Journal of Network and Computer Applications 49 (2015) 112–127

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

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

Review

Autonomic schemes for threat mitigation in Internet of Things

Qazi Mamoon Ashraf*, Mohamed Hadi Habaebi

Department of Electrical and Computer Engineering, University Islam Antarabangsa, Jalan Gombak, Selangor, Malaysia

ARTICLE INFO

Article history:
Received 26 June 2014
Received in revised form
17 November 2014
Accepted 23 November 2014
Available online 16 December 2014

Keywords:
Internet of Things
Autonomy
Security
Self-management
Wireless sensor networks
Self-security

ABSTRACT

Internet of Things (IoT) refers to the expansion of Internet technologies to include wireless sensor networks (WSNs) and smart objects by extensive interfacing of exclusively identifiable, distributed communication devices. Due to the close connection with the physical world, it is an important requirement for IoT technology to be self-secure in terms of a standard information security model components. Autonomic security should be considered as a critical priority and careful provisions must be taken in the design of dynamic techniques, architectures and self-sufficient frameworks for future IoT. Over the years, many researchers have proposed threat mitigation approaches for IoT and WSNs. This survey considers specific approaches requiring minimal human intervention and discusses them in relation to self-security. This survey addresses and brings together a broad range of ideas linked together by IoT, autonomy and security. More particularly, this paper looks at threat mitigation approaches in IoT using an autonomic taxonomy and finally sets down future directions.

Contents

* Corresponding author. Tel.: +60 182600034.
E-mail addresses: mamoonq@gmail.com (Q.M. Ashraf), habaebi@iium.edu.my (M.H. Habaebi).

http://dx.doi.org/10.1016/j.jnca.2014.11.011
1084-8045/

1. Introduction

During the last three decades, tremendous work on the Internet has led to the growth of Internet of Things (IoT) where intelligent interconnections are being created between diverse objects for a globally integrated communication platform (Iera et al., 2010; Zheng et al., 2011). The main vision behind IoT is that embedded devices, also called smart objects, are becoming Internet Protocol (IP) enabled in an attempt to compute, organize and communicate. IoT is setup and maintained economically and energy-efficiently through sensors attached to these objects. A combination of Internet connected embedded devices, smart objects, sensors and supplementary web-based services makes IoT what it is today (Shelby and Bormann, 2011). Furthermore, it is estimated that IoT market adoption will take around 5–10 more years (Gubbi et al., 2013)

It is the need of the hour to secure the communication channels as well as to introduce the supporting security technologies in the IoT devices (O'Neill, 2014). Security represents a critical component for enabling the worldwide adoption of IoT technologies and applications. Some of the recent security research has focused on network based cryptographic mechanisms (Kothmayr et al., 2013; McCusker and O'Connor, 2011), embedded security (Ukil et al., 2011; Babar et al., 2011), distributed approaches for IoT service provisioning (Roman et al., 2013), security solutions for applications (Chen et al., 2011; Liu et al., 2012) as wellas system security frameworks and strategies (Roman et al., 2011; Pan et al., 2011; Zhou and Chao, 2011). A recent study by Ning et al. (2013) identifies the areas in cyber-entity security, and presents security requirements as well as proposes recommendations to meet those requirements. Some security options are currently provided by the existing Internet protocols; nevertheless the device and network limitations prevent their full use. For example, implementation of full IP security (IPsec) suite to protect mobile devices (Arkko et al., 2004), implementation of transport layer security (TLS), as well as the use of firewalls on each end device is rather restricted (Shelby and Bormann, 2011). Furthermore, innovations such as firewall implementations in the lower layers are inefficient as they can be overridden over the wireless channel directly and remote devices can be stolen and compromised.

IoT can be looked at as a highly dynamic and distributed networked system, composed of a large number of smart objects capable of producing and consuming information. There is a vast set of supporting technologies which are necessary to realize the vision of IoT. These include Radio Frequency Identification Devices (RFIDs), sensors, actuators, and similar machine-to-machine (M2M) communication devices. Historically, IoT referred to RFID based technologies where the security solutions have mostly been devised in a vertically integrated ad hoc manner (Miorandi et al., 2012). Such heterogeneity in technology required specific security mechanisms to meet the requirements. For the wide variety of IoT devices today, there exists a huge tradeoff among performance, cost and security which make security for IoT a big challenge. Consequently, IoT offers a wealth of areas where the security aspect is to be thoroughly researched.

IoT is extremely vulnerable to attacks for several reasons. First, its components are often unattended and remotely located. This gives attackers a chance for physical attacks, and it is even harder to manage security in such a case. Therefore, it is essential for security solutions to become more autonomic and to rely less on human intervention. Furthermore, systems are becoming increasingly