A PROPOSED FRAMEWORK FOR SMART CYBER INFRASTRUCTURES SECURITY USING IOT

[1] Vallem Sushma Latha, [2] Garidepalli Revathi

[1] sushmacjits@gmail.com , [2] g.revathi57@gmail.com ,

[1, 2] Assistant Professor Department of CSE, Talla Padmavathi College of Engineering,Warangal, Telangana, India.

ABSTRACT: The 5th generation wireless system (5G) will support Internet of Things (IoT) by increasing the interconnectivity of electronic devices to support a variety of new and promising networked applications such as the home of the future, environmental monitoring networks and infrastructure management systems. However, IoT infrastructures and services will introduce grand security challenges due to the significant increase in the attack surface, complexity, heterogeneity and number of resources. This includes an investigation into the security requirements of three different characteristic IoT scenarios (concretely, body IoT, home IoT and hotel IoT). This paper attempts to address this problem through the development of a prototype security framework along with Anomaly Behavior Analysis Intrusion Detection System (ABA-IDS) with robust and transparent security protection. The ABA-IDS can detect and classify a wide range of attacks against IoT sensors. This prototype security framework gives us an insight into some of the major difficulties of IoT security as well as providing some feasible solutions.

KEYWORDS: IoT, cyber security, smart infrastructures and Anomaly Behavior Analysis.

I. INTRODUCTION

The Internet of Things (IoT) aims to improve our lives by increasing the interconnectivity of an increased variety of embedded computing devices using components of existing Internet infrastructure. This will allow for communications between sensors in home appliances, mobile phones, cars, laptops, factory machineries and many other devices that are already capable of network access through existing protocols like 3G, Wi-Fi, Bluetooth and ZigBee. Practical applications of this new technology are numerous, ranging from environmental monitoring to infrastructure management and home automation. This is the idea of ubiquitous computing where computers appear everywhere and applications run seamlessly between devices to manage everything from efficient energy consumption in factories to our weekly shopping.

Advances in mobile and pervasive computing, social network technologies and the exponential growth in Internet applications and services will lead to the development of the next generation of Internet services (Internet of Things (IoT)) that are pervasive, ubiquitous and touch all aspects of our life. It is expected that the number of IoT devices will reach more than 50 billion devices by 2020 [4] [5]. The integration of physical and cyber systems as well as the human behaviors and interactions (e.g., producers, consumers and attackers) will dramatically increase the vulnerability and the attack surface of interdependent infrastructure ecosystems. The most common architecture to monitor and control smart infrastructures such as Smart Homes (SH) and Smart Buildings (SB) are Building Automation Systems (BAS) and Supervisory Control and Data Acquisition (SCADA) systems. As BAS and SCADA systems become interconnected with Internet resources and services, they become easy

targets to cyber adversaries, especially since they were never designed to handle cyber threats; they were designed to operate in a completely isolated environment from corporate networks and the Internet. This makes control system data vulnerable to falsification attacks that lead to incorrect information delivery to users, causing them to take wrong and dangerous actions or to be unaware of an attack underway, as it was the case with Stuxnet attack [7]. It also allows adversaries to potentially execute malicious commands on control systems and remote devices, causing harmful actions. Therefore, it is critically important to secure and protect the IoT operations of such systems against cyber-attacks. In this paper, first IoT security framework is introduced for Smart Homes that consists of four layers: devices (end nodes), network, services, and application. An ABA-IDS is there to detect anomalies that could be triggered by attacks against the sensors of the first layer will be developed. Our approach by launching several cyber attacks against our Smart Home test bed developed at the University of Arizona Center for Cloud and Autonomic Computing is evaluated.

II. RELATED WORK

In order to develop our IoT security framework, our analysis is based on three IoT environments where user experience is particularly important. These are a body area IoT, a home IoT and a service industry hotel IoT.

Body area IoT: Nowadays, there are over three million pacemakers and 1.7 million implantable cardio-verter defibrillators inside people's chests. In 2006, they started becoming wireless. In 2013, a computer hacker called Barnaby Jack claimed that he can hack pacemakers to either shut them down or make them send a high voltage shot to the heart [8]. The US Food and Drug Administration also issued guidance to medical technology manufacturers warning against the security risks in body area devices' systems [9]. Therefore, currently, body area devices really need protections. A session key between the device and its coordinator can dramatically improve the security of body area IoTs.

Home IoT: Smart homes are becoming very popular in recent years. This includes home automation, intelligent lighting, security services and many other services. All services require many different types of devices or sensors installed in different places. Security of wireless communications between devices and the coordinator plays an important role in this situation.

Hotel IoT: Hotels provide a wireless access service. Thus, guests can access the Internet using this service. Guests' devices, for example, mobile phones and on-body sensors, can also access the Internet using this service. If an attacker sets up a hotspot with the same name as the hotspot provided by the hotel and if a guest chooses to connect to the fake hotspot, their private information and even bank details (provided for purchasing wireless service) will be known to the attacker.

IOT CYBER SECURITY

IoT can be viewed as a ubiquitous network that enables monitoring and controlling a large number of heterogeneous devices that are geographically dispersed by collecting and processing and acting on the data generated by smart objects [10]. It represents intelligent end-to-end systems that enable smart solutions and covers a diverse range of technologies including sensing, communications and networking, in [10]. This diverse and dynamic use of resources made security a major challenge. Traditional IT security solutions are not directly applicable to IoT due to the following issues [10]: 1) The IoT extends the "internet" through the traditional

internet, mobile network, non IP networks, sensor network, cloud computing and fog computing; 2) Computing platforms, constrained in memory and processing capability and consequently may not support complex security algorithms; 3) All "things" will communicate with each other. This leads to multiple access points that can be used to exploit existing vulnerabilities and 4) Some IoT devices and services may be shared and could have different ownership, policy and connectivity domains.

III. PROPOSED MODEL

A. IOT/M2M SECURITY FRAMEWORK

There are several IoT frameworks that can be used to create a threat model and apply mitigation strategies. To address the highly diverse IoT environment and the related security challenges, a flexible security framework is required. Figure 1 shows an architecture that can be used to guide the security development of an IoT smart infrastructure and framework to secure the IoT environment and is comprised of four components:

1. Authentication
2. Authorization
3. Network Enforced Policy
4. Secure Analytics: Visibility and Control

1. Authentication

At the heart of this framework is the authentication layer, used to provide and verify the identify information of an IoT entity. When connected IoT/M2M devices (e.g., embedded sensors and actuators or endpoints) need access to the IoT infrastructure, the trust relationship is initiated based on the identity of the device. The way to store and present identity information may be substantially different for the IoT devices. Note that in typical enterprise networks, the endpoints may be identified by a human credential (e.g., username and password, token or biometrics). The IoT/M2M endpoints must be fingerprinted by means that do not require human interaction.

2. Authorization

The second layer of this framework is authorization that controls a device's access throughout the network fabric. This layer builds upon the core authentication layer by leveraging the identity information of an entity. With authentication and authorization components, a trust relationship is established between IoT devices to exchange appropriate information. For example, a car may establish a trust alliance with another car from the same vendor. That trust relationship, however, may only allow cars to exchange their safety capabilities. When a trusted alliance is established between the same car and its dealer's network, the car may be allowed to share additional information such as its odometer reading, last maintenance record, etc.

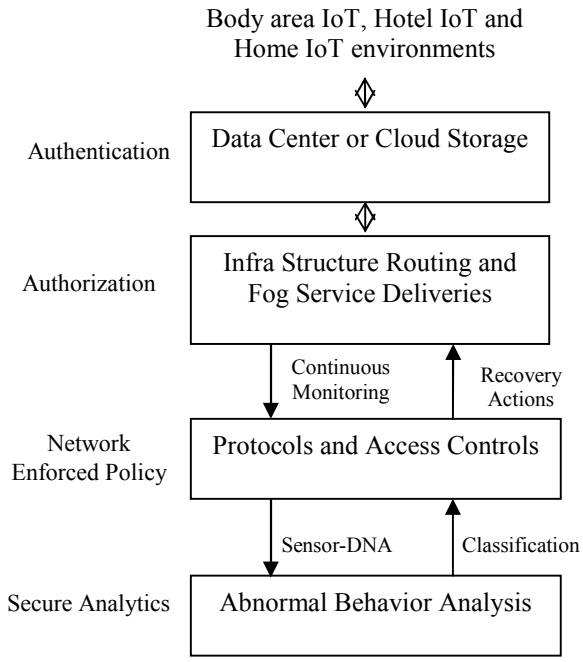

Fig. 1: IOT/M2M SECURITY FRAMEWORK WITH ABA METHODOLOGY

3. Network Enforced Policy

This layer encompasses all elements that route and transport endpoint traffic securely over the infrastructure, whether control,

management or actual data traffic. Like the Authorization layer, there are already established protocols and mechanisms to secure the network infrastructure and affect policy that are well suited to the IoT/M2M use cases.

4. Secure Analytics: Visibility and Control

This secure analytics layer defines the services by which all elements (endpoints and network infrastructure, inclusive of data centers) may participate to provide telemetry for the purpose of gaining visibility and eventually controlling the IoT/M2M ecosystem. The data, generated by the IoT devices, is only valuable if the right analytics algorithms or other security intelligence processes are defined to identify the threat. Better analytical outcome can be gotten by collecting data from multiple sources, applying security profiles and statistical models that are built upon various layers of security algorithms. It is all known that network infrastructures are becoming more complex. Imagine topologies with both public and private clouds; the threat intelligence and defense capabilities must also be cloud-based. Orchestration of the visibility, context and control is required to drive accurate intelligence. The components within this layer include the following:

- The actual IoT/M2M infrastructure from which telemetry and reconnaissance data is acquired and gathered
- The core set of functions to coalesce, analyze the data for the purposes of providing visibility and provide contextual-awareness and control
- The delivery platform for the actual analytics, built from the first two components, discussed above

While the actual IoT/M2M implementations may be different, the framework can be applied to any architecture. The framework is simple and flexible enough to service manned devices as well (e.g., laptops, handheld scanners, etc.) if they reside in the IoT infrastructure. Security threats are continuously emerging and require us to develop an architecture that can defend itself against those threats. This security framework provides the foundation from which appropriate security services can be selected. As specific contexts and verticals are considered, gaps can also be identified and addressed.

B. ABNORMAL BEHAVIOR ANALYSIS METHODOLOGY

Strategies have been developed to protect the operations of end nodes against any type of threat by using continuous monitoring and performing anomaly behavior analysis of the end nodes operations. The main modules to implement our approach are shown in Figure 2: 1) Continuous Monitoring, 2) Data structure, 3) Anomaly Behavior Analysis, 4) Sensor Classification, and 5) Recovery Actions.

1) Continuous monitoring

Software tools have been used to capture the behavior of SHT components that are important to characterize their normal operations. For example, let us use Wireshark monitoring tool to capture the required sensor operational data [24]. The information obtained from Wireshark includes source IP, destination IP, and content of packets. The sensor's data is extracted from the payload and sent to the Data Structure module, where the sensor is automatically identified and its runtime profile. Let us refer to the sensor profile as the Sensor- DNA data structure (s-DNA) that is built by using Discrete Wavelet Transform (DWT) method.

2) Data Structure

This module performs two tasks: 1) Compute the DWT coefficients form the signal and 2) Identify sensor type based on received data to create the runtime profile

that will be compared with the reference s-DNA in the ABA module.

a. DWT coefficients

The data obtained from the sensor is decomposed using DWT method as shown in Equations (1) and (2). In each level of the decomposition, the extracted coefficients are used to build the s-DNA data structure which is used by the ABA module.

$$y_{high}[k] = \sum_n x[n] * g[2k - n] \text{ ---- (1)}$$

$$y_{low}[k] = \sum_n x[n] * h[2k - n] \text{ ---- (2)}$$

The original signal $x[n]$ is decomposed into an approximation co-efficient $y_{high}[k]$ and a detail coefficient $y_{low}[k]$by applying a high pass $g[n]$ and a low pass $h[n]$ filters respectively. The number of samples in the signal follows $n = 2i$ form. The DWT can be computed efficiently in a linear time, which is important when dealing with large datasets. Haar wavelet is used as the function to extract the coefficients because any continuous function can be approximated with this function. Once the signal is decomposed, the coefficients of each level are aggregated in a single vector that is used to build the s-DNA data structure.

b. Sensor classification

The next step is to identify the sensor type based on the received data. For this task, the Euclidean distance D_j in Equation (3) is computed between the runtime coefficient vector $\boldsymbol{v}$ and a matrix $\boldsymbol{M}$ of coefficients obtained during the offline training phase.

$$D_j = \sqrt{\sum_{i=1}^{n} \left(M_{i,j} - v_i\right)^2} \text{ ------ (3)}$$

The smallest distance obtained is used to classify the sensor type. Once the sensor type has been identified, the rest of the data is compared with the coefficients in the same column (j) of the matrix to obtain the Euclidean distance.

3) Abnormal Behavior Analysis

The Euclidean distance is compared with the reference model in the ABA. The reference model is built during the offline training by using normal measurement attributes (normal Euclidean distance). Five vectors are used to find the control limits for normal operation [24]. Each vector is compared with the rest. Once all the distances are computed, the mean value (CL) is calculated from the samples. The Upper Control Limit (UCL) and the Lower Control Limit (LCL) for the normal behavior are calculated using Equations (4) and (5), where $\bar{x}$ is the mean value, α is the standard deviation and σ is a sensibility level.

$$UCL = \bar{x} + \alpha\sigma \text{ ----- (4)}$$

$$UCL = \bar{x} - \alpha\sigma \text{ ----- (5)}$$

For normal control limits, let us assume α =3. However, which can establish warning upper and lower limits (WUL and WLL, respectively) at α =*2*.

4) Classification

Once the ABA module has determined that there is an abnormality in the data provided by the sensor, the classification unit function is to identify the type of observed abnormality. For this task the Euclidean distance is used to detect behaviors and trends. For example in a DoS attack, the distance shows sudden changes above the UCL.

5) Recovery actions

When an abnormal behavior is detected, several recovery actions can be taken (e.g. discard data, authenticate the sensor, change network configuration, etc.). However, there is a possibility that the attack cannot be classified (e.g. new attacks), in such cases the data is rejected.

IV. RESULT

The performance of ABA approach is evaluated for the attacks shown in table (1) when they are launched against all the sensors available in our test bed. It also summarizes the detection and classification accuracy of propose approach for each attack type.

Table. 1: TESTED ATTACKS

Attack	Detection Rate	Classification Rate
Replay Attack	96	98
Sensor Impersonation	96	88
Delay Attack	98	85
DoS Attack	95	95
Flooding Attack	85	95

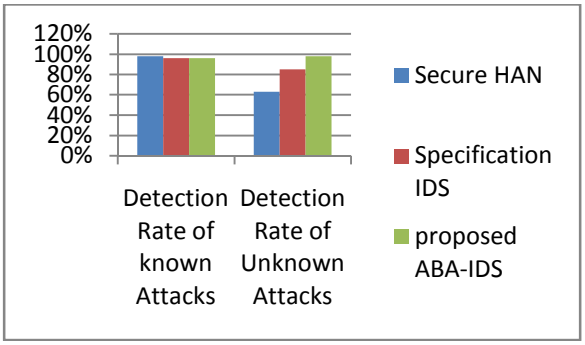

Fig. 2: RATE COMPARISON OF DIFFERENT METHODS

Figure (2) shows that the ABA-IDS has a detection rate better than the compared approaches for unknown attacks and unlike signature-based IDS, it is able to detect new attacks.

V. CONCLUSION

In this paper, three typical IoT applications, namely, body area IoT, home IoT and hotel IoT, are reviewed through user studies and was found that IoT security is a serious problem concerned by users. Furthermore, a security framework for the IOT environment along with anomaly behavior analysis methodology was designed. The framework can serve as a foundation for supporting the security of IoT applications that provides essential authentication and secure communications thus satisfying the main concerns of users derived from the user studies. The proposed anomaly behavior analysis methodology includes the use of a sensor-DNA profile (s-DNA) that is developed to accurately characterize normal sensor operations. It was also shown that the ABA approach can detect both known and unknown attacks with high detection rates and low false positive alarms. An attack classification methodology was developed with 98% accuracy for known attacks and up to 96% for unknown attacks (classified as "new attacks").

VI. REFERENCES

[1] L. Xiao, X. Wan, X. Lu, Y. Zhang and D. Wu, "IoT Security Techniques Based on Machine Learning: How Do IoT Devices Use AI to Enhance Security?", *IEEE Signal Processing Magazine*, vol. 35, no. 5, pp. 41-49, Sept. 2018.

[2] J. Sonnerup and J. Karlsson, "Robust Security Updates for Connected Devices", pp. 105, March 2016.

[3] R. Schlegel, S. Obermeier, J. Schneider, "Structured System Threat Modeling and Mitigation Analysis for Industrial Automation Systems", IEEE 13th International Conference on Industrial Informatics (INDIN), July 2015.

[4] Verizon (January, 2015). Create intelligent, more meaningful business connections. Retrieved from http://www.verizonenterprise.com/solutions/connected-machines/

[5] Z. Andrea, B. Nicola, Angelo C., Lorenzo V., and Michele Z., "Internet of Things for Smart Cities", IEEE Internet of Things journal, vol. 1, no. 1, February 2014.

[6] Osseiran A, Boccardi F, Braun V, et al. Scenarios for 5G mobile and wireless communications: the vision of the METIS project. IEEE Communications Magazine 2014; 52(5):26–35.

[7] D. Kushner, "The Real Story of Stuxnet, How Kaspersky Lab tracked down the malware that stymied Iran's nuclear-fuel enrichment program", IEEE Spectrum, February 2013.

[8] US Food and Drug Administration. Content of premarket submissions for management of cyber security in medical

devices: draft guidance for industry and food and drug administration staff. 2013.
[8] Kirk J. Pacemaker hack can deliver deadly 830-volt jolt. Computerworld 2012, 17.
[10] H. Suo, J. Wan, C. Zou, J. Liu, "Security in the Internet of Things: A Review", International Conference on Computer Science and Electronics Engineering (ICCSEE), 2012, vol. 3.

Vallem Sushma Latha is currently working as an Assistant Professor in the Department of Computer Science & Engineering, Talla Padmavathi College of Engineering,Warangal, Telangana, India. She is having 9+ years of experience in teaching and her area of interest includes Machine Learning, IOT, and Cloud Computing etc.

Garidepalli Revathi is currently working as an Assistant Professor in the Department of Computer Science & Engineering, Talla Padmavathi College of Engineering,Warangal, Telangana, India. She is having 4+ years of experience in teaching and her area of interest includes Networking, Machine Learning, IOT, Cloud Computing etc.