Secure IoT Deployment Checklist for Building Management System

Raymond Chan[1], Wye Kaye Yan[2], Alaric Tang[3], Jingquan Chen[4], Malcolm Low[5], Kar Peo Yar[6]
Singapore Institute of Technology
Habib Rehman[7], Thong Chee Phua[8]
Firefish Communications
{Raymond.Chan, Malcolm.Low, Wyekaye.Yan}@singaporetech.edu.sg
{2000890, 2101268}@sit.singaporetech.edu.sg
{habib, thongchee}@firefishcomms.com

Correspondence address: Cluster of Infocomm Technology
Singapore Institute of Technology
Singapore
Tel: (65) 6592 5549
Fax: (65) 6592 1190

Abstract
A building management system (BMS) enables the capability to control the infrastructure within a building. BMS can be considered a miniature industrial control system, which is much more common to reach and find by users. The legacy architecture of the BMS assumes every device has to be connected physically. Due to this reason, installing a new Internet of Things (IoT) system allows external connections to enable new security loopholes in the existing BMS. Moreover, potential cyber-attacks target the communication between the BMS and IoT devices.

In this paper, we created a prototype setup of the BMS with IoT devices to study the deployment and how the system can be installed. We introduced a comprehensive deployment checklist to assess the security posture of IoT solutions, which specifically focused on the BMS system. This checklist is novel to the market as the existing works are mostly targeted to IoT but not fully applicable to BMS.

Keywords*: Building management system, vulnerability assessment, cyber-security, deployment security, Internet of Things*

1. INTRODUCTION

In recent years, the smart city has become a popular trend worldwide. It encourages the integration of the IoT to have more convenient administration, monitoring, and analysis of the surrounding physical environment. A building automation system (BMS) is one of the systems that will install IoT devices and sensors. A BMS includes a power control system, water and gas supply system, elevator system, and fire alarm system. All of these subsystems are critical for building operations. The reasons for installing IoT devices and sensors are to enhance monitoring and control capabilities, reduce the subsystems' malfunctioning, and perform predictive maintenance.

Simultaneously, building owners and facility managers are increasingly using physical security systems that are getting smarter and more intelligent. One example is adopting CCTV systems incorporating video analytics that can perform people counting [20], perimeter fencing, attributes tagging, unattended items detection, and even specialized capabilities such as fight detection [21]. Another example is using multi-factor electronic door access and lock management system incorporating facial recognition [22], user heuristic analysis, and mobile device integration to replace the physical smart card [23]. There is much excitement in the market over these technologies' potential for increasing productivity and efficiency. However, to harness these new technologies, understanding their security posture is important.

The rest of this paper is organized as follows. Section 2 summarizes existing works about IoT and BMS security. Section 3 introduces the case study for the BMS and IoT integration system prototype. Section 4 presents the proposed deployment checklist. Section 5 gives a conclusion and the future works.

2. RELATED WORK

While the adoption of IoT solutions is becoming more popular, many underestimate the vulnerabilities mainly in eavesdropping, little to no authentication, and these devices' protocol and network security design [14]. Some of the devices, such as a smart lighting system [1], wearable fitness trackers [2], and thermostats [19], have been found vulnerable, causing potential damages. Besides the vulnerabilities on the devices are attacks focused on the network connections [4, 5]. While IoT deployments have become increasingly popular, various technical vulnerabilities such as limited storage, power, and computational capabilities hinder IoT devices' security requirements [3]. Moreover, the lack of IoT access controls [6] and audit mechanisms allows IoT-centric malicious attacks to penetrate the system [15].

Due to the original architecture of the BMS, installing a new IoT system allows an external connection to bring new security loopholes into the existing BMS [3]. Moreover, the communication between the BMS and IoT devices creates potential loopholes for cyber attacks. There are no standards for guiding the vendors to use a common protocol to communicate between devices. The communication medium is not protected either and does not have to be secure. Therefore, a vulnerability assessment should be conducted to guarantee BMS availability. Our previous work [16, 17] showed the need for a workflow or standards for managing and mitigating cyber attacks.

Singapore Infocomm Media Development Authority (IMDA) released an IoT Cyber Security Guide to help enterprise users and vendors secure IoT Systems [14]. The guide provides advice for designing, implementing, and procuring IoT systems. Nevertheless, this is

a generic framework for IoT devices. A comprehensive analysis and a deployment checklist are necessary for the BMS.

On the other hand, some new IoT architectures have been proposed. King proposed a distributed security mechanism for resource-constrained IoT devices [7]. Pirbhulal introduced a novel secure IoT-based smart home automation system utilizing a wireless sensor network [8]. Wei proposed an encryption protocol for practical IoT devices [10]. Moosavi introduced an authentication and authorization architecture for IoT-based healthcare using smart gateways [11]. Gajewski suggested a distributed IDS architecture model for smart home systems [12]. Mantoro proposed using a smartphone to perform authentication and message integrity for smart homes [13].

To summarize, few studies have been conducted to assess the actual BMS vulnerabilities and propose solutions to reduce the security risks. Although some researchers have tried to propose a novel secure architecture and new communication protocols, the industry may not adopt it easily due to the diversity of the devices and brands. The existing work did not address the fact that many of those IoT devices are increasingly being deployed in the BMS. To fill this gap, we propose a secure deployment checklist for the BMS. It can be used to ensure that the installation of the IoT devices has a standard operating procedure (SOP) for security.

3. CASE STUDY

Regarding the threat modeling checklist sample provided by IMDA [14], the target of protection (TOP) for the system's components and subcomponents can be identified and illustrated through the system architecture.

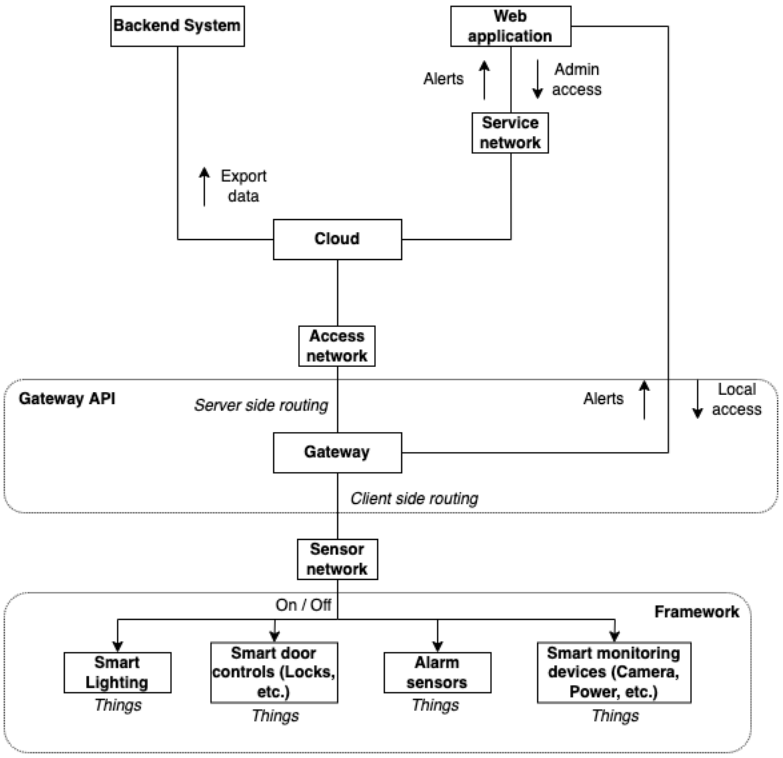

Figure 1: Building management system testbed architecture

As shown in Figure 1, the system architecture can be divided into two main sections: access network and sensor network. Within the access network (cloud services for the backend system and the frontend web application that connects to the gateway), it also enables the subcomponents to be controlled from the web application via a secure TLS tunneling service.

Further illustrating the sensor network, the architecture for it can be derived from four components. The smart lighting system and smart door controls connect to the gateway via the Zigbee protocol. The alarm sensors and smart monitoring devices are connected via Wi-Fi and MQTT, respectively. The gateway acts as a hub between the cloud services.

4. DEPLOYMENT CHECKLIST

Based on the deployment knowledge we gained from the configuration and setup described above, we propose a secure deployment checklist for the BMS.

In this section, we introduce the proposed deployment security checklist. There are two phases included in the checklist: the deployment phase and the post-deployment phase. The deployment phase addresses the preparation and configuration of the device during installation. It also covers the rollback procedure if the deployment cannot be completed on schedule. The post-deployment phase ensures the stability and protection against potential future threats that are targeting the devices. This phase also covers the open-source intelligence workflow to ensure that the operator monitors whether the devices are being affected by the latest vulnerabilities and attacks. Figure 2 shows the deployment checklist workflow. It provides a summary so that the engineer can verify the device before, during, and after the deployment.

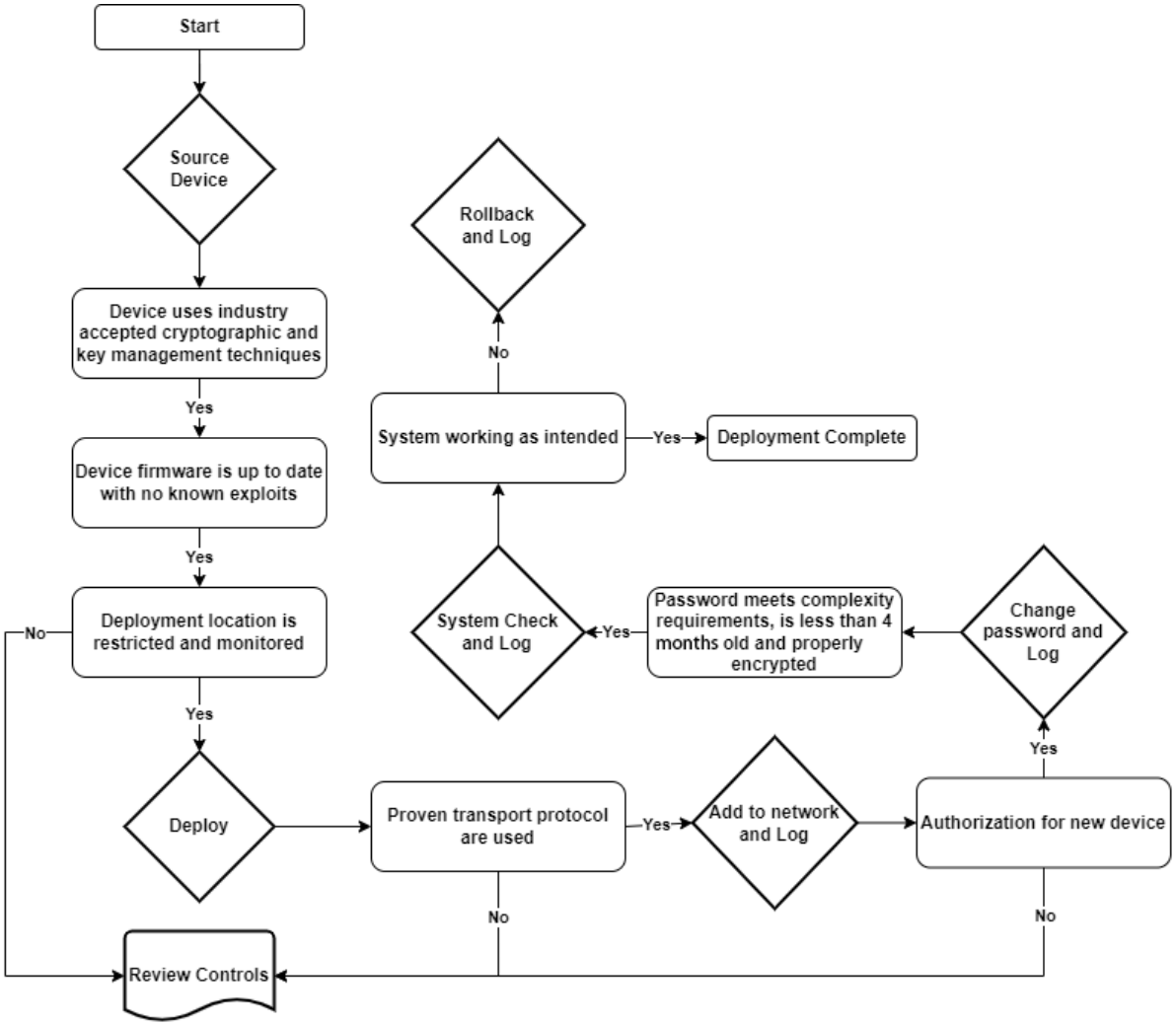

Figure 2. Proposed security deployment checklist workflow

1. Deployment phase

In a BMS, the deployment and maintenance time frame might be only five or six hours at night. The BMS engineer must ensure that the following factors are considered to prevent issues during deployment:

1.1 Security deployment checklist

The BMS engineer must prepare a security deployment checklist to verify the configurations and security measurements. It will ensure that the engineer has checked proper deployment of the devices or systems

If the installation takes more than one maintenance time frame, the checklist should include the configurations and settings that must be verified every time.

1.2 Rollback checklist

The engineer must define the rollback procedure to prevent the deployment if it cannot be completed within the expected maintenance time frame.

The procedure should include steps to restore the deployment and verify that the existing system is working normally after rollback.

1.3 Deployment verification checklist

The procedure verifies that the deployment is complete and that the newly installed device is working as expected.

The security deployment checklist should include the deployment verification process to ensure that the configuration is secure.

2. Post-deployment phase

After the deployment, the operator should have a proper procedure for maintaining and

monitoring the devices and systems, especially if the patches and version upgrades are related to the firmware, which might require a restart.

2.1 Patch and upgrade checklist

This procedure must undergo the testing and deployment phase to ensure the patch or update will not affect the existing functionality and reliability.

The patch and upgrade procedure may require another deployment to address follow-up actions.

2.2 Drill checklist

A proper drill must be conducted periodically in the trial and production environment during the maintenance time frame, if possible. The operator is suggested to perform drills after new devices are deployed, patched, or upgraded.

The drill should simulate if the devices are attacked by an intruder, and the operator should react and mitigate impact on the BMS. Vulnerability assessment and penetration testing should be considered in the drill. This will be useful for understanding potential attacks.

2.3 Monitoring and open-source intelligence workflow

There might be an urgent security bulletin issued by the vendor or the Company Emergency Response Team (CERT). The BMS operator needs to prepare the standard operating procedure (SOP) to react to those security incidents.

A decision to apply a quick fix and monitor the behavior of the BMS must be made before the patch is deployed. The operator should have a repository to maintain their version of the system and device to ensure they can quickly verify against the version of the BMS in the CERT announcement.

5. CONCLUSIONS AND FUTURE WORKS

We introduced the setup of BMS and IoT integration systems for understanding the methods to connect existing BMS and IoT devices. Based on the knowledge of the installation, we proposed the security deployment checklist to address the security issues that may make the BMS vulnerable to potential cyber attacks.

For future works, we planned to design and develop a POC orchestration software platform ingesting information from various BMS subsystems and IoT devices to demonstrate the feasibility of monitoring the whole infrastructure and mitigating cyberattacks.

References

[1] P. Morgner, S. Mattejat, and Z. Benenson, “All your bulbs belong to us: Investigating the current state of security in connected lighting systems,” arXiv preprint arXiv:1608.03732, 2016.
[2] A. K. Das, P. H. Pathak, C.-N. Chuah, and P. Mohapatra, “Uncovering privacy leakage in BLE network traffic of wearable fitness trackers,” in Proceedings of the 17th International Workshop on Mobile Computing Systems and Applications, pp. 99–104, 2016.
[3] J. Wurm, K. Hoang, O. Arias, A.-R. Sadeghi, and Y. Jin, “Security analysis on consumer and industrial IoT devices,” in 21st Asia and South Pacific Design Automation Conference (ASP-DAC), pp. 519–524, 2016.
[4] P. Pongle and G. Chavan, “A survey: Attacks on RPL and 6LoWPAN in IoT,” in 2015 International Conference on Pervasive Computing (ICPC), 2015, pp. 1–6.
[5] A. Rghioui, A. Khannous, and M. Bouhorma, “Denial-of-service attacks on 6lowpan-RPL networks: Issues and practical solutions,” Journal of Advanced Computer Science & Technology, vol. 3, no. 2, pp. 143–153, 2014.
[6] A. Mayzaud, R. Badonnel, and I. Chrisment, “A Taxonomy of Attacks in RPL-based Internet of Things,” International Journal of Network Security, vol. 18, no. 3, pp. 459–473, 2016.
[8] J. King and A. I. Awad, “A distributed security mechanism for resource-constrained IoT devices,” Informatica, vol. 40, no. 1, 2016.
[9] S. Pirbhulal et al., “A novel secure IoT-based smart home automation system using a wireless sensor network,” Sensors, vol. 17, no. 1, p. 69, 2017.
[10] B. Wei, G. Liao, W. Li, and Z. Gong, “A practical one-time file encryption protocol for IoT devices,” in 2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC), vol. 2, pp. 114–119, 2017.

[11] S. R. Moosavi et al., “SEA: A secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways,” Procedia Computer Science, vol. 52, pp. 452–459, 2015.
[12] M. Gajewski, J. M. Batalla, G. Mastorakis, and C. X. Mavromoustakis, “A distributed IDS architecture model for Smart Home systems,” Cluster Computing, vol. 22, no. 1, pp. 1739–1749, 2019.
[13] T. Mantoro, M. A. Ayu, and S. M. binti Mahmod, “Securing the authentication and message integrity for Smart Home using smart phone,” in 2014 International Conference on Multimedia Computing and Systems (ICMCS), pp. 985–989, 2014.
[14] Infocomm Media Development Authority, “IMDA IoT Cyber Security Guide,” URL: https://www.imda.gov.sg/regulations-and-licensing-listing/ict-standards-and-quality-of-service/Telecommunication-and-Security-Standards/reference-standards, 2020.
[15] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, “IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices,” IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8182–8201, 2019.
[16] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, “Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on Internet-scale IoT exploitations,” IEEE Communications Surveys & Tutorials, vol. 21, no. 3, pp. 2702–2733, 2019.
[17] R. Chan and K.P. Chow, “Threat analysis of an elevator control system,” in International Conference on Critical Infrastructure Protection, pp. 175–192, 2017.
[18] R. Chan, F. Tan, U. Teo, and B. Kow, “Vulnerability Assessments of Building Management Systems,” in International Conference on Critical Infrastructure Protection, pp. 209–220, 2020.
[19] NewSky Security, “IOT thermostat bug allows hackers to turn up the heat,” URL: https://blog.newskysecurity.com/iot-thermostat-bug-allows-hackers-to-turn-up-the-heat-948e554e5e8b, 2017.
[20] Z. Q. Al-Zaydi, D. L. Ndzi, M. L. Kamarudin, A. Zakaria, and A. Y. Shakaff, “A robust multimedia surveillance system for people counting,” Multimedia Tools and Applications, vol. 76, no. 22, pp. 23777–23804, 2017.
[21] M. Perez, A. C. Kot, and A. Rocha, “Detection of real-world fights in surveillance videos,” in ICASSP 2019–2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 2662–2666, 2019.
[22] C. Ganeshan and S. kumar Singh, “Smart Industrial System for Monitoring, Control and Security Using Internet of Things,” in 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI), pp. 958–963, 2018.
[23] Y.C. Chen, C. Chu, H.M. Sun, J. Yeh, R.S. Chen, and C.S. Koong, “Development of an Intelligent Equipment Lock Management System with RFID Technology,” in 2017 18th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT), pp. 33–38, 2017.