and resilience on its own, as organizations are increasingly globally interconnected and exposed to the same global cyber security threats. Collaboration with partners across organizational, sectoral, and national boundaries, and from small and medium enterprises up to multinationals and governments is therefore required in order to counter cyber security threats, which may negatively impact the organization and its services. A recent study by RSA [2] showed the vast extent of potential exposure to malware and data loss within some of the world's largest organizations. Currently, more than 60 million different malware variants are indexed from which one third came up only in the last year. The reports on cyber security show that attacks become increasingly sophisticated, customized and coordinated. Therefore, organizations need to collaborate and employ targeted and coordinated counter measures [1], [3]. Therefore, we need to create a platform which organizations can share the cyber information with their trusted peers. In this paper, we motivate the need for cyber security alliances, where organizations can form strong partnerships to collaboratively notify about novel threats and protect against corresponding attacks. Many researchers have focused on sophisticated technical means to set up the effective counter measurements (e.g. event logging, correlation over new data and reasoning algorithms and anomaly detection approaches) [4].

In this paper, we focus on the social aspect of information sharing and selecting the right partner to collaborate in the joint tasks. More precisely, we address trust amongst organizations in this paper. In particular, a cyber security alliance requires:

- a common benefit to provide a strong incentive to partners to join an alliance, and encouraging partners to actually share information as sharing outweighing risk,
- a trust framework to create and organize trust among the members,

This work is funded by the Dutch Science Foundation project SARNET (grant no: CYBSEC.14.003/618.001.016) and the Dutch project COMMIT (WP20.11). Special thanks go to our research partner KLM. The authors would also like to thank anonymous reviewers for their comments.

2324-9013/18/31.00 ©2018 IEEE
DOI 10.1109/TrustCom/BigDataSE.2018.00213

- a federated governance model to create common policies, standards for alliance's members.

Tackling these aspects, besides others, is of paramount importance when it comes to sharing potentially sensitive and company-internal information. A well-defined trust model helps to dispel reservations as a mean of reducing risk. However, since such trust relations can hardly be technically enforced, we employ a social model to address this issues. Traditionally, information sharing on a peer-to-peer basis was mostly informative, e.g. through phone calls or free-text e-mail messages. The social network of organizations evolve over time, therefore, we need to define a more sophisticated method to select the trusted peer for sharing the information. Moreover, the exchange of sensitive information is usually shaped by social trust relations [5]. Our model of cyber security alliances aims at transferring the mentioned issues to the cyber space on a large scale.

In this work, we discuss the following contributions:

1) motivation for cyber security alliance setup from the social viewpoint. First, we thoroughly motivate the need for security defense alliances, and subsequently, discuss concrete challenges that need to be addressed.
2) Service Provider Group (SPG) Framework [6]. We use the SPG framework as a common framework to arrange trust by defining a set of rules for the members.
3) social computational trust model. We discuss our proposed social computational trust model. In detail, we present social trust and its antecedents, which are important for creating the alliance and platform to gain momentum by arranging trust.

The remainder of the paper is organized as follows. Section II shows challenges and the problem statement. In section III, we will introduce the SARNET alliance followed by a section IV introducing the SPG framework as a governance model that helps to shape the function of a cyber alliance explaining the role of its common policies and standards as a way of arranging trust. Then, section V highlights the trust model and its components. Finally, section VII concludes the paper.

II. Challenges in Creating Alliances

In reality, there are several risk factors that discourage organizations from sharing information about cyber security incidents that they experience. These factors include:

- competition. An organization is often hesitant to share information with its competitors due to the conflict of interest.
- trust. Organizations have to rely on their partners' performance and remain vulnerable to partners' actions.
- reputation. Public disclosure of security information often damages the reputation of an organization, especially commercial organizations such as financial institutes. This significantly deters them from sharing information with others.
- legal. Alliances consist of different companies with different legal frameworks as they may operate in different countries.

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

III. SARNET Alliance

SARNET (Secure Autonomous Research NETworks) leverages the dynamic properties of novel networking approaches, such as Software Defined Networks and Network Function Virtualization, to provide automatic or assisted response to attacks on network infrastructures and distributed computer systems. SARNET alliance is a collaborative network, which consists of multiple autonomous network domain owners. The aim is to estimate trust where each domain needs to trust other parties to correctly detect and mitigate cyber threats, whilst authorizing each other to be involved. A typical example where collaboration is required is

- a mutual defense against Distributed Denial of Service (DDoS) attacks. In such volumetric DDoS scenarios, the attacker floods the ingress point of the victim's network making it impossible for legitimate traffic to reach the services. The victim domain can only effectively defend if the choking point in the network is on the link to the upstream provider. The only effective response is to ask the upstream domain, who has the equipment of dealing with larger amounts of traffic for help.

In order to organize effective defense strategies, the partners in the SARNET alliance will have to take measures that will be beneficial to their downstream partners, but may negatively impact their own performance and consequently their clients. Deciding to help their partners under attack is based upon the trust that in similar circumstances those partners would take reciprocal actions (quid pro quo). The defense strategy decisions in such an environment do require the organization and evaluation of trust next to the development of effective technical defense mechanisms. The trust framework representing social trust enables the members of such alliance to make the decision about collaborating with other parties. At SC17 [1] we demonstrated how SARNET can be applied in a multi-domain environment. We demonstrated SARNET alliance where each domain needs to trust other parties to share the requested information. Particularly, we focused on implementing the collaboration described in the mentioned example but the focus was in this case on the defensive capabilities. We showed that when there is a collaboration, victims are more capable and, in some cases, more efficient in defending. To make the example work, we used the most ideal form of collaboration: all domains can always fulfill the requests, all domains provide the information requested in a timely manner, requests and responses follow a strict API and, the disclosure level is equal to all. In a more realistic domain,

[1]The technical details of this demonstration can be found here: http://sc.delaat.net/sc17/demo01/index.html

we could not simply assume that everyone is equally good in performing all actions, hence results in the need of extending our simulation environment with a trust framework.

IV. Service Provider Group (SPG)

In this paper, we use the SPG framework that covers some essential elements of collaboration. The SPG represents a group of organizations that act together as one single business delivering a service. The SPG provides one or more services that none of its members could provide on their own. To a user, the SPG appears as a single autonomous provider. To members, the SPG appears as a collaborative group with standards and rules that each member translates into its own conforming policies. The policies regulate the provisioning of the services and the user terms and conditions that are enforced by the group. A user signs a service agreement with a member representing the SPG. The SPG recognize the directorated role that oversees the interactions and inter-operation of its members. Fig. 1 shows the schema of the SPG.

As we mentioned, we use the SPG as a governance framework to manage alliance by creating and maintaining group policies and standards. In our research, the cyber security alliance consists of different SPG's members that collaborate to share an incident information [6]. A priori identification of benefits and risks for each members' alliances is essential. This is a challenging task that needs coordination and oversight to ensure quality and manage risk and liability. Leon Gommans *et al.* [7] described the SPG, as a way to coordinate the collaborative network activities by defining a set of rules which leads to arrange trust between members. The SPG provides a set of rules, which is typically based on each participant personally trusting one another. Trust inherently introduces risk as trust can be disappointed. The risks associated with information sharing and safeguarding are reduced through the adoption of sound policies and standards. Building trust in sharing and safeguarding requires the ability to manage risk [8]. Risk decreases with sound policies and standards, increased awareness and comprehensive training, effective governance, and enhanced accountability.

Instituting the SPG is a way to establish and maintain a common set of inter-organizational rules that are translated into intra-organizational policies such that each entity knows that the policy it is authorizing is correct. In the case of the rule violation, the SGP has an enforcement component that is used to enforce the agreed rules according to the spirit of the group. The authors [7] made the assumptions that protocols, exchanging authorization transactions between organizations will provide enough message confidentiality, authenticity and integrity such that the security of an exchange is never disputed. In this paper, we adopt the SPG framework as a way to define a set of common rules and establish the alliance model. The set of SPG's rules are used to monitor the members' behavior and evaluate trust among each pair of partners. In the previous works, we have presented an agent based model (ABM) to simulate the SPG in order to observe the members' behavior and identify the benefits and risks

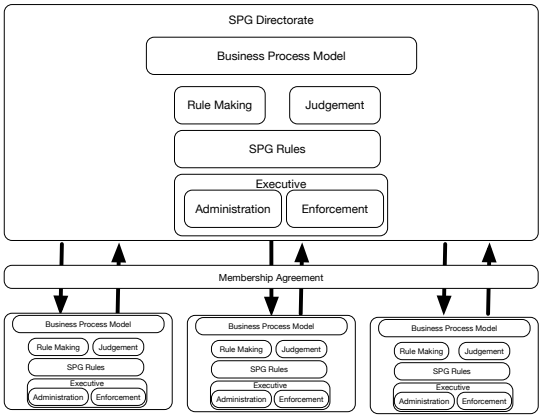

Fig. 1. The SPG framework.

of collaboration for each member [9], [10]. The SPG rules are defined under the assumption and expectation that each member will behave according to these rules. In general the behavioral variance in a society subjected to rules is smaller compared to a non-regulated one, i.e. the behavior is more predictable, therefore the risks for each society member is reduced. The SPG provides a way to justify trust among members by observing the members' behavior, nevertheless, members may not act according to the rules (non-compliant behavior of a member). The set of common rules will be used as input for one of the trust model components, which is presented in the following section.

V. Trust

Trust is an essential part of social interaction. Trust is a broad concept studied in areas such as sociology and psychology [11]. The concept of trust has received ample attention from various disciplines, and although prior research has put forth diverse interpretations of trust, a common core emerges [2]. The following description has been extracted from their studies and used as a definition: "Trust is the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other parties [11]". Building on this prior research, we define inter-organizational trust as the expectation held by one party that the another will not exploit its vulnerabilities when faced with the opportunity to do so [11]–[13]. This expectation is confirmed when parties

- demonstrate competence related to the potential ability of the evaluated entity to do a given task,
- act accordingly to fulfill the commitments (i.e. the SPG rules) even when acting on them is not in self-interest and accept the consequences, and

[2]An elaborated overview of the concepts used within this context can be found in studies performed by Bachmann [8].

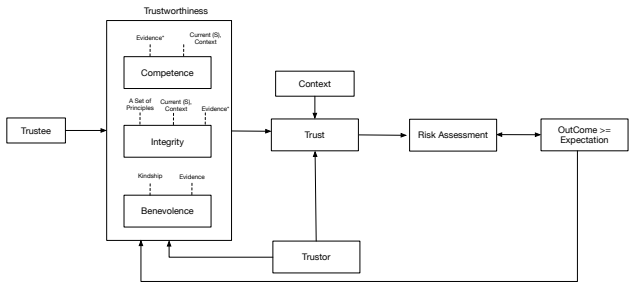

Fig. 2. Trust framework.

- do good and an act of kindness even if unforeseen contingencies arise. We depict the trust framework in Fig. 2.

Our definition thus bases the inter-organizational trust on three related components: competence, integrity, and benevolence which have been proposed by Mayer *et al.* [11]. Computational trust is considered as an enabler technology in virtual societies, and the estimation of trustworthiness is paramount to assess the trust that a trustor agent has on a given trustee. An individual is more or less trustworthy in performing a task in a given situation depending on its ability in the matter, his overall integrity, and the stage of his relationships with the trustor. Therefore, in order to better estimate the trustworthiness of trustees, it is important to consider these three dimensions individually and to combine them in a dynamic way taking into consideration the situation and the development of the relationship. However, the majority of the computational trust approaches presented in literature estimate the trustworthiness of trustees as a block and does not distinguish between these trustees' attributions. In following, we present a computational trust approach grounded on multidisciplinary literature on trust that is able to capture the competence, benevolence, and integrity of the trustee under evaluation.

VI. Our Social Computational Trust Model

In this section, we introduce the social computational trust model. Our aim is to define a mechanism for estimating trustworthiness of a member (i.e. trustee) under evaluation and make decisions about the future relationship with the given member. In the following, we present our method to evaluate trust based on its components (i.e. competence, benevolence, and integrity).

A. Notation

Our generic computational trust model is applied to environments where trustor agents select the best trustees to interact with, with the posterior establishment of dyadic agreements between partners.

Therefore, we define the society of agents A, which includes trustee and trustor $x, y \in A$. In this research, each selected member can be represented as a trustee or trustor. We represent $T_{(x,y)}$ as the amount of trust x has upon y with respect to a situation s_i, where $s_i \in S = \{s_1, s_2, ..., s_N\}$ is the set of all the possible situations in the society. In the following, we assign values to each situation ($s_i \in S$). The outcome of interactions between trustor (x) and trustee (y) is called evidence (E). We define a set of evidence ($e_i \in E$) and assign value to each evidence where ($e_i \in [0, 1]$). Finally, the set of all the existing evidence on a given trustee is represented by $E_{(*,y)}$. Following, $E_{(x,y)}$ shows all the evidence about the direct interactions between trustor (x) and trustee (y).

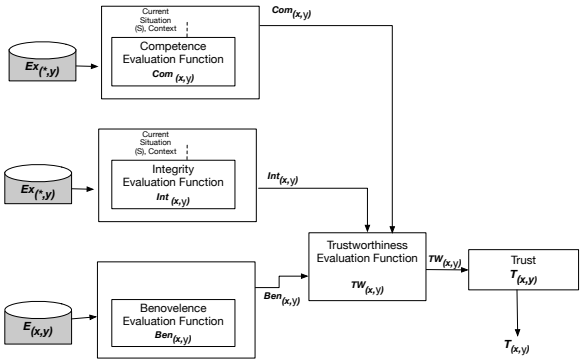

Fig. 3. Social computational model of trust.

B. Social Computational Trust Model

The social computational model of trust that we present in this paper integrates three distinct functions: the competence evaluation function ($Com_{(x,y)} : S \times Ex_{(*,y)} \in [0, 1]$), the benevolence evaluation function ($Ben_{(x,y)} : E_{(x,y)} \in [0, 1]$), and the integrity evaluation function ($Int_{(x,y)} : S \times Ex_{(*,y)} \in [0, 1]$). The function shown in Equation 1 returns the estimated value of the trust that trustor x has in trustee y in situation s.

$$T_{(x,y)} : Ben_{(x,y)} \times Com_{(x,y)} \times Int_{(x,y)}. \quad (1)$$

We illustrated the computational model in Fig. 3.

C. Benevolence function

Benevolence is considered as a key element of trust and an antecedent of trustworthiness by several scholars(e.g. [14], [15]). The estimated value of the benevolence of trustee (x) toward trustor (y), $Ben_{(x,y)}$, is derived from the direct interactions (i.e. $E_{(x,y)}$) between trustee and trustor in the situations $s_i (s_i \in S)$. The output of the benevolence evaluation function $Ben_{(x,y)}$, defined in $[0, 1]$, is.

$$Ben_{(x,y)} = \frac{1}{|S|} \sum_{E_{x,y}} (val(E_{x,y})). \quad (2)$$

Where S is the set of situations, in which x has interactions with y.

D. Integrity function

The Integrity evaluation function $Intx_{(x,y)}$ estimates the general integrity of the trustee under evaluation in performing a given task t in a specific situation s_i. This function takes as input all the evidence available on the trustee under evaluation,

$Ex_{(*,y)}$. The output of the integrity evaluation function is in the range of $[0, 1]$.

$$Intx_{(x,y)} = \frac{1}{|S|} \sum_{s_i \in S} (val(E_{*,y})). \quad (3)$$

E. Competence function

The competence evaluation function $Com_{(x,y)}$ estimates the general ability of the trustee under evaluation in performing a given task t in a specific situation s_i. This function takes as input all the evidence available on the trustee under evaluation, $Ex_{(*,y)}$. The output of the competence evaluation function is the estimated competence of the agent, $Com_{(x,y)}$, defined in $[0, 1]$. Competence, as risk, involves an agent making a judgment about the trustee's ability to perform the given task. We consider three different possible situations to evaluate trustee's ability.

1) There is no evidence available from the trustee. To judge the trustee's competence, the trustor will calculate the risk of trusting a stranger and decide based on the risk.
2) Situation β: there are some evidence but not for the considered context. In this situation, the trustor collects all the evidence from other agents and evaluates the competence of trustee based on them.

$$Com = \frac{1}{|N|} \sum_{\beta \in N} (val(E_{*,y}) \times \widehat{T}_x(y, \beta)), \quad (4)$$

where $\widehat{T_x(y, \beta)}$ denotes the basic trust that x has on y and β is the set of all situations in which x has had interactions with y. This basic trust y calculated as $1 \,/\, |N| \sum_{\beta \in N} T_x(y)$. N denotes as the set of situations similar to the present situation (S) in which x has interactions with y.

3) Situation α: there is related evidence about the agent in this or similar context.

$$Com = \frac{1}{|N|} \sum_{\alpha \in N} (val(E_{*,y})), \quad (5)$$

where α is the set of all situations in which x has interactions with y. There are three possible situations to consider (no evidence available, β and α) as mentioned above to help an individual to make the decision.

VII. Conclusion and Discussion

In this paper, we described the concept of cyber defense alliances. The overall aim of this approach is to help the organization to share critical information on security incidents amongst trusted parties and increase the efficiency. Information sharing is crucial for alliance members to give insights into ongoing attacks, new malware and detected vulnerabilities. We proposed a social computational trust model that can help alliances' members to estimate trustworthiness of a given trustee and make decisions based on that. Our proposed computational trust model consists of three different components called competence, integrity and benevolence; this computational model will help each member to evaluate trust in a more accurate way. We aim to implement the proposed trust model in the SARNET alliance case study. The future work is to test our proposed cyber defense alliance in a real-world context and evaluate its applicability using our ABM environment in the ongoing research project.

References

[1] T. A. Cellucci and M. C. C. Officer, "Innovative public private partnerships," 2010.

[2] RSA. Current state of cybercrime. [Online]. Available: https://www.rsa.com/content/dam/en/white-paper/2018-current-state-of-cybercrime.pdf

[3] R. Koning, A. Deljoo, S. Trajanovski, B. de Graaff, P. Grosso, L. Gommans, T. van Engers, F. Fransen, R. Meijer, R. Wilson *et al.*, "Enabling e-science applications with dynamic optical networks: Secure autonomous response networks," in *Optical Fiber Communications Conference and Exhibition (OFC), 2017*. IEEE, 2017, pp. 1–3.

[4] R. Koning, B. De Graaff, R. Meijer, C. De Laat, and P. Grosso, "Measuring the effectiveness of sdn mitigations against cyber attacks," in *IEEE Conference on Network Softwarization (NetSoft), 2017*. IEEE, 2017, pp. 1–6.

[5] F. Skopik, D. Schall, and S. Dustdar, "Modeling and mining of dynamic trust in complex service-oriented systems," in *Socially Enhanced Services Computing*. Springer, 2011, pp. 29–75.

[6] A. Deljoo, L. Gommans, C. de Laat, and T. van Engers, "The service provider group framework." in *Looking Beyond the Internet: Workshop on Software-defined Infrastructure and Software-defined Exchanges,2016*. Flux Research Group, University of Utah, 2016.

[7] L. Gommans, J. Vollbrecht, B. Gommans-de Bruijn, and C. de Laat, "The service provider group framework: A framework for arranging trust and power to facilitate authorization of network services," *Future Generation Computer Systems*, vol. 45, pp. 176–192, 2015.

[8] R. Bachmann, "Trust, power and control in trans-organizational relations," *Organization studies*, vol. 22, no. 2, pp. 337–365, 2001.

[9] A. Deljoo, L. Gommans, T. van Engers, and C. de Laat, "An agent-based framework for multi-domain service networks: Eduroam case study," in *The 8th International Conference on Agents and Artificial Intelligence (ICAART'16)*, 2016, pp. 275–280.

[10] A. Deljoo, L. Gommans, C. de Laat, and T. van Engers, "What is going on: Utility-based plan selection in bdi agents," in *The AAAI-17 Workshop on Knowledge-Based Techniques for Problem Solving and Reasoning WS-17-12*, 2017.

[11] R. C. Mayer, J. H. Davis, and F. D. Schoorman, "An integrative model of organizational trust," *Academy of management review*, vol. 20, no. 3, pp. 709–734, 1995.

[12] J. B. Barney and M. H. Hansen, "Trustworthiness as a source of competitive advantage," *Strategic management journal*, vol. 15, no. S1, pp. 175–190, 1994.

[13] R. Krishnan, X. Martin, and N. G. Noorderhaven, "When does trust matter to alliance performance?" *Academy of Management journal*, vol. 49, no. 5, pp. 894–917, 2006.

[14] D. Z. Levin, R. Cross, L. C. Abrams, and E. L. Lesser, "Trust and knowledge sharing: A critical combination," *IBM Institute for Knowledge-Based Organizations*, vol. 19, 2002.

[15] T. R. Koscik and D. Tranel, "The human amygdala is necessary for developing and expressing normal interpersonal trust," *Neuropsychologia*, vol. 49, no. 4, pp. 602–611, 2011.