Future Generation Computer Systems 83 (2018) 326–337

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

On security challenges and open issues in Internet of Things

Kewei Sha[a,*], Wei Wei[a], T. Andrew Yang[a], Zhiwei Wang[b], Weisong Shi[c]

[a] University of Houston — Clear Lake, Houston, TX, United States
[b] Nanjing University of Posts and Communications, Nanjing, China
[c] Wayne State University, Detroit, MI, United States

HIGHLIGHTS

- Analysis of security related characteristics of IoT systems and IoT applications.
- The insufficiency of the existing security solutions.
- Comparison of three architectural security designs.
- Example implementations of the three architectural security designs.
- Identifying a set of open security issues in the context of IoT architecture.

ARTICLE INFO

Article history:
Received 31 October 2017
Received in revised form 27 December 2017
Accepted 28 January 2018
Available online 7 February 2018

Keywords:
Internet of Things
Security
Architecture
Challenges
IoT
Open issues

ABSTRACT

When Internet of Things (IoT) applications become a part of people's daily life, security issues in IoT have caught significant attention in both academia and industry. Compared to traditional computing systems, IoT systems have more inherent vulnerabilities, and meanwhile, could have higher security requirements. However, the current design of IoT does not effectively address the higher security requirements posed by those vulnerabilities. Many recent attacks on IoT systems have shown that novel security solutions are needed to protect this emerging system. This paper aims to analyze security challenges resulted from the special characteristics of the IoT systems and the new features of the IoT applications. This could help pave the road to better security solution design. In addition, three architectural security designs are proposed and analyzed. Examples of how to implement these designs are discussed. Finally, for each layer in IoT architecture, open issues are also identified.

1. Introduction

Internet of Things (IoT) is becoming the largest computing platform [1]. With recent developed applications such as Smart Transportation [2], Smart City [3], Smart House [4], and Smart Grid [5], IoT technologies are significantly changing our life style [6,7]. The pervasive interconnection of smart IoT things which are physically distributed extends the computation and communication to IoT things with various specifications. Sensing capability of these devices helps collect real-time data from the physical world directly or remotely. The analysis of the collected data provides us the ability of building an intelligent world and making better decisions to manage it.

IoT devices are becoming pervasive and they extend the Cyber world to the physical world, which creates new types of and more complex security issues and concerns. If those security concerns cannot be adequately addressed, wider adoption of IoT applications will be greatly hindered. For example, considering two of the typical application domains of IoT, i.e., Smart Home and Smart Healthcare, it is essential to protect the sensitive information moving around the system and the critical assets in the system [8–10]. The characteristics of the IoT devices, however, make the security design in IoT more challenging than before. These characteristics include extremely large scale, low cost design, resource constraints, device heterogeneity, preference of functions over security, higher privacy requirements, and harder trust managements. To be more specific, resource constraints often include limited computation power, energy supply, and memory capacity. These features make it difficult to apply many traditional security solutions to IoT, including the widely used public key scheme and IP-based security solution. Due to insufficient IoT security design, it is often easier to compromise IoT devices than conventional computers. For example, Forbes.com reports a successful hack into a baby monitor in Houston area [11]. Someone also demonstrated how to hack and remotely control and stop a Jeep car on the road

[*] Corresponding author.
E-mail addresses: sha@uhcl.edu (K. Sha), wei@uhcl.edu (W. Wei), yang@uhcl.edu (T. Andrew Yang), zhwwang@njupt.edu.cn (Z. Wang), weisong@wayne.edu (W. Shi).

https://doi.org/10.1016/j.future.2018.01.059
0167-739X/© 2018 Elsevier B.V. All rights reserved.

when the driver is in operation [12]. It is also reported by CNN Money that hackers have found volatilities in most smart home devices [13], including Smart Plugs [14,15], Smart Cameras [16,17], DVRs [18] as well as vulnerabilities revealed by researchers [19–25].

Above cases illustrate the urgent needs of improving security of IoT systems. Serious consequences can be expected from security breaches in IoT systems. For example, fatal accidents can be the result of remotely turning off a vehicle through a security breach. Current weaknesses in IoT security may be attributed to insufficient understanding of security challenges of new IoT systems. In this paper, we aim to conduct a detailed analysis of security challenges in IoT systems, because we believe an intimate understanding of IoT security challenges will pave the road to better security solution design. Moreover, the differences in security challenges between IoT systems and Wireless Sensor Networks (WSNs) are summarized and compared. Finally three architectural security designs for IoT are proposed and compared. Examples of how to implement these designs are presented and discussed. One of our findings is that, without aid of highly capable devices, it is difficult to achieve high level of security with the low capable devices in the system. This observation necessitates the deployment of secure services in the new Edge computing paradigm [26,27]. The contributions of the paper include in-depth analysis of IoT security challenges, proposals of security function deployment, and identification of open issues in IoT security designs.

The rest of the paper is organized as follows. Importance of security in IoT applications in the context of several typical IoT applications is discussed in Section 2. Then Section 3 overviews a typical IoT architecture. A comprehensive analysis on new IoT security challenges is presented in Section 4, which is followed by comparisons of security challenges between WSNs and IoT in Section 5. In Section 6 our proposal of architectural designs of IoT security solutions are presented and discussed. We list a set of related work in Section 7. Finally, conclusion and future work are depicted in Section 8.

2. IoT applications and needs of security

IoT is becoming the largest computing platform. It has been applied in many application domains including Logistics [28], Smart Home [4], Smart City [3], Smart Health, Smart Connected Vehicles [2], Smart Grid [5], and so on [1]. In this section, we present three typical applications of IoT in the context of the importance of security in these applications.

2.1. Smart home

Smart Home is becoming increasingly popular recently [29]. Gartner's IT Hype Cycle 2016 Report identifies that smart connected home is an emerging technology. It is predicted that a typical home could contain 500 or more smart devices by 2022 [30]. Smart Home has the vision of adding intelligence to everyday home objects, such as appliances, door locks, surveillance cameras, furniture, garage doors, and so on, and making them communicate with existing cyber-infrastructure. The addition of intelligence to physical objects offers many benefits to better human lives, including increased convenience, safety, security, and efficient usage of natural resources. For example, the Smart Home can adjust the blinds to save energy based on the environmental changes, automatically open the garage door when it senses an authorized vehicle approaching, or automatically order medical service when emergency is detected. In Smart Home, traditional physical home devices become a part of the extension of the existing Internet. If devices are compromised, the consequence can be severe. For example, successfully hacking smart lock will enable strangers to enter the house; compromising of baby monitors can scare babies remotely by strangers; hacking microwave can cause fire at the home. Owners of Smart Home may not want to live in Smart Home if security is a concern. Instead, they may expect to improve the safety of the house by using intelligent surveillance services [4]. In addition, privacy of Smart Home owners need to be preserved. However, continuously collecting data from Smart Home devices can reveal private activities of home owners as indicated in [31,32]. It poses serious threats to the home owners' privacy.

2.2. Smart grid

The other typical IoT application is to build Smart Grid. Smart Grid has been designed and implemented to improve the reliability, reduce the cost, and optimize the performance of the traditional power grid systems [33]. In addition to integrating more green and renewable energy such as wind power, geothermal heat and solar power, it also aims to improve the reliability and management of the traditional power grid more efficiently. Smart grid data communication networks, which interconnect many smart grid devices, play a critical role to achieve above goals. It not only collects the energy usage data, but also monitors the status of the smart grid system. Many novel applications can be developed based on the smart grid data communication networks. For instance, based on the collected energy usage information, utility companies can distribute and balance the load more wisely. It also helps to design a fair but scaled pricing model by considering the unbalanced energy consumption in the dimension of time and space. By building smart grid status monitoring applications, it is possible to identify failures in the grid system as early as possible, and design novel fault-tolerant mechanisms to better respond to the failures. Many techniques including automated metering infrastructure (AMI) [34,35] have been proposed to build the smart grid communication networks. Having so many data moving around this mission-critical system, security is also one of the most important concerns in building such systems. Intrusion to Smart Grid [36] and cutting electricity supply to a large area can cause huge physical and economical damage to the society. Analyzing power usage data can also reveal people's daily private activities [37]. Moreover, attacks against data integrity [38,39] and false data injection [40–42] can disturb the billing system of the smart grid and mess up start grid state estimation, torture the power flow, and delay demand response.

2.3. Smart connected health

Smart Connected Health is proposed to improve the efficiency of healthcare systems and to reduce healthcare costs [43]. The analysts at MarketResearch.com claim that the sector will be worth $117 billion by 2020. By embedding smart healthcare devices in the existing medical infrastructure, healthcare professionals will be able to monitor patients more effectively, and use the data collected from these devices to figure out who needs the most attention. In other words, by making the most of this network of devices, healthcare professionals could build a system of proactive management based on the collected data, as it is believed that prevention can be more important and effective than the cure. Researchers also study techniques on how to implant sensors into human body and monitor the health condition of these people [44]. Analyzing the collected data, healthcare professionals are able to discover behavioral changes of patients with the disease and with the medicines during the treatments. In Smart Connected Health, security is also a critical concern. With networked medical devices, it is convenient to collect data and check the status of that device, but it is also risky because instructions can be sent to stop the function of the device [45]. It will be extremely dangerous to stop