Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 07, July-2021

Emerging Technology IoT and OT: Overview, Security Threats, Attacks and Countermeasures

Aman Srivastava
Department of Computer Science and Engineering,
Babu Banarasi Das Institute of Technology and Management, Lucknow-226028, India

Ankita Agarwal
Assistant Professor,
Department of Computer Science and Engineering,
Babu Banarasi Das Institute of Technology and Management, Lucknow-226028, India

***Abstract*—This paper provides an overview of Internet of Things (IoT) and Operational Technology (OT) with an emphasis on major security challenges and attacks faced by these technologies. With increased deployment of IoT and OT systems in today's world, e.g., IoT is often seen in office or home automation and smart appliances, this increases the possibility of malicious threats than ever before. While a number of researches have been done to explore such challenges. Compared to previous work, this paper aims to provide a detailed analysis of security goals which covers common problems faced by IoT and OT devices, OWASP top 10 security threats, The Purdue Model, IT/OT convergence and addresses most of the important security attacks and their countermeasures for IoT and OT systems.**

Keywords— Internet of Things (IoT), Operational Technology (OT), The Purdue Model, Security Threats, Attacks, Countermeasures

I. INTRODUCTION

The IoT is an important and emerging topic in the field of technology, economics, and society in general. The Internet of Things (IoT), is commonly defined as network of physical objects that can sense, collect, analyse, and send data using internet protocols. IoT have revolutionized the very way of living. Lately, internet is not only limited to computers, but it has expanded to vehicles, smart phones, industrial systems, home appliances and so on [1, 2]. Some real-world examples of IoT are fitness trackers (like Fitbit), voice assistants (Alexa and Google Home), smart appliances (like Amazon echo, Phillips Hue, etc.).

Operational Technology (OT) plays a major role in today's modern society, as it drives a collection of devices that are designed to work together as a homogenous or integrated system [3]. OT generally referred as software and hardware that are used to manipulate changes in industrial operations through monitoring and controlling physical processes, devices and infrastructure [4]. The rate at which IoT and OT systems are growing and being deployed in real life has become ubiquitous, which also has potential consequences that need to be addressed.

II. RISKS VS. FUTURE TRENDS

Although IoT is growing at such a rate and has enormous advantages, but some devices still have not got the security updates/patches that make them vulnerable and restrict them to limited functionalities [5]. The threats to IoT can be sorted into three primary categories: Security, Privacy and Safety. The importance of these categories is clear, as IoT devices are becoming more pervasive in our lives than smartphones and other gadgets [6]. It will have access to the most confidential and sensitive information, such as financial records, personal records and social security numbers [7].

For example, if we take smartphones or laptops, there are less concerns, whereas when it comes to IoT devices, then the concern quickly multiplies in numbers. In the future, we will witness a deadly combination of IoT and AI at it's very best. They both together work in a cycle where data collected by IoT devices is processed with help of AI algorithms which in turn give useful results that are further implemented using IoT devices [8]. There is continuous work going on in fields like VUI and Miniaturization of things (smart objects) as they result in many perks for users. Reduction in power consumption or proper use of available sources of power is a very important aspect where work is constantly being done. Such will be the scope of IoT that almost all sectors including key areas like Transportation, Manufacturing and Agriculture will be hugely influenced by it [9].

With the advent of OT, its security aspect is the biggest deal to encounter. So, if we give proper attention to possible threats and employ required techniques to overcome the issues, we can have an improved communication, less risk of cyber-attacks, amplified efficiency and will add to user friendliness.

III. PROBLEMS OF IOT

IoT devices are loaded with numerous features and applications but a lack of basic security policies makes it easy prey for hackers [10, 11]. Some of the challenges that makes IoT devices vulnerable to threats:

- Vulnerable Web Surfaces
- Lack of Legal, Regulatory and Rights
- Buffer Overflows
- Storage Issues
- Physical Theft and Tampering
- Difficult-to-Update Firmware and OS

TABLE I. OWASP TOP 10 IOT THREATS AND SOLUTIONS

	Vulnerabilities	Solutions
1.	**Weak, Guessable, or Hardcoded Passwords**	• Use complex passwords or passphrases • Use password management system
2.	**Insecure Network Services**	• Use firewall and IDS • Use encrypted version of the services • Close unnecessary open ports
3.	**Insecure Ecosystem Interfaces**	• Implement multi-factor authentication mechanisms • Periodically evaluate the interfaces
4.	**Lack of Secure Update Mechanisms**	• Implement secure delivery by encrypting communications route

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 07, July-2021

		• Use checksum and hash to verify the integrity of updates
5.	**Use of Insecure or Outdated Components**	• Remove insecure software libraries or dependencies • Avoid using third-party software or hardware components from a compromised supply chain
6.	**Insufficient Privacy Protection**	• Implement CIA triad • Anonymize data collected from users
7.	**Insecure Data Transfer and Storage**	• Use encrypted channels for transferring data • Implement Access control mechanism properly
8.	**Lack of Device Management**	• Monitor runtime-settings • Blacklist device that seem suspicious
9.	**Insecure Default Settings**	• Change default username and passwords • Avoid using remote access feature
10.	**Lack of Physical Hardening**	• Configure password for BIOS • Minimize the use of external ports

IV. LET'S BEGIN WITH SOME IOT ATTACKS THAT ARE DONE GLOBALLY:

A. BlueBorne Attack

A BlueBorne attack is performed by an attacker to gain full access of the target device by leveraging Bluetooth connection. In this attack, it is not required that the targeted device is paired with the attacker's device or even set to discoverable mode, that leads to conduct a large range of offenses, which includes remote code execution as well as Man-in-The-Middle attacks. BlueBorne attack can be performed on various IoT devices which also includes devices those are running operating systems such as Android, Linux, Windows, etc [12]. These steps can be followed to perform BlueBorne attack:

- Attacker tries to locate all active Bluetooth-enabled devices around him/her
- Then attacker obtains the MAC address of the device
- Now, the attacker tries to determine the OS by continuously probing the target device
- After OS is identified, attacker exploits the vulnerabilities in the Bluetooth protocol to gain access to the target device
- Now that an adversary has full access to the device, she/he can perform RCE or MiTM attack

Countermeasures: To prevent BlueBorne attack, one must turn off Bluetooth when not in use, turn off discoverable feature and install the latest patch released by vendors, because ones an attacker has made it to your device using BlueBorne vector, there is no way to stop him except resetting the device [13].

B. Rolling Code Attack

Nowadays, most smart vehicles use smart locking system, which works using RF signal that is transmitted in the form of code from a key to lock or unlock the vehicle. This code is only used once and it is rejected, if a vehicle receives the same code again. This is done to prevent replay attacks. This code that locks or unlocks a car is called a rolling code or hopping code. Now the attacker thwarts the transmission of a signal to obtain the rolling code. This attack is performed using a jamming device which jams the signal and sniffs the code simultaneously and attacker can use that code later to unlock the vehicle [14].

Here are some steps that are followed by an attacker to perform a rolling code attack:

- Victim presses remote button to unlock the car
- Attacker uses the jammer to sniff the first code and jams the car's receptor device
- Victim tries sending code again by car remote button as the car did not unlock first time
- Attacker sniffs the second code this time also, but he forwards the first code which unblocks the car
- Now the attacker can use the recorded second code to unlock the car.

Countermeasures: Defending against rolling code attack is almost impossible because RF protocols that are used are themselves so weak that nothing can prevent capturing, replaying and analyzing the broadcasted RF signals. But there are some steps that can be adapted to increase the defense such as avoid using remote dongle to lock or unlock car instead use the push button in the handle of door. One can buy theft insurance, financial defence is better step than physical defence in this scenario [15].

C. SDR-Based Attacks.

A SDR system is a radio communication system in which software (or firmware) is used instead of hardware for generating radio communications and signal processing. The usage of wireless physical communication in IoT devices leads to unprecedented opportunities for attackers like examining the communication signals in IoT networks and sending exploit to interconnected devices. Hung et al. [16] have discussed about four vulnerabilities which can be exploited using SDR:

a) Reconnaissance of a Target:

Operating system of an IoT device is the most important thing, sometimes it can be found with FCC ID information or on the device's website. Sometimes SDR tools like HackRF one is used to monitor a wide range of frequency spectrum and determine the frequency of at which the device is normally operating on.

b) Decode Data Unknown RF Protocol:

GNURadio companion tool is used to decode the signal data. Some additional steps like reverse engineering the protocol is carried out to obtain the original signal. HackRF One is used to capture the signal emitted by transmitter and recorded in wav format. The wav file is then opened in Audacity, it is a tool which is used to analyze and modify the audio and raw captured files. Then, the signal is finally segregated into 8-bit blocks to convert into text.

Fig. 1. HackRF One

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 07, July-2021

c) Replay Attacks:

Replay attack is the major attack using SDRs. In this attack signal is captured and then retransmitted. As a result, after replaying the signal, receiver circuit performs the operation as usual. Below are some steps to perform a replay attack:

- During reconnaissance, operating frequency of the device was found, monitor that frequency to capture the signal once initiated between the interconnected devices.
- The, command sequence is segregated and injected into the signal using tools like Universal Radio Hacker (URH).
- Then this frequency containing segregated command sequence is broadcasted, which replays the operation of the device.

d) Jamming Attack:

Jamming RF is a type of attack in which communication between transmitter and receiver gets disrupted. This is done by transmitting high- power signal on operating frequency of the device, which results in a DoS attack. This makes the endpoints unable to communicate with each other. Every wireless access point is vulnerable to this attack [17].

Countermeasures: Defence against SDR-based attack can be achieved by following some techniques such as using large frequency spectrum to switch frequency, securing the signal using encryption protocols such as RSA encryption. Implement AES for standard communication or authentication protocols. Avoid using same command frequently instead use rolling technique [18].

D. DDoS Attack

A distributed denial-of-service attack is an attack in which multiple compromised systems are used to flood servers, online systems, or networks with traffic to exhaust resources and bandwidth. As a result, systems become slow or unavailable to fulfil valid requests. In case of IoT DoS or DDoS attack is initiated to compromise the device or make it botnet [7, 11]. To achieve this, attacker first exploit the vulnerabilities in the device and launches the attack by installing malicious software in their operating system. Target systems receive large volume of requests from various IoT devices present in different location, which slows down the target or sometimes shut it down completely [19].

Roohi et al. [20] categorised the DDoS attack in IoT domain according to their impact on resource, availability of bandwidth, impact on infrastructure of the device and impact of the bug that is exploited by the attacker.

a) Resource Depletion Attack:

This attack directly impacts the resources (memory, CPU, and socket) that are deployed in an IoT environment [20]. This attack can be achieved by either exploiting network vulnerability, weaknesses in transport or application layer protocols, or by sending malformed packets such as Ping-of-Death attack.

b) Bandwidth Depletion Attack:

This attack is done to consume all the bandwidth of IoT network. This can be achieved by amplifying or broadcasting the malformed packets to increase the density of the attack [19]. UDP flood attack and ICMP flood attacks are the type of bandwidth depletion attack.

c) Infrastructure Attack:

This attack directly impacts the IoT device and its components by making the bandwidth and resources unavailable to the users [20].

d) Zero Day Attack:

Zero day attack is initiated by exploiting a software vulnerability which is unknown to the vendor or developer. Patch for these types of vulnerabilities is released after the attack [21].

Countermeasures: To prevent DDoS attack different security solutions need to be implemented at different IoT layers. Researchers have introduced many lightweight encryption mechanisms for IoT architecture that can improve the security at perception layer [22, 23]. To secure the network layer IPv6 techniques, Encapsulation Security Payload (ESP), and Authentication Header (AH) can be configured to encrypt the data between the endpoints and verify its integrity [24]. Santos et al. [25] introduced a method in which DTLS can be used to provide secured end to end communication and certificate management using IoTSSP (Internet of Things Security Support Provider). Access control and authentication techniques can be used to secure the middleware layer [26]. For application layer, machine learning model can be deployed to learn and monitor the traffic patterns and give alerts in case of any unusual traffic. Afek et al. [27] proposed use of Double Heavy Hitters (DHHs) and Triple Heavy Hitters (THHs) algorithms, which helps in solving DoS attacks via string hits.

E. Side Channel Attack

Almost all IoT devices emit signals (side channel emissions) that provides information about their internal processes. By monitoring these signals, intruder can extract information about encryption keys to perform side channel attack [28]. The concept of SCAs is such that data is always leaking, which intruders exploit either via power consumption or electromagnetic emissions. Abrishamchi at el. [29] described main types of side channel attacks.

a) Timing Analysis Attacks:

A timing analysis involves analysing the associated timestamps assigned to each event. An adversary may use specialized attack strategies to get the information about events such as packet transmission in a network. This attack is achieved by exploiting the difference in time of execution for different branches in ecosystem [30][31].

b) Power Analysis Attacks:

In power analysis attacks, an adversary observes the power consumption of the devices. To measure the power consumption of the sensor node, attacker need to be in close proximity to that node. Power analysis are of two types, namely simple power analysis (SPA) and differential power analysis (DPA). SPA is an approach of power consumption analysis of cryptographic operation, while in DPA analysis of power consumption is done on both cryptographic and non-cryptographic operations [32, 33].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 07, July-2021

c) Fault Analysis Attacks:

Fault analysis attack can be achieved when some fault occurs in the cryptosystem and useful information gets leaked. These faults may occur naturally or manually injected by an adversary in two ways. One is to use equipment such as laser pointer to flip some bits in memory or by giving invalid inputs to program [34]. Biham et al. [35] have discussed this attack in detail.

d) Traffic Analysis Attacks:

Traffic flow contains information about critical nodes, such as aggregator node in a sensor network. Aggregator nodes are the sensor nodes that are used to relay transmission between nodes and base station. Traffic analysis attacks are initiated by analysing these traffic flows (i.e., tracking data packets, recording transmission interval and counting packet number) to gather topological information [36].

e) Acoustic Attacks:

An adversary may gain secret information by analysing the associated acoustic oscillations produced by devices [37].

f) Electromagnetic Leakage Attacks:

Electromagnetic radiations are emitted by the devices those are performing cryptographic operations such as encryption and decryption. Attacker exploit leaked radiations to perform electromagnetic analysis. This analysis is further used for finding relations between leaked radiation and ciphertext [38].

g) Thermal Imaging Attacks:

Thermal imaging attack is similar to acoustic attack except that the emission which gets exploited is heat instead of sound.

Countermeasures: Defence against side-channel attacks is done in mainly two ways either by reducing the signals leaked by the systems or by segregating the connection between sensitive data and leaked information. This can be achieved by implementing more advanced cache allocation; add unnecessary breaks, or random noise into the process, and by using detection system which can identify modifications of the cryptographic operations [39].

It's not possible to discuss every security threat and attacks related to IoT in one paper, important one's are discussed. Now comes the operational technology. Security challenges and mechanisms have been studied in various fields, but current operational technology research has not comprehensively investigated. The authors in [40] and [41] focuses on security threats and attacks on industrial control system (ICS), which comprise only a subset of network systems consisting OT systems. The threats related to SCADA systems and ICS is addressed in [42] and for better understanding, first start with OT security. Initially, OT systems were not connected to the internet, so there was no need for OT cyber security.

As IT OT network converged due to expansion of digital innovation initiatives, businesses started addressing specific issues and their solutions which lead to OT security. OT security involves practices and techniques that are used to monitor or control physical process, and systems; protect assets, people and their information [43]. Operational technology consists of Industrial Control Systems (ICSs), which comprises Supervisory Control and Data Acquisition (SCADA), Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), Distributed Control Systems (DCSs) and several dedicated systems that help in monitoring and controlling the operations.

V. Problems of OT

OT plays a vital role in several sectors of critical infrastructure, like healthcare, power plants and water utilities. Unfortunately, most OT systems run on old versions and hardware, which makes them vulnerable to many exploits like spying, phishing, ransomware attacks, etc. [9, 40]. Some of the challenges to OT that makes it vulnerable to many threats and exposures:

- Lack of antivirus protection
- Lack of skilled professionals
- Convergence with IT
- Outdated systems
- Vulnerable communication protocols
- Insecure connections

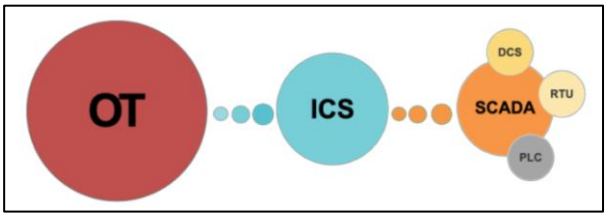

Fig. 2. Components of OT

VI. IT/OT Convergence

IT/OT convergence can be referred as the integration of information technology (IT) computing systems and operational technology (OT) monitoring systems. By converging IT and OT, not just only technologies but also teams and operations are combined [44]. Industrial Internet of Things (IIoT) systems comprise of intelligent devices interconnected sensors, control systems, network modules, and other devices to monitor, analyze, and control the physical devices. These systems differ from traditional industrial control systems (ICS) by being connected extensively to other systems and people, increasing the diversity and scale of the systems [45].

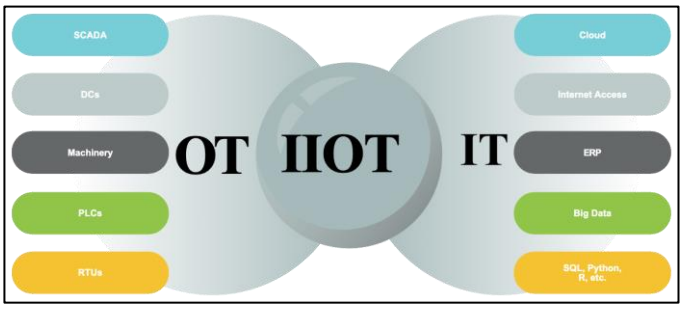

Fig. 3. IT/OT Convergence

This convergence has improved the productivity, efficiency and performance of current operational processes and enabled the creation of new methods of operational data. But with the salient advantages, there are some disadvantages as well. Systems originally designed to be isolated are now exposed to attack. Successful attacks on the IIoT system are likely to be

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 07, July-2021

as serious as the worst industrial hazards ever such as the Chernobyl disaster. These accidents will affect the human life in various forms, also impact the environment causing serious issues to the plants, atmospheric layers, etc. There is also technical damage such as exposing sensitive data during an attack, disrupting operations and destroying the system. The effects of attacks on IIoT systems are widespread and sometimes it can be compared to major natural disasters and it come from malicious intent. Properties of various components and their nature results in key characteristics of an IIOT system: security, safety, reliability, privacy and resilience [46].

VII. THE PURDUE MODEL

The Purdue model is derived from the Purdue Enterprise Reference Architecture (PERA) model by ISA-99, and used as a concept model to represent internal network segmentations. The Purdue model consists of three zones namely, enterprise zone (IT), industrial zone (OT), and demilitarized zone (DMZ) [47, 48].

A. Enterprise Zone (IT)

This is IT network zone, where primary business tasks such as supply chain management and scheduling are performed by using Enterprise Resource Planning (ERP) and System Application and Products (SAP) systems. Enterprise zone can further be divided into two levels:

Level 5 – Enterprise Network: This is a network where corporate level business operations are performed. It uses collected data gathered from subordinate systems to report the inventory and production status.

Level 4 – Business Planning and Logistics Systems: This level involves all the IT systems that support the production process at the plant. Systems at level 4 usually include file servers, database servers, application servers, email clients, etc.

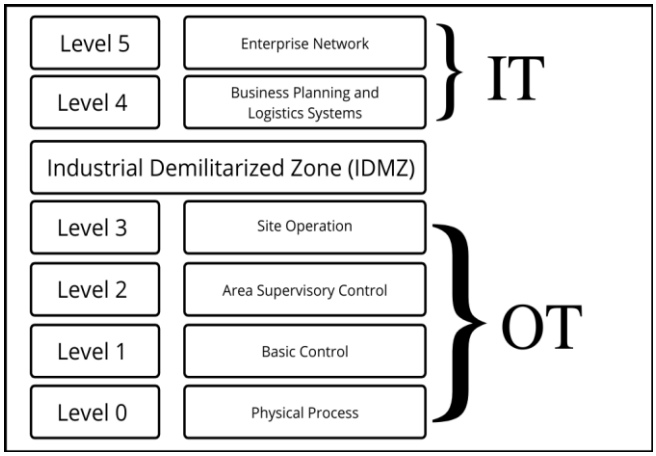

Fig. 4. The Purdue Model

B. Industrial Demilitarized Zone (IDMZ)

This zone lies between the enterprise zone and manufacturing zone which is used as a barrier to restrict direct communication between IT and OT systems. This zone helps in inspecting and separating the overall architecture. By preventing the direct communication between IT and OT, it helps in securing the system by shutting down the IDMZ in case anything malicious happens that can compromise the system in the IDMZ. IDMZ systems typically include database replication servers, Microsoft domain controllers, and proxy servers.

C. Manufacturing Zone (OT)

This zone consists of all the networks, devices, control and monitoring systems. The manufacturing zone is divided into four levels:

Level 3 – Site Operations: This level includes production systems, control functions, and plant monitoring. At this layer production data is collected from lower levels which can be send to higher level systems.

Level 2 – Area Supervisory Control: In this level, supervising, monitoring, and controlling the specific parts of the system is carried out with the help of HMI systems. This level usually includes HMIs and supervisory control systems.

Level 1 – Basic Control: Physical processes can be analyzed and controlled at this level. This level includes basic control operations like, move actuators, open valve, start motor, etc.

Level 0 – Physical Process: In this level, actual physical process is carried out and product is made. This level includes devices and sensors that directly interact and control the manufacturing operations.

The ICS-CERT alert contains information related to the vulnerability of Industrial Control System reported to them. Common Security Vulnerabilities in Industrial Control Systems Reported to ICS-CERT in 2009 and 2010 [39]:

- Improper Input Validation
- Improper Authentication
- Credential Management
- Permissions, Privilege, and Access Controls
- Cryptographic Issues
- ICS Security Configuration and Maintenance

VIII. MOST ATTACKS THAT ARE DONE FOR GAINING ACCESS TO IOT DEVICES CAN BE DONE TO OT SYSTEMS AS WELL. MAJOR SECURITY ATTACK FACED BY OT SYSTEMS ARE DISCUSSED BELOW:

A. HMI-Based Atttacks

HMI system is core hub, by exploiting this, an adversary can cause physical damage to the SCADA systems. Sayegh et al. [49] showed different types of attacks that can be done to compromise the SCADA systems by exploiting vulnerabilities in HMI system.

Replay attack was carried out by exploiting the Screen Data Protection Function which is used for password-based authentication to gain permission to program the HMI. Zero-Length Fragmentation Attack was performed by sending IP packets whose length are equal to zero. These type of attacks crashes the HMI systems.

DoS attack on HMI systems can be performed by exploiting certain functions such as HMI touch screen can be made unresponsive by flooding large number of random IP packets or SYN packets. HTTP port can be attacked by sending large number of HTTP requests.

Countermeasures: To protect HMI systems, there are number of technologies which needs to be implemented. Firewalls and Intrusion Detection Systems should be configured to monitor and isolate the suspicious events on the network. Security Information and Event Management (SIEM) technology can be used for reviewing security logs from

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 07, July-2021

firewalls, intrusion detection systems and other devices. Use of Demilitarized Zones (DMZs) and Virtual Lans helps in securing the network by separating into different smaller subnetworks [50].

B. Hacking Modbus Slaves

Modbus is one the communication protocols for ICS. Modbus communication happens between one Master (i.e., HMI system or Operational PC) and several Slaves (i.e., Programmable Logic Controllers). Modbus Master and Slaves communicate in plaintext and there is no authentication at all [51]. Attacker can leverage this vulnerability to access Slave's register and coils by sending similar query packets to Modbus slave [52]. Metasploit Framework can be used to achieve this goal. Below are the steps to perform this attack:

- First scan and find all Modbus Slaves connected to LAN or Modbus gateway of the target network. Set "RHOST" to the target IP address.

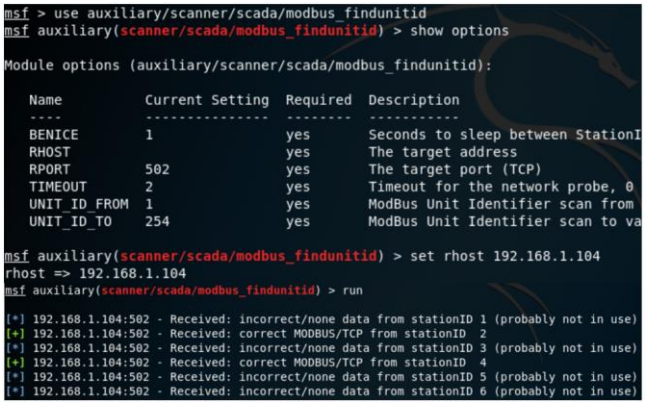

Fig. 5. Scanning Modbus Slaves

- Use "modbusclient" attack module to read or write registers and coils on target Modbus Slave.

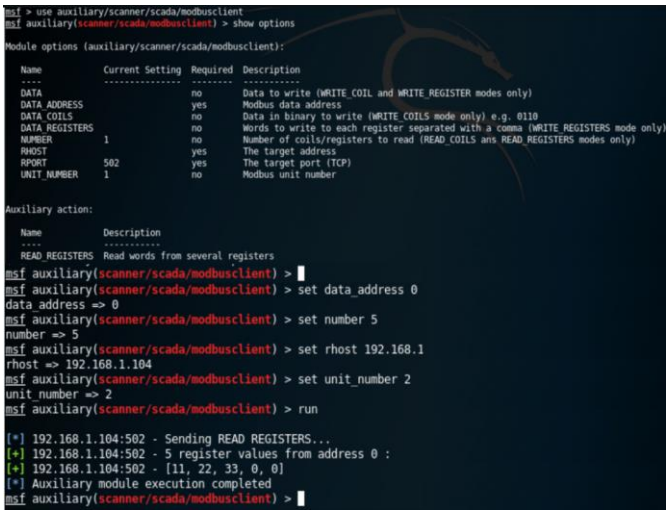

Fig. 6. Reading Modbus Slave Registers

- To write multiple coil values, change "ACTION" option to "WRITECOILS"

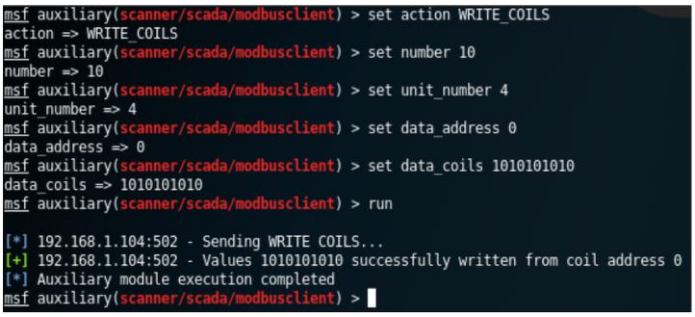

Fig. 7. Writing coils of Modbus Slave Registers

Possible Mitigation Techniques: To reduce the attack surface, restrict the read and write access to Modbus registers and coils not required for control implementations. PLC program vulnerabilities should be analysed and removed for extra security.

C. Command Injection Attacks

This attack can be performed by an adversary by injecting false command sequence into the system which compromises the security of the control systems. Morris et al. [53] discussed about how an adversary can perform command injection attacks to overwrite C code, ladder logic, and register settings of remote terminal devices that are present at remote locations to control the physical processes. Malicious command injection attack is one of the worst attacks that can happen to an industrial control system. Upon successful attack, an adversary can interrupt device communications, manipulate interrupt controls, and perform intended modifications to the device.

Further, command injection attacks were grouped into three categories, namely Malicious State Command Injection (MSCI) attacks, Malicious Parameter Command Injection (MPCI) and, Malicious Function Code Injection (MFCI).

Countermeasures: To mitigate the risk of command injection attack, the best practise that can be done is input validation. Usage of secure function while developing any program for ICS can prevent this attack to happen. Rasapour et al. [54] proposed a framework based on Intrusion Detection System to detect command injection attacks on Industrial Control Systems.

IX. ACKNOWLEDGEMENT

This work was supported by my research guide, Ankita Agarwal, Assistant Professor, CSE, BBDITM. I am thankful to the guide and faculties of my college who helped us in this research.

X. CONCLUSION

This paper has discussed the security challenges and attacks faced by Internet of Things (IoT) and Operational Technology (OT) systems. During analysis of different attacks, steps to reproduce different attacks was proposed, as to provide clear understanding of the vulnerabilities and attacks. In addition, the paper proposes different countermeasures to mitigate that risk and some theoretical models that governs the operations of these systems.

The study that has been carried out during this research aims to provide new knowledge of security attacks and their

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 07, July-2021

mitigation techniques in OT and IoT systems. They are derived from generalization of the results of previous studies and some are proposed after analysing the current trends among security communities.

XI. REFERENCES

[1] S. M. P. Keyur KPatel, Internet of things-iot: Definition, characteristics, archi- tecture, enabling technologies, application and future challenges, International Journal of Engineering Science and Computing 6 (2016) 6122–6125.

[2] M. H. Miraz, M. Ali, P. S. Excell, R. Picking, A review on internet of things (iot), internet of everything (ioe) and internet of nano things (iont), in: 2015 Internet Technologies and Applications (ITA), 2015, pp. 219–224. doi:10.1109/ITechA.2015.7317398.

[3] What is operational technology, {https:// www.fortinet.com/solutions/industries/ scada-industrial-control-systems/ what-is-ot-security}.

[4] A.Hahn,OperationalTechnologyandInformationTechnologyinIndustrial Con- trol Systems, Springer International Publishing, Cham, 2016, Ch. 4, pp. 51–68. doi:10.1007/978-3-319-32125-7 4.

[5] A. RADOVICI, C. RUSU, R. S ¸ERBAN, A survey of iot security threats and so- lutions, in: 2018 17th RoEduNet Conference: Networking in Education and Re- search (RoEduNet), 2018, pp. 1–5. doi:10.1109/ROEDUNET.2018.8514146.

[6] I. Cvitic´, M. Vujic´, S. Husnjak, Classification of security risks in the iot envi- ronment, in: 26TH DAAAM INTERNATIONAL SYMPOSIUM ON INTEL- LIGENT MANUFACTURING AND AUTOMATION, 2015, pp. 0731–0740. doi:10.2507/26th.daaam.proceedings.102.

[7] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, G. Pantziou, A survey on jamming attacks and countermeasures in wsns, IEEE Communications Surveys Tutorials 11 (4) (2009) 42–56. doi:10.1109/SURV.2009.090404.

[8] M. Kuzlu, C. Fair, O¨. Gu¨ler, Role of artificial intelligence in the internet of things (iot) cybersecurity, Discover Internet of Things, Springer 1 (02 2021). doi:10.1007/s43926-020-00001-4.

[9] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, Internet of things (iot): A vi- sion, architectural elements, and future directions, Future Generation Computer Systems 29 (07 2012). doi:10.1016/j.future.2013.01.010.

[10] L. Farhan, S. T. Shukur, A. E. Alissa, M. Alrweg, U. Raza, R. Kharel, A survey on the challenges and opportunities of the internet of things (iot), in: 11th International Conference on Sensing Technology, ICST 2017, Institute of Electrical and Electronics Engineers (IEEE), United States, 2017, pp. 1–5. doi:10.1109/ICSensT.2017.8304465.

[11] Y. Yang, L. Wu, G. Yin, L. Li, H. Zhao, A survey on security and privacy is- sues in internet-of-things, IEEE Internet of Things Journal 4 (2017) 1250–1258. doi:10.1109/JIOT.2017.2694844.

[12] O. Stan, R. Bitton, M. Ezrets, M. Dadon, M. Inokuchi, O. Yoshinobu, Y. Tomo- hiko, Y. Elovici, A. Shabtai, Extending attack graphs to represent cyber-attacks in communication protocols and modern it networks, IEEE Transactions on De- pendable and Secure Computing (2020) 1–1doi:10.1109/TDSC.2020.3041999.

[13] M.Almiani,A.Razaque,L.Yimu,M.J.khan,T.Minjie,M.Alweshah,S.Atiewi, Bluetooth application-layer packet-filtering for blueborne attack defending, in: 2019 Fourth International Conference on Fog and Mobile Edge Computing (FMEC), 2019, pp. 142–148. doi:10.1109/FMEC.2019.8795354.

[14] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, G. Pantziou, A survey on jamming attacks and countermeasures in wsns, Communications Surveys & Tu- torials, IEEE 11 (2009) 42–56. doi:10.1109/SURV.2009.090404.

[15] B. Danev, H. Luecken, S. Capkun, K. El Defrawy, Attacks on physical-layer identification, in: Proceedings of the Third ACM Conference on Wireless Net- work Security, WiSec '10, Association for Computing Machinery, New York, NY, USA, 2010, pp. 89–98. doi:10.1145/1741866.1741882.

[16] P. D. Hung, B. T. Vinh, Vulnerabilities in iot devices with software-defined radio, in: 2019 IEEE 4th International Conference on Computer and Communication Systems (ICCCS), 2019, pp. 664–668. doi:10.1109/CCOMS.2019.8821711.

[17] Y. Sun, X. Wang, X. Zhou, Jamming attack in wsn: A spatial perspective, in: Proceedings of the 13th International Conference on Ubiquitous Computing, Ubi- Comp '11, Association for Computing Machinery, New York, NY, USA, 2011, pp. 563–564. doi:10.1145/2030112.2030214.

[18] K. Li, X. Yu, H. Zhang, L. Wu, X. Du, P. Ratazzi, M. Guizani, Security mech- anisms to defend against new attacks on software-defined radio, in: 2018 Inter- national Conference on Computing, Networking and Communications (ICNC), 2018, pp. 537–541. doi:10.1109/ICCNC.2018.8390381.

[19] J. H. P. Mikail Mohammed Salim, Shailendra Rathore, Distributed denial of ser- vice attacks and its defenses in iot: a survey, in: The Journal of Supercomputing, Vol. 76, Springer International Publishing, 2020, pp. 5320–5363.

[20] A. Roohi, M. Adeel, M. A. Shah, Ddos in iot: A roadmap towards security coun- termeasures, in: 2019 25th International Conference on Automation and Com- puting (ICAC), 2019, pp. 1–6. doi:10.23919/IConAC.2019.8895034.

[21] M. M. Hossain, M. Fotouhi, R. Hasan, Towards an analysis of security issues, challenges, and open problems in the internet of things, in: 2015 IEEE World Congress on Services, 2015, pp. 21–28. doi:10.1109/SERVICES.2015.12.

[22] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, M. Ylianttila, Pauthkey: A per- vasive authentication protocol and key establishment scheme for wireless sensor networks in distributed iot applications, International Journal of Distributed Sen- sor Networks 10 (7) (2014) 357430. arXiv:https://doi.org/10.1155/2014/357430, doi:10.1155/2014/357430.

[23] S. Al Salami, J. Baek, K. Salah, E. Damiani, Lightweight encryption for smart home, in: 2016 11th International Conference on Availability, Reliability and Security (ARES), 2016, pp. 382–388. doi:10.1109/ARES.2016.40.

[24] L.Hu,H.Wen,B.Wu,F.Pan,R.F.Liao,H.Song,J.Tang,X.Wang,Cooperative jamming for physical layer security enhancement in internet of things, IEEE In- ternet of Things Journal 5 (1) (2018) 219–228. doi:10.1109/JIOT.2017.2778185.

[25] G. Lessa dos Santos, V. T. Guimara˜es, G. da Cunha Rodrigues, L. Z. Granville, L. M. R. Tarouco, A dtls-based security architecture for the internet of things, in: 2015 IEEE Symposium on Computers and Communication (ISCC), 2015, pp. 809–815. doi:10.1109/ISCC.2015.7405613.

[26] J.-L. Tsai, N.-W. Lo, A privacy-aware authentication scheme for distributed mo- bile cloud computing services, IEEE Systems Journal 9 (3) (2015) 805–815. doi:10.1109/JSYST.2014.2322973.

[27] Y. Afek, A. Bremler-Barr, S. L. Feibish, Zero-day signature extraction for high- volume attacks, IEEE/ACM Transactions on Networking 27 (2) (2019) 691–706. doi:10.1109/TNET.2019.2899124.

[28] A. A. Pammu, K.-S. Chong, W.-G. Ho, B.-H. Gwee, Interceptive side channel attack on aes-128 wireless communications for iot applications, in: 2016 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS), 2016, pp. 650–653. doi:10.1109/APCCAS.2016.7804081.

[29] M. A. N. Abrishamchi, A. H. Abdullah, A. David Cheok, K. S. Bielawski, Side channel attacks on smart home systems: A short overview, in: IECON 2017 - 43rd Annual Conference of the IEEE Industrial Electronics Society, 2017, pp. 8144–8149. doi:10.1109/IECON.2017.8217429.

[30] H. H. YF Alias, Mohd Anuar Mat Isa, Timing attack: An analysis of prelimi- nary data, Journal of Telecommunication, Electronic and Computer Engineering (JTEC) 9 (2017) 29–32.

[31] K. Pongaliur, Z. Abraham, A. X. Liu, L. Xiao, L. Kempel, Securing sensor nodes against side channel attacks, in: 2008 11th IEEE High Assurance Systems Engi- neering Symposium, 2008, pp. 353–361. doi:10.1109/HASE.2008.26.

[32] P. Kocher, J. Jaffe, B. Jun, Differential power analysis, in: Advances in Cryptology — CRYPTO' 99, Springer Berlin Heidelberg, 1999, pp. 388–397. doi:10.1007/3-540-48405-1 25.

[33] E. Prouff, M. Rivain, R. Bevan, Statistical analysis of second order differen- tial power analysis, IEEE Transactions on Computers 58 (6) (2009) 799–811. doi:10.1109/TC.2009.15.

[34] S. Skorobogatov, R. Anderson, Optical fault induction attacks, in: Lecture Notes in Computer Science, Vol. 2523, 2002, pp. 2–12. doi:10.1007/3-540-36400-5 2.

[35] E. Biham, A. Shamir, Differential fault analysis of secret key cryptosystems, in: Advances in Cryptology — CRYPTO '97, Springer Berlin Heidelberg, Berlin, Heidelberg, 1997, pp. 513–525. doi:10.1007/BFb0052259.

[36] I. Hafeez, M. Antikainen, S. Tarkoma, Protecting iot-environments against traffic analysis attacks with traffic morphing, in: 2019 IEEE International Conference on Pervasive Computing and Communications

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 07, July-2021

Workshops (PerCom Workshops), 2019, pp. 196–201. doi:10.1109/PERCOMW.2019.8730787.

[37] S. V. GM Deepa, G SriTeja, An overview of acoustic side-channel attack, In- ternational Journal of Computer Science & Communication Networks 3 (2013) 15.

[38] J. Longo, E. De Mulder, D. Page, M. Tunstall, Soc it to em: Electromagnetic side-channel attacks on a complex system-on-chip, in: Cryptographic Hardware and Embedded Systems – CHES 2015, Springer Berlin Heidelberg, 2015, pp. 620–640. doi:10.1007/978-3-662-48324-4 31.

[39] K. Mai, Side Channel Attacks and Countermeasures, Springer New York, 2012, Ch. 8, pp. 175–194. doi:10.1007/978-1-4419-8080-9 8.

[40] M. Marali, S. D. Sudarsan, A. Gogioneni, Cyber security threats in indus- trial control systems and protection, in: 2019 International Conference on Ad- vances in Computing and Communication Engineering (ICACCE), 2019, pp. 1–7. doi:10.1109/ICACCE46606.2019.9079981.

[41] S. Abe, M. Fujimoto, S. Horata, Y. Uchida, T. Mitsunaga, Security threats of internet-reachable ics, in: 2016 55th Annual Conference of the Society of Instrument and Control Engineers of Japan (SICE), 2016, pp. 750–755. doi:10.1109/SICE.2016.7749239.

[42] R. Piggin, Industrial systems: cyber-security's new battlefront [information tech- nology operational technology], Engineering Technology 9 (8) (2014) 70–74. doi:10.1049/et.2014.0810.

[43] Operational technology security – focus on securing industrial control and au- tomation systems [online].

[44] CISCO, It/ot convergence white paper, https://www.cisco.com/c/dam/en_us/solutions/industries/manufacturing/ ITOT-convergence-whitepaper.pdf (2018).

[45] C. V. Glenn Murray, Michael N. Johnstone, The covergence of it and ot in critical infrastructure, https://doi.org/10.4225/75/5a84f7b595b4e (December 2017).

[46] R. Martin, S. Schrecker, H. Soroush, J. Molina, J. LeBlanc, F. Hirsch, M. Buch- heit, A. Ginter, H. Banavara, S. Eswarahally, K. Raman, A. King, Q. Zhang, P. MacKay, B. Witten, Industrial internet security framework technical report, Industrial Internet Consortium (09 2016). doi:10.13140/RG.2.2.28143.23201.

[47] T. J. Williams, H. Li, PERA and GERAM—enterprise reference architectures in enterprise integration, Springer US, 1999, pp. 3–30. doi:10.1007/978-0-387- 35385-2 1.

[48] P. Ackerman, Industrial Cybersecurity, Packt, 2017.

[49] N. Sayegh, A. Chehab, I. H. Elhajj, A. Kayssi, Internal security at- tacks on scada systems, in: 2013 Third International Conference on Communications and Information Technology (ICCIT), 2013, pp. 22–27. doi:10.1109/ICCITechnology.2013.6579516.

[50] K. Stouffer, J. Falco, K. Scarfone, Guide to industrial control systems (ics) security, in: NIST Special Publication 800-82 Revision 2, 2015, pp. 0–247. doi:10.6028/NIST.SP.800-82r2.

[51] E. I. Evangelia, Vulnerabilities of the modbus protocol, https://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/11394/Evangeliou_1508.pdf?sequence=1&isAllowed=y (Febru- ary 2018).

[52] M. Hoffman, Vulnerabilities on the wire: Mitigation for insecure ics device communication, https://www.sans.org/reading-room/whitepapers/ICS/paper/39425 (February 2020).

[53] T. Morris, W. Gao, Industrial control system cyber attacks, in: ICS-CSR, 2013. doi:10.14236/ewic/ICSCSR2013.3.

[54] F. Rasapour, E. Serra, H. Mehrpouyan, Framework for detecting control com- mand injection attacks on industrial control systems (ics), in: 2019 Seventh In- ternational Symposium on Computing and Networking (CANDAR), 2019, pp. 211–217. doi:10.1109/CANDAR.2019.00035