A Multi-Layer Industrial-IoT Attack Taxonomy: Layers, Dimensions, Techniques and Application

Syed Ghazanfar Abbas
IRIL-KICS
University of Engineering & Technology
Lahore, Pakistan
ghazanfar.abbas@kics.edu.pk

Fabiha Hashmat
IRIL-KICS
University of Engineering & Technology
Lahore, Pakistan
fabiha.hashmat@kics.edu.pk

Ghalib A. Shah
IRIL-KICS
University of Engineering & Technology
Lahore, Pakistan
ghalib@kics.edu.pk

***Abstract*—Industrial IoT (IIoT) is a specialized subset of IoT which involves the interconnection of industrial devices with ubiquitous control and intelligent processing services to improve industrial system's productivity and operational capability. In essence, IIoT adapts a use-case specific architecture based on RFID sense network, BLE sense network or WSN, where heterogeneous industrial IoT devices can collaborate with each other to achieve a common goal. Nonetheless, most of the IIoT deployments are brownfield in nature which involves both new and legacy technologies (SCADA (Supervisory Control and Data Acquisition System)). The merger of these technologies causes high degree of cross-linking and decentralization which ultimately increases the complexity of IIoT systems and introduce new vulnerabilities. Hence, industrial organizations becomes not only vulnerable to conventional SCADA attacks but also to a multitude of IIoT specific threats. However, there is a lack of understanding of these attacks both with respect to the literature and empirical evaluation. As a consequence, it is infeasible for industrial organizations, researchers and developers to analyze attacks and derive a robust security mechanism for IIoT. In this paper, we developed a multi-layer taxonomy of IIoT attacks by considering both brownfield and greenfield architecture of IIoT. The taxonomy consists of 11 layers 94 dimensions and approximately 100 attack techniques which helps to provide a holistic overview of the incident attack pattern, attack characteristics and impact on industrial system. Subsequently, we have exhibited the practical relevance of developed taxonomy by applying it to a real-world use-case. This research will benefit researchers and developers to best utilize developed taxonomy for analyzing attack sequence and to envisage an efficient security platform for futuristic IIoT applications.**

***Index Terms*—Attack, Industrial Control Systems, IIoT, Multi-layer Taxonomy, SCADA**

I. Introduction

The Industrial Internet of Things (IIoT) refers to the application of Internet of Things (IoT) in industrial sector to monitor, collect, exchange, process and analyze data gained from industrial devices [1]. IIoT empowers industries with self-organizing and self-optimizing capabilities via real time monitoring and control of production environment [2] [3] [4]. The potential technologies which utilize IoT to enable IIoT for facilitating improvement in productivity, efficiency, and revenue are Artificial Intelligence (AI), Big Data, Radio Frequency Identification (RFID), and Wireless Sensor Network (WSN) and cognitive computing.

Industrial Internet of Things (IIoT) encompasses a vast amount of disciplines such as energy production, manufacturing, agriculture, healthcare, retail, transportation, logistics and many more [5]. According to a recent estimation of Gartner, there were approximately 4.80 billion IIoT assets present in the world in the year 2019. Further, Gartner has predicted that in the year 2020, this number will increase by 21 percent [5]. However, in spite of these manifold opportunities, the advancement of IIoT leads to a multitude of cyber security risks. Additionally, in 2019, Talos published 87 advisory articles about IoT and ICS vulnerabilities [5] Nevertheless, most of the practical IIoT deployments are brown-field in nature which involves both new and legacy technologies (SCADA). The merger of these technologies causes high degree of cross-linking and decentralization which ultimately provides support for numerous access points into the industrial network. Therefore, industrial organizations are not only vulnerable to SCADA attacks but also to IIoT specific attacks. Conventional industrial systems consist of resource powerful devices, for instance computers and smart phones, while on the other hand IIoT have resource constrained devices such as sensors [6] [7]. This scenario make the protection of IIoT components more expensive and made the system vulnerable to advance types of attacks such as node capturing, and tampering [8]. In addition to that IIoT nodes are mostly connected to insecure wireless medium which is constrained in nature in terms of energy, processing power and memory [6].

The attack span and probability of attack conduction have increased with the integration of IoT technology in industrial sector as industries are also exposed to IoT specific attacks. Therefore, a common in depth understanding and knowledge of various types of IIoT attacks is indispensable for the documentation, communication and derivation of mitigation measures of attack. This paper has focused on provisioning of a method for the in-depth analysis and categorization of IIoT specific attacks, thus providing aid in resisting new attacks and improving IIoT security. For this, we have developed a dedicated IIoT specific attack taxonomy. There are so many taxonomies present in the literature [9] [10] [11] [12] [13] related to IoT attacks but they are of little use when conducting a IIoT specific security assessment. The developed taxonomy focuses on adversaries whose primary goal is to

978-1-6654-0392-4/20/$31.00 ©2020 IEEE
DOI 10.1109/TrustCom50675.2020.00249

disrupt an industrial control process, destruction of property by causing temporary or permanent damage and further creation of knowledge base which could effectively characterize and describe post compromise adversary behavior in IIoT domain.

The proposed taxonomy consists of 11 layers which are: *Initial Access, Execution, Persistence, Evasion, Discovery, Lateral Movement, Collection, Command and Control, Inhibit Process Control* and *Impact*. These layers presents attack conduction steps in a sequenced manner. Our developed multi-layer taxonomy provides an objective methodology to analyze vulnerabilities at a deeper level of granularity. Contrary to this, linear or horizontal taxonomies [15] [16] [17] [18] present in the literature are helpful only for understanding the features of a particular attack and does not aid in reducing the subjectivity of the process of attack. Our developed taxonomy begin with a high level of abstraction and progressively go lower in minute details to identify techniques and tactics of specific attack. Each layer is further divided into dimensions. These dimensions are used to further refine the way of conduction of attack. There are total 94 dimensions present in the taxonomy. Each dimension consist of possible attack techniques which could be used for the conduction of specific dimension attack. We have identified approx. 100 IIoT attack techniques.

To sum up, our developed taxonomy is primarily of value to risk assessment management, security analysts' system designers and as well as network administrator of IIoT domain. Following are the major contributions of this paper. Fig. 1 provides a comprehensive overview of key contributions in the paper.

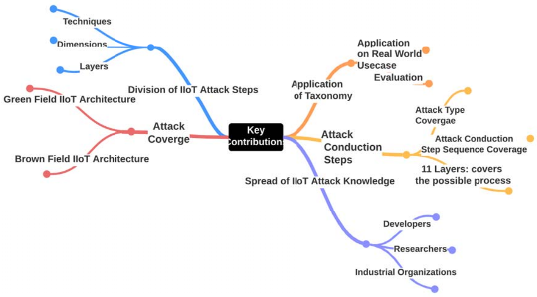

Techniques
Dimensions
Layers
Division of IIoT Attack Steps
Green Field IIoT Architecture
Attack Coverge
Brown Field IIoT Architecture
Key Contributions
Application of Taxonomy
Application on Real World Usecase
Evaluation
Attack Conduction Steps
Attack Type Covergae
Attack Conduction Step Sequence Coverage
11 Layers: covers the possible process
Spread of IIoT Attack Knowledge
Developers
Researchers
Industrial Organizations

Fig. 1. Technical Key Contributions of Paper

- *Attack Coverage for Greenfield and Brownfield IIoT Architectures:* Development of Multi-Layer Attack Taxonomy for attack coverage of both Greenfield IIoT architectures and Brownfield IIoT architectures (IIoT + Legacy technologies).
- *Attack Conduction Steps and Types Coverage:* The 11 layers of the proposed taxonomy are presented in a attack conduction step sequence. It covers the possible process of attack starting from initial access to its impact on the industrial environment.
- *Application of Taxonomy:* We further contributes in this paper by the application of developed taxonomy on a real world use-case.
- *Knowledge of IIoT Attacks:* A taxonomy of IIoT attacks based on various layers, dimensions, techniques is presented. The developed taxonomy contributes theoretically to the knowledge of IIoT attacks by providing a source to identify extensive security considerations which are prevalent in industrial sector.

The organization of the paper is as follows. In Section II, we have presented our developed Multi-Layer IIoT Attack Taxonomy8. Section III presents the application of taxonomy on a real world use-case. Finally, Section IV concludes the paper.

II. Multi-layer IIoT Attack Taxonomy

In this section, we have presented our taxonomy which consists of IIoT attack techniques, dimensions and impact. The taxonomy consist of 11 layers, 94 dimensions, and approximately 100 techniques as shown in Fig. 3 Layers in the taxonomy are presented in attack conduction sequence manner. It covers the possible sequence of attack starting from initial access to its impact. Further, the layers are divided into dimensions. These dimensions represents the type of attacks which could be conducted under the specific taxonomy layer. Associated attack techniques are stated along with every dimension. In Fig. 2 shows the relationship of IoT, IIoT and SCADA technologies. It elaborates that IIoT is a part of IoT and SCADA is the part of IIoT incase of brownfield architecture of IIoT which includes legacy technologies such as SCADA. This clearly exhibits that SCADA attacks are the part of IIoT attacks. Some of the examples of IIoT techniques are also shown in 4. Following is the description of taxonomy.

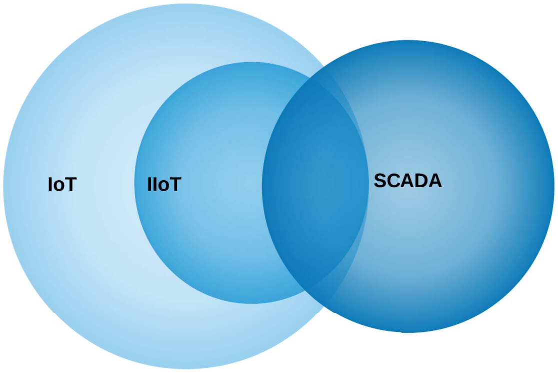


Fig. 2. Relationship between IoT, IIoT and SCADA

A. Layer 1: Initial Access

Initial access layer consists of the techniques which adversaries use to get into the IIoT environment. The purpose of these techniques is to compromise the operational technologies assets and external remote services. The operational technologies may include physical devices, software and operational equipment. Initial access mechanism may also intervene in the operation of outside devices such as controllers or removable media to infect IIoT operations. Initial Access Layer's dimensions are: Internet Accessible Device, Exploit Public Facing Application, Wireless Compromise, Data Historian Compromise, Engineering Workstation Compromise, External Remote Services, Replication through Removable Media, Drive by Compromise, Supply Chain Compromise and Spear-phishing attachment.

B. Layer 2: Execution

Execution consists of attacks that enables adversary to run adversary-controlled code on a local or remote system in an industrial environment. Execution of the malicious code may depend upon on the end user or may trigger on the execution of specific function or event. Execution layer's dimensions are: Scripting, Graphical User Interface, Project File Infection, Command Line Interface, Execution through API, Program Organization Units, Change Program State and Man in the Middle.

C. Layer 3: Persistence

Persistence consists of attacks and techniques which are used to maintain continuous unauthorized access to the industrial environment. Execution layer's dimensions are: System Firmware, Program Download, Hooking, Module Firmware, Valid Accounts and Project File Infection.

D. Layer 4: Evasion

Avoidance of detection of adversary both from human operators and technical defenses throughout adversary operation is called evasion. Evasion layer's dimensions are: Utilize/Change Operating Mode, Rogue Master Device, Spoof Reporting Message, Indicator Removal on Host, Masquerading, Exploitation for Evasion and Rootkit.

E. Layer 5: Discovery

Discovery consists of techniques which are used to gain information about the industrial environment such as information about internal network, control system devices and running processes. These techniques help adversaries to identify that which network they could control and perform malicious operations. Discovery layer's dimensions are: Network Sniffing, Input/Output Module Discovery, Network Connection Enumeration, Remote System Discovery, and Control Device Identification.

F. Layer 6: Lateral Movement

Lateral movement techniques are used by adversaries to enter and control remote systems present on the network. These techniques make use of default credentials, known account credentials and vulnerable services for entering into the control systems present on the network. Lateral Movement Layer's dimensions are: Valid Accounts, Program Organization Unit, Remote File Copy, Default Credentials, Exploitation of Remote Services, and External Remote Services. .

G. Layer 7: Collection

Collection consists of attack techniques in which the adversary tries to obtain contextual feedback such as device role identification or gathering system schematics in an industrial environment. Collection layer's dimensions are: Program Upload, Point and Tag Identification, Monitor Process State, Location Identification, Automated Collection, Detect Program State, Data from Information Repositories, I/O Image, Role Identification, Screen Capture and Detect Operating Mode.

H. Layer 8: Command and Control

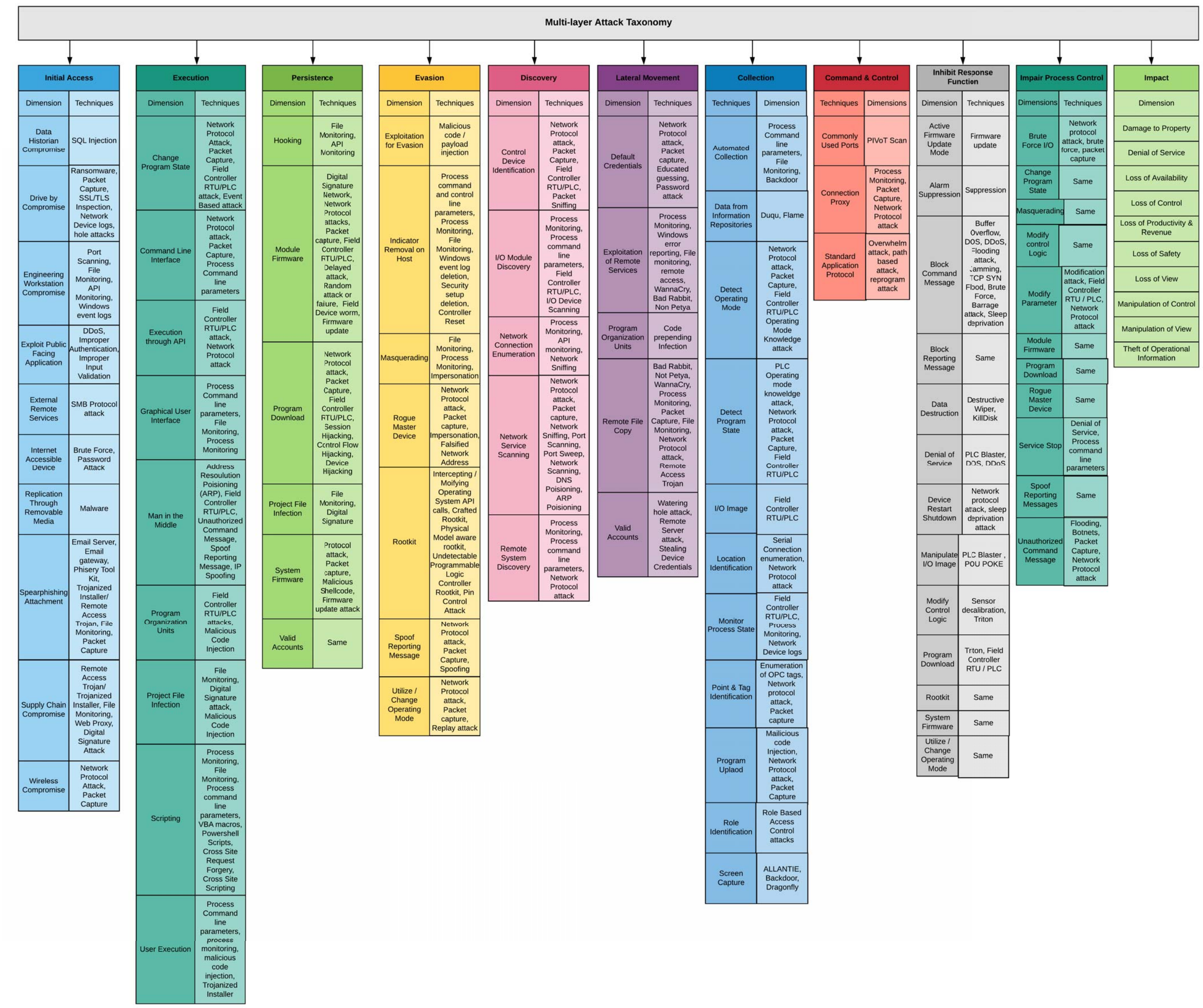
Command and control consists of techniques that adversaries utilize to send unauthorized commands to compromised systems, devices and controllers in the industrial environment. The compromised assets may include HMIs, servers, data historians and engineering workstations. Command and Control layer's dimensions are: Standard Application Layer Protocol, Connection Proxy, and Commonly Used Ports.

I. Layer 9: Inhibit Response Function

Inhibit response function consist of techniques which adversaries use to hide feedback coming from industrial systems related to safety, quality assurance, and operator intervention function which respond back in case of failure, hazard or unstable state. Inhibit Response function layer's dimensions are: Utilize/Change Operating Mode, Manipulate I/O Image, Modify Alarm Settings, Modify Control Logic, Program Download, Rootkit, System Firmware, Active Firmware Update Mode, Block Reporting Message, Block Command Message, Data Destruction, Device Restart/Shutdown, Denial of Service, and Alarm Suppression.

J. Layer 10: Impair Process Control

Impair process control consist of techniques which adversaries use to malfunction control logic and cause adverse effects on the processes being controlled in the targeted industrial environment. In addition to that, these techniques could also include blockage or manipulation of reporting messages and control logic. Impair Process Control layer's dimensions are: Unauthorized Command Message, Service Stop, Spoof Reporting Message, Modify Parameter, Program Download, Change Program State, Masquerading, Modify Control Logic, Rogue Master Device, Brute for I/O and Module Firmware.



Multi-layer Attack Taxonomy	

Initial Access	
Dimension	Techniques
Data Historian Compromise	SQL Injection
Drive by Compromise	Ransomware, Packet Capture, SSL/TLS Inspection, Network Device logs, hole attacks
Engineering Workstation Compromise	Port Scanning, File Monitoring, API Monitoring, Windows event logs
Exploit Public Facing Application	DDoS, Improper Authentication, Improper Input Validation
External Remote Services	SMB Protocol attack
Internet Accessible Device	Brute Force, Password Attack
Replication Through Removable Media	Malware
Spearphishing Attachment	Email Server, Email gateway, Phisery Tool Kit, Trojanized Installer/ Remote Access Trojan, File Monitoring, Packet Capture
Supply Chain Compromise	Remote Access Trojan/ Trojanized Installer, File Monitoring, Web Proxy, Digital Signature Attack
Wireless Compromise	Network Protocol Attack, Packet Capture

Execution	
Dimension	Techniques
Change Program State	Network Protocol Attack, Packet Capture, Field Controller RTU/PLC attack, Event Based attack
Command Line Interface	Network Protocol attack, Packet Capture, Process Command line parameters
Execution through API	Field Controller RTU/PLC attack, Network Protocol attack
Graphical User Interface	Process Command line parameters, File Monitoring, Process Monitoring
Man in the Middle	Address Resoulution Poisioning (ARP), Field Controller RTU/PLC, Unauthorized Command Message, Spoof Reporting Message, IP Spoofing
Program Organization Units	Field Controller RTU/PLC attacks, Malicious Code Injection
Project File Infection	File Monitoring, Digital Signature attack, Malicious Code Injection
Scripting	Process Monitoring, File Monitoring, Process command line parameters, VBA macros, Powershell Scripts, Cross Site Request Forgery, Cross Site Scripting
User Execution	Process Command line parameters, process monitoring, malicious code injection, Trojanized Installer

Persistence	
Dimension	Techniques
Hooking	File Monitoring, API Monitoring
Module Firmware	Digital Signature Network, Network Protocol attacks, Packet capture, Field Controller RTU/PLC, Delayed attack, Random attack or faiure, Field Device worm, Firmware update
Program Download	Network Protocol attack, Packet Capture, Field Controller RTU/PLC, Session Hijacking, Control Flow Hijacking, Device Hijacking
Project File Infection	File Monitoring, Digital Signature
System Firmware	Protocol attack, Packet capture, Malicious Shellcode, Firmware update attack
Valid Accounts	Same

Evasion	
Dimension	Techniques
Exploitation for Evasion	Malicious code / payload injection
Indicator Removal on Host	Process command and control line parameters, Process Monitoring, File Monitoring, Windows event log deletion, Security setup deletion, Controller Reset
Masquerading	File Monitoring, Process Monitoring, Impersonation
Rogue Master Device	Network Protocol attack, Packet capture, Impersonation, Falsified Network Address
Rootkit	Intercepting / Moifying Operating System API calls, Crafted Rootkit, Physical Model aware rootkit, Undetectable Programmable Logic Controller Rootkit, Pin Control Attack
Spoof Reporting Message	Network Protocol attack, Packet Capture, Spoofing
Utilize / Change Operating Mode	Network Protocol attack, Packet capture, Replay attack

Discovery	
Dimension	Techniques
Control Device Identification	Network Protocol attack, Packet Capture, Field Controller RTU/PLC, Packet Sniffing
I/O Module Discovery	Process Monitoring, Process command line parameters, Field Controller RTU/PLC, I/O Device Scanning
Network Connection Enumeration	Process Monitoring, API monitoring, Network Sniffing
Network Service Scanning	Network Protocol attack, Packet capture, Network Sniffing, Port Scanning, Port Sweep, Network Scanning, DNS Poisioning, ARP Poisioning
Remote System Discovery	Process Monitoring, Process command line parameters, Network Protocol attack

Lateral Movement	
Dimension	Techniques
Default Credentials	Network Protocol attack, Packet capture, Educated guessing, Password attack
Exploitation of Remote Services	Process Monitoring, Windows error reporting, File monitoring, remote access, WannaCry, Bad Rabbit, Non Petya
Program Organization Units	Code prepending Infection
Remote File Copy	Bad Rabbit, Not Petya, WannaCry, Process Monitoring, Packet Capture, File Monitoring, Network Protocol attack, Remote Access Trojan
Valid Accounts	Watering hole attack, Remote Server attack, Stealing Device Credentials

Collection	
Techniques	Dimension
Automated Collection	Process Command line parameters, File Monitoring, Backdoor
Data from Information Repositories	Duqu, Flame
Detect Operating Mode	Network Protocol attack, Packet Capture, Field Controller RTU/PLC Operating Mode Knowledge attack
Detect Program State	PLC Operating mode knowledge attack, Network Protocol attack, Packet Capture, Field Controller RTU/PLC
I/O Image	Field Controller RTU/PLC
Location Identification	Serial Connection enumeration, Network Protocol attack
Monitor Process State	Field Controller RTU/PLC, Process Monitoring, Network Device logs
Point & Tag Identification	Enumeration of OPC tags, Network protocol attack, Packet capture
Program Uplaod	Mailicious code Injection, Network Protocol attack, Packet Capture
Role Identification	Role Based Access Control attacks
Screen Capture	ALLANTIE, Backdoor, Dragonfly

Command & Control	
Techniques	Dimensions
Commonly Used Ports	PIVoT Scan
Connection Proxy	Process Monitoring, Packet Capture, Network Protocol attack
Standard Application Protocol	Overwhelm attack, path based attack, reprogram attack

Inhibit Response Function	
Dimension	Techniques
Active Firmware Update Mode	Firmware update
Alarm Suppression	Suppression
Block Command Message	Buffer Overflow, DOS, DDoS, Flooding attack, Jamming, TCP SYN Flood, Brute Force, Barrage attack, Sleep deprivation
Block Reporting Message	Same
Data Destruction	Destructive Wiper, KillDisk
Denial of Service	PLC Blaster, DOS, DDoS
Device Restart Shutdown	Network protocol attack, sleep deprivation attack
Manipulate I/O Image	PLC Blaster , P0U POKE
Modify Control Logic	Sensor decalibration, Triton
Program Download	Triton, Field Controller RTU / PLC
Rootkit	Same
System Firmware	Same
Utilize / Change Operating Mode	Same

Impair Process Control	
Dimensions	Techniques
Brute Force I/O	Network protocol attack, brute force, packet capture
Change Program State	Same
Masquerading	Same
Modify control Logic	Same
Modify Parameter	Modification attack, Field Controller RTU / PLC, Network Protocol attack
Module Firmware	Same
Program Download	Same
Rogue Master Device	Same
Service Stop	Denial of Service, Process command line parameters
Spoof Reporting Messages	Same
Unauthorized Command Message	Flooding, Botnets, Packet Capture, Network Protocol attack

Impact
Dimension
Damage to Property
Denial of Service
Loss of Availability
Loss of Control
Loss of Productivity & Revenue
Loss of Safety
Loss of View
Manipulation of Control
Manipulation of View
Theft of Operational Information

Fig. 3. Multi-layer IIoT Attack Taxonomy

K. Layer 11: Impact

Impact consist of effects which adversaries have caused during destruction, disruption or manipulation of the control system operations, processes and devices. Impact layer's dimensions are: Theft of Operational Information, Damage to Property, Loss of Availability, Loss of Control, Loss of View, Loss of Productivity and Revenue, Manipulation of View, Denial of View, Loss of Safety, Denial of Control, and Manipulation of Control.

III. Application And Evaluation Of Taxonomy

After the completion of the development of IIoT Multi-Layer Attack Taxonomy, we validated it by its application on a real world use-case of an IIoT attack incident. For application of taxonomy, we have selected the use-case of a German Steel Factory which was attacked in 2014 [19]. We

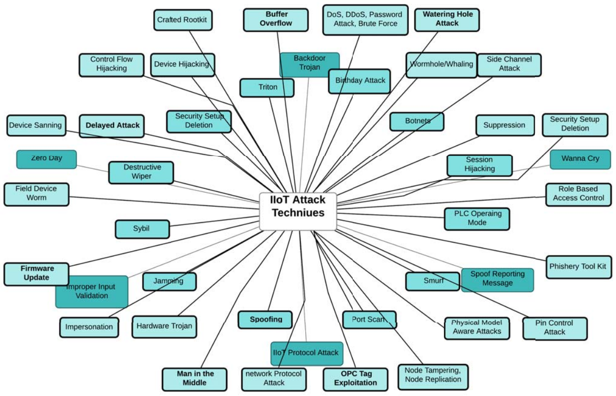


Fig. 4. Example of IIoT Attack Techniques

have divided the incident into manageable steps as shown in Fig.5, which helps us to segregate attack steps of the incident for analyzing incident in depth by utilizing our developed taxonomy. Following are the steps for attack.

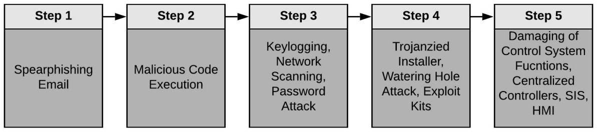

Step 1
Spearphishing Email
Step 2
Malicious Code Execution
Step 3
Keylogging, Network Scanning, Password Attack
Step 4
Trojanzied Installer, Watering Hole Attack, Exploit Kits
Step 5
Damaging of Control System Fucntions, Centralized Controllers, SIS, HMI

Fig. 5. German Steel Factory Attack Steps

- *Step 1:* The adversary gain access to the industrial system using spear phishing email. The phishing email consisted of a document which was infected with malicious code.
- *Step 2:* Once the spear phishing email was opened, the attached malicious code targets the vulnerabilities of an application on the system of steel factory. In this way, the adversary gain remote access to the industrial network.
- *Step 3:* In the third step, the adversary established a foothold on the industrial network system by compromising various workstations. For entering into the network, the adversary make use of key loggers, network scanning and password attacks.
- *Step 4:* After establishing a foothold on the industrial network, adversary started its further movement and damage using trojanized installers, exploit kits and watering hole attack.
- *Step 5:* System which are known to be impacted are:
  - Control system components and functions such as hot blast system, kinetic process model, mass and energy balancers.
  - Centralized controllers (PLCs)
  - Safety Instrumented System (SIS)
  - HMI

The combined effect of all these attacks, resulted in Loss of Control (LoC) of plant and its sub-functions which has lead to physical destruction.

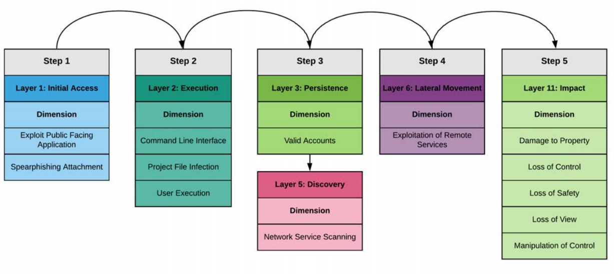


Fig. 6. Application of Multi-layer Attack Taxonomy on German Steel Factory Attack Steps

After dividing the incident into steps, we applied our developed taxonomy on it layer by layer. Fig.6 shows the application of taxonomy. We start with the first step of the attack in which the attacker initially tries to gain access of the industrial network using spear phishing email. Spear phishing attack technique is used in which the attacker make us of malicious email attachment to install malware on the targeted system of gain confidential information. According to our taxonomy, this attack can be classified under *Initial Access* layer and lies under its dimension of *Exploit Public Facing Application* and *Spear-phishing Attachment*.

In the second step, the attacker has installed a malware into any of the device or computer of industrial system via spear-phishing attachment execution (opening). The installed malware opened hidden doors in the system for the attacker to provide remote access to disrupt the plant operation. This attack lies under the second layer of the taxonomy which is *Execution* and lies under the dimension of *Command Line Interface*, *Project File Infection* and *User Execution*.

In the third step, the attacker has gained credential information of various industrial devices and workstations for the continuation of attack. For this attacker has used key-logging, password attack and network scanning. This behavior lies under the third layer of *Persistence* and under the dimension of *Valid Accounts*. In addition to that, this behavior may also lie under the layer of *Discovery* and under the dimension of *Network Service Scanning* because of the conduction of network scanning attack in this step.

In the fourth step, the attacker make further movement and conduction of attacks using trojanized installers, exploit kits and watering hole attack. According to our taxonomy, this step lies under the layer of *Lateral Movement* and under the dimension of *Exploitation of Remote Services*.

According to the damage information provided in Step 5 , this step lies under the layer of *Impact* and under the dimension of *Damage to Property, Loss of Control, Loss of Safety, Loss of View* and *Manipulation of Control*.

Our application of the taxonomy shows that the attack steps involved in the real world incident differ with respect to their unique characteristics, attack layers, attack dimensions and attack techniques. Our taxonomy, helps to illustrate the attack conduction in a structured way and provide means to analyze the attack deeply using layers and dimensions. Furthermore, it also helps to analyze the attack conduction pattern and provides a holistic view of the incident.

IV. Conclusion

The tally of attacks on Industrial-IoT and so the damage to industrial production system and revenue - continues to increase exponentially, provoked by high degree of cross linking and resource constrained nature of IoT devices. Yet, the techniques,complexity, impact of attacks on IIoT remain deficiently illustrated and unsatisfactorily understood. In response to this problem, we developed a multi-layer IIoT attack taxonomy.The taxonomy consist of 11 layers, 94 dimensions and approx.100 IIoT specific attack techniques. Layers represent the attack conduction steps of an incident in a timely fashion, starting from initial access to the impact of an incident. Each layer consist of dimensions which represents the possible types of attacks which fall under the category of that specific layer. With each dimension, we have mentioned possible IIoT attack techniques which could be used to exploit that specific dimension of IIoT.

To exhibit the application and practical usefulness of our developed IIoT attack taxonomy, we applied it to a real world attack use case of German Steel Factory. First, we divided the incident into single attack steps. Then, we mapped those attack steps to our taxonomy layers and further dimensions according to the nature of those steps. In this way, our taxonomy provided a holistic overview of an incident along with the attack conduction sequence, steps, and techniques. Additionally, it provides a foundation for researchers and developers to determine and analyze attacks in a structured manner in order to devise their mitigation measures.

REFERENCES

[1] Alasdair Gilchrist.Industry 4.0: the industrial internet of things.Springer, 2016.

[2] M Brettel, N Friederichsen, M Keller, and M Rosenberg. How virtualization, decentralization and network building change the manufacturing landscape: International journal of information and communication engineering, 8 (1), 37–44, 2014.

[3] Michael Rüßmann, Markus Lorenz, Philipp Gerbert, Manuela Waldner,Jan Justus, Pascal Engel, and Michael Harnisch. Industry 4.0: Thefuture of productivity and growth in manufacturing industries.Boston Consulting Group, 9(1):54–89, 2015.

[4] Agnieszka Radziwon, Arne Bilberg, Marcel Bogers, and Erik SkovMadsen. The smart factory: exploring adaptive and flexible manufacturing solutions.Procedia engineering, 69:1184–1190, 2014

[5] Securing Industrial IoT, (accessed April 26,2020). [Online]. Available: https://blogs.cisco.com/security/securing-industrial-iot/

[6] Tianbo Lu, Jinyang Zhao, Lingling Zhao, Yang Li, and Xiaoyan Zhang.Security objectives of cyber physical systems. In2014 7th International Conference on Security Technology, pages 30–33. IEEE, 2014

[7] Qi Jing, Athanasios V Vasilakos, Jiafu Wan, Jingwei Lu, and Dechao Qiu. Security of the internet of things: perspectives and challenges.Wireless Networks, 20(8):2481–2501, 2014.

[8] Fadele Ayotunde Alaba, Mazliza Othman, Ibrahim Abaker Targio-Hashem, and Faiz Alotaibi. Internet of things security: A survey.Journal of Network and Computer Applications, 88:10–28, 2017.

[9] Jayavardhana Gubbi,Rajkumar Buyya,Slave n Marusic,and Marimuthu Palani swami. Internet of things (iot): A vision, architectural elements, and future directions.Future generation computer systems,29(7):1645–1660, 2013.

[10] Simon Hansman and Ray Hunt. A taxonomy of network and computer attacks.Computers Security, 24(1):31–43, 2005

[11] Kai Zhao and Lina Ge. A survey on the internet of things security.In2013 Ninth international conference on computational intelligence and security, pages 663–667. IEEE, 2013.

[12] L Atzori, A Iera, and G Morabito. The internet of things: A survey comput. netw. 2010.

[13] Brendon Harris and Ray Hunt.Tcp/ip security threats and attack methods.Computer communications, 22(10):885–897, 1999.

[14] Engin Leloglu. A review of security concerns in internet of things.Journal of Computer and Communications, 5(1):121–136, 2016.

[15] ayasree Sengupta, Sushmita Ruj, and Sipra Das Bit. A comprehensive survey on attacks, security issues and blockchain solutions for iot and iiot.Journal of Network and Computer Applications, 149:102481,2020.

[16] Xingjie Yu and Huaqun Guo. A survey on iiot security. In 2019 IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS),pages 1–5. IEEE, 2019

[17] Zeinab Bakhshi, Ali Balador, and Jawad Mustafa. Industrial iot security threats and concerns by considering cisco and microsoft iot reference models.In2018 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), pages 173–178. IEEE, 2018.

[18] Hansong Xu, Wei Yu, David Griffith, and Nada Golmie. A survey on industrial internet of things: A cyber-physical systems perspective.IEEE Access, 6:78238–78259, 2018.

[19] Lee, RM. , MJ. Assante, and T. Conway. 2014. German steel mill cyber attack, (accessed 09 March 2020). [Online]. Available: https:// ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks$_{Facility.pdf}$/