Journal of Network and Computer Applications 83 (2017) 12–27

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

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

A framework for automating security analysis of the internet of things

Mengmeng Ge*, Jin B. Hong, Walter Guttmann, Dong Seong Kim

University of Canterbury, Private Bag 4800, Christchurch, New Zealand

ARTICLE INFO

Keywords:
Attack graphs
Internet of things
Security analysis
Security modeling

ABSTRACT

The Internet of Things (IoT) is enabling innovative applications in various domains. Due to its heterogeneous and wide-scale structure, it introduces many new security issues. To address this problem, we propose a framework for modeling and assessing the security of the IoT and provide a formal definition of the framework. Generally, the framework consists of five phases: (1) data processing, (2) security model generation, (3) security visualization, (4) security analysis, and (5) model updates. Using the framework, we can find potential attack scenarios in the IoT, analyze the security of the IoT through well-defined security metrics, and assess the effectiveness of different defense strategies. The framework is evaluated via three scenarios, which are the smart home, wearable healthcare monitoring and environment monitoring scenarios. We use the analysis results to show the capabilities of the proposed framework for finding potential attack paths and mitigating the impact of attacks.

1. Introduction

In the Internet of Things (IoT), every physical object becomes locatable, addressable and reachable in the virtual world (Roman et al., 2011, 2013; Sicari et al., 2015). As more and more objects in the physical world are expected to connect to the Internet, the IoT is supposed to contain millions or billions of objects which will communicate with each other and with other entities (e.g., human beings). These objects not only include computers and laptops which already exist in traditional networks, but also physical devices (such as home appliances), vehicles, *etc*. The heterogeneity of devices and technologies that are used for providing services has a great impact on the interoperability and management of IoT devices. Besides, many devices have constrained resources and limited computational capabilities and are deployed in an open environment (e.g., street lights), which makes them prone to being controlled or destroyed by malicious people. With its inherent complexity and heterogeneous structure, the IoT is facing numerous threats and attacks which will negatively affect its normal functionality. Thus protecting the security of the IoT is a difficult yet important task.

The motivation of our work lies within the field of security modeling for the IoT. Vulnerabilities of the IoT reside in different aspects, including devices (hardware, operating systems), communication protocols, service applications, service APIs and the design of the IoT architecture. By exploiting such vulnerabilities, an attacker can launch various attacks including eavesdropping, Denial of Service (DoS) attacks, node capture and node controlling (Roman et al., 2013). With the presence of varied and complex attacks, the ability to discover potential attack scenarios (e.g., an attacker's paths to a target IoT device) and to mitigate the impact of malicious attacks becomes a critical issue. Research on modeling the security of the IoT is also very limited due to the pioneering nature of the IoT.

In this paper, we propose a framework for modeling and assessment of the security of the IoT. The framework is used to construct a graphical security model and a security evaluator to automate the security analysis of the IoT. More specifically, the graphical security model is based on the Hierarchical Attack Representation Model (HARM) (Hong and Kim, 2012) to capture potential attack paths in the network. We refer to our model as the extended HARM; it adds to the basic HARM another layer describing subnets and their connectivity. The security evaluator uses various security metrics to assess the security and interacts with an analytic modeling and evaluation tool, Symbolic Hierarchical Automated Reliability and Performance Evaluator (SHARPE) (Sahner et al., 1996), to output the analysis results. The driving idea behind the framework is to mitigate the impact of potential attacks in the IoT and increase the IoT security level.

An earlier version of this paper appeared in Ge and Kim (2015), and we have extended the earlier version with (1) a formal definition of the framework, (2) a three-layer graphical security model (i.e., the extended HARM) for the IoT, (3) detailed calculation steps of security metrics and (4) a comprehensive evaluation using both heterogeneous

* Corresponding author.
E-mail addresses: mge43@uclive.ac.nz (M. Ge), jho102@uclive.ac.nz (J.B. Hong), walter.guttmann@canterbury.ac.nz (W. Guttmann), dongseong.kim@canterbury.ac.nz (D.S. Kim).

http://dx.doi.org/10.1016/j.jnca.2017.01.033
Received 20 April 2016; Received in revised form 28 November 2016; Accepted 25 January 2017
Available online 29 January 2017

and homogeneous networks.

To the best of our knowledge, this work is the first approach to use a graphical security model in modeling and assessing security for the IoT. The main contributions of this paper are summarized as follows:

- Propose a framework for modeling and assessing security of the IoT (Section 4.1);
- Develop a graphical security model to compute attack scenarios (Section 4.1);
- Formally define this framework (Section 4.2);
- Use various security metrics to carry out the analysis (Section 4.2); and
- Evaluate the framework using three scenarios, including a smart home, wearable healthcare monitoring and environment monitoring (Section 5).

The rest of the paper is organized as follows. Section 2 gives background information about the graphical security model, HARM and the evaluation tool (SHARPE). Section 3 presents related work on existing security modeling approaches for the IoT and discusses their constraints. Our framework for modeling and analyzing security of the IoT is described and formally defined in Section 4. The framework is evaluated with three different scenarios in Section 5. Extensions and limitations of the framework are discussed in Section 6. Finally, Section 7 concludes the paper.

2. Background

We introduce the HARM and the extended HARM, which is used as our security model and the SHARPE, which is used as our external evaluator.

Graph-based and tree-based security models (e.g., attack graphs (AGs) (Sheyner et al., 2002), attack trees (ATs) (Saini et al., 2008)) have been widely used in assessing the security of systems. In graph-based attack models, an AG shows all possible sequences of attackers' actions that eventually reach the target. With increasing size of the network, calculation of a complete AG has exponential complexity, thus causing a scalability problem. In tree-based attack models, an AT is a tree with nodes representing attacks and the root representing the goal of attacks. It systematically presents potential attacks in the network. However, an AT does not explicitly reflect the sequences of attackers' actions.

In order to address the above issues, the two-layer HARM (Hong and Kim, 2012) was introduced to combine AGs and ATs. In the HARM, the upper layer captures the network reachability information and the lower layer represents the vulnerability information of each node in the network. The layers of the HARM can be constructed independently of each other. This decreases the computational complexity of calculating and evaluating the HARM compared with the calculation and evaluation of an AG. Thus, the HARM addresses the scalability problem of the single layer AG. Besides, by using an AG for the network reachability in the upper layer, the HARM can show the sequences of attackers' actions which cannot be captured by using an AT.

To further improve the scalability, the three-layer HARM was developed in Hong and Kim (2016) with the subnet reachability at the highest layer. In the three-layer HARM, the complexity of the security evaluation is further decreased because computations are grouped in each layer using a bottom-up approach. The mobility of devices (e.g., node addition or removal) can be easily adjusted in the three-layer HARM without reconstruction of the whole model. Additionally, more layers can be used based on different IoT scenarios. For example, a smart home with several networks (e.g., Wi-Fi, Bluetooth, *etc*) can be modeled using the three-layer HARM; a number of smart homes in an area can be modeled using the four-layer HARM with the home connectivity in the highest layer.

The SHARPE (Sahner et al., 1996) is a software package for performance and reliability analysis of computer systems. It accepts a mathematical model of the system and analyzes it using various algorithms. Several model types are provided, for example, Markov chains, Semi-Markov chains, reliability block diagrams, fault trees and reliability graphs. Each model type supports at least one analysis algorithm; for example, fault trees have five analysis algorithms including reliability, unreliability, mean-time-to-failure, *etc*. Given the behavior of the components of a system in the form of time-dependent functions and the structure of the system in the form of a model type, the SHARPE can compute the behavior of the system as a function of time which is used for performance and reliability analysis.

3. Related work

We discuss current work on security models for IoT networks and non-IoT networks.

3.1. Security models for the IoT

Several papers focus on developing security modeling approaches for the IoT. We discuss them in three aspects: security frameworks, game-based security modeling and adaptive security models.

Security frameworks: some papers proposed a high-level description or a theoretical framework of security modeling without any simulation work or with incomplete analysis.

Radomirovic (2010) proposed a dense IoT model along with a Dolev-Yao adversary model to address security and privacy issues of communication protocols in the IoT. The dense IoT is defined as an asynchronous communication network with high connectivity and ubiquitous functionality. An attacker model is also introduced in which the adversary has corruption and fingerprinting abilities. The paper pointed out future work towards a formal model limiting the adversary's capabilities.

Yang and Fang (2011) presented a high-level security framework for the IoT. The framework is based on a model encompassing three interlinked elements, which are communication, control and computation. They regarded the IoT as the linkage between control and computation. The computation algorithms have a direct influence on the end devices. As the direct control can be intervened by attackers, they put security control between computation and control. They concluded protecting IoT is not only a technical issue but also a social issue.

Stepanova and Zegzhda (2014) proposed a theoretical framework for modeling the IoT security based on graph theory. By defining the IoT as “net of nets of things”, they designed formalized network property indicators to assess the sustainability of nets of things (NoT) and described a method to maintain the sustainability of the NoT entities. Their future work includes the efficiency evaluation of the method with pre-defined indicators.

Atamli and Martin (2014) provided a threat model which consists of three sources of threats and eight types of attack vectors to determine where efforts should be invested to secure systems. Using the threat model, they analyzed the impact of threats and deduced the security and privacy properties for the IoT based on three use cases: power management, smart car and smart healthcare system. Their future work includes the design of a security package that can be used for any use case.

Huang et al. (2015) proposed a security framework named SecIoT under the 5th generation wireless system. SecIoT consists of a secure authentication system, which employs the multi-channel security protocol for device authentication, a role-based access control mechanism with fine-grained roles, and a risk indicator interface based on security risk analysis techniques. A prototype IoT was presented with an authentication protocol analysis and user acceptance studies on access control and risk indicator. The user studies indicated that a fine-