GU J Sci 30(4): 216-230 (2017)

Gazi University

Journal of Science

http://dergipark.gov.tr/gujs

Experimental Analysis of The Internal Attacks on Scada Systems

Erdal IRMAK*[1], İsmail ERKEK[2], Mert Melih ÖZÇELİK[3]

[1]*Faculty of Technology, Electrical and Electronics Engineering Department, Gazi University, 06500 Besevler/Ankara/Turkey*

[2]*Information Security Engineering Graduate Program, Gazi University, 06500 Besevler/Ankara/Turkey*

[3]*Information Systems Graduate Program, Gazi University, 06500 Besevler/Ankara/Turkey*

Article Info

Received: 13/03/2017
Accepted: 09/08/2017

Keywords

SCADA
PLC Security
Cyber-attack
Counter-measures
Internal attacks

Abstract

Supervisory control and data acquisition (SCADA) systems play an important role in electrical power systems, which is one of the most critical infrastructures. They usually include digital controllers like PLCs to realize the automation of electromechanical processes and to accomplish the real time services. Ensuring a secure communication between these field devices and the command center is vital from the security point of view. Because the most vulnerable part of SCADA systems is their communication protocols, this work focuses on the weaknesses of SCADA systems against the internal cyber-attacks such as Denial of Service (DoS), Man-in-the-Middle (MITM) and Replay. For this aim, a sample SCADA testbed environment has been designed at first and then the attacks mentioned above are tested on it. Experimental results show that although SCADA systems accomplish some mission critical tasks, the protocols used in their communication systems still lack of crucial security measures. Therefore, some immediate precautions to mitigate the vulnerabilities are suggested at the end of study.

1. INTRODUCTION

SCADA systems are used by government agencies and private industry organizations and corporations to communicate system issues, control and maintain productivity, distribute data for smarter decisions and help reduce downtime [1, 2]. They provide remote monitoring and controlling of information collected from the field to a central computer in such industries as power grid, oil and gas pipelines, utilities, communications systems, transportation systems, and banking and financial systems [3, 4], most of which are called as critical infrastructures. Thus, the purposes of SCADA systems can be classified as: (i) controlling the geographically dispersed assets, in most cases without the need for on-site personnel, (ii) gathering the data created by the field devices into a centralized database, (iii) carrying out any necessary analysis and then displaying that information on a number of operator screens or displays in real time.

A SCADA control center, based on information received from remote stations, can push automated or operator-driven supervisory commands to remote station control devices, which are often referred to field devices. Field devices are deployed in geographically distributed manner and they transfer the real-time information to the central station using LAN/WAN links [5]. In order to transfer the messages between the control center and field devices safely, the communication protocols used for this aim should be selected carefully.

In order to control the geographically distributed systems, often located over thousands of square kilometers, many protocols are used in SCADA systems today such as Modbus, DNP3, ICCP, UCA 2.0 etc., most of which lack of crucial security features. When these protocols were initially created, they were thought to serve specific local tasks without a connection with the outside world. However, SCADA systems need to communicate with external systems day by day as a result of the rapid advancement on

* Erdal IRMAK, e-mail: erdal@gazi.edu.tr

Internet technology [6]. Nowadays, the critical-infrastructures that control many aspects of people's daily lives are in the wild without any built-in security features. Many researchers, like [7], have investigated Shodan search engine [8, 9] to map SCADA systems directly connected to the Internet and find out the critical infrastructure vulnerabilities. It is evident that the number of "unprotected" devices attached to Internet is on the rise.

Considering such issues mentioned above, a testbed representing a simple SCADA system based on a PLC device is designed in this paper in order to show how easily an insider can exploit the vulnerable protocols which are designed without any security consideration. Then, it is shown that performing cyber-attacks such as Denial of Service (DoS), Man-in-the-Middle (MITM) and Replay is much easier than it might be thought. The aims and the motivation of the study can be outlined as following: first, to demonstrate how internal cyber-attacks can be devastating. Second, to raise questions about trustworthiness of SCADA systems and finally to improve the situational awareness about the SCADA system protocols.

The remain of this paper is organized as follows; section II reviews the related works and provides a literature survey about attacks on SCADA systems and summarizes studies trying to mitigate vulnerabilities in communication protocols. Section III explains the designed testbed and its hardware/software components in detail. Section IV explains the technical details about the cyber-attacks performed on the testbed. Finally, section VI concludes the paper and presents some counter measures.

2. RELATED WORKS

Although the security issues of SCADA systems have not been studied adequately in recent literature, there are some valuable studies that reveal the vulnerabilities in their communication protocols. Some of these studies are summarized below.

In [10 and 11], the authors managed to capture clear-text data that were sent to the PLC using "Wireshark" due to the usage of unencrypted protocol during the data exchange. This information was used by authors to perform replay attacks against the FINS (Factory Interface Network Service) protocol that is used by Omron PLCs, over different physical networks like Ethernet, Controller Link, DeviceNet and RS-232C.

In [12], the author demonstrated that ISO-TSAP and Profinet protocols, which are widely used for communication of Siemens PLCs, could be exploited easily by using TCP dump. He also showed that an attacker could obtain passwords because they were sent in an unencrypted way. Additionally, he presented that replay and MITM attacks could be performed by using gathered information and, most significantly, PLCs could be re-programmed, turned on or off, their authentication process could be bypassed, passwords could be changed or completely deleted and read-write operations on the memory could be performed with these attacks. The vulnerabilities of Modbus protocol used for communication of energy automation systems were investigated in [13] and an open source firewall to eliminate detected vulnerabilities were suggested to make the system more secure.

As an example of possible DoS attacks, TCP SYN flood attacks on the systems used to control the energy systems were investigated in [14]. The aim of these attacks was to disrupt the normal operation of the smart meter so that the power consumption would be transported to the center with a delay. This delay caused SCADA system operator to make wrong decisions. The experiments showed that impact of DoS attacks against SCADA systems could be devastating. In [15], a simulation environment for chemical plant was created and DDoS attacks were performed. With these attacks, target system was forced to deal with a huge number of request packets and the system couldn't be able to carry normal traffic, finally the system was down. In order to fight against DDoS attacks, the importance of risk assessment was investigated and it concluded that all devices on the network should be evaluated thoroughly, time and resource consuming functions should be determined and the network should be tested by creating a testbed environment with simulation of real DDoS attacks.

The authors of [16] reported that Linux based operating systems could be more secure against the DDoS attacks when compared to other operating systems. Resource allocation of Linux based operating systems was put forward as a reason to support their assertions. Since Linux based operating systems allocate resources only when client receives the ACK command and SYN cookies are used after receiving the first SYN packet instead of reserving source for connections, they proposed to use Linux based operating system in SCADA systems.

In [17], an assessment of SCADA vulnerabilities to DDOS attacks was presented. The main reasons behind the successful hacking events against industrial control centers were specified as follows: Connecting the control systems to other networks, not trying to eliminate known vulnerabilities using standard technologies, restrictions on the existing security technologies and applications, insecure remote connections, accessibility to technical information of control systems from everyone. In addition, unprecedented number of vulnerabilities in SCADA systems were mentioned in the study, and it was stated that preventing DDoS attacks completely was near to impossible. The authors warned the readers to keep in mind that DDoS attacks could damage many critical systems and these attacks would cause serious performance economic losses.

The authors of [18] created a hybrid testbed environment consisting of SCADA devices, an attacker and network based intrusion detection system. By performing ARP poisoning attack that exploits the weaknesses in the design of ARP protocol, they managed to enter between SCADA control server and PLC. Meanwhile, the attacker captured the packets flowing between the two devices and made changes on these packets.

Another successful MITM attack against SCADA systems was described in [19] using the technique called ARP poisoning against DNP3 protocol. The works [18 and 19] clearly showed how easy to perform MITM attacks so long as having access to internal network because of inherent weaknesses in protocols.

In order to mitigate the effect of MITM attacks on SCADA systems, an encryption method was proposed in [20] that aimed to prevent the ARP poisoning. The method of Ticket-based ARP (TARP) was the suggested approach in which servers such as Secure Key Distribution Center could solve the problems in certain points for Secure ARP (S-ARP) and Local Ticket Agent (LTA). However, it was put forward that this solution was not sufficient for wireless communication.

Another effort to prevent the process of MAC address spoofing, ARP Spoof and MITM was introduced in [21] as a design of "architecture and protocols" for the LAN security. The work concentrated on the installation of DHCP servers that used as MAC-IP database center to protect against MITM attack. A new DHCP was recommended to perform the transmission of MAC address between each user. However, replacing the widely used DHCP is almost impossible in practice.

The authentication process during the exchange of MAC addresses between the nodes was claimed as a primary reason for successful ARP poisoning attacks and therefore a model based on AES and RSA encryption techniques was proposed in [22]. The proposed model was based on a defense mechanism that did not require neither changes on the network protocol nor usage of expensive equipment. Additionally, the system automatically renewed the reliable MAC address information to the ARP table as a static type to protect users from ARP spoofing. However, in this protection method, the client side was protected but the gateway was not fully protected and the system still remained vulnerable against ARP poisoning attacks.

In another effort to prevent MITM attacks, the notion of SSL/TLS session-aware user authentication was introduced, and presented different possibilities for implementing it [23]. The aim of the model was to drop the malicious users by recognizing with the help of the server. Clients should be protected from malicious software in the use of UAC (user authentication code). Otherwise, the user's PIN could be captured with malicious software such as Trojans and the system could become vulnerable to attacks.

All studies above show that SCADA systems have some crucial vulnerabilities against the cyber-attacks and more studies should be made on this topic. As a result of this motivation, this study is focused on the security of SCADA systems considering up to date threats for them.

3. RISK, VULNERABILITIES, THREATS, IMPACT AND SECURITY MEASURES

In this section, just before delving into the details of the experiment about the security of PLC protocols and their weaknesses, some important notions and the relationship among them are investigated.

Although it is very easy to find many risk definitions in the literature, Eq.1 is an ideal model to demonstrate the relationship between risk, vulnerabilities, threats, impact and security measures [24]. Before discussing the equation, the terms included in the formula are explained in detail below.

$$\text{Risk} = \frac{\text{Vulnerabilities x Threats x Impact}}{\text{Security Measures (Controls)}} \tag{1}$$

3.1. Vulnerability

According to NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE), a cyber-vulnerability is a "property of a cyber-entity that is susceptible to exploitation" [25]. It is also any kind of security flaws or weaknesses that can be exploited by attackers. That is why those weaknesses should be "patched" or "fixed" before they are used maliciously. The identification of vulnerabilities and the possibilities of reducing those vulnerabilities are vital to mitigate risks involving in cyber domain.

A vulnerability requires three elements: a weakness, an attacker's access to the weakness, and the attacker's ability to exploit the weakness using a tool or technique. Attackers constantly try to figure out those weaknesses before defending side strengthen the weaknesses. This paves a competition between bad and good people. In order to be ahead of bad people a systematic approach, which is dubbed as "Vulnerability Management", should be implemented, and, if successfully implemented, it can be invaluable by providing those benefits.

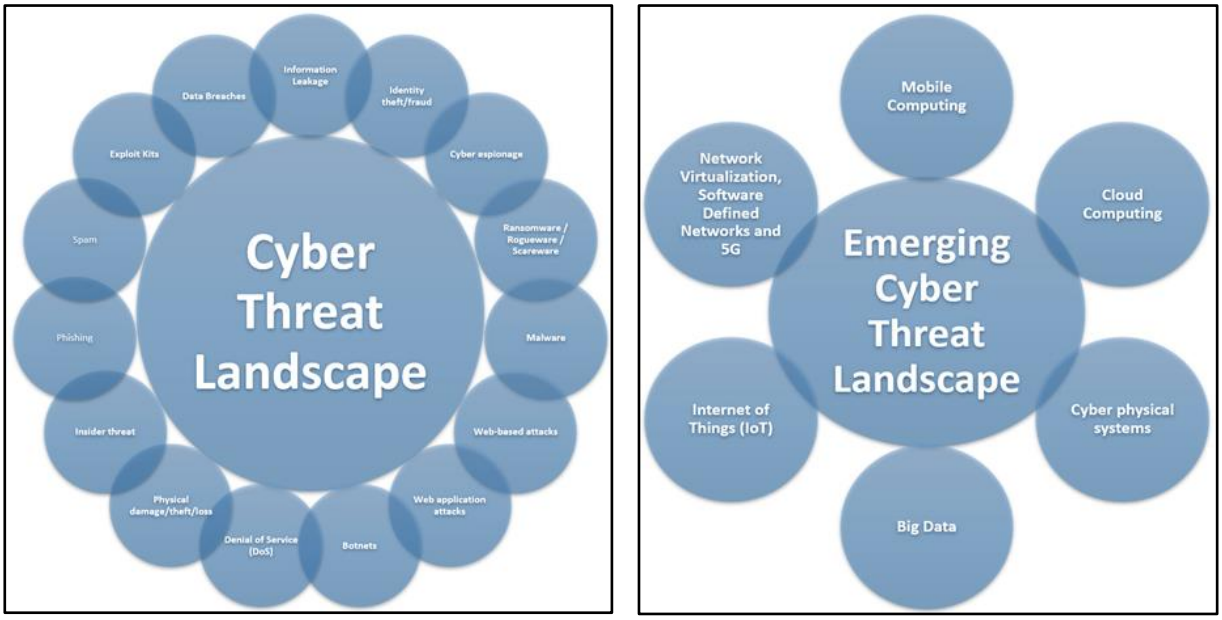
Firstly, vulnerability management can ease organizations' burden of compliance by helping to reduce risk levels, to perform due diligence, to provide forensic data and to generate reports that can be used as technology metrics.

Secondly, organizations' security posture can be improved significantly, which means that performing vulnerability management will be adding yet another layer to the defense in depth. Finally, it can help position the organization for a safer, more secure computing environment.

3.2. Threat

Threat is an important concept used in both risk management and risk assessment. It can be defined as "any circumstance or event with the potential to adversely impact organizational operations and assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service" [26]. Some of the current threat landscape was mentioned in [27] as seen in Fig. 1 (a).

It should be kept in mind that cyber threats are not static, they evolve continually. For this reason, organizations, security policies and procedures should be flexible to counter those dynamic threats. Some emerging threats mentioned in [27] are given in Fig. 1 (b).



(a) (b)

Figure 1. *a) Cyber threat landscape (2015), b) emerging cyber threat landscape (2015)*

3.3. Impact

Cyber-attacks can cause significant loss of business intelligence and intellectual property, drive up the cost of security, disrupt workflow, and damage reputation. Since the dependency on information technology of each organization is different, impact of cyber-attacks can vary among them. For instance, successful cyber-attacks on an international bank providing online banking for its users can cause much more damages than attacks on a local grocery market that provides its users to order online. That's why possible impacts of cyber-attacks should be considered while a risk assessment is being made.

3.4. Security Measure (Control)

Security controls are safeguards or countermeasures to avoid, to detect, to counteract, or to minimize the security risks for physical properties, information systems, computer systems, or similar assets. Controls help to reduce the risk of damage by stopping, deterring, or slowing down an attack against an asset. Information security controls protect the confidentiality, integrity, availability of information as well as non-repudiation and accountability [28].

While the security practitioners cannot usually control the other terms in Eq.1, they perform security controls intentionally in order to mitigate risks. From the mathematical perspective, if the denominator of a fraction increases, the value will be lower. In order to demonstrate that security controls are the only means used to mitigate the risks involved in cyber domain, it is in the denominator of equation.

3.5. Risk

As it is stated clearly in [26], risk is "a measure of the extent to which an entity is threatened by a potential circumstance or event, and is typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence." The key point of risk is to determine the areas where the organization can suffer from loss. Once these areas have been determined, the appropriate countermeasures or controls should be put into place in order to prevent these areas from being completely destroyed. From the security point of view, loss of confidentiality, integrity, or availability of information or information systems can cause a huge business impact on an organization. Therefore, every organization wants to minimize the risks and maximize the profits in order to provide the sustainability.

In conclusion, making a rigorous risk assessment plays a vital role for minimizing risks. As it can be understood from Eq. 1, the risk evaluation requires the careful analysis on the threat and the vulnerability information to figure out the extent to which events could adversely affect an organization and the possibility of the occurrence of such events. After carrying out a careful risk assessment, required counter measures could be determined to mitigate the risk.

4. SCADA COMPONENTS

As shown in Fig. 2, a SCADA system generally consists of master terminal units (MTU) or master stations, remote terminal units (RTU) or remote stations, communication networks, data collection units, sensors, SCADA system terminals, computer monitors, printers and uninterruptible power supplies. Thanks to the system, it is possible to control and monitor all units of a facility or operation such as production planning, environmental control units and auxiliary operations. The MTU allows administrators to monitor visually the operating operators, maintenance equipment and the entire operating system in real-time. Unlike the central computer at the MTU, there are computer terminals, computer screens and printers. MTU is a form of connecting to a server or a group of computers with a main server with a local network (LAN) or a wide area network. HMI (Human-Machine Interface) software is installed in MTU or control center to add visualization of information collecting from field devices. It provides a graphical interface environment for the SCADA components to communicate with the operator. Assignments of MTU are as follows: (i) collecting data coming from RTU, (ii) collected data is processed by software programs and sent to the monitor or printer, (iii) sending the control commands to the devices to be controlled in the system, (iv) generating alarms in response to certain events and deliver the alarms to the operator, (v) running high level application programs such as deployment management system or energy management system.

RTU is a SCADA hardware unit that collects, stores and sends information about the center of the system to the control center via a specific communication medium if necessary, and receives commands from the control center. At the same time, RTUs are the units that carry out the measurement and supervision operations. RTU devices are deployed in many geographically diverse locations and distribute the real-time information to the central station using LAN / WAN links [30].

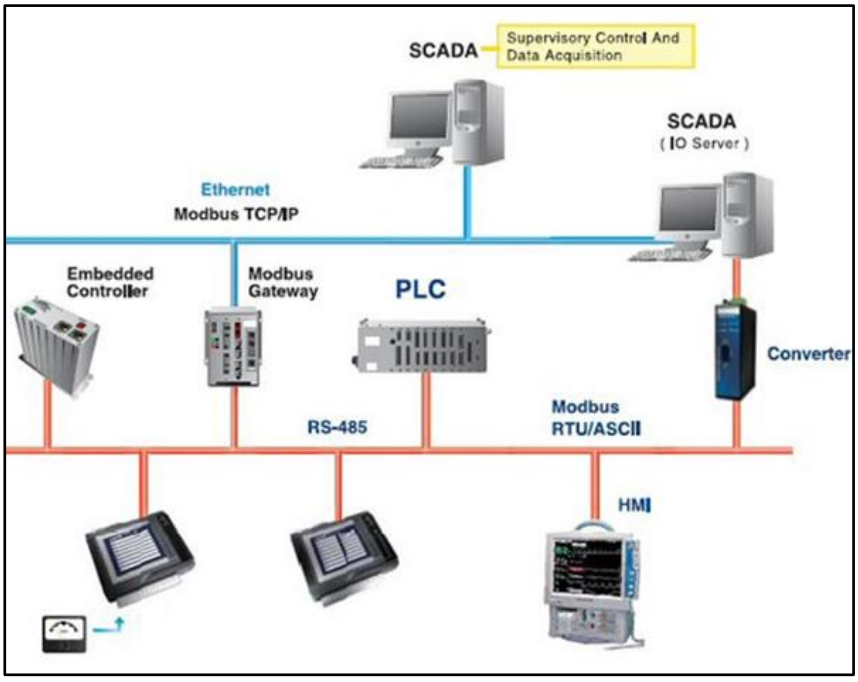


Figure 2. *A typical network topology of SCADA systems [29]*

With the development of new communication technologies and the acceleration of communication channels, older systems have left their place to them. Therefore, all the processing power takes place over

SCADA networks in order to speed up communication channels and make RTU units smarter. With the development of Intelligent Electronic Devices (IED), the RTU has begun to have more intelligent processing power. IEDs have the ability to run simple logic processes independently that do not require a server. Thus, RTU devices allow many functional operations to be performed such as system protection, local processing capacity, and data collection from subsystems [31].

The idea of developing intelligent field devices that can accomplish tasks similar to those which are achieved in MTU brings about some security problems. From the security point of view, adding new features to the systems without considering security might cause intrusions and a great amount of damage could be inevitable. That is why security problems of those intelligent devices that interact with physical world should be addressed.

5. EXPERIMENTAL STUDY

In this section, three types of internal attacks such as Replay, Denial of Service and MITM are discussed by demonstrating those on a testbed environment. The success of attacks stems from the inherent weaknesses of PROFINET (Process Field Net) protocol. PROFINET protocol is the Industrial Ethernet Standard developed by PROFIBUS International for "Ethernet on the plant floor" [32].

The testbed environment designed in the study represents a simple SCADA system. The testbed environment consists of a Siemens S7-1200 PLC device, a controller PC and an attacker PC. Although the PLC device from a specific vendor is used in the system, it can be easily extended to cover equipment from other vendors.

As illustrated in Fig. 3, all the testbed components are connected via Ethernet using a switch. Open source exploit modules have been installed to attacker's Kali Linux computer so as to exploit communication between the PLC and the controller. Monitoring of the PLC device has been carried out by TIA Portal V13 editor. A basic input/output network has been designed as shown in Fig. 4.

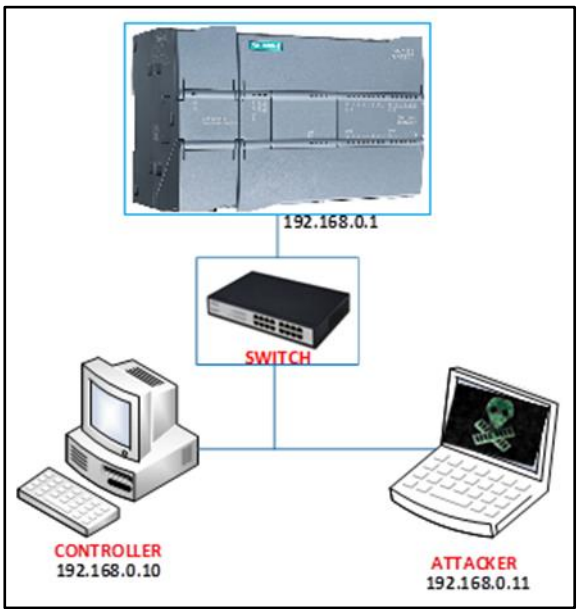


Figure 3. *Testbed environment and its components*

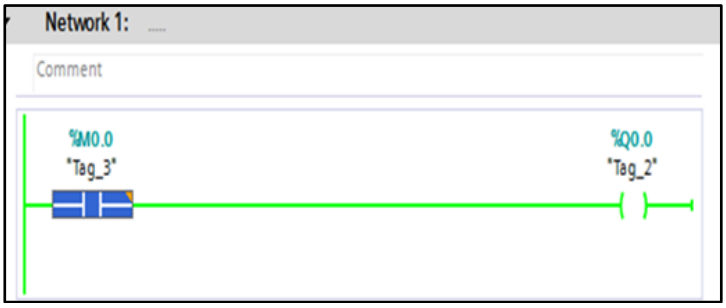


Figure 4. *Basic input/output network of PLC*

Unfortunately, PROFINET was designed without security considerations initially. It was designed to create a truly open and ubiquitous interconnected environment between industrial automation and common networking standards and protocols. The idea was to facilitate the management of hundreds or thousands of PLC devices distributed throughout an industrial environment by a single person (or small team) via a centralized management system [12]. The PLC device that was used in the work also use PROFINET [33] and Wireshark supports PROFINET recording [34] that permits the analysis of the Ethernet message frames. This allows attackers to record packets going to and from the engineering workstation to the PLC, and makes the PLCs a prime target for attackers who are able to reverse the protocol and craft their own packets based on the traffic moving across an automation network. Additionally, technical information about the PLC device that was used in the work can be accessed in the "SIMATIC Step 7 Engineering Software Application" [35], a skillful attacker can easily make use of the information provided by the vendor.

The details of each attack performed in the study are explained below.

5.1 Replay Attack

In the reconnaissance phase, a network scan by using nmap tool has been performed and it showed that port 102 in PLC device was open and ISO-TSAP protocol was running on it. Additionally, MAC address and brand name of the PLC device were obtained easily. Upon completing nmap scans, all traffics between the PLC and the controller have been captured by Wireshark running on the attacker's computer. Thanks to the designed testbed, the entire content of the communication between these systems could be monitored as shown in Fig. 5.

Since a replay attack, illustrated in Fig. 6, means that valid data transmission is maliciously or fraudulently repeated or delayed by an adversary who intercepts the data and retransmits it, analysis of ISO-TSAP packets was needed to be done correctly. In order to create authenticated packets from attacker's computer to PLC, an open source metasploit module, which was developed in [12], has been used. Thanks to this metasploit module, the attempts to perform replay attack has been succeeded easily. Because it have the ability to remove the memory protection independently from the Step 7 TIA, it is possible to save the packages returned to the controller and then send them again to disable the protection secretly. Authenticated packets can then be captured or installed by the attacker to be combined with the attacker's own session or controller.

After performing the attack, changes in the TIA Portal editor running on the control computer is demonstrated in Fig. 7. As seen, it has been possible to make some changes in an unauthorized way such as disconnecting the link and open/close operations.

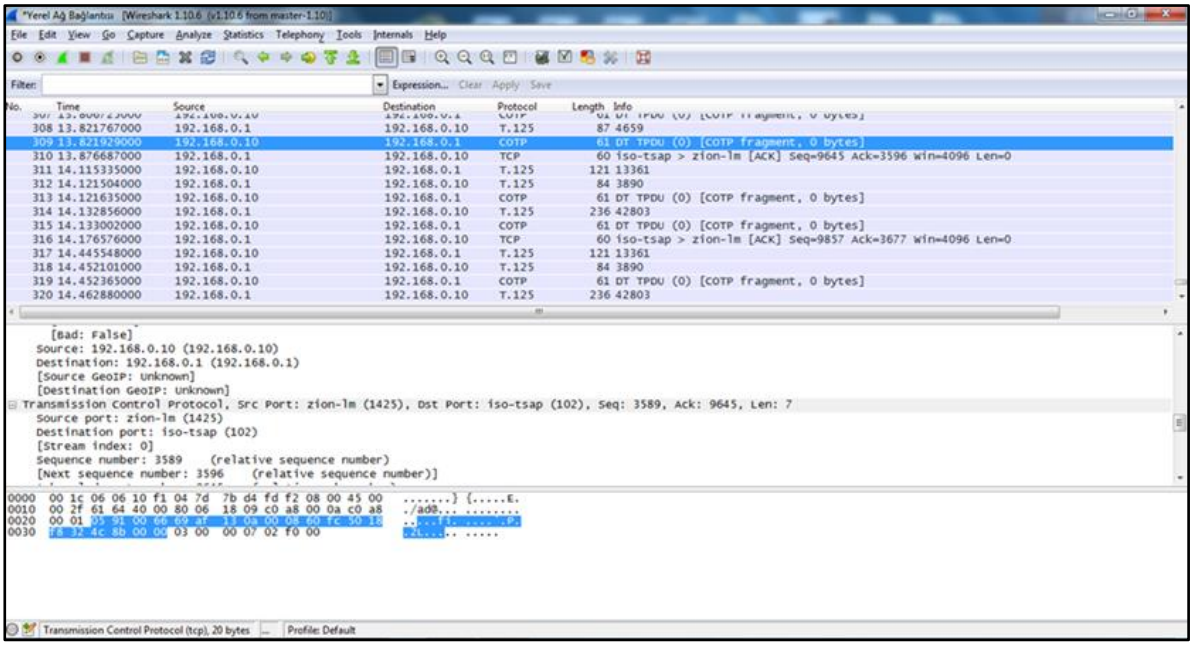


Figure 5. *Captured packets with Wireshark in attacker's computer*

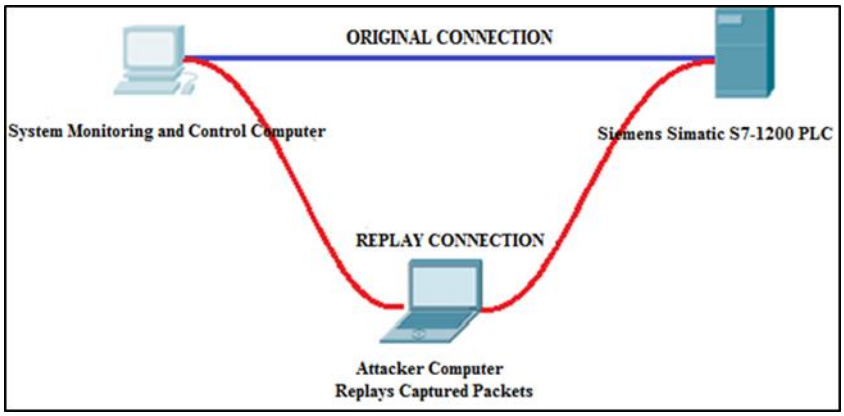


Figure 6. *Replay attack*

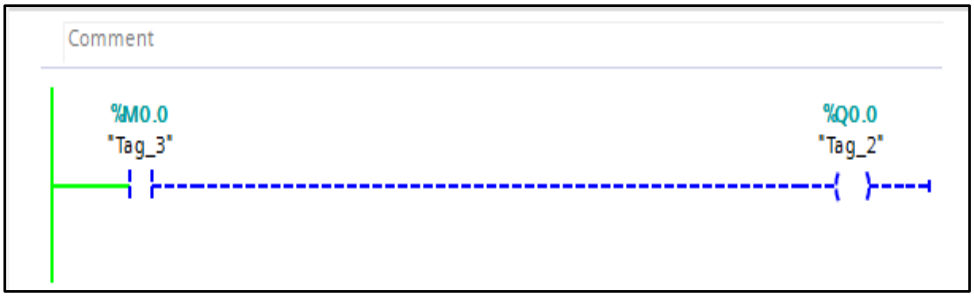


Figure 7. *TIA portal after the replay attack*

5.2. Denial of Service (DoS) Attack

As the second experimental test in the study, the impact of DoS attacks on PLC has been investigated by using TCP SYN Flood, which is a form of DoS attack. This technique exploits the TCP 3-way handshake procedure in order to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host. In TCP 3-way handshake procedure, client sends a SYN message to the server to establish a TCP connection. The server sends SYN-ACK message as a response to the client to verify the connection. Finally, client provides the connection successfully and completes the triple handshake by sending back ACK message. After those steps, data

transfer begins. However, attackers send a succession of SYN requests to a target's system in an attempt to consume server resources to make the system unresponsive to legitimate traffic. The hping3 tool on the attacker's computer has been used to successfully perform this attack.

In the experiment performed during the tests, attacker's computer tried to send some packets to disrupt the PLC as shown in Fig. 8. In order to observe the impact of DoS attack, Wireshark program has been installed in controller. After starting TCP SYN flood attack, it has been observed that the controller could not respond legitimate packets.

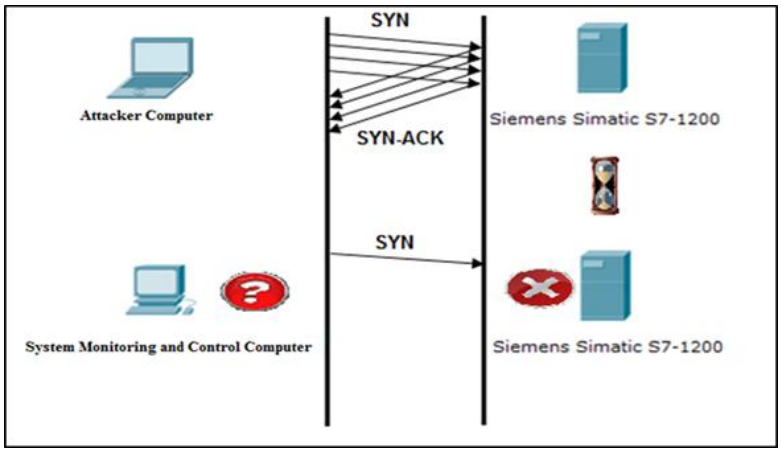


Figure 8. *SYN flood attack*

As shown in Fig. 9, the attack carries out until 45th second and then stops. After 80th second, the attack is restarted. The traffic in the controller's Ethernet port is getting higher immediately after the attack started. Once the attack is started, it is impossible to control the system.

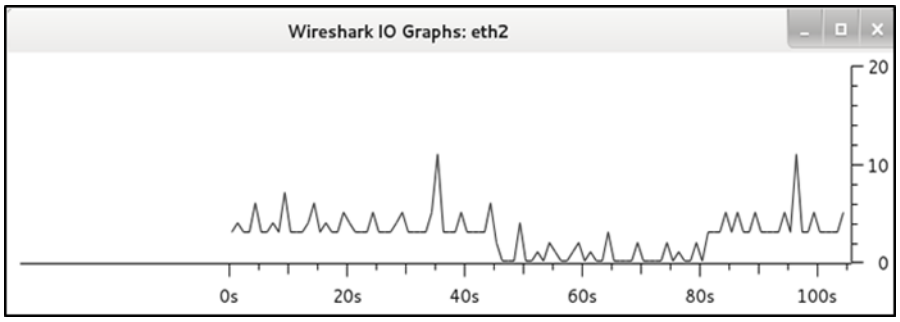


Figure 9. *I/O graphic during TCP SYN flood*

5.3 Man-in-The-Middle (MiTM) Attack

MITM attack is the capture of data flowing between victim machines and a router on a network by intruding between machines. As shown in Fig. 10, system monitoring and control computer supposes it is communicating with Siemens Simatic S7-1200 PLC device, in actual fact the communication flows through the attacker machine. In this attack, the attacker replaces the mac address of the router with its MAC address by sending ARP packets to the victim computer. Likewise, the attacker tells the router that the victim's mac address has changed and the new mac address is his mac address now, so the attacker intrudes between the victim and router machine.

In reality, MITM attacks can be performed in different ways including ARP cache poisoning, DNS spoofing, HTTP session hijacking, passing the hash, and more. In the third experimental test performed in this study, ARP cache poisoning technique has been used for two reasons. First, ARP cache poisoning requires to be an internal attacker that complies with the main purpose of this study which can be outlined as investigating the impact of internal attacks. Second, it has been aimed to improve internal attack

awareness since the security efforts have usually focused on the network perimeter by the security practitioners.

ARP cache poisoning exploits the insecure nature of the ARP protocol. Differently from protocols such as DNS, which can be configured to only accept secure dynamic updates, ARP-enabled devices will accept updates at any time. Thus, any device can send an ARP reply packet to another host and can force to update the ARP cache using the new value of the host. If attackers create a large number of well-prepared ARP packets, they could easily deceive their victims with a host computer, but in fact they would be in communicating with a listening attacker.

In order to accomplish ARP cache poisoning, ettercap [36] program has been installed on attacker's Kali Linux machine that is used to poison the controller's ARP table. Then Wireshark has been used to monitor the traffic between the controller and PLC. As clearly seen from Fig. 11, all traffic also flows through the attacker, but so as to proof the attack, ARP table of controller is checked after the attack started.

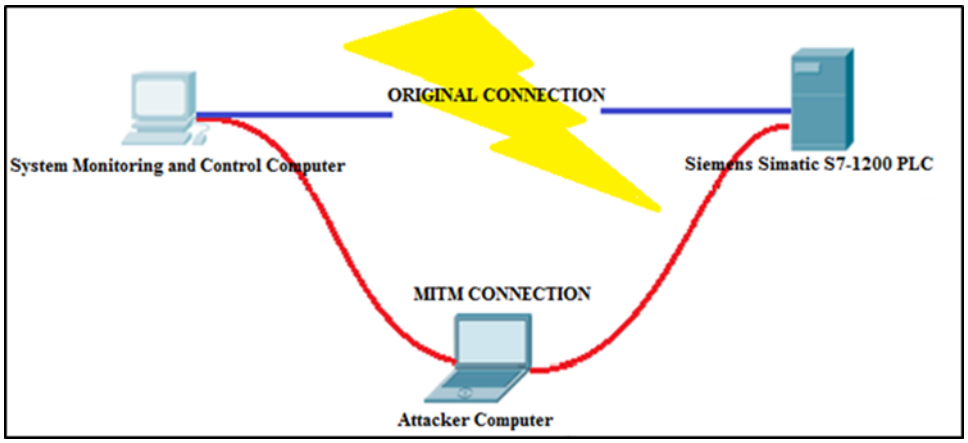


Figure 10. *MITM attack*

```
Interface: 192.168.0.10 --- 0x29
  Internet Address      Physical Address      Type
  192.168.0.1           08-00-27-11-cf-c9     dynamic
  192.168.0.11          08-00-27-11-cf-c9     dynamic
```

Figure 11. *Controller's ARP table after poisoning*

6. CONCLUSION

In this study, a typical SCADA system, which includes a control computer and a PLC widely used in SCADA networks, has been created. The communication between the PLC and the control computer has been analyzed. Replay, MITM and DoS attacks against the system have been performed and the impact of those attacks has been investigated.

The results obtained are remarkable for the following reasons; first, although the PROFINET protocol has provided great advantages for industrial networks such as reliability and real-time communication, it transfers the messages into a plain text. It has no inherent security functions in the sense of endpoint security. There might be several reasons why some automation systems currently do not have their own autonomous security functions. For instance, some automation systems may not have the technical resources necessary for security functions. However, as it is clear from Stuxnet virus technical explanation [37], protocols and devices that control physical entities without security features are a prime target for cyber physical weapons. Secondly, the assumption that security is unnecessary as long as the industrial control system is deployed inside a local network which has no internet connection has to change. The recent cyber events have made it obvious that "security by obscurity" is not a good choice

and this notion does not provide adequate security. That is why the assumption must be left as soon as possible.

• The threats against the industrial control systems and vulnerabilities on those are real, and these devices control a huge part of critical infrastructures. That is why risks to be exploited are very high, the attacks are imminent and precautions should be taken immediately by deploying security measures. After the experiences obtained in this study, those are the recommendations for enhancing the industrial systems' security posture, which will help to reduce the risk of exposing cyber-attacks.

• The need for secure protocols in industrial control systems is urgent; the product vendors have the ability to make this a reality.

• The assumption of "security by obscurity" should be left as soon as possible.

• Perimeter security is not enough to feel secure.

• Tamper protection might be used in high critical systems.

• Most of critical infrastructures are controlled by SCADA systems and these systems operate in real-time. The slightest variations in these systems can cause serious financial losses, collapse of public order moreover national security threat. Therefore, penetration tests on these systems should be made before system deployment.

• Cyber security issues should be kept in mind from the starting point. Since it is hard to make the system secure once it is manufactured without any security concerns.

• A holistic approach, which is called "defense-in-depth", should be deployed.

• "Situational awareness" should be increased by making careful inventory checks. Because unmanaged or forgotten single device can be enough for attackers.

• "Continuous network monitoring" should be done to understand any abnormal activities in the environment.

• "Forensic Readiness" is needed before any events happen to figure out root causes of both accomplished and imminent attacks.

• An effective "Incident Handling Management System" will deter the attackers.

Some specific security recommendations for enhancing the PLC security are listed below:

• Limit the connections of PLC with the Internet and other networks.

• Provide appropriate physical access security to systems and locations.

• Use encryption schemes as much as possible.

• Create built-in functionality for user authentication and assigning permissions to users.

• Log user actions to a database.

• Find a way to be notified of security updates.

• Verify that any upgrades, new tools or functionality added to the system come from a correct source and have not been tampered with or corrupted.

• Implement a password policy minimally includes: complexity of passwords, change frequency, change of default accounts and passwords, including a guarantee for deleting such accounts, requirements regarding administrator accounts.

• Deploy a policy for the use of (removable) media (such as USB sticks, hard disks and CD-ROMs) and implement technical measures to enforce this policy.

• Implement the principle of least privileges.

• Harden system by switching off superfluous functions and unused services, deleting non-used or unnecessary user accounts and change default passwords.

• Document system changes and configurations.

• Define a patch policy and remain informed about vulnerabilities, security patches and workarounds of all your system components.

• Define a policy for connecting mobile equipment, such as laptops, tablets, and smartphones.

• Make use of an Intrusion Detection System (IDS) for detecting attacks.

CONFLICTS OF INTEREST

No conflict of interest was declared by the authors.

REFERENCES

[1] C. Yulia, et al. "A review of cyber security risk assessment methods for SCADA systems." Computers & Security, 1-27, (2016)

[2] G. Niv, and A. Wool, "Accurate modeling of Modbus/TCP for intrusion detection in SCADA systems." International Journal of Critical Infrastructure Protection, 63-75, (2013).

[3] O. Hamed, et al. "Creating a cyber moving target for critical infrastructure applications using platform diversity." International Journal of Critical Infrastructure Protection, 30-39, (2012).

[4] C. Queiroz, A. Mahmood, J. Hu, Z. Tari, and X. Yu, "Building a SCADA Security Testbed," Third International Conferance Network and System Security, 357–364, (2009).

[5] NIST SP 800-82, "Guide to Industrial Control Systems (ICS) Security", (2011).

[6] G. Devarajan, "Unraveling SCADA Protocols:Using Sulley Fuzzer", Defcon (2015).

[7] Kiravuo, T. Tiilikainen, S. Sarela, M. and Manner, J. "Peeking Under the Skirts of a Nation: Finding ICS Vulnerabilities in the Critical Digital Infrastructure", Proceedings Of The 14th European Conference On Cyber Warfare And Security (Eccws-2015), 137-144, 2015.

[8] Internet: "Shodan", https://www.shodan.io/, Access Date: 21.12.2016.

[9] R. C. Bodenheim, "Impact of the Shodan computer search engine on internet-facing industrial control system devices", AFIT-ENG-14-M-14. Air Force Institute of Technology Wright-Patterson AFB OH Graduate School Of Engineering And Management, (2014).

[10] N. Sayegh, A. Chehab, I. H. Elhajj, and A. Kayssi, "Internal security attacks on SCADA systems," Third International Conference on Communications and Information Technology, ICCIT, 22–27, (2013).

[11] Internet: "Omron FINS Ethernet Driver Help", https://www.kepware.com/en-us/products/kepserverex/drivers/omron-fins-ethernet/documents/configuring-an-omron-plc-with-omron-fins-ethernet/, Access Date: 23.12.2016.

[12] D. Beresford, "Exploiting Siemens Simatic S7 PLCs," Black Hat USA, 1–26, (2011).

[13] R. Bayindir, S. Sagiroglu, A. Ozbilen, and I. Colak, "Investigating Industrial Risks Based On Informatıon Security For Observerable Electrical Energy Distribution System And Suggestions," Journal of The Faculty of Engineering and Architecture of Gazi University, (24)4, 715–723, (2009).

[14] C. Queiroz, A. Mahmood, and Z. Tari, "SCADASim-A Framework for Building SCADA Simulations," IEEE Transactions on Smart Grid, (2)4, 589–597, (2011).

[15] R. Chabukswar, B. Sinópoli, G. Karsai, A. Giani, H. Neema, and A. Davis, "Simulation of Network Attacks on SCADA Systems," First Workshop on Secure Control Systems, (2010).

[16] N. Kakanakov and G. Spasov, "Securing against Denial of Service attacks in remote energy management systems," Annual Jornal of Electronics, (2011).

[17] J. D. Markovic-Petrovic and M. D. Stojanovic, "Analysis of SCADA system vulnerabilities to DDoS attacks," 11th International Conference on Telecommunications in Modern Satellite, Cable and Broadcasting Services (TELSIKS) , 591–594, (2013).

[18] E. Ciancamerla, B. Fresilli, M. Minichino, T. Patriarca, and S. Iassinovski, "An electrical grid and its SCADA under cyber attacks: Modelling versus a Hybrid Test Bed," International Carnahan Conference on Security Technology (ICCST), 1–6, (2014).

[19] D. Lee, H. Kim, K. Kim, and P.D. Yoo, "Simulated Attack on DNP3 Protocol in SCADA System," Proceedings of the 31th Symposium on Cryptography and Information Security, Japan, (2014).

[20] W. Lootah, W. Enck, and P. McDaniel, "TARP: ticket-based address resolution protocol," 21st Annual Computer Security Applications Conference, 106–116, (2005).

[21] D. Pansa and T. Chomsiri, "Architecture and Protocols for Secure LAN by Using a Software-Level Certificate and Cancellation of ARP Protocol," Third International Conference on Convergence and Hybrid Information Technology, 21–26, (2008).

[22] S. Hong, M. Oh, and S. Lee, "Design and implementation of an efficient defense mechanism against ARP spoofing attacks using AES and RSA," Elsevier Science Direct, Mathematical and Computer Modelling, (58)1–2, 254–260, (2013).

[23] R. Oppliger, R. Hauser, and D. Basin, "SSL/TLS Session-Aware User Authentication—Or How to Effectively Thwart the Man-in-the-Middle," Computer Communications, (29)12, 2238–2246, (2006).

[24] Q. Chen, K. R. Abercrombie, and F. T. Sheldon. "Risk assessment for industrial control systems quantifying availability using mean failure cost (MFC)", Journal of Artificial Intelligence and Soft Computing Research, 205-220, (2015).

[25] NATO Cooperative Cyber Defence Centre of Excellence, 2016, https://ccdcoe.org/about-us.html.

[26] NIST SP 800-30 v.1 "Guide for Conducting Risk Assessments", (2012).

[27] Internet: European Union Agency for Network and Information Security (ENISA), "ENISA Threat Landscape 2015", https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/etl, Access Date: 29.12.2016.

[28] NIST SP 800-53A Revision 4. "Assessing Security and Privacy Controls in Federal Information Systems and Organizations", (2014).

[29] Internet: "PLC & Scada Workshop", https://www.robosapi.com/plc-scada#supertab15, Access Date: 29.12.2016.

[30] F. Daryabar, A. Dehghantanha, N. I. Udzir, N. F. B. Mohd Sani, and S. Bin Shamsuddin, "Towards secure model for SCADA systems," Proceedings 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic, CyberSec 2012, 60–64, (2012).

[31] Z. J. Zhang, et al., "A survey of SCADA test bed.", International Journal of Wireless and Mobile Computing, 9-14, (2015).

[32] M. Antolovic, K. Acton, N. Kalappa, S. Mantri, J. Parrott, J. Luntz, J. Moyne and D. Tilbury. "PLC Communication using PROFINET: Experimental Results and Analysis". Emerging Technologies and Factory Automation, 1-4, (2006).

[33] Internet: "Siemens Simatic S7-1200 Programmable Controller System Manual", http://www.generationrobots.com/media/manuel-plc-siemens-s7-en.pdf, Access Date:30.12.2016.

[34] Internet: "Wireshark", https://wiki.wireshark.org/PROFINET, Access Date:10.10.2016.

[35] Internet: "Simatic Step 7", http://w3.siemens.com/mcms/simatic-controller-software/en/step7/pages/default.aspx, Access Date: 30.12.2016.

[36] Internet: "Ettercap", https://ettercap.github.io/ettercap/, Access Date:03.10.2016.

[37] Internet: "A Technical Analysis of What Stuxnet's Creators Tried to Achieve: To Kill a Centrifuge", http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf, Access Date: 28.12.2016