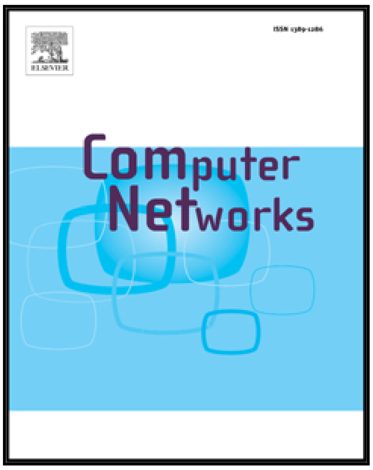

The rise of ransomware and emerging security challenges in the Internet of Things

I. Yaqoob, E. Ahmed, M.H. Rehman, A.I.A. Ahmed, M.A. Al-garadi, M. Imran, Mohsen Guizani

PII: S1389-1286(17)30346-8
DOI: 10.1016/j.comnet.2017.09.003
Reference: COMPNW 6302

To appear in: *Computer Networks*

Received date: 16 December 2016
Revised date: 31 August 2017
Accepted date: 6 September 2017

Please cite this article as: I. Yaqoob, E. Ahmed, M.H. Rehman, A.I.A. Ahmed, M.A. Al-garadi, M. Imran, Mohsen Guizani, The rise of ransomware and emerging security challenges in the Internet of Things, *Computer Networks* (2017), doi: 10.1016/j.comnet.2017.09.003

The rise of ransomware and emerging security challenges in the Internet of Things

Ibrar Yaqoob, Ejaz Ahmed, *Member, IEEE,*
Muhammad Habib-ur Rehman, Abdelmuttlib Ibrahim Abdalla Ahmed, Mohammed Ali Al-Garadi, Muhammad Imran, *Member, IEEE,* and Mohsen Guizani, *Fellow, IEEE*

Abstract—With the increasing miniaturization of smartphones, computers, and sensors in the Internet of Things (IoT) paradigm, strengthening the security and preventing ransomware attacks have become key concerns. Traditional security mechanisms are no longer applicable because of the involvement of resource-constrained devices, which require more computation power and resources. This paper presents the ransomware attacks and security concerns in IoT. We initially discuss the rise of ransomware attacks and outline the associated challenges. Then, we investigate, report, and highlight the state-of-the-art research efforts directed at IoT from a security perspective. A taxonomy is devised by classifying and categorizing the literature based on important parameters (e.g., threats, requirements, IEEE standards, deployment level, and technologies). Furthermore, a few credible case studies are outlined to alert people regarding how seriously IoT devices are vulnerable to threats. We enumerate the requirements that need to be met for securing IoT. Several indispensable open research challenges (e.g., data integrity, lightweight security mechanisms, lack of security software's upgradability and patchability features, physical protection of trillions of devices, privacy, and trust), are identified and discussed. Several prominent future research directions are provided.

Index Terms—Internet of Things, Security, Authentication, Ransomware, Trust.

1 Introduction

Immigrating to a promising era of Internet of Things (IoT), ubiquitously small embedded devices are implanted with various sensors to sense data from their surroundings and provide smart controlling decisions. The proliferation of miniaturized sensors and connected IoT devices is expected to reach 26 billion by 2020, most of which are wearable devices [1]. In this modern era of technology, people have started to deploy real-world IoT applications, from connected smart homes [2], connected cars [3], [4], smart parking [5], and health monitoring [6], [7] to smart utility meters [8], as shown in Figure 1. Although IoT can facilitate different aspects of people's lives, enabling high security, developing ransomware prevention, and establishing solutions are the key remaining concerns, given that IoT devices hold sensitive information [9].

A HP study reveals that 70% of IoT devices are vulnerable to attacks [1]. Hacking of smart cars is also one of the security threats in IoT [10]. According to Markets and Markets, the IoT security market is expected to

- *I. Yaqoob, E. Ahmed, and A.I.A. Ahmed are with the Department of Computer System & Technology, University of Malaya, 50603 Kuala Lumpur, Malaysia. (E-mail: {ibraryaqoob@siswa.um.edu.my, ejazahmed@ieee.org, abdelmuttlib@siswa.um.edu.my)*
- *M.H. Rehman is with COMSATS Institute of Information Technology, Wah Campus, 47040 Pakistan. (Email: habibcomsats@gmail.com)*
- *M.A. Al-garadi is with the Department of Information Systems, University of Malaya, Malaysia. (Email: mohammedali@siswa.um.edu.my)*
- *M. Imran is working with the College of Computer and Information Sciences, King Saud University, Saudi Arabia. (Email: dr.m.imran@ieee.org)*
- *Mohsen Guizani is working with the Department of Electrical and Computer Engineering, University of Idaho, USA. (Email: mguizani@ieee.org)*

[1] http://www.itpro.co.uk/security/22804/hp-70-of-internet-of-things-devices-vulnerable-to-attack