PLOMS Journal of Artificial Intelligence (PLOMS AI)

PLOMS AI

Review Article

Internet of Things (IoT) Security Vulnerabilities: A Review

Rabie A. Ramadan[1,*]
Computer Engineering Department, Faculty of Engineering, Cairo, Egypt; rabie@rabieramadan.org
Correspondence: rabie@rabieramadan.org

Received: 30-12-2021; Accepted: 15-01-2022; Published: 21-01-2022

Abstract: The Internet of Things (IoT) collects and processes data from remote locations, substantially increasing the productivity of dispersed systems or individuals. Due to the restricted budget available for power consumption, IoT devices usually lack advanced data encryption and device authentication. The hardware components used in IoT devices are not high-end, and therefore, the integrity and security of the majority of IoT devices are in question. For instance, an adversary may include a Hardware Trojan (HT) during the manufacturing phase of IoT hardware devices to trigger data leakage or device failures in addition to other security issues. Here, we examine security risks to IoT in this paper, with a particular focus on attacks aimed at compromising the software, hardware, communication, and chip.

Keywords: Internet of Things; security; IoT; applications; physical security; smart cities.

I. Introduction

The Future Internet's objective is to provide an infrastructure that enables instant access to data about the physical world and its objects. Physical objects may be used in various application areas, including e-health, warehouse management, etc. Each application domain may use a variety of different physical devices. Each physical device has its own set of standards that must be followed to communicate with it. To accomplish the future Internet objective, a layered vision that enables data access is needed. The Internet of Things (IoT) is a concept that, via a layered architecture, seeks to connect the virtual world of information to the physical world of objects. The term "Internet of Things" is made up of two words: Internet and Things. The Internet is a term that refers to a worldwide network architecture that provides scalable, reconfigurable capabilities based on public, interoperable communication protocols. Things may be real things or devices, virtual objects, or information with identities, physical characteristics, and virtual personalities interacting intelligently. For example, a virtual object may represent an abstract unit of sensor nodes that includes information that enables it to be identified and discovered. Thus, IoT refers to objects that may transmit data from their physical environment to the Internet.

Typically, an IoT system consists of three main stages: data collection, data transmission, and data analysis. The first stage is responsible for data capturing, which is accomplished via sensor antennae and microcontrollers. Additionally, this level is referred to as a physical layer. The second step is data transmission, which is accomplished via an IoT hub, gateway, or network. The last step is data analysis, which comprises user interfaces and the back-end technology, which may be hosted in the cloud. Any compromise at those phases will result in the leakage of vital information from IoT devices. Numerous vulnerabilities have recently been discovered in IoT devices due to a lack of advanced encryption and authentication systems. Regrettably, no commercial security solution exists to defend against security threats. The digital industry has generated significant income and growth as a result of the increased connection. Smart manufacturing, smart supply chain, intelligent power grid, and smart cities have all experienced promising growth due to industry-level automation and control enabled by IoT devices.

In industry, IoT applications are used in many fields. The Amazon warehouse robots handle and deliver products using IoT. The robots utilize sensors to navigate the warehouse without human assistance. The robots interact with one another and with the central cloud system using Zigbee and Bluetooth protocols. However, widespread IoT device use has led to security and privacy issues. Also, low power Zigbee wireless protocol

is based on IEEE 802.15.4. The stack profile in IEEE 802.15.4 is network and application-based. Security keys for Zigbee are symmetric, and key sharing relies on the security model [1]. Vidgren has shown that the Zigbee key may be readily hacked [2].

As a consequence of the network weakness, the attacker gains control of the IoT device. The Cisco IoT reference model and layers are illustrated in Fig. 1 [3]. Sensor applications such as USB, WiFi, and embedded sensors are found at the physical layer. The sensor collects environmental data, such as temperature, pressure, acceleration, optical measurement, and gas. Generally, the sensor is new to the current systems. Consequently, every exposed layer may be used as an attack entry point.

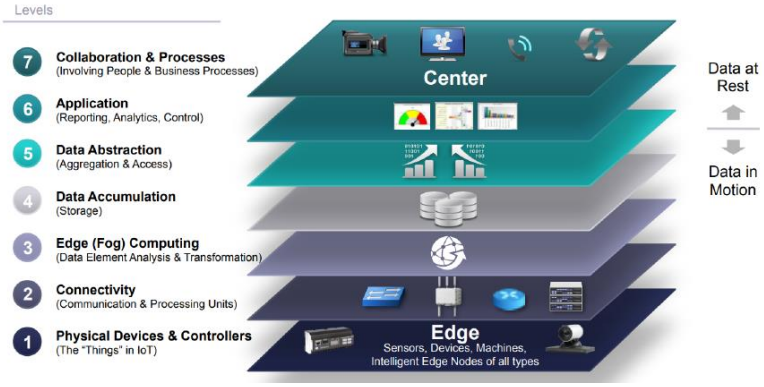

Figure 1. Internet of Things Cisco reference model [3]

The Internet of Things is built on a layered architecture that was created to meet the demands of various industries, businesses, and societies. A general layered architecture for the IoT consists of five levels, which are described below: [4]

1. **Physical Layer**
   This is a hardware layer that includes embedded systems, RFID tags, sensor networks, and other sensors. This hardware layer may collect data from a system or environment, process data, and facilitate communication.
2. **Gateway layer**
   This layer manages data and is responsible for publishing and subscribing to the "Things" services, message routing, and platform communication.
3. **Internet layer**
   The Internet layer is where routing occurs. Its primary function is to move packets across networks, and it enables network-to-network communication.
4. **Middleware layer**
   This layer is responsible for collecting and filtering data from hardware devices, performing information discovery, and regulating application access.
5. **Application layer**
   This layer delivers application services. The middleware layer provides these services to various applications and users in IoT-based systems. These services may be utilized in industries including logistics, retail, and healthcare.

According to Morgner [7], connecting the Zigbee Light Link base station to the host network may leak sensitive data. The author showed that distributing pre-defined keys results in insecure key management. According to Rodrigo [8], four Key Management System classes, a key pool framework, a mathematical framework, a negotiation framework, and a public key framework, are all inapplicable due to the required unique features. The key management system may be compromised due to IoT device energy consumption. According to Simplicio [9], large-scale deployment of lightweight key authentication management methods is insufficient. Remote access is possible for IPv6 and IPv4. Czyz showed that remote access to IoT devices using a command-line interface like Telnet is possible [5]. At the same time, IoT networks constantly manage big data, and data loss or denial of service may lead to network congestion and loss of control. According to Angrishi [6], malware may stay dormant in IoT devices and launch DDoS attacks once activated.

In 2013, a self-inflicted DDoS attack disrupted the Austrian and German power grids, flooding the central command center [8]. DDoS attacks may deactivate IoT device communication networks and protocols. In the future, the smart grid will be fully automated. The sensor network collects real-time data to monitor equipment and control plants. As a result, the plant operation loses network monitoring capabilities. Any malware or spyware attack may damage a nuclear power plant. Stuxnet is a programmed virus that may infect a plant through USB. Once compromised, the control system will spy on network activity to collect data. After obtaining enough data, Stuxnet began seizing the plant's control module and attempting to shut it down.

Security researchers usually start with a specific attack model, and it is restricted to one layer of the network for threat analysis and attack detection. The malicious efforts from many network levels may be combined in real-world attacks. Defending against attacks from various levels of IoT and sensor networks may be difficult, and a full-stack network is required for comprehensive evaluation. Defensive techniques' latency, power consumption, and side-channel leakage cannot be measured accurately by simulation-based assessment. Determining the robustness of IoT and sensor networks requires much more profound insight. A primary assembly using off-the-shelf devices and equipment is also inadequate to prototype complex IoT and sensor networks. The paper starts by reviewing IoT protocols, and then it explores the IoT variabilities at different layers. The next section explains the IoT vulnerabilities in terms of hardware, software, communication, and chip.

II. IoT Vulnerabilities

This section explores the IoT vulnerabilities based on four major areas: software, hardware, networks, and Chip vulnerabilities. In the following subsections, those variabilities are discussed.

A. Software Vulnerability

Vulnerabilities in software may have a devastating impact on the IoT. Through a software vulnerability, adversaries may gain control of the IoT device. Existing research demonstrates that a lack of security protection mechanisms directly contributes to the security issues associated with IoT devices. Chapman [8] and Rodrigues [9] exploit vulnerable settings or poor authentication on IoT devices. Max [10] performed a security analysis on a smart lock and discovered that the authentication and default configuration are unsafe and insecure. Fernandes et al. [11] showed how implicit trust compromises the security of Smart Home IoT devices when third-party apps are used. Costin investigated firmware upgrades and discovered a slew of vulnerabilities [12].

Malicious software often carries out a cyber-attack to leak data from a targeted attack to interrupt regular operation flow. The automated smart grid system is largely reliant on the Internet of Things monitoring network, and the sensor network collects real-time data to monitor the equipment and manage plants' conditions. Several power plants operate on earlier operating systems, such as Windows XP or Windows 7, and they are vulnerable to worm attacks through internet browsing since they lack a host firewall [13]. Once the Office network is compromised, the connected server is also affected, affecting other operating systems across the plant and control network.

Any transmission line or distribution system problem will go undetected by the control center, resulting in a blackout. In 2000, a Russian gas business was attacked by a Trojan virus, which resulted in the loss of control of the pipeline [7]. The Trojan software may collect information about the operation, which an adversary might use to launch an attack. Due to a software weakness, the attacker may obtain access to and control of the IoT. According to L. Markowsky [14], inadequate user authentication continues to leave IoT applications vulnerable. IoT devices are energy efficient, and software optimization further lowers power usage when deployed in remote locations. Firmware vulnerability is a significant security risk for IoT devices since it may interrupt their normal operation. Costin [15] extracted the password in plaintext, 109 private RSA keys, and 56 SSL certificates from the 428 implanted firmware files.

B. Hardware Vulnerability

To collect data in real-time, the sensor measures and connects to the IoT device remotely. These sensors may process real-time data on the fly at the node, reducing the core network's burden. Additionally, this kind of sensor may be installed in the power production section of a power plant. The sensor monitors load demand and regulates the generator's turbine [16]. Most sensors are low-power Internet of Things devices, and data is

encrypted before being sent to the monitoring system. An attacker may conduct a man-in-the-middle attack to steal important data or transmit a modified signal to the control center.

Attacks on the Advanced smart Metering Infrastructure (AMI) provide a new entry point for attackers to compromise the power network's data security. The primary implications of AMI attacks include data theft, power theft, localized or global denial of service attacks, and power grid disruption. Smart meters and data collectors for the power grid usually interact using radio frequency methods in the 900MHz ISM band (industrial, scientific medical band). Numerous unlicensed devices compete for spectrum use in the ISM band. Consequently, a successful spoofing attack on the ISM frequency is very simple—a mesh network for data transmission between smart meters, substation data collectors, and utility analysis centers. When a mesh topology is used, smart meters transmit measurements from one node to the next; the data is still sent to the data collector in the substation. Due to the nature of data transmission, a masquerade attack may penetrate the network and inject erroneous monitoring data, thus interrupting regular power distribution. Through the Replay attack, which re-sends old measurements, an attacker may tamper with the smart meter without being detected in the substation or meter data management system.

C. Network Vulnerability

Security protection for such networks has lagged behind the exploding pace at which low-end edge nodes are connected. Cybersecurity is a major issue in the age of big data, the Internet of things (IoT), machine learning, and artificial intelligence. Any security flaw allows an attacker to execute attack vectors and expose sensitive information. According to recent reports, attackers were able to breach Amazon Internet of Things devices such as the Ring doorbell and the Home security camera. [15]. The attacker intercepted user names and passwords through the local user network's unencrypted HyperText Transfer Protocol (HTTP), thus obtaining access to the IoT devices. According to industry experts, it is very simple to compromise the security of IoT security cameras and voice assistants like Alexa and Google Home [17].

Numerous Internet of Things devices depends on UPnP protocols to provide capabilities such as simple setup and control. However, UPnP makes use of the HTTP protocol, which lacks confidentiality and integrity protection. Garcia [18] discusses several attack techniques for breaking the UPnP protocol because of its authentication, validation, and logging deficiencies. As a result, current research indicates that IoT devices in the Smart Home setting are susceptible if not secured by some defensive protection.

Security protection for IoT networks has fallen behind the exploding pace at which low-end edge nodes are connected. Cybersecurity is a major problem in the age of big data, the Internet of things (IoT), machine learning, and artificial intelligence. Any security flaw allows an attacker to execute attack vectors and expose sensitive information. According to recent reports, the attacker could access Amazon's IoT devices, including the Ring doorbell and the Home security camera [17][18][19]. The attacker intercepted usernames and passwords through the local user network's unencrypted HyperText Transfer Protocol (HTTP), thus obtaining access to the IoT devices. According to industry experts, it is straightforward to compromise the security of IoT security cameras and voice assistants like Alexa and Google Home [17][20].

. According to Morgner [21], connecting the Zigbee Light Link base to the host network may result in data leakage. By distributing pre-defined keys, the author highlighted the problem of insecure key management. According to Rodrigo Roman [22], four Key Management System classes, a key pool framework, a mathematical framework, a negotiation framework, and a public key framework are all inapplicable due to the required unique features.

D. Chip Vulnerability

A Hardware Trojan (HT) is a malicious insertion into an existing circuit that, when activated, modifies its functioning. Adversaries inject an HT payload into an IoT device to cause it to leak information, manipulate it, or circumvent the system's security. Integrate chip devices, such as application-specific system-on-a-chip and field-programmable gate array devices, are vulnerable to digital and analog high-temperature events. Due to IoT's low power consumption characteristic, cryptography units are more vulnerable to attack than high-performance integrated circuits. A firmware update is a simple and cost-effective way to repair a software problem. However, hardware vulnerabilities such as HTs cannot be eliminated with a simple firmware update

and are thus more expensive. Due to the difficulty of the restoration process, HT may result in lasting damage and service degradation [23].

To manufacture IoT device microchips, HT may be readily applied by untrusted third-party IP suppliers, untrusted design houses, and third-party Electronic Design Automation tools. By using passive side-channel electromagnetic analysis, the author Spreitzer showed that the attacker might monitor the IoT device's activity without interfering with it [24]. Side-channel attacks are non-invasive and may result in the physical execution of the data extraction method. The objective of side-channel attacks is to get the secret key of embedded IoT devices. A side-channel attack may be used to obtain the crypto block module's encrypted key information. Critical information, such as passwords and keys, maybe guessed by monitoring and analyzing cryptographic processes' power usage and electromagnetic emissions. The attacker can decode the device's critical information by analyzing side-channel information such as voltage, current, thermal radiation, and timing. Pammu presented a Correlation Electromagnetic Analysis attack to successfully intercept the AES-128 encryption module and recover the secret key [25]. Genkin demonstrated how to obtain the entire 4096-bit RSA decryption keys using a sensitive microphone positioned 4 meters away from an IoT device [23].

III. Conclusions

IoT devices and applications are critical components of modern life. We see IoT devices practically everywhere, including our homes, workplaces, shopping malls, schools, and airports, providing secure and on-demand services. The Internet of Things devices facilitate cooperation with stakeholders and help understand business needs and results. Additionally, analytics and data processing powered by the Internet of Things may help industrial infrastructures' productivity and efficiency.

Additionally, IoT systems are enabling a variety of beneficial technical advancements in a variety of industries. Many vendors and businesses have implemented a variety of rules to safeguard their connected devices from malicious attacks. With an increase in the number of smart devices connected to our private networks and the Internet, additional privacy and security issues have been raised. We read and hear stories that our coffee machine is listening in on our conversations and that our smart doorbell is transmitting images of our visitors to federal authorities. Numerous real-world instances demonstrate the gravity of the security risks inherent in the use of IoT devices. This paper reviewed the common security challenges of IoT systems, including software, hardware, chip, and communication.

IV. References

[1]. Farahani, S. (2011). ZigBee wireless networks and transceivers. newnes.

[2]. Vidgren, N., Haataja, K., Patino-Andres, J. L., Ramirez-Sanchis, J. J., & Toivanen, P. (2013, January). Security threats in ZigBee-enabled systems: vulnerability evaluation, practical experiments, countermeasures, and lessons learned. In 2013 46th Hawaii International Conference on System Sciences (pp. 5132-5138). IEEE.

[3]. Internet of things world forum (iotwf) leaders announce new iot reference model and iotwf talent consortium, https://telecomreseller.com/2014/10/14/internet-of-things-worldforum-iotwf-leaders-announce-new-iot-reference-model-and-iotwf-talent-consortium/ .

[4]. What is series (1): What is the osi reference model ?, https://nicolaswindpassinger.com/osi-reference-model, 2018.

[5]. Czyz, J., Luckie, M., Allman, M., & Bailey, M. (2016). Don't forget to lock the back door! A characterization of IPv6 network security policy. In Network and Distributed Systems Security (NDSS).

[6]. Angrishi, K. (2017). Turning Internet of things (iot) into Internet of vulnerabilities (iov): Iot botnets. arXiv preprint arXiv:1702.03681.

[7]. C. Wueest, Targeted attacks against the energy sector, https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/targeted_attacks_against_the_energy_sector.pdf, 2014.

[8]. A. Chapman, Hacking into Internet connected light bulbs, https://www.contextis.com/en/blog/hacking-into-internet-connected-light-bulbs, 2014.

[9]. B. Rodrigues, Arris cable modem has a backdoor in the backdoor, https://w00tsec.blogspot.com/2015/11/arris-cable-modem-has-backdoor-in.html, 2015.
[10]. Jmaxxz, Backdooring the frontdoor, DEF CON, https://doi.org/10.5446/36251 Lastaccessed : 10Jul2020, 2016.
[11]. Fernandes, E., Rahmati, A., Jung, J., & Prakash, A. (2017). Security implications of permission models in smart-home application frameworks. IEEE Security & Privacy, 15(2), 24-30.
[12]. Costin, A., Zaddach, J., Francillon, A., & Balzarotti, D. (2014). A large-scale analysis of the security of embedded firmwares. In 23rd {USENIX} Security Symposium ({USENIX} Security 14) (pp. 95-110).
[13]. V. Stoffer, Outdated computers and operating systems, https://commons.lbl.gov/display/cpp/Outdated+Computers+and+Operating+Systems, 2013.
[14]. Markowsky, L., & Markowsky, G. (2015, September). Scanning for vulnerable devices in the Internet of Things. In 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS) (Vol. 1, pp. 463-467). IEEE.
[15]. Costin, A., Zaddach, J., Francillon, A., & Balzarotti, D. (2014). A large-scale analysis of the security of embedded firmwares. In 23rd {USENIX} Security Symposium ({USENIX} Security 14) (pp. 95-110).
[16]. Kayastha, N., Niyato, D., Hossain, E., & Han, Z. (2014). Smart grid sensor data collection, communication, and networking: a tutorial. Wireless communications and mobile computing, 14(11), 1055-1087.
[17]. Lei, X., Tu, G. H., Liu, A. X., Li, C. Y., & Xie, T. (2018, May). The insecurity of home digital voice assistants-vulnerabilities, attacks and countermeasures. In 2018 IEEE Conference on Communications and Network Security (CNS) (pp. 1-9). IEEE.
[18]. Aboshosha, B. W., Dessouky, M. M., Ramadan, R. A., El-Sayed, A., & Galalb, F. H. (2018). Evaluation of lightweight block ciphers based on general feistel structure (GFS). WAS Science Nature (WASSN) ISSN: 2766-7715, 1(1).
[19]. Ramadan, R. A. (2021). Detecting adversarial attacks on audio-visual speech recognition using deep learning method. International Journal of Speech Technology, 1-7.
[20]. Ramadan, R. A., Aboshosha, B. W., Yadav, K., Alseadoon, I. M., Kashout, M. J., & Elhoseny, M. (2021). LBC-IoT: Lightweight Block Cipher for IoT Constraint Devices. CMC-COMPUTERS MATERIALS & CONTINUA, 67(3), 3563-3579.
[21]. Morgner, P., Mattejat, S., & Benenson, Z. (2016). All your bulbs are belong to us: Investigating the current state of security in connected lighting systems. arXiv preprint arXiv:1608.03732.
[22]. Roman, R., Alcaraz, C., Lopez, J., & Sklavos, N. (2011). Key management systems for sensor networks in the context of the Internet of Things. Computers & Electrical Engineering, 37(2), 147-159.
[23]. Wang, X., Salmani, H., Tehranipoor, M., & Plusquellic, J. (2008, October). Hardware Trojan detection and isolation using current integration and localized current analysis. In 2008 IEEE international symposium on defect and fault tolerance of VLSI systems (pp. 87-95). IEEE.
[24]. Aboushosha, B., Ramadan, R. A., Dwivedi, A. D., El-Sayed, A., & Dessouky, M. M. (2020). SLIM: a lightweight block cipher for Internet of health things. IEEE Access, 8, 203747-203757.
[25]. Pammu, A. A., Chong, K. S., Ho, W. G., & Gwee, B. H. (2016, October). Interceptive side channel attack on AES-128 wireless communications for IoT applications. In 2016 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS) (pp. 650-653). IEEE.