Computers & Security 97 (2020) 101955

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

False data injection attacks and the insider threat in smart systems

Serkan Gönen [a], H. Hüseyin Sayan [b], Ercan Nurcan Yılmaz [b,*], Furkan Üstünsoy [b], Gökçe Karacayılmaz [c]

[a] Istanbul Gelisim University, Faculty of Engineering and Architecture, Istanbul 34310, Turkey
[b] Gazi University, Faculty of Technology, Ankara, 06500, Turkey
[c] Hacettepe University, Forensic Sciences, Ankara 06680, Turkey

ARTICLE INFO

Article history:
Received 7 November 2019
Revised 30 June 2020
Accepted 4 July 2020
Available online 5 July 2020

Keywords:
Cyber security
Industrial control systems
PLC security
FDI
Data manipulation

ABSTRACT

Smart networks and smart city systems, which are increasing in use with new approaches every day, are now in the investment plan of each state. At many points, these two concepts combine. Industrial Control Systems (ICS), which constitute the infrastructure of these systems, have opened to external networks due to the requirements of the era. Once smart grids are integrated with smart cities, ICS left its isolated structure. This process has emerged more security vulnerabilities. In this study, False Data Injection (FDI) attack was carried out to change the memory address values of Programmable Logic Controller (PLC)s which is an important component of ICS. Initially, the feasibility of the attack was examined. Thereafter, in the event of an attack, the effect on the systems was revealed. Eventually, important software and hardware solution suggestions to prevent the attack are mentioned. Thus, in the possible cyber attacks that may occur, it is aimed to recover critical systems with minimum damage and make them to be operational as soon as possible. It is considered that this study will make important contributions to other studies regarding ICS security.

© 2020 Elsevier Ltd. All rights reserved.

1. Introduction

The transition to both smart cities and smart networks today and in the future will be a necessity, not a luxury. The introduction of many systems such as natural gas distribution monitoring, traffic signaling, IP CCTV monitoring, energy monitoring and control in critical infrastructures of industrial zones, health centers, big shopping malls and some cities is an indication that this transition will accelerate and increase (Üstünsoy and Sayan, 2018).

ICS are one of the most critical components used in smart grid and smart city infrastructures. The vulnerabilities of the ICS and infrastructure architectures built on them effect the entire system. There are several attack methods that can be done through these vulnerabilities, but the FDI attack is one of the most damaging. Because with FDI attack, it is possible to change the data in a controlled way and to change the firmware codes. When the impact of the FDI attack on the system is evaluated, it will take a long time especially to bring the system back to its current working state and great damage may occur. In addition, with this attack, it is possible to obtain data by manipulating the data in a controlled manner. For this reason, it is critical to take the countermeasures by revealing the procedures of the FDI attack.

1.1. Related works

Industrial Control Systems (ICS), which constitute the infrastructure of smart city and smart network systems providing very important contributions to human life, were opened to external networks (internet-intranet) due to the requirements of the era such as efficiency, early failure intervention and remote access. These systems have become vulnerable to various cyber attacks because of the hybrid communication protocols (TCP / IP (Transmission Control Protocol / Internet Protocol), wireless IP and Bluetooth) used with this transition (Adepu et al., 2018). Since some SCADA systems have been avoided updating over the years for the high risk of interference that may result in a live system, older technologies are still present in many environments. As a result, nations have confronted with very dangerous attacks on the CNI (Critical National Infrastructure) via ICS, such as the Trans-Siberian Pipeline Explosion (Miller and Rowe, 2012), Maroochy Shire Water System (Stouffer et al., 2011), Stuxnet (Lagner, 2013), Flame (Kim et al., 2014), Duqu (Bencsáth et al., 2011), Havex (Thames and Schaefer, 2017), Black Energy (Lee et al., 2016). When incidents occur, a forensic investigation must be carried out to identify the cause and those responsible, but traditional IT forensic tools

* Corresponding author.
E-mail address: enyilmaz@gazi.edu.tr (E.N. Yılmaz).

https://doi.org/10.1016/j.cose.2020.101955
0167-4048/© 2020 Elsevier Ltd. All rights reserved.

and methodologies cannot be directly applied in ICS because they are COTS (Commercial/Consumer off-the-shelf) products. There are studies on ICS forensics in literature, although it is not sufficient. In this context of the study, Vliet et al. Examined forensic analysis after a fire in the wind turbine in their research. In the analysis phase of the study, while traditional forensics tools were used for device analysis, SCADA-specific OPC was used in historian in network analysis (Van Vliet et al., 2015). In another study for ICS forensics, Knijff introduced the tools that can be used after important ICS events. In the study, evaluations were made regarding tools that can be used in ICS such as OPC, Sleuth Kit and Xiraf due to the difficulty of using existing traditional network specific tools in ICS (Van der Knijff, 2014). Wu et al. proposed a new SCADA forensic process model, in their study on ICS forensics. They argued that although there are significant deficiencies, Historian and OPC client can be used in the storage and analysis of SCADA data in the model, while RSLogix 5000 can be used in fault logging (Wu et al., 2013). Therefore, continuous monitoring of the ICS, on a 24/7 basis, managing smart cities/grids has to be essential (Yılmaz and Gönen, 2018; Zanella et al., 2014). Because there are different types of attacks including attacks on data availability, data privacy, and data integrity for smart cities/grids (Cintuglu et al., 2016). One such attack is the injection of false data into the Programmable Logic Controller (PLC), a vital component of the intelligent grid operating module. This attack is an example of a data integrity attack. Recently, these types of attacks, commonly known as False Data Injection (FDI) attacks (Myers et al., 2018), have attracted great attention as they can bypass existing security measures and take advantage of system operations. In these types of attacks, either insider contribution or stealing data by intervening communication plays an important role. For example, almost all of the nuclear theft and sabotage incidents have been carried out with the help of insiders. In 2014, an insider at the Doel-4 nuclear power plant in Belgium emptied all the lubricant inside the turbine, causing the plant to remain closed for months and hundreds of millions of dollars of economic damage. (Bunn et al., 2016) In an attack at waste management facilities in Queensland, Australia, large amounts of waste were poured into public areas. This attack was also carried out by a former employee of the institution (Slay and ve Miller, 2008).

Its widespread use and the embedded existence of the Modbus protocol in all devices increase the utilization tendency of this communication protocol to design compatible and trouble-free systems. Besides, many PLCs used in the industry support Modbus protocols, while they do not support other protocols or require additional modules. For this reason, this protocol has become indispensable in ICS for different brand model PLCs to work in harmony with each other.

In the vast majority of the studies above ready-made simulation programs or simulated mathematical models have been used and the results have been presented. Simulation and modeling techniques are useful for modeling and testing complex systems. The development of realistic models can help create scenarios that do not yet exist or are very costly to build. However, the approach based on simulation systems has two main disadvantages. The first is the difficulty of fully reflecting the real system and second is the possibility that the analyzes may not give the same results in the real system. Also, by utilizing the configuration information of an industrial control system or measurement system, an attacker could inject malicious measurements that would mislead the forecasting process without being detected by any of the available techniques.

The Modbus protocol has some basic security issues, such as authentication, encryption, and no integrity at all (Nardone et al., 2016). For example, if the master sends data to the slave, the slave must first authenticate the device from which it receives the data packet and then processes the packet. The Modbus protocol does not have this capability and therefore man-in-the-middle attacks (MitM) can easily take place in Modbus. As a result, the widely used Modbus protocol has serious cyber security vulnerabilities. Therefore, these vulnerabilities of the Modbus protocol were utilized in the target of the attack analysis of the study.

Apart from Modbus protocol, there are many other communication protocols, such as Distributed Network Protocol (DNP) 3.0 and Profibus, currently used in the industry. The DNP 3.0 protocol transmits unsolicited data along with requested data from field elements in SCADA systems. In this way, the SCADA system does not have to send continuous requests to the field staff. However, a small number of large data transmissions can be provided with this protocol. Although some improvements in security vulnerabilities have been made, it has not become widespread such as Modbus. Profibus protocol has found a wide range of applications in production and building automation. On the other hand, Modbus protocol is frequently used in many devices due to its open source and simple operation structure.

1.2. FDI attack and previous studies

To perform an FDI attack, it is not easy for the attacker to obtain the power grid topology and transmission line acceptance value. In their study, Sun et al. aimed to circumvent the bad data detection systems. In the result of the study, it was claimed that the attack on IEEE 30-bus simulation test systems was successful (Sun et al., 2015). When the literature is examined, there are several studies on FDI attacks like (Li and Wang, 2019). In the majority of these studies, theoretical modeling and experimental evaluation methods have been used on various simulation-based test environments (IEEE benchmark, IEEE-RTS-24-bus) (Li and Wang, 2019; Liu et al., 2015). In another section of studies, mathematical modeling (Rahman and Mohsenian-Rad, 2012) and graphical theoretical approach to network modeling (Kosut et al., 2011) have used for the detection of attacks. Although the simulation systems are used in the majority of the attacks and detections carried out for ICS, there are also studies, such as (Alves and Morris, 2018; Anwar et al., 2015), about attacks and detections carried out on the actual ICS. Simulation studies have important contributions to ICS security, however, the biggest deficiency of studies based on simulation systems is the difficulty of fully reflecting the real system and therefore the probability of the analyzes performed may not give the same results in the real system. However, the PLC (OpenPLC) designed with (Alves and Morris, 2018) could overcome this specific injection attack, but could not solve the authentication, integrity and confidentiality issues associated with the Modbus protocol that initially made the injection attack possible. The study carried out in (Anwar et al., 2015) has also consisted of a theoretical framework for integrity attacks. In the study by Urbina et al., they proposed physics-based intrusion detection algorithms for erroneous data ejection to real ICS testbeds (Urbina et al., 2016). In the study conducted by Adepu and Mathur, they proposed a detection algorithm labeled Distributed Intrusion Detection against successful intruder attacks. They carried out attacks analysis on an operational water treatment facility called Secure Water Treatment (SWaT) established in the iTrust research (Adepu and Mathur, 2018a). In another study conducted by Adapu and Mathur on the real ICS systems at iTrust research center, the effectiveness of attack detection mechanisms was addressed in the Hackfests event named SWaT Security Showdown (S3) (Adepu and Mathur, 2018b). The results obtained are very important because these three studies were implemented on the real ICS systems in the iTrust center. Lin et al. proposed a machine learning based ICS IDS model for detecting attacks on water level control and air pol-

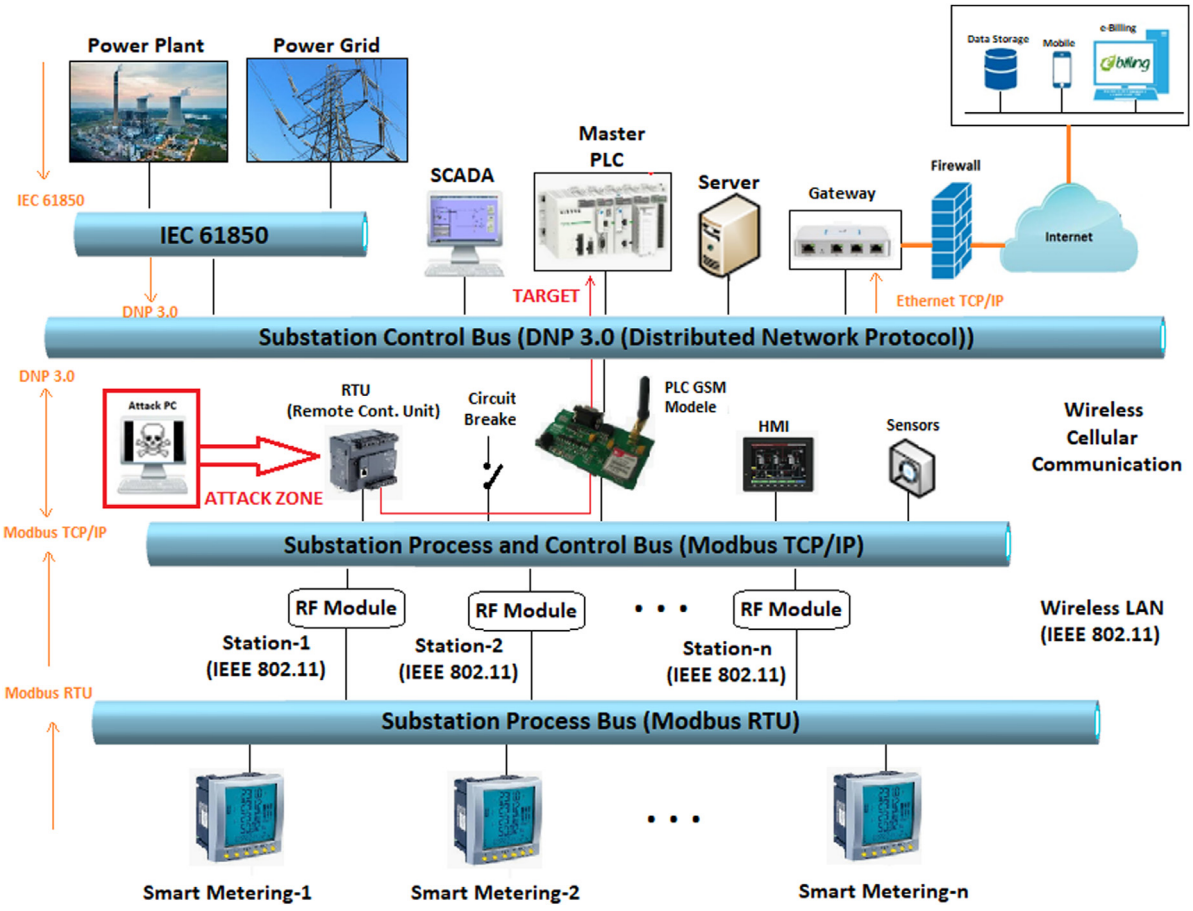


Fig. 1. Projected System Architecture and Attack Point.

lution control infrastructures. However, the attack on the testbed and subsequent outcomes for detection were not mentioned in the study (Lin et al., 2017).

In this study, an FDI attack was carried out on SCADA infrastructure designed to represent the smart city and smart grid systems by taking advantage of the vulnerabilities of communication protocols used in ICS. Although security measures (Firewall, IDS / IPS) were active during the attack, user electricity consumption costs in the system were changed and the integrity component of the system was disrupted.

The analysis of the study consists of an FDI attack on SCADA and detection and prevention of the attack. Therefore, an FDI attack was carried out by using the vulnerabilities of Modbus protocol and the data was physically manipulated despite password protection in ICS and SCADA system. Followingly, after enumerating recommendations for the prevention of this attack, the detection and prevention model (LiFi Model) were proposed.

The remainder of this paper is organized as follows: In Section 2, the testbed used in the study is explained in detail. While Section 3 deals with the register manipulation with false data injection attack carried out on PLC, which is an important component of ICS, the effects on the system are discussed in Section 4. In the 5th section of the study, the precautions to be taken against the FDI attack on the system have been stated and subsequently the continuous monitoring model with the LiFi model has been proposed as a solution. The study has been completed with the conclusion section.

2. Testbed

In order for the work to be done correctly, a real system structure must be used first. For this purpose, a system prediction covering a whole system was realized before the testbed was prepared. The system architecture and the point where the attack is carried out are shown in Fig. 1.

The system architecture consists of the transmission of energy consumption and network data received from the smart meter of each electricity consumer to the distribution transformer that transmits energy to the building via the industrial RF-Module (Wireless LAN). Finally, the data is transferred to the central monitoring and control unit by PLC GSM module (cellular communication) using DNP 3.0. In addition, it is also projected that the specific data of the grid and power plants will be transferred to the interface with the IEC 61,850 protocol and then transferred to the central control center again with DNP 3.0.

In the test environment prepared, the data was transferred to the central unit using RF-Module via Modbus communication protocol and IEEE 802.11bg (Wireless LAN) standard. The PLC-SCADA software, which performs visual monitoring from the center, remote load control, invoicing and historical data storage in the database, has been applied. In addition, the original web interface has been designed for real-time invoice tracking over the internet. Briefly, the design in the laboratory environment includes the layers up to the attack zone in the system architecture.

Thus, it is aimed to show that all invoices can be changed by only attacking the RTU of the SCADA system without the need to

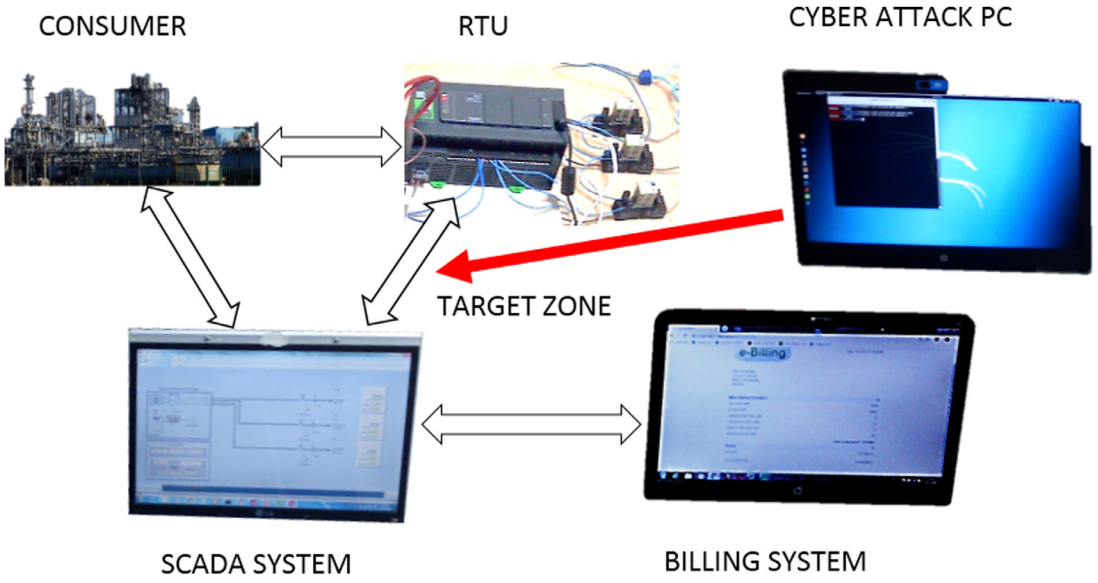


Fig. 2. Testbed.

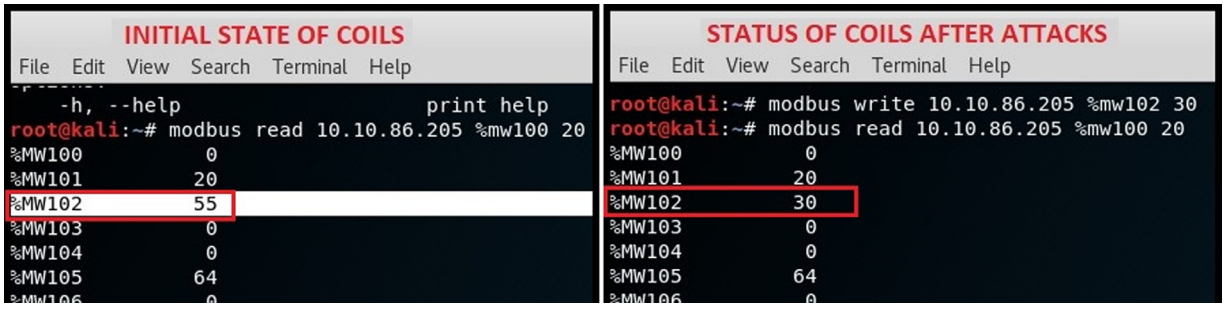


Fig. 3. The FDI attack on PLC without read / write password protection.

attack the web page or internet server. The attack zone planned to be carried out on a large system is shown in more detail in Fig. 2. Here, targets and objectives of the attack are seen more clearly.

3. Register manipulation with false data injection

FDI attack was carried out by an insider to Schneider M241 PLC used as a controller in the test environment according to the attack procedure listed below and the results were observed in WEB, PLC program interface (Somachine) and SCADA interface (Vijeo Citect).

FDI Attack Procedure;

➢ Username and password identification:

Firstly, user name and password were defined to device and interface to prevent read / write in order to prevent insider attacks via PLC program interface (Somachine). In this way, all the changes that could be made on the program interface without entering the user name and password were closed to the user.

➢ Determining the IP address of the controller:

In this phase, IP address of the controller was determined by scanning port 502 (Modbus Communication Port) with Nmap.

➢ Capturing device-specific information:

After determining the IP address of the PLC, critical information such as the brand, model and serial number specific to the device was seized.

➢ Open source intelligence:

Thanks to the finding the brand model of the device (Schneider M241), open source intelligence was conducted to detect the vulnerabilities of the brand model. As a result of the research, HMI, communication protocol and web interface vulnerabilities were determined.

➢ The attack is done with/without password protection:

As can be seen in Fig. 3, it was determined that the memory addresses (register) and I / O digital addresses (coils) of the device could be changed via Modbus communication protocol used by PLC device. As the identified vulnerability was very critical and priority, the exploitation of this vulnerability was emphasized in the attack analysis. User protection (read / write, read only, download) can be enhanced with password on Schneider PLCs. In the first installation, user descriptions are turned off in default. In order to increase security measures, password protection should be activated by the authorized user and the user rights must be regulated. In this context, in the first stage of attack analyses were carried out on the PLC without read / write protection with a password. Subsequently, the same analyses were carried out on PLC whose without read / write protection with a password activated by Somachine interface.

As a result of attack analyses, firstly the status of the memory addresses and I / O digital addresses were read without protection, and new values were sent to the memory addresses for changing the values at these addresses. As can be seen in Fig. 3, the values of 16-bit digital data in% MW102 memory could be changed. That is,

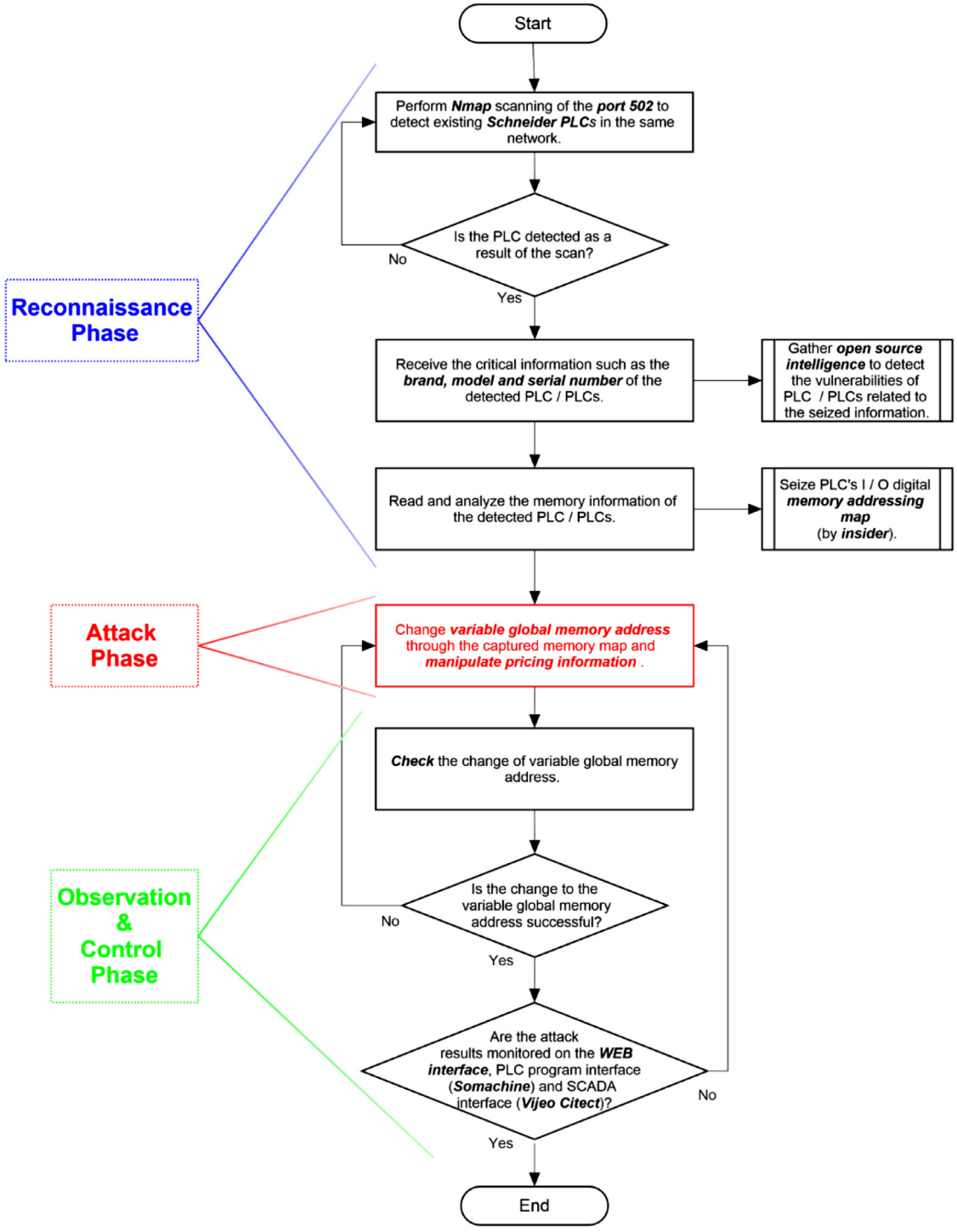


Fig. 4. Analysis steps for an FDI attack carried out on PLC devices.

if the insider seizes the addressing map, it is seen that the targeted memory addresses can be changed.

In summary, the attack to change the register addresses of the controller (PLC) was carried out according to the flow diagram depicted in Fig. 4.

The same analyses were repeated by activating password protection on the PLC to restrict read / write authorization. As it is seen in Fig. 5, password protection did not affect reading and changing the status of the values in memory and I / O digital addresses and the values could be changed.

Considering that not only the energy consumption data can be monitored but also the energy flow control with the designed system, the results of the memory attack will be vital. The attack was carried out on variable global addresses in the master PLC (MTU) as described in Fig. 1. In the case of smart grid / city systems, the values of all addresses and the status of I / O digital addresses can be changed by insider attack, except for the memory that is continuously overwritten in the PLC.

The attack analysis of the study was carried out on smart city / network systems. However, the attack should not be evaluated only from the perspective of a smart city or smart grid. For example, in a nuclear power plant, it is possible to change the reference value given for the flow rate of the main refrigerant pump of the reactor

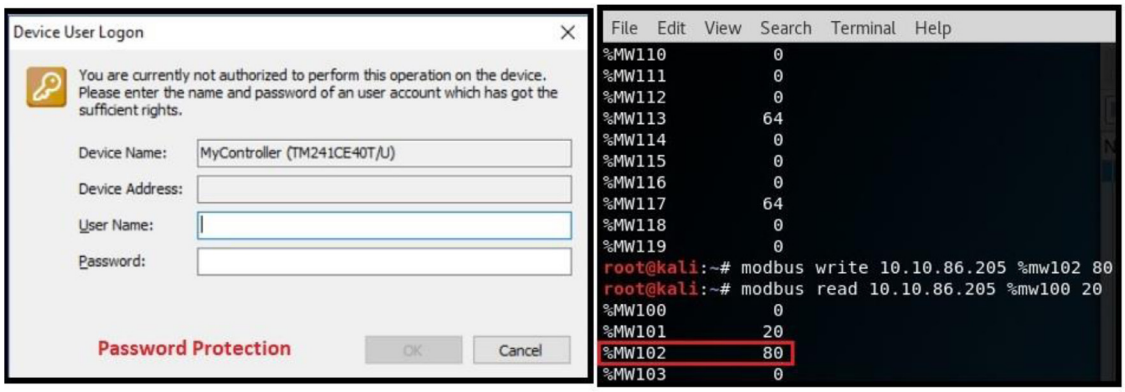


Fig. 5. The FDI attack on PLC with read / write password protection.

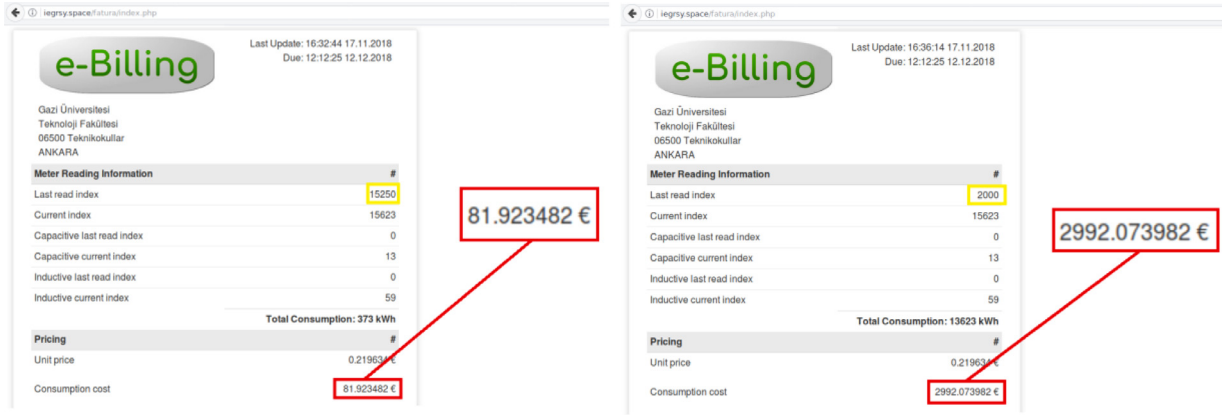


Fig. 6. a) Actual Invoice Cost of Consumer b) Increased Invoice Value After Attack.

by this attack. In this respect, such an attack on the nuclear power plant will have fatal consequences.

4. Attack analysis

With the FDI attack, the invoice cost was raised to high levels by changing the memory address which was defined as variable global at% MW1448 address in PLC and known to an insider. In this study, the variable global memory address was the first index data of invoice consumption price and entered manually by the operator. This first index value, which was not a consistently overwritable memory address, was decreased and the consumption value was increased. In this way, the invoice price was increased.

With the change of the value in PLC memory address, the alteration was observed instantly on SCADA, database and WEB. As an example, the change of invoice consumption price on WEB is shown in Fig. 6. WEB design was realized as a prototype for single user and electricity consumption values were reflected on the WEB in real-time.

The real-time change of the first index values in the SCADA screen designed in Vijeo Citect program as a result of cyber attack is given in Fig. 7.

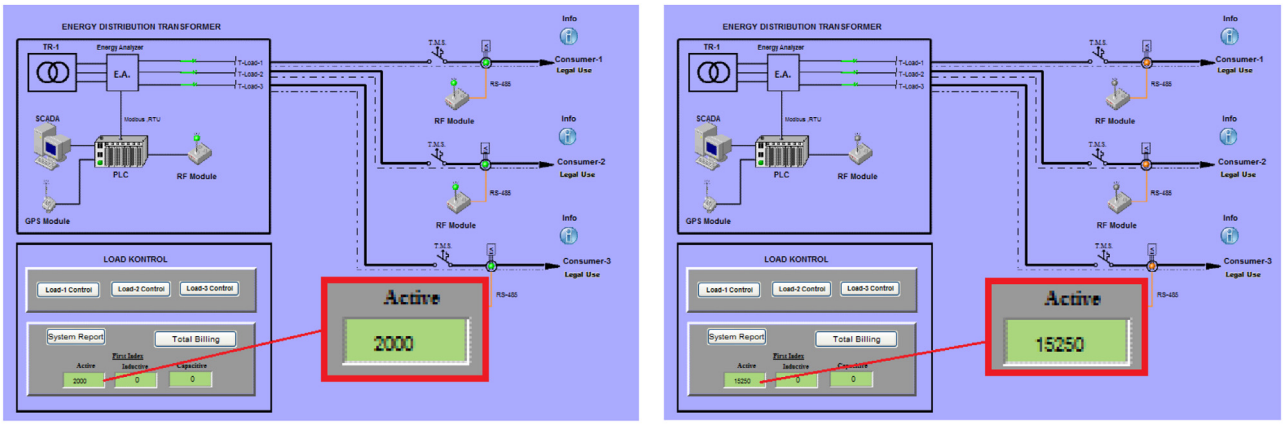
Considering the results obtained after the attack, the network data sent from the energy analyzer to the PLC-SCADA system in real time by exploiting the vulnerabilities of the Modbus protocol were manipulated. In this way, not only the invoice consumption cost was changed, but also all the coils that provide power flow control were changed and the control of the whole system was seized.

As a result of the change of register and coils, The MTU (Master Terminal Unit) and all RTUs (Remote Terminal Units) could be controlled by the attacker. If this attack occurs on the actual grid, there may be an interruption in the desired area or interruptions due to the load imbalance that may affect each other under the domino effect, causing the entire network frequency to collapse. Such a scenario will cause a region or the whole country to be de-energized for a long time and cause significant economic consequences. The US Northeast power outage in 2003 showed that even a small error in one part of the network (the interruption of a single transmission line in northern Ohio) had a gradual impact, causing billions of dollars in economic losses (Liu et al., 2015).

5. Precautions to be taken

Although IDS / IPS are effectively used within the scope of the measures taken against cyber attacks in traditional networks, IDS / IPS for ICS and SCADA systems have some limitations. We can state these limitations in the following headings:

- Lack of a well-known threat model,
- High probability of false alarm or false-negative,
- The development of IDS systems customized for ICS environments is not yet proven for real systems,
- The ability to analyze intrusion detection and prevention software to be used on the live system in ICS may interfere with system continuity/ availability,
- There are a few of data collection tools and methodologies, which are indicated in the introduction, designed specifically for SCADA systems (Rahman and Mohsenian-Rad, 2012).



(a) (b)

Fig. 7. a) SCADA First Index Actual Value b) SCADA First Index Value After Attack.

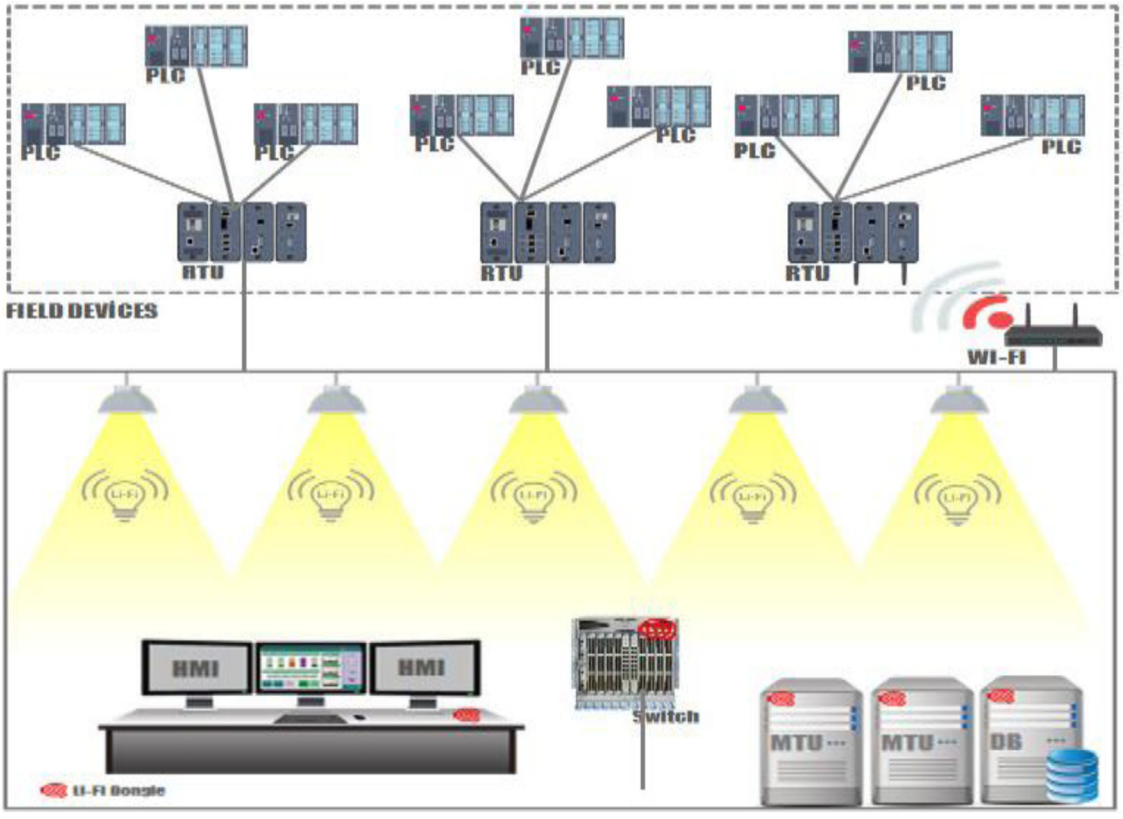


Fig. 8. LiFi Usage in ICS Security.

Therefore, some precautions can be taken from the design phase against such attacks on the system.

- Running continuous writing of memory addresses in the design of systems (using forced register and coils),
- Sharing of syslog data by activating log system in SCADA-PLC design and reporting to the security manager,
- Separation of external and internal networks and concealment of internal networks,
- Not connecting ICS network directly to the Internet and planning network segmentation,
- Running NAT / NPAT (Network Address Translation and Network Port Address Translation),
- Keeping the hardware-software design information of the system and the memory map in ICS software confidential,
- Use intrusion detection systems into the system host or network,
- Continuously monitoring ICS network, especially critical ones,
- Use of manageable smart network switches in the system in order to maintain bandwidth and prioritize data,
- Agent software to be used to detect cyber attacks on all devices of the system (Server, PLC, RTU, MTU, etc.)

The security measures to be taken against FDI attacks are mentioned above. However, given that the attack's success can be achieved by the attacker having critical information such as ICS 'register topology map, the importance of authorization, authentication and continuous monitoring of the network comes to the fore. In this context, a model shown in Fig. 8 is proposed for authentication and authorization. Only the authorized personnel

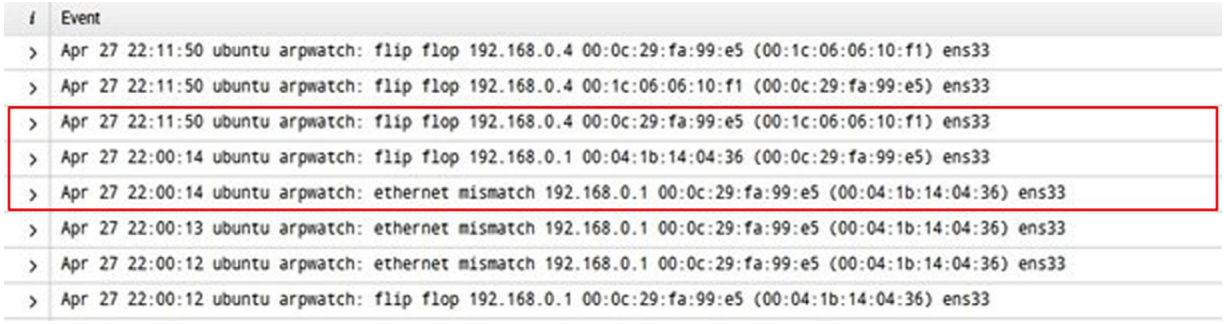


Fig. 9. SIEM GUI for ARP Alerts.

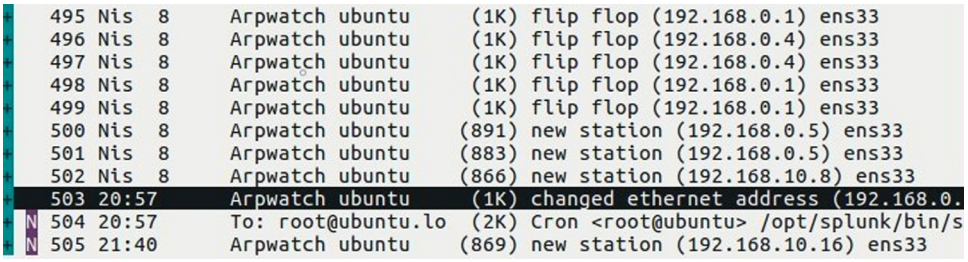


Fig. 10. ARP Table Alerts.

checked physically (dongle) are accessed to the management center where the critical components of ICS are located in the model. If this model is used, access will be provided only by authorized personnel. Precautions will be taken against insider attacks, as control of people with physical keys can be made easier.

At this point, correct network segmentation is of great importance for the success of the proposed mentioned model. If network segmentation is not performed correctly, the possibility of infiltration into the network may occur and the measures taken with the model mentioned above will be invalid by providing the attacker with access to the critical management network.

Although many precautions have been taken, it should not be forgotten that the control of alarms belonging to security software and hardware is the most critical factor and continuous monitoring should be done correctly. For this reason, against the unauthorized access and manipulation of the data by intervening in the network, with attacks such as FDI and MitM, generating alarms in the event of any alteration in critical data (MAC, IP, etc.) by continuously monitoring is critical.

The most important information needed for the attacker in FDI attacks is the predetermination of the memory / coil addresses to be injection. In this way, while the system is distracted by screening attacks such as DoS / DDoS attack, the attacker will be able to reach his goal in a short time. In this way, while the system is distracted by screening attacks such as DoS / DDoS attack, the attacker will be able to reach his goal in a short time. Therefore, the attacker should either be supported by an insider, or she/he should carry out one of the intervention attacks to get the information needed.

In this study, packet analysis could be done without adding additional load to the system using the mirroring technique. In this way, the Arpwatch application was used to follow the changes (ARP and IP mapping) of the information (ARP and IP mapping) of all new devices and existing devices in the system. The human readable GUI interface was also described for easier monitoring of changes by system users / security administrators. MitM, which is the first stage of the FDI attack, can be traced by following the changes in the system at Layer 2/3 level. Since MitM cannot be performed, the FDI attack will be very difficult for the attacker and will not be feasible as it will be difficult to get the memory address of the attack. In Fig. 9, the alarms generated after the changes occurring for continuous monitoring in Fig. 10 are displayed on the GUI. This will facilitate 24/7 continuous monitoring.

On the other hand, the integration of agent software into all devices may restrict or prevent the devices from performing control tasks. Therefore, either the control software must run independently or the agent software must be located in manageable smart network switches. As it is understood, both software and hardware security measures should be taken when designing the system architecture and automation designers must consider these issues.

In addition to the aforementioned measures, considering the fact that the human factor is the weakest link in cyber security and that the attack was carried out by the insider, "need to know" and "least to know" principles (Sindiren and Ciylan, 2019) should be taken into consideration.

6. Conclusion

Cyber attacks, especially industrial espionage and information disclosure, could result in serious financial damage. It is important to know the attack method to prevent cyber attack. In this study, it is focused on insider changing the consumption cost by exploiting PLCs, which is one of the important components of ICS, Subsequently, precautions taken to overcome this attack are listed. Attack analyses results have emphasized the importance of the integrity component, which is one of the three components of cyber security, for ICS.

This study reveals that the register addresses of the controller (PLC) can be easily changed. It has been proved that FDI attacks can control the disconnectors and breakers in high voltage transmission lines and make illegal energy interruptions. After the illegal interruption in the network, the load values read in the ICS memory are shown in their normal values so determining the source of the problem on SCADA may take a very long time.

Similarly, waiting times at the desired location in the traffic signaling system can be changed and this may cause financial and even life loss. At the desired points in the distribution of natural gas in the city, by changing the position of the valves, natural gas

flow directions can be changed and stopped or the pressure values in the gas transmission line can be increased by changing the reference values of the pumps and these undesired alterations may cause fatal damages.

Based on FDI, determining where the attack will be injected is the most important information of the attack. Without an insider or its support, it can take a long time for the attack to be made to the desired addresses, and it may no longer be feasible for the attacker, so this situation makes the attacker change the target. Considering the FDI attack phases performed in this study, as depicted in Fig. 3, access to critical components of ICS and the confidentiality of critical information is crucial. According to least to know the principle, this type of critical information should only be known by a minimum number of authorized personnel and should be kept only local systems that are not open to the Internet. In addition, the job status of such authorized users should check continuously and take necessary measures for cases such as dismissal and transfer of authority, and the privileged accounts of the no longer authorized personnel should be canceled.

Consequently, cyber security measures should be considered from the design phase of ICS components, which play a critical role in the management of critical infrastructures, and continuous monitoring should be performed on a 24/7 basis. For this purpose, by taking into account the business continuity, which is the most important function of industrial control systems, continuous monitoring of information disclosure attacks was carried out without bringing the additional load to the existing system. In addition, with the designed LiFi model, the Privacy and Integrity dimensions are provided as the critical data of ICS is only transmitted in a masked data form among authorized users. Thus in the event of possible cyber attacks, these critical systems can be recovered with the least damage and will be operational as soon as possible.

Credit author statement

Serkan Gönen: Cyber security expert, Software, Writing- Reviewing and Editing

H. Hüseyin Sayan: Applied mathematics, formulations

Ercan Nurcan Yılmaz: Supervision, Writing- Reviewing and Editing, Software

Furkan Üstünsoy: SCADA program development, Software

Gökçe Karacayılmaz: Cyber security expert.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

Adepu, S., Mathur, A., 2018a. Distributed attack detection in a water treatment plant: method and case study. IEEE Trans. Depend. Secure Comput. doi:10.1109/TDSC.2018.2875008.

Adepu, S., Mathur, A., 2018b. Assessing the effectiveness of attack detection at a hackfest on industrial control systems. IEEE Trans. Sustain. Comput. doi:10.1109/TSUSC.2018.2878597.

Adepu, Sridhar, Kandasamy, Nandha Kumar, Mathur, Aditya, 2018. EPIC: an Electric Power Testbed for Research and Training in Cyber Physical Systems Security. In: Computer Security. Springer, Cham, pp. 37–52.

Alves, T., Morris, T., 2018. OpenPLC: an IEC 61,131–3 compliant open source industrial controller for cyber security research. Comput. Secur. 78, 364–379.

Anwar, A., Mahmood, A.N., Tari, Z., 2015. Identification of vulnerable node clusters against false data injection attack in an AMI based smart grid. Inf. Syst. 53, 201–212.

Bencsáth, B., Pék, G., Buttyán, L., Félegyházi, M., 2011. Duqu: a Stuxnet-like malware found in the wild. CrySyS Lab. Techn. Report 14, 1–60.

Bunn, M., Malin, M.B., Roth, N., Tobey, W.H., 2016. Preventing Nuclear Terrorism: Continuous Improvement Or Dangerous Decline? (Cambridge, Mass.: Project on Managing the Atom. Belfer Center for Science and International Affairs, Harvard Kennedy School.

Cintuglu, M.H., Mohammed, O.A., Akkaya, K., Uluagac, A.S., 2016. A survey on smart grid cyber-physical system testbeds. IEEE Commun. Surv. Tutor. 19 (1), 446–464.

Kim, S.J., Cho, D.E., Yeo, S.S., 2014. Secure model against APT in m-connected SCADA network. Int. J. Distrib. Sens. Netw. 10 (6), 594652.

Kosut, O., Jia, L., Thomas, R.J., Tong, L., 2011. Malicious data attacks on the smart grid. IEEE Trans. Smart Grid 2 (4), 645–658.

Lagner, R., 2013. A Technical Analysis of What Stuxnet's Creators Tried to Achieve -To Kill a Centrifuge. The Langner Group, Arlington, Hamburg, Munich.

Lee, R.M., Assante, M.J., ve Conway, T., 2016. Analysis of the Cyber Attack On the Ukranian Power Grid. E-ISAC, Washington, DC, USA, pp. 1–29.

Li, Y., Wang, Y., 2019. False data injection attacks with incomplete network topology information in smart grid. IEEE Access 7, 3656–3664.

Lin, C.T., Wu, S.L., Lee, M.L., 2017. Cyber attack and defense on industry control systems. In: 2017 IEEE Conference on Dependable and Secure Computing. IEEE, pp. 524–526.

Liu, X., Zhu, P., Zhang, Y., Chen, K., 2015. A collaborative intrusion detection mechanism against false data injection attack in advanced metering infrastructure. IEEE Trans. Smart Grid 6 (5), 2435–2443.

Miller, B., Rowe, D.C., 2012. A survey SCADA of and critical infrastructure incidents. RIIT 12, 51–56.

Myers, D., Suriadi, S., Radke, K., Foo, E., 2018. Anomaly detection for industrial control systems using process mining. Comput. Secur. 78, 103–125.

Nardone, R., Rodríguez, R.J., Marrone, S., 2016. Formal security assessment of Modbus protocol. In: 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST). IEEE, pp. 142–147.

Rahman, M.A., Mohsenian-Rad, H., 2012. False data injection attacks with incomplete information against smart power grids. In: 2012 IEEE Global Communications Conference (GLOBECOM). IEEE, pp. 3153–3158.

Sindiren, E., Ciylan, B., 2019. Application model for privileged account access control system in enterprise networks. Comput. Secur. 83, 52–67.

Slay, J., ve Miller, M., 2008. Lessons Learned from the Maroochy Water Breach. In: International Conference on Critical Infrastructure Protection (ICCIP), Hanover, NH, United States, pp. 73–82.

Stouffer, K.A., Falco, J.A., ve Scarfone, K.A., 2011. Guide to Industrial Control Systems (ICS) Security-SP 800-82. National Institute of Standards and Technology (NIST), pp. 1–155.

Sun, Y., Li, W.T., Song, W., Yuen, C., 2015. False data injection attacks with local topology information against linear state estimation. In: 2015 IEEE Innovative Smart Grid Technologies-Asia (ISGT ASIA). IEEE, pp. 1–5.

Thames, L., Schaefer, D., 2017. Cybersecurity For Industry 4.0. Springer, New York, pp. 73–76.

Urbina, D.I., Giraldo, J.A., Cardenas, A.A., Tippenhauer, N.O., Valente, J., Faisal, M., Sandberg, H., 2016. Limiting the impact of stealthy attacks on industrial control systems. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pp. 1092–1105.

Üstünsoy, F., Sayan, H.H., 2018. Sample laboratory work for energy management with SCADA supported by PLC. J. Polytech. 21 (4), 1007–1014.

Van der Knijff, R.M., 2014. Control systems/SCADA forensics, what's the difference? Digi. Invest. 11 (3), 160–174.

Van Vliet, P., Kechadi, M.T., Le-Khac, N.A., 2015. Forensics in industrial control system: a case study. In: Security of Industrial Control Systems and Cyber Physical Systems. Springer, Cham, pp. 147–156.

Wu, T., Disso, J.F.P., Jones, K., Campos, A., 2013. Towards a SCADA forensics architecture. In: 1st International Symposium for ICS & SCADA Cyber Security Research 2013 (ICS-CSR 2013), 1, pp. 12–21.

Yılmaz, E.N., Gönen, S., 2018. Attack detection/prevention system against cyber attack in industrial control systems. Comput. Secur. 77, 94–105.

Zanella, A., Bui, N., Castellani, A., Vangelista, L., Zorzi, M., 2014. Internet of things for smart cities. IEEE Inter. Thing. J. 1 (1), 22–32.