TECHNISCHE UNIVERSITÄT
CHEMNITZ

Faculty of Electrical Engineering and Information Technology

Professorship of Communication Networks

Master Thesis

Autonomous security response orchestration with machine learning-based traffic prediction for programmable networks

for the fulfillment of the academic degree

M.Sc. in 'Information and Communication Systems'

Vibha R Goutham

Chemnitz, 1st Jan 2020

Supervisor : Prof.Dr.Ing-.Thomas Bauschert
Supervisor : Mr. Trung Phan Van

Declaration

I hereby declare that this Master's thesis titled "*Autonomous security response orchestration with machine learning-based traffic prediction for programmable networks*" is my own independent work. This work has not been, in part or in whole, presented or published elsewhere for academic assessment. Any form of content or information by other sources or authors that is used in this report is explicitly acknowledged or referred.

Chemnitz, 1st Jan 2020

_____

Vibha R Goutham

Acknowledgments

Add Acknowledgments later!

Abstract

The advent of Internet has impacted the world in an irreversible manner. The global network of interconnected computers opened up the virtual domain of cyberspace. The fast evolving domain of cyberspace, in the past few decades, has impacted people's lives in unimaginable ways while also making innumerable mundane tasks fairly simple. The speed at which the cyber world continues to advance marks a testament to the technological affiliations of the modern world but the malicious use of the same reminds the downside as is the case with most present day technologies. The nature and complexity of cyber-attacks is growing prominently as fast as the advance in Internet technologies itself making cybersecurity a vital area of research. This stresses on the need to tackle cyber-attacks and respond to them at speeds beyond human capabilities and necessitates for security functions to be automated. The focus of this thesis is to develop an automated security function using virtualization techniques to aide in dealing with a certain kind of cybersecurity threat. In the course of this research, a desired security function was designed, implemented, deployed and further analysis was performed using machine learning.

Contents

1. Introduction

1.1. Motivation

The Internet and the World Wide Web(WWW) are among the most successful inventions of the modern world and has been a medium to access information. People relying on the Internet has been a phenomenon like one seen never before. Internet is not only a source of entertainment but also a medium for the functioning of various domains such as secure banking and investment, healthcare, education while also critical for military and defence strategies. With the advent of 5G mobile technology the number of smartphone users is estimated to increase even further. This emphasizes on providing reliable service to end users and further stresses on the need for secure communication. Meanwhile, in the past several new age complex cyber-attacks have proved a serious threat by impacting critical businesses ranging from several minutes to few hours incurring huge financial losses. Cybersecurity, thus becomes an absolutely necessary field of research for these reasons. To deal with new age attacks, automating security functions with lower response times becomes essential to detect and deflect complex threats which in turn minimizes human intervention as much as possible. This thesis takes place in the context of NWO SARNET project on Security Autonomous Response with programmable NETworks [SARNET], a Dutch research collaboration project between research organizations including TNO, Netherlands. SARNET will be discussed in more detail in the next chapter. Further, traffic prediction and analysis for the cyber-threat was performed under the Chair of Communication Networks at TU Chemnitz, Germany.

1.2. Aim of the Thesis

Data ex-filtration is a type of cyber-attack type involving unauthorized copying, transfer or retrieval of data from a computer or server. The thesis aims at developing an automated security function focusing on providing a solution to a cyber-security threat of data exfiltration. In the course of this project, a model of an attacker-victim was set-up on a virtual switching domain. The aim at first is to detect the onset of the attack based on traffic volume prediction using machine learning techniques. For this purpose, customized malicious traffic data sets are used to train and test the machine learning algorithm in order to predict future malicious behavior in the network. Secondly, the aim is to mitigate the attack by transferring the infected traffic and/or infected node to a safe node over an encrypted secure medium. At the safe node, further inspection about the nature of attack or the attacker can be performed. The goal is also to achieve the transfer of the infected traffic or node to a safe node without providing any knowledge of the aforementioned actions to the attacker in question. The automated

security function is designed by combining the principles of SDN, NFV and orchestration. The traffic prediction analysis performed is discussed as attack detection and the design, implementation, deployment of the automated security function in the orchestrated cloud is discussed as attack mitigation. The detection and mitigation plan together forms the crux of this thesis and will be discussed in the subsequent chapters.

1.3. Structure of the Thesis

This thesis begins with the chapter of introduction, the motivation and aim of this thesis that presents the reader an understanding and the need for the security function to be developed. The second chapter covers an overview that presents definition for cyber attack and lists its types while also discussing about cyber security. Further in the third chapter, a theoretical detailing is provided on underlying concepts of SDN, NFV, security orchestration among other principles the course of the project relies on. Also here, the security function design and use cases are discussed in detail. Subsequently, in the next two chapters, the attack detection and attack mitigation is presented respectively. In the attack detection chapter, machine learning algorithm and techniques used to achieve traffic prediction are elaborated, while the attack mitigation chapter explains the implementation of the security function and offers automated mitigation plan in the form of security orchestrator playbooks. In the sixth chapter, results are presented with further statistical analysis and its evaluation is recorded. Finally, the seventh and the last chapter summarizes with a conclusion and outlook of the thesis.

2. An Overview on Cyber-security

2.1. A definition of cyber-attack

The foremost challenge in addressing a problem is to estimate the nature and scope while specifying its inclusions and exclusions leading to a formal definition. A variety of definitions have been applied to cyber-attacks as cyberspace pursuits deviate from traditional principles and classification. Although several definitions aim to convey a similar meaning, it is all the more important to define cyber-attacks so that a legal framework is formulated to deal with it. In this section, two definitions are presented below.

The UK based legal publishers, Practical Law Company (PLC) defines cyber-attack as 'an attack initiated from a computer against a website, computer system or individual computer (collectively, a computer) that compromises the confidentiality, integrity or availability of the computer or information stored on it' [1]. Deriving from this definition, the CIA triad model is formed comprising of Confidentiality, Integrity and Availability that steers information security policies for organizations. Confidentiality underlines the access of sensitive information by intended users and preventing access to ones it is not intended for. Integrity ensures prevention of data altering by un-authorized users and maintaining accuracy throughout the process cycle. Availability emphasizes on hardware and software resource maintenance and prompt recovery of faulty resources to ensure continued use of resources. Further, dealing with cyber-attacks is discussed in [1], which states that procedures for investigating and responding to a cyber-attack depends largely on the nature of the attack itself.

Cyber-attacks has been proposed in [2] as 'any form of assault or retreat operation engage by individuals or organizations that focus on computer information systems, infrastructures, computer networks, and/or personal computer devices by various means of malevolent acts usually originating from an unidentified source that either steals, alters, or destroys a specified target by hacking into a susceptible system'. This provides an insight to interpret activities of cyber-attack perpetrators and to begin understanding laws accorded by existing legal bodies. It is interesting to note that the Shangai Cooperation Organization comprising China, Russia and other South-Asian observing countries such as India, Iran, and Pakistan recognizes cyber-attacks in a different perspective from that of the U.S. National Research Council as reviewed in [2].

Cyber-crime is a computer-oriented crime where the computer or Internet is used to carry out a malicious activity or is the target in itself. Complaints such as human traffickers using the internet to lure victims, illicit drug business, and cyber-bullying are a few examples of identified cyber-crimes. A cybercriminal(s) is an individual or organization performing malice due to an ulterior motive to gain unauthorized access to or make unauthorized use of an asset. Cyber-attacks in the past have demonstrated that varied motives lead to execution of such

attacks. Large scale cyber-attacks carried out with specific political, military or commercial interest have been accused of being State-sponsored attacks. Hacktivist is an Internet coined word for individuals or group who hack the cyberspace to promote a social, political or religious agenda. An Insider threat is also a commonly observed attack type where an employee or third-party worker of an organization performs a deliberate malicious action but could also arise out of negligence or by accident. Countries across the world have dedicated cyber cells working in co-operation with police, prosecutors and judges to understand such crimes and punish perpetrators. However, the United Nations Organization (UNO) notes [3] that out of 194 member states of the United Nation Conference on Trade and Development (UNCTAD), 138 countries have enacted cyber-crime legislations and more than 30 countries have no legislation in place. On comparing E-Commerce legislations worldwide, the report states 79% of countries have adopted E-Transaction laws and 52% have consumer protection laws. Also, while 72% of countries have adopted legislation for cyber-crime, only 58% have data protection and privacy legislation in place.

2.1.1. Vulnerabilities and Threats

A system that adheres to the CIA triad model of Confidentiality, Integrity and Availability for data and resources is considered to be secure as stated in [1]. and noted earlier in this chapter. The systems that defy either one of the three components of the CIA triad model is said to be compromised [4]. Hence, such systems that fail to comply with the model are often easily subjected to possible risks which therefore are recognized to be classified as threats and vulnerabilities. The systems that come under threats result in being exploited. In table 2.1, commonly encountered threats are discussed. An existing shortcoming in systems often leads to threats discussed here. Further, the state of systems being exposed to weakness of being attacked or harmed is therefore termed as vulnerability. In table 2.2, vulnerabilities commonly found in electronic systems [4] are broadly differentiated and discussed.

Table 2.1.: Threats

Type	Description
Unstructured Threats	Developed by security administrators or developers to identify loopholes and to ensure robustness.
Structured Threats	Deliberate attempts by hackers using advanced techniques.
External Threats	Arising from people who are not indigenous to a network or system and are trying to gain access for the same.
Internal Threats	Originated from authorized or unauthorized access, but arising from within the system or network.

Table 2.2.: Vulnerabilties

Type	Description
Network Technology weakness	Arising out of unsecure network equipment such as routers, switches and firewalls; on badly designed or installed unpatched operating systems with security loopholes; on bug-laden applications or databases; lack of built-in security mechanism on the TCP/IP protocol such as HTTP, FTP, SNMP, etc.
Configuration weakness	Due to unsecure user accounts exposing critical account information; weakly configured DNS authentication systems; common or easy passwords that can be cracked; adhering to default settings of products ridden with vulnerable settings.
Security Policy weakness	Arising from poorly drafted security policies due to insufficient monitoring and auditing; insufficiently informed security administrators or end-users; missing disaster recovery action plan.

2.1.2. Types of cyber-attack

The chapter initially presented prevalent definitions of cyber-attacks and how consequences of the vulnerabilities of a system and threats encountered can lead to a cyber attack. It is important to also note the types of such existing attacks. With the advent of cyber security measures While various new ways of attacks are continuously being invented, some of the types of cyber-attacks are noted in [5]. Commonly observed attack types are listed below.

- Data exfiltration: A type of attack involving the malicious activity of copying, retrieving or transferring of data by an unauthorized user. Also, leakage of sensitive data to an unauthorized entity by an external threat leading to data theft can be noted here. Advanced Persistent Threats (APTs) can be mentioned here, which is an advanced attack type where the primary goal is data exfiltration and a continuous effort to steal restricted company or organizational data.
- Malware: A collective word used to describe an attack type comprising of notorious and rogue software that includes ransomware, spyware, viruses and worms is broadly called as malware. It encashes on an existing system vulnerability resulting in blocking access or disrupting parts of the network, transferring data from the hard drive of the computer or installing unnecessary, harmful software. Typically the attack can arise when a suspicious email attachment or a malicious link is clicked on.
- Phishing: An attack type that relies on fraudulent communication, mostly email, coaxing users to reveal personal information such as passwords or bank details and in turn gaining unauthorized access to the system for performing malicious activity.
- Man-in-the-middle attack: In simpler terms this attack type is known as eavesdropping, where an unauthorized person thrusts between an ongoing transaction between two

parties and aims to filter or steal data. This attack type can be observed commonly on unprotected public Wi-Fi networks. Session hijacking, IP spoofing are common examples.

- Denial-of-service attack: The attacker overloads the system with enormous number of valid requests such that system or network is flooded and in turn becomes incapable of fulfilling them. This attack exhausts resources and bandwidth making sure any future genuine request cannot be completed either. Distributed-denial-of-service (DDoS) is a popular attack type where several already compromised systems are used to deny service to users. Teardrop and Smurf attack are other examples.

- Zero-day exploit: When a network vulnerability is detected or announced usually, there exists a window of time where a patch or an update is implemented to rectify it. A zero-day exploit abuses this disclosed window to carry out an attack.

- Drive-by attack: Attackers identify insecure websites to position malicious script containing HTTP or PHP code. This attack type does not require an active action from the victim's end but on simply visiting such suspicious websites, malware gets installed on the user's system.

- Password attack: The most common form of authentication end users have are passwords. Stealing passwords can have systematic approaches such as sniffing insecure connection to track unencrypted passwords; using a random approach of using 'brute-force' to try and test possible passwords; using a dictionary to guess and gain access to a system called as the 'dictionary attack'.

2.2. Cyber-crimes in the past

Cyber incidents targeting Government institutions, defence and infrastructure companies, economic and technology companies have been repeatedly observed in the past. A study made by Centre for Strategic and International Studies (CSIR) records cyber incidents since 2006, [6] comparing countries being targets against them being victims as shown in Fig. 2.1.

Based on possible motivation and specified targets cyber-attacks have been further classified as listed in [7]. These attack types are listed below while also noting relevant incidents that have had impact and been popular in the past.

- Attacks aimed at Nation States:
  Countries are targeted specifically with cyber-attacks aiming to derange normal functioning. In 2007, Estonia was targeted by Distributed Denial of Service (DDoS) attack by the Russian Government when the former decided to remove a Soviet World War II memorial in Tallinn [8]. While commoners were unable to access the Internet or their bank accounts it was reported that the Estonian President and parliament websites, Government ministries, media houses were also the targets. Recently, in January 2019 Iran was alleged to be involved in a global DNS hijacking campaign in the North America,

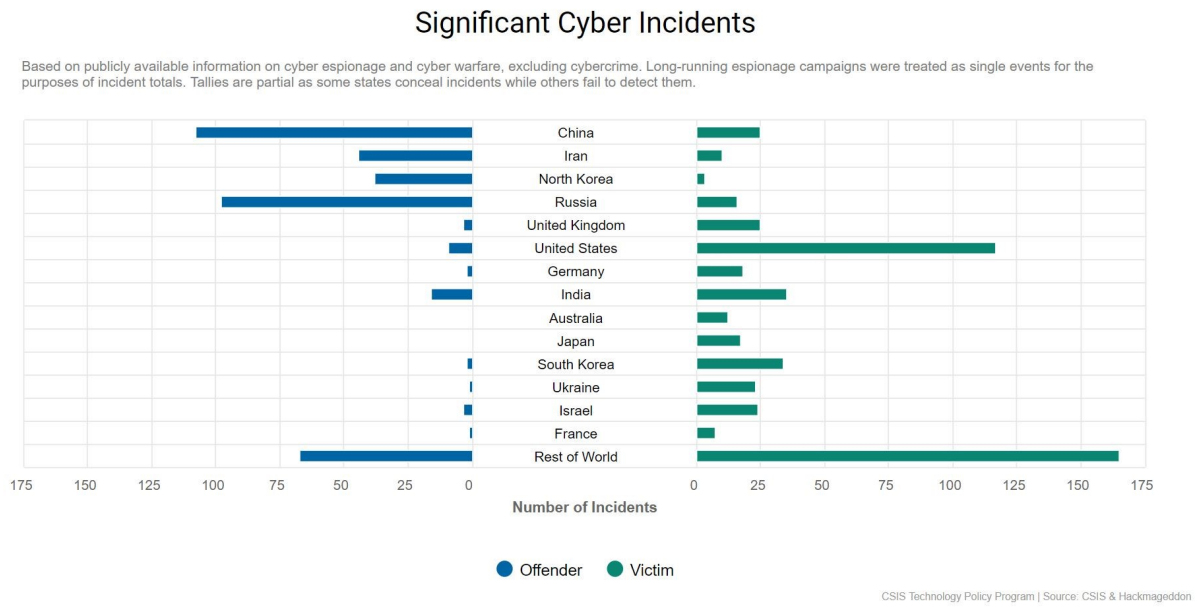

Figure 2.1.: Countries involved in cyber incidents as offender vs. as victim.

Europe and Middle East where target victims were Internet and telecommunications service providers and Government agencies [9].

- Attacks on National security:
  Cyber-attacks are reported on Government institutions, military and defence networks to procure information and to alter engagements that are political, strategic or military among other vital areas. In February 2019, Airbus, the European aerospace company reported theft of personal and IT access related information of European employees by Chinese hackers. Earlier in January 2019, a North Korean botnet was interrupted and taken down by the U.S.A following perpetrated attacks on its media houses, aerospace and financial sectors. Lockheed Martin, an American based global defence, aerospace and security company was under a cyber-attack in 2011 that brought one of its networks down for a week. Data from the SecurID, a RSA based security system was breached. The Department of Defence and the Homeland Security assisted in analysing and mitigating the attack [9].

- Attacks aimed at critical infrastructure:
  The network of systems and assets that are necessary for continued operation of a country to maintain its security, public safety and health, economy, oil and energy is termed by Governments as critical infrastructure. An incident in 2010 where a cyber-worm, Stuxnet was used to infiltrate a nuclear plant in Iran demonstrates this type of attack. The worm was undetected by security systems which made its way to machine controlling software. It targeted Centrifuges that spin material at high speeds and were isolating Uranium types used in nuclear weapons. As a result, infected machines were

disintegrated and further decommissioned by the Government of Iran [10].

- Attacks aimed at companies:
  Several organizations in the sectors of banking, finance, technology, communications and private sector companies are targeted by cyber-attacks from foreign Nations or from within one's own country. In 2018, Google experienced a data diversion attack that re-routed traffic via servers in Russia, China and Nigeria and was reported as a consequence of gateway protocol hijacking attack. As a result, access to a few Google services were impacted [11].

2.2.1. WannaCry: A worldwide cyber-attack

In May 2017, a ransomware crypto-worm targeted more than 230,000 computers in at least 150 countries [12]. The systems that became vulnerable to the malware were mostly running out-of-support Microsoft Windows OS and specially systems that had not installed the security patches that were released earlier in 2017. The Server Message Block(SMB) protocol uses TCP and UDP ports for file sharing and printing purposes. The SMB interface allows any code to be introduced into the system, which is an implementation vulnerability of the interface. WannaCry, upon entering vulnerable systems acquired different types of files such as document, image, video or audio files located either on the hard drive or on the network drive. The infected files were then encrypted while files got modified with a .WNCRY extension. Due to this, users were unable to access infected systems thereafter, while a message pop-up as shown in fig. 2.2, requested a crypto-currency ransom amount be paid to be able to free the system from the infection. The infected code intended to generate individual bitcoin address to receive ransom from each affected system. However, this generation feature failed and the attackers were unable to recognize payments made was for which infected system.

Figure 2.2.: Message pop-up on systems affected by WannaCry

All over the world, several companies were affected from the attack as depicted in fig 2.3. National Health Service (NHS) hospitals in England and Scotland were one of the worst affected. Around 61 NHS organisations were disrupted which included infected medical equipment. Among several other affected companies were Deutsche Bahn (Germany), Ministry of Internal Affairs of the Russian Federation, Nissan Motor Manufacturing (UK), O2 Telefonica (Germany), Renault (France), FedEx [13]. Before the attack infested widely, a 'kill switch' was discovered which acted as an emergency switch to prevent spread of the infection further. The attack was finally curbed when Microsoft released emergency security patches. The total losses claimed by different institutions was reported to be around billions of dollars.

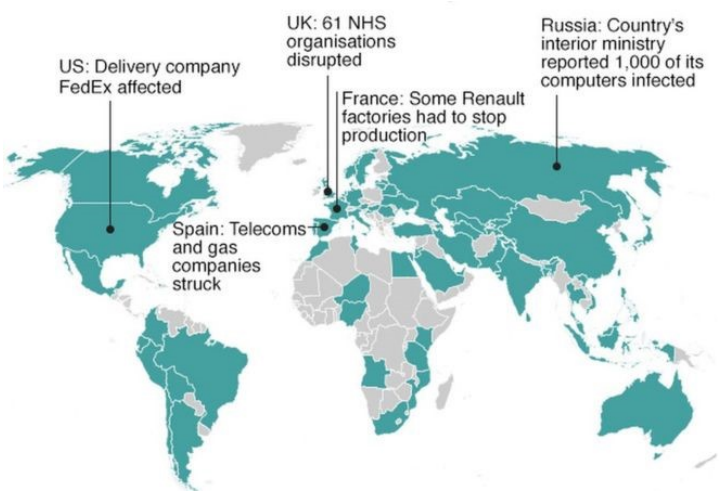

Figure 2.3.: Companies affected worldwide from WannaCry

2.3. Cyber Security and Robustness

The International Telecommunication Union (ITU) in [14] defines cybersecurity as a collection of various factors that forms a framework comprising of guidelines, tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies to safeguard the cyber environment, organization and user's assets. Cybersecurity also ensures in attaining and maintaining the security properties of assets and of the organization against pertinent cyber threats and risks in accordance to the CIA model of Confidentiality, Integrity and Availability as defined by the ITU in [15]. It is important to note that security in general and cybersecurity in particular is a continuous process and not an end state. Various standards have been developed and practiced by organizations to deal with cyber threats, implement security controls that have optimum cost benefits while also complying with legal and regulatory security guidelines. Cyber security standards define functional and assurance requirements within a product, system, process or technology environment [16]. The objective of these standards are to upgrade security infrastructure of systems and networks.

A survey by the European Union (EU) in 2017, reports that 80% of European companies had experienced at the least one cybersecurity incident in that year [17]. To equip the EU organizations with counter-mechanism a wide range of security control measures have been undertaken by the Union. The European Union Agency for Network and Information Security (ENISA) is the expertise centre to assist Member States in dealing with cyber-attacks and the centre put forth the Cyber Security Strategy in 2013 [18]. Since 2009, ENISA is responsible for cyber-security standardization, record challenges, co-ordination between different countries and to work on EU initiatives in the direction of standardization as noted in [18]. A "Joint framework for EU Diplomatic Response to Malicious cyber activities" was proposed to strengthen international co-operation including relations between the EU and NATO along with a blueprint to respond quickly to large-scale cyber-attacks [17]. The industry standards are increasingly relying on the Cloud for application deployment, mobile and distributed services among several of its other applications. While the cloud is comparable to the term Internet, cloud computing aims at offering services such as storage, databases, networking, software over the Internet. The usage of Cloud paves way for flexible usage of resources and increased innovation while also simultaneously stressing on security due to the wide range of services it can offer. The implementation of this thesis also uses the Cloud as a service. The 'EU initiatives' as part of the security standardization proposed the 'EU Cloud Strategy' in 2012. Depicted in fig. 2.4, the strategy focused on increased innovation, reduced costs in the Union while emphasizing on legal framework around Cloud computing.

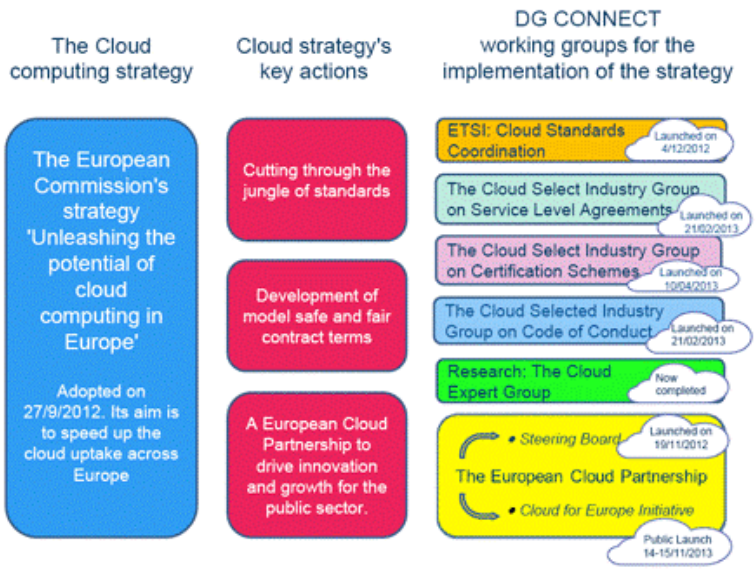

Figure 2.4.: The EU Cloud Strategy

Also, it works towards fostering adoption of security standards and to provide certification schemes to improve trust between Government bodies, cloud providers and industry [18]. By the year 2020, a net gain of 2.5 million new jobs and a boost of 160 billion euro annual rise in the Gross Domestic Product(GDP) of the European Union was estimated as a result of

employing this strategy. It is beyond doubt that with innovation in the field of cyber security methods to deal with complex cyber-attacks will come to the fore but also by having robust systems, a financially profitable environment would be created.

2.4. Cyber Security and Robustness (CSR) at TNO

At TNO in the Netherlands, the Cyber Security and Robustness (CSR) department comprising a dedicated team of professionals works on continued secure and robust ICT networks and services [19]. It is responsible for developing innovative solutions for design, assessment and optimizing complex ICT infrastructures for improved cyber security, performance and resilience to failures and cyber threats. The Research and Development wing mainly focuses on the following four areas of Transaction Security- developing secure transaction designs by employing techniques such as cryptography and blockchain solutions; Security monitoring and detection- developing solutions for identifying and dealing with unknown attacks using anomaly-based techniques and network traffic analysis; Performance of Networks and Systems- designing reliable and robust ICT networks to control and optimize performance of networks and systems. This thesis is however a part of the Automated security group, developing quick automated response solutions to aid in security decision support. The execution of optimal responses to possible cyber-attacks and cyber threats, modelling potential cyber-attacks employing machine learning techniques are focus areas of the group. TNO handles projects for the Government in the area of defence. Customers are also in the field of banking, telecommunications and logistics and TNO values partnerships with Universities, research groups, knowledge institutes and product vendors.

2.5. SARNET

The abbreviated form for 'Security Autonomous Response NETwork' is called SARNET, a Dutch research project group headed by University of Amsterdam in collaboration with TNO along with other industry partners of the group Air France – KLM, COMMIT and CIENA [20]. The research group works on developing best ways of autonomous protection against various types of cyber-attacks using software defined, virtualized detection and defence mechanisms. The second sub-project of the SARNET group focusses on 'Creating a SARNET alliance', with the focus on organizing SARNET functionalities across multiple service provider and enterprise networks to build a trust based alliance to detect and mitigate cyber threats while authorizing each of the collaboration partners to be involved. The project structure of SARNET is organized at three levels. The Tactical level- determining best defence scenario against cyber-attacks by deploying functions [21] and analysing security state and KPI information [22]; the Strategic level- autonomous SARNET behaviours are modelled to identify risks and advantages for stakeholders; Operational level- designing functionalities to operate a SARNET using Software Defined Networking (SDN) and Network Function Virtualization (NFV), delivering security state and KPI information [20].

3. Designing the security function

3.1. Theory

3.1.1. OODA Loop

To be continued

A. General Addenda

A.1. Detailed Addition

to be added

List of Figures

List of Tables

Bibliography

[1] V. Farhat, B. McCarthy, and R. Raysman. "Cyber Attacks: Prevention and Proactive Responses". In: (2011).

[2] J. B. Marshall and M. A. Saulawa. "International Journal of International Law: ISSN: 2394-2622 (Volume 1 Issue 2)". In: ().

[3] U. Nations. "Conference on Trade and Development". In: (). DOI: https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx.

[4] A. Singh and M. Singh. "An Empirical Study on Automotive Cyber Attacks". In: (2018).

[5] Cisco. "Types of cyber-attacks". In: (). DOI: https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html.

[6] C. for Strategic International Studies. "Significant cyber incidents". In: (). DOI: https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity.

[7] T. Vaidya. "Survey and Analysis of Major Cyberattacks". In: (). DOI: https://security.cs.georgetown.edu/~tavish/cyberattacks_report.pdf.

[8] F. Policy. "10 years After the Landmark Attack on Estonia, Is the World better prepared for Cyber Threats?" In: (). DOI: https://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/.

[9] C. for Strategic International Studies. "Significant Cyber Incidents since 2006". In: (). DOI: https://csis-prod.s3.amazonaws.com/s3fs-public/190211_Significant_Cyber_Events_List.pdf.

[10] BBC. "Timeline: How Stuxnet attacked a nuclear plant". In: (). DOI: https://www.bbc.com/timelines/zc6fbk7.

[11] T. Sun. "CYBER WARFARE? Google 'hit by WORST EVER cyberattack' with traffic 'hijacked' and routed through Russia and China in 'war games"". In: (). DOI: https://www.thesun.co.uk/news/7726913/google-cyber-attack-traffic-highjacked-russia-china/.

[12] W. Smart. "Lessons learned review of the WannaCry Ranswomware Cyber Attack". In: (2018).

[13] B. News: "Ransomware cyber-attack: Who has been hardest hit?" In: (). DOI: https://www.bbc.com/news/world-39919249.

[14] I. T. Union: "Definition of cybersecurity". In: (). DOI: https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx.

[15] NIST. "Cyber Security Standards". In: (). DOI: https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=152153.

[16] E. Commission. "State of the Union 2017 – Cybersecurity: Commission scales up EU's response to cyber-attacks". In: (). DOI: http://europa.eu/rapid/press-release_IP-17-3193_en.htm.

[17] D. S. Purser. "Best practices in Computer Network Defense: Incident Detection and Response". In: (2014).

[18] E. Commission: "European Cloud Strategy 2012". In: (). DOI: https://ec.europa.eu/digital-single-market/en/european-cloud-computing-strategy.

[19] TNO. "Cyber Security Robustness". In: (). DOI: https://www.tno.nl/en/focus-areas/information-communication-technology/expertise-groups/cyber-security-robustness/.

[20] SARNET. "Security Autonomous Response with programmable NETworks". In: (). DOI: https://delaat.net/sarnet/index.html.

[21] B. G. e. a. Leon Gommans John Vollbrecht. "The Service Provider Group Framework: A framework for arranging trust and power to facilitate authorization of network services". In: (2014).

[22] L. Gommans. "Multi-Domain Authorization for e-Infrastructures". In: (2014).