International Journal of Engineering & Technology, 7 (2.14) (2018) 145-152

SPC

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper

A review: towards practical attack taxonomy for industrial control systems

Qais Saif Qassim [1]*, Norziana Jamil1 [2], Razali Jidin [1], Mohd Ezanee Rusli1 [2], Md Nabil Ahmad Zawawi1[,2], Md Zaini Jamaludin [1], Muhammad Reza Z'aba [3], Wan Azlan Wan Kamarulzaman [4]

[1] Institute of Informatics and Computing in Energy, Universiti Tenaga Nasional, Selangor, Malaysia
[2] College of Computer Science and Information Technology, Universiti Tenaga Nasional, Selangor, Malaysia
[3] Faculty of Computer Science and Information Technology, University of Malaya, Kuala Lumpur, Malaysia
[4] Tenaga Nasional Berhad, Malaysia
**Corresponding author E-mail: qaissaif@uniten.edu.my*

Abstract

Supervisory Control and Data Acquisition (SCADA) system is the underlying control system of most national critical infrastructures such as power, energy, water, transportation and telecommunication. In order to understand the potential threats to these infrastructures and the mechanisms to protect them, different types of cyber-attacks applicable to these infrastructures need to be identified. Therefore, there is a significant need to have a comprehensive understanding of various types of cyber-attacks and its classification associated with both Opera-tion Technology (OT) and Information Technology (IT). This paper presents a comprehensive review of existing cyber-attack taxonomies available in the literature and evaluates these taxonomies based on defined criteria.

Keywords: *SCADA; Cyber-Attack; Taxonomy.*

1. Introduction

Cyber-attacks have greatly increased over the years, where the attackers have progressively improved in devising attacks toward a specific target. With cyber threats on the rise, it is necessary to correctly identify the suspected threat in a timely manner [1]. In today's world, there is an increasing overlap between the cyber-based technologies and the physical systems. For example, modern critical infrastructures such as power plants and water supply systems heavily rely on information and communications technologies, to reduce costs as well as to increase efficiency, flexibility and interoperability [1-2]. As a result, these technologies are exposed to significant cyber threats. One of the heightened risks with cyber-attacks against critical infrastructure is the physical component to these attacks. An attack in this area is not limited to information or processes [4]. The physical components of these systems suggest that any impact on the information also has a possibility of causing an impact within the physical world. The recent Stuxnet worm is the first malware that was specifically designed to attack networked industrial control systems [5]. Stuxnet's ability to reprogram the logic of control hardware and alter physical processes demonstrates the danger of modern cyber threats.

Although existing research works with regard to taxonomies of SCADA/ICS attacks is limited, analyzing attacks against computer and network systems will enlighten the classification of SCADA/ICS attacks due to the overlapping infrastructure. Therefore, in this work, we surveyed attack taxonomies in the areas of computer, network and SCADA systems to identify SCADA/ICS possible attacks and present a better understanding on their influence on the cyberphysical systems. This paper is organized as follow. Section 2 presents the cyber-attack taxonomies, which have been considered in this work for evaluation. Section 3 presents the analysis of the examined taxonomies. We present a new cyber-attack taxonomy in section 4, while section 5 concludes the results obtained from this work.

2. Cyber-attacks taxonomies

Attack taxonomy is a framework for describing the characteristics of attacks and the classifiers chosen are fundamental to achieve a systematic attack classification. There have been many attempts to define cyber-attack taxonomy for classifying cyber-attacks or incidents. In this section, we provide a brief survey of existing taxonomies that assist with identifying attacks. In [6] presented the first attempt at unified security taxonomy. It was considered as one of the most comprehensive studies of computer security incidents. In this work, a detailed analysis of data collected by CERT/CC consisting of over 4,500 security incidents between 1989 and 1995 was executed. Based on this data, the authors proposed a network and attack taxonomy for classifying and comparing such incidents. This taxonomy contained five primary components:

- Tools of attack: Defined as the means of exploiting a computer or network vulnerability. Attack tools include physical attack, information exchange, user command, script, toolkit, data trap.
- System vulnerability: Vulnerability is a weakness in a system allowing unauthorized action, weakness in design, implementation or configuration.
- Action represents a spectrum of activities that can take place on computers and networks. More specifically, an action is a step taken by a user or a process in order to achieve a result. Actions can be as probe, scan, flood, authenticate, bypass, spoof, read, copy, steal, modify and delete.

- Target is a computer or network logical entity (account, process or data) or physical entity (computer and network devices).
- Unauthorized result which is defined as unauthorized consequence of an event such as increased access, disclosure of information, corruption of information, denial of service and theft resources.

In [7] proposed an attack-centric taxonomy called VERDICT (Validation, Exposure Randomness, De-allocation and Improper Conditions Taxonomy). In this taxonomy, Lough focuses on four major causes of security errors: improper validation, improper exposure, improper randomness and improper de-allocation which are defined as follow:

- Improper validation: Insufficient or incorrect validation results in unauthorized access to information or systems.
- Improper exposure: A system or information is improperly exposed to attack.
- Improper randomness: Insufficient randomness results in exposure to attack.
- Improper de-allocation: Information is not properly deleted after use and thus can be vulnerable to attack.

In [8] have provided what was considered as most thorough taxonomy of network and computer attacks. Their work extended earlier proposed taxonomies by introducing multiple tiers of threats, with a greater exposition of levels and description within each category. Specifically, they classified attacks on four main dimensions:

- Attack vectors (the main means by which the virus reaches the target).
- Target(s) of the attack (hardware/software/etc.).
- Specific vulnerabilities and exploits that the attack uses (security flaws).
- Payload of the attack (outcome and effects, possibly beyond the attack itself).

These dimensions were decomposed based on the specificity of detail. Target categories consisted of six levels, ranging from generic descriptors (level 1: Hardware versus software) to very precise (level 6: Specific versions of specific programs). Altogether, this gave a very thorough picture of the attack space and available methods. They demonstrated how 15 well-known attacks could be classified on the dimensions of this taxonomy, from generic to specific levels of detail in each instance. The work of [9] was notable for adding a quantitative component to the classification of network attacks. In [9] sought not only to classify the attacks, but also to determine which factors were most likely to co-occur in an attack. Attack analysis was based on a sample of 2,755 reported incidents to CERT/CC. The author have classified the incidents based on four categories:

- Source sectors (com, gov, edu, intl, user, unknown).
- Method of operation (misuse of resources, user/root compromise, social engineering, virus, web compromise, Trojan, worm, denial of service).
- Impact (disrupt, distort, destruct, disclosure, unknown)
- Target services.

In [10] advocated for the development of an attack taxonomy that would provide a comprehensive understanding of cyber-attacks against ICS in the energy critical infrastructure sector. They identified four questions that a taxonomy should address. These questions include analysis of the:

- Different manner in which attacks against control systems can be perpetuated.
- Type of damage that can be caused.
- Challenges involved in defeating the attacks.
- Requirements for development of adequate defence mechanisms.

As the first step towards the development of an attack taxonomy, an Attack-Vulnerability-Damage (AVD) Model was created. The AVD Model consists of three components: attack, vulnerability and damage. The study defined the cyber-attack as an action originating either within or outside the target. The attack is directed against an exploitable weakness (vulnerability). Finally, the attack causes damage represented by descriptions of both state change and performance degradation and quantified by the level of impact on the target. In [11] proposed a cyber-attack taxonomy primarily inspired by the work of [8], which provides nine classes of cyber-attacks. Viruses, worms, Trojans, buffer overflow, denial of service, network attacks, physical attacks, password attacks and information gathering. In [12] have proposed a cyber-attack taxonomy focuses on attacks carried out on the Distributed Network Protocol (DNP3), which define how SCADA devices communicate control commands and data. The study proposed to classified attacks based on targets and threat categories. Target category may include control center, outstation devices and network/communication paths. On the other hand, threat categories may include interception, interruption, modification and fabrication. The study had identified 28 possible attacks on DNP3 protocol associated with each of the three principle DNP3 protocol layers: data link layer, pseudo-transport layer and application layer.

A broadly inclusive taxonomy of cyber-attacks on SCADA systems was developed by [13]. The study has proposed a taxonomy of cyber-attacks on supervisory control and data acquisition (SCADA) systems. The aim is to capture the understanding of SCADA systems by presenting the relation to IT systems. The taxonomy classifies attacks on SCADA systems using the vulnerability, the type of attack on hardware, the type of attack on software and the type of attack on the communication stack. The various attack classifications compose the cyber-physical related attacks. The authors provide more descriptive categories in the software and communication related attacks, whereas the vulnerability and hardware related classifiers are general in nature. This research gives rise to incorporating physical attack initiatives relative to cyber security.

In [14] has proposed cyber-attack taxonomy for SCADA systems based on the taxonomy presented by [9]. The study categorizes attacks based on source, method of operation, attack impact and targets. The study also demonstrates how a modified version of [9] taxonomy can efficiently classify attacks targeting control systems through analyzing several cyber-security incidents involving critical infrastructure and SCADA systems.

In [15] presented a taxonomy of general cyber-attacks on smart grid communication. These attacks involve device attacks aiming to compromise a grid. The taxonomy consists of three major attack categories as follow:

- Data attacks that attempt to insert, alter or delete data in network traffic to deceive smart grid decision-making. Data attacks that attempt to insert, alter or delete data in network traffic to deceive smart grid decision-making.
- Privacy attacks aim to capture privacy related data, while analyzing electricity usage data.
- Network availability attacks aim to overwhelm or fully consume resources of smart grid resulting in a delay or disruption of communication.

In [16] proposed a taxonomy of security aspects of cloud computing systems. Cloud computing system attacks presented are infrastructure, application, platform, and administration. Infrastructure related threats are classified using physical security, virtualization, host, and network. Application threats involve data security and application security. Platform involves platform security; lastly administration encompasses provider and government. The study has presented a good starting point to begin the improvement of predecessor taxonomies associated with cloud computing attack incidents. In [17] described a network attack taxonomy and ontology framework. The proposed taxonomy consists of fifteen dimension; actor, actor location, aggressor, attack goal, automation level, attack mechanism, automation level, effects, motivation, phase, sabotage, scope, scope size, target and vulnerability. Due to the space constrains and the focus of this paper, only attack mechanism and target has been considered and elaborated on. Heerden have classified cyber-attacks and their exploit methodology into three main categories: access, data manipulation and information gathering. Access category may include brute force, buffer overflow and spear phishing. on the other hand, data manipulation category refer to attack methodologies that use data as an attack vector which may include various network-based, infective malware and web application-based attacks. Lastly, port-scanning and other computer network-related scanning methodology are classified under the information gathering category.

In [18] proposed a high-level cyber-attack taxonomy to classify various attacks and the mode of action for appropriate defence. The taxonomy has five main classifiers, which are attack purpose, legal classification, severity of involvement, scope and network type. Attack purpose involves reconnaissance attack, access attack and denial of service attack. Legal classification contains cybercrime, cyber espionage, cyber terrorism and cyber war. Severity of involvement corresponds to either passive or active attacks. Scope pertains to malicious large scale or non-malicious small scale. Lastly, network type classifies attacks either in mobile ad-hoc network (MANET) or wireless sensor network (WSN).

In [19] proposed defence-oriented multidimensional attack taxonomy (DMAT). The taxonomy utilizes nine classifiers to capture the characteristic of the attack. These classifiers are attack target, attack impact, attack purpose, attack cost, attack exploiting, attack source, attack automation, attack loss and defence. The proposed taxonomy classifies the cyber-attacks based on their targets, impact and purpose. Attack targets covers system infrastructure, operating systems, network and its applications, while attack purpose include several goals such as denial of service attack, privilege elevation, unauthorized read and write data, probe. On the other hand, attack impact dimension categorize attacks based on their mechanism such as password attack, buffer overflow, virus, worm, Trojan horse, information collection, network attack and physical attack.

In [20] proposed taxonomy of network security tools that can be utilized by both attacker and defender to strengthen the research of network security. The taxonomy classifies network security tools according to attacker tools and defender tools. Attacker tools involve information gathering and attack launching. Attack launching classifies the tools with respect to Trojans, DoS/DDoS and packet forging attack, application layer attack, fingerprinting attack, user attack and others. Information gathering is shared between the attacker and defender, which encompass sniffing and network mapping/scanning. Classifying tools beneficial to the defender are considerably limited; comprise information gathering and network monitoring. Network monitoring classifiers only include visualization and analysis. Cyber security taxonomy deliberate on cross-domain attacks is presented by [21]. The proposed taxonomy consolidates the quantitative and qualitative analysis of cyber-physical attacks to improve critical infrastructure security. The study has proposed a six-dimensional taxonomy derived from attack, target and effect as follow:

- Influenced Element describes the object that is manipulated by an attack. This element can reside in cyber or physical domain. It can be either an integral part of CPS or be part of cyber or physical environment CPS is interacting with.
- Influence describes the manipulation on the Influenced Element that implicate the change of the element’s state.
- Victim Element is a counterpart of the Influenced Element dimension that represents indirectly affected element(s) due to the interactions between the cyber and physical domains.
- Impact on Victim is the counterpart of the Influence dimension. It describes the impact on the Victim Element.
- Attack Means defines how the manipulation on the Influenced Element has been performed.
- Preconditions dimension defines conditions under which Attack Means will lead to the consequences described in Effects dimensional group.

Based on the defined dimensions, the study has classified existing attacks into four distinct categories: cyber-to-cyber, cyber-to-physical, physical-to-physical and physical-to-cyber

In [22] have presented a review on attacks against SCADA control systems. The study presented a set of 17 attacks against SCADA control systems classified into four categories reconnaissance, response and measurements injection and denial of service attacks. SCADA reconnaissance attacks gather control system network information and identify the device characteristics such as model number, supported network protocols and system memory map. Response and management injection attacks utilize the lack authentication features of many industrial control system network protocols to capture, modify and forward response packets which contain sensor reading values. On the other hand, command injection attacks utilize the same weakness in the protocol implementation to inject false control and configuration commands into a control system. Lastly, similar to the standard IT systems Denial of Service (DOS) attacks against industrial control system attempt to stop the proper functioning of some portion of the cyber physical system to effectively disable the entire system.

In [23] created a cyber-attack taxonomy called AVOIDIT which described attacks using five, extensible classifications: attack vector, operational impact, defence, informational impact and target. This taxonomy was created as a network taxonomy which unlike previous efforts, allowed the classification of blended attacks. Additionally, it also allowed for the classification of attacks by both operational and informational impacts and was designed to help educate defenders by looking at attacks’ various impacts, vectors or target types. While this taxonomy focused exclusively on cyber-attacks, its structure and style were very useful in designing the proposed taxonomy in this paper, especially the ability to view and categorize attacks from Applegate different taxonomic perspectives.

Another research on cyber-physical attack taxonomy for classifying security incidents that focuses on cross domain and impact oriented analysis is presented by [24]. The study showed that cross domain analysis provides insights into how systems interact with each other, while the impact oriented approach identifies the effects an incident has on the system and the surrounding environment. The proposed taxonomy includes four main categories with sub-classifications and modifiers to provide further detail. The four main categories are source type, means, impact and victim which are defined as follow:

- Source type describes the general features of the entity where an incident originated, the described source types include Commercial, Government, Educational, Non-Profit Organization, Individual, Identified Group and Unknown.
- The Means category is used to indicate how an incident occurred which implicate the methods used by the attacker. It would also describe what went wrong in the case of an unintentional failure. Cyber-attacks can be classified within the means category as Misuse of Resources, User level Resource Compromise, Root-level Resource Compromise, Social Engineering, Virus, Website Compromise, Trojan, Worm, Recon, Denial of Service and Other System Failure.
- The impact of an incident describes what effect the incident had on the system or surrounding environment. This category is designed to describe the effect of an incident on the computer system, the physical system, the organization and the community where the incident occurred.
- Lastly, The Victim of an incident denotes where an incident occurs. The victim may be the target of a purposeful attack or it may be the entity where an accident or failure occurs.

A more narrowly drawn taxonomy developed by [1] looked at the characteristics of the attack itself. The Taxonomy for Targeted Attacks was developed after identifying common characteristics from several well-known attacks on ICS. This taxonomy incorporates four attack elements: purpose of the attack; initial attack vector; lateral movement; location of the command and control server. The components of this taxonomy are conceptualized around characteristics of the nature of the attack on ICS. The four attack elements incorporate methodologies by which attacks on ICS are initiated and the desired end-product of the attack.

3. Analysis of existing taxonomies

Table 1 lists a summary of the reviewed attack taxonomies. The summary demonstrates the classification criteria for each study along with attack categories. The table shows that most the reviewed works on attacks taxonomy have focused on the classification of attacks against the IT systems communication standards and its protocols. Other works has focused on the attack taxonomy for SCADA systems, which categorized the attacks based on their target in the SCADA component by listing each attack description and the vulnerability exploited by the attacker. The table also show that very limited number of studies have proposed taxonomy of cyber-attacks on industrial protocols by enumerating the cyber-attacks on the protocols regardless the implementation of the vendors. A comparison of the existing works on cyber-attack taxonomies is given in Table 2. The table presents a comparison of the reviewed taxonomies based on the classification criteria covered which include: method, impact, defence, target, tools, vulnerabilities, sources, actions, sector and intention. Where method refer to the means by which an attacker can gain access to a computer or network system in order to deliver a payload or malicious outcome. The impact is the state that determines how much damage/harm an attack could cause to the system, the impact may refer to unauthorized result (e.g. misuse of resources, denial of service), informational impact (e.g. disclosure or corruption of information) or operational impact (e.g. data and network availability). Defence refer to various defence tools used to properly defend using preventative and/or reactive methods to a potential attack. Target is the system or part of a system that the attacker is targeting, the review of related works revealed three different categories of cyber-attack targets; logical/software (e.g. accounts, process and data), physical/hardware (e.g. computer and network components) and operational (e.g. control center and outstation devices). Other categories can be defined as follow:

- Tools of attacks: refer to tools used to exploit a vulnerability e.g., user commands, scripts, toolkits and data trap.
- Vulnerability is a weakness in a system which may be used to alter the intended behaviour of the system. System vulnerability can allow for memory dumps, impersonating a system administrator or sabotage system’s availability. Such outcomes can be caused by design, implementation and configuration vulnerabilities.
- Source: The attack origin describes the location of the attacker with respect to the target such as local or remote attacks.
- Actions are steps taken by a user or process in order to achieve a result, such as to probe, scan, flood, authenticate, bypass, spoof, read, copy, steal, modify or delete. Actions may also refer to any act that attempt to intercept, interrupt, modify and fabricate a control system command or reading,
- Intention: refer to the intention of an attack such as cyber-crime, espionage, terrorism and cyber war.
- Sector: refer to type of the source of an attack (commercial, government, education, international, individual uses and unknown sources).
- Intention: refer to the intention of an attack such as cyber-crime, espionage, terrorism and cyber war. It also may refer to the type of the victim of an attack (e.g. commercial, government etc.).

Table 2 shows that the majority of the existing taxonomies categorize cyber-attacks based on attack vectors (method) and their intended targets. Other studies focused on the attack consequences, which have been broadly categorized into unauthorized results, informational and operational impacts. Table 2 also shows that only a few studies covered cyber-attack and defence tools, as well as attack categorization based on system vulnerability that an attack attempt to exploit. In general, little attention has been given to other classifiers such as actions, source and intentions as well as attack origin. One of the most significant attack taxonomies in the literature is presented by [23] called AVOIDIT. The presented taxonomy classifies attack components by attack vectors, operational impact, defence, informational impact and target. One of the key features of this taxonomy is that it provides a systematic attack description covering its caused, impact and target as well as the defence mechanism to conquer the attack. AVOIDIT intended to provide the defender with attack vector details to what encompasses an attack and any impact the attack may have on a targeted system, as well as strategies a defender can employ to remain vigilant in defending against attacks before and after its occurrence. Therefore, for the purpose of this paper a modified version of AVOIDIT taxonomy shall be considered.

4. Avoidit attack taxonomy

In [23] claimed that AVOIDIT provides a more apparent approach to educate the defender on attack vectors used to launch attacks. The presented taxonomy classifies attacks in a tree structure, which provides a systematic method of characterizing a variety of attacks and enumerates the ways an attack could occur. This is done using the cause, action, defence, analysis and target process used to facilitate attack classification. AVOIDIT uses five major classifiers to characterize the nature of an attack: classification by attack vector, operational impact, defence, informational impact and classification by attack target. The following subsections explain the AVOIDIT categories in details.

4.1. Classification by attack vectors

Attack vector is defined as a path by which an adversary can gain unauthorized access to a host. Attack vectors may utilize one or more system vulnerabilities as they are the main source of threat penetration. System vulnerabilities including (hardware, software and protocol vulnerabilities) are most common targets of cyber-attacks. For example, vulnerabilities, bugs and glitches of software grant hackers remote access to system and correspondingly to the data, local network resources and other sources of information. In [23] has presented 10 attack vectors. Attack vectors are briefly described in Table 3.

4.2. Classification by operational impact

Cyber-attacks can be categorized based on their operational impact. AVOIDIT taxonomy presented 6 attack classes under this category: misuse of resources, user compromise, root compromise, web compromise, install malware and denial of service. Table 4 presents a brief description on operational impact classes.

4.3. Classification by defence

One of the main significant characteristics of AVOIDIT taxonomy is that, the taxonomy highlights several strategies a defender can employ to remain vigilant in defending against attacks before and after its occurrence. This is to provide the defender available solutions to defend against attack vectors thwarting a potential threat. In [23] suggested two main methods of defending that can be used separately or consecutively when describing an attack; mitigation and remediation.

Table 1: Summary of the Reviewed Attack Taxonomies

Study	Domain	Classification Criteria	Attack Categories / Examples
[6]	Standard IT	Tool	Physical attack, information exchange, user command, script, toolkit, data trap.
		Vulnerability	Design, implementation or configuration vulnerabilities.
		Action	Probe, scan, flood, authenticate, bypass, spoof, read, copy, steal, modify and delete.
		Target	Account, process, data, component, computer, network and internetwork.
		Unauthorized result	Increased access, disclosure of information, corruption of information, denial of service and theft resources.
[7]	Standard IT	Vulnerabilities	Improper Validation, Improper Exposure, Improper Randomness and Improper De-allocation.
[8]	Standard IT	Attack vector	Virus; worms; Trojan; buffer overflow; denial of service attack; network attacks; physical attacks; password attacks and information gathering attacks.
		Attack targets	Hardware; software (operating systems; applications and network protocols).
		Vulnerabilities	Vulnerability in implementation; vulnerability in design and vulnerability in configurations.
		Payloads	Corruption of information; disclosure of information; theft of service and subversion.
[9]	Standard IT	Source sector	Commercial, government, education, international, individual uses and unknown sources.
		Method of operation	Misuse of resources, user/root compromise, social engineering, virus, web compromise, Trojan, worm, denial of service.
		Impact	Disrupt, distort, destruct, disclosure, unknown.
		Target services	Commercial, government.
[10]	SCADA	Attack origin	Local; remote.
		Attack action	Probe; scan; flood; authenticate; bypass; spoof; eavesdrop; misdirect; read/copy; terminal; execute; modify and delete.
		Attack target	Network; process; system; data; user.
[11]	Standard IT	Attack Vector	Viruses; worms; Trojans; buffer overflow; denial of service; network attacks; physical attacks; password attacks and information gathering.
[12]	SCADA	Target	Control centre, outstation devices and network/communication paths.
		Threat	Interception, interruption, modification and fabrication.
[13]	SCADA	Target	Cyber-attacks on hardware; software; communication stack and implementation of protocols.
[14]	SCADA	Source sector	Commercial, government, education, international, individual uses and unknown sources.
		Method of operation	Misuse of resources, user/root compromise, social engineering, virus, web compromise, Trojan, worm, denial of service.
		Impact	Disrupt, distort, destruct, disclosure, unknown.
		Target services	Commercial and government.
[15]	Smart grid	Operational impact	Data, privacy and network availability.
[16]	Cloud computing	Target	Infrastructure (e.g. physical security, virtualization, host and network), application, platform and administrator.
[17]	Standard IT	Attack vector	Access: brute force, buffer overflow and spear phishing. Data manipulation: network-based, infective malware and web application-based attacks. Information gathering: probe and network scanning attacks.
[18]	Wireless networks	Attack purpose	Reconnaissance attack, access attack and denial of service attack.
		Legal classification	Cyber-crime, cyber espionage, cyber terrorism and cyber war.
		Involvement	Passive or active attacks.
		Scope	Malicious large scale or non-malicious small scale.
		Network type	Mobile ad-hoc network (MANET) or wireless sensor network.
[19]	Standard IT	Attack target	Infrastructure, operating systems, network and application.
		Attack impact	Password attack, buffer overflow, virus, worm, Trojan horse, information collection, network attack and physical attack.
		Attack purpose	Denial of service attack, privilege elevation, unauthorized read and write data, probe and others.
[20]	Standard IT	Attacker Tools	Information gathering (e.g. sniffing and network mapping/scanning). Attack launching (e.g. Trojans, DoS/DDoS, packet forging attack, application layer attack, fingerprinting attack, user attack and others).
		Defender Tools	Information gathering (e.g. sniffing and network mapping/scanning). Network monitoring (IDS and pentest tools).
[21]	CPS	Target	Cyber-to-cyber, cyber-to-physical, physical-to-physical and physical-to-cyber.
[22]	SCADA	Mechanism	Reconnaissance; response and measurement injection; command injection and denial of service.
[23]	Standard IT	Attack Vector	Mis-configuration; kernel flaws; design flaws; buffer overflow; insufficient authentication validation; insufficient input validation; symbolic link; file descriptor; attack race condition; incorrect permissions and social engineering.
		Operational impact	Misuse of resources; user compromise; web compromise; installed malware and denial of service.
		Defence	Mitigation and remediation.
		Informational impact	Distort; disrupt; destruct; disclose and discover.
		Target	Operating system (kernel / user / driver); network; local; user and application
[24]	Cyber physical attacks	Source type	Commercial, Government, Educational, Non-Profit Organization, Individual, Identified Group and Unknown.
		Attack Means	Misuse of Resources, Userlevel Resource Compromise, Root-level Resource Compromise, Social Engineering, Virus, Website Compromise, Trojan, Worm, Recon, Denial of Service and Other System Failure.
		Impact	Service Disruption, Information Distortion, Physical Destruction, Environmental Destruction, Information Destruction, Information Disclosure, Death/Serious Injury and Unknown.
		Victim	Victim type (e.g., Commercial, Government, Educational, Non-Profit Organization, Individual, Identified Group and Unknown.

[1]	SCADA		Victim Market Sector (e.g. Utilities, industrial process control, healthcare, transportation, aerospace, military and consumer electronics).
		Purpose of the attack	Exfiltration of sensitive information from target such as intellectual property theft and identity theft attacks.
		Initial attack vector	Automatic (e.g. drive-by-download attack) Manual (spear phishing attack)
		Lateral movement	Attacker establishes presence in victim's network then attempts to compromise additional computers.
		Location of the command and control server	Compromised computer used as C&C to give orders to infected machines connected computers connect to remote servers to receive orders.

Table 2: Summary of the Reviewed Cyber Attack Taxonomies

Study	Method	Impact	Deface	Target	Tools	Vulnerabilities	Sources	Actions	Sector	Intention
[6]		x		x	x	x		x		
[7]						x				
[8]	x	x		x		x				
[9]	x	x							x	x
[10]				x			x	x		
[11]	x									
[12]				x				x		
[13]				x						
[14]	x	x							x	x
[15]		x								
[16]				x						
[17]	x									
[18]	x								x	
[19]	x	x		x						
[20]			x		x					
[21]				x			x			
[22]	x									
[23]	x	x	x	x						
[24]	x	x							x	x
[1]	x	x		x						

Prior to vulnerability exploitation or during an attack, there are several steps a defender can use to mitigate damage an attack has caused, or has the potential to cause. For example, in case of worm propagation within a computer network, the defender is able segregate the infected hosts from the network to prevent further damage. On the other hand, remediation would involve taking the appropriate steps to correct the situation prior to or during an exploitation. Remediation involves system patching and source code rectification to minimize the risk of existing vulnerabilities.

4.4. Classification by informational impact

In [23] claim that any form of cyber-attack has the potential to impact sensitive information in various ways. One of the information security requirements is that a system should be able to protect themselves against theft, disruption, distortion or destruction of sensitive information assets. Therefore, it is important to identify cyber-attacks those have a significant impact on systems information. This section classifies an attack's impact or the effect on information and defines the criteria used.

- Distort A distortion in information, usually when an attack has caused a modification of a file. When an attack involves
- distort, it is a change to data within a file or modification of information from the victim such as website defacement, man-in-the-attacks and viruses that destroy data.
- Disrupt A disruption in services, usually from a Denial of Service. When an attack involves disrupt, it is an access change, or removal of access to victim or to information.
- Destruct: A destruction of information, usually when an attack has caused a deletion of files or removal of access.
- Disclosure: A disclosure of information, usually providing an attacker with a view of information they would normally not have access to. Disclosure may include sniffing password off the wire, illegitimate data access of a hard drive and an authorized access to confidential information.
- Discovery: The discovery of information not previously known. For example, when a scanning tool probes for information, the information discovered can be used to launch an attack on a particular target.

Table 3: Outline of Avoid it Attack Vector

No.	Attack Vector	Description
1	Mis-configuration	An attacker may take the advantage of improperly configured systems or applications such as network routers default settings to gain access to a network in order to cause a variety of attacks.
2	Kernel Flaw	Security kernel flaws within an operating system may lead an attacker to gain certain privileges and carryout range of cyber-attacks.
3	Buffer Overflow	An attacker can exploit buffer overflow vulnerability within an operating system or specific software to gain higher privileges at the administrative level or even a possible exploitation of arbitrary code execution.
4	Insufficient Authentication Validation	An attacker can exploit vulnerability in the authentication validation process to compromised user credentials in order to impersonate a valid user, gain access to a specific system or even attain higher privileges at the administrative level.
5	Insufficient Input Validation	An attacker can exploit a vulnerability in the input validation process with the intention of inject arbitrary code.
6	Symbolic Links	A symbolic link is a special file-system object that contains a reference to another file or directory in the form of an absolute or relative path. An attacker can exploit a symbolic link vulnerability to direct the process of the operating system to a malicious

		file in the intention of executing variety of attacks.
7	File Descriptor	In Unix and related computer operating systems, a file descriptor is an abstract indicator used to access/handle a file or other input/output resource. An attacker can exploit a file descriptor vulnerability to gain elevated privileges or perform unauthorized I/O operations.
8	Race Condition	An undesirable situation that occurs when a device or system attempts to perform two or more operations at the same time. Race condition may allow an attacker to gain higher privileges, while a program or process in privilege mode.
9	Incorrect File/ Directory Permission	An attacker may exploit incorrect permissions associated to a file or directory to carryout range of attacks.
10	Social Engineering	Social engineering includes psychological manipulation of people into performing actions or divulging confidential information.

Table 4: Outline of Avoid it Operational Impact

No.	Operational Impact	Description
1	Misuse of resources	Refer to any unauthorized use of IT resources that requires a certain privileges.
2	User Compromise	Attacks under this category utilize unauthorized user privileges on a host.
3	Root Compromise	Refer to any attacks that grant elevated privileges above the user such as administrative and/or root privileges.
4	Web compromise	Attacks under this category involve the use of a malformed website or web application to exploit system vulnerability.
5	Installed malware	An attacker exploit system vulnerabilities or trick the user into install malicious software, which allow an adversary to gain full control of the compromised system leading to the exposure of sensitive information or controlled remotely.
6	Denial of service	Refer to an interruption in an authorized access to a computer network or a particular resource or service, typically one caused with malicious intent.

4.5. Classification by target

Cyber-attacks target various resources such as operating systems, computer networks and software applications leaving the defender unknowingly susceptible to the next attack. This section classifies targets an attack will use to perform unauthorized privileges.

- Operating system: An attack can be formulated to target vulnerabilities within a particular operating system.
- Network: Target a particular network or gain access through a vulnerability within a network or one of the network protocols.
- Local: An attack targeting a user’s local computer.
- User: An attack against a user is an attack to retrieve a user’s personal information.
- Application: An attack towards specific software. An application can be either client or server. A client application is software that is available to aid a user performing common tasks. A server application is software designed to serve as a host to multiple concurrent users.

5. Conclusion and future work

Industrial control systems in the energy sector involve a hierarchy of sensing, monitoring and control devices connected to centralized control stations or centers. The incorporation of commercial off-the-shelf technologies in energy control systems makes them vulnerable to cyber-attacks. A taxonomy of cyber-attacks against control systems can assist the energy sector in managing the cyber threat. This paper takes the first step towards a taxonomy by presenting a review of existing attacks taxonomy related to both IT and control systems. This research showed that, the majority of the existing taxonomies categorize cyber-attacks based on attack vectors (method) and their intended targets. Other studies focused on the attack consequences, which have been broadly categorized into unauthorized results, informational and operational impacts. It also showed that, only a few studies covered cyber-attack and defence tools, as well as attack categorization based on system vulnerability that an attack attempt to exploit. From this study, we conclude that in general, little attention has been given to other classifiers such as actions, source and intentions as well as attack origin.

Acknowledgement

This research study is funded by TNB Seed Fund 2016 under a project 'R&D in Micro Cryptographic Engine for Protecting Data in SCADA Link'.

References

[1] Line MB, Zand A, Stringhini G & Kemmerer R (2014), Targeted attacks against industrial control systems: Is the power industry prepared? *Proceedings of the ACM 2nd Workshop on Smart Energy Grid Security*, pp. 13–22.

[2] Johansson E, Sommestad T & Ekstedt M (2009), Issues of cyber security in scada-systems-on the importance of awareness. *Proceedings of the IET 20th International Conference and Exhibition on Electricity Distribution-Part 1*, pp. 1–4.

[3] Fadul J, Hopkinson K, Sheffield C, Moore J & Andel T (2011), Trust management and security in the future communication-based" smart" electric power grid. *Proceedings of the IEEE 44th Hawaii International Conference on System Sciences*, pp. 1–10.

[4] Dondossola G, Garrone F & Szanto J (2011), Cyber risk assessment of power control systems-A metrics weighed by attack experiments. *Proceedings of the IEEE Power and Energy Society General Meeting*, pp. 1–9.

[5] Karnouskos S (2011), Stuxnet worm impact on industrial cyber-physical system security. *Proceedings of the 37th Annual Conference on IEEE Industrial Electronics Society*, pp. 4490–4494.

[6] Howard JD & Longstaff TA (1998), *a common language for computer security incidents*. Technical report, California: Sandia National Labs.

[7] Lough DL (2001), *a taxonomy of computer attacks with applications to wireless networks*. PhD thesis, Blacksburg: Virginia Polytechnic Institute and State University.

[8] Hansman S & Hunt R (2005), a taxonomy of network and computer attacks. *Computers and Security* 24, 31–43.

[9] Kjaerland M (2006), a taxonomy and comparison of computer security incidents from the commercial and government sectors. *Computers and Security* 25, 522–538.

[10] Fleury T, Khurana H & Welch V (2008), towards a taxonomy of attacks against energy control systems. *Proceedings of the International Conference on Critical Infrastructure Protection*, pp. 71–85.

[11] Meyers CA, Powers SS & Faissol DM (2009), *Taxonomies of cyber adversaries and attacks: A survey of incidents and approaches*. Technical report, California: Lawrence Livermore National Laboratory.

[12] East S, Butts J, Papa M & Shenoi S (2009), A taxonomy of attacks on the DNP3 protocol. *Proceedings of the International Conference on Critical Infrastructure Protection*, pp. 67–81.

[13] Zhu B, Joseph A & Sastry S (2011), A taxonomy of cyber-attacks on SCADA systems. *Proceedings of the IEEE International Conference on Internet of Things and fourth International Conference on Cyber, Physical and Social Computing*, pp. 380–388.

[14] Miller B & Rowe D (2012), a survey SCADA of and critical infrastructure incidents. *Proceedings of the ACM 1st Annual Conference on Research in Information Technology*, pp. 51–56.

[15] Li X, Liang X, Lu R, Shen X, Lin X & Zhu H (2012), Securing smart grid: Cyber-attacks, countermeasures, and challenges. *IEEE Communications Magazine* 50, 38–45.

[16] Hashemi SM & Ardakani MR (2012), Taxonomy of the security aspects of cloud computing systems-A survey. *International Journal of Applied Information Systems* 4, 21–28.

[17] Van Heerden RP, Irwin B, Burke ID & Leenen L (2012), a computer network attack taxonomy and ontology. *International Journal of Cyber Warfare and Terrorism* 2, 12–25.

[18] Uma M & Padmavathi G (2013), a survey on various cyber-attacks and their classification. *International Journal of Network Security* 15, 390–396.

[19] Jiang W, Tian ZH & Xiang CU (2013), DMAT: A new network and computer attack classification. *Journal of Engineering Science and Technology Review* 6, 101–106.

[20] Hoque N, Bhuyan MH, Baishya RC, Bhattacharyya DK & Kalita JK (2014), Network attacks: Taxonomy, tools and systems. *Journal of Network and Computer Applications* 40, 307–324.

[21] Yampolskiy M, Horvath P, Koutsoukos XD, Xue Y & Sztipanovits J (2013), Taxonomy for description of cross-domain attacks on CPS. *Proceedings of the second ACM International Conference on High Confidence Networked Systems*, pp. 135–142.

[22] Morris TH & GAO W (2013), Industrial control system cyber-attacks. *Proceedings of the first International Symposium on ICS and SCADA* Cyber Security Research, pp. 22–29.

[23] Simmons C, Ellis C, Shiva S, Dasgupta D & Wu Q (2014), AVOIDIT: A cyber-attack taxonomy. *Proceedings of the ninth Annual Symposium on Information Assurance*, pp. 12–22.

[24] Miller WB (2014), *Classifying and cataloging cyber-security incidents within cyber-physical systems*. Master thesis, Utah: Brigham Young University.