Enabling Risk Management for Smart Infrastructures with an Anomaly Behavior Analysis Intrusion Detection System

Jesus Pacheco[1] Xiaoyang Zhu[2] Youakim Badr[2] Salim Hariri[1]

[1]Electrical and Computer Engineering Department
The University of Arizona
Tucson, USA

{Jpacheco, hariri}@email.arizona.edu

[2]University Lyon, INSA-Lyon,
LIRIS UMR 5205, F-69621
Lyon, France

{youakim.badr, xiaoyang.zhu}@insa-lyon.fr

Abstract— The Internet of Things (IoT) connects not only computers and mobile devices, but it also interconnects smart buildings, homes, and cities, as well as electrical grids, gas, and water networks, automobiles, airplanes, etc. However, IoT applications introduce grand security challenges due to the increase in the attack surface. Current security approaches do not handle cybersecurity from a holistic point of view; hence a systematic cybersecurity mechanism needs to be adopted when designing IoT-based applications. In this work, we present a risk management framework to deploy secure IoT-based applications for Smart Infrastructures at the design time and the runtime. At the design time, we propose a risk management method that is appropriate for smart infrastructures. At the design time, our framework relies on the Anomaly Behavior Analysis (ABA) methodology enabled by the Autonomic Computing paradigm and an intrusion detection system to detect any threat that can compromise IoT infrastructures by. Our preliminary experimental results show that our framework can be used to detect threats and protect IoT premises and services.

Keywords- IoT; cyber security; anomaly behavior analysis; threat model; risk management.

I. INTRODUCTION

Advances in mobile and pervasive computing, social network technologies and the exponential growth in Internet applications and services lead to the development of the next generation of Internet services known as the Internet of Things. It is expected that the number of IoT devices will reach more than 50 billion devices by 2020 [1]. IoT-based services will be a key enabling technology to the development of smart cities that will revolutionize the way we do business, maintain our health, manage critical infrastructures, conduct education, and how we secure, protect, and entertain ourselves [2][3].

IoT applications, such as critical infrastructures (e.g., smart grid) are large-scale distributed systems, comprised of complex systems and characterized by interdependence, independence, cooperation, competition, and adaptation [4][5]. Examples of large-scale IoT applications comprise electric grids interconnected with other sectors (smart grids), the urban transportation sector interconnected with the wireless network (smart transportation), building devices integrated into a larger home monitoring system (smart buildings), federated health information systems (smart health), just to mention a few. In this context, systems interact with each other using different levels of trust relationships, and consequently, require ultimate security solutions to protect information and processes.

With the use of IoT techniques, we are experiencing grand challenges to secure and protect such advanced information services due to the significant increase in the attack surface [6]. The interconnections between growing amounts of devices expose the vulnerability of IoT applications to attackers. Even devices, which are intended to operate only in local area networks, are sometimes connected to the Internet due to careless configuration or to satisfy special needs (e.g., they need to be remotely managed). As a result, devices can be easily compromised and become subject to cyber-security risks and attacks with severe impacts (e.g., life threatening scenarios) [3][5].

In order to reduce security threats, risk management is used to support information systems by identifying security constraints on what should be protected by applying systematic and reliable risk management methodologies [6]. However, applying risk management to the IoT is not as straightforward as the risk management in information systems [7]. In fact, IoT is still in its infancy with lack of common standards and a wildly divergent number of communication protocols, hardware and software platforms to solve IoT problems, and rapid changes in technologies, which bring new, and unforeseen risks.

Given this, a new risk management approach is needed to protect IoT-based applications by continuously identifying security risks not only at design time of IoT-based applications but also at runtime.

To this end, we introduce an IoT risk management framework for smart Infrastructures to recognize vulnerabilities and identify possible countermeasures in order to mitigate their exploitation. Our framework consists of four layers: devices (end nodes), network, services, and application and relies a general threat model covering risks at each layer. At run-time, the framework provides an Anomaly Behavior Analysis Intrusion Detection System (ABA-IDS) to detect anomalies that could be triggered by attacks against elements in each layer (e.g., sensors, protocols, wireless

978-1-5090-6558-5/17 $31.00 © 2017 IEEE
DOI 10.1109/FAS-W.2017.167

communication, etc.). The main feature of ABA-IDS is its capability in detecting novel attacks. Our ABA-IDS defines a baseline model for normal behavior of each layer through off-line training, and considers any activity, which lies outside of this normal model as anomaly.

From experimental standpoint, we have evaluated our framework by launching several cyberattacks (e.g. Sensor Impersonation, Replay, and Flooding attacks) against our Smart Building testbed developed at the University of Arizona Center for Cloud and Autonomic Computing. The results show that our IoT security framework can be used to develop effective security mechanisms to protect the normal operations of each layer. Moreover, our framework can detect known and unknown attacks against IoT elements with high detection rate and low false alarms.

The rest of the paper is organized as follows. Section II gives a brief overview on the related work. Section III is devoted to explain our IoT security framework for smart infrastructures. In section IV we show some of our preliminary results for each layer of our framework. The last section concludes the paper and discusses future research directions.

II. Related Work

The need for sharing resources and information expose the vulnerability of IoT systems and their data to attacks (e.g., falsification attacks), leading to incorrect information delivery to users and causing them to take wrong and dangerous actions. For example, the case with Stuxnet attack [11], was successfully launched and compromised nuclear plant facilities. In this case, the main concern was the elevation of privileges to perform malicious actions against cyber physical systems. Another example is in [12], where the authors show how a Bluetooth connection was used in a smart city to change traffic sensors firmware to gather information and to modify the data provided by those sensors. In this attack, the main concern is information disclosure and falsification. The aforementioned examples are some real-world scenarios that show how critically important is to secure and protect IoT operations against cyberattacks.

Studies have shown that security in any IoT application will be crucial in the years to come. Hence, various approaches have been proposed in the literature to deal with key IoT elements (e.g., end devices, protocols, services, etc.). For instance, in [14] the authors show how the pre-shared keys solutions could be used in limited real-life scenarios where the distribution of keys in an offline mode is possible. In [15] an Internet Key Exchange compression scheme has been proposed to provide a lightweight automatic mechanism to establish security associations for IPsec and HIP Base Exchange. Another approach can be seen in [16], in which the authors introduced a delegation procedure that enables a client to delegate certificate validation to a trusted server. While the proposed delegation approaches reduce the computational load at the constrained nodes, they break the end-to-end principle by requiring a trusted third party.

Improving security and reducing risks in the Internet of Things rely on analysing threats, risks and vulnerabilities to specify appropriate countermeasures. Many methodologies of risk assessments are proposed in literature for information systems such as EBIOS [21], OCTAVE [22], CRAMM [23] and MEHARI [24]. These methods cover the identification of *asset*, *access mode*, *actor involved*, *motivations*, *effect* and links them to actions and estimates their *impacts* and cost. They require a well-known context definition as en entry point to asset all related elements to the risk analysis and vulnerability evaluation. Unfortunately, the context is unpredictable in the Internet of Things since all devices and actuators are distributed in a dynamic environment. Despite their differences they share a main factor, which is "The context definition". This factor makes risk management harder to be adapted in dynamic environments where the system's context may change permanently.

The pervasive, distributed, and evolving nature of IoT applications makes it difficult to consider security from a holistic point of view. To address this problem, we have proposed an IoT risk management framework that can be used at design time when architecting smart infrastructures. We will discuss our approach in the next sections.

III. IoT Risk Management Framework for Smart Infrastructures

In the realm of the Internet of Things, risk management should take into account dynamic context. In addition, Continuous evolution of dynamic environments and advances of IoT-based technologies require new strategies to secure resources connected devices. Risk evaluation should be adapted to an ever-changing context during the execution of connected devices and without loss of functionalities. A global security policy must be adapted at any time to address new changes, which leads to new challenges in risk management in the Internet of Things.

We propose to extend the risk management in traditional information systems to enable security and risk management in the Internet of Things. The first step toward secured critical infrastructures in the Internet of Things in a dynamic environment tackles with the definition of the 'context' and the identification of functionalities and characteristics to establish a risk management framework of trust communities.

Our proposed risk management framework aims at reducing security risks not only at the design time by assessing risks but also at runtime by enabling an Anomaly Behavior Analysis Intrusion Detection System (ABA-IDS). The risk management framework consists of a risk management methodology, covering four levels (applications, services, communications and end nodes) and applying four fundamental functions (see Fig. 1):

- Model Specification: To characterize the normal operations for each layer. This is helpful to build the reference model that describes the normal behavior of the system at each stage.

- Attack Surface Identification: To identify the entry points that can be exploited by a cyber adversary.
- Impact Analysis: To analyze the impact of a cyber-attack.
- Risk Mitigation: To accurately choose the protection mechanism to be applied in compliance to the impact analysis.

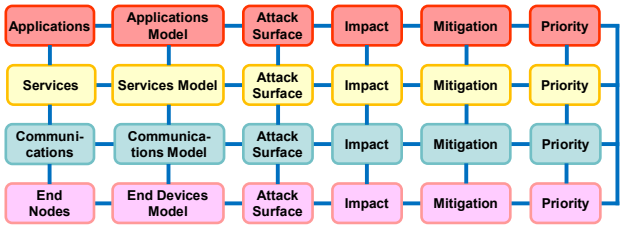

Fig. 1. IoT Risk Management Framework for Smart Infrastructures

In the first level (end nodes) the information passes through physical devices to identify or modify the physical world. These information include object properties, environmental conditions, raw data, etc. The key components in this level are sensors for capturing and representing the physical world into the digital world, actuators to modify the environment to a desired state, local controllers to take immediate actions when required. The targets at this level are local controllers, sensors, actuators, and information. The impact can be loss or waste of energy, human safety, and provider's reputation. Mitigation mechanisms include lightweight encryption, sensor authentication, IDS, and behavior analysis.

Communications are responsible for reliable transmissions of information from, and to end nodes. The technologies used in this level include the Internet protocols (HTTP, TCI/IP), radio and mobile communication networks (LoRa, GSM, LTE, ...) and network infrastructures,. An intruder can target protocols, firewalls, routers, or communication bus to gather information or to launch malicious commands. The impact can be measured in terms of money loss, human safety, privacy, and energy consumption. To overcome the mentioned issues, authentication and encryption techniques can be used (among other techniques).

At service level, all the required computational power is mostly provided as a cloud and/or fog services. This level is used for remotely monitoring and controlling the system, as well as to store data and analyze large amount of information. An attacker can target cloud storage to gather information or change the content in cloud-based databases/containers, leading to scenarios such as life threatening scenarios, loss of money, and information disclosure. Mitigation mechanisms at this level include encryption, intrusion detection systems, selective disclosure, and data distortion.

The application layer provides the personalized services according to the needs of the user. The access to the IoT services is through this layer and it can be via mobile technology such as cellphone, mobile applications, or a smart appliance or device. In this layer, data sharing is an important characteristic and consequently application security must address data privacy, and access control.

At each level, risk management is assessed by enforcing accurate security policies, this way our framework complies with the National Institute of Standards and Technology (NIST) Security Framework for Critical Infrastructures [8]. As shown in Fig. 1, each layer of the IoT architecture has its own threat model that can be defined in terms of five components: Layer service model, Attack surface, Impact, Mitigation and Priority. For each level, after we define the behavior or functional model, we identify the Attack Surface that characterizes the entry points that can be exploited by attackers to inject malicious events to impact the normal operations of that layer. Then we identify the potential impact of exploiting the vulnerabilities. With the obtained information, we identify the mitigation mechanisms that can be implemented to diminish these threats. Finally we prioritize the mitigation strategies according to the potential impact to the system. By following this architecture, we can ensure the development of highly secure and trustworthy IoT services.

IV. Preliminary Results

A. *End Nodes Level*

As we previously mentioned, the key components in this layer are the sensors, actuators, and local controllers. We have experimented with sensors in the first level to detect when an IoT sensor has been compromised by an adversary. For this case we first extract unique signatures to describe the behavior of sensors using Discrete Wavelet Transform (DWT) [3]. A set of signatures is used to build the reference model which is built taking into consideration the Euclidean Distance (ED) between signatures. From the obtained EDs, we compute the mean and standard deviation to create establish the limits of normal operation [3]. The reference model contains a sample signature and the limits of normal operation. After we obtain the reference model, we extract runtime signatures to detect any drift in the behavior (when ED exceeds normal operation limits) that we call it abnormal behavior. This method can be also used to create signatures for known attacks (e.g., replay attack), this way our risk management approach can take more accurate mitigation actions. Table I shows some of the results we obtained for a set of attacks against IoT sensors.

TABLE I. TESTED ATTACKS VS DETECTION RATE FOR END NODES

Attack	Detection Rate
Replay Attack [17]	98 %
Delay Attack [18]	98 %
DoS Attack [18]	99.9 %
Flooding Attack [18]	98 %
Sensor Impersonation [19]	97.4 %
Pulse DoS [18]	96 %
Noise injection [20]	100 %

From Table I, the pulse DoS and noise injection attacks were not used to train the system but they can be detected. There are two cases that trigger false positives, the first case happens when the behavior is not considered in the training phase (e.g. a cold object near the temperature sensor). In the second case, the sensor needs to reach its steady state after an attack. Our experiments show that at most 3.2% of these situations produced false positives alerts.

B. Communications Level

A key component in the communications level is the secure gateway which is the point of access (locally) to the system, to monitor sensors or issue commands to the actuators. To highlight the usability of our framework, in this layer we have developed an anomaly behavior analysis (ABA) methodology to detect attacks targeting the availability of a secure gateway, which is part of the communication layer in our IoT risk management framework. Our ABA methodology uses as principle that, systems normal behavior can be characterized using global variables such as system memory, devices mounted, hardware configuration, etc. We divided our methodology in two stages:

- **Offline training.** The final goal of this stage is to create the reference model of the system. The first step is to select the features that are useful to characterize the system, after verifying the correlation of 260 system variables available, we found that 11 are enough to represent the secure gateway normal behavior. The next step is to create a dataset of the selected features. Our dataset contains both the normal data, which represents the normal behavior of the system, and the abnormal data, which represents the behavior of the system under known attacks. We built the model of normal operations based on the selected features using datamining techniques (e.g., JRip [9]). Once the model is extracted, it is tested in the second stage (runtime) looking for detection accuracy and false positive alerts.

- **Runtime testing.** The main goal of the runtime unit is to classify the behavior of the system and rank the impact of an abnormal behavior to perform accurate risk management. The first step is to collect the information (monitoring) about the selected features. Then we classify the incoming traffic as normal or abnormal having into consideration a rule-based model created using JRip. If the traffic has determined to be abnormal, the impact of the abnormality is classified using a decision tree [9].

Some of the obtained results at this level are shown in Table II. As it can be seen from Table II, the worst-case scenario for our methodology is 92.3% detection rate for Pulse DoS. However some of the detected attacks were not trained in the system, meaning that our ABA methodology can be used to detect known and unknown attacks with high detection rate and low false positives (less than 3% in the worst-case scenario).

TABLE II. TESTED ATTACKS VS DETECTION RATE FOR COMMUNICATIONS

Attack	Detection Rate (%)
Flooding [18]	94.2
Replay [17]	96.3
PulseDoS [18]	92.3
HTTP GET [20]	98.0
Replay + HTTP GET	99.2

C. Services Level

At services layer, all the required computational power is mostly provided by cloud services. This layer is used for remotely monitoring and controlling IoT systems, as well as to store data and analyze large amount of information. In general, IoT services can be allocated in four categories:

1) identity services,
2) information aggregation services,
3) collaborative-aware services, and
4) ubiquitous services.

Based on our work in [10], we adopted a holistic approach to define a security conceptual model that covers all elements at the business, service, and infrastructure levels (Fig. 2) and illustrates the casual relationships between these levels. In practice, the dependency model is a complex graph because it is built from instances of each type of essential assets, and, hence, it can be learned from lists of essential assets using Bayesian networks for example.

Since the information security is subject to uncertain and unforeseen threats, we proposed a fuzzy logic decision system that helps identify security risks based on the security conceptual model and select appropriate security measures based on security objectives.

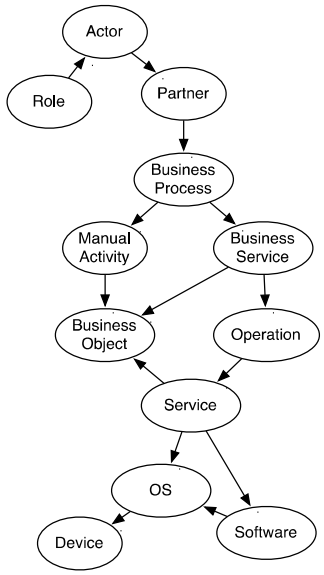

Fig. 2. The Dependency Model

D. *Application Level*

The application layer provides the services requested by customers. For instance, a mobile application can report home temperature measurements when it is requested by the home user. The relevance of this layer from the point of view of the IoT is that it has the ability to provide high-quality smart services to meet users' needs. In [6] we distinguish between steady and dynamic environments in which information systems are deployed and monitored. We demonstrated that a global security policy must be adapted at any time to address new changes in dynamic environments to cope with new challenges in risk management. We introduce a holistic approach for risk and security management through the definition of Service Characteristics Infrastructure, including certificate authorities, signed service characteristics, and security policies.

V. Conclusion and Future Work

Due to the exponential growth in number of interconnected devices, cyber-security in the IoT is a major challenge. It heavily relies on the digital identity concept to build security mechanisms such as authentication and authorization. In this paper we introduced an IoT Risk Management Framework for Smart Infrastructures that can be used as a systematic way to build general protection mechanisms for IoT applications rather than creating ad-hoc solutions for each IoT application.

We are currently experimenting with a Blockchain-based Identity Framework for IoT (BIFIT). The idea is to apply our approach to IoT smart infrastructures to autonomously extract appliances signatures and creates Blockchain-based identities for the appliance owners.

Acknowledgements: This work is supported by Thomson Reuters in the framework of the Partner University Fund project: "Cybersecurity Collaboratory: Cyberspace Threat Identification, Analysis and Proactive Response". The Partner University Fund is a program of the French Embassy in the United States and the FACE Foundation and is supported by American donors and the French government.

References

[1] Verizon (May, 2017). Create intelligent, more meaningful business connections. Retrieved from http://www.verizonenterprise.com/solutions/connected-machines/

[2] 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.

[3] J. Pacheco, S. Hariri, "IoT Security Framework for Smart Cyber Infrastructures", IEEE 1st International Workshops on Foundations and Applications of Self-* Systems, Germany, 2016.

[4] V. Chiprianov, L. Gallon, M. Munier, P. Aniorte, and V. Lalanne.. Challenges in Security Engineering of Systems-of-Systems. In Troisième Conférence en IngénieriE du Logiciel (p. 143).

[5] R. Valerdi, A.M. Ross, and D.H. Rhodes. A framework for evolving system of systems engineering.

[6] P.B. Nassar, Y. Badr, K. Barbar, and F. Biennier, "Risk management and security in service-based architectures." In Advances in Computational Tools for Engineering Applications, 2009. ACTEA'09. International Conference on, pp. 214-218. IEEE, 2009.

[7] 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.

[8] National Institute of Standards and Technology (NIST), and United States of America. "Framework for Improving Critical Infrastructure Cybersecurity." (2017)

[9] I. Witten, F. Eibe, A.H. Mark, and J.P. Christopher. Data Mining: Practical machine learning tools and techniques. Morgan Kaufmann, 2016.

[10] Y. Badr, and Soumya Banerjee. "Managing End-to-End Security Risks with Fuzzy Logic in Service-Oriented Architectures." In Services (SERVICES), 203 IEEE Ninth World Congress on, pp. 111-117. IEEE, 2013.

[11] 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.

[12] D. Legezo (Kaspersky lab): How to trick traffic sensors. (April 2016). Retrieved from: https://securelist.com/blog/research/74454/how-to-trick-traffic-sensors/

[13] D. Takahashi, Y. Xiao, and F. Hu, "A survey of security in telemedicine with wireless sensor networks." Mobile Telemedicine: A Computing and Networking Perspective (2008): 209-235.

[14] Prashar M, Vashisht R. Survey on pre-shared keys in wireless sensor network. Int J Sci Emerging Technol Latest Trends. 2012;4(1):42–48.

[15] Sahraoui S, Bilami A. Efficient HIP-based approach to ensure lightweight end-to-end security in the internet of things. Comput Networks. 2015;91:26–45.

[16] T. Freeman, R. Housley, A. Malpani, D. Cooper, W. Polk, 2007. Server-based certicate validation protocol (scvp). Internet Proposed Standard RFC 5055.

[17] A. Hoehn, P. Zhang. "Detection of replay attacks in cyber-physical systems." In American Control Conference (ACC), 2016, pp. 290-295. IEEE, 2016.

[18] V. Namboodiri, V. Aravinthan, S. Mohapatra, B. Karimi, W. Jewell, "Toward a Secure Wireless-Based Home Area Network for Metering in Smart Grids," Systems Journal, IEEE, vol.PP, no.99, pp.1,12, 0 doi: 10.1109/JSYST.2013.2260700

[19] N. Tanabe, E. Kohno, Y. Kakuda. "A path authenticating method using bloom filters against impersonation attacks on relaying nodes for wireless sensor networks." In 2013 IEEE 33rd International Conference on Distributed Computing Systems Workshops 2013 Jul 8 (pp. 357-361). IEEE.

[20] V.P. Illiano, E. Lupu. "Detecting malicious data injections in wireless sensor networks: A survey". ACM Computing Surveys (CSUR). 2015 Nov 21;48(2):24.

[21] DCSSI: EBIOS - Expression of Needs and Identification of Security Objectives. 2004 http://www.ssi.gouv.fr/en/confidence/ebiospresentation.html

[22] J. Eom, S. Park, Y. Han, T. Chung, Risk Assessment Method Based on Business Process-Oriented Asset Evaluation for Information System Security, proc. ICCS 2007, Lecture Notes in Computer Science, Vol. 4489 (Springer Berlin, 2007) 1024-1031.

[23] Insight Consulting: CRAMM (CCTA Risk Analysis and Management Method) User Guide version 5.0. SIEMENS http://www.cramm.com/

[24] CLUSIF: MEHARI 2007 (Méthode Harmonisée d'Analyse du Risque Informatique). https://www.clusif.asso.fr/fr/production/mehari/