TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technology
Department of Software Science
TUT Centre for Digital Forensics and Cyber Security

ITC70LT

Henry Okechukwu Okere 173972IVCM

ANALYSIS OF A NODE-BASED INTEGRITY ATTACK ON NETWORKED SCADA POWER PLANT

Master's thesis

Supervisor: Hayretdin Bahsi
Ph.D
Senior Research Scientist

Tallinn 2019

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia kool
Tarkvara teaduse osakond
TTÜ küberkriminalistika ja küberjulgeoleku keskus

ITC70LT

Henry Okechukwu Okere 173972IVCM

Analüüs võrgustatud SCADA elektrijaama sõlme-põhise terviklikkuse rünnaku kohta

Magistritöö

Juhendaja: Hayretdin Bahsi
PhD
Vanemteadur

Tallinn 2019

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Henry Okechukwu Okere
21st April, 2019

Abstract

Supervisory Control and Data Acquisition (SCADA) has been most significant in industrial and economic development as its deployment in nuclear power stations ensures the efficient operation of these critical infrastructures. However, these systems have recently been the focal point of target by malicious actors taking advantage of the inherent vulnerabilities in the systems and their connectivity to the internet to stage an attack capable of compromising it. To better understand the sophisticated nature of cyber attacks and the capabilities of adversaries targeting critical infrastructure of this nature in this paper we built attack tree models depicting six different ways the integrity of a fundamental component of the system—the master terminal unit can be compromised. Thereafter analyzed the attacks using a well documented expert peer reviewed cyber sophistication index categorization to determine and compare the relative level of sophistication for each of the modeled attack scenarios. We used the MITRE Adversarial Tactics Techniques and Common Knowledge (ATT&CK) and the cyber threat metric frameworks in determining attack vectors for the buildup of the respective attack tree models. We also adopted the concept of cyber kill chain in the buildup of our model. Further, we extend the work of Sanjay Goel and Nick DePaula's attack sophistication index in analyzing and determining the various sophistication levels of our attack models. Our aim is that adequate knowledge of an attacker's strategies and capabilities would further aid in decisions on efficient mitigation techniques that can be employed to curtail the effect of threats on these systems.

This thesis is written in English language and contains 87 pages of text, 7 chapters, 9 figures and 14 tables.

Table of Abbreviations and terms

SCADA	Supervisory Control and Data Acquisition
ATT&CK	Adversarial Tactics Techniques & Common Knowledge
MTU	Master Terminal Unit
HMI	Human Machine Interface
RTU	Remote Terminal Unit
IED	Intelligent Electronic Device
SQL	Structured Query Language
CVE	Common Vulnerability and Exposures
XSS	Cross-Site Scripting
MITM	Man In the Middle Attack
APT	Advanced Persistent Threat
NIST	National Institute of Standards and Technology
OSVDB	Open Source Vulnerability Database
VPN	Virtual Private Network
RAT	Remote Administrative Tool
SI	Sophistication Index
SLR	Systematic Literature Review

Table of Contents

List of Figures

List of Tables

1. Introduction

The importance of nuclear energy and the proliferation and sustenance of nuclear power plants for efficient and alternate source of electrical energy cannot be overemphasized. It is recorded that the total capacity of energy generation from nuclear power stations in the United States account for over 20 percent in the year 2018 [1]. Much of the reliability and production efficiency of these nuclear stations can be attributed to the efficiency in process functionality of the SCADA system in place. The Supervisory Control and Data Acquisition (SCADA) have its applicability in *leaps and bounds* in industrialization cutting across myriad sectors few of which are manufacturing, power generation, transmission and distribution, water treatment, oil and gas, telecommunication, space stations, etc. Being capable of performing supervisory and control functions these automated systems help increase efficiency of industrial processes thus impacting on the general standard of living of the average 21st century *Homo sapiens.* Sadly these industrial control systems are bedeviled with security issues capable of affecting its overall performance.

The security of SCADA systems have been an issue since the advent of cyber terrorism on Critical Infrastructures. SCADA systems have been in existence long before cyber attack became an issue that has recently plagued these systems. It is known that the initial design of the SCADA technology did not cater for cyber security probably due to the lack of internet integration owing to unavailability of the necessary technology at the time, hence the only protection afforded to the system is security by obscurity. The system has over the years been modified to meet changing demands of functionality and security and as the level of sophistication of cyber attack increases it is important for security analyst and designers of security systems to be a step ahead of cyber detractors.

Regardless of security improvements and modifications there has been reported cyber incidents related to attacks on SCADA systems deployed in nuclear power stations. For example, the Edwin Hatch Nuclear Power Plant in the United States on March 2008, it was reported that an accidental shutdown of the power plant was caused by software update [2]. In June 2010 at the Natanz nuclear facility in Iran, the Stuxnet worm was intentionally used to sabotage the nuclear centrifuges [3]. Also, at the Gundremmingen nuclear power plant in Germany on April 2016 it was reported that viruses were introduced into the plant’s fuel rod monitoring system from unknown cause [4]. In his book on the Art of War, Sun Tzu categorically stated: “…if you know your enemy and know yourself, you will not be imperiled in a hundred battles [5].” It is equally important to state that sometimes the best form of defense is to attack and learn about the attackers’ strategy.

The topic of research based on the Analysis of a node-based integrity attack on a networked SCADA power plant is intended to describe all possible and feasible attacks targeted against the master terminal unit otherwise known as the supervisory system of a SCADA, by way of attack tree depicting a representation of attackers’ strategy to compromising the target system, and thereafter analyzing and comparing the required level of sophistication for each of the attack scenarios. It is with the intention that proper knowledge of the attackers’ strategy is a vital step forward in planning towards mitigation.

To achieve the aforementioned, we employ an observational approach. This method is chosen since we will be modeling the attack tree from case studies of sketchy attack citations obtained from the web since it is most likely no detailed attack scenario on the subject matter has been documented. As such we will review systematically literatures of related attacks. We will aggregate the piece by piece information obtained from different sources and use them to form attack scenarios. We will then create attack tree models that encompass the various stages of the attack from ground-up following the concept of cyber kill chain whilst adopting the MITRE ATT&CK framework. Further, we will draw up an analysis using a well documented expert peer reviewed cyber sophistication index categorization to determine and compare the relative level of sophistication for each of the modeled attack scenarios.

1.1 Research Motivation

Cyber attacks targeted against critical infrastructure are fast becoming a new normal. SCADA systems deployed in most critical infrastructure play a vital role in the day to day running of any advanced society. Attackers target SCADA infrastructures for various reasons since it is the life wire of any society and once an attack against these facilities are successful the resultant physical effect are mostly disastrous. This research is borne out of the interest I developed in instrumentation and control having at one time worked within the field. More so, with the knowledge that security issues ravage these systems, I look forward to exploring possible ways the system could be compromised. Due to the versatility of the system as a whole I decided to narrow my scope to attacks against the integrity of the MTU since the latter perform a very critical function in administering relevant control on all other SCADA subcomponents. Further, to ascertain the level of attack sophistication required to compromise the integrity of the MTU with respect to the six attack tree models developed.

1.2 Scope of Research

SCADA systems being a form of industrial control system are affected by a lot of security issues. As mentioned earlier, the system was developed when cyber security wasn’t a major concern hence the protocols and implementations at the onset do not cater for cyber security leaving the system vulnerable to a lot of issues. Security issues affecting a typical SCADA are boundless ranging from hardware, software, communication and protocol. For the purpose of this research I look forward to investigating attacks capable of compromising the integrity of the MTU, determining the attack sophistication necessary to compromise the integrity of the MTU, and then compare the level of sophistication for each of the modeled attack trees. The level of sophistication of a cyber attack is determined in part by the scale of the attack, technicality of the perpetrator and perpetration process, and the effectiveness of the overall attack. The effectiveness is the impact the attack causes which in most cases is physical.

1.3 Research Questions

At the end of the day, the study will provide answers to the following questions:

- What are the possible attack paths that can result in the compromise of MTU data integrity?
- What is the minimum sophistication level required to cause an integrity compromise of MTU data.

1.4 Research Relevance and Novelty

Many studies have discussed security of SCADA system. Few have focused on security of subcomponents of the system taking into consideration different forms of attacks. This study is unique because it utilizes systematic literature review method to obtain related attack information. We then aggregate the piece by piece information obtained from different sources and use them to create custom attack scenarios that addresses the integrity compromise of a SCADA MTU. We then model the resultant attack scenarios in the form of an attack tree that provide at a glance six different ways of compromising MTU integrity. Thereafter we determine the respective level of sophistication.

The outcome of this work will provide an answer to the aforementioned research questions. Further, it will demonstrate how the integrity of MTU can be compromised, and from the resultant attack trees the attack possibilities would be revealed, hence knowledge of these attack possibilities can aid in attack mitigation. It will also help security personnel and SCADA designers with an idea of improvements and enhancements that could be implemented to cushion the effect of threats on these systems in new designs.

1.5 Research Limitations

The major limitation encountered in the course of this work is regarding the extent of information made public on the subject matter. The very fact that we chose to investigate attack methods capable of affecting the master terminal unit is enough challenge since the information provided on the public domain is very limited. The information on attack methods available on the web is mostly peripheral as no detailed information is given. Hence much of this work involves frantic effort to connect the dots from peripheral information available.

1.6 Thesis Structure

The organization of this work follows the pattern. Having given an introduction into the topic in chapter 1 we proceed to studying the background in chapter 2, highlighting the key cyber actors and their respective motivation, the structure of the SCADA system, the components, their definitions, and security issues affecting them. Summary of important literatures derived from systematic review that deals to a greater extent on the subject matter is given in chapter 3. Chapter 4 gives the systematic literature review methodology used in selecting important primary studies and a summary of the documentation process. Chapter 5 consist of an in-depth approach into the research method, evidence gathering, attack tree modeling, and an explanation to aid in proper understanding of the model. Chapter 6 gives the analysis of attack sophistication of respective attack scenarios using the work of a well documented expert reviewed cyber sophistication index categorization. It also presents summary of the findings and answers to the research questions. Conclusion is provided in chapter 7.

2. Background

In this chapter we examine the architecture of the SCADA model used in this research, the mode of operation, the respective components making the SCADA model and their underlying security issues. We take a further glance at the SCADA attack vectors which provides a route for attackers into the system and finally we consider the common threat agents or SCADA cyber actors and what motivates them.

2.1 Architecture of our SCADA model

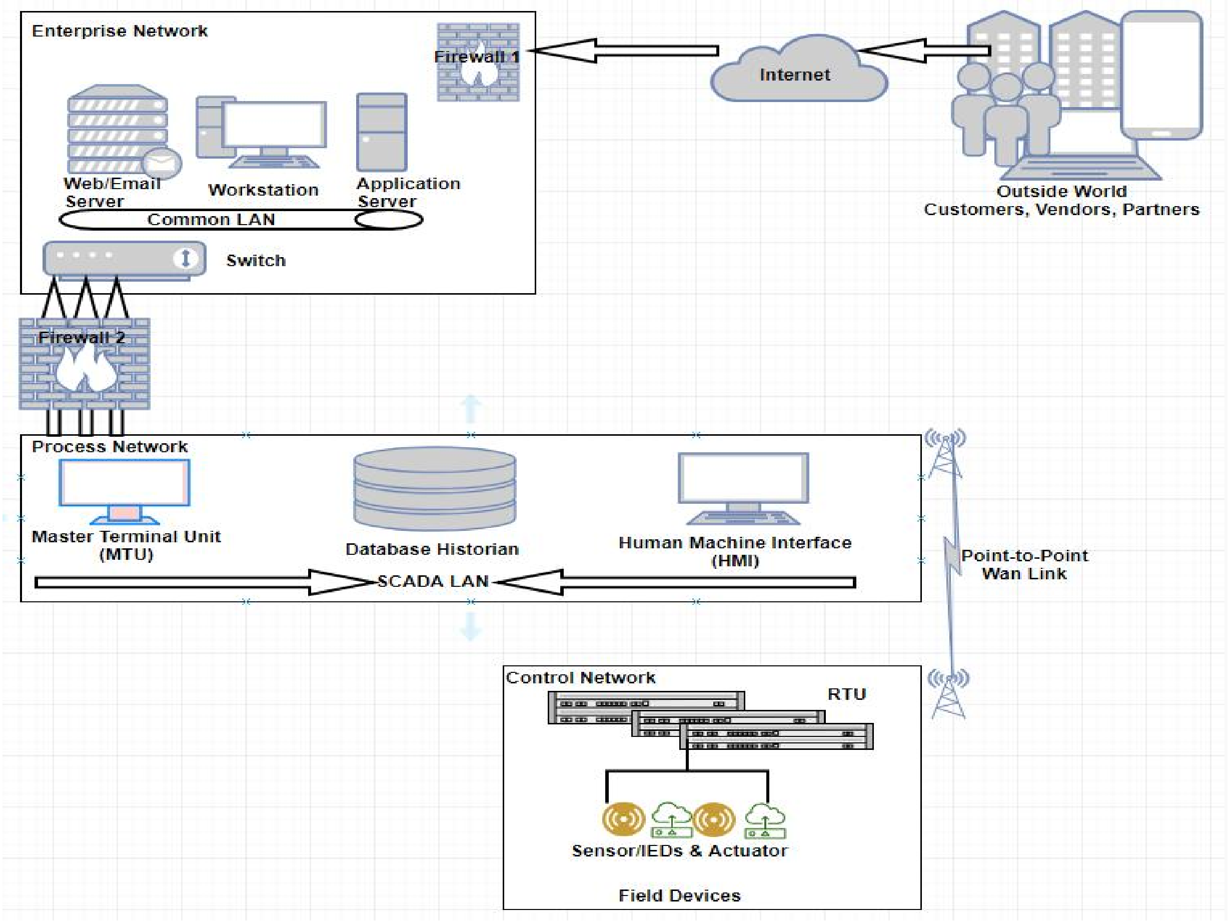


Figure 1. Hypothetical structure of SCADA model used in this research. (Images adopted from: The United States Government Accountability Office Report. GAO-04-354 [6], Practical SCADA for industry [7] and Journal of International Critical Infrastructure Protection [8])

2.1.1 Mode of Operation

The figure 1 above shows the typical SCADA model adopted for the purpose of this research. The model consist of 3 major compartment or network area namely the Enterprise network [6], the Process Network [8] and the Control Network [8]. Forgoing in this research we shall refer to the above diagram as SCADA system. The diagram also shows the outside world consisting of vendors, customers and third party partners that also possibly interact with the SCADA system.

The Enterprise Network provides services for running all of the enterprise business operations [6]. As shown in the diagram typical components within the enterprise network are the everyday components used in an IT shop such as Web/Email Servers, Application server, Workstations etc. The enterprise network users can regularly access the internet to interact with their third party partners and vice versa [6]. Firewall 1 situated at the boundary of the Enterprise network protects it from possible cyber intrusion from the internet. It is also not uncommon for the Enterprise to integrate their network to the Process and Control networks, providing for more operational flexibility [6].

The Process Network consists of the Master Terminal Unit (MTU), Human Machine Interface (HMI) and the Database Historian. A layer of Firewall 2 borders between the Enterprise and Process Network, and help prevent possible cyber intrusion from adversaries [9] who successfully gained access to the Enterprise network. For the purpose of this work it is assumed that the aforementioned components of the process network are connected by a common LAN [6] known as SCADA LAN in the figure. The MTU otherwise known as the supervisory system being one of the major nodes of the SCADA system provides an interface where the operator administers control and supervisory actions on all other subcomponents and field devices for efficient operation of the SCADA system [7]. The supervisory system interprets the output of an alarm/abnormality from the field instrumentation devices (Sensors/IEDs, and Actuators) interfaced with the Remote Telemetry Unit (RTU) in the control network. The output which measures variation in temperature, voltage and current etc are sensed by the sensors attached to the RTU. The RTU aggregates data from different sensors in different locations attached to it forming a cluster head [10] with these sensors. The aggregated data are transmitted over the point-to-point WAN link and received at the respective components of the process network. The database historian logs in process data and data received from the RTU [8]. The HMI provides a graphical view of the activities at the field network. In some SCADA implementations, the HMI and MTU are linked by a single interface where an operator sitting at the front of the screen can view graphically the activities of the entire system, able to monitor and control parameters [11].

The Control Network in our architecture comprises the field instrumentation devices such as the Remote Telemetry Unit (RTU), the Sensors/IEDs and Actuators. Because of the need for miniaturization and smarter operation, modern SCADA incorporates an Intelligent Electronic Device (IED) which is an intelligent sensor and capable of functioning in place of the Programmable Logic Controller (PLC) [7]. The sensors and actuators connect directly to the infrastructure equipment of the nuclear station. The sensor is able to extract readings such as temperature, current and voltage from these equipments and transmit the message to the RTU. The RTU processes the sensor signals to data and sends them over the WAN link to the MTU who in turn relays control instructions with a function code specifying what action is to be taken [10], to the controller. The controller activates the Actuator to execute the control action such as turning on/off a valve [6].

2.2 Security Issues of SCADA Components

Here we will study some of the known security issues affecting SCADA system component which makes it possible for hackers to exploit the system.

2.2.1 Security Issues with the MTU

A good number of security issues affecting the supervisory computers result from outdated operating system (OS), software applications and antivirus used on these machines [12]. A major reason for not updating the system is to keep the system of incompatibilities as updating to latest versions might cause operational instability, affecting system availability [12]. As a result of this several attacks such as SQL injection, Buffer overflow, Lack of privilege separation, etc can be contrived to exploit the resultant vulnerabilities. In chapter 5 of this work we developed attack trees of six different attack scenarios that can be used to compromise the integrity of the master terminal unit. Another possible issue with the MTU could be ignorance of the operator in identifying false alarm or the negligence of the operator in adhering to outlined security best practices of the company [13]. Physical and deliberate compromise by an insider conspirator could also pave a way to rendering this system vulnerable to cyber attack.

2.2.2 Security Issues with the HMI

As with the MTU the HMI are also affected with security issues resulting from outdated operating system, software and antivirus program. Some possible threats resulting from these issues are:

Input Validation Vulnerability: Arising as a result of improper validation of input variable causing the software to write more data than it can normally hold [11]. Typical attack that can exploit this vulnerability is the Buffer overflow attack. Example is CVE-2011-3142, the WellinTech KingView 6.52/6.53 ActiveX Control vulnerable to heap buffer overflow vulnerability [14]. SQL injection attacks are also possible from incorrect filtering of user input that can cause an attacker to construct and run SQL queries through the input field of a web application [11]. An example of this is CVE-2018-5443, vulnerability found in Advantech WebAccess SCADA up to 8.2, of which manipulation results in SQL injection vulnerability [15]. It is reported that this particular vulnerability has been fixed for this product if a user upgrades to a later version [15].

System Level Access: System level is regarded as the highest level at which an administrator can operate to perform or administer any kind of operation. When the HMI default access level is system it could pose a security challenge as an attacker who succeeds in compromising the HMI will not face difficulty in taking control of its entire functionality to cause havoc. A notable example of this incident is with the CVE-2016-5787 vulnerability found in General Electric Digital Proficy HMI and SCADA CIMPLICITY up to 8.1 which can lead to privilege escalation [16]. It is also reported that this vulnerability has been fixed for this product by upgrading to a higher version [16].

2.2.3 Security issues with Database Historian

Database historian as with any database application can be affected by attacks resulting from Buffer overflow, SQL injection attacks, Cross-site scripting attack, [17] etc. These attacks are possible owing to continual usage of deprecated software and applications, lack of efficient patch management and improper application development. Notable of such is CVE-2011-4035 vulnerability found in Schneider Electric Vijeo Historian 4.1-3; CitectHistorian and CitectSCADA vulnerable to Cross Site Scripting allowing an attacker access to cookie-based authentication credentials [18] to gain access to the system.

2.2.4 Security issues with Sensors

Sensors are prone to security issue arising from signal jamming and interference. It is possible for an attacker within compromisable distance from the sensor to jam the signal causing signal distortion and denial of service [19]. Also, since the sensor communicates directly with the RTU it is possible for an attacker who successfully penetrated the network to conduct a man-in-the-middle attack. MiTM attack is possible due to the lack of sufficient cryptographic mechanism in Modbus protocol hence the packets are usually sent in plain text owing to lack of encryption [20]. Similarly, sensor packet could also be intercepted and a skilled attacker could use intercepted packet to cause denial of service through flooding attack. Field sensor devices are also susceptible to tampering by intruder gaining physical access it. By tampering, the sensor readings could be modified resulting in sensor data integrity compromise. Replay attack is also possible if an intruder is able to gain access to the sensor network, he could capture the packet and retransmit them at a different time [19].

2.2.5 Security issues with RTU

RTU is one of the major field instrumentation devices responsible for receiving signals from the sensor, transmitting them to the master stations, and relaying the instruction back to the controller for execution via the actuator. RTU is notable for several security issues such as:

Packet Modification: RTU packet in transit can be captured and modified since the protocol used within the field devices lacks proper encryption mechanism hence the messages are in plain text [20]. Once these packets are intercepted via MiTM attack the message can be modified and retransmitted causing a lot of integrity, confidentiality and availability issues.

Buffer Overflow: Memory allocation on field devices such as RTU are usually fixed [20] hence knowledgeable attackers can take advantage of this to cause a denial of service or cause the RTU to behave erratic. Because of the need for availability, RTU as well as other field devices are rarely rebooted. The accumulated memory can result in memory fragmentation [20] causing the RTU behave erratic eventually stalling its functionality.

Replay Attack: RTUs can be the route to stage a replay attack. Replay attack occurs when a captured message is retransmitted at some other time [21]. An attacker who gains access to the network can capture packets from the sensor, inject them onto the RTU and transmit them to the process network in a replay attack.

Privilege Escalation: An attacker who has successfully penetrated the control network via MiTM attack can increase his access level by exploiting privilege escalation vulnerability, should the RTU in use be susceptible to such vulnerability. A typical example is with CVE-2013-0694, which is a vulnerability found in Emerson DI 8000 Remote Terminal Unit, having hardcoded credential in ROM, allowing an attacker obtain shell access [22] to the RTU operating system. An attacker exploiting this vulnerability can cause confidentiality, integrity and availability issues [22] for the concerned system.

2.2.6 Security issues with SCADA Communication Protocols

The two most common protocol used in SCADA network is Modbus and DNP3. While Modbus is proprietary, Distributed Network Protocol (DNP3) is non-vendor specific. These two protocols have common security issues such as:

Lack of Cryptography: SCADA protocols have been existent long before the issue of security on SCADA systems became manifest. The protocol was designed in its simplest way to transmit and receive SCADA instructions in form of function codes thus fostering operational efficiency [23]. No security implementation was done hence in the face of present security challenges such as packet sniffing, eavesdropping, spoofing, SCADA protocols are susceptible to attack [10] since by design there is no way a receiver or sender can ascertain the true originator of the packet. More so, the system lack proper encryption and authentication mechanism [24] thus messages are usually sent in plain text hence attackers can exploit this vulnerability to steal sensitive information and stage a replay attack.

2.3 SCADA Attack Vectors—A compliance with MITRE ATT&CK Framework [25] and Cyber Threat Metrics [26]

These represent the starting point or point of compromise with which an adversary use to gain initial foothold within the target's network. With respect to this work we have identified and used six possible attack vectors to compromise the SCADA master terminal unit from the documentation of MITRE ATT&CK framework and Cyber Threat Metrics, namely: removable media, malicious web components (SQL, XSS, BOF), Drive-by Compromise and Spear Phishing Attachment.

2.3.1 Removable Media

This form of attack vector is mostly used in networks that are not easily reachable or accessible, also known as air-gapped networks e.g. SCADA and DCS network. The malware is copied into the removable media e.g. USB stick, thumb drive etc, and inserted into the target system mostly by disgruntled employee who has physical access to the system. Notable examples of attacks that used this infection method are with Agent.btz [27], Flame [28], APT28 [29], etc.

2.3.2 Spear Phishing Attachment

This form of compromise involves a more targeted approach in which an adversary gains access to the target network by way of malicious email attachment. It is a form of social engineering technique that uses a well constructed target-specific email to deliver the malware. The execution of the malware depends to a large extent on the complicity of the target. Once the target opens the attachment on the email the malware executes and infiltrate his network. Notable example of attacks that used this medium includes: CobaltGroup [30], Dragonfly2.0 [31], etc.

2.3.3 Drive-by Compromise:

This method of malware infection takes advantage of a user visiting a website in the process of browsing. This form of exploitation is mostly effective as once successful it gives the adversary access to the internal network systems. An adversary delivers the exploit code by injecting malicious code on a rather legitimate website. Cross-site scripting and watering hole attack are methods used. Other ways are through malicious adware and spywares served through legitimate websites. Example of attacks that utilized this method are: Dark Caracal [32], Elderwood [33], etc.

2.3.4 Malicious Web Component (SQL Injection, Buffer Overflow & Cross-site Scripting Attacks) [26]

This can be a tool for an attack to be propagated by using web pages that has been compromised with malware. An individual visiting such compromised webpage can also possibly expose his system or network to such vulnerability and in the process inadvertently download the malware. SQL injection, Buffer Overflow attack and Cross-site scripting attack are possible for webpages that are not properly secured or code not properly written and tested for bugs.

2.4 SCADA Threat Agents [34]

Threat agent or threat actors can be referred to as an individual, group of persons, and/or organization that has the intention, the opportunity and capability of exploiting a system's vulnerability to cause harm. SCADA threat agents are more focused on seeking ways to exploit vulnerabilities in a SCADA system. Regardless of the numerous taxonomy of threat agents, they can widely be classified into two distinct groups: Targeted and Non-Targeted threat agents. For a threat agent to exercise a threat he/she must be having the required motivation (fame, money, curiosity, etc), the capability (resource and skills) and the right opportunity (target's vulnerable system). We examine some of the common threat agent and show their possible and/or future interactions with SCADA systems.

2.4.1 Non-Targeted Threat Agents

2.4.1.1 Script-kiddies

These groups of threat agent also referred to as hobbyist are those that are heavily dependent on already made tools to carry out their aim. They are motivated by their curious nature and in most cases do not mean to cause harm to a system, but their actions could put a system in jeopardy either by exposing system flaw or revealing the internal network structure of a system as well as sensitive information. They have little or no real capability of causing harm to a system, and may not be concerned about whether a system is vulnerable or not. On the other hand they could be security researcher or gray hat hacker trying to explore system vulnerability either by making it known i.e. responsibly disclosing it or seeking to profit from it [35] in a bounty program. There is no recorded script-kiddy activities causing harm to a SCADA but that does not mean it cannot happen in the future. With the availability of exploit codes and tools around the web it is possible for an ambitious script-kiddy to try something new out of his curiosity. With the level of attack sophistication necessary to achieve the goal in our attack tree, I would rather say it is beyond the scope of script-kiddies.

2.4.1.2 Disgruntled Employees

These set of people are sometimes the precursor to most attacks. Due to the fact that they are within the organization [35], they have good knowledge of the organization's internal system and sometimes possess the required security clearances. They may be directly employed to the organization or a third party with some access level. Their lack of loyalty to the organization or motivation to the job may prove costly especially in their nonchalant work attitude causing either configuration error, exposing important security detail or may even be co-opted or bought over by a rival company or adversary group and may act as spy on their behalf. With respect to our attack tree model a disgruntled employee or malicious insider could be a source of attack initiation. For instance, a malicious insider might introduce a compromised removable drive into network component which could allow an adversary remote access to the system, as was the case with Stuxnet [8].

2.4.2 Targeted Threat Agents

2.4.2.1 Hacktivists

These set of individuals are mostly driven by political motives. Since they are more concerned about fighting for a cause they believe in, they are capable of staging an attack that will create the necessary awareness. They may also use a staged attack to distribute propaganda [35] about an opposing organization or political party for the purpose of discrediting them. They have the required capability—resource and skill set to cause damage to an opposing organization and the attack they stage are usually targeted. Since a nuclear power station presents a high value target and any successful attack targeted at it could result in disastrous physical effect, Hacktivists group might look for a window of opportunity to compromise the system. With respect to our attack tree, it is not unlikely for a Hacktivists group to stage an attack targeted at the master terminal unit and obtain as much information as possible regarding system configuration, vulnerabilities, sensitive personal identifiable information, etc and threaten to make it public knowledge.

2.4.2.2 Cyber Criminal

These categories of threat actors are motivated by the profit [34] they make in carrying out cyber crimes targeted at individuals and organizations. They obtain confidential information such as credit card number, health information, social security number, etc of their target either through the dark web, or social engineering techniques and sell this information for profit. They also deploy ransomware where they threaten to reveal sensitive information and demand a ransom for it.

2.4.2.3 State Sponsored Group

These groups of threat agent are sponsored by nation state. They are usually well funded hence possess all the resource, the time and the capability to carry out an attack [35] [34]. Attack perpetrated is usually targeted, and they are motivated politically, economically, and sometimes are used to conduct industrial cyber espionage. They have the resource and capability to carry out Advanced Persistent Threat (APT). A notable example of state sponsored cyber attack is with Stuxnet that was deployed to compromise the nuclear centrifuge of the Natanz Nuclear facility in Iran. This attack was attributed to a joint hacker group sponsored by the United States and Israeli government in a bid to halt Iran's nuclear program [36]. Another example is with the Ukraine power outage that occurred in December 2015, causing blackout for over 230,000 residents. [37]

Having analyzed the various groups of threat agents, it can be seen that categories of threat agents that could possibly carry out and achieve the goal in our attack tree models are the state sponsored group, cyber criminals, and Hacktivists. Hence it can be concluded that for an adversary to achieve the goal of compromising the integrity of the master terminal unit possibly resulting in a physical effect the level of attack must be targeted, and the attacker must have the required capability, be well motivated, and must take advantage of an opportunity if it presents itself.

3. Literature Review

This chapter provides an avenue to present the contributions and related work of other authors as it directly relates to our research topic. Several studies have been made and publicized on a peer reviewed basis regarding the security of SCADA systems. We couldn’t have a better way of sourcing information prior to conducting this research than culling the minds, ideas and opinions of industrial security experts and academicians in their publications as well as referencing technical report of prominent security breaches. Although many of such studies have been used in the formulation of this research paper we will only review a few of them that directly reference attack approach in compromising security of SCADA and industrial control systems bringing to bear several exploits whilst taking advantage of known and publicized vulnerabilities.

3.1 Multi Tree View of Complex Attack—Stuxnet (Shivani Mishra, et al. 2012) [38]

The crux of this paper lies with the descriptive methodology with which Stuxnet prevailed. The authors have dissected the process of Stuxnet attack, which is one of the most widely known cyber-physical attack till date, using attack tree to enumerate the steps. According to the author, six major goals were required to penetrate and compromise the SCADA system using USB drive as the attack vector. The six goals includes: sabotaging the facility, installing the Stuxnet worm, spreading the worm, loading the worm, customized search for Siemens SCADA software (step 7, PCS 7, WinCC files), and reprogramming the PLC. As a precondition to sabotaging the facility the author identified subgoals such as gaining access to the SCADA centre system, disrupting communication and field control devices as different ways of achieving this feat. Prior to the Stuxnet worm propagation a positive confirmation of the value of 19790509 for NTVM trace in system registry is required and upon this confirmation the worm proceeds to disabling firewall settings to commence installation. Being a worm Stuxnet was able to replicate and spread across the system via peer to peer communication and network shares, and the attacker ensured Stuxnet executes anytime the infected system boots up by injecting the worm into certain boot-up processes aided by mrxcls.sys driver. In the process of propagation Stuxnet effectively searches for step7 project file infecting it, and thereafter it was able to reprogram the PLC causing it to spin itself to failure. The author also enumerated several vulnerabilities and attack method that aid in successful execution of the stuxnet worm on the control system, and has created a graphical representation of attack severity for each subgoal.

3.2 A taxonomy of cyber attacks on SCADA systems (Bonnie Zhu, et al 2011) [20]

In this paper the author critically looked into the possible cyber attacks that could compromise the components of the SCADA systems including the hardware, software, communication and protocol. According to the author SCADA hardware are susceptible to compromise due to remote unauthenticated access allowing an attacker alter certain value which are critical to field environmental condition notification. Further, attacks on software and SCADA application are possible due to poorly written code hence such attack as lack of privilege separation—allowing tasks to execute with the highest privilege; buffer overflow—resulting from fixed memory allocation and accumulated memory fragment; and sql injection attack are all possible. Another loophole with which attacker can penetrate SCADA system is through the communication system in place. The communication protocol existent in primitive SCADA is modbus which lacks proper cryptographic implementation and it’s naturally susceptible to eavesdropping, packet sniffing and man in the middle attack. With the recent de-airgapping and introduction of the internet to most SCADA and industrial control system makes the system even more susceptible to cyber attack since the protocols used with the internet—TCP/IP, ARP, DNS, etc have inherent weaknesses.

3.3 Extending the cyber-attack landscape for SCADA-based critical infrastructure (Nicholas Rodofile et al. 2019) [39]

Herein the author classified a wide range of cyber attacks possible with critical infrastructure into 4 classes viz: traditional IT-based, protocol, configuration-based and control process attack. This paper also gave some useful insights on attack tree development as it tries to explain the processes and steps taken for some of the attacks enumerated most especially the replay attack and some ideas as to how it can be deployed to compromise a system. Regarding the replay attack, similar methodology was also given in [21] [40]. It is noteworthy to mention that replay attacks does not necessary require breaking into any authentication process insofar the packet can be captured and retransmitted at a later time. In addition the author described the practical application of the aforementioned attacks on real world SCADA test bed and has shown with the demonstration how each attack fall under the respective category. Although the practical implementation does not fall within the scope of our work it has given more understanding as to how these attacks are carried out.

3.4 The Role of Malware in Reported Cyber Espionage: A Review of the Impact and Mechanism. (Gaute Wangen 2015) [41]

The author in this paper provided a way of classifying cyber attack due to malware proliferation for easy accessibility and understanding. Most common attacks due to malware have been explained herein and with such explanation the paper gave useful idea aiding our development of the attack tree especially for attacks using malware as adversarial vector. It is important to note that most of the attacks described herein follow somewhat the same pattern but the mechanism differs. As much as there are information on the internet regarding cyber attacks due to malware the author has focused mostly on those articles or publications from renowned security vendor and peer review literature concerning attacks used in industrial espionage from execution to conclusion. Notable of such are stuxnet, flame, duqu, red october, mandiant APT1, their mechanism of operation, impact caused by such attack which in most case is physical and the problem of attribution.

3.5 Analysis of Exploitable Vulnerability Sequences in Industrial Networked Systems: A Proof of Concepts. (Manuel Cheminod, et al 2015) [42]

Much of this work rest upon description of vulnerabilities inherent in software, hardware and communication protocol used in industrial control systems. The author has also provided a way of representing the information in vulnerability databases in machine readable way that can be readily fed into an automated software tool, and by automation it would be easier to detect sequences of common vulnerabilities which would aid in better remediation and protection against attacks especially in complex networks. The author also rightly pointed that vulnerabilities result from poor design and implementation of components and although not dangerous except a malicious actor discovers and exploit these weaknesses. The author also made reference to several vulnerability databases such as NIST, OSVDB, etc in which publicly known vulnerabilities are shared to create a reference point for users and security practitioners, and with this knowledge has aided in the development of attack tree using exploit codes to compromise the system.

3.6 A Sophistication Index for Evaluating Security Breaches (Nic DePaula and Sanjay Goel, 2016) [43]

This paper provides a guide to compare and estimate the level of sophistication with each security breach or incidents so as to provide a way of measuring and assessing the level of the impact. In the process of developing this index the author examined the evolution of malware and security breaches resulting from cyber security incidents whilst developing a good enough dataset of security incident occurring over the last decade and which has been peer reviewed by security experts. The outcome of their work shows that the developed sophistication index is proportionate to the level of perceived sophistication. The writer observes that the level of sophistication of well known attacks have not increased much over the years and that regardless of the sophistication of an attack is not a major determinant in estimating the impact of an attack since simpler attacks also impact damage. The authors also opined that sophistication can be seen in the light of the complexity of the code, resource, technical expertise on the part of the perpetrator and processes adopted in compromising the target, which in most cases determine the effectiveness of the attack. The author developed this model of calculating attack sophistication to be based on the presence of 5 attack features. The features include social engineering—targeted form such as spear phishing, use of remote administration tool, stealth mechanism, use of zero day exploit, and APT. The feature were chosen based on peer reviewed literature, and also based on expert input from survey conducted. The developed scoring system which can serve as a framework of deducing sophisticated nature of an attack is given in appendix section of this report.

3.7 Data Integrity Attacks and their Impacts on SCADA Control System (S. Sridhar and G. Manimaran 2010) [44]

In this paper the author focused on the aspect of integrity attack and defined it as a cyber attack which results in the manipulation of data either stored or in transit. The author paid particular attention to data compromise at the control centre which in our work is described as the master terminal unit. Compromising of data in transit occurs when data is transmitted from the sensor to the control centre. While our work also focused on the possible way of compromising data in transit from sensor to master terminal unit as demonstrated in the replay attack, we also focused on other sources of data to the MTU. Further, the author extends the integrity attack to automatic generation control which is a mechanism used in the power plant, and parameters such as power, voltage, frequency could easily be affected when the integrity of the sensor data are compromised. The author also demonstrated that integrity attack would be difficult to detect if the malicious data does not deviate significantly from the true value, otherwise the operator at the control centre would attribute such deviation to error resulting from communication hence leading to the failure of the attack.

3.8 Attack Tree-based Threat Risk Analysis (Terrance Ingoldsby 2013) [45]

The methodology devised in our work employed attack tree approach where we modeled possible attack scenarios to compromising the integrity of master terminal unit in the SCADA system. The vast majority of our modeling comes from the usage of the attack tree tool known as Secur*lT*ree, license of which was provided by Amaneza technologies limited solely for the purpose of this research. The tree model helps transform our attackers' mindset into diagrammatical representation to better understand, evaluate and interpret the attack strategy. The author explained the methods with which the attack tree can be used to model attack scenarios. The attack tree is made up of symbols and functions. The symbols square, dome-shaped, and dome-arc shape represents the leaf, AND function and OR function respectively. Each of these symbols are regarded as nodes which is a vital point of strategy in the attack tree. As shown in the figure below, the topmost symbol forms the root or overall goal or motive of the attack. Every other node are combined in a tree like manner and condensed to achieve the root goal. The AND and OR functions are derivative of the Boolean algebra. The AND function is used when both criteria or condition must be met to achieve a subgoal, while the OR function is used when there are several alternate ways of achieving a goal, of which only one is required and can be chosen. We have used this attack tree methodology not only in attack modeling but also in analysis of the threat and attack sophistication levels.

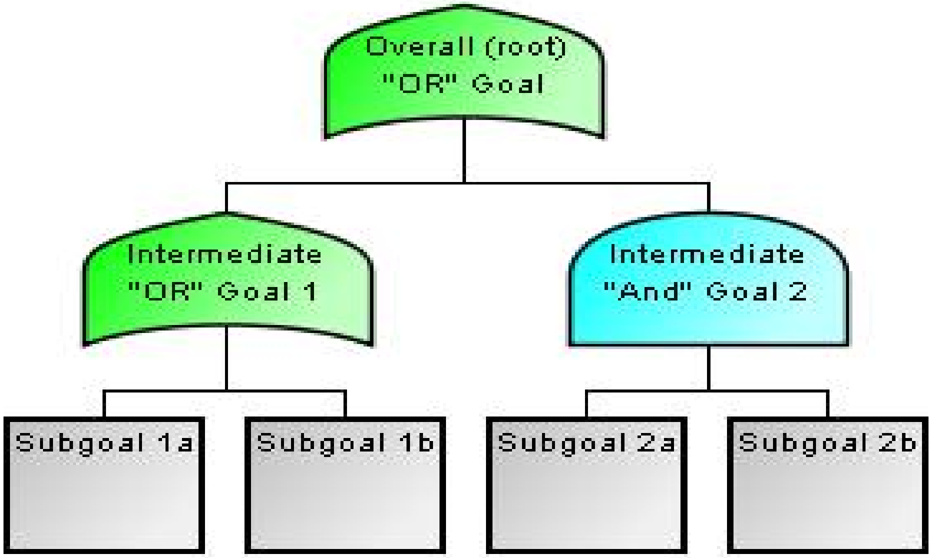


Figure 2. Sample Attack tree [45] (goal oriented).

4. Systematic Literature Review Methodology

The methodology adopted in our work involves a systematic literature review. This approach is a qualitative analysis of established facts and work done by other authors otherwise known as primary studies [46]. As such we are able to use certain key words to obtain relevant documentation of peer reviewed literatures by security researchers and published on important publication sites such as Scopus and IEEExplore. Using this method we are able to gather, identify, analyze and interpret all the relevant and available evidences as they relate to the research question in focus. This would help in drawing suitable and a more general conclusion on the phenomenon investigated having analyzed available facts on ground. The paragraphs that follow detail our methodology for sourcing required information in our systematic review process. We adopt the guidelines detailed in [46] for performing systematic literature review.

4.1 The Need for a Systematic Review

Our purpose of conducting a systematic review is to gather as much evidence as there are on the cyber space that specifically relates to the subject matter. Prior to the start it was controversial if at all there were information regarding exploits that will result in compromising the integrity of a SCADA MTU as it was preconceived such information are not usually made available to the public. We intend to know the mindset of security experts on the subject matter, hence the need for this review. We also want to collate as much information on attack strategies aimed at the target in question, to present our findings in a more logical way, to derive a general conclusion and to use our findings for a post attack analysis. We know for sure that the capability of an attacker becomes more sophisticated with development in technology and with each passing time hence this study will enable us build attack tree models that will illustrate how the integrity of SCADA MTU can be compromised.

4.2 Defining the Research Question

Bearing in mind the criticality of a good research question which amongst other factors can affect in the selection of the right study material, we follow recommendations given by Petticrew and Roberts in [47] using the PICOC (Population, Intervention, Comparison, Outcome, Context) criteria in framing the research question. These criteria ensure that the key element of the research is reflected in the research question. This research question is aimed at selection of appropriate study materials. Hence:

- What attack scenarios can be deployed to compromise integrity of a SCADA
- What are the existing vulnerabilities of SCADA or ICS systems
- How to exploit industrial control system or SCADA vulnerabilities to yield successful attack.

4.3 Search Strategy

In order to develop an effective and workable search strategy we partly adopt the framework developed by Kable et al in [48]. Our aim is to identify existing systematic review documentations and also assess potential relevant primary studies. We also employed snowballing techniques which involve checking the references of relevant primary studies obtained against the derived search key string. With the help of my supervisor, we were able to derive the search string which comprises keywords of important terminologies obtained from the above research questions and linked with the Boolean AND/OR function. The search strings are derived by breaking down the research questions into different facets in accordance with the PICOC criteria [47] earlier mentioned. We draw up a list of possible synonyms, abbreviations and alternate terminologies used in journals and online databases. Search strings are then constructed by linking keywords with Boolean functions.

Hence our derived search string is:

> *(SCADA OR "industrial control") AND ("attack tree" OR "attack path" OR exploit) AND (compromise OR exploit) AND (threat OR vulnerability)*

This search string is further broken down and used one word after the other resulting in six (6) different search instances as detailed in the table 1 below. Different online database may require different coinage of search string to fit their requirement. We were able to redefine search string on case by case basis.

4.4 Database Used

In as much as there are a handful of online databases we limited our search to two most important databases which are: Scopus and IEEExplore. It is claimed that Scopus provides sources to the largest abstract and citation database of peer-reviewed literature, and the most relevant and well documented technological related studies are usually present in these digital libraries, hence our choice of them. Manual searches were also carried out using the snowballing techniques discussed earlier to cover all grounds.

4.5 Search Limits

The following search limits were applied:

4.5.1 Peer-reviewed journals and conference papers in English Language

Our search was limited to peer-reviewed journals and conference papers. It is our believe that journals and papers reviewed by different security researchers and experts prior to publication will provide up-to-date and valid information. Also we assume that since these digital libraries are sources to the largest database of conference papers and journals that important and high impact research must have been translated to English prior to uploading. Hence we are able to source for all relevant papers on the subject matter without the need to worry about language of publication.

4.5.2 Time scope of research

Owing to our believe that not much work might possibly be documented on the research topic in question we did not limit our search to any time frame. Another reason that prompted our decision is due to the fact that SCADA security and hacking of SCADA systems is not really an antiquated approach hence we chose not to set time limit on our search.

4.6 Search Method and Scope

As mentioned previously the methods for searching differ in each digital library. For Scopus we limited our search to article titles, abstract and keywords. Scopus search engine has a well defined search pattern that link search keywords with the Boolean function. We simply chose the required *AND/OR/AND NOT* function to give what we required hence reducing the chances of false positives. To reduce the chance of omitting relevant literature we broke down the keywords into individual words and used *AND/OR* to link them. For IEEExplore, we used the already constructed search string on the query box to derive relevant documents while interchanging the search string by alternative derivative of the primary string to reduce the chance of omitting relevant studies.

4.7 Assessment of Study Relevance

In order to ensure that the search outcomes meet our requirements and to reduce the likelihood of bias we draw up a list of inclusion and exclusion criteria which are based on the research questions.

4.7.1 The inclusion criteria are

- Any study that enumerate attack scenarios aimed at SCADA
- Any study that discusses attacks against integrity on SCADA server
- Any study that discusses SCADA server vulnerabilities and potential exploitation.
- Any study that discusses attack perspectives, discusses attack tree modeling against SCADA infrastructure or the smart grid system.

4.7.2 The exclusion criteria are

- Any study that do not discuss SCADA with respect to its vulnerabilities and possibility of exploitation.
- Any study that does not contain the relevant keywords used in the search
- Any studies that does not describe specific method to compromise the SCADA

4.8 Ascertaining Relevance of Retrieved Studies

After obtaining a large number of papers (Scopus—310, IEEExplore—343, Total—653) we conducted relevance test to further reduce the list. We used the formulated inclusion and exclusion criteria to decide which ones to eliminate or to consider as primary. The following screening method were applied to enable us determine the relevance of our search result. First, we assess the document based on their titles. The titles of some papers are sufficient to determine the extent with which the content relates to our research topic while some are not. Papers that do not meet the inclusion criteria are eliminated. Some document title might give some level of relation and might also appear vague.

Our first stage screening also involved reading the abstract and assessing against the criteria for inclusion and exclusion. We were able to skim the abstract for relevance and remove those that do not meet our criteria. Some articles gave little information that were somewhat related to our research topic. Those set of articles were reserved for the final screening process. Abstract of articles that contained what we needed were also reserved for the final screening process, while those that are not related were eliminated. After the first screening stage we were able to reduced the number of studies to about 159 (Scopus—77, IEEExplore—82, Total—159). Some of the important papers selected had similar contents with each other. In order to reduce the chances of having duplicate papers (duplicate in the context of having paper conveying the same or similar information) we further pruned by removing the less relevant of them. In the course of searching we did not ignore certain related keywords that appear in our search like "smart grid", "IOT devices". We had to look into these documents as they may be conveying important information. We also navigated the site map to determine whether or not the exact info is included in the paper.

The final screening process involve skimming through the body of text, glancing through table of content and jumping to the body of text where specific detail were explained, and also skimming through the summary page. We were able to finally reduce the number of selected articles to 31 (Scopus—18, IEEExplore—13, Total—31). These numbers will form what is called our relevant primary study documents.

4.9 Summary of Findings

The table below show at a glance the summary of our document search process and the result.

Table 1. Summary of SLR Findings

S/N	Search Query	**Scopus (All Publications)**			**IEEExplore (All Publications)**		
		Initial Search Result	First Review (Title & Abstract)	Second Review (Main Text)	Initial Search Result	First Review (Title & Abstract)	Second Review (Main Text)
1	SCADA *AND* exploit *AND* threat	20	8	3	19	9	2
2	SCADA *AND* attack *AND* exploit *AND* vulnerability	21	12	5	23	11	3
3	"industrial control" *AND* exploit *AND* vulnerability	34	12	3	51	15	3
4	"industrial control" *AND* attack *AND* vulnerability	200	34	5	168	23	2
5	SCADA *AND* exploit *AND* vulnerability	32	10	2	29	7	2
6	SCADA *AND* vulnerability *AND* "attack method*"	3	1	-	53	17	1
	TOTAL	**310**	**77**	**18**	**343**	**82**	**13**

4.10 Data Extraction Strategy

After the whole screening process we were able to obtain a total of 31 relevant documents. There is a need to extract information from these documents hence the document were carefully read and all important point were summarized. Due to the very sensitive nature of the topic, only just a few paper outlined attack scenario for example the paper on "Multi Tree View of Complex Attack" the vast majority gave some important pointers relating to SCADA attack, SCADA vulnerabilities and the components affected, etc. We formed a summary of these papers. From the summary we connected the dots of all related attacks and incidents described in each of the papers and then we used the information to form attack scenarios.

5. Design Methodology

The methodology deployed in our work involves more of an observational approach. This method is chosen since we will be modeling the attack tree from case studies of sketchy attack citations and conceptualizations. To recapitulate, we have explained the procedure adopted in obtaining relevant documentation by a systematic literature review process, in chapter 4 of this work. The systematic literature review formed the principal methodology used in evidence gathering. As a summary, we reviewed a total of 31 documents from two most widely used databases of peer reviewed literatures—Scopus and IEEExplore. See table 1 above.

We extracted the relevant context from the papers, which includes attack pattern, attack methods, vulnerabilities exploitable, and SCADA components upon which these attack characteristics relates. We used the extracted attack characteristics to form attack scenarios. Afterwards, we mapped, blended and fine-tuned the attack scenarios formed with relevant cyber attack frameworks—MITRE ATT&CK framework, Cyber Kill Chain Framework, and Sandia Cyber Threat Metrics. We also used databases of Common Vulnerabilities and Exposures (CVEs) to lay critical examples of known and exploited SCADA component vulnerabilities, as well as consulted *shodan* to acquire general information about connected SCADA infrastructures to give more insights. We also used exploit database (exploit-db.com) to gather further information regarding the known vulnerabilities and how they can be exploited. We aggregated these information and used it to build our attack tree models. Our attack tree models illustrate steps with which an attacker can compromise the integrity of data on the SCADA master terminal unit. We identified six different ways in which an attacker can perform the aforementioned and as such we have built six different attack tree models with exclusive attack vectors. We used the Secur*IT*ree® Attack Tree Analysis Tool [49] from Amenaza Technologies Limited to model the attack tree.

5.1 System Model Showing Attacker's Position Relative to Attack Scenarios and Attack Progression

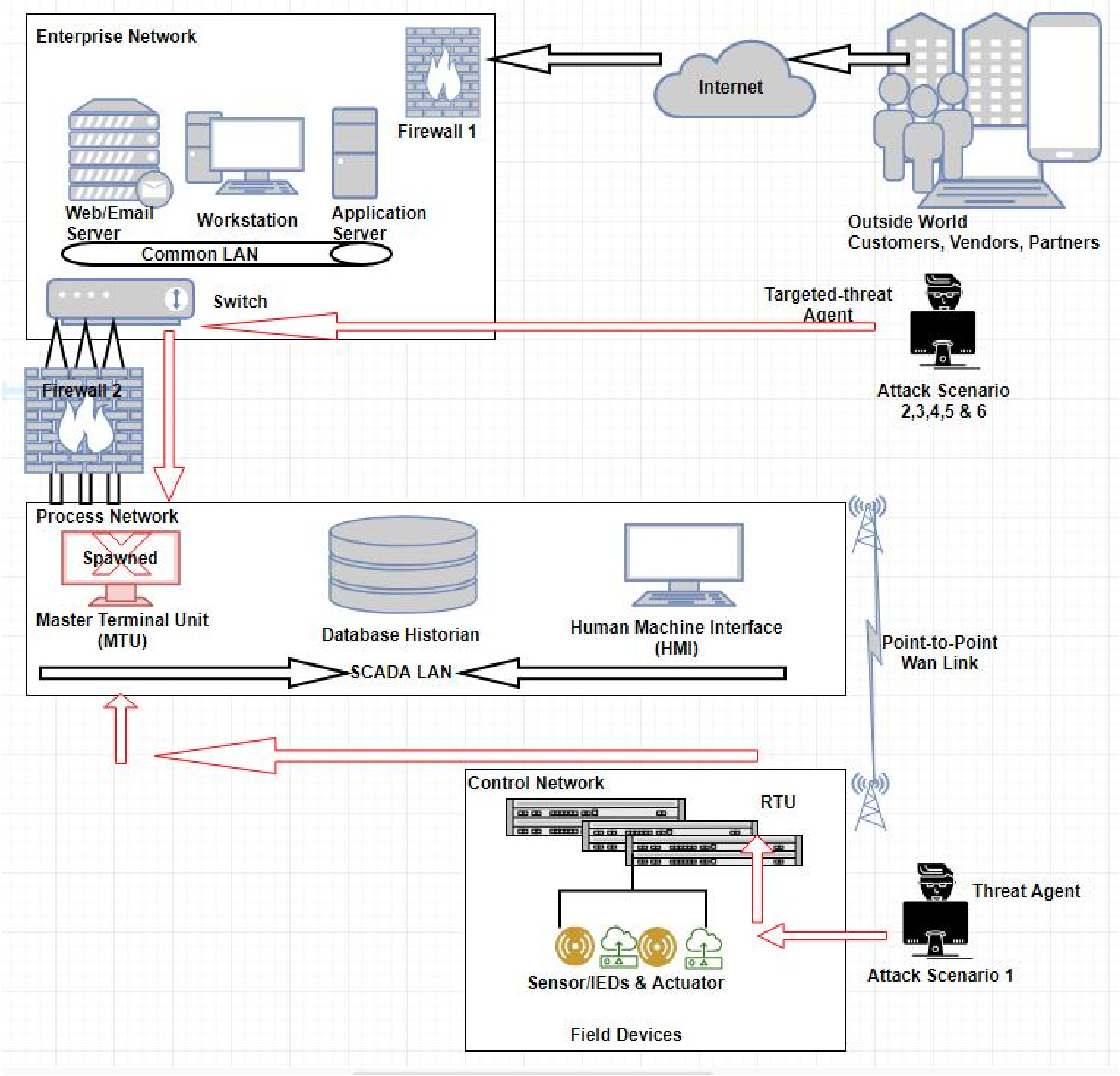


Figure. 3 (Image partly adopted from: The United States Government Accountability Office Report. GAO-04-354 [6], Practical SCADA for industry [7] and Journal of International Critical Infrastructure Protection [8])

5.2 Attack Scenario

We have been able to come up with six different attack models illustrated in the proceeding section of this chapter. The ultimate goal of our attack in each of the model is to compromise the integrity of data of a SCADA Master Terminal Unit. The MTU as explained previously is where the ultimate control decision is made and translated in the form of a command which is transmitted over the communication link and effected on the respective field devices. The effect of an MTU integrity-based compromise is far reaching and can result in physical damage. In the context of our work, we define integrity-based compromise as any attempt perpetrated by an attacker to circumvent the authority of the operator of the SCADA MTU gaining full control of the component and issuing out malicious instructions, or a deceptive action by a malicious agent geared towards luring the operator of the SCADA MTU to perform and issue out wrong commands in response to a false alarm.

The attack tree shows step by step attackers' approach of compromising the SCADA MTU in six different ways. Before an attack takes place the attacker with the capability and intention looks for a window of opportunity to penetrate and attack the system. We adopted the MITRE [25] initial access tactics and Cyber Threat Metrics [26] representing attack vectors which tells the six different ways attackers gain initial access to a target system in our approach in building the attack tree. We have also taken the work of security consultant Joaquin Rodriguez in "the most common attack vector for critical infrastructures [50]" to consolidate our choice of attack vectors.

5.2.1 Attack Scenario 1

Table 2. Attack Scenario 1

Attack Scenario 1	
Attack Goal	Compromising MTU integrity by Replay Attack
Attack Vector	Removable Media (USB) [25]
Attack Agents	Disgruntled Field Operative (Malicious Insider) and any Targeted-threat Agent [34]
Attack Scope	Control and Process Network

5.2.1.1 Attack Tree Model

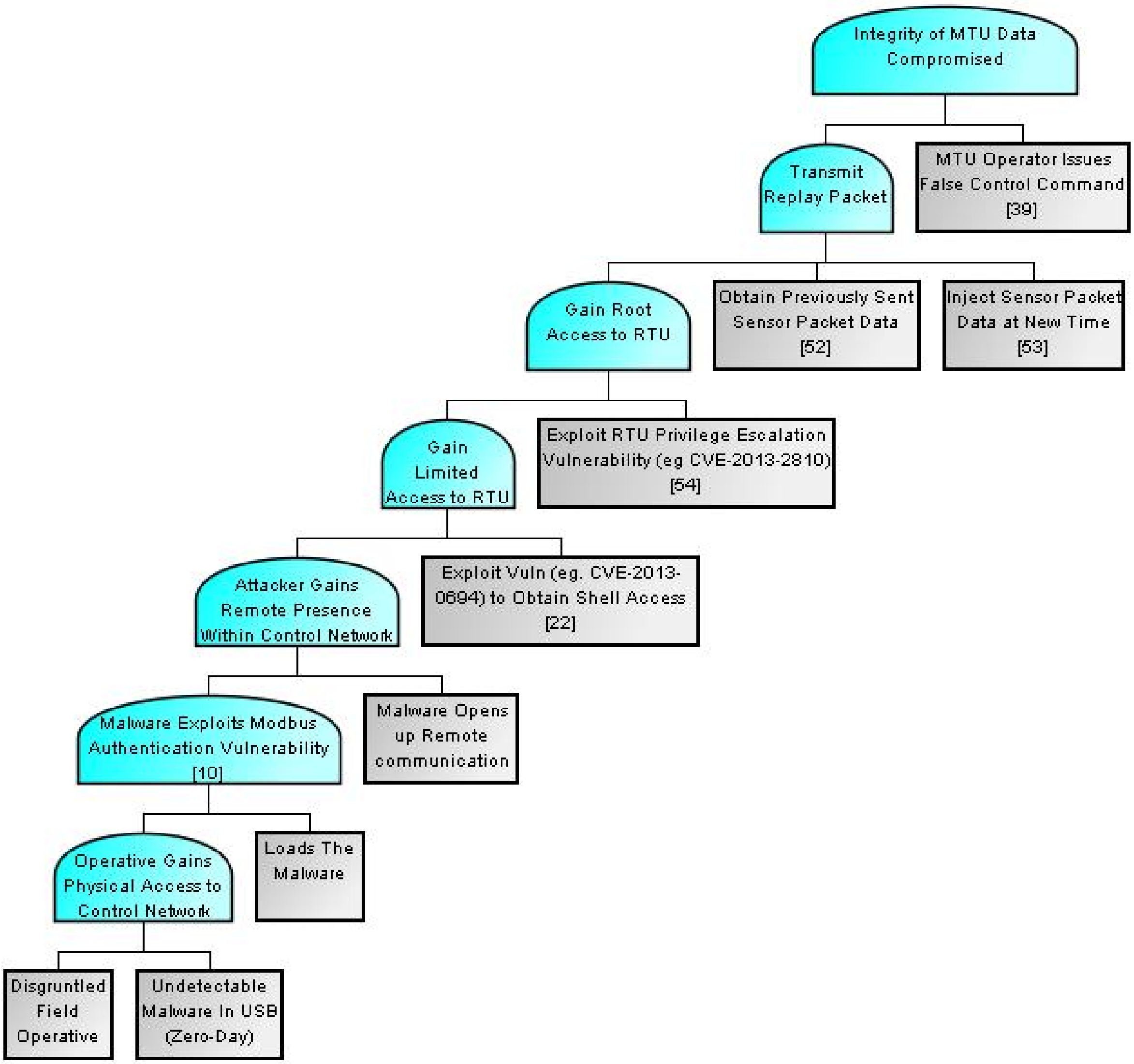

Integrity of MTU Data Compromised
Transmit Replay Packet
MTU Operator Issues False Control Command [39]
Gain Root Access to RTU
Obtain Previously Sent Sensor Packet Data [52]
Inject Sensor Packet Data at New Time [53]
Gain Limited Access to RTU
Exploit RTU Privilege Escalation Vulnerability (eg CVE-2013-2810) [54]
Attacker Gains Remote Presence Within Control Network
Exploit Vuln (eg. CVE-2013-0694) to Obtain Shell Access [22]
Malware Exploits Modbus Authentication Vulnerability [10]
Malware Opens up Remote communication
Operative Gains Physical Access to Control Network
Loads The Malware
Disgruntled Field Operative
Undetectable Malware In USB (Zero-Day)

Figure 4. Replay Attack Tree Model

The diagram in figure 4 above shows a single attack tree to compromise MTU SCADA integrity in the replay attack.

5.2.1.2 Assumptions Made

Prior to this attack certain assumptions are made:

- The attacker knows the schematics of the systems and geographical distribution of sensors
- The attacker has knowledge of which sensor controls a given area

- Attacker understands and can interpret sensor readings. He is also capable of altering sensor readings in sensor packet in such a way that the MTU operator at the process network would not dismiss as erroneous [40], and in response to the false alarm issue out the wrong command.
- The HMI and MTU functionality are integrated in a single workstation
- Attacker is able to clone or manipulate the HMI in such a way that it reveals exactly what is portrayed in the replay packet [51].
- Operative is not able to physically access the RTU
- All exploits used are zero-day

5.2.1.3 Attack Description

The goal here is to compromise the integrity of the SCADA MTU by transmitting replay packets. In a typical replay attack scenario we are considering a situation where packet is generated from the lower field device such as the sensors, transmitted to the control field device—the RTU which further transmits it to the SCADA MTU. In this attack an attacker is able to obtain packet generated at a previous time say t_0 from the sender which in this case is the field device—sensor, and transmit the packet at some other time [52] [53] say t_1 to the receiver which is the SCADA MTU. To achieve this goal the attacker takes series of steps as detailed in the attack tree. The success of this attack depends in part on the ability to gain elevated access to the RTU. The attacker is able to use the help of an insider known as a disgruntled field operative, with possession of an undetectable malware in USB (or other hardware eg laptop as the case may be). Malware is a zero day hence cannot be detected by security scanner and intrusion detection software since both security appliances do not have the signatures. Operative knowing his way around the control network and in possession of access credential is able to beat on-site security systems and gain physical access to specific site within the control network. Within the control network the operative introduces the malware (worm) by inserting the compromised USB into a device (for example laptop or any other hardware he can conveniently use to load malware, not necessarily the RTU directly). The malware exploits authentication vulnerability of the Modbus communication protocol [10] since it was specifically developed for this purpose, and as a result opens up remote communication with the attacker, enabling the attacker gather more intelligence about the system and further grant attacker remote presence within control network. Being present within target’s control network attacker is able to further exploit a known vulnerability that would enable him gain minimum level access to the RTU component. Typical of such vulnerability is identified as CVE-2013-0694, which is a vulnerability with a CVSS score rating of 8.8 inherent with the Emerson process management ROC800 RTU software 3.50 and earlier which contains credentials that have been hardcoded in their ROM thus making it easy for attacker to obtain shell access to the underlying component Operating System [22]. Once the attacker has gain preliminary user level access to the RTU he is able to elevate his privilege thus gaining administrative access to the device which would ultimately give him the opportunity to inject replay packet for onward transmission to the MTU. An attacker can elevate privilege by further exploiting vulnerability that is inherent in the RTU software. A typical example of this is with the CVE-2013-2810. This vulnerability is common with the “Emerson Process management ROC 800 RTU with software 3.50 and earlier, DL8000 RTU with software 2.30 and earlier, and ROC800L with software 1.20 and earlier [54]”. This vulnerability has a CVSS score of 9.8 meaning that exploitation of this can have an adverse effect on the integrity of the system [54]. This vulnerability can allow an attacker escalate privilege on the RTU granting him full access to the RTU, and with such access attacker is able to extract sensor packet data at one time, re-inject the data at some other time and transmit. With this action attacker is able to execute a replay attack. The attacker is thus able to transmit an old packet at a new time in a replay attack which would possibly cause the operator at the MTU to see the new malicious message as legit [39] and in response issue the wrong control command, and by virtue of issuing the wrong command the operator would have inadvertently compromised the integrity of the SCADA MTU. The effect of this integrity compromise can be far reaching and would equally translate in affecting vital processes of the SCADA system.

5.2.2 Attack Scenario 2

Table 3. Attack Scenario 2

Attack Scenario 2	
Attack Goal	Compromising MTU Integrity by SQL Injection Attack
Attack Vector	Drive-by Compromise [25]
Attack Agent	Targeted-threat Agent [35]
Attack Scope	SCADA Enterprise and Process Network

5.2.2.1 Attack Tree Model

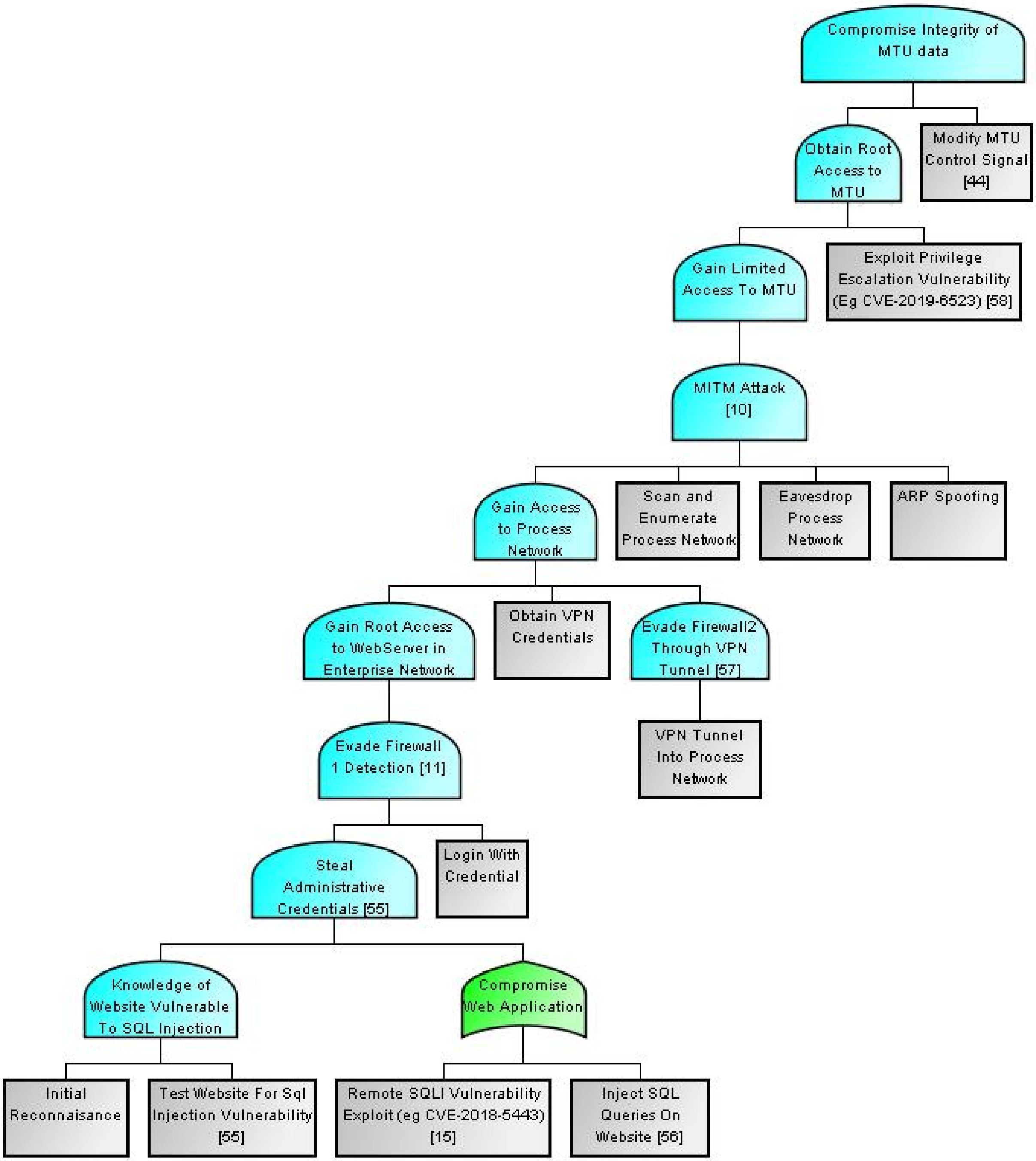

Compromise Integrity of MTU data
Obtain Root Access to MTU
Modify MTU Control Signal [44]
Gain Limited Access To MTU
Exploit Privilege Escalation Vulnerability (Eg CVE-2019-6523) [58]
MITM Attack [10]
Gain Access to Process Network
Scan and Enumerate Process Network
Eavesdrop Process Network
ARP Spoofing
Gain Root Access to WebServer in Enterprise Network
Obtain VPN Credentials
Evade Firewall2 Through VPN Tunnel [57]
VPN Tunnel Into Process Network
Evade Firewall 1 Detection [11]
Steal Administrative Credentials [55]
Login With Credential
Knowledge of Website Vulnerable To SQL Injection
Compromise Web Application
Initial Reconnaisance
Test Website For Sql Injection Vulnerability [55]
Remote SQLI Vulnerability Exploit (eg CVE-2018-5443) [15]
Inject SQL Queries On Website [56]

Figure 5. SQL Injection Attack Tree Model

5.2.2.2 Assumptions Made

- Web Application used at enterprise network is vulnerable to SQL injection attack.

- It is possible to access the process network component from remote locations
- Attacker is well vast with function code and can alter and manipulate data [20] at the MTU that is capable of causing a physical effect on the entire SCADA infrastructure.
- The Enterprise network connects to the process network via VPN tunneling.
- All exploits used are zero-day

5.2.2.3 Attack Description

SCADA software used at MTU has several loopholes because in most cases it has remained unpatched for a long period of time and possibly no longer supported by vendors [10]. It is not unusual to find an old application used on these devices. The main reason is because updating software or application may give rise to compatibility issues with most of the firmware and hardware used in the control system, degrading performance [10]. This is a loophole attacker exploit via SQL injection attack.

An attacker first tries to detect if a website is vulnerable to sql injection attack by carrying out initial reconnaissance and performing small sql injection test on target website [55]. Once test is confirmed positive he proceeds with compromising the web application via sql injection. Attacker can achieve this in either ways. First, he can carefully craft and inject sql queries on website [56] or he can leverage on known exploit, which might be a zero-day for instance. A typical example is identified as CVE-2018-5443 [15] which is vulnerability found in Advantech WebAccess SCADA software up to version 8.2 and the vulnerability has been declared as critical [15]. Although it's been reported that this vulnerability has been fixed for this product by upgrading to a higher version [15]. By virtue of compromising web application via sql injection attack, attacker is able to steal administrator credentials [55], and logging in with this credentials he is able to evade firewall 1 [11] detection thus gaining root access to the webserver in the Enterprise network. With the required access level offered by administrative access rights the attacker is able to obtain VPN credentials and use VPN tunneling techniques to tunnel into process network thus evading firewall 2 detection [57]. With the initial access into the process network the attacker is able to gather relevant information within the process network structure by scanning and enumeration process and by this act attacker is able to identify which node has a specific network address. Attacker eavesdrop communication within the process network and by

ARP spoofing technique he is able to successfully stage a man in the middle attack [10] enabling him gain limited access to the MTU. Since the target is the master terminal unit the attacker further escalates his privilege by taking advantage of some exploit. Typical example is with the vulnerability identified as CVE-2019-6523 found in Advantech WebAccess SCADA 8.3 software where it has been stated that the manipulation of this vulnerability can lead to privilege escalation [58]. The attacker finally gains root access to the MTU and by virtue of this access he can successfully modify MTU control signal [44] causing an integrity compromise at the MTU that would affect the SCADA system in entirety.

5.2.3 Attack Scenario 3

Table 4. Attack Scenario 3

Attack Scenario 3	
Attack Goal	Compromising MTU Integrity by Cross-site scripting Attack
Attack Vector	Malicious Web Component [26] (XSS Attack)
Attack Agent	Targeted-threat Agent [34]
Attack Scope	SCADA Enterprise and Process Network.

5.2.3.1 Attack Tree Model

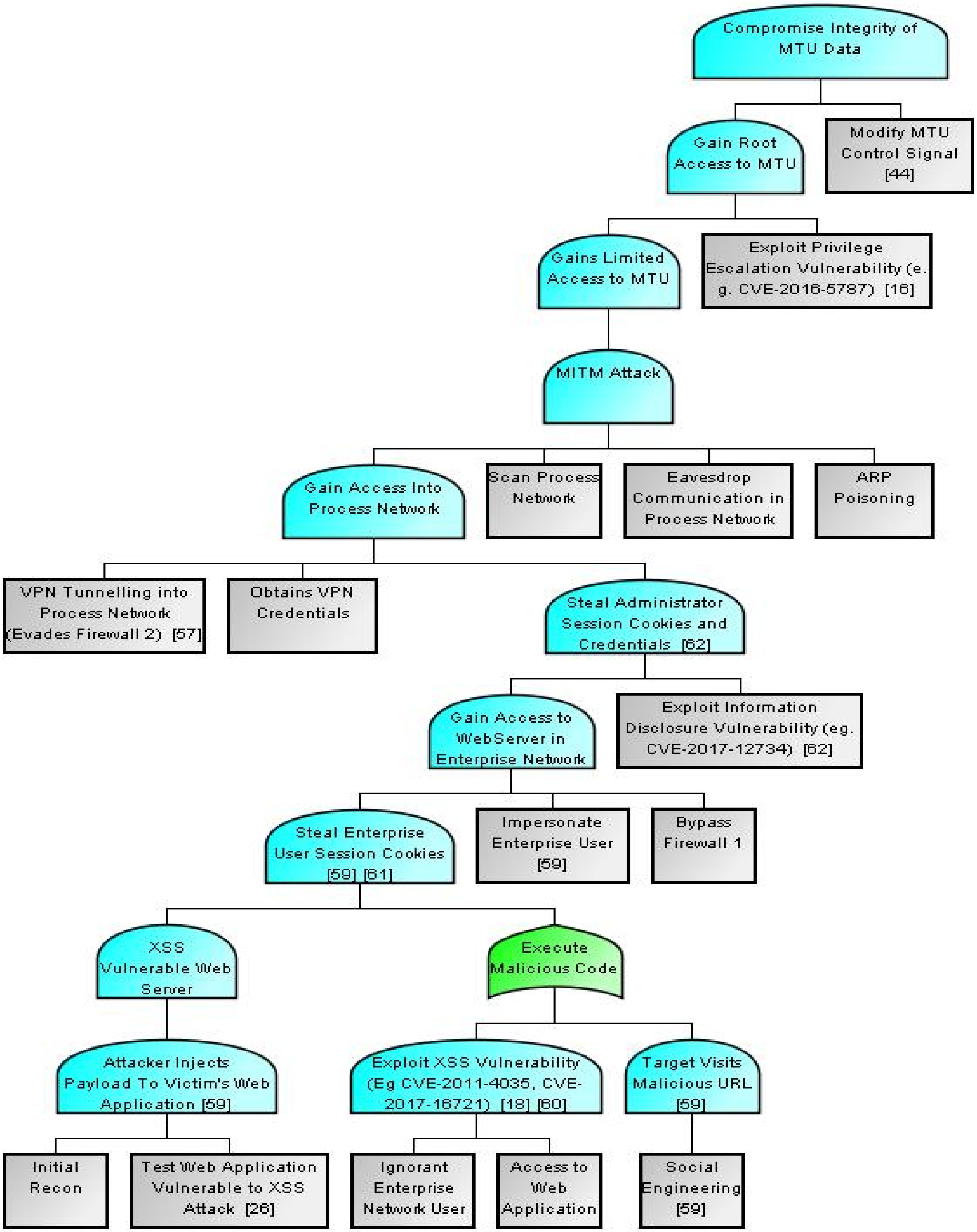

Compromise Integrity of MTU Data
Gain Root Access to MTU
Modify MTU Control Signal [44]
Gains Limited Access to MTU
Exploit Privilege Escalation Vulnerability (e.g. CVE-2016-5787) [16]
MITM Attack
Gain Access Into Process Network
Scan Process Network
Eavesdrop Communication in Process Network
ARP Poisoning
VPN Tunnelling into Process Network (Evades Firewall 2) [57]
Obtains VPN Credentials
Steal Administrator Session Cookies and Credentials [62]
Gain Access to WebServer in Enterprise Network
Exploit Information Disclosure Vulnerability (eg. CVE-2017-12734) [62]
Steal Enterprise User Session Cookies [59] [61]
Impersonate Enterprise User [59]
Bypass Firewall 1
XSS Vulnerable Web Server
Execute Malicious Code
Attacker Injects Payload To Victim's Web Application [59]
Exploit XSS Vulnerability (Eg CVE-2011-4035, CVE-2017-16721) [18] [60]
Target Visits Malicious URL [59]
Initial Recon
Test Web Application Vulnerable to XSS Attack [26]
Ignorant Enterprise Network User
Access to Web Application
Social Engineering [59]

Figure 6. Cross-site Scripting Attack Tree Model

5.2.3.2 Assumptions Made

- Web application in Enterprise Network is vulnerable to cross-site scripting attack
- Attacker has the capability of crafting and injecting malicious code to Web Application used on Enterprise Network
- Attacker is well vast with function code and can alter and manipulate data at the MTU [20] that is capable of causing a physical effect on the entire SCADA infrastructure
- Attacker is able to use social engineering technique to lure enterprise network user to visit XSS-compromised website.
- The Enterprise network connects to the process network via VPN tunneling.
- All exploits used are zero-day

5.2.3.3 Attack Description

Another possibility of compromising the SCADA MTU integrity is by staging a cross site scripting attack. This is an attack in which an attacker injects malicious code into the victim’s webpage, upon which the code executes once the victim visits the web page [11]. The attack can be carried out as demonstrated in the attack tree.

The attacker performs initial reconnaissance to gather relevant information regarding the victim who happens to be an ignorant Enterprise Network user. Attacker ascertains that the web application is vulnerable to cross-site scripting attack by conducting few tests. Once the test is positive attacker carefully crafts and inject payload (malicious code) into the victim’s web application [59]. Since execution of exploit code in cross site scripting attack depends on the target’s interaction with the vulnerable and compromised web application, the execution of the malicious code is achieved in two ways. First, via social engineering technique where attacker lures [59] the ignorant Enterprise Network user to visit malicious URL, and secondly via a known exploit. With respect to an exploit, a typical example of an XSS vulnerability for this purpose is identified as CVE-2017-16721, which is a vulnerability found in Geovap Reliance SCADA upto 4.7.3 update 2 [60], and CVE-2011-4035 found in Schneider Electric Vijeo Historan Web Server (applications such as Vijeo Historan v4.3 and earlier, citectHistoran v4.3 and earlier) [18], are just a few. It is stated that the attack can be launched remotely and no form of authentication is needed to exploit this vulnerability [60] [18]. By exploiting this vulnerability the attacker is thus able to steal cookie based authentication credentials and gain access to sensitive information [59] [61]. Being in possession of the victim’s cookie the attacker can have access to enterprise user’s session consequently impersonating him [59]. In this process, the attacker easily bypasses firewall 1 detection and gains access to the web server in the enterprise network. Once a foothold has been established within the enterprise network, the attacker can further exploit a known information disclosure vulnerability for example a vulnerability identified as CVE-2017-12734, is a vulnerability found in Siemens LOGO! up to 1.81.1, and known to affect confidentiality [62]. Although it is reported that this vulnerability has been fixed for this product by upgrading to a higher version [62]. By virtue of exploiting an information disclosure vulnerability the attacker is able to steal administrator’s session cookies credential [62] and also obtain VPN credentials. With the required access level offered by administrative access rights the attacker is able to use VPN tunneling techniques to tunnel and gain access into process network thus evading firewall 2 detection [57]. Within the process network, attacker performs some scanning operation to acquire more information, which enables him determine which node has a specific network address. With this information attacker can stage a man in the middle attack by eavesdropping on communication between components of the process network. Attacker is thus able to gain limited access to the MTU by this action. Attacker further exploit a known privilege escalation vulnerability for example, vulnerability identified as CVE-2016-5787 and found in SCADA CIMPLICITY up to 8.1, whose manipulation results to privilege escalation [16]. Although it is reported that this vulnerability has been eliminated on this product by upgrading to a higher version [16]. By virtue of exploiting this vulnerability attacker is able to gain root access to the MTU which gives him ultimate control over the MTU and with such control he is able to modify MTU control signal [44], compromising the integrity of data of the MTU which would consequently result in manifesting a physical effect on the SCADA system as a whole.

5.2.4 Attack Scenario 4

Table 5. Attack Scenario 4

Attack Scenario 4	
Attack Goal	Compromising Integrity of MTU by Buffer Overflow Attack

Attack Vector	Malicious Web Component [26] (Buffer Overflow)
Attack Agent	Targeted-threat Agent [34]
Attack Scope	SCADA Enterprise and Process Network

5.2.4.1 Attack Tree Model

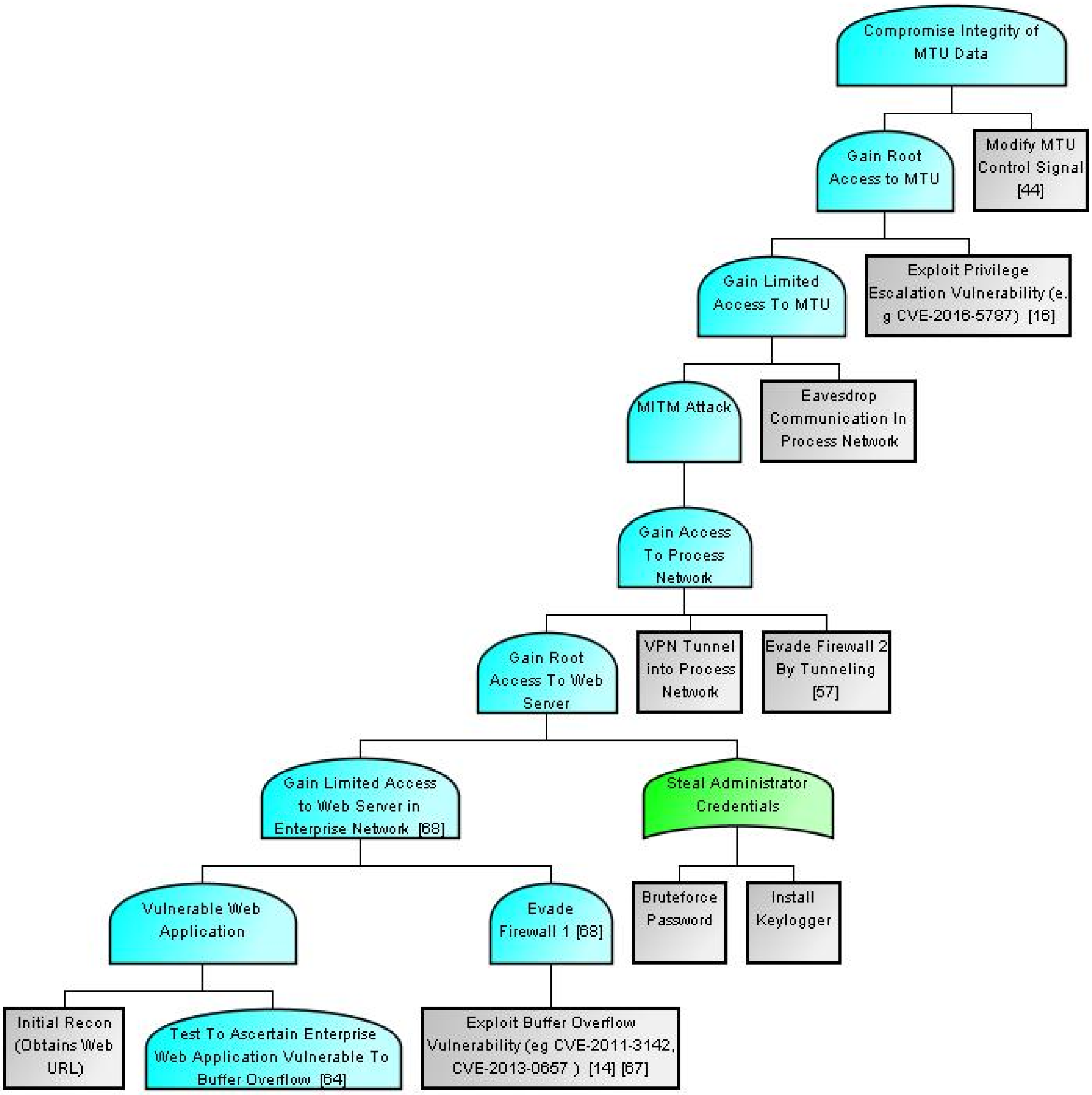

Compromise Integrity of MTU Data
Gain Root Access to MTU
Modify MTU Control Signal [44]
Gain Limited Access To MTU
Exploit Privilege Escalation Vulnerability (e.g CVE-2016-5787) [16]
MITM Attack
Eavesdrop Communication In Process Network
Gain Access To Process Network
Gain Root Access To Web Server
VPN Tunnel into Process Network
Evade Firewall 2 By Tunneling [57]
Gain Limited Access to Web Server in Enterprise Network [68]
Steal Administrator Credentials
Vulnerable Web Application
Evade Firewall 1 [68]
Bruteforce Password
Install Keylogger
Initial Recon (Obtains Web URL)
Test To Ascertain Enterprise Web Application Vulnerable To Buffer Overflow [64]
Exploit Buffer Overflow Vulnerability (eg CVE-2011-3142, CVE-2013-0657) [14] [67]

Figure 7. Buffer Overflow Attack Tree Model

5.2.4.2 Assumptions made

- Web Application in Enterprise Network is vulnerable to Buffer overflow attack
- Attacker is capable of crafting and injecting arbitrary code inputs to the web application used at the enterprise network to eventually take control of the machine.
- Attacker is able to use VPN to tunnel into different network areas
- Attacker is well vast with function code and can alter and manipulate data [20] at the MTU that is capable of causing a physical effect on the entire SCADA infrastructure
- All exploits used are zero-day

5.2.4.3 Attack Description

With a buffer overflow attack an attacker can send carefully crafted code input to a web based application causing the application to execute arbitrary code and possibly taking control of the web application server [63]. The attack is explained thus:

First off, attacker is able to ascertain that the web application used at Enterprise network is vulnerable to buffer overflow attack by carrying out some preliminary tests [64] while performing some initial reconnaissance and gathering information about the system and network configurations, once the vulnerability is confirmed attacker is able to exploit this vulnerability either by crafting the required exploit code [65] [66] to compromise the system or using a known exploit. An example of a known exploit is given by CVE-2011-3142, which is a vulnerability found in WellinTech KingView 6.52/6.53 and has been rated as very critical [14]. Another typical example is giving in CVE-2013-0657 which is a vulnerability found in Schneider Electric Interactive Graphical SCADA system upto 9.0 [67]. Both of this vulnerability has been allocated a CVSS score of 10.0 depicting its high criticality and the attack can also be executed remotely without authentication, as at time of writing this there is no information about possible countermeasure [14] [67]. By virtue of exploiting this vulnerability the attacker is able to gain limited access to the web server in Enterprise Network [68] thus evading firewall 1 detection. In an attempt to increase his access level, attacker steals administrator credentials either by brute forcing password or by installing keylogger to log keystrokes. Attacker is thus able to gain root access to web server, and with this access level he is able to obtain VPN tunnel access, tunneling and gaining access into the process network evading firewall 2 detection in the process [57]. With limited access within the process network attacker is able to scan the network and obtain useful information about the components hence determining which component is the MTU. He then stages a man in the middle attack to gain limited access to the MTU. In a bid to increasing his access level attacker is able to exploit privilege escalation vulnerability. Notable example of such vulnerability is identified as CVE-2016-5787, which is a vulnerability found in General Electric Digital Proficy SCADA [16]. Exploitation of this vulnerability leads to escalated privilege hence attacker is able to gain root access to the MTU. With this access level attacker is able to modify MTU control signal [44] thus compromising the integrity of data from this component which will translate in compromising the SCADA system as a whole resulting to a physical damage.

5.2.5 Attack Scenario 5

Table 6: Attack Scenario 5

Attack Scenario 5	
Attack Goal	Compromising MTU Integrity by Spear Phishing
Attack Vector	Spear Phishing Attachment [25]
Attack Agent	Targeted-threat Agent [35]
Attack Scope	SCADA Enterprise and Process Network

5.2.5.1 Attack Tree Model

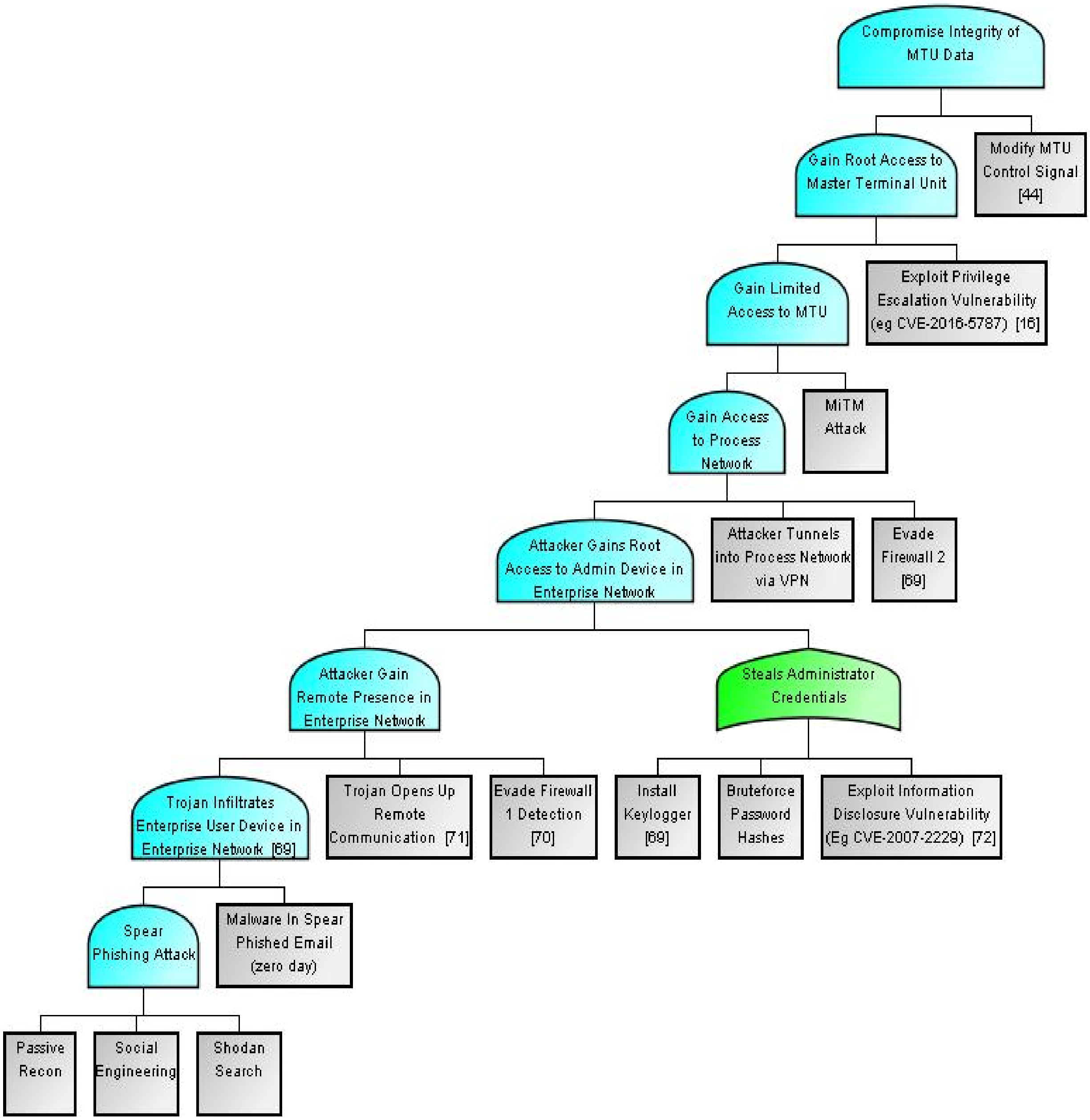

Compromise Integrity of MTU Data
Gain Root Access to Master Terminal Unit
Modify MTU Control Signal [44]
Gain Limited Access to MTU
Exploit Privilege Escalation Vulnerability (eg CVE-2016-5787) [16]
Gain Access to Process Network
MiTM Attack
Attacker Gains Root Access to Admin Device in Enterprise Network
Attacker Tunnels into Process Network via VPN
Evade Firewall 2 [69]
Attacker Gain Remote Presence in Enterprise Network
Steals Administrator Credentials
Trojan Infiltrates Enterprise User Device in Enterprise Network [69]
Trojan Opens Up Remote Communication [71]
Evade Firewall 1 Detection [70]
Install Keylogger [69]
Bruteforce Password Hashes
Exploit Information Disclosure Vulnerability (Eg CVE-2007-2229) [72]
Spear Phishing Attack
Malware In Spear Phished Email (zero day)
Passive Recon
Social Engineering
Shodan Search

Figure 8. Spear Phishing Attack Tree Model

5.2.5.2 Assumptions Made

- Attacker is capable of using spear phishing attachment to initiate attack process
- Firewall and other detection systems is not capable of detecting malware in spear phished attachment since they don’t have the signature

- Attacker is well vast with function code and can alter and manipulate data [20] at the MTU that is capable of causing a physical effect on the entire SCADA infrastructure
- Attacker is capable of obtaining VPN credentials to tunnel into process network.
- All exploits used are zero-day

5.2.5.3 Attack Description

With spear phishing as attack vector the attacker use spear phished email with malware attachment to infiltrate target's network. The method illustrated here is similar to that which was adopted to compromise the Ukraine power grid in 2015 [69] and also the black energy 3 Trojan attack [69]. The attacker is able to obtain information of prominent personnel within the enterprise network through different social engineering techniques, as well as passive reconnaissance and shodan search to obtain other important information about the target system. With this information attacker carefully constructs and delivers a spear phished mail laden with malware to the target who then inadvertently opens and deploys the malware into the devices within the enterprise network [69]. Spear phishing utilizes a combination of email spoofing, drive-by downloads and dynamic URLs to possibly evade existing firewall defenses especially with the use o zero-day malware in such malicious attachments [70]. The Trojan initiates a call back, opening up remote communication likened to command and control server with the remote attacker which aids attacker extract information about the network, issue command and perform further exploits [71]. The Trojan also ensures attacker maintain presence within enterprise network while performing stealth reconnaissance to evade firewall or antivirus detection [69]. With the amount of information gathered attacker is able to steal administrator credentials either by using the malware to install keylogger [69], exploiting a known information disclosure vulnerability (for purpose of illustration: Microsoft windows which is the assumed operating system deployed at the enterprise network has an information disclosure vulnerability identified as CVE-2007-2229, capable of affecting component of file system [72]) or bruteforcing password hashes. With the help of administrator credentials obtained, attacker is able to gain root access to admin device in enterprise network. With this access level attacker is able to tunnel into process network by way of VPN tunneling thus evading firewall 2 detection [69]. Within the process network attacker stages a man in the middle attack to gain limited access to the MTU. And with the help of an exploit attacker is able to escalate his privilege (for example vulnerability identified as CVE-2016-5787 [16]) to obtain root access level to the MTU component. With this access level attacker has unlimited capabilities to compromise the integrity of the system by modifying MTU control signals [44], which to a large extent will result in a physical effect.

5.2.6 Attack Scenario 6

Table 7: Attack Scenario 6

Attack Scenario 6	
Attack Goal	Compromising MTU Integrity using Viruses and Malwares
Attack Vector	Various Malwares [26] (APT-Like)
Attack Agent	Targeted-threat Agent [34]
Attack Scope	SCADA Enterprise and Process Network

5.2.6.1 Attack Tree Model

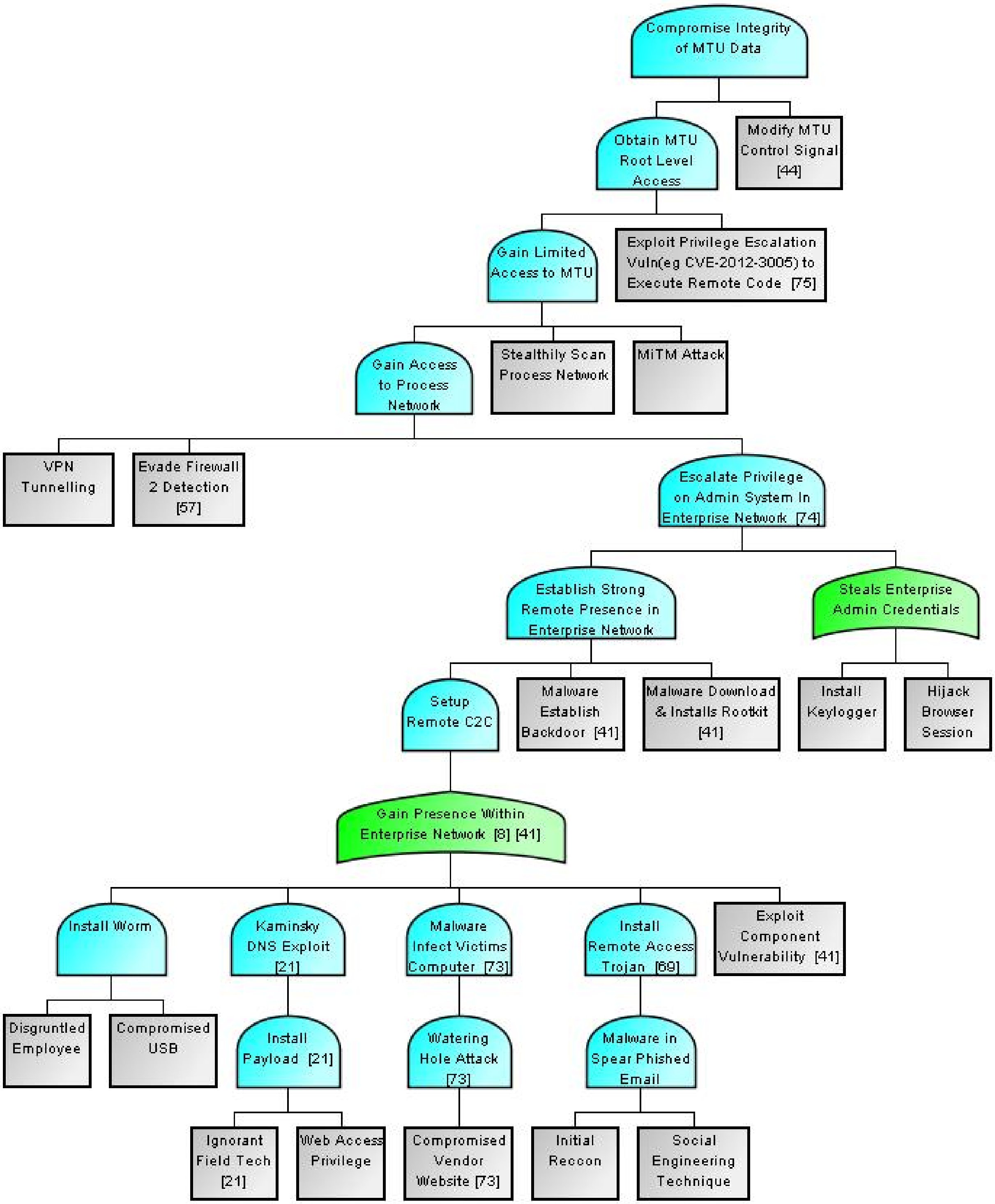

Compromise Integrity of MTU Data
Obtain MTU Root Level Access
Modify MTU Control Signal [44]
Gain Limited Access to MTU
Exploit Privilege Escalation Vuln(eg CVE-2012-3005) to Execute Remote Code [75]
Gain Access to Process Network
Stealthily Scan Process Network
MiTM Attack
VPN Tunnelling
Evade Firewall 2 Detection [57]
Escalate Privilege on Admin System In Enterprise Network [74]
Establish Strong Remote Presence in Enterprise Network
Steals Enterprise Admin Credentials
Setup Remote C2C
Malware Establish Backdoor [41]
Malware Download & Installs Rootkit [41]
Install Keylogger
Hijack Browser Session
Gain Presence Within Enterprise Network [8] [41]
Install Worm
Kaminsky DNS Exploit [21]
Malware Infect Victims Computer [73]
Install Remote Access Trojan [69]
Exploit Component Vulnerability [41]
Disgruntled Employee
Compromised USB
Install Payload [21]
Watering Hole Attack [73]
Malware in Spear Phished Email
Ignorant Field Tech [21]
Web Access Privilege
Compromised Vendor Website [73]
Initial Reccon
Social Engineering Technique

Figure 9. Various Malwares Attack Tree Model

5.2.6.2 Assumptions Made

- Attacker has the necessary VPN skills to successfully tunnel between different networks.
- Attacker is well vast with function code and can alter and manipulate data [20] at the MTU that is capable of causing a physical effect on the entire SCADA infrastructure.
- All exploits used are zero-day

5.2.6.3 Attack Description

In an advanced persistent threat an attacker dedicates time, resource and with best of skills and capability in compromising a targeted system. There are several variants of an APT attack but in general the following attack steps in conjunction with the attack tree above can be used to describe the process.

This attack mimics the situation of a typical APT. In an APT attacker has unlimited resource to compromise the target system. As shown in the attack tree we have enumerated all possible (five 5) initial access route to portray the true definition of APT.

Since this attack is mostly targeted the attacker uses spear phishing as the primary attack vector. Information used to construct the spear phished email is usually obtained from intensive initial recon process as well as social engineering techniques. A victim falling for spear phishing tactics would inadvertently deploy the remote access Trojan to the network consequently giving the attacker initial presence within the enterprise network. From the attack tree other ways of deploying this Trojan could be through a disgruntled employee who has been bought over as an insider conspirator—He can deliver the Trojan by way of compromised USB. Also by exploiting vulnerability in devices within the enterprise network—for example the print spooler exploit as was the case with Flame and LNK exploit with stuxnet [41]. Also through watering hole attack where employees of the SCADA company visits its vendor's website in a bid to download and install component updates as was the case with Havex [73]; and also through the Kaminsky DNS exploit—where an ignorant field operative accessing the webpage of SCADA application with the intention of obtaining latest patch or general information surfing, is being redirected to another webpage that is malware laden [21]. With the help of undetectable malware the attacker gains presence within the enterprise network thus evading firewall 1 detection as was the case with Stuxnet [8] and Flame [41]. Once a foothold has been established within the enterprise network the malware opens up a command and control server to its remote site for frequent communication with its handlers and in the process the attacker uses this medium to execute further action such as establishing strong presence via backdoor and rootkit infections to operate stealthily [41]. With this strong presence the attacker is able to gather more information, perform stealth scan, install keylogger to obtain keystroke eventually leading to obtaining user and administrative credentials to escalate privilege [74]. With this increased access level attacker is able to obtain VPN access enabling him to tunnel into the process network evading firewall 2 detection in the act [57]. Once a foothold is established in the process network stealth scanning takes place and data exfiltration and analysis enables the attacker determine which node is the MTU. Attacker eventually gains limited access to the MTU by staging a man-in-the-middle attack. In order to increase this access level attacker exploit a known privilege escalation vulnerability for example the Multiple Invensys Product Privilege escalation vulnerability in wonderware application server, wonderware information server, Foxboro control software and identified as CVE-2012-3005 is known to allow local users gain privileges via Trojan horse DLL [75], he is able to increase his privilege to the MTU enabling him assume administrative role and taking control of the command issuing process to modify MTU control signal [44], consequently compromising integrity of data transmitted from the MTU which would ultimately affect the normal operation of the SCADA as a whole.

5.3 Determination of Respective Attack Sophistication Index for SCADA Attack Scenarios

Now that we have come up with the attack scenarios and attack tree model depicting all possible ways of compromising the SCADA MTU integrity, it is important for us to review our mode of analysis and comparison of attack sophistication levels. We will us the model or better put the framework developed by Sanjay Goel and Nick DePaula in their work on attack sophistication analysis for this purpose. According to the authors it is stated that an attack that has the following five features namely: social engineering through spear phishing, Remote Administration, Stealth, use of zero day vulnerabilities, and APT, can be analyzed as sophisticated depending on the number of features present in such attack [43]. For example, an attack that uses all five features is considered the most sophisticated while an attack that uses just 1 feature is considered least sophisticated. Some of the nodes in our attack tree model do not exactly depict the feature but with proper coinage we will be able to map these nodes with the respective feature. By way of analyzing attack sophistication through this method, it will enable us determine and compare the relative sophistication levels of each of the attack models. More of this analysis is given in chapter 6 of this work.

6. Analysis and Results

In this chapter we shall be carrying out a comparative analysis of the respective attack sophistication for each of the attack tree model detailed in chapter 5. To achieve this, we shall be using the sophistication index framework presented by Sanjay Goel and Nick DePaula. A succinct review of their work has been given under the literature review section of this work, and also the categorization of sophistication index has been presented in tabular form in the appendix B section.

First off, we will juxtapose in a tabular form the various sophistication index features with attack nodes derived from our attack tree model, and assign a value for perceived sophistication index, depending on the use or prevalence of any of the features in the respective attack model. The description of the SI features in the chart (see appendix) will help us adjudge the placement of SI values. Thereafter we will calculate the sum total of the SI values to determine the overall sophistication. Upon completion of this process, we would have determined the sophistication index value for each of the six attack model. The evaluation and comparison will be made thereafter. By virtue of doing this we will then be able to give answers to our research questions and present a summary.

It is important to mention here that during the course of modeling our attack tree we made some important assumptions. These assumptions will also be put into consideration in the derivation and determination of the overall sophistication. This is because the assumptions are vital part of the attack and the completion and eventual success of the respective attacks would not be possible if these assumptions are not factored in. Armed with these detail, we shall proceed with the classification.

6.1 Analysis of Attack Scenario 1

6.1.1 Determination of Sophistication Index for Replay Attack Scenario

The table below shows the generation of sophistication index for the replay attack tree model. Social engineering was assigned a score of zero since no social engineering technique was applied in attack tree generation. Although attacker must have used a certain social engineering technique to acquire information about the schematics of the system and distribution of sensors but certainly not a technique that involved spear phishing. Further, this attack certainly involved deployment of remote administration tool since the attack characteristics involves remote administration, the attacker can only possibly use a RAT to inject sensor packet data and transmit replay packet. The Malware (Trojan) also created a backdoor that helped attacker gain access to the control network, hence a positive for the SI. The design of the malware and its mode of propagation which enables it exploit authentication vulnerability and grants attacker access to the control network depict stealth since this operation can only be successful if hidden, hence the reason for a positive SI. It is generally assumed that all exploits used in our attack are zero-day since the success of the attack depends to a larger extent on the undetectability by any security appliance, hence only zero-day can guarantee such. A condition to assigning a positive for APT is that the attack must use multiple (at least 3) zero-day vulnerabilities which was the case in this attack. Put together we have a total of 4 out of 5 for the overall sophistication index.

6.1.2 Result

Table 8: Result of Analysis for Attack Scenario 1

Feature Type	Attack Nodes From Model	SI Score
Social Engineering	None	0
Remote Administration	“Malware Opens up Remote Communication”; “Inject Sensor Packet Data”; “Transmit Replay Packet”	1
Stealth	“Modbus authentication vulnerability exploited leading to undetected access to control network”	1
Zero-Day vulnerability	“Malware present in USB for initial compromise” and two Zero-day vulnerabilities exploited—First: to obtain shell access to remotely administer control on RTU, Second: to escalate privilege.	1
APT	Multiple zero-day exploits used namely: Modbus Authentication vulnerability exploit, RTU credential vulnerability exploit to obtain shell access and RTU	1

	privilege escalation vulnerability exploit.	
Total		**4**

6.2 Analysis of Attack Scenario 2

6.2.1 Determination of Sophistication Index for SQL Injection Attack Scenario

The table shows the classification and assignment of SI score for the attack model involving SQL injection as an attack vector. In this attack Social engineering by spear phishing is not a requirement for execution hence an SI score of zero. Regardless the attack certainly involves the administration of a remote access tool to perform the sql injection, to obtain administrative credentials, to deploy VPN tunneling and to stage man-in-the-middle attack hence a positive for the SI. VPN tunneling enables the attacker evades firewall detection since VPN involves using an encrypted channel to route the traffic. The purpose of applying encryption in VPN is definitely to disguise one's activity hence a stealth approach. Recall that we have assumed all the exploits used for this attack to be zero-day to drastically reduce the chance of detection by any security device, thus we assign a positive for this SI. For this attack APT is less likely to be considered since we have fewer exploits than required. Overall we deduce a sophistication index of 3 out of 5 for this attack model.

6.2.2 Result

Table 9. Result of Analysis for Attack Scenario 2

Feature Type	**Attack Nodes From Model**	**SI Score**
Social Engineering	None	0
Remote Administration	"Inject SQL queries"; "Steal Administrative Credentials"; "VPN tunneling"; "MITM Attack"	1
Stealth	"VPN tunneling"; "Evade Firewall detection"	1
Zero-Day Vulnerability	Two zero-day used: First: Remote SQL vulnerability exploit; Second:	1

	Exploited Vulnerability for Privilege Escalation.	
APT	None	0
Total		**3**

6.3 Analysis of Attack Scenario 3

6.3.1 Determination of Sophistication Index for Cross-site scripting Attack Scenario

The table below shows the analyzed sophistication index for an attack involving cross-site scripting vector. Social engineering is a requirement for the success of this attack since the execution of the payload requires user interaction with the compromised URL; the attacker devises a means to lure the unsuspecting victim to visit malicious URL. This means is well achievable via spear phishing email so we have assigned an SI of 1 for this attack feature. Remote administration is a necessity to further on this attack since processes involving XSS payload injection to web application, stealing admin credentials and session cookies, VPN tunneling and MITM attack requires it. VPN Tunneling is also considered a stealth approach since it involves using encrypted communication channel. We have also used multiple zero day exploit such as XSS exploit, information disclosure vulnerability exploit, and privilege escalation vulnerability exploit. The presence of multiple exploits and the deployment of techniques that will involve obtaining user sessions and impersonating the user is considered an APT according to the reference given earlier. In totality this attack involve all 5 features hence we have assigned a sophistication index of 5.

6.3.2 Result

Table 10: Result of Analysis for Attack Scenario 3

Feature Type	**Attack Nodes From Model**	**SI Score**
Social Engineering	“Target Visits Malicious URL”	1
Remote Administration	“XSS payload injected to web Application”, “Steal Session Cookies”; “Steal Administrator Credentials”; “VPN Tunneling”; “MITM Attack”	1

Stealth	“VPN Tunneling”	1
Zero-Day Vulnerability	Three Zero-day used. “Xss Vulnerability exploit”; “Information disclosure vulnerability exploit”; “Privilege Escalation Vulnerability exploit”	1
APT	Multiple Zero-day exploits; Steal User Session; “Impersonate User”	1
Total		**5**

6.4 Analysis of Attack Scenario 4

6.4.1 Determination of Sophistication Index for Buffer Overflow Attack Scenario

In a buffer overflow attack, an attacker takes advantage of the vulnerable web application to compromise and infiltrate the system. An attack of this nature leading up to the goal does not include an element of social engineering hence we have allocated an SI score of zero. Remote administration is a requirement in the aspect of VPN tunneling and man in the middle attack since this process is administered using specialized tools from a remote location. Also, in this attack stealth is achieved using VPN tunneling to evade firewall detection due to its encrypted nature. Two zero day vulnerability also has been identified for this attack namely the vulnerability presented by the web application to buffer overflow and the vulnerability exploited to escalate privilege. APT is considered not a requirement here. Overall we have a total sophistication index value of 3 out of 5 for this attack.

6.4.2 Result

Table 11: Result of Analysis for Attack Scenario 4

Feature Type	**Attack Nodes From Model**	**SI Score**
Social Engineering	None	0
Remote Administration	“VPN tunneling”; “MITM Attack”	1
Stealth	“VPN tunneling to evade firewall”	1
Zero-Day Vulnerability	Two Zero-day used. “Buffer Overflow vulnerability exploit”;	1

	“Privilege Escalation Vulnerability exploit”	
APT	None	0
Total		**3**

6.5 Analysis of Attack Scenario 5

6.5.1 Determination of Sophistication Index for Spear Phishing Attack Scenario

A well constructed spear phishing email by some experienced attacker is very difficult to detect and the success rate is almost certain. This attack deploys spear phishing technique to deliver the malicious content to the unsuspecting victim. With the use of this technique we have assigned a positive for the SI score for social engineering. To further on his mission the attacker deploys remote administrative tool to steal administrator credential, to create or use existing VPN tunnels to move between networks and to stage man in the middle attack, hence we have assigned a positive here as well. Reiterating our attack VPN tunneling technique involves a stealth operation hence we have assigned a positive as well. Two zero day vulnerabilities namely information disclosure and privilege escalation vulnerabilities have also been identified as a requirement for this attack so we assigned a positive for this feature type too. APT is not a requirement here so we have no score for it. In total we have assigned a sophistication index score of 4 out of 5 for attack involving spear phishing attachment as vector.

6.5.2 Result

Table 12. Result of Analysis for Attack Scenario 5

Feature Type	**Attack Nodes From Model**	**SI Score**
Social Engineering	“Malware in Spear Phished email”	1
Remote Administration	“Trojan opens up remote communication”; “Steals Admin credentials”; “VPN Tunneling”; “MITM Attack”	1
Stealth	“VPN Tunneling”	1

Zero-Day Vulnerability	Two zero-day used. “Information disclosure vulnerability exploit” and “privilege escalation vulnerability exploit”	1
APT	None	0
Total		**4**

6.6 Analysis of Attack Scenario 6

6.6.1 Determination of Sophistication Index for Various Malwares (APT-like) Attack Scenario

In this scenario we are assuming the adversary is a nation state actor that deploys greater sophisticated attack mechanism to compromise the system. An attacker of this nature has all the resource and capabilities to stage an attack and most of the time his strategies are usually successful. We considered that spear phishing is one of the initial route to penetrate the system amongst others considered by the attacker hence we have assigned a positive SI score for social engineering by spear phishing. Looking at the attack tree the progressive attack involve use of malware to establish a backdoor and a remote command and control to issue further instruction and exfiltrate information consequently stealing credentials and staging MITM attack as required. As a result of this we have assigned a positive for SI score involving remote administration. Stealth is one vital requirement for all attacks of this nature as the attacker tries as much as possible to ensure the covert nature of the attack while within target premise to avoid detection. In that light rootkit and encryption via VPN tunneling for lateral movement to the process network has been deployed. In this attack we have also considered two zero day exploits which are the component vulnerability exploit and exploit for privilege escalation. We have also considered kaminsky exploit being a technique used to gain initial presence to the enterprise network as one technique involving APT, hence a positive for this feature as well. In total we have assigned an SI score of 5 for attack deploying various malwares as vectors.

6.6.2 Result

Table 13: Result of Analysis for Attack Scenario 6

Feature Type	**Attack Nodes From Model**	**SI Score**
Social Engineering	“Malware in Spear Phished email”	1
Remote Administration	“Malware establish backdoor”; “Steal Credentials”; “MITM Attack”	1
Stealth	“Rootkit Installed via backdoor”; “VPN Tunneling”	1
Zero-Day Vulnerability	Two zero-day used. “Component vulnerability exploit” and “Privilege escalation vulnerability exploit”	1
APT	Multiple exploits used including Kaminsky DNS exploit, Component vulnerability exploit, and Privilege escalation exploit	1
Total		**5**

6.7 Comparing the Sophistication Indexes of Attack Models.

Table 14: Comparison of Sophistication Indexes for All Attack Scenarios

Feature Type/SI Score	**Scenario 1 (Replay Attack)**	**Scenario 2 (SQLI)**	**Scenario 3 (XSS)**	**Scenario 4 (BOF)**	**Scenario 5 (Spear Phishing)**	**Scenario 6 (Malwares)**
Social Engineering	0	0	1	0	1	1
Remote Admnistration	1	1	1	1	1	1
Stealth	1	1	1	1	1	1
Zero-Day Vulnerability	1	1	1	1	1	1
APT	1	0	1	0	0	1
Total	**4**	**3**	**5**	**3**	**4**	**5**

6.8 Summary

The above table shows at a glance the sophistication index classification and the derived SI score for all the attack scenarios analyzed. The attack scenario analyzed comprises attacks capable of compromising the integrity of a SCADA MTU from 6 attack vectors such as Replay attack, SQL injection, Cross-site scripting, Buffer overflow, Spear Phishing, and the use of various malwares. From the table it can be inferred that attack that uses all 5 feature types are considered the most sophisticated. Referencing and comparing our attack tree model with this table shows that the cross-site scripting attack model and attack model involving the use of various malwares used all of the 5 features in its development hence is regarded as the most sophisticated. It is important here to state that attacks that uses multiple (three or more) exploits of which mostly are zero-days have a higher success rate compared to attack that uses traditional exploits or attack mechanism since the former cannot be halted by defense mechanisms in place and has very little chance of detection.

Furthermore, the Replay attack has an APT feature but the derived SI score is 4. This is because of the absence of social engineering feature. In this attack, the prime adversary relies on the service of a disgruntled employee to deliver the malware via USB drive. This pose some difficulty and the chances of delivery is slim considering the nature of security within the control network in real life instance. So viewing from logical perspective, it can be considered relatively effective to stage an attack that does not involve human-factor physical presence to infiltrate and compromise the system. Apart from using the service of a malicious insider the prime attacker can also spread the malware to third party vendors of the SCADA company who without knowing it will deploy the malware on direct interaction with the SCADA component, as was the case with Stuxnet [76] but this hasn't been considered in this attack.

Attack involving spear phishing resulted in an SI score of 4. This attack although having to use fewer exploits still have the possibility of achieving success since the attacker's initial access to target network is via well constructed spear phished attachment. The very fact that most humans fall prey to continual neglect and non-implementation of security best practices makes this attack highly feasible and successful. Despite having equal SI score with the replay attack, if all other conditions remains the same I would rather adjudge spear phishing a little above replay attacks in terms of sophistication and likelihood of success.

Finally, the attacks involving SQL injection and Buffer overflow have each a derived SI score of 3. It is important to note that both these attacks use fewer exploits and lack the social engineering by spear phishing feature, hence judging from our analysis the least sophisticated. Having completed the analysis we can take a second look at the research questions and try to answer them.

6.8.1 Review of Research Questions

Question 1: What are the possible attack paths that can result in the compromise of MTU data integrity?

Answer: The attack paths are the routes that an attacker takes to compromise the system. We have modeled the six different attack paths or scenarios (see chapter 5) using the following adversarial vectors: Removable media (for replay attack route), Drive-by compromise (for SQL injection attack route), Malicious web component (for XSS, SQL and Buffer overflow attack route), Spear phishing attachment (compromise by spear phished email), and various malwares (compromise using unlimited entry route typical of APT)

Question 2: What is the minimum level of sophistication required to cause an integrity compromise of SCADA MTU data

Answer: Considering the criticality of the specific target component and its importance to the SCADA as a system an attack with the minimum sophistication index of 3 is just sufficient to compromise the integrity of data at the master terminal unit.

7. Conclusion

The security of SCADA systems and related components is as important as ensuring the availability of service to the populace provided by critical infrastructures. In order to underscore the importance and criticality of the security of SCADA systems we have studied in this research the various ways in which a fundamental component of the system—the master terminal unit can be compromised. We have been able to obtain attack characteristics via a systematic review process, and used them to build up attack models depicting the possible attack paths an attacker can take to compromise the system. Thereafter we measured the required sophistication levels. The term sophistication was first used in the events that followed the Stuxnet incident because of the nature of the attack, the methods used and the resultant effect. Following our analysis it is clear that sophistication is an important factor for the success of an attack, and that a more sophisticated attack implies a higher probability of success. Sophistication is seen in the light of the attack methods used, the tools deployed, the skills and high-handedness of the attacker.

Many literatures discussed SCADA related attacks and vulnerabilities but not one of them have analyzed in greater depth the security of the MTU component and the attack paths that can be used to compromise the integrity of this component. This formed the main goal of this research, hence the major contribution. We were able to come up with attack models that focus on integrity attacks on the master terminal unit of a SCADA system. We have also explained the processes involved in each of the model and how the attack can be carried out to aid understanding. We have also been able to draw up analysis determining the relative level of sophistication for the respective attack models, and made comparison. Because of the nature of the target and the security systems in place, in our analysis we were able to establish that an attack that uses multiple exploits and attack features such as stealth, APT and zero-day is sufficient to cause an integrity compromise, thus can be regarded as sophisticated.

The attack tree models we built serves to present a way the attacker thinks and the different routes he can use the compromise a system of this nature. Being knowledgeable about how an attacker thinks, how attack is perpetrated and the security status of these components can go a long way in helping SCADA security analyst make informed decisions on how best to mitigate attacks and the loopholes with which attacker can penetrate the system thus exemplifying the need for a robust security approach, providing cues for strengthening defenses, and ultimately wading off intruders. It is therefore imperative for security analysts and designers of security systems to put all these into considerations as it is better to be on red alert than to be victim of the next cyber assault. In closing we recapitulate the words of Sun Tsu in his book on the Art of War "…if ye know thy enemy and know thyself, ye will not be imperiled in a hundred battles [5]".

References

[1] "EIA Independent Statistics & Analysis," U.S. Energy Information Administration, [Online]. Available: https://www.eia.gov/tools/faqs/faq.php?id=427&t=3. [Accessed 1 April 2019].

[2] K. Brian, "Washington Post," 5 June 2008. [Online]. Available: http://www.washingtonpost.com/wpdyn/content/article/2008/06/05/AR2008060501958.html??noredirect=on. [Accessed 2 December 2018].

[3] J. Williams, et al, "The New York Times," 15 January 2011. [Online]. Available: https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html.. [Accessed 2 December 2018].

[4] G. Sean, "ARS TECHNICA," 27 April 2016. [Online]. Available: https://arstechnica.com/informationtechnology/2016/04/german-nuclear-plants-fuel-rod-system-swarming-with-old-malware/.. [Accessed 2 December 2018].

[5] S. Tzu, "Sun Tzu's Art of War," 15 May 2012. [Online]. Available: https://suntzusaid.com/book/3.. [Accessed 2 December 2018].

[6] GAO, "Critical Infrastructure Protection. Challenges and Efforts to Secure Control Systems," March 2004. [Online]. Available: https://www.gao.gov/new.items/d04354.pdf. U.S. General Accounting Office, Washington D.C.. [Accessed 2 April 2019].

[7] D. Bailey & E. Wright, "Practical SCADA for Industry," Perth, Australia., Newnes (An imprint of Elsevier), 2003, p. 4.

[8] V. Graveto et al, "International Journal of Critical Infrastructure Protection: A stealth monitoring mechanism for cyber-physical systems," 22 October 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1874548218300672. [Accessed 20 March 2019].

[9] M. Cheminod, et. al, "Detection of attacks based on known vulnerabilities in industrial networked systems," *Journal of Information Security and Applications,* vol. 34 Part 2, no. 2 https://doi.org/10.1016/j.jisa.2016.06.003, pp. 153-165, 2016.

[10] A. Gustavo, et. al, "ASTORIA: A framework for attack simulation and evaluation in smart grids," in *NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium*, Istanbul, Turkey., 2016.

[11] E. Irmak and I. Erkek, "An overview of cyber-attack vectors on SCADA systems," in *2018 6th International Symposium on Digital Forensic and Security (ISDFS).*

https://ieeexplore.ieee.org/abstract/document/8355379, Antalya, Turkey, 2018.

[12] P. Kotzanikolaou, et. al, "Evaluating Security and Resilience of Critical networked Infrastructures after Stuxnet," *Critical Information Infrastructure Protection and Resilience in the ICT Sector. IGI Global,* p. 153, 2013.

[13] F. Howarth, "SecurityIntelligence: The Role of Human Error in Successful Security Attacks," IBM, 2 September 2014. [Online]. Available: https://securityintelligence.com/the-role-of-human-error-in-successful-security-attacks/. [Accessed 2 April 2019].

[14] *Vulnerability database,* https://vuldb.com/?id.58301. [Accessed March 28 2019].

[15] *Vulnerability database,* https://vuldb.com/?id.112417. [Accessed April 17 2019].

[16] *Vulnerability Database,* https://vuldb.com/?id.89479. [Accessed April 6 2019].

[17] P. Kamal, et. al, "Identifying and Scoring Vulnerability in SCADA Environments," in *Future Technologies Conference (FTC)*, Vancouver, Canada, 2017.

[18] *Vulnerability database,* https://vuldb.com/?id.59571. [Accessed April 4 2019].

[19] T. Pramod and N. Sunitha, "An approach to detect malicious activities in SCADA systems," 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), 4-6 July 2013. [Online]. Available: https://ieeexplore.ieee.org/document/6726619. [Accessed 18 March 2019].

[20] B. Zhu, et. al, "A Taxonomy of Cyber Attacks on SCADA Systems," in *2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing*, Dalian, China, 2011.

[21] E.D Knapp and R. Samani, "Hacking the Smart Grid," in *Applied Cyber Security and the Smart Grid*, Rockland, MA, United States, Syngress Media. http://dx.doi.org/10.1016/B978-1-59-749998-9.00003-7, 2013, pp. 76-77.

[22] *Vulnerability database,* https://vuldb.com/?id.65174. [Accessed March 23 2019].

[23] A. Nicholson, et. al, "SCADA security in the light of cyber warfare," *Computer and Security,* vol. 31, pp. 418-436, 2012.

[24] I. Fovino, et. al, "An experimental investigation of malware attacks on SCADA systems," *International Journal of Critical Infrastructure Protection,* vol. 2, no. 4, pp. 139-145, 2009.

[25] The MITRE Corporation, "ATT&CK Matrix for Enterprise," MITRE Corporation, 2018. [Online]. Available:

https://attack.mitre.org/. [Accessed 3 April 2019].

[26] M. Mateski, "Cyber Threat Metrics," Sandia National Laboratories, Alberqueque, New Mexico, 2012.

[27] S. Shevchenko, "A Threat That Hit Pentagon," 30 November 2008. [Online]. Available: http://blog.threatexpert.com/2008/11/agentbtz-threat-that-hit-pentagon.html. [Accessed 3 April 2019].

[28] A. Gostev, "The Flame: Questions and Answers," 28 May 2012. [Online]. Available: https://securelist.com/the-flame-questions-and-answers-51/34344/. [Accessed 3 April 2019].

[29] C. Anthe, et. al, "Microsoft Security Intelligence Report," Microsoft_Security_Intelligence_Report_Volume_19_English.pdf, June 2015.

[30] M. Mesa, et. al, "Microsoft Word Intruder Integrates CVE-2017-0199, Utilized by Cobalt Group to Target Financial Institutions," proofpoint, 1 June 2017. [Online]. Available: https://www.proofpoint.com/us/threat-insight/post/microsoft-word-intruder-integrates-cve-2017-0199-utilized-cobalt-group-target. [Accessed 3 April 2019].

[31] US-CERT, "Alert (TA17-293A). Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors," Official Website of the Department of Homeland Security, 20 October 2017. [Online]. Available: https://www.us-cert.gov/ncas/alerts/TA17-293A. [Accessed 3 April 2019].

[32] A. Blaich, et. al, "Dark Caracal: Cyber Espionage at a Global Scale," 18 JAnuary 2018. [Online]. Available: https://info.lookout.com/rs/051-ESQ-475/images/Lookout_Dark-Caracal_srr_20180118_us_v.1.0.pdf. [Accessed 3 April 2019].

[33] P. Paganini, "Elderwood Project: Who is Behind Op. Aurora and Ongoing Attacks?," 9 September 2012. [Online]. Available: http://securityaffairs.co/wordpress/8528/hacking/elderwood-project-who-is-behind-op-aurora-and-ongoing-attacks.html. [Accessed 3 April 2019].

[34] Canadian Centre for Cyber Security, "Cyber Threat and Cyber Threat Actors," Government of Canada, Canada, 2018 https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors.

[35] A. Giandomenico, "Know Your Enemy: Understanding Threat Actors," 27 June 2017. [Online]. Available: https://www.csoonline.com/article/3203804/know-your-enemy-understanding-threat-actors.html. [Accessed 4 April April].

[36] P. Roberts, "New York Times: Stuxnet A Joint US-Israeli Operation," 16 January 2011. [Online]. Available: https://threatpost.com/new-york-times-stuxnet-joint-us-israeli-operation-011611/74851/. [Accessed 5 April 2019].

[37] P. Polityuk, et. al, "Ukraine's power outage was a cyber attack: Ukrenergo," 18 January 2017. [Online].

Available: https://www.reuters.com/article/us-ukraine-cyber-attack-energy-idUSKBN1521BA. [Accessed 4 April 2019].

[38] S. Mishra, K. Kant and R. Yadav, "Multi Tree View of Complex Attack – Stuxnet," in *Advances in Computing and Information Technology*, Chennai, India, Springer-Verlag Berlin Heidelberg, 2012, pp. 171-188.

[39] N. Rodofile, et.al, "Extending the Cyber-Attack Landscape for SCADA-based Critical Infrastructure," *International Journal of Critical Infrastructure Protection,* vol. 25, pp. 14-35, 2019.

[40] Y. Mo and B. Sinopoli, "Secure Control Against Replay Attacks," in *Forty-Seventh Annual Allerton Conference*, Allerton House, UIUC, Illinois, USA, 2009.

[41] G. Wangen, "The Role of Malware in Reported Cyber Espionage: A Review of the Impact and Mechanism," 18 May 2015. [Online]. Available: https://www.mdpi.com/2078-2489/6/2/183/htm. [Accessed 20 March 2019].

[42] M. Cheminod et. al, "Analysis of exploitable vulnerability sequences in industrial networked systems: a proof of concepts," in *ICS-CSR '15 Proceedings of the 3rd International Symposium for ICS & SCADA Cyber Security Research*, Ingolstadt, Germany, 2015.

[43] N. DePaula and S. Goel, "A Sophistication Index for Evaluating," in *11th Annual Symposium on Information Assurance (ASIA '16)*, Albany, NY, United States of America, 2016.

[44] S. Sridhar and G. Manimaran, "Data integrity attacks and their impacts on SCADA control system," in *IEEE PES General Meeting*, Providence, RI, USA, 2010.

[45] T. Ingoldsby, "Attack Tree-based Threat Risk Analysis," Amenaza Technologies Limited, Calgary, Alberta, Canada, 2013.

[46] B. Kitchenham and S. Charters, "Guidelines for performing Systematic Literature reviews in Software Engineering," EBSE Technical Report EBSE-2007-01, Keele University and Durham University, Durham, United Kingdom, July 2007.

[47] M.Petticrew and H. Roberts, "Systematic Review in the Social Sciences: A practical Guide," Blackwell Publishing, 2005 ISBN 1405121106.

[48] A. Kable, J.pich and S.E Maslin-Prothero, "A structured approach to documenting a search strategy for publication," Australia, February 2012.

[49] Amenaza Technologies Limited, "SecurITree Attack Tree Modelling," Amenaza Technologies Limited, [Online]. Available: https://www.amenaza.com/SS-analysis.php. [Accessed 8 April 2019].

[50] J. Rodriguez, "Most common attack vector over Critical Infrastructures," 26 January 2019. [Online]. Available: https://www.cipsec.eu/content/most-common-attack-vector-over-critical-infrastructures. [Accessed 20 March 2019].

[51] H. Suleiman et al, "Integrated smart grid systems security threat model," October-November 2015. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0306437914001896. [Accessed 19 March 2019].

[52] T. Pramod and N. Sunitha, "An approach to detect malicious activities in SCADA systems," in *2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT)*, Tiruchengode, India, 2013.

[53] T. Bartman and K. Carson, "Securing communications for SCADA and critical industrial systems," in *2016 69th Annual Conference for Protective Relay Engineers (CPRE)*, College Station, TX, USA, 2016.

[54] *Vulnerability database,* https://vuldb.com/?id.73134. [Accessed March 25 2019].

[55] Acunetix, "What is SQL Injection (SQLi) and How to Prevent It," Acunetix, 2019. [Online]. Available: https://www.acunetix.com/websitesecurity/sql-injection/. [Accessed 15 April 2019].

[56] A. Prodromou, "Exploiting SQL Injection: a Hands-on Example," Acunetix, 26 February 2019. [Online]. Available: https://www.acunetix.com/blog/articles/exploiting-sql-injection-example/. [Accessed 15 April 2019].

[57] W. Du, "Firewall Evasion Lab: Bypassing Firewalls using VPN," Syracuse University, 2018. [Online]. Available:http://www.cis.syr.edu/~wedu/seed/Labs_16.04/Networking/Firewall_VPN/Firewall_VPN.pdf. [Accessed 15 April 2019].

[58] *vulnerability database,* https://vuldb.com/?id.130569. [Accessed April 1 2019].

[59] Acunetix, "Cross-site Scripting (XSS)," Acunetix, 2019. [Online]. Available: https://www.acunetix.com/websitesecurity/cross-site-scripting/. [Accessed 15 April 2019].

[60] *Vulnerability database,* https://vuldb.com/?id.110185. [Accessed March 13 2019]

[61] *Symantec Corporation. Security Focus: Control Microsystems ClearSCADA Multiple Remote Vulnerabilities. 2010,* https://www.securityfocus.com/bid/46312/discuss Accessed March 2019.

[62] *vulnerability database,* https://vuldb.com/?id.105994. [Accessed March 15 2019].

[63] *OWASP: Buffer Overflows,* https://www.owasp.org/index.php/Buffer_Overflows. [Accessed 10th April 2019].

[64] B. Kerestan, "How to Detect, Prevent, and Mitigate Buffer Overflow Attacks," DZone, 12 July 2017. [Online]. Available: https://dzone.com/articles/how-to-detect-prevent-and-mitigate-buffer-overflow. [Accessed 15 April 2019].

[65] R. Grill, "Testing Web Applications for Malicious Input Attack Vulnerabilities," SANS, 2002. [Online]. Available: https://pen-testing.sans.org/resources/papers/gcih/testing-web-applications-malicious-input-attack-vulnerabilities-100140. [Accessed 15 April 2019].

[66] Syracuse University, "Buffer-Overflow Vulnerabilities and Attacks," [Online]. Available: http://www.cis.syr.edu/~wedu/Teaching/IntrCompSec/LectureNotes_New/Buffer_Overflow.pdf. [Accessed 15 April 2019].

[67] *Vulnerability database,* https://vuldb.com/?id.63381. [Accessed March 21 2019]

[68] IBM Knowledge Centre, "Buffer Overflow Attacks," IBM, [Online]. Available: https://www.ibm.com/support/knowledgecenter/en/SSB2MG_4.6.0/com.ibm.ips.doc/concepts/wap_buffer_overflow.htm. [Accessed 10 April 2019].

[69] R.M. Lee, M.J Assante and T. Conway, " E-ISAC Electricity Information Sharing and Analysis centre. TLP: White Analysis of the Cyber Attack on the Ukrainian Power grid. Defense Use case," SANS ICS, Washington, 2016.

[70] FireEye, "Advanced Targeted Attacks: How to Protect Against the Next Generation of Cyber Attacks," FireEye, 2012. [Online]. Available: https://www.softbox.co.uk/pub/fireeye-advanced-targeted-attacks.pdf. [Accessed 15 April 2019].

[71] *Trend Micro. Command and Control [C&C] Server,* Accessed March 20 2019. https://www.trendmicro.com/vinfo/us/security/definition/command-and-control-server.

[72] *vulnerability database,* https://vuldb.com/?id.37252. [Accessed March 18 2019].

[73] NJCCIC, "Havex," 10 August 2017. [Online]. Available: https://www.cyber.nj.gov/threat-profiles/ics-malware-variants/havex. [Accessed 20 March 2019].

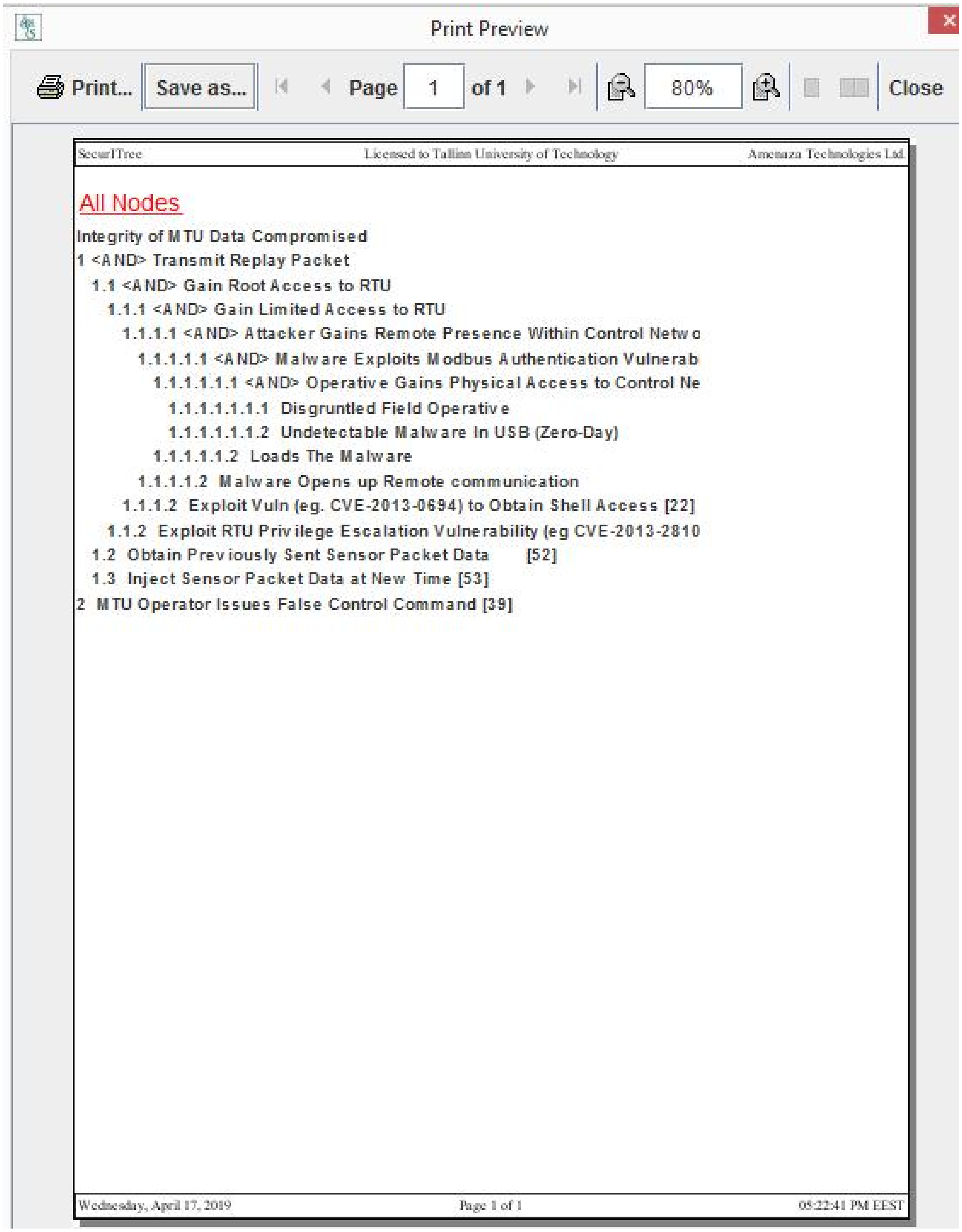
[74] B. Bencsath et al, "Duqu: Analysis, detection, and lessons learned. In Proceedings of the ACM European Workshop on System Security (EuroSec)," Bern Switzerland, April 2012.

[75] *Skybox Security. Multiple Invensys Products Local Privilege Escalation Vulnerability via a Trojan Horse DLL,* https://www.vulnerabilitycenter.com/#!vul=35968. [Accessed March 20 2019].

[76] Crash Reboot, "Iran and STUXnet, Iran is HACKED," 19 February 2017. [Online]. Available: https://youtu.be/TGGxqjpka-U. [Accessed 15 April 2019].

Appendix

Appendix A: Secur*IT*ree Nodes

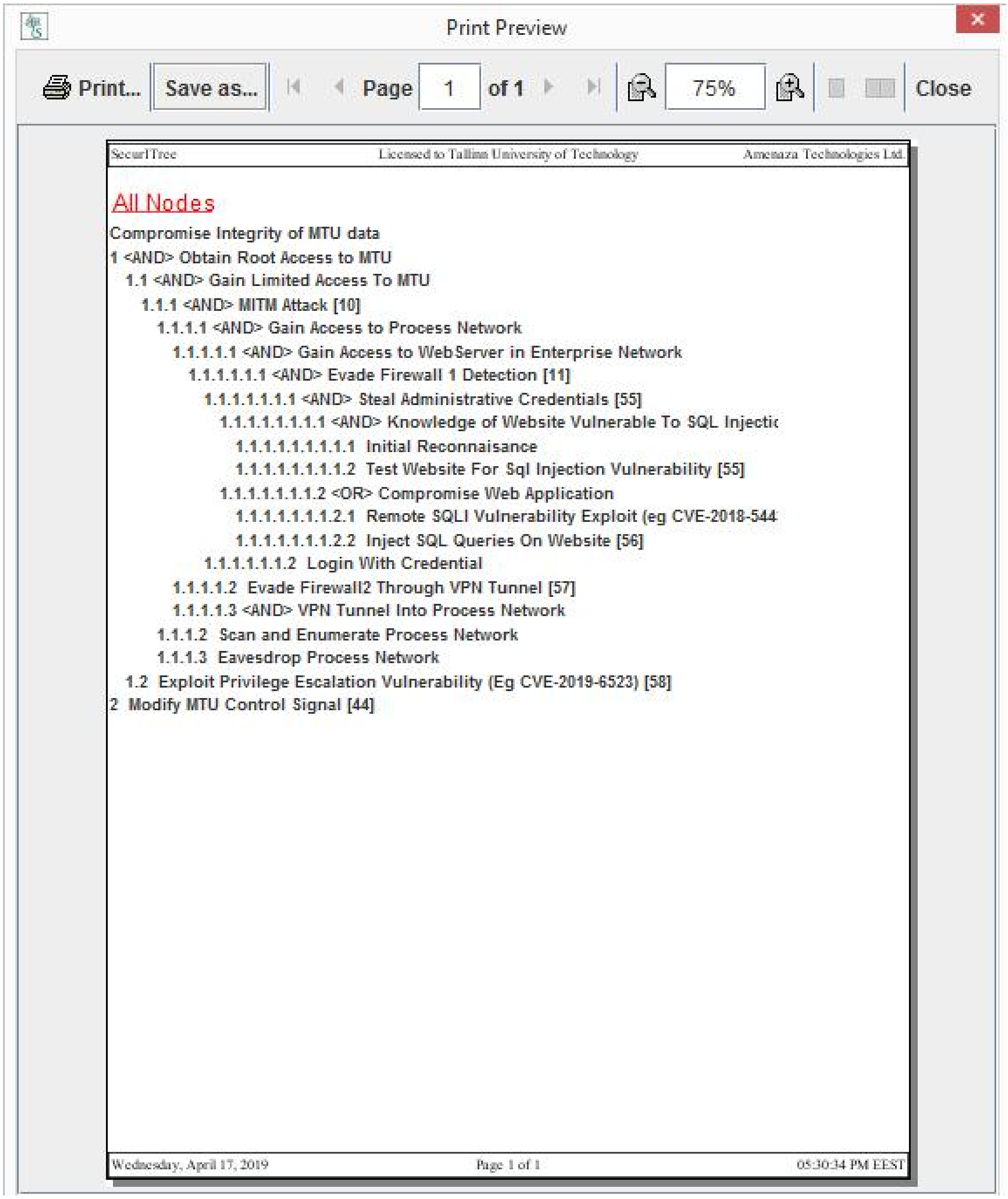


SecurITree   Licensed to Tallinn University of Technology   Amenaza Technologies Ltd.

All Nodes

```
Integrity of MTU Data Compromised
1 <AND> Transmit Replay Packet
  1.1 <AND> Gain Root Access to RTU
    1.1.1 <AND> Gain Limited Access to RTU
      1.1.1.1 <AND> Attacker Gains Remote Presence Within Control Netwo
        1.1.1.1.1 <AND> Malware Exploits Modbus Authentication Vulnerab
          1.1.1.1.1.1 <AND> Operative Gains Physical Access to Control Ne
            1.1.1.1.1.1.1  Disgruntled Field Operative
            1.1.1.1.1.1.2  Undetectable Malware In USB (Zero-Day)
          1.1.1.1.1.2  Loads The Malware
        1.1.1.1.2  Malware Opens up Remote communication
      1.1.1.2  Exploit Vuln (eg. CVE-2013-0694) to Obtain Shell Access [22]
    1.1.2  Exploit RTU Privilege Escalation Vulnerability (eg CVE-2013-2810
  1.2  Obtain Previously Sent Sensor Packet Data      [52]
  1.3  Inject Sensor Packet Data at New Time [53]
2  MTU Operator Issues False Control Command [39]
```

Wednesday, April 17, 2019   Page 1 of 1   05:22:41 PM EEST

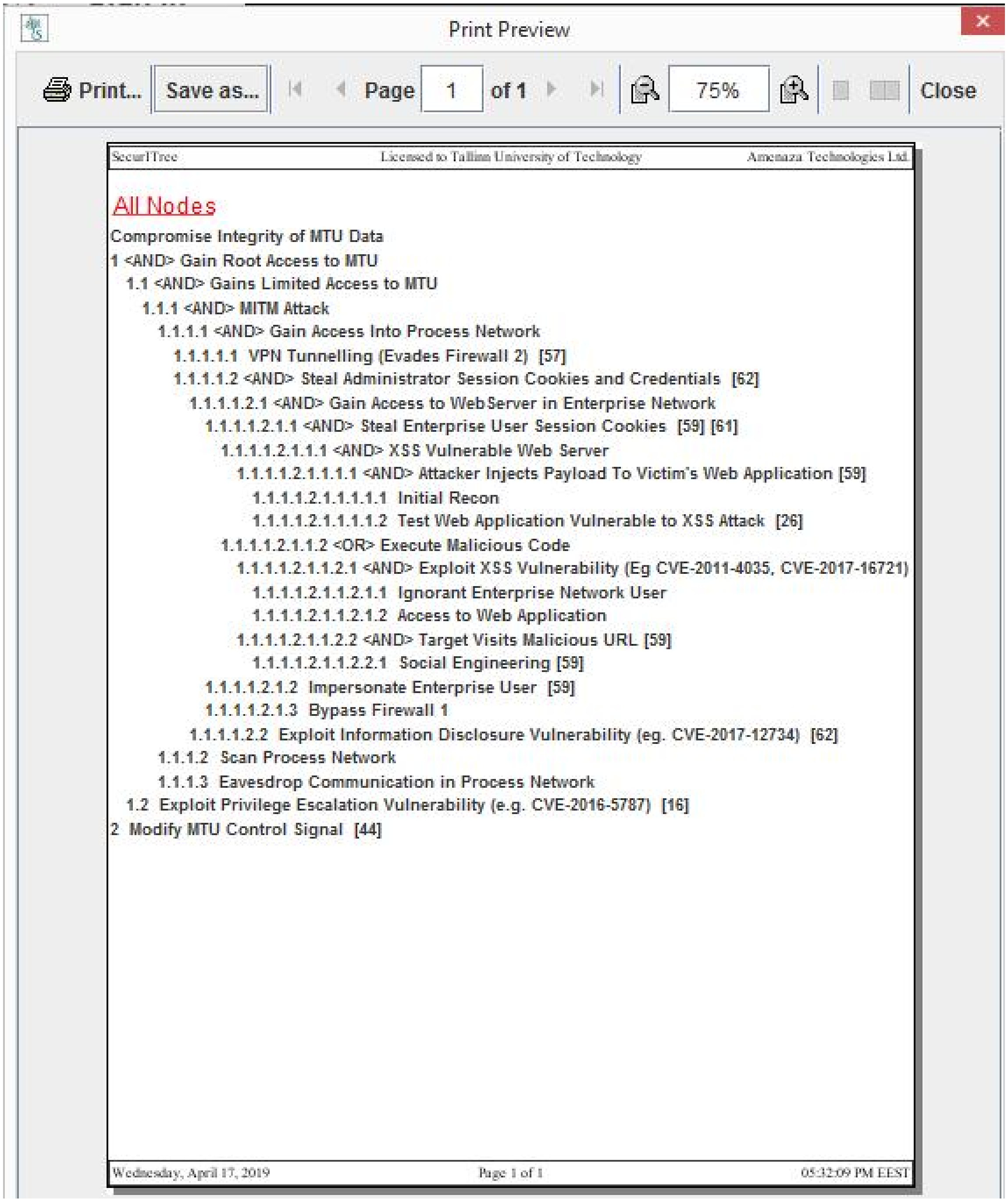


SecurITree Licensed to Tallinn University of Technology Amenaza Technologies Ltd.

All Nodes

```
Compromise Integrity of MTU data
1 <AND> Obtain Root Access to MTU
  1.1 <AND> Gain Limited Access To MTU
    1.1.1 <AND> MITM Attack [10]
      1.1.1.1 <AND> Gain Access to Process Network
        1.1.1.1.1 <AND> Gain Access to WebServer in Enterprise Network
          1.1.1.1.1.1 <AND> Evade Firewall 1 Detection [11]
            1.1.1.1.1.1.1 <AND> Steal Administrative Credentials [55]
              1.1.1.1.1.1.1.1 <AND> Knowledge of Website Vulnerable To SQL Injectic
                1.1.1.1.1.1.1.1.1  Initial Reconnaisance
                1.1.1.1.1.1.1.1.2  Test Website For Sql Injection Vulnerability [55]
              1.1.1.1.1.1.1.2 <OR> Compromise Web Application
                1.1.1.1.1.1.1.2.1  Remote SQLI Vulnerability Exploit (eg CVE-2018-544
                1.1.1.1.1.1.1.2.2  Inject SQL Queries On Website [56]
            1.1.1.1.1.1.2  Login With Credential
        1.1.1.1.2  Evade Firewall2 Through VPN Tunnel [57]
        1.1.1.1.3 <AND> VPN Tunnel Into Process Network
      1.1.1.2  Scan and Enumerate Process Network
      1.1.1.3  Eavesdrop Process Network
  1.2  Exploit Privilege Escalation Vulnerability (Eg CVE-2019-6523) [58]
2  Modify MTU Control Signal [44]
```

Wednesday, April 17, 2019 Page 1 of 1 05:30:34 PM EEST

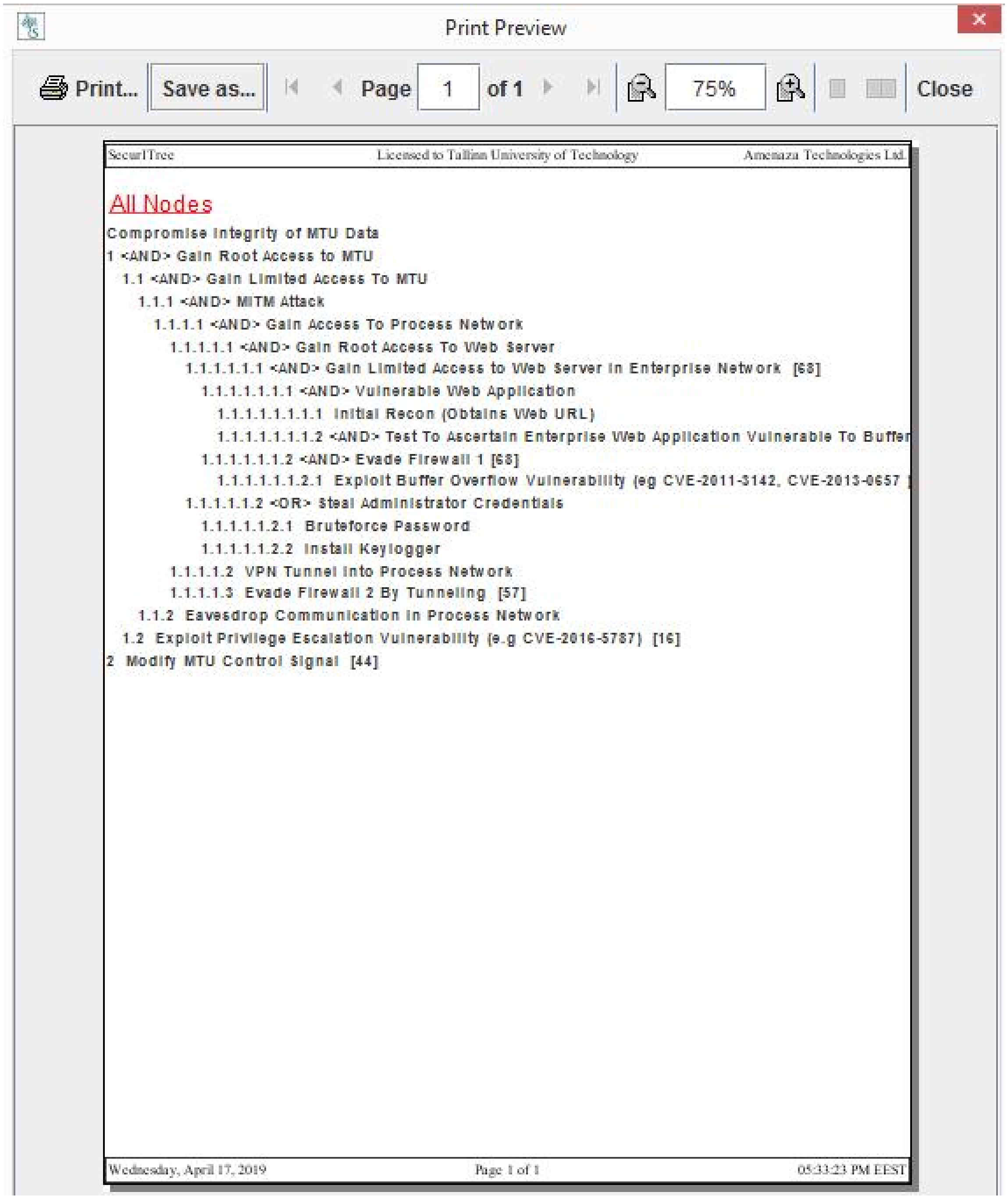


SecurITree Licensed to Tallinn University of Technology Amenaza Technologies Ltd.

All Nodes

```
Compromise Integrity of MTU Data
1 <AND> Gain Root Access to MTU
  1.1 <AND> Gains Limited Access to MTU
    1.1.1 <AND> MITM Attack
      1.1.1.1 <AND> Gain Access Into Process Network
        1.1.1.1.1  VPN Tunnelling (Evades Firewall 2)  [57]
        1.1.1.1.2 <AND> Steal Administrator Session Cookies and Credentials  [62]
          1.1.1.1.2.1 <AND> Gain Access to WebServer in Enterprise Network
            1.1.1.1.2.1.1 <AND> Steal Enterprise User Session Cookies  [59] [61]
              1.1.1.1.2.1.1.1 <AND> XSS Vulnerable Web Server
                1.1.1.1.2.1.1.1.1 <AND> Attacker Injects Payload To Victim's Web Application [59]
                  1.1.1.1.2.1.1.1.1.1  Initial Recon
                  1.1.1.1.2.1.1.1.1.2  Test Web Application Vulnerable to XSS Attack  [26]
              1.1.1.1.2.1.1.2 <OR> Execute Malicious Code
                1.1.1.1.2.1.1.2.1 <AND> Exploit XSS Vulnerability (Eg CVE-2011-4035, CVE-2017-16721)
                  1.1.1.1.2.1.1.2.1.1  Ignorant Enterprise Network User
                  1.1.1.1.2.1.1.2.1.2  Access to Web Application
                1.1.1.1.2.1.1.2.2 <AND> Target Visits Malicious URL [59]
                  1.1.1.1.2.1.1.2.2.1  Social Engineering [59]
            1.1.1.1.2.1.2  Impersonate Enterprise User  [59]
            1.1.1.1.2.1.3  Bypass Firewall 1
          1.1.1.1.2.2  Exploit Information Disclosure Vulnerability (eg. CVE-2017-12734)  [62]
      1.1.1.2  Scan Process Network
      1.1.1.3  Eavesdrop Communication in Process Network
  1.2  Exploit Privilege Escalation Vulnerability (e.g. CVE-2016-5787)  [16]
2  Modify MTU Control Signal  [44]
```

Wednesday, April 17, 2019 Page 1 of 1 05:32:09 PM EEST

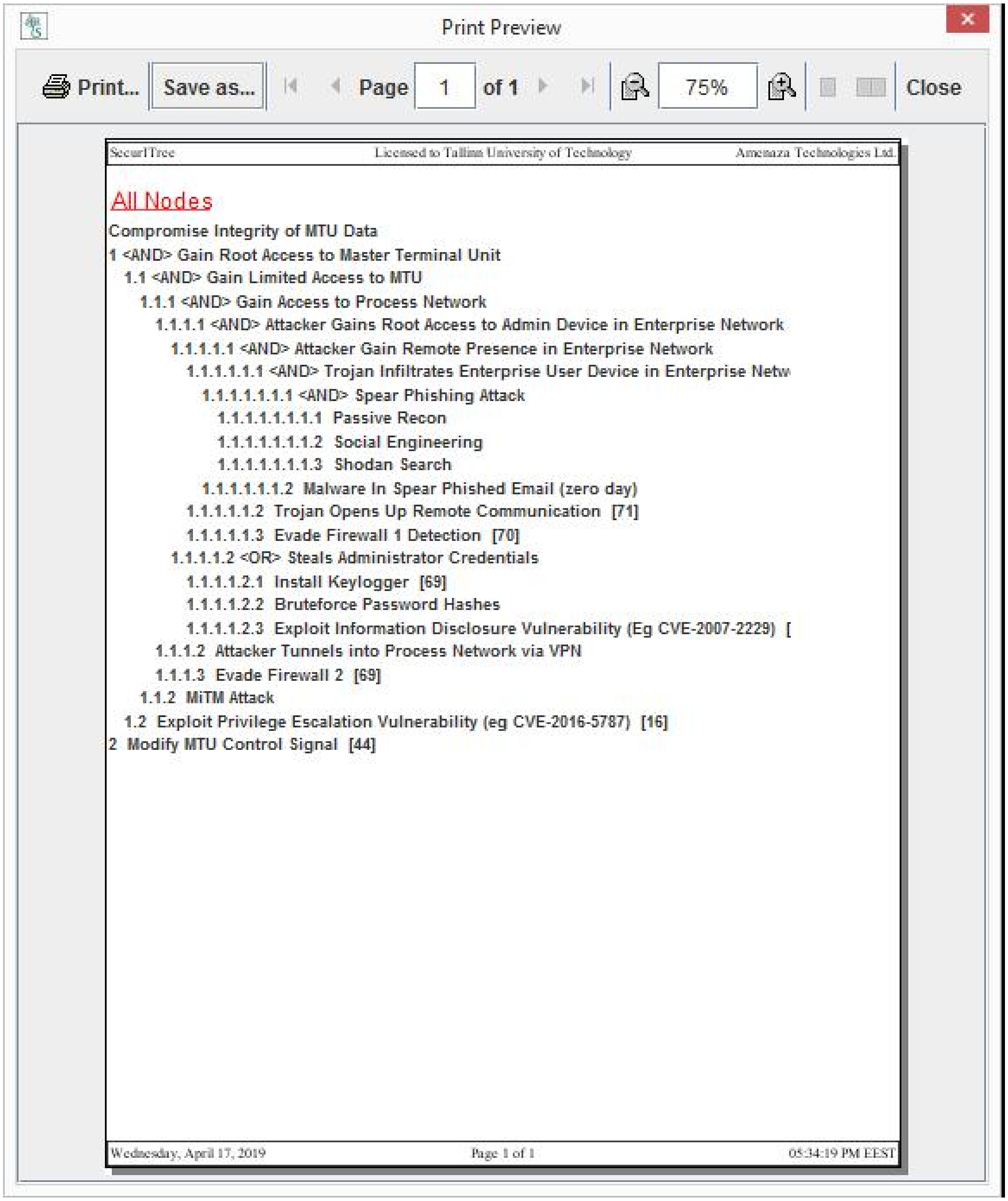


SecurITree Licensed to Tallinn University of Technology Amenaza Technologies Ltd.

All Nodes

```
Compromise Integrity of MTU Data
1 <AND> Gain Root Access to MTU
  1.1 <AND> Gain Limited Access To MTU
    1.1.1 <AND> MITM Attack
      1.1.1.1 <AND> Gain Access To Process Network
        1.1.1.1.1 <AND> Gain Root Access To Web Server
          1.1.1.1.1.1 <AND> Gain Limited Access to Web Server in Enterprise Network  [68]
            1.1.1.1.1.1.1 <AND> Vulnerable Web Application
              1.1.1.1.1.1.1.1  Initial Recon (Obtains Web URL)
              1.1.1.1.1.1.1.2 <AND> Test To Ascertain Enterprise Web Application Vulnerable To Buffer
            1.1.1.1.1.1.2 <AND> Evade Firewall 1 [68]
              1.1.1.1.1.1.2.1  Exploit Buffer Overflow Vulnerability (eg CVE-2011-3142, CVE-2013-0657
          1.1.1.1.1.2 <OR> Steal Administrator Credentials
            1.1.1.1.1.2.1  Bruteforce Password
            1.1.1.1.1.2.2  Install Keylogger
        1.1.1.1.2  VPN Tunnel Into Process Network
        1.1.1.1.3  Evade Firewall 2 By Tunneling  [57]
    1.1.2  Eavesdrop Communication in Process Network
  1.2  Exploit Privilege Escalation Vulnerability (e.g CVE-2016-5787)  [16]
2  Modify MTU Control Signal  [44]
```

Wednesday, April 17, 2019 Page 1 of 1 05:33:23 PM EEST

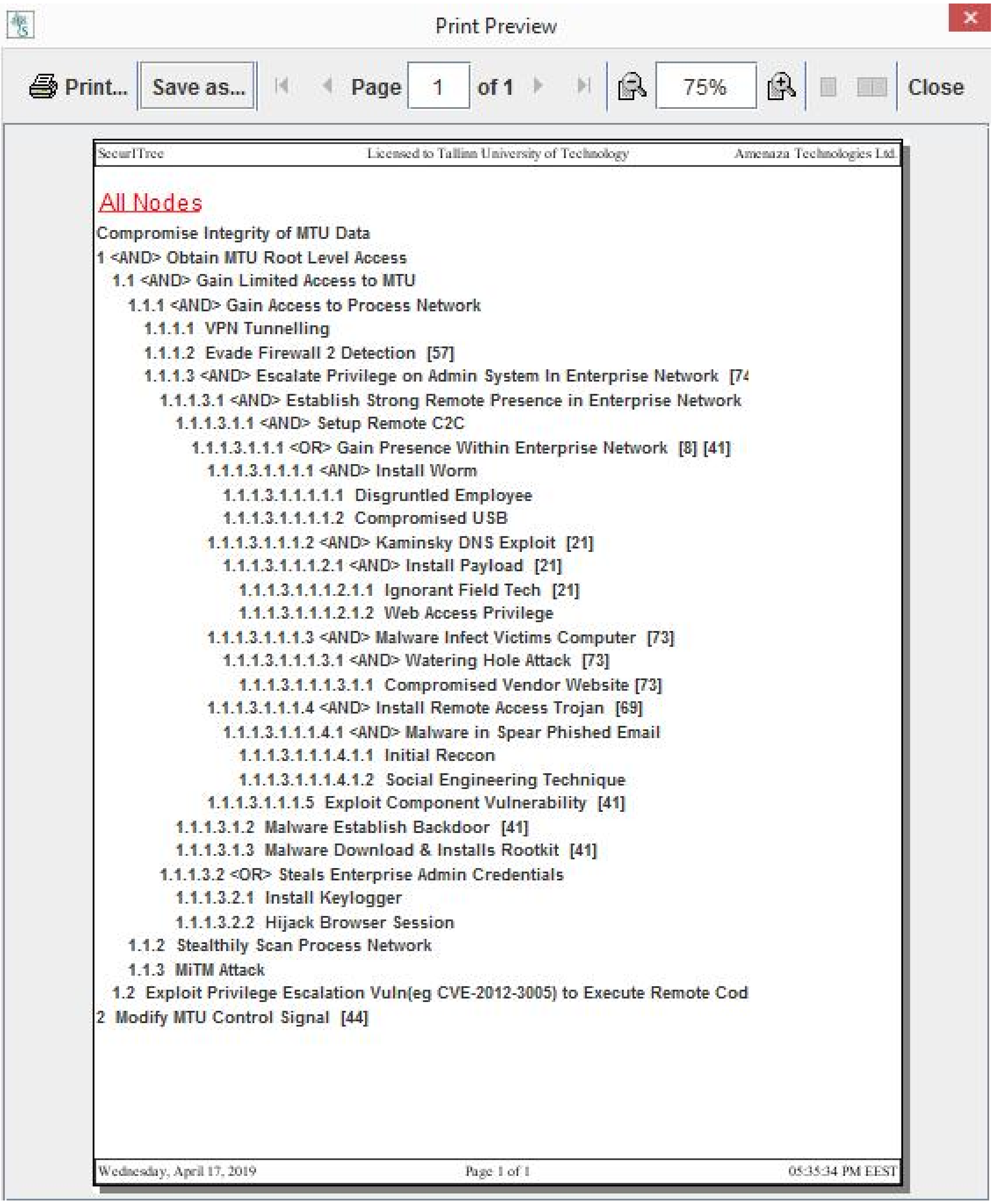


SecurITree   Licensed to Tallinn University of Technology   Amenaza Technologies Ltd.

All Nodes

```
Compromise Integrity of MTU Data
1 <AND> Gain Root Access to Master Terminal Unit
  1.1 <AND> Gain Limited Access to MTU
    1.1.1 <AND> Gain Access to Process Network
      1.1.1.1 <AND> Attacker Gains Root Access to Admin Device in Enterprise Network
        1.1.1.1.1 <AND> Attacker Gain Remote Presence in Enterprise Network
          1.1.1.1.1.1 <AND> Trojan Infiltrates Enterprise User Device in Enterprise Netw
            1.1.1.1.1.1.1 <AND> Spear Phishing Attack
              1.1.1.1.1.1.1.1  Passive Recon
              1.1.1.1.1.1.1.2  Social Engineering
              1.1.1.1.1.1.1.3  Shodan Search
            1.1.1.1.1.1.2  Malware In Spear Phished Email (zero day)
          1.1.1.1.1.2  Trojan Opens Up Remote Communication  [71]
          1.1.1.1.1.3  Evade Firewall 1 Detection  [70]
        1.1.1.1.2 <OR> Steals Administrator Credentials
          1.1.1.1.2.1  Install Keylogger  [69]
          1.1.1.1.2.2  Bruteforce Password Hashes
          1.1.1.1.2.3  Exploit Information Disclosure Vulnerability (Eg CVE-2007-2229)  [
      1.1.1.2  Attacker Tunnels into Process Network via VPN
      1.1.1.3  Evade Firewall 2  [69]
    1.1.2  MiTM Attack
  1.2  Exploit Privilege Escalation Vulnerability (eg CVE-2016-5787)  [16]
2  Modify MTU Control Signal  [44]
```

Wednesday, April 17, 2019   Page 1 of 1   05:34:19 PM EEST



SecurITree Licensed to Tallinn University of Technology Amenaza Technologies Ltd.

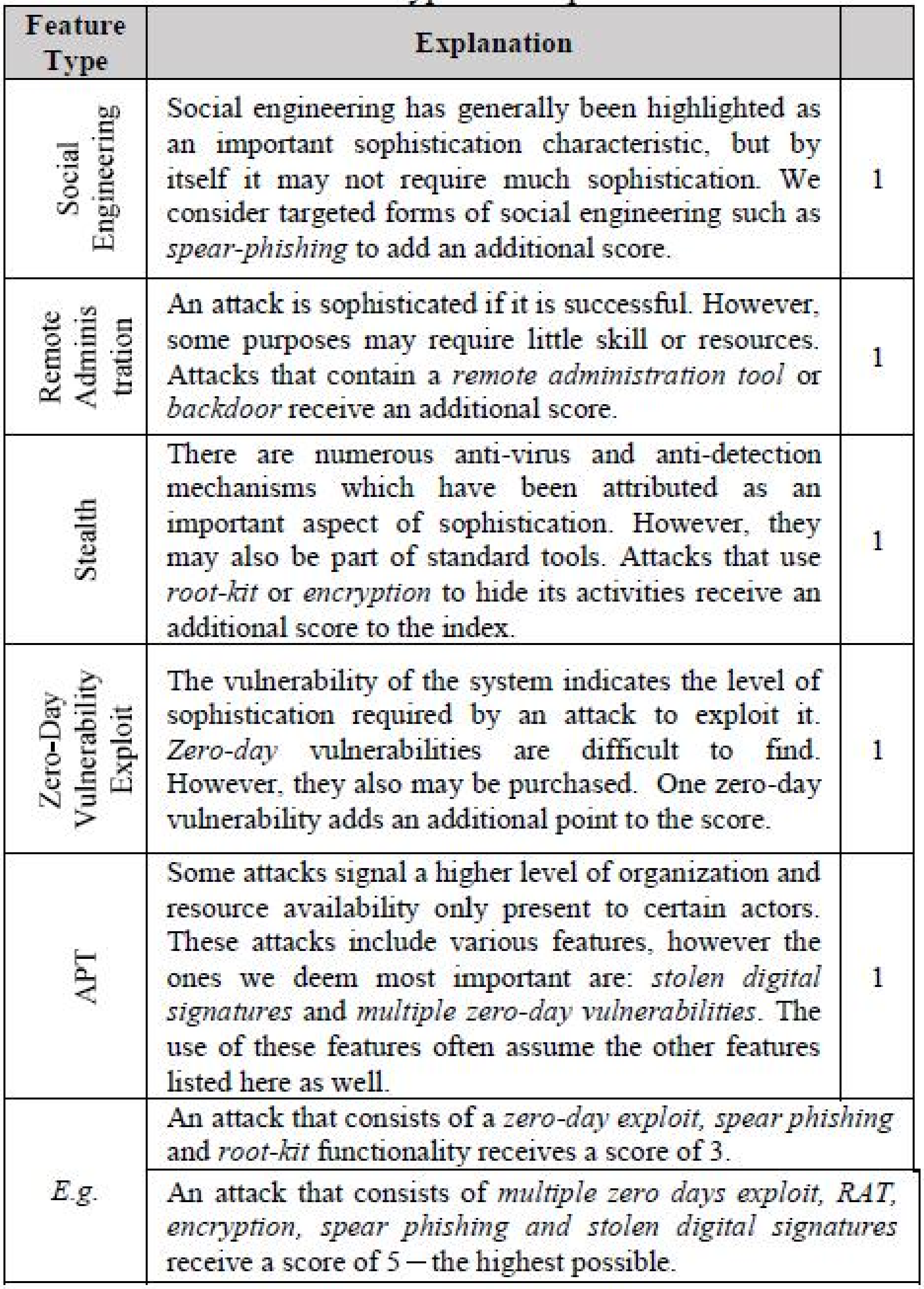
All Nodes

```
Compromise Integrity of MTU Data
1 <AND> Obtain MTU Root Level Access
  1.1 <AND> Gain Limited Access to MTU
    1.1.1 <AND> Gain Access to Process Network
      1.1.1.1  VPN Tunnelling
      1.1.1.2  Evade Firewall 2 Detection  [57]
      1.1.1.3 <AND> Escalate Privilege on Admin System In Enterprise Network  [74
        1.1.1.3.1 <AND> Establish Strong Remote Presence in Enterprise Network
          1.1.1.3.1.1 <AND> Setup Remote C2C
            1.1.1.3.1.1.1 <OR> Gain Presence Within Enterprise Network  [8] [41]
              1.1.1.3.1.1.1.1 <AND> Install Worm
                1.1.1.3.1.1.1.1.1  Disgruntled Employee
                1.1.1.3.1.1.1.1.2  Compromised USB
              1.1.1.3.1.1.1.2 <AND> Kaminsky DNS Exploit  [21]
                1.1.1.3.1.1.1.2.1 <AND> Install Payload  [21]
                  1.1.1.3.1.1.1.2.1.1  Ignorant Field Tech  [21]
                  1.1.1.3.1.1.1.2.1.2  Web Access Privilege
              1.1.1.3.1.1.1.3 <AND> Malware Infect Victims Computer  [73]
                1.1.1.3.1.1.1.3.1 <AND> Watering Hole Attack  [73]
                  1.1.1.3.1.1.1.3.1.1  Compromised Vendor Website [73]
              1.1.1.3.1.1.1.4 <AND> Install Remote Access Trojan  [69]
                1.1.1.3.1.1.1.4.1 <AND> Malware in Spear Phished Email
                  1.1.1.3.1.1.1.4.1.1  Initial Reccon
                  1.1.1.3.1.1.1.4.1.2  Social Engineering Technique
              1.1.1.3.1.1.1.5  Exploit Component Vulnerability  [41]
          1.1.1.3.1.2  Malware Establish Backdoor  [41]
          1.1.1.3.1.3  Malware Download & Installs Rootkit  [41]
        1.1.1.3.2 <OR> Steals Enterprise Admin Credentials
          1.1.1.3.2.1  Install Keylogger
          1.1.1.3.2.2  Hijack Browser Session
    1.1.2  Stealthily Scan Process Network
    1.1.3  MiTM Attack
  1.2  Exploit Privilege Escalation Vuln(eg CVE-2012-3005) to Execute Remote Cod
2  Modify MTU Control Signal  [44]
```

Wednesday, April 17, 2019 Page 1 of 1 05:35:34 PM EEST

Appendix B: Attack features definition and sophistication index score

TABLE I. Features Types of Sophistication Index



Feature Type	Explanation	
Social Engineering	Social engineering has generally been highlighted as an important sophistication characteristic, but by itself it may not require much sophistication. We consider targeted forms of social engineering such as *spear-phishing* to add an additional score.	1
Remote Adminis tration	An attack is sophisticated if it is successful. However, some purposes may require little skill or resources. Attacks that contain a *remote administration tool* or *backdoor* receive an additional score.	1
Stealth	There are numerous anti-virus and anti-detection mechanisms which have been attributed as an important aspect of sophistication. However, they may also be part of standard tools. Attacks that use *root-kit* or *encryption* to hide its activities receive an additional score to the index.	1
Zero-Day Vulnerability Exploit	The vulnerability of the system indicates the level of sophistication required by an attack to exploit it. *Zero-day* vulnerabilities are difficult to find. However, they also may be purchased. One zero-day vulnerability adds an additional point to the score.	1
APT	Some attacks signal a higher level of organization and resource availability only present to certain actors. These attacks include various features, however the ones we deem most important are: *stolen digital signatures* and *multiple zero-day vulnerabilities*. The use of these features often assume the other features listed here as well.	1
E.g.	An attack that consists of a *zero-day exploit, spear phishing* and *root-kit* functionality receives a score of 3.	
	An attack that consists of *multiple zero days exploit, RAT, encryption, spear phishing and stolen digital signatures* receive a score of 5 – the highest possible.	