الجمهورية الجزائرية الديمقراطية الشعبية
People's Democratic Republic of Algeria
وزارة التعليم العالي والبحث العلمي
Ministry of Higher Education and scientific research
المدرسة الوطنية العليا للتكنولوجيا
National Higher School of Technology
Department of Electrical Engineering And Industrial Computing

Final Year Project to Obtain the Diploma of
Master

Field:
Communication

Speciality: Communication Systems and Networks

- Subject -

Cyber-attacks targeting SCADA systems and their classification

By
Djamila CHABI
Hawa KEBBAL

Examination Committee:

Mr. BOUDIAR Toufik	Chair
Mrs. BOUTERFAS Malika	Supervisor
Mr. CHERIFI Tarek	Supervisor
Mr. BOUCHACHI Islem	Examiner
Mr. KHOUMERI El hadi	Examiner

Algiers, the 22/06/2023

Academic year 2022 –2023

***Abstract*—SCADA (Supervisory Control and Data Acquisition) systems are used for monitoring industrial devices. However, theirsecurity is at risk of being compromised due to the increasinguse of open-access networks. This article proposes a classificationof attacks targeting SCADA systems to enhance understanding of these attacks and provide insights to improve the security of these systems. It begins with a brief retrospective of the cyber- security history, tracing back to the 1970s with the creation of the first computer viruses, and also presents a typology of different types of hackers. Furthermore, this article offers a methodology to assess cyber-security risk, addressing the associated challenges and providing recommendations to overcome them.**

***Index Terms*—SCADA systems,Hackers,Vulnerabilities,Cyber-attacks,SCADA Threats,DoS,Trojan, Warm ,MITM.**

I. Introduction

In our interconnected world, Supervisory Control and Data Acquisition (SCADA) systems play a crucial role in various sectors such as energy, critical infrastructure, industrial production, and water distribution. SCADA systems are designed to monitor, control, and collect real-time data from physical processes. Their importance lies in their ability to automate operations, improve efficiency, and ensure the smooth functioning of critical infrastructures.

With rapidly evolving technologies and increasing connectivity, SCADA systems have become more vulnerable to cyberattacks. Compared to older, isolated, and autonomous SCADA systems, modern SCADA systems are interconnected with computer networks and information technologies, providing greater flexibility and significant operational advantages. However, this also introduces new potential vulnerabilities.

Attacks targeting these systems can be highly specific, aiming to exploit vulnerabilities unique to SCADA systems. Attackers may target different parts of SCADA systems, such as controllers, sensors, supervisory software, human-machine interfaces (HMIs), or communication protocols. Each attack targets a specific aspect of these systems, underscoring the importance of understanding the specific vulnerabilities they face.

The potential consequences of these attacks are particularly concerning, as they can lead to severe or even catastrophic disruptions in critical infrastructures. A successful attack can compromise the availability of essential services, damage expensive equipment, cause substantial financial losses, and endanger public safety.

The classification of attacks targeting SCADA systems poses a major challenge in the field of securing these critical systems. Understanding and categorizing these attacks is of paramount importance, as it would enable companies to better understand the threats they face and implement more effective security measures. However, the current classification has limitations that restrict its relevance and specific applicability to SCADA systems. Therefore, the central issue is to determine how to improve the classification of attacks targeting SCADA systems, considering their specific characteristics, in order to enhance the security of these systems.

This paper is organized as follows In Section 2,we mention most important attacks over history . In Section 3, we describe scada system security requirements and objectives. In Section 4,we explain different classifications of attacks in scada system . In Section 5,we enumerate different types of hackers . In Section 6 we describe measurement of cyber-security.Finally in section 7,offers the conclusion.

II. Time line of Cybersecurity

In opposite of common thoughts the cyber security is not recently discovered or invented but it can be traced back to the 1970s , when the first computer viruses were created. These early viruses were simple in nature and mainly spread through floppy disks.

As the use of computers became more widespread, security became a major concern. In the 1980s and 1990s, hackers and cybercriminals began to target businesses and government organizations for financial gain.

The development of firewalls and antivirus software in the 1990s and early 2000s helped to protect computer systems, but as the internet grew, new threats emerged. The rise of phishing scams, identity theft, and ransomware attacks became more prevalent. In recent years, cybersecurity has become even more critical as society has become increasingly reliant on technology. The increased use of mobile devices, cloud computing, and the Internet of Things (IOT) has created new vulnerabilities that cybercriminals can exploit.

Governments and businesses have been forced to invest heavily in cybersecurity, but it remains a never-ending battle. And As new threats emerge, cybersecurity technology must continue to evolve to stay ahead of cybercriminals.

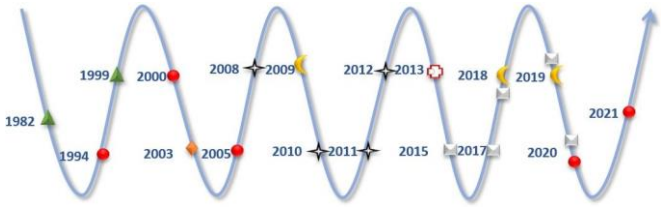


Figure 1 – time line.

1) most important cyber incidents : :

— 1982 : Siberian pipeline explosion caused by Torjan horse , it was a cyber incident with critical damages conduct to a powerful explosion Caused by Torjan horse placed in SCADA System by altering important organs [8] .

— 1994 : SRP (Salt River Project) It was a significant event in history highlighting the potential consequences of cyber attacks on critical infrastructure with an aceess to the company's computer [24].

— 1999 : Russian gas pipelines also caused by Trojan horse ; hackers used to hack into Gazprom and control the central switchboard which controls gas flow through the pipelines [24].

— 2000 : Maroochy water breach , It was in the Australian state involving a computer hacker (Mr. Boden) ex-employee motivated by his revenge and use an unauthorized access to control system and released raw sewage into local waterways which caused significant environmental damage [25].

— 2003 : The Slammer worm (SQL Slammer) , It Was a computer worm that caused widspread damage to computer networks . One of the affected networks was the Davis Besse Nuclear Power station in Ohio , which was forced to shut down for several hours as a result of the attack [26].

— 2005 : Taum Sauk hydroelectric power station failure caused by a breach in the upper reservoir of the power station where a catastrophic failure occurred at the power station, resulting the release of 1.3 billion gallons of water causing significant damage to the park and injuring several people who were camping nearby [14].

— 2008 : Georgia Cyberwar : During the 2008 South Ossetia War between Georgia and Russia, there were numerous cyber attacks on Georgian government websites and critical infrastructure, such as banks and media outlets. The attacks were believed to have been carried out by Russian hackers [27].

— 2009 : pierce of Electricity grid in U.S. penetrated by spies which installed malware on the grid's control systems , it was reported that the U.S. electricity grid had been penetrated by foreign spies it was suspected that Russia and China were involved . The news came from a report published in The Wall Street Journal [14].

— 2010 : Stuxnet virus , Stuxnet is a computer worm considered to be one of the most complex computer viruses ever created and which is widely believed to have been developed by the United States and Israel to disrupt Iran's nuclear program. It was specifically designed to target industrial control systems, particularly those used in nuclear facilities [24].

— 2011 and 2012 : Duqu and Flame virus , Duqu was in the middle east designed to steal sensitive information from computers and was similar in some ways to the Stuxnet virus, Duqu was believed to have been created by a nation-state for cyber espionage purposes, and its primary targets were in the Middle East [14], [24].

Flame virus in Iran , was one of the most complex and sophisticated pieces of malware ever discovered at the time. It was designed to collect and steal a wide range of data from infected computers, including documents, emails, and audio conversations. Like Duqu, Flame was also believed to have been created by a nation-state for cyber espionage purposes [14], [24].

— 2011 :The RQ-170 Sentinel is an unmanned aerial vehicle (UAV) designed and built by Lockheed Martin for the United States Air Force (USAF). In December 2011, an RQ-170 Sentinel was reportedly captured by Iranian authorities while conducting surveillance over Iranian airspace.
Iran claimed that they used electronic warfare techniques to take control of the drone and safely land it. They also released footage of the drone, which appeared to be in good condition, contradicting US claims that the drone had crashed due to a malfunction. The incident caused diplomatic tensions between the US and Iran [20].
— 2013 : OpIsrael an annual coordinated cyberattack, using DDoS attacks and other methods where Hacktivists target Israeli government yearly [42].
— 2015 : an attack against Ukrainian regional power companies using phishing email . The attack started with a phishing email that contained a malware attachment , once the malware was installed, it allowed hackers to gain remote access and control systems to shut down power distribution equipment.The Ukrainian government blamed the Russian one for this attack [8].

— 2017 : Attack on many western energy companies with the Phishing mails , a Russian hacking group, attacked many western energy firms, enter into networks of around 20 + firms, also get operation control in the US and Turkey, and also aimed to sabotage operational systems at energy facilities [14].

— 2017 :The NotPetya attack. In June 2017, a destructive malware attack known as NotPetya spread across the globe, affecting businesses in Ukraine, Russia, and other countries. The attack is believed to have been carried out by the Russian government [34].

— 2018 : Here are some of the significant SCADA cyber incidents that occurred in 2018 :
  — Atlanta Ransomware Attack : In March 2018, the city of Atlanta was hit by a ransomware attack that affected its SCADA system, causing widespread disruption to city services. The attack encrypted important files and demanded a ransom to restore

access [28].

- Dragonfly 2.0 Cyber Espionage : In October 2018, the US Department of Homeland Security issued a warning about a Russian hacking group known as Dragonfly 2.0, which had been targeting critical infrastructure, including SCADA systems. The group was believed to have carried out reconnaissance operations against a number of energy companies [29].

- Bank of Chile Cyber Attack : In May 2018, the Bank of Chile was targeted in a cyber attack that affected its online and mobile banking services. The attack was believed to have been carried out by a group known as Lazarus, which has been linked to North Korea.
- MyEtherWallet DNS Hijacking : In April 2018, MyEtherWallet, a popular cryptocurrency wallet service, was hit by a DNS hijacking attack that redirected users to a phishing site. The attack was believed to have been carried out by a group of attackers who were able to compromise the DNS settings of the site's domain registrar [30].

- 2019 :
  - Norsk Hydro Cyber Attack : In March 2019, Norwegian aluminum producer Norsk Hydro suffered a major cyber attack that affected its production facilities worldwide. The attackers used ransomware to encrypt files and demanded a ransom to restore access [31].
  - Triton Malware Attack : In August 2019, the Saudi Arabian petrochemical plant was hit by a cyber attack using malware, which was specifically designed to target industrial control systems (ICS). The attack caused a shutdown of the plant's safety systems, and it is believed to be the first-ever successful attack on a safety instrumented system (SIS) [32].
  - APT10 Cyber Espionage : In May 2019, the US Department of Justice charged two Chinese nationals with being members of the APT10 hacking group, which targeted numerous companies, including those in the SCADA industry. The group was involved in stealing sensitive information and intellectual property from the targeted organizations [33].
  - Electric Grid Cyber Attack : In May 2019, the US Department of Energy reported that hackers had gained access to the networks of several electric utilities in the US. While the attackers did not appear to have caused any damage or disruption, the incident raised concerns about the vulnerability of the country's critical infrastructure [43].
- 2020 :
  - Oldsmar Water Treatment Facility Hack : In February 2021, a cyber attack targeted a water treatment facility in Oldsmar, Florida, in which the attacker gained access to the SCADA system and attempted to increase the levels of lye, a chemical used to treat drinking water. Fortunately, the attack was detected in time, and no harm was done to the water supply [35].
  - Honda Cyber Attack : In June 2020, Japanese automaker Honda suffered a cyber attack that disrupted its production and supply chain operations worldwide. The attack affected the company's SCADA systems, causing production to come to a halt in several of its plants [36].
  - ExPetr Cyber Attack : In 2020, several Ukrainian power companies were targeted by the ExPetr malware, which disrupted their SCADA systems and caused power outages in several regions. The attack was attributed to the Sandworm hacking group, which has been linked to the Russian government.
- 2021 :
  - Colonial Pipeline Cyber Attack : In May 2021, the US-based Colonial Pipeline was targeted by a ransomware attack that disrupted its operations and caused a temporary shutdown of the pipeline, which supplies fuel to several states on the East Coast. The attack was attributed to the DarkSide hacking group [37].
  - Microsoft Exchange Server Hack : In March 2021, Microsoft Exchange Server was targeted by a cyber attack that exploited vulnerabilities in the software to gain access to email accounts and other sensitive data. The attack affected thousands of organizations worldwide, including those in the SCADA industry [38].
  - JBS Cyber Attack : In May 2021, JBS, one of the world's largest meat processing companies, suffered a ransomware attack that disrupted its operations worldwide. The attack affected the company's SCADA systems, causing production to come to a halt in several of its plants.
    - Kaseya Supply Chain Attack : In July 2021, the software company Kaseya suffered a supply chain attack that affected its VSA software, which is used by several managed service providers (MSPs) worldwide. The attack was carried out by the REvil ransomware group, and it affected several organizations, including those in the SCADA industry [38].

These incidents highlight the growing threat of cyber attacks on SCADA systems and the need for improved security measures to protect critical infrastructure.

III. SCADA SYSTEM SECURITY REQUIREMENTS AND OBJECTIVES

SCADA systems process and store sensitive information such as processing, control and other operational data. High security level is necessary to secure all the data of this system against vulnerable attacks [8]. This means that the main security objectives must be achieved [2].

A. cyber-attacks objectives

Main security objectives are confidentiality, integrity, and availability (CIA triad) [2].The CIA triad is a model designed to guide policies for information security in smart grid systems which is shown in Figure 2 [9].



FIGURE 2 – The CIA triad [10].

1) Confidentiality: protects the information and data in the scada system from unauthorized access and disclosure. In other words, the confidentiality criterion requires protecting both personal privacy and proprietary information from being accessed or disclosed by unauthorized entities, individuals, or processes [1]. Once an unauthorized disclosure of information occurs, confidentiality is lost [1].

2) Integrity: The integrity of SCADA systems is crucial to ensure that the system works as expected and that the data generated by the system is accurate and reliable.in other words , The information should not be modified in an unauthorized or undetected manner [9].

3) Availability: Availability is the protection of the information system from breakdown [2].It also means that information must be available to authorized parties when it is needed without any security compromise [9].

B. cyber-attacks security requirements

There are also some security requirements in addition to the CIA triad to ensure cyber-security in smart grid applications [2].For example , Authentication as described below .

1) Authentication: is the key process of verifying the identity of a device or user to protect scada systems from unauthorized access [9].There are three methods to verify the identity of the legitimate user. They are password, tokens and biometrics [11].By these verification methods it can be ensured that resources are accessed only by the appropriate parties that are correctly identified [9].

IV. CLASSIFICATION OF ATTACKS

SCADA systems are becoming increasingly connected to enterprise networks and the internet, which makes them vulnerable to cyber attacks. Attacks against these systems can be devastating, as they can result in significant material and human damages.

In this section, we will examine different classifications of cyber attacks targeting SCADA systems, as well as examples of attack types located in TABLE II that fall under each classification.

A. Classification of SCADA cyber-attacks according to the CIA triad

cyber attacks in the scada systems based on CIA Triad can be classified as below :

1) Cyber Attacks Targeting Confidentiality: involve malicious actors attempting to access, use, or modify confidential information without authorization.

2) Cyber Attacks Targeting Integrity: are malicious cyberattacks aimed at altering or destroying data and information.

3) Cyber Attacks Targeting Availability: are designed to disable or disrupt a target's ability to access systems, networks, or services. These attacks are often referred to as denial of service (DoS) or distributed denial of service (DDoS) attacks.

B. classification by origin of attack

1) Internal attacks: Internal attacks are attempts to endanger the SCADA system by a user or group of users who have access to the system. These attacks may include attempts to gain unauthorized access to sensitive systems or data, attempts to gain access to unauthorized functions, unauthorized system or data modifications, data theft, and data manipulation. Internal attacks can also be carried out by attackers and malware such as viruses and Trojans.

2) External attacks: External attacks are attempts to compromise the SCADA system by individuals or organizations that do not have access to it. These attacks may include attempted hacking, denial of service, distributed denial of service (DDoS) and attempts to gain unauthorized access to sensitive systems or data. External attacks may also include attempts to undermine the SCADA system using known or undocumented security vulnerabilities. External attacks can also be carried out by malware such as viruses and Trojans.

C. Classification by attack impact

1) Passive attacks : Passive attacks target the confidentiality of systems [3]. They aim to gather information about the system without disrupting the normal functioning of the network. This collected information can be used to prepare other active attacks, or for malicious activities. Detection of passive attacks is very difficult, as the network operation, itself is not affected. For example, the snoping attack [4]as explained in Table 2.

2) Active attack : Active attack is a direct attack against SCADA systems that modify or destroy data exchanged in the network, this attack aims to cause an impact on the system. Its consequences can be serious, including the loss of control of industrial processes and the destruction of critical data. For example, Denial-of-Service(DoS) Attack [4]as explained in Table 2.

D. classification by attack location

1) attacks on hardware: Hardware attacks against SCADA systems can take many forms, including physical modifications, reverse engineering, and the use of firmware vulnerabilities. The attacker could obtain unauthenticated remote accees to peripherics and modify their functionality .for example, the doorknob-rattling attack as explained in Table 2.

2) attacks on software : A software attack on a SCADA system is a malicious attack on software components of the system. These attacks can be used to access sensitive data, disrupt the operation and damage the SCADA system. For example, SQL injection as explained in Table 2.

3) attacks on network connection: The attack on communication stack can be on the network layer, transport layer, and the application layer [5]. Table 1 gives a classification of attacks based on the layers of the Open Systems Interconnection (OSI) model [2, 6].

TABLE I – classification of attacks based on the layers of (OSI) model

Layer	Attacks
Application layer	Ransomware,Viruses/Worms,ARP Spoofing,Botnets,Man-in-the-Middle (MITM) [10].
Presentation layer	
Session layer	
Transport Layer	IP Spoofing , Data Injection, Flooding Attacks, RIP attack ,Replay attack [6], [10].
Network Layer	IP Smurfing,Vulnerable old firmwares,Default Passwords [10].
Data Link Layer	
Physical Layer	Environmental and physical threats [10].

E. Cyber attacks classification in scada system based on the attacking cycle

Generally, a computer attack unfolds in four steps : Reconnaissance,Scanning, Exploitation, Maintaining access,as shown in Figure 3 [7]. The explanation of these is described below.



FIGURE 3 – Attacking cycle followed by hackers to get control over a system.

In Sacda systems, attackers follow the same steps mentioned in Figure 3, to take control of the system and compromise the security criteria [7] . The types of attacks can be classified according to these steps as shown in Figure 4 [7]. As can be seen, most types of attacks can occur during the exploitation step [7].



FIGURE 4 – Cyber attacks classification in scada systems based on the attacking cycle.

1) Reconnaissance: in the first step, the attacker gathers and collects information about its target [7] without interacting with target systems. There are two types of reconnaissance named active and passive [12].

reconnaissance active : you will directly interact with the computer system to gain information [12].

reconnaissance passive :you will not be directly connected to a computer system [12].

2) Scanning: It involves taking the information discovered during reconnaissance and using it to examine the network [12]. In this step, attacker tries to find out the weakest link in the system or the vulnerability of the system [8].

3) Exploitation: Here, attacker executes his plan of action and tries to get full control of the system and compromise the data [8].This is the phase where the real hacking takes place [12].

4) Maintaining access: In the final step,the attacker installs an undetectable and cloaked program [8] that could be used to gain permanent access to the target [7] .

V. HACKERS TYPES

To understund the difference between each type of hacking it must define theire knowledgement and activities for that Two patterns, knowledge acquisition and knowledge provision, are noted to be particularly informative. Based on these two features hacker profiles are classified in general into four types : guru hackers, casual hackers, learning hackers, and beginner hackers [40].

A. Eathical hackers or (white hat hacker) :

Behaviour : legal.
Motivation : Provide security.
Operation : cyber security activities.

white hat hackers known as ethical hackers, golden guys and hero's of government ; they are the opposite polar of black hat hackers have same techniques trying to enter and steal like a thief but have noble intentions with improving safety.

TABLE II – CYBER ATTACKS IN SCADA SYSTEMS , THEIR OBJECTIVE AND DESCRIPTION.

Attacking cycle step	type of attack	Objective violation	description of the attack
Reconnaissance	Social engineering	Confidentiality	Social engineering is a manipulation technique that exploits human error to gain private information [15].
	snoping attack		Is an unauthorized access to another persons´ data[4]. its purpose is to gather confidential information, such as configuration data, passwords, in order to facilitate a attack against the system.
Scanning	Scanning IP	Confidentiality	Is the process of scanning a network to search for information about connected machines, such as their IP addresses and services [7] .
	Scanning Port		Is a technique used to search for open ports on a remote host and identify the services running on those ports [7] .
Exploitation	Virus / worms	Confidentiality,Integrity, Availability	Virus is malware that is installed in a hidden way on a computer or equipment [17]. Worms is a type of virus that spreads through the network [17].
	Trojan horse		A trojan horse is a malicious program that can execute commands on a computer without the users´ knowledge.
	Ransomwares		Is a type of malware that prevents or limits users access to their system [17].
	Masquerade		The attacker uses a fake identity to pretend to be a legitimate user [5], in order to gain access to a system or gain greater privileges to perform unauthorized actions [7].
	SQL injection		Is a technique used by hackers to execute commands in a database.
	Doorknob rattling		The type of attack when the failed attempts of brut force remains hidden from the detection system of the network [5].
	Man-in-the-Middle (MITM)	Confidentiality,Integrity	In this type of attack, the attacker intercepts to modify interchanged messages between two posts according to his need [7].
	Replay attack		As the industrial control traffic is transmitted in plain text, an attacker could maliciously capture packets, inject a specific packet [7], and replay them to the legitimate destinations, compromising then the communications´ integrity [7].
	Denial-of-Service(DoS)	Availability	is an active attack [3]. The goal of a DoS attack is to disrupt some legitimate activity [16].
	Jamming channel		Jamming channel attacks can be used to disrupt wireless services or to prevent access to sensitive data.
Maintaining access	Backdoor	Confidentiality,Integrity, Availability	is an undetectable program, stealthy installed on the target to get back later easily and quickly [7]

white hat hackers use their technical skills and tools for protection they use their knowledge in term of legal with having permission of clients to access to their information so they act only when they are legally permitted to discover vulnerabilities of companies for fixing the defects before they are manipulated by bad actors and malicious hackers [41].

White hat hacking tools and techniques : As we had mention white hat hackers use same techniques like black hats but with the intent of helping and improving security and we mention the following :

- Pen testing :to discover system vulnerabilities .
- Email phishing : they use it to find problems of network and fix it before an attack can occur .
- Email phishing tricks the recipient of the email into providing sensitive information or clicking on a malicious file or link.
- Denial-of-service (DoS) attack. It damaged the network and degrades the performances of machines for different purpose of organizations to limit access and unaccess users .
- Security scanning : using Acunetix or Netsparker , open source pen testing tools to find and detect web application vulnerabilities

But what are their motivations ? White hat hackers hack to :

- Find and fix vulnerabilities in the system before black hat hackers exploit them.
- Develop tools that can detect cyberattacks and mitigate or block them.
- Strengthen the overall security posture of the software and hardware components.
- Build security software like antivirus, anti-malware, anti-spyware, honeypots, firewalls, etc.

B. security expert or (Grey hat hacker) :

this type fall between white hat and black hat hackers even it may be difficult to know where to draw the line , they may have good intention but in a bad way for example they look for vulnerabilities in a system without a permission but they don't cause any harm so to resume the gray hats are the middle of white and black hats ; working illegally and using all techniques with out permission but under organizations coverage . They are dangerous especially for the organizations that has critical data [43]. And there are two types : Classic Grey Hat Hackers and Malicious Insider .

a Classic Grey Hat Hackers
Behaviour : illegal .
Motivation : Data gain.
Operation : Steal critical Data .

b Malicious Insider
Behaviour : illegal.
Motivation : commercial Data gain.
Operation : Steal critical Data .

They are a group who works in coverage of organizations to pick information against theire rivals , stealls critical data illegally and without permission in favor of the company .

C. Cracker or (black hat hacker) :

A black hat hacker is someone who engages in unlawful computer and network activities to cause harm or exploit vulnerabilities for personal gain or malicious purposes. They are commonly associated with cybercrime, such as stealing sensitive data or creating malware. Black hat hackers may also engage in activities such as defacing websites, conducting DDoS attacks, and exploiting software vulnerabilities. Their goal is to hack into systems and networks with the intent of compromising security and stealing data [42].

They use their technical skills to defraud and blackmail others. They usually have the expertise and knowledge to break into computer networks without the owners permission, exploit security vulnerabilities and bypass security protocols.There are two categories under Black Hat Hacking : Classic Black Hat Hackers and Suicide Hackers

a Classic Black Hat Hackers
Behaviour : illegal.
Motivation : Money , theft data , personal purpose .
Operation : manipulate , stealing and causing harm.

Black Hat Hackers are the most dangerous Hacker types They work in the dark part of the web and to make money, they are ready to do all illegal activities such as :

- Sending phishing emails and messages.
- Using malware like viruses worms and Trojan horses.
- Crash websites or slow them down using cyber attacks such as dDoS .
- Gain money for doing political espionage.
- Selling personal information on the Dark Web and execute financial publish it .
- Threatening victims with confidential data , personal photos , videos to publish it if they don’t pay

b Suicide Hackers
Behaviour : illegal .
Motivation : Revenge and money.
Operation : stealing critical data .

This type of hackers are practically the same as suicide bombers , although they know the danger of cyber teams they work and hack systems . they just matter to their own gain of high money or revenge for personal issues .

D. penetration testers or (red hat hacker)

Behaviour : legal agressive.
Motivation : Revenge.
Operation : cyber Security Activities and attack back .

"Red Hat" is a company that produces commercial open-source software systems and contributes to many open-source projects. "Red Hat hackers" is not a term commonly used within the cyber security community. Any activities that involve unauthorized access to computer systems or networks are considered illegal and can result in severe legal and criminal consequences. So to resume Red Hat Hackers have same purpose as the White Hat Hackers but a little agressive using illigal manners to reach the goal and take aggressive steps to bring down black hat hackers servers and destroy their resources [45].

Red hat hackers use all types of tactics to do this, including :

- Infecting the bad hackers systems with malware,
- Launching DDoS attacks,
- Using tools to gain remote access to the hacker s computer to demolish it.

E. Neophyte or (Green hat hacker)

Behaviour : unidentified.
Motivation : to become an experienced hacker.
Operation : Simple attacks .

Green Hat Hackers are another hackers type that is not defined already if it is ethical or not . They are not expert but they aspire to be , they know hacking programs, codes and they are eager to learn more. But we do not know, where will they stay. At the White Part or At the Dark Part.

Green Hat Hackers can can work alongside white hat hackers , who focuses on defending against attacks , and ’black hat’ hackers , who engage in illegal hacking activities [44], [45].

F. Hacktivists :

Hacktivists" are individuals or groups of hackers who use their computer skills to carry out attacks or promote a particular social or political agenda. They typically target websites or computer systems of organizations or governments that they view as unethical or oppressive, with the goal of raising awareness or effecting change [3], [42].

G. Cyber terrorists :

"cyber terrorists" use similar tactics, but with the intention of causing widespread fear, harm, or destruction for political or ideological reasons. Their actions can cause significant damage to computer systems, and can sometimes result in physical harm or loss of life.

It is important to note that while hacktivists may be seen as engaging in a form of activism, their actions can still be illegal and can cause harm to innocent individuals or organizations. Cyber terrorism is a serious threat to national and global security, and can have devastating consequences. It is important to distinguish between the two and to work towards finding peaceful and legal means of advocating for change [3, 46].

H. State hackers

State hackers are individuals or groups employed by governments to carry out cyber-attacks or surveillance activities against other countries, organizations, or individuals. State-sponsored hacking can involve a wide range of activities, from stealing intellectual property to disrupting critical infrastructure, and can have serious consequences for national security and international relations.

State-sponsored hacking is often carried out by highly skilled and well-funded teams of hackers who are trained to exploit vulnerabilities in computer systems and networks. They may use a variety of tactics, including phishing attacks, malware, and other sophisticated techniques to gain access to sensitive information.

The use of state-sponsored hacking is controversial, as it can be seen as a violation of the sovereignty of other nations and a breach of international norms. It is important for governments to adhere to international laws and regulations, and to engage in responsible and ethical behavior when it comes to cybersecurity and information security [3].

I. Amateurs and script-kiddies

Amateurs" refers to individuals who have limited experience or knowledge in a particular field or activity. "Script kiddies" are individuals who use pre-existing computer programs or scripts to carry out cyber-attacks without fully understanding the underlying code or the potential consequences of their actions.

While amateurs may simply lack the necessary skills and experience to carry out complex tasks, script kiddies represent a more dangerous threat. They can cause significant damage to individuals or businesses, often without even realizing the full extent of their actions. It's important to note that both amateurs and script kiddies can pose security risks to networks and systems, which is why it's essential to practice responsible technology use and seek proper education and training in any field or activity that one wishes to pursue [3], [45].

J. Disgruntled employee

Disgruntled employee hackers" are individuals who are employed by an organization and use their insider knowledge and access to carry out cyber-attacks against their employer or other organizations. This can be motivated by a variety of reasons, such as revenge, financial gain, or ideology.

These types of attacks can be particularly damaging, as the hackers already have access to the organization's systems and networks, and may be able to cause significant damage or steal sensitive information. They may use tactics such as installing malware, stealing credentials, or exploiting vulnerabilities to gain access to sensitive data or systems.

To mitigate the risk of disgruntled employee hacking, it is important for organizations to have strong cybersecurity policies and practices in place, including access controls, monitoring systems, and employee training programs. It is also important for employers to maintain a positive work environment and to address employee concerns or grievances in a timely and respectful manner, in order to prevent potential insider threats [3].

VI. Measurement of Cyber -security

Measuring cybersecurity is a complex task as it involves evaluating the effectiveness of a wide range of technical and non-technical security controls, policies, and procedures that protect information and information systems from various cyber threats.

A. Why cybersecurity needs better measurement ?

Cybersecurity is a critical concern for organizations and individuals alike, as cyber attacks can result in significant financial losses, damage to reputation, and even physical harm. However, measuring cybersecurity can be difficult, as it is often a complex and multifaceted issue that requires a comprehensive approach.

Better measurement is necessary for a few reasons. First, it can help organizations better understand their current level of cybersecurity and identify areas where they need to improve. Without proper measurement, it is difficult to accurately assess the effectiveness of security controls and the overall security posture of an organization.

Second, better measurement can help organizations prioritize their cybersecurity efforts and allocate resources more effectively. By identifying the most critical security risks and vulnerabilities, organizations can focus their attention and resources on the areas that are most likely to be targeted by cyber attackers.

Third, better measurement can help organizations demonstrate their cybersecurity capabilities to stakeholders, including customers, partners, and regulatory bodies. In today's business environment, having strong cybersecurity measures in place is often a prerequisite for doing business, and being able to demonstrate the effectiveness of those measures can be a competitive advantage.

Overall, better measurement is crucial for improving cybersecurity and mitigating the risks of cyber attacks. By implementing more robust measurement frameworks and using data-driven approaches to assess cybersecurity, organizations can more effectively protect their systems, data, and networks from cyber threats [41].

B. The familiar risk matrix :

The familiar risk matrix is a commonly used tool in cybersecurity to help organizations assess and prioritize risks. The risk matrix typically consists of a two-dimensional grid that plots the likelihood of a security incident occurring against the potential impact of that incident. The likelihood is usually measured on a scale from low to high, and the impact is measured on a scale from minor to catastrophic. The intersection of these two factors determines the level of risk associated with a particular threat or vulnerability [19].

			Impact				
			Negligible	Minor	Moderate	Critical	Catastrophic
			1	2	3	4	5
Likelihood	Frequent	5	Medium	Medium	High	High	High
	Likely	4	Medium	Medium	Medium	High	High
	Occasional	3	Low	Medium	Medium	Medium	High
	Seldom	2	Low	Low	Medium	Medium	Medium
	Improbable	1	Low	Low	Low	Medium	Medium

FIGURE 5 – Risk matrix.

C. Common ways to measure cybersecurity effectiveness : [21]

1) Risk Assessment : A comprehensive risk assessment can help identify vulnerabilities and potential threats that can impact an organization's security posture. A risk assessment involves analyzing the likelihood and potential impact of specific cyber threats and vulnerabilities to identify areas that require attention and prioritization.

2) Security Metrics : Measuring security metrics is essential to determine how well an organization is protecting its assets and systems against cyber threats. Security metrics can include various measures, such as the number of security incidents, the number of successful attacks, and the time to detect and respond to cyber incidents.

3) Penetration Testing : Penetration testing, also known as ethical hacking, involves simulating a cyber attack to identify vulnerabilities and test the effectiveness of security controls. Penetration testing can help organizations identify potential security gaps and improve their overall security posture [36].

4) Employee Training : Human error is a significant factor in cybersecurity incidents. Therefore, measuring the effectiveness of employee training programs is essential to minimize the risk of human error. Regular training and awareness programs can help employees recognize potential threats and follow best practices to protect organizational assets and systems [36].

D. SCADA ATTACK DETECTION SOLUTIONS

1) Types of attacks : SCADA systems are susceptible to various types of attacks, including Denial of Service (DoS) attacks, ManintheMiddle (MitM) attacks, and more. Figure 6 depicts these different attacks along with their corresponding symbols which refer to the time line in figure 1.

Category 3

Category 2

Category 1

symbols	Attack	Type	Objectives
	DoS	Targeted	Availability
	Espionage	Targeted	Confidentiality
	MITM	Targeted	Confidentiality and Integrity
	System break-in	Targeted	Authentication and Authorization
	Virus	Untargeted	Integrity and Availability
	Warm	Untargeted	Authentication and Confidentiality
	Trojan	Untargeted	Confidentiality and Integrity
	Malware and phishing emails	Targeted	Integrity and Confidentiality

FIGURE 6 – Attack types in SCADA [18].

2) Methodology against Scada attacks :

— Conduct a Risk Assessment : Identify assets, vulnerabilities, threats, and potential consequences to understand the risk landscape [22].
— Develop a Security Strategy : Develop a comprehensive security strategy based on the results of the risk assessment. This strategy should consider people, processes, and technology.
— Implement Access Controls : Implement access controls to limit system access to authorized personnel only. This includes implementing strong authentication mechanisms and restricting access to critical systems.
— Implement Network Segmentation : Segment networks to reduce the attack surface and minimize the impact of an attack [22].
— Implement Security Monitoring : Implement security monitoring to detect and respond to attacks in real-time. This includes deploying intrusion detection and prevention systems, security information and event management (SIEM) systems, and other security monitoring tools [24].
— Implement Incident Response Procedures : Develop and implement incident response procedures to respond to security incidents in a timely and effective manner [24].
— Train Employees : Train employees on security best practices, including how to identify and respond to security incidents.
— Conduct Regular Security Assessments : Regularly assess the security posture of the SCADA system to identify vulnerabilities and areas for improvement.

VII. CONCLUSION :

SCADA systems are crucial to industrial applications such as power generation and distribution, telecommunications infrastructures, transportation, and manufacturing industries [18]. And since they are interconnected with the Internet, they face security threats that can disrupt their normal functioning.

the security breaches targeting SCADA systems pose a significant risk to critical infrastructure and various industries that depend on these systems for their day-to-day functioning.In parallel Cyber attacks continue to increase in fre-

quency, sophistication, and impact, and it is necessary to take proactive measures to protect against them.

The consequences of successful SCADA attacks can be catastrophic, including physical damage, financial losses, and even loss of life. Therefore, it is crucial to implement robust security measures and develop effective defense mechanisms to detect and prevent SCADA attacks. This includes conducting regular risk assessments, implementing access controls, employing intrusion detection systems, and ensuring the security of network infrastructure. It is also important to stay informed of emerging threats and continuously adapt security measures to stay ahead of attackers. By taking a proactive and comprehensive approach to SCADA security, organizations can mitigate the risks associated with these attacks and protect their critical systems and infrastructure.

RÉFÉRENCES

[1] El Mrabet, Z., Kaabouch, N., El Ghazi, H., El Ghazi, H. (2018). Cyber-security in smart grid : Survey and challenges. Computers Electrical Engineering, 67, 469-482.

[2] Gunduz, M. Z., Das, R. (2020). Cyber-security on smart grid : Threats and potential solutions. Computer networks, 169, 107094.

[3] Cherifi, T. (2019). Developpement dun protocole SCADA temps reel securise a base de lÍEC 60870-5-101 (Doctoral dissertation).

[4] Rai, A. K., Tewari, R. R., Upadhyay, S. K. (2010). Different types of attacks on integrated manet-internet communication. International Journal of Computer Science and Security, 4(3), 265-274.

[5] Ghosh, S., Sampalli, S. (2019). A survey of security in SCADA networks : Current issues and future challenges. IEEE Access,7, 135812-135831.

[6] Ahmed, M. R., Huang, X., Sharma, D. (2012). A taxonomy of internal attacks in wireless sensor network. Memory (Kbytes), 128, 48.

[7] El Mrabet, Z., Kaabouch, N., El Ghazi, H., El Ghazi, H. (2018). Cyber-security in smart grid : Survey and challenges. Computers & Electrical Engineering, 67, 469-482.

[8] Mahajan, V., Chowdhury, A., Padhy, N. P., & Lezama, F. (Eds.). (2022). Sustainable Technology and Advanced Computing in Electrical Engineering : Proceedings of ICSTACE 2021 (Vol. 939). Springer Nature.

[9] Rawat, D. B., & Bajracharya, C. (2015). Cyber security for smart grid systems : Status, challenges and perspectives. SoutheastCon 2015, 1-6.

[10] Nikander, J., Manninen, O., & Laajalahti, M. (2020). Requirements for cybersecurity in agricultural communication networks. Computers and electronics in agriculture, 179, 105776.

[11] Uma, M., & Padmavathi, G. (2013). A Survey on Various Cyber Attacks and their Classification. Int. J. Netw. Secur., 15(5), 390-396.

[12] http ://blog.tofte-it.dk/ethical-hacking-tools-for-the-5-phases-of-hacking/

[13] Kim, H. (2012). Security and vulnerability of SCADA systems over IP-based wireless sensor networks. International Journal of Distributed Sensor Networks, 8(11), 268478.

[14] Do, V. L. (2015). Sequential detection and isolation of cyber-physical attacks on SCADA systems (Doctoral dissertation, Troyes).

[15] https ://www.kaspersky.com/resource-center/definitions/what-is-social-engineering

[16] Kalluri, R., Mahendra, L., Kumar, R. S., & Prasad, G. G. (2016, December). Simulation and impact analysis of denial-of-service attacks on power SCADA. In 2016 national power systems conference (NPSC) (pp. 1-5). IEEE.

[17] Flaus, J. M. (2019). CybersÃ©curitÃ© des systÃ¨mes industriels. ISTE Group.

[18] Pliatsios, D., Sarigiannidis, P., Lagkas, T., & Sarigiannidis, A. G. (2020). A survey on SCADA systems : secure protocols, incidents, threats and tactics. IEEE Communications Surveys Tutorials, 22(3), 1942-1976.

[19] Hubbard, D. W., & Seiersen, R. (2023). How to measure anything in cybersecurity risk. John Wiley Sons.

[20] Hartmann, K.,& Steup, C. (2013, June). The vulnerability of UAVs to cyber attacks-An approach to the risk assessment. In 2013 5th international conference on cyber conflict (CYCON 2013) (pp. 1-23). IEEE.

[21] Hubbard, D. W., & Seiersen, R. (2023). How to measure anything in cybersecurity risk. John Wiley Sons.

[22] Khadidos, A. O., Manoharan, H., Selvarajan, S., Khadidos, A. O., Alyoubi, K. H., Yafoz, A. (2022). A classy multifacet clustering and fused optimization based classification methodologies for SCADA security. Energies, 15(10), 3624.

[23] Krutz, R. L. (2005). Securing SCADA systems. John Wiley Sons.

[24] Miller, B., Rowe, D. (2012, October). A survey SCADA of and critical infrastructure incidents. In Proceedings of the 1st Annual conference on Research in information technology (pp. 51-56).

[25] Slay, J., Miller, M. (2008). Lessons learned from the maroochy water breach (pp. 73-82). Springer US.

[26] Moore, D., Paxson, V., Savage, S., Shannon, C., Staniford, S., Weaver, N. (2003). Inside the slammer worm. IEEE Security Privacy, 1(4), 33-39.

[27] Swanson, L. (2010). The era of cyber warfare : Applying international humanitarian law to the 2008 Russian-Georgian cyber conflict. Loy. LA Int'l Comp. L. Rev., 32, 303.

[28] Kraszewski, K. (2019, May). SamSam and the silent battle of Atlanta. In 2019 11th international conference on cyber conflict (CyCon) (Vol. 900, pp. 1-16). IEEE.

[29] Izycki, E., Vianna, E. W. (2021, February). Critical infrastructure : A battlefield for cyber warfare ?. In ICCWS 2021 16th International Conference on Cyber Warfare and Security (p. 454). Academic Conferences Limited.

[30] Pillai, A., Saraswat, V., VR, A. (2019). Smart wallets on blockchainâattacks and their costs. In Smart City and Informatization : 7th International Conference, iSCI 2019, Guangzhou, China, November 12â15, 2019, Proceedings 7 (pp. 649-660). Springer Singapore.

[31] LeppÃ¤nen, S., Ahmed, S., Granqvist, R. (2019). Cyber Security Incident ReportâNorsk Hydro. Procedia Economics and Finance.

[32] Eggers, S. L. (2020). The nuclear digital IC system supply chain cyber-attack surface (No. INL/CON-20-57213-Rev000). Idaho National Lab.(INL), Idaho Falls, ID (United States).

[33] Nelson, T., & Kettani, H. (2020, March). Open source powershell-written post exploitation frameworks used by cyber espionage groups. In 2020 3rd International Conference on Information and Computer Technologies (ICICT) (pp. 451-456). IEEE.

[34] Greenberg, A. (2018). The untold story of NotPetya, the most devastating cyberattack in history. Wired, August, 22.

[35] Hunt, J. S. (2021). Countering cyber-enabled disinformation : implications for national security. Australian Journal of Defence and Strategic Studies, 3(1), 83-88.

[36] Sebastian, G. (2021). A descriptive study on cybersecurity challenges of working from home during COVID-19 pandemic and a proposed 8 step WFH cyber-attack mitigation plan. Communications of the IBIMA, 2, 2-7.

[37] Kilovaty, I. (2022). Cybersecuring the pipeline. Hous. L. Rev., 60, 605.

[38] Buchan, R. (2021). Eye on the Spy.

[39] Zhang, Z., Natarajan, S., Banerjee, A. Detecting Process Hijacking and Software Supply Chain Attacks Using IntelÂ® Threat Detection Technology.

[40] Zhang, X., Tsang, A., Yue, W. T., Chau, M. (2015). The classification of hackers by knowledge exchange behaviors. Information Systems Frontiers, 17, 1239-1251.

[41] Gandhi, F., Pansaniya, D., Naik, S. (2022). Ethical Hacking : Types of Hackers, Cyber Attacks and Security. International Research Journal of Innovations in Engineering and Technology, 6(1), 28.

[42] Taylor, P. A. (2005). From hackers to hacktivists : speed bumps on the global superhighway ?. New Media Society, 7(5), 625-646.

[43] Gupta, A., Anand, A. (2017). Ethical hacking and hacking attacks. Int. J. Eng. Comput. Sci, 6(6), 2319-7242.

[44] Imran, M., Faisal, M., Islam, N. (2019, November). Problems and Vulnerabilities of Ethical Hacking in Pakistan. In 2019 Second International Conference on Latest trends in Electrical Engineering and Computing Technologies (INTELLECT) (pp. 1-6). IEEE.

[45] Vishnuram, G., Tripathi, K., Tyagi, A. K. (2022, January). Ethical Hacking : Importance, Controversies and Scope in the Future. In 2022 International Conference on Computer Communication and Informatics (ICCCI) (pp. 01-06). IEEE.

[46] Hua, J., Bapna, S. (2012). How can we deter cyber terrorism ?. Information Security Journal : A Global Perspective, 21(2), 102-114.

[47] https ://www.cpacanada.ca/fr/ressources-en-comptabilite-et-en-affaires/domaines-connexes/technologies-et-gestion-de-linformation/publications/questions-administrateurs-cybersecurite

[48] https ://www.jstor.org/stable/resrep09462.7

[49] https ://link.springer.com/article/10.1186/s13705-019-0199-y