ACADEMICIA
An International Multidisciplinary Research Journal
(Double Blind Refereed & Peer Reviewed Journal)

DOI: 10.5958/2249-7137.2021.00676.5

INTERNET-OF-THINGS SECURITY AND VULNERABILITIES: IOT SECURITY, IOT TAXONOMY

Sanjar Muminov Saidkulovich*; Husanboy Shoraimov Uktamboyevich; Umarbek Akramov Farkhodugli*****

* Teacher of the Department,
"Systematic and Practical Programming",
Tashkent University of Information Technologies named after Muhammad Al-Khwarizmi,
UZBEKISTAN

** Assistant Teacher,
Department "Systematic and Practical Programming",
Tashkent University of Information Technologies named after Muhammad Al-Khwarizmi,
UZBEKISTAN
Email id: khusan@shoraimov.uz,

***Student of the Department "Radio and mobile communication",
Tashkent University of Information Technologies named after Muhammad Al-Khwarizmi,
UZBEKISTAN
Email id: hmm.a.u.f@gmail.com,

ABSTRACT

Today, our world includes billions of sensors and computing devices that are continually sensing, collecting, consolidating, and analyzing significant amount of our personal information. Such information may include our location, contact list, browsing patterns, and health and fitness information. Many researches focus on IoT security and privacy, but the countermeasures presented in these research often aim at a particular type of attack. Therefore, it is necessary to consider the IoT architecture as a whole and provide holistic protections. Furthermore, the technologies and devices themselves are highly heteroge- neous. This makes their management a difficult and com- plex enterprise.

KEYWORDS: IoT security, IoTtaxonomy ,Vulnerabilities

INTRODUCTION

The early years of the Internet-of-Things (IoT) primarily involved data communication through machine to machine (M2M) interactions. However, the concept has evolved rapidly to include human interactions as well, ushering in an era of Internet-of-Everything (IoE). Today, our world includes billions of sensors and computing devices that are continually sensing, collecting, consolidating, and analyzing significant amount of our personal information. Such information may include our location, contact list, browsing patterns, and health and fitness information. The sensing, collecting, and propagating of such intimate personal data by computing devices is primarily motivated by convenience: as devices get smarter, they can react better to our needs, wishes, and even moods (e.g., a home thermostat can adjust temperature based on number of occupants, time of day, day of week, season of year, etc.) and handle emergencies (e.g., a home security system can react to a fire or break-in). Unfortunately, this convenience comes at the expense of security and privacy challenges: the private, personalized information, if accessible to an unauthorized, malicious agent, can result in significant damage to our wealth, reputation, and personal security. In addition to our own personal data, these devices also include assets introduced by their manufacturers at various stages during their production supply chain. These include fuses, firmware, and debug modes. Unauthorized access to these assets can result in loss of millions of dollars in stolen intellectual properties, as well as potentially dangerous misuse of the assets. With the ubiquitous deployment of these devices, such security vulnerabilities can be catastrophic.

Generic IoT Architecture

Internet-of-Things architecture can be conveniently viewed as an abstraction of several hierarchical layers. Three key layers in the abstraction are the application layer, the net- work layer, and the perception layer. The technologies of each layer are different, even though the technology used by the device of the same layer may be heterogeneous. The devices and technology in the Internet-of-Things are used to provide a diversity of services, each with its own requirements, constraints, and trade-offs. Furthermore, the technologies and devices themselves are highly heteroge- neous. This makes their management a difficult and com- plex enterprise. To address this challenge, a middleware layer is also sometimes added to manage different types of service, shielding the underlying implementation details. The task of the middleware layer is to collect information from the network layer and store them into the cloud and database. Besides, the middleware layer also provides data processing ability. The four-layer architecture of the IoT constituted by the above factors is used in this paper, and this architecture can be applied to the actual application development. Figure 1 describes the four-layer architecture of the IoT and the corresponding technologies in each layer. In this section, we discuss the functionality of these layers to motivate their unique security needs.

Application Layer

The application layer is the social division of the Internet-of- Things, combining with the industry demand and realizing extensive intellectualization. This layer implements different applications for different scenarios. This layer is used to manage and process data from the middleware layer, also providing quality service to the final user. The problem of application layer mainly occurs in the operation of sensitive data, such as illegal access to data, malicious

modification of data, and the lifetime of permission. Attackers can exploit code vulnerabilities to attack systems to gain sensitive data and modify it

Middleware Layer

The middleware layer obtains data from the network layer, links the system to the cloud and database, and performs data processing and storage . With the continuous development of cloud computing and IoT, middleware layer can provide more powerful computing and storage capabilities. Meanwhile, this layer provides APIs to meet the demands of the application layer. Database security and cloud security are the main issues in the middleware layer, which affect the quality of service in the application layer.

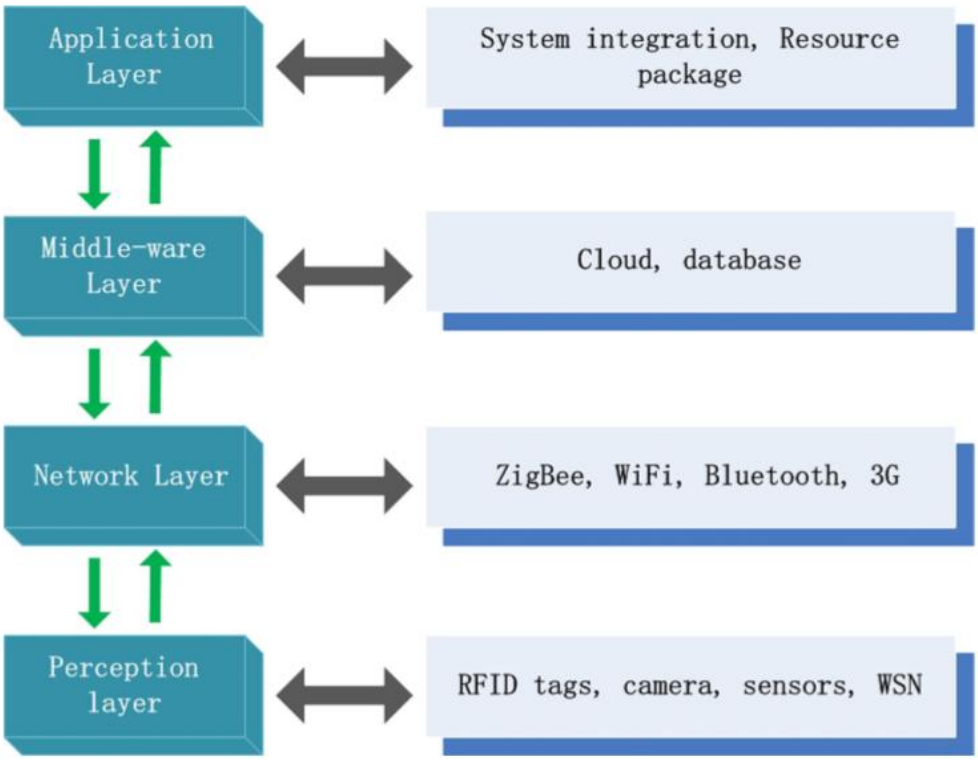

Fig. 1 Four-layer architecture of IoT

Code Injection

This attack entails introduction of malicious code into the system by exploiting program errors . Code injection can be used for a variety of purposes, e.g., to steal data, get system control, and to propagate worms . The common attacks include shell injection and HTML script injection. This type of attack can cause the system to lose control and compromise the user's privacy to the attacker, or even to a complete system shutdown.

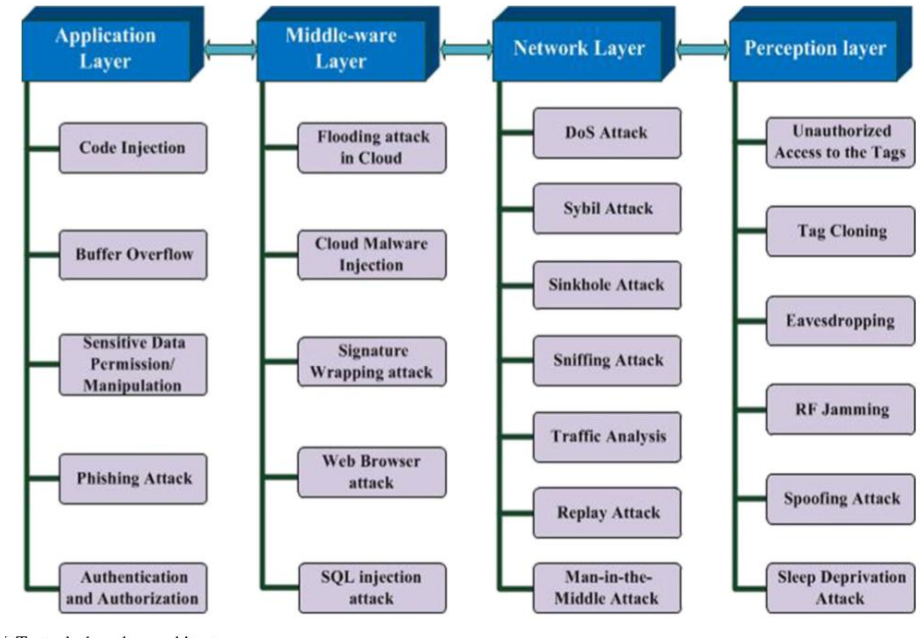

Fig.2 IoT attacks based on architecture

CONCLUSION

The IoT technology has changed people's life style due to information collection, communication, and processing abilities. In the development of the Internet-of-Things, one of the major obstacles is security and privacy issues. IoT attacks may cause privacy violation and threaten people's life and privacy safety. Protecting the privacy of users has become another important challenge in the development of IoT. Many researches focus on IoT security and privacy, but the countermeasures presented in these research often aim at a particular type of attack. Therefore, it is necessary to consider the IoT architecture as a whole and provide holistic protections. In this paper, we discuss the security threats and privacy concerns in each layer of the IoT architecture. We discussed two attack classifications, one based on the IoT architecture and another based on application scenarios. The attack in IoT is analyzed according to different classification standards. The security of each layer on the IoT architecture should be implemented at the same time. Significant further research is required to design a comprehensive security mechanism for the entire IoT architecture.

REFERENCES

1. Iqbal MA, Olaleye OG, Bayoumi MA (2017) A review on Internet of Things (IoT): security and privacy requirements and the solution approaches, Global Journal of Computer Science and Technology

2. Arias O, Ly K, Jin Y (2017) Security and privacy in IoT era. In: Smart Sensors at the IoT Frontier. Springer, pp 351–378

3. Halperin D, Heydt-Benjamin TS, Ransford B, Clark SS, Defend B, Morgan W, FuK, KohnoT, Maisel WH (2008) Pacemakers and implantable cardiac defibrillators: software adio attack

sandzero- power defenses. In: IEEE Symposium on Security and Privacy, 2008. SP 2008. IEEE, pp 129–142

4. Checkoway S, McCoy D, Kantor B, Anderson D, Shacham H, Savage S, Koscher K, Czeskis A, Roesner F, Kohno T et al (2011) Comprehensive experimental analyses of automotive attack surfaces. In: USENIX Security Symposium San Francisco

5. Ray S, Peeters E, Tehranipoor M, Bhunia S (2017) System-on- chip platform security assurance: architecture and validation. In: Proceedings of the IEEE

6. Ray S (2017) System-on-chip security assurance for IoT devices: cooperations and conflicts. In: IEEE Custom Integrated Circuitsx Conference