Chapter 26
Internet of Things:
The Argument for Smart Forensics

Edewede Oriwoh
University of Bedfordshire, UK

Geraint Williams
IT Governance Limited, UK

ABSTRACT

The Internet of Things (IoT), a metaphor for smart, functional Cyberphysical Environments (CPE), is finding some usefulness in various sectors including healthcare, security, transportation, and the Smart Home (SH). Within the IoT, objects potentially operate autonomously to provide specified services and complete assigned tasks. However, the introduction of new technologies and/or the novel application of existing ones usually herald the discovery of unfamiliar security vulnerabilities, which lead to exploits and sometimes to security breaches. There is existing research that identifies IoT-related security concerns and breaches. This chapter discusses existing Digital Forensics (DF) models and methodologies for their applicability (or not) within the IoT domain using the SH as a case in point. The chapter also makes the argument for smart forensics, the use of a smart autonomous system (tagged the Forensics Edge Management System [FEMS]) to provide forensic services within the self-managed CPE of the SH.

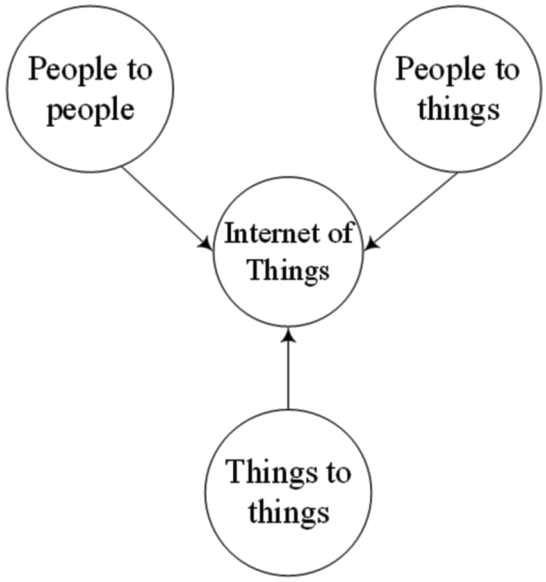
INTRODUCTION: THE INTERNET OF THINGS

The Internet of Things (IoT) (Lu Tan & Neng Wang, 2010; Uckelmann, 2011) is also referred to variously as the Internet of Objects (Xia, Yang, Wang, & Vinel, 2012), Future Internet (FI) (Hernández-Muñoz et al., 2011), Machine to Machine (M2M) communications (Y. Chen, 2012; Igarashi, Ueno, & Fujisaki, 2012), and the Internet of Everything (IoE) (Castro, Jara, & Skarmeta, 2012; Lin, Leu, Li, & Wu, 2012; Ning & Hu, 2011). It is an extension of traditional networks such as the Internet and social networks. It is the true Network of networks because it describes the potential for the interconnection of every (feasible) object to every other (feasible) object and all the underlying processes and protocols that enable and support these interconnections (Figure 1).

Ericsson estimates that more than 50 billion devices will be connected by 2020 (Ericsson White paper, 2011) while Morgan Stanley suggests that by the same date there will be 75 billion devices connected to the IoT (Proffitt, 2013). These connected items will be of a variety of types and shapes and will vary from traditional

DOI: 10.4018/978-1-4666-6324-4.ch026

Figure 1. Key interconnected elements that make up the IoT



computing devices to ordinary everyday objects. For instance within the Smart Home (SH), Things (also known as *Blogjects* (Nova & Bleecker, 2006), *Spimes* (McFedries, 2010) or *IoT-ware* (Oriwoh, Jazani, Epiphaniou, & Sant, 2013)) may include kettles, cars, fridges, Personal Computers, smart phones and washing machines. Various sectors and industries currently benefit from having these interconnections including the transportation, communication, healthcare, smart houses and leisure industries (Fleisch, 2010; Juels, 2006; Kozlov, Veijalainen, & Ali, 2012; Laranjo, Macedo, & Santos, 2012). In the SH, these objects will be interconnected for the purpose of improving people's lives and making things more convenient for them (Alam, Reaz, & Ali, 2012; Hyungkyu Lee, Jooyoung Lee, & Jongwook Han, 2007). The IoT is enabled by technologies including sensors, Machine to Machine communications (M2M), Radio Frequency Identification (RFID) and so on. See Figure 2 for a summary of some cardinal elements of the IoT including the enabling technologies.

However, although the application domains and benefits of the IoT are numerous, a growing number of security concerns have been recognised in relation to the IoT (Juels, 2006). These concerns include *logical* threats (e.g. Denial of Service or DoS) and *physical* threats (e.g. tampering and theft). The discussion in this chapter is particularly focused on one of the many manifestations of the IoT - the SH, which is described by Ding et al. as "a residence equipped with technology that observes the residents and provides proactive services" (Ding, Cooper, Pasquina, & Fici-Pasquina, 2011). Some example SH projects are described in (Chan, Estève, Escriba, & Campo, 2008).

SH environments are susceptible to both traditional attacks such as burglary, theft, DoS as well as tailored attacks e.g. a fridge used as part of a botnet to propagate malware. There is already research that discusses providing security in home-based IoT applications (Chan et al., 2008; D. Chen et al., 2011; Ding et al., 2011; Ning & Liu, 2012; Seigneur, Jensen, Farrell, Gray, & Chen, 2003). However, there is no guarantee that every single logical and physical security measures will be completely attack-proof. Any breaches within SH environments will therefore have to be investigated both from the physical and the digital perspectives. In this light, some DF models and methodologies have been developed that propose to be applicable to CPE (Ademu, Imafidon, & Preston, 2011; Vlachopoulos, Magkos, & Chrissikopoulos, 2013).

This chapter, for its own part, proposes that as part of addressing security issues within SH environments, DF should become *smart* - i.e. through the use of automated smart devices to provide DF services within homes without the requirement for commercial (human) investigators except when absolutely necessary. As part of this contribution, the Forensics Edge Management System (FEMS) is introduced. Prior to this, a methodology for approaching IoT-based crime scenes is proposed. The aim of the methodology