ISSN 2347 - 3983
Volume 8. No. 9, September 2020
International Journal of Emerging Trends in Engineering Research
Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter59892020.pdf
https://doi.org/10.30534/ijeter/2020/59892020

Security Threats and Concerns, Firmware Vulnerability Analysis in Industrial Internet of Things

Vishnupriya Borra[1], Dr. Venkateswarlu S[2]
[1]M.Tech (Cyber Security and Digital Forensics) student, KLEF Deemed to be University, Vaddeswaram, India, 182034002@kluniversity
[2] Professor, Dept. of CSE, KLEF Deemed to be University, Vaddeswaram, India,somu23@kluniversity.in

ABSTRACT

This paper includes Internet of Things(IOT), Industry 4.0, Industrial Internet of Things (IIOT).Industrial IOT applications and sectors which are used them. The basic architecture of Industrial IOT. The protocols are used in these wireless sensor networks using machine to machine communication. The communication or data transfer among these industrial devices using Industrial Internet. This paper characterize security concerns and threats in Industrial IOT. This paper also presents identification of vulnerabilities, backdoors and password leaks or weak passwords are in the IOT devices. These IOT devices are used in the smart factories or industries which are used for efficient Human to machine communication. This paper represents firmware vulnerability analysis. This analysis includes the firmware unpacking and reverse engineering. This analysis using the specified tools. This paper includes possible attack surfaces are based on vulnerabilities of the Industrial Internet of Things with in the security standards. The security standard is the IOT attack surface area of OWAPS Internet of things project.

Key words: Industrial Internet, Industrial Internet of Things, Industry 4.0, Internet of Things, machine to machine communication, vulnerabilities, wireless sensor networks.

1.INTRODUCTION

Internet of things are system of interconnected computing devices and embedded devices using internet. The embedded devices connected with smart interfaces for their communication [1].The applications of IoT are smart homes, environment monitoring, health care systems, energy management, building automation and transportation [1].Internet of things (IOT) are used for Machine to Machine (M2M) communication in the industries or factories. This revolution in Industrial sector is Industry4.0. The Industry 4.0 includes IOT devices, Automation Techniques such as AI (Artificial Intelligence), Machine Learning, Deep Learning and data analytics. Industrial IoT will revolutionize factory and industrial segmentations by presenting excellence [1].The benefits of Industrial IoT are greater efficiency, accuracy, scalability, time saving, money saving and predictive maintenance. Industries or organizations involve their operations in Industrial IoT are used in logistics, manufacturing, construction, supply chain [10].

1.1Basic Architecture of Industrial IoT:

The basic architecture of Industrial IoT as shown in below figure 1.In this architecture, there are three layers are as a reference from IoT architectural structure. Because Industrial IoT is a subset of IoT. The layers in Industrial IoT architecture are Perception layer, Network layer and Application layer. Perception layer consists of sensors, controllers, actuators, surveillance cameras, alarms are interconnected by independent wired or wireless local area networks to an edge IIoT gateways [2]. These gateways connect to Industrial network, which are in Network layer. The Industrial network is a network of Industrial Internet for communication, routers, switches and other network infrastructure. The application layer consists of PLCs, Databases, Message Buses, SCADA systems, MES systems and ERP.

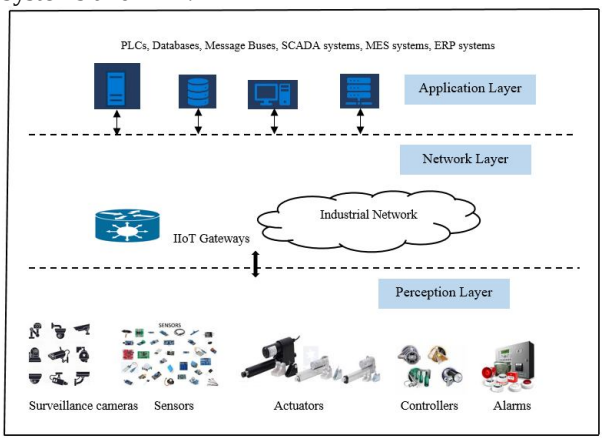

Figure 1: Basic architecture of Industrial IoT

1.2Machine to Machine (M2M) Communication Protocols for IIoT:

Communication protocols are used for delivery, routing and storage of the information without the necessity of implementing different mechanisms in different devices or

applications [3].The most used protocols among machine to machine communication are:

1.2.1 IPV6 over Low Power Wireless Personal Area Network (6LoWPAN):

An Internet Protocol version 6 (IPv6) over low-power wireless personal area networks (6LoWPAN) standard used for development of IoT and M2M applications. This protocol enables IP-based M2M devices to connect to the Internet. A necessary application is to monitor the manufacturing process in industry. In this application where a number of sensors, actuators and controllers to achieve monitoring, active control and automation [3].

1.2.2 Message Query Telemetry Transport (MQTT):

MQTT protocol is used in routing process. It deploys different routing mechanisms. They are one-to-one, one-to-many or many-to-many, to make the connection for IoT and M2M connected devices[3]. This protocol is publish /subscribe messaging transport protocol designed for M2M telemetry in low bandwidth environments[4].

1.2.3 Advanced Message Queuing Protocol (AMQP):

AMQP is used for communications over TCP. This protocol implements asynchronous publish/subscribe approach for communication over TCP. Data latency, reliability, bandwidth requirement, memory and code footprints are implemented in the application layer, which are in IOT communications [4]. AMQP supports message-oriented communication [3]. AMQP implements TLS/SSL security over TCP. AMQP send messages from publishers to subscribers among using message queues and exchange method in broker [3], [4].

1.2.4 Constrained Application Protocol(CoAP):

COAP is a web transfer protocol. This protocol supports unicast and multicast requests for use networks and in constrained devices. It is using request and response structure of communication between the end points. The clients sending requests with using an URI. They can receive response in the form of GET,PUT, POST and DELETE resources from the server [3]. The messages exchange communication over on UDP between endpoints. COAP provides security with Datagram Transport Layer Security. COAP supports both unicast and multicast communication [4].

1.2.5 Extensible Messaging and Presence Protocol (XMPP):

XMPP is a TCP communication protocol based on XML used for real-time messaging, online presence and request-response services [3].Clients communicate through a distributed network and without using a central broker. XMPP uses publish/subscribe model. It provides security with authentication through SASL. And communication security through TLS.

1.2.6 Data Distribution Service (DDS):

DDS is publish-subscribe model protocol provides real-time M2M communication. It uses broker-less structure and provides multicasting. This protocol supports high reliability for its applications. Communication [3]. This protocol states a set of QoS policies. These policies contribute control on dynamic discovery, content-aware routing, filtering, fault tolerance and deterministic real-time behaviour [3].

2. SECURITY THREATS AND CONCERNS IN INDUSTRIAL IOT:

The security threats and concerns in Industrial IoT are as follows:

Metadata Spoofing: an intruder modify database and cause data integrity to be compromised. Then the attacker use system errors to bypass authentication and access target data [1].

SQL Injection: The attacker uses Structured Query Language (SQL) commands to steal contents within a database. SQL injection can be other forms of attacks like,(a) Remote command execution (b) Information disclosure,(c) Authentication Bypass, (d) Compromise Availability, (e) Compromise Data Integrity [1].

Resource Exhaustion: A large number of components in an integrated Industrial IoT system and each of them needs computing resources. Data communication, data storing, process management and all need resources. This is caused by bad design or inefficient implementation or resource leakages [1].If the system fails to resource distribution or resource leaks.

Ransom ware: This is a denial of access attack. With using malwares to target data using crypto virology techniques until the demanded ransom is fully paid to hackers. Ransomware will also migrate to Industrial IoT [1].

Malicious Attack: A malicious attacker attacks to target a service or data. This type of attack done by other type of techniques such as phishing, IP spoofing, DNS poisoning attacks or malicious code injection [1], [11].

Distributed Denial of Service (DDoS): DDoS is a denial of service performed by multiplatform and multi architecture systems are infected by malwares cause an attack the target system [1].In 2016,the Mirai IoT botnet was used by attackers to attack high-impact DDoS on the Dyn DNS service and caused an extended internet outage [5]. This Mirai IoT botnet is compromised internet-enabled digital video recorders (DVRs), surveillance cameras, and other internet-enabled embedded devices.

Brute force: In this type of attack to find the credentials of devices to gain access them. With using dictionary attack, cracking authentication detail techniques [1].

3. FIRMWARE VULNERABILITY ANALYSIS

The firmware is software of Internet of Things for working. Industrial Internet of Things (IIoT)is subset of Internet of Things which using cyber physical systems. This firmware has software errors. These are memory corruption flaws, command injection vulnerabilities and application logic flaws [6]. Firmware vulnerability analysis using security penetration testing. Which includes reverse engineering, static analysis and dynamic analysis to find vulnerabilities, password leaks and hidden backdoors [7].

Reverse engineering: The embedded firmware reverse engineering with open source tools are Binwalk and Firmware-mod-kit(FMK)are used for extract embedded firmware files. The extracting firmware includes firmware headers, Linux kernels, boot loaders and signatures of filesystems [7].

Static analysis using firmwalker, Johnny, Interactive Disassembler (IDA Pro). Firmwalker is a bash script run on extracted firmware of root folder and it gives information about password files, system configuration files, ssh key files, DB files, keywords, strings(are URLS,IP addresses and emails) and executables [7]. Johnny is a GUI for john the ripper tool for identifying passwords of password hash codes. Interactive Disassembler (IDA Pro) is used for code analysis and information about subroutines and API calls.

Firmware Analysis Toolkit (FAT) is a toolkit analyze firmware of embedded device to find vulnerabilities.It performs Dynamic analysis with the tools Firmadyne and QEMU [8].

4. RESULTS

In this section, we show three case studies of IoT devices are IP camera and two Wi-Fi routers. IP camera has authentication credentials in its firmware code. Take firmware from vendor website. Unzip the zip file with unzip command in terminal of Kalilinux platform and reverse engineering through Binwalk tool. Then run firmwalker on root folder of IP camera firmware. And it gives information in the firmwalker text file [9].Figure-2 shows the firmwalker result on cpio-root folder of IP camera and its credentials.

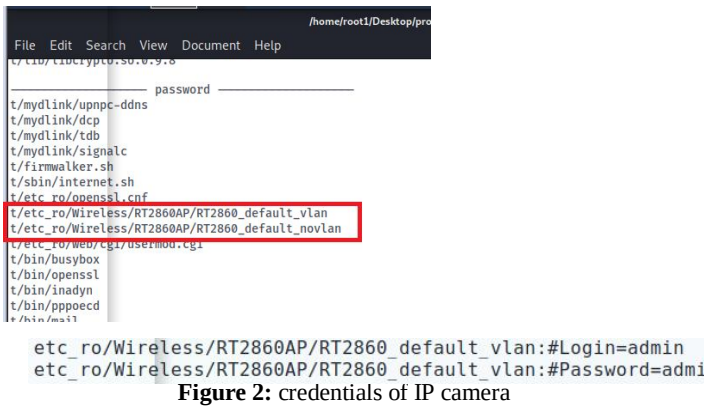

Figure 2: credentials of IP camera

Another router firmware download from vendor website. Unzip the zip file of firmware. Then reverse engineering the firmware file using binwalk tool. Then run the firmwalker on root folder of firmware of router. Credentials are decrypted using Johnny tool run on shadow file in path of the file is /etc/shadow. The user name and password are identified in the /etc/shadow file. Figure 3 shows firmwalker result and Johnny tool.

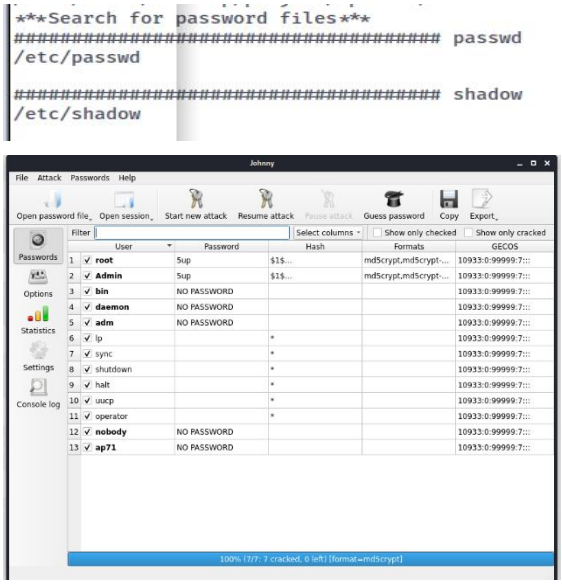

Figure 3: user name and password credentials

Another router has unknown string and it may be working as secret code or hidden backdoor.Router firmware download from vendor website. Unzip the zip file of firmware. Then reverse engineering the firmware file using binwalk tool. Then run the firmwalker on root folder in firmware of router. By manual analysis using “grep” command and to find telnetd suspicious command. The telnet assign with a Alpha networks: $image_sign in etc/init0.d/S80telnetd.sh file. And image_sign has the known string is wrgn28_dlob_dir412 in usr/sbin/login [7], [9]. Figure 4 shows the manual detection of telnetd, code of etc/init0.d/S80telnetd.sh and the unknown string.

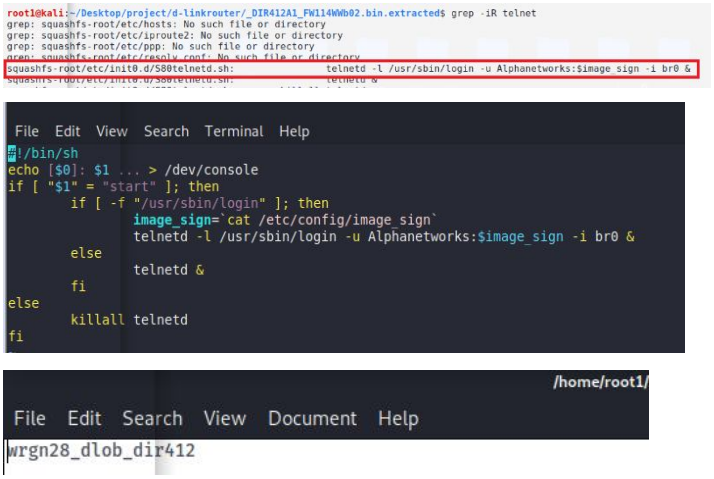

Figure 4: Security concern in router

5.CONCLUSION

In this paper we include Industrial IoT basic architecture, protocols and security threats and concerns. Find out security vulnerabilities such as password leakage, password hash cracking and security concern in Firmware of IP camera and two routers with firmware analysis method. This method include reverse engineering, manual analysis command and dynamic analysis tools. There is a need to find other network security threats with efficient way which cause modifications in firmware of Industrial IoT devices. Protect them effective and efficient mechanisms for improving security of Industrial IoT devices in Industrial Control Systems.

REFERENCES

[1] Zeinab Bakhshi, Ali Balador and Jawad Mustafa,**"Industrial IoT Security Threats and Concerns by Considering Cisco and Microsoft IoT reference Models**".*IEEE Wireless Communications and Networking Conference Workshops (WCNCW): TC-CPS: Time-Critical Cyber Physical Systems*,2018.

[2] Emiliano Sisinni, Abusayeed Saifullah, Song Han, Ulf Jennehag and Mikael Gidlund, "**Industrial Internet of Things: Challenges, Opportunities, and Directions**", *IEEE Transactions On Industrial Informatics*,vol.14,no. 11, Nov.2018.

[3] Alireza Esfahani, Georgios Mantas, Rainer Matischek, Firooz B. Saghezchi, Jonathan Rodriguez, Ani Bicaku, Silia Maksuti, Markus Tauber, Christoph Schmittner, and Joaquim Bastos, "**A Lightweight Authentication Mechanism for M2M Communications in Industrial IoT Environment"**,*IEEE Internet of Things*,vol.6,no.1,Feb.2019.

[4] Rahul Shokeen, Bharanidharan Shanmugam, Krishnan Kannoorpatti, Sami Azam, Mirjam Jonkman andMamoun Alazab, "**Vulnerabilities Analysis and Security Assessment Framework for the Internet of Things** ", *2019Cyber security and Cyber forensics Conference (CCC),* Melbourne, Australia,2019.

[10]M. Srilatha , V. H. P. Bhargava , A. R. Sridhar , P. Sainag , CH. Madhukar , "**Energy Efficient Secured Device Control using IOT**" , *International Journal of Emerging Trends in Engineering Research*, Vol. 8, No. 5, May 2020.

[11]Hitesh Mohapatra1, Subhashree Rath , Subarna Panda , Ranjan Kumar, "**Handling of Man-In-The-Middle Attack in WSN Through Intrusion Detection System**" ,*International Journal of Emerging Trends in Engineering Research*, Vol. 8, No. 5, May 2020.

[5] Qiao Yan, Wenyao Huang, Xupeng Luo, Qingxiang Gong, and F. Richard Yu "**A Multi-Level DDoS Mitigation Framework for the Industrial Internet of Things**", *IEEE Communications Magazine*,vol.56,no.2, Feb. 2018.

[6] Yan Shoshitaishvili, Ruoyu Wang, Christophe Hauser, Christopher Kruegel, Giovanni Vigna and UC Santa Barbara , "**Firmalice - Automatic Detection of Authentication Bypass Vulnerabilities in Binary Firmware**", NDSS '15, 8-11 February 2015, San Diego, CA, USA,2015 Internet Society, available at http://dx.doi.org/10.14722/ndss.2015.23294.

[7] Chin-Wei Tien, Tsung-Ta Tsai, Ing-Yi Chen and Sy-Yen Kuo, "**UFO - Hidden Backdoor Discovery and Security Verification in IoT Device Firmware**", *2018 IEEE International Symposium on Software Reliability Engineering Workshops*,D.O.C.:15-18 oct.2018,Memphis, TN, USA.

[8] Meriem Bettayeb , Qassim Nasir and Manar Abu Talib ,"**Firmware Update Attacks and Security for IoT Devices** ", ARABWIC 6th Annual International Conference on Arab Women in Computing (ArabWIC2019). ACM, Rabat, Morocco, 6 pages, available athttps://doi.org/10.1145/3333165.3333169.

[9] Pen testing IoT devices, available at "https://blog.mindedsecurity.com/2018/09/pentesting-iot-devices-part-1-static.html".