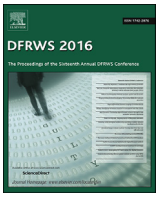
Digital Investigation xxx (2017) 1–11

Contents lists available at ScienceDirect

Digital Investigation

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



Future challenges for smart cities: Cyber-security and digital forensics

Zubair A. Baig*, Patryk Szewczyk, Craig Valli, Priya Rabadia, Peter Hannay, Maxim Chernyshev, Mike Johnstone, Paresh Kerai, Ahmed Ibrahim, Krishnun Sansurooah, Naeem Syed, Matthew Peacock

Security Research Institute & School of Science, Edith Cowan University, Perth 6027, Australia

ARTICLE INFO

Article history:
Received 16 February 2017
Received in revised form
21 June 2017
Accepted 27 June 2017
Available online xxx

ABSTRACT

Smart cities are comprised of diverse and interconnected components constantly exchanging data and facilitating improved living for a nation's population. Our view of a typical smart city consists of four key components, namely, Smart Grids, Building Automation Systems (BAS), Unmanned Aerial Vehicles (UAVs), Smart Vehicles; with enabling Internet of Things (IoT) sensors and the Cloud platform. The adversarial threats and criminal misuses in a smart city are increasingly heterogenous and significant, with provisioning of resilient and end-to-end security being a daunting task. When a cyber incident involving critical components of the smart city infrastructure occurs, appropriate measures can be taken to identify and enumerate concrete evidence to facilitate the forensic investigation process. Forensic preparedness and lessons learned from past forensic analysis can help protect the smart city against future incidents. This paper presents a holistic view of the security landscape of a smart city, identifying security threats and providing deep insight into digital investigation in the context of the smart city.

Introduction

More than 50% of the world's population today reside in urban areas and this percentage is expected to increase because of population migration to these regions in the quest for better jobs and education (Khatoun and Zeadally, 2016). The concept of the *smart city* represents the first major impetus for change in metropolis-sized urban planning since Victor Gruen re-envisioned the urban landscape in America in the 1950s. As a consequence, smart cities have recently gained attention; comprising a collection of entities deployed and maintained in a city to facilitate convenient and improved living for a nation's population. Various initiatives worldwide have facilitated the emergence of smart cities that address the needs of businesses, institutions, and citizens, through targeted and efficient delivery of service. The smart city promise of provisioning a connected environment for all its citizens is realized through intelligent and sustainable enabling technologies and platforms including the Internet of Things (IoT) and the Cloud.

Smart city services can extend into many diverse domains including the environment, transportation, health, tourism, home energy management and safety and security (Byun et al., 2014; Kantarci and Mouftah, 2014; Lopes et al., 2015). The U.S. National Institute of Standards and Technology (NIST) smart city model is one of the most widely adopted reference models (Khatoun and Zeadally, 2016). It comprises six categories, namely, smart environment, smart mobility, smart economy, smart governance, smart people and smart living; with IoT as the enabling technology. We base our study on four components of the above categories:

- Smart Grids (*Smart Environments*)
- Building Automation Systems (*Smart Living*)
- Unmanned Aerial Vehicles (*Smart Mobility*)
- Smart Vehicles (*Smart Mobility*)

The smart city will include several types of IoT sensors including those required for smart parking, structural health awareness, urban noise mapping in real-time, traffic level monitoring and route optimization and smart street lighting. The enabling technology for the above smart city components is the IoT whilst the enabling platform for centralized data storage and rendering is the Cloud.

* Corresponding author.
E-mail addresses: z.baig@ecu.edu.au (Z.A. Baig), p.szewczyk@ecu.edu.au (P. Szewczyk), c.valli@ecu.edu.au (C. Valli), p.rabadia@ecu.edu.au (P. Rabadia), p.hannay@ecu.edu.au (P. Hannay), m.chernyshev@ecu.edu.au (M. Chernyshev), m.johnstone@ecu.edu.au (M. Johnstone), p.kerai@ecu.edu.au (P. Kerai), ahmed.ibrahim@ecu.edu.au (A. Ibrahim), k.sansurooah@ecu.edu.au (K. Sansurooah), n.syed@ecu.edu.au (N. Syed), m.peacock@ecu.edu.au (M. Peacock).

http://dx.doi.org/10.1016/j.diin.2017.06.015
1742-2876/

Smart cities are exposed to a diverse set of cyber security threats and criminal misuses. In this environment, a single smart city vulnerability, when exploited by an individual or organized group, may put the entire city at risk (Khatoun and Zeadally, 2016). This complex environment also presents a significant challenge for digital forensic investigations, which will invariably rely upon the data generated by the smart city components. To envision a secure smart city cyber security platform with access to reliable forensic evidence, due diligence for data transfer and storage in the Cloud is mandatory. Such forensic preparedness can provide help to develop more effective ways to detect and prevent problems before they cause widespread harm (Sachowski, 2016; Casey, 2009).

In addition, if a cyber-attack transpires against critical components of a connected smart city ICT infrastructure, as illustrated in Fig. 1, a standard scientifically proven method must be applied for acquisition and subsequent analysis of the data, as part of the forensic investigation.

In this paper, we present a comprehensive analysis of the vulnerabilities and the associated threat landscape for each of the four identified components of a smart city, namely, Smart grids, Building Automation Systems (BAS), Unmanned Aerial Vehicles (UAVs), Smart Vehicles; with enabling IoT sensor technology and the Cloud. Following this, we present a detailed analysis of challenges associated with forensic investigations of smart city data.

Smart city entities

Smart grids

Smart grid technology is changing the way traditional power grids operate (Fig. 2) by reducing energy demands, global warming and consequently, utility costs. Consumers are required to share information about their energy consumption with their utility providers, over communication channels using smart meters. The interconnection of multiple smart meters and computerized infrastructure of the grid makes them vulnerable to several network based attacks (McDaniel and McLaughlin, 2009).

Data from smart grid devices can be essential for studying energy consumption patterns and supply/demand management. Traditional data management applications are not designed to handle large scale data generated by the grid. Cloud computing is an appropriate choice that can be leveraged to store and process such large volumes of data (Bera et al., 2015). Data can also be used for detecting anomalous behaviour in smart grids and can assist in forensic investigations. Anomaly detection techniques applied to data from different IoT components operating in a smart grid can detect compromised devices and protect smart grid operations.

Smart grid threats can be categorized into those that affect: network availability, data integrity and information privacy. Devices such as smart meters and IoT devices within a consumer's household are located in physically insecure locations and can be exploited by an adversary. Since the grid maintains a two-way communication channel with multiple intelligent smart grid devices and the Cloud, these exposed devices create numerous entry points for an adversary to penetrate the smart grid, and also expose smart grid data stored in the Cloud to various security threats.

Consumption patterns could also be utilized by an adversary to extract household information such as the number of individuals living in a house, and the various types of appliances in use (Jokar et al., 2016). Another challenge to privacy of smart grid data is the ownership and accessibility of consumer data stored in the Cloud. Jokar et al. (2016) suggest using anonymization of the data to haze out attribution of any traits to a particular customer.

Smart grids are also vulnerable to attacks that can affect the timely delivery of messages between interconnected systems, which is critical to the successful operations of the grid. Lu et al. (2010) categorize an attack targeting the time constraints in grid communication as a Denial of Service (DoS) attack, exploiting

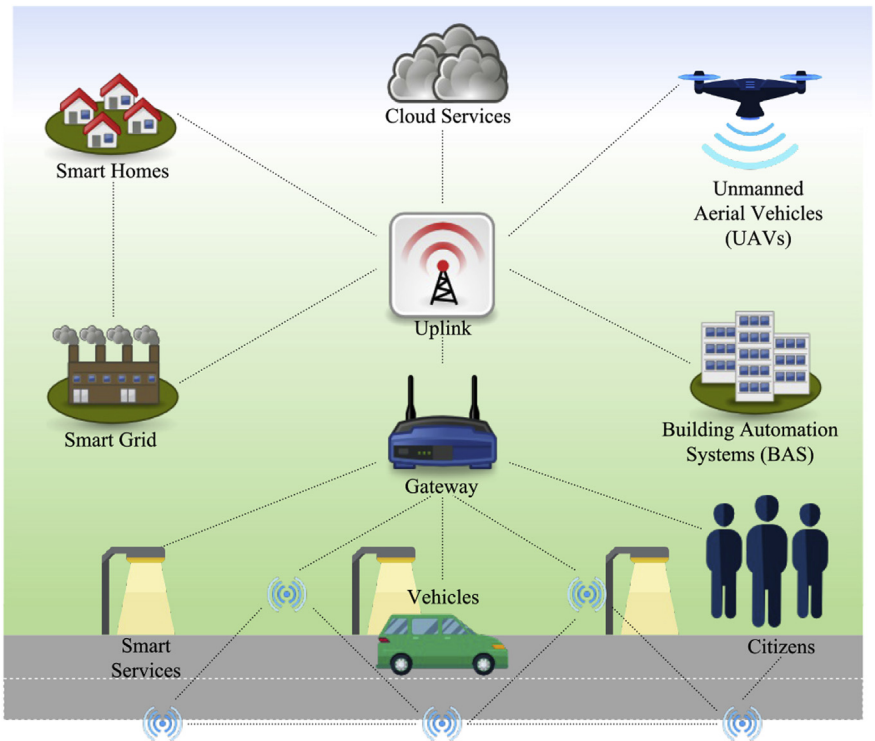


Fig. 1. High level overview of interconnected smart city components.

Please cite this article in press as: Baig, et al., Future challenges for smart cities: Cyber-security and digital forensics, Digital Investigation (2017), http://dx.doi.org/10.1016/j.diin.2017.06.015