IoT Firmware Security

Name:-Ravi Pandey roll no:-54 registration no: 11910459

Abstract

The Internet of things is framework of connected thing's (sensor, refrigerator, smart phone, etc.) which change the sense we live, communicate, play, work and conduct business. Even though these things have such great affect in our lives, they prone to security issues and vulnerabilitie which always result in negative consequence's such as loss of integrity,confidentiality, and availability. Hence some user's are still skeptical about use of IoT. This papers explore the security problem that arise's due to IoT device firmware updatability. New vulnerabilitie's are uncovered all of the time. If a device is non upgradeable, then the vulnerability will exist for rest of the device's lifetime. As a countermeasure, it is imperative to design security measure's to enable automatic update of IoT device. This paper focuse on current research works based on IoT firmware update's with the aim of highlightings issue related with securities of firmware update. It specifically focuse on the security challenge's that

faces low end IoT device's and Low-powers Wide Area Networks. Keywords— Firmware Internet of Things, Firmware, Security, Low-end devices ,LPWAN.

INTRODUCTION

Internet of Things (IoT) has experienced exponential growth both in researchs and in industry. however, privacy and security remain challenge [1]. Several types of malicious method exist that attempt to compromise's the securities and expose's the privacy of the IoT device's[2]. These various maliciou's activitie are motivated by known Vulnerabilities that exist in IoT Therefore, it is important that after the initial deployment. the IoT device's need to stay updateds and well patched to mitigates subsequent security vulnerabilities which may lead to various attacks [3]. Internet of Things device's can be updated using wireless communication technologies categorized as Short Range Network's and Low Power Wide Area Network's (LPWANs). Short Range Networks include communication protocols such as Bluetooth, Wi-Fi, WiMax, ZigBee[4]. These communication protocols could not address the need's for IoT device's. which include long battery life low power consumption and long ranges data transmission. To

accommodate these needs the LowPower Wide Area Networks communication protocols were developed. This includes LoRa, NB-IoT, Sigfox, IQRF[5]. Both of these communication technologies present their own security challenges. For instances in LPWANs offer's long-ranges connectivity therefore it is more exposed to variou's attacks. One of the top hacks took place in 2015 know the jeep hack[6]. Two researchers took advantages of many vulnerabilities including the firmware update vulnerability, where reverse engineerings was performes on the firmware. As the results, the researcher were able to take control of a jeep using the vehicles Controller Area Network (CAN) bus, which enables communication between different element's on vehicle such as break's, steering wheel heaters, locks, headlights etc. They were able to send CAN messages taking control of variou's element of the vehicle to makes it speed up, slow down and even veer of the road. The lacks of security on firmware updates made this attack possible therefore, strong encryption mechanisms are required to ensures security during the firmware update. Firmware update is challenge in IoT due the variou's reasons such as resource constraint's devices since most of the present technology is not suitable's for the IoT devices due to their nature's and limitation like as storage and processing power. These limitations make it difficult to secure the updates for the IoT devices. Open Web Application Security Project (OWASP) has listed

vulnerabilities created on IoT that attacker's use to compromise IoT devices. This includes insufficient authentication/authorization, lack of transport encryption, privacy concerns, insufficient security configuration, poor physical security and insecure software firmware updates [7].As attackers, take advantages of these vulnerabilities one
of the recovery mechanisms would be to introduce a secure firmware update procedure . The purpose of the firmware update procedures is to fix bug's and improve device functionality[8]. If the initiated firmware update mechanism is insecures it could lead to compromises of the user data enable unauthorized control over the devices which can lead to launch more attack's against other devices. The contribution of this survey are:

- We discuss the overviews of over-the-air (OTA) update and the importants component that need security during the update process.

- The papers provide the security challenge that exist when updatings low-end IoT device's in LPWANs.

- This paper give's the present state of the art based of the firmware modified solutions presented by different researchers. The focus is based on the

specific type of IoT devices (Low-end IoT device – battery powered), which use's LPWANs for communication. Classify the existing studies based on what type of devices the existing mechanism are targeting (Low-end IoT devices and Medium/High-end IoT devices).

OVERVIEW OF FIRMWARE SECURITY THREATS

This section provide with the overviews of firmware update and common threat involved as the firmware is distributed from the manufacturers to the IoT device's. It look at the three main entities that need's to be secure namely firmware repository, communication channel and IoT device.

There are differents attack that can happen at different Level's as the firmware is transmitted to the IoT device's and

after the firmware has safely delivered to the IoT. Figure 1 depicts the possible threats in IoT.

1) Firmware manufacturers is the entities that produce's the new version of firmware images and distribute it

over the untrusted network.
2) The untrusted network communication channel may be eavesdropped by an attacker. An attacker can take hold of firmware image and extract sensitive data from it and the file can be changed and returned for a distribution.
3) Customer's got the firmware then distribute's it among the IoT devices.
4) The same attack's of insecure channels may take place as the firmware is distributeds from customers to IoT device. Additional risks maybe involved such as loading unauthorized firmware onto unauthorized devices or to completely abort the update procedure.
5) An attacker can extract sensitive information from the devices like the keys and even do attack's directly to the firmware like system-safety patch vulnerabilities, Firmware bricking[9]. Figure 1 depict the possible attack's at the communication level and physical layer. Therefore, the firmware need to be secures both in transits and at rest. Figure 1, also shows three main element's thats can be compromised during the update process namely firmware repository, communication path and IoT device.

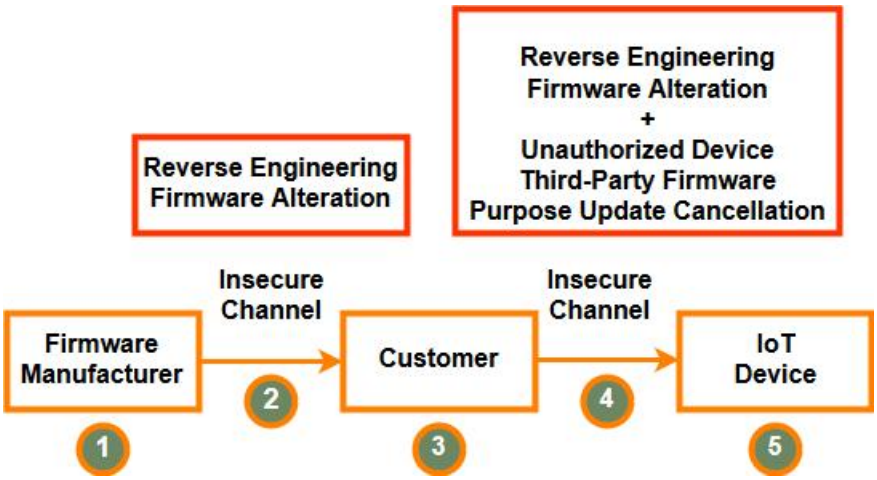

Fig 1.Possible attack's related with the firmware update[10]

Figure 1
depicts the possible attacks at the communication level and physical layer. Therefore, the firmware needs to be secure both in transits and at rests.
Figure 1
also shows three main element's that can compromised during the update process namely firmware repository, communication path and IoT device:

Firmware Repository

The firmware must securely stored on the repository. This is the initial step the attackers use to make attack possible. Attacker's can get hold the firmware in different way's such as obtaining it from the vendors google support,website and community forums, reversing the mobile application, sniffing

the OTA updates mechanism and dumping it from the devices[11]. Once firmware is obtained then reverse engineering can be performe to extract the sensitive informations such as Application Programming Interface (API) and encryption keys Access token, encryption algorithms, hard-coded credentials, sensitive URLs and more[12]. Therefore it is important to store the firmware on repository securely. The firmware must be encrypted and signed before it gets stored to the repository. Usually Advanced Encryption (AES) is use to ensure integrity and confidentiality of the firmware at rest. Apart from AES the XOR encryption[13] can be used to encrypt the firmware. To ensure authentication, confidentiality and integrity the firmware manufacturer must sign the firmware image using the private key, which is held secret. When firmware have this signature attache to it. device with the features enabled will validate the firmware before accepting to install it. The process of signing firmware is initiated through the computation of cryptographic hash value. The value is then signed with private key of a private/public key pair before the signature is attache to the firmware image figure 2 show this process.

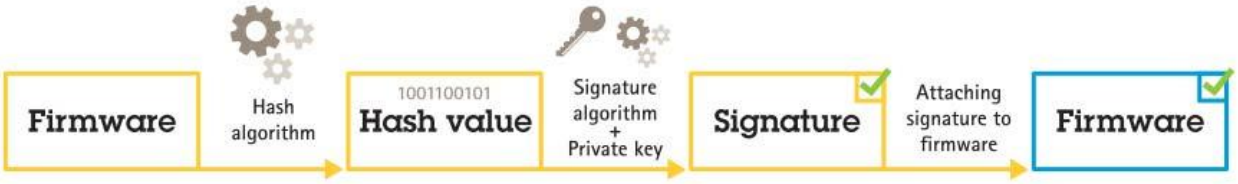

Fig 2: The process of signing firmware [14]

IoT Device

After the firmware have been securely delivere to the IoT devices then the firmware need's to be flashed. Before it get's flashed possibles attack could happen like as time-of check-to-time-of-use attack (TOCTOU). The security needs to be applied to ensure consistent integrity of the firmware [15], meaning the integrity of the firmware must be also checked after the firmware has been flashed to memory. The physical security of IoT devices is also required. Unnecessary ports such as JTAG and UART should be blocked to avoid any interruption in update process by adversaries[15]. There are two firmware update strategies can be taken to updates the IoT devices. The popular one is through the client-server model where the device manufacturers use servers (possibly using cloud providers) to distribute firmware updates to IoT client devices. This centralized approach exhibits a single point of failure for both the availability and the integrity of the firmware update [16]. The second strategy is blockchain-based. It has more

advantages over the client-server model by able to keep track of all events[17] (stored in the immutable ledger) associated with the firmware update. It provides manufacturers with the ability of using smart contracts to enforce the firmware updates conditions in a flexible manner. The smart contract (logic) is securely stored and decentralized on every peer on the network, and also consider to be permanently tamperproof [18], unlike the client-server logic, which is centralized and exposed to a single point of failure. The distributed nature of the blockchain frameworks makes blockchain ledger and smart contract to be resilient to network failures and cyberattacks.

PRIVACY AND SECURITY CHALLENGES

In this section we focuses on the security challenge's and privacy need specifics for the Low-End IoT devices. There are two main qualities explained which include's IoT devices, and the challenges faced with IoT communication/connectivity specific in LPWANs.

FIRMWARE UPDATE MECHANISM

This section look's at existing firmware update's mechanism available for the IoT. The literature is categorize based on what type of IoT device's the updates mechanisms are targeting i.e. low-end IoT devices,

Medium-end IoT devices/high-end IoT devices. On each of these categories the LWM2M/server-based, blockchain based mechanism can be found.

Firmware Targeting Low-End IoT Devices

In [10], author's presents the secure delivery of firmware Updates to the internet of thing's devices as well as a designs of safe and secure bootloader for radio-frequency identification reader. The main goals of author's was to finds out whether's it would be possible's to integrates security features like as AES, which is use for encryption as well as others security feature's into the existing IoT devices. Author's developed anapplication in order to encrypt the firmware images file and be able to flash the firmware in the device's. The application use's AES to encrypt the firmware files where the encryption key is required togethers with the initialization vector, which is an arbitrary number that can be used along with the encryption key. Authors concluded that it is possible to integrate such kind of encryption and it leaves more space to integrate other security techniques. The results show that minimum flash memory of 49.7 kB and RAM of 10 kB are required

CONCLUSION

The Internet of Thing's is growing exponential with lots of

the device's being deployed and connecteds to the internet. These device's are resources constrained and for this reasons, it Is tough to integrates the existings cryptographic's techniques since most of these require more resources. This has more effect it comes to firmware update. In this paper, we investigateds the security issues and challenges faced with the resources constrained devices with more focu's on low-end IoT devices. We first provide with the basics overview's of the existing threats in firmware update. The further discussed the security problems and challenge's faced in firmware update's with the resource-constrained devices in LPWANs. The current state-of-the-art was presented and categorized based on what types of the devices the mechanism's are targeting and the security approaches took by researchers were discussed.

REFERENCES

[1] K. R. Özyılmaz and A. Yurdakul, "Designing a blockchain-based
IoT infrastructure with Ethereum, Swarm and LoRa," pp. 1–6, 2018.
[2] Z. Alansari et al., "Internet of Things: Infrastructure, Architecture, Security and Privacy," in IEEE International Conference on Computing, Electronics & Communications Engineering, 2018, vol. 2018, no. August, pp. 211–238.
[3] A. Boudguiga et al., "Towards better availability and

accountability for IoT updates by means of a blockchain,” Proc. -
2nd IEEE Eur. Symp. Secur. Priv. Work. EuroS PW 2017, pp. 50–58, 2017.
[4] D. Ismail, M. Rahman, and A. Saifullah, “Low-power wide-area
networks,” pp. 1–6, 2018.
[5] Leverege LCC, An Introduction to the Internet of Things. .
[6] Z. Tyree, R. A. Bridges, F. L. Combs, and M. R. Moore, “Exploiting the Shape of CAN Data for In-Vehicle Intrusion Detection,” IEEE Veh. Technol. Conf., vol. 2018-Augus, pp. 1–5,
2019.
[7] OWASP, “OWASP Top 10 Internet of Things,” Salem Press Encycl. Sci., pp. 5–7, 2018.
[8] M. Kameswarao & P. Bhavya Sree, “a secured firmware update
procedure to prevent cross channel scripting attack in embedded devices,” Int. J. Electron. Commun. Eng., vol. 2, no. 2, pp. 161–168, 2013

[9] D. J. Chris, M. H. Saleem, M. Evanglopoulou, M. Cook, and R.

Harkness, “Defending Against Firmware Cyber Attacks on Safety-Critical Systems.”
[10] L. Kvarda, P. Hnyk, L. Vojtech, Z. Lokaj, M. Neruda, and T.
Zitta, “Software implementation of a secure firmware update solution in an IOT context,” Adv. Electr. Electron. Eng., vol. 14, no. 4Special Issue, pp. 389–396, 2016.

[11] R. A. Grimes, “IoT Hacking,” Hacking the Hacker, pp. 189–191,
2017.

[12] A. Gupta, The IoT hacker’s handbook [electronic resource]: A
practical guide to hacking the internet of things / Aditya Gupta. 2019.
[13] A. A. Tamimi, A. M. Abdalla, and P. O. Box, “An Image Encryption Algorithm with XOR and S - box,” pp. 166–169.
[14] A. Axis Communications, “Signed firmware, secure boot, and
TPM key storage in Axis products,” no. November, 2018.

[15] I. Makhdoom, M. Abolhasan, H. Abbas, and W. Ni, “Journal of
Network and Computer Applications Blockchain ’ s adoption in IoT : The challenges , and a way forward,” J. Netw. Comput. Appl., vol. 125, no. November 2018, pp. 251–279, 2019.
[16] L. Hang and D. H. Kim, “Design and implementation of an integrated iot blockchain platform for sensing data integrity,” Sensors (Switzerland), vol. 19, no. 10, 2019.
[17] B. Pichon, O. Kahl, B. Hammer, and J. S. Gray, “Blockchain - an
introduction,” vol. 6, no. 4, pp. 382–387, 2006.