Enabling E-Science Applications with Dynamic Optical Networks

Secure Autonomous Response Networks

R. Koning[1], A. Deljoo[1], S. Trajanovski[1], B. de Graaff[1], P. Grosso[1], L. Gommans[2,1], T. van Engers[1], F. Fransen[3], R. Meijer[3], R. Wilson[4], and C. de Laat[1]

[1]University of Amsterdam, FNWI, Science Park 904 Amsterdam, The Netherlands [2]Air france–KLM, Tupolevlaan 2–24a Schiphol-Rijk, Amsterdam, The Netherlands [3]TNO, Eemsgolaan 3, Groningen, The Netherlands[4]Ciena, 5050 Innovation Drive, Ottawa, Canada

{*R.Koning,A.Deljoo,S.Trajanovski,B.deGraaff,P.Grosso,T.M.vanEngers,delaat*}*@uva.nl, Leon.Gommans@klm.com,* {*frank.fransen,robert.meijer*}*@tno.nl,rwilson@ciena.com*

Abstract: Secure Autonomous Response NETworks (SARNET) is a framework for automated response against attacks on computer network infrastructures. The framework addresses several cyber-security problems at three crucial levels: strategic, tactical and operational.

OCIS codes: 060.0060, 060.4250.

1. Introduction

By means of Secure Autonomous Response NETworks (SARNETs), we provide a framework to address cyber attacks autonomously and decrease response complexity by offering automated defense mechanisms for computer networks. The complexity of cyber attacks has in fact increased and this makes effective defense strategies more difficult. Given that attacks are nowadays made accessible by using attacks-as-a-service [1], it becomes imperative that similar approaches are available for defense. Defense tactics are complex because the defender has to make decisions to recover using limited resources and attack knowledge which might incur in additional monetary risks. A SARNET addresses the defense complexity by responding autonomously using the knowledge and resource sharing that are implemented by forming SARNET Alliances.

2. SARNET

Our research goal is to obtain the knowledge to create ICT systems that model their state, discover by observations and reasoning if and how an attack is developing and calculate the associated risks. In addition, we apply the domain knowledge to calculate the effect and risk of counter measures such that we can choose and execute one.

In SARNET we recognize that resolving cyber security problems is not just an operational problem that can be resolved by an engineering team, but requires coordination on all levels within an organization: Strategic, Tactical and Operational, see Fig. 1. In order to execute automated response, business values, risks, and policies need to be translated into a set of rules that can be used by the tactical level to determine the set of actions required on the operational level when such an attack occurs.

2.1. Strategic

At the strategic level, we aim to set policies expressed as a set of rules that guide and constrain the effective defense strategies against cyber attacks that are operationalized at the tactical level. These strategies can be related to a single organization, or to multiple organizations that collaborate with interconnected SARNETs. We intend to develop a computational model that allows us to check the impact on organizations by the (non-)compliancy of its members. Such a model can help us to find the best strategies against attacks and consequently will help organizations in minimizing their risks. However, to detect and mitigate an attack (e.g., Distributed Denial of Service) correctly, the members need to collaborate with each other. The members mentioned here may be organizations themselves, such as Internet Service Providers (ISP_s), Enterprise Networks, and Service Providers (SP_s). To create and maintain effective collaboration, each member organization must trust the other members to detect and mitigate threats and operate according to the agreed defense policy. In our SARNET alliance research (Sec. 3) we address trust across multiple domains.

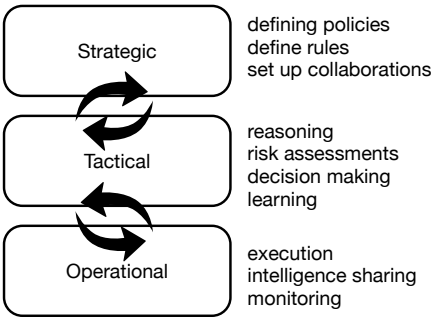

Fig. 1: SARNETs exhibit coordinated response on three levels: strategic, tactical, operational.

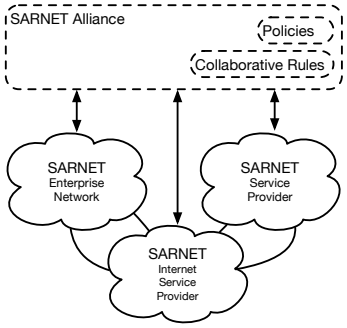

Fig. 2: A SARNET alliance enforces a common set of rules on collaborating networks.

2.2. *Tactical*

At the tactical level, we aim to find a response scenario that can prevent or mitigate the negative effects of an attack on the network. Ideally, the network should autonomously anticipate new threats by taking preventative measures, by containing the attack, and to recover efficiently from the attack. Determining the best possible response depends not only the attack itself but also depends on the environment, costs, and the risks of applying countermeasures. Therefore, it is key to learn from past attacks and from the solutions previously implemented.

We started by looking at the DDoS scenario described in Sec. 2.3. Our goal is to maximize the legitimate flows from clients to services while reducing flows from the attackers with minimum cost. Some actions provided by the operational level are: (i) add a new link from the list of permitted/possible links; (ii) remove a currently in use link; (iii) scale (increase or decrease) the link capacity; (iv) filter a flow between two nodes on an intermediate link. There are additional constraints and decision variables to preserve legitimate traffic flows: the maximum number of added, removed, or filtered links, and insurance measures to prevent consistency issues. Due to the link addition and removal actions, the optimization problem is non-linear and therefore difficult to solve. The important tasks here are: (i) finding an exact algorithm as well as heuristics to solve the optimization problem, and (ii) compare their performance in terms of accuracy and runtime in practice.

2.3. *Operational*

To obtain an autonomous response we expect a certain controllability and flexibility from a network. Cloud facilities in combination with dynamic optical networks, Software Defined Networking (SDN), and Network Function Virtualization (NFV) provide this flexibility by allowing on demand instantiation of resources. This software defined infrastructure allows the SARNET to adapt and scale up or out when required.

Strijkers et al. [2] proposed to express and use network components as objects in a programming language such that interaction with these objects results in underlying network changes. This approach enables the development of 'control programs' that can force the network to behave according to a predetermined set of rules and policies. These control programs can be used to ensure that certain security conditions are met.

At Super Computing 2015 we explored some of the primitives that an SDN can provide by implementing them in an interactive visualization environment [3]. The environment showed a Distributed Denial of Service attack against a web service. The user was asked to defend by using the primitives provided by the SDN (block, filter, scale up/down) in any location in the network such that the impact of the attack is minimized. The defense was focused on the recovery of virtual revenue; the user had to make decisions to keep the costs of the defense low and consider the trade-off between the effectiveness and the risk of applying a countermeasure. Ultimately, in order for autonomous response to take place, these decisions need to be made by the tactical layer.

Another task of the operational layer is to provide the correct information to the tactical layer, which in turn can make comprehensive decisions. This information can include an inventory of physical and virtual systems, network topology information, monitoring information. Van der Ham et al. provide an overview of information models [4] that include models suitable to contain topology and monitoring information. Another source of information comes from Intrusion Detection Systems (IDS). IDS systems detect suspicious activities that on the network that can be part of an

attack. These events are usually stored in Security Information and Event Management (SIEM) systems to correlate generated events. To provide more context to such an event, we worked on CoreFlow [5], a system that is built to correlate events to non-event data from a variety of sources (e.g. NetFlow) and appends this data to the event for a richer view on what caused the event.

3. SARNET Alliance

A SARNET Alliance organizes SARNET functionalities across multiple Service Providers (SPs) and Enterprise Networks, where each participant must collaborate with and consequently be able to trust the other participants to detect and mitigate cyber threats autonomously as well as in a collaboration, see Fig 2. The goal of the SARNET alliance is the creation of business value out of the collaboration between SARNET members in terms of risk reduction, cost benefits, and revenue impact. The distributed computational models we develop will provide a-priori insight into the rationale of collaboration. Based on the Service Provider Group framework (SPG) [6], the SARNET alliance institutionalizes trust by arranging common rules, their execution, and judgment [7]. Our models of alliances can be used to analyze the individual policies that each autonomous member constructs from the alliance policy expressed as a common set of rules and the emerging effects on the alliance as a whole.

We proposed a computational framework implemented as an agent based model representing the organizations and their relationships with other stakeholders [8]. This model helps us to study the behavior of alliances that emerges from the behavior of its individual members. The model also enables us to test the effectiveness of alternative SARNET policies and strategies to monitor and to identify (non-)compliant members according to the collaborative rules. From these models we can derive components that will become part of an information security management system that establishes, reviews, maintains, and improves information security among SARNET alliance members.

4. Conclusion

SARNET solves current cyber security problems by utilizing SDN technologies to enable autonomous response capabilities on network infrastructures. SARNET recognizes that automated response requires coordination between the strategic, tactical, and operational layers. SARNET alliances establish governance structures that define the policies, rules, and agreements and provides the coordination that enables SARNETs to share intelligence and exhibit comprehensive multi–domain responses. This coordinated automated response enables SARNET alliances to defend against developing attacks before they reach their peak and become a threat to one of the participating SARNETs.

5. Acknowledgments

This work is funded by the Dutch Science Foundation project SARNET (grant no: CYBSEC.14.003/618.001.016) and by the Dutch project COMMIT (WP20.11).

References

1. J. J. Santanna *et al.*, “Booters: An analysis of ddos-as-a-service attacks,” in “2015 IFIP/IEEE International Symposium on Integrated Network Management (IM),” (IEEE, 2015), pp. 243–251.
2. R. Strijkers *et al.*, “Internet factories: Creating application-specific networks on-demand,” Computer Networks **68**, 187–198 (2014).
3. R. Koning *et al.*, “Interactive analysis of sdn-driven defence against distributed denial of service attacks,” in “2016 IEEE NetSoft Conference and Workshops (NetSoft),” (IEEE, 2016), pp. 483–488.
4. J. van der Ham *et al.*, “Trends in computer network modeling towards the future internet,” CoRR **abs/1402.3951** (2014).
5. R. Koning, *et al.*, “Coreflow: Enriching bro security events using network traffic monitoring data,” INDIS workshop at SC16 (2016).
6. L. Gommans *et al.*, “The service provider group framework: A framework for arranging trust and power to facilitate authorization of network services,” FGCS **45**, 176–192 (2015).
7. A. Deljoo *et al.*, “Regulating complex adaptive systems: Towards a computational model for simulating the effects of rules,” in “Proc. of International Conference, CCS 2016,” (2016).
8. A. Deljoo *et al.*, “An agent-based framework for multi-domain service networks,” (2016).