International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 20 (2017) pp. 10454-10457

IoT: Security and Privacy in Future Home appliances

Marlen S Bissaliyev

Faculty of Mechanics and Mathematics, dept. of Information Systems
Al-Farabi Kazakh National University, Al-Farabi 71, PO Box: 050040, Almaty, Kazakhstan.

Orcid: 0000-0002-3622-5477

Abstract

With the development of social economy and technology, many appliances present in our homes. While mainstream Internet of Things (IoT) research is focused on solving privacy and security issues, the paper focuses on the conceptual framework and architecture of future home appliances. In this paper we cover Man in The Middle Attack (MITM), physical attack, cloning, data tampering and routing attacks. To address these issues, conceptual architecture is proposed, where security concerns are observed from different perspectives. The proposed architecture considers security requirements proposed by the Internet Engineering Task Force (IETF) for a successful deployment of IoT.

Keywords: Internet of Things, Network Security, Network

INTRODUCTION & MOTIVATION

Internet of things (IoT) is a rapidly growing paradigm in wireless network telecommunications. The concept of the technology is to provide connectivity between heterogeneous network nodes [1]. The IoT provides a capability of appliances like TV, microwave, door or AC to connect to the Internet. As the technology provides the communicating capability it opens a security threats. The attacker might gain access of smart devices and lock user inside his smart home. Consider a scenario, where the attacker would be able to get access of smart door and Heating, Ventilation and Air Conditioning (HVAC), he would be able to lock user inside his home and turn HVAC temperature to a minimum. In addition, compromised hardware would leak user's data to unauthorized parties. In order to address the problem, there are several security considerations have to be assessed [2].

The confidentiality – data cannot be used by unauthorized listeners. This can be achieved with the cryptographic encryption mechanism. Integrity – data cannot be tampered by other parties. This can be achieved by integrity checks and encryption of the file system. The availability – The system should be available and not be a subject to Denial of Service (DoS) attacks. This can be achieved by traffic filtering. Control – the user have to control the system and data he is interacting. This can be achieved by providing ability of manual operation.

The proposed conceptual architecture is to secure the access to these devices based on conceptual architecture with layered security based on scheme of smart home control system proposed by Wang, et al., embedded security concerns covered by Babar, et al. and concept of Intrusion Detection System (IDS) proposed in SVELTE [3,4,5]. To generate private keys we use biometric parameters.

The paper is organized as follows. In section II, we discuss the related work and security concerns on IoT. In section III, we evaluate proposed solutions. In Section IV, we describe our proposed model to address the security issues. In section V, we compare our results to existing works.

RELATED WORK

Smart home networking was proposed by Wang et.al. The control system uses IoT with Radio Frequency (RF) 433 MHz wireless sensor and actual network (WSAN). The controller is responsible for managing and organizing wireless network nodes with control modules [3]. To get access to the internet, smart controller has to be connected to the wireless router via Wi-Fi interface. A remote control device, such as mobile phone or application interacts with the router via the Internet. It provides capability of managing control modules over the Internet.

A security design and framework proposed by Babar, et al. [4] covers the security on hardware, software and mixed levels. Their highlighted software hardware based security architecture explicitly describes the hardware security. They propose to have security keys on storage to provide the base for the operations. The method of physical security is to embed Trusted Platform Module (TPM) with secure boot. Secure boot would bring system to trusted and known state. This reduces the probability of attacker to access the data on the chip.

The concept of integrating Intrusion Detection Systems in IoT was proposed by Raza, Wallgren and Voigt in their SVELTE, Real-time Intrusion Detection System [5]. The system consists from three detection techniques. First, detect tampered or spoofed information. Second, detect sinkhole attacks, where attacker is able specify the route of the packets to his network. Third, detect selective forwarding attacks, where attacker is able to forward selected packets.

The hardware key management was covered in BitLocker, developed by Microsoft Corporation [6]. The key generation process may be done by using biometric parameters, such as voice, face or fingerprint. Once the key is generated it is stored on the storage of the appliances. When the key is authenticated, the data is available to the user.

DETAILED ANALYSIS

In order to subjectively analyze proposed solutions, it is important to know the security concerns developed by standardization organizations. Internet Engineering Task Force (IETF) covers the security needs for the IoT: cloning, spoofing of the devices, MITM, network sniffing, firmware replacement, extraction of security parameters, routing attack and DoS [7].

The architecture proposed by Wang, et al. covers the security on the application layer of Open Systems Interconnection (OSI) model. The authors' security concerns focused on zone configuration of the appliances. Users may define policies for different appliances in its zones. The architecture is subject to vulnerability for physical, MITM and dictionary attacks.

The embedded security proposed by Babar, et al. covers hardware and software security. However the main emphasize of physical security is focused on the Trusted Platform Modules and key storage should be done at storage of the appliances. To enhance the embedded security may be achieved thru user's biometric parameters as an input to generate the private keys.

The Intrusion Detection System proposed by Raza, Wallgren and Voigt covers the security concerns of routing, spoofing and forwarding attacks.

To sum up the solutions and security concerns, it is important to visualize the possible threats.

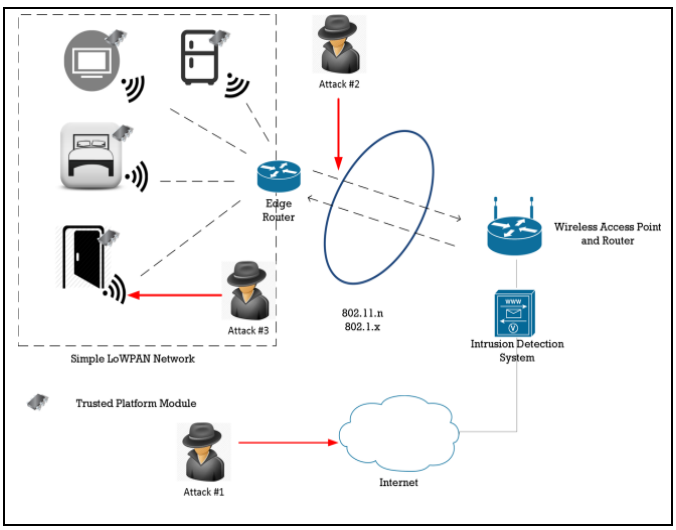

Figure 1: Threat Analysis on Smart Home Appliances

Figure 1 illustrates the conceptual topology of interconnected devices and possible threats. Nodes in simple LoWPAN network are operating via edge router. Every node carries the Trusted Platform Module (TPM) to store cryptographic keys. This will increase security on physical level, while the attackers try to access the memory physically. If data tampering detected, the data will be wiped off, so the attacker will not able to access any data. To prevent traffic sniffing, authorization of the wireless devices should be performed. This can be done using 802.1.x authentication protocol. If the attacker will access from internet, the IDS would be able to detect abnormal activity and trigger the alarm. The system will erase private keys and require user to generate new key.

CONTRIBUTION

In order to meet security requirements, we evaluate security concerns on physical, network and application layers.

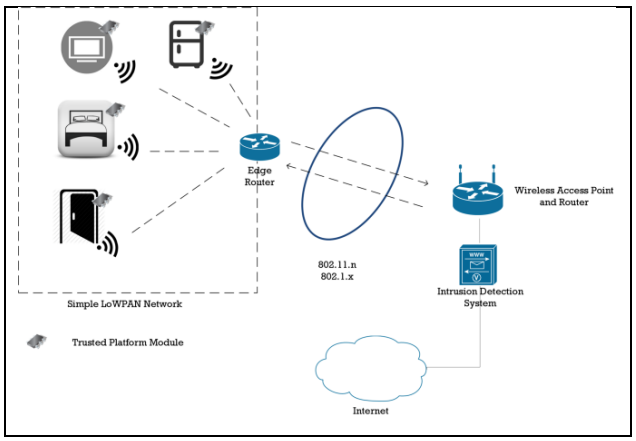

Figure 2: Proposed solution

Figure 2 illustrates the conceptual topology of interconnected devices. Nodes in simple LoWPAN network are operating via edge router. Embedded security with TPM modules in home appliances will protect the user from physical attacks. The authentication of wireless devices should be done using 802.1.x protocol to prevent traffic sniffing. To secure the home network from internet, the IDS should be at the start of incoming traffic.

A. Key Management

User has to use his biometric parameters to generate new private key. As security option private key maybe stored on external device, such as USB, in case manual operation is required. Once key is generated it the system compares the entered key and user defined key. If key is authenticated, the data will be release for next use. If key is not authenticated, the data will be locked system will request to place USB key to release the data. The process is described in Algorithm 1.

Algorithm 1. Key Management

Step 1. Encrypt Data with Biometric Parameters

Step 2. Access key on storage of the appliance

Step 3. Check private key parameters

3.1 if key is authenticated

Release data;

3.2 else
Lock Data;
Request USB device to release data;

B. Intrusion Detection System

The purpose of IDS is to detect abnormal activity. The conceptualized framework is an IDS based on Bayesian Inference Probability comparing to the packet payload. In example if TV in normal state communicates with a local provider, so the destination address is known and maintained by the system. If there is abnormal activity in packet exchange, the system will trigger an alarm and erase private keys. To define an abnormal activity we assume that the destination address occurrence is less than allowed threshold. The following describes the steps how alarm might be triggered. The process is described in Algorithm 2.

Algorithm 2. IDS anomaly detection

Step 1. Select nodes to Monitor

Step 2. Establish Relationship

Step 3. Establish Probability of Occurrence

Step 4. Analyze Payload

4.1 if *destination_address* < destination_address.probablity_occurence

alarm_counter++;

Step 5. if *alarm _counter < threshold*

trigger_alarm();

erase_private_key();

The drawbacks of IDS are false results in optimum payloads and positive results in malicious payloads. This can be adjusted analyzing and evaluating the traffic.

RESULTS AND COMPARATIVE ANALYSIS

The IDS is implemented in the Contiki OS, operating system for the IoT [8]. The Contiki OS has a tested implementation of 6LoWPAN. To test IDS in 6LoWPAN network, we use contiki 6LoWPAN modules. We use µIP, an IP stack in Contiki OS, to provide communication between 6LoWPAN nodes.

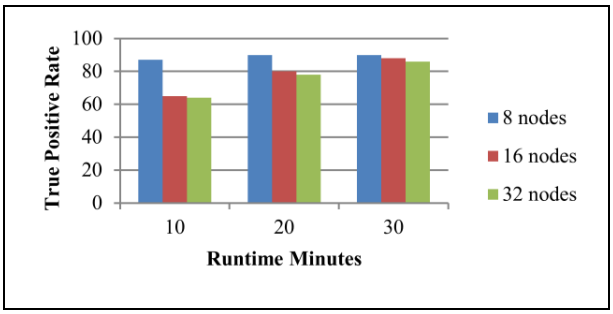

Figure 3: True Positive Rate of Raza, Wallgren and Voigt IDS

Figure 3 explains that authors reached higher true positive rate when number of nodes increasing. IDS detection rate is almost 90% when 32 nodes are operating.

Instead of predicting true positive detection rate, we evaluate the false positive results. We pre-determined the domain list of trusted sources. The percentage of occurrence of untrusted addresses was recorded.

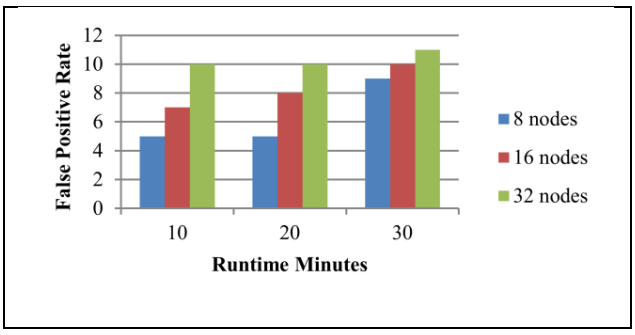

Figure 4: False Negative Rate of proposed IDS based on abnormal activity of destination address.

The tests showed that 10% false positive rate after analyzing the payload and untrusted destination address occurrence. Following we adjust 10-12% alarm trigger threshold to the IDS parameters to adequately detect abnormal activities.

CONCLUSIONS

There are several layers of the security have been assessed. The proposed model is not the best one, however it describes that

security has be evaluated from different layers and serious considerations have to be taken. The hardware level encryption is required in case the attacker is related to maintenance person, and by somehow will try to access the memory. The wireless security is required to prevent sniffing and unattended listeners. There are issues may be raised in IDS as it may output false positives results. With the improvement of algorithm and parameters, there is possibility to lower false positive rate.

The proposed architecture covers the security considerations mention in IETF document. The need for embedded security in TPM modules covers the physical attacks. The authentication of network devices has to be performed to prevent traffic sniffing. The need of IDS is to prevent routing, spoofing and forwarding attacks.

The future considerations and research will cover the performance management. We will evaluate how the implementation of IDS and security authentication will affect network performance.

REFERENCES

[1] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer Networks,* vol. 54, pp. 2787-2805, 2010 2010.

[2] Z. Shelby and C. Bormann, *6LoWPAN: The Wireless Embedded Internet*: Wiley Publishing, 2010.

[3] M. Wang, G. Zhang, C. Zhang, J. Zhang, and C. Li, "An IoT-based appliance control system for smart homes," 2013, pp. 744-747.

[4] S. Babar, A. Stango, N. Prasad, J. Sen, and R. Prasad, "Proposed embedded security framework for Internet of Things (IoT)," 2011, pp. 1-5.

[5] S. Raza, L. Wallgren, and T. Voigt, "SVELTE: Real-time intrusion detection in the Internet of Things," *Ad Hoc Networks,* vol. 11, pp. 2661-2674, 2013/11// 2013.

[6] M. Corporation. *BitLocker Drive Encryption Overview*. Available: http://windows.microsoft.com/en-us/windows-vista/bitlocker-drive-encryption-overview

[7] O. Garcia-Morchon, S. Keoh, S. Kumar, P. Research, R. Hummen, R. Aachen*, et al.*, "draft-garcia-core-security-06 - Security Considerations in the IP-based Internet of Things," IETF2013.

[8] Contiki. (2013). *Contiki: The Open Source Operating System for the Internet of Things*. Available: http://www.contiki-os.org/