Cybersecurity and Privacy Solutions in Smart Cities

Rida Khatoun and Sherali Zeadally

ABSTRACT

The increasing proliferation and deployment of ICT in the infrastructure of cities has increased interest in smart cities. The long-term objective of a smart city is to enhance the quality of services provided to citizens and ultimately improve their quality of life. However, incorporating ICT opens up various security and privacy issues in smart cities, along with the people living in them. We briefly present the fundamental design concepts of a smart city and review recent smart city initiatives and projects. After identifying several security vulnerabilities and privacy issues within the context of smart cities that must be addressed, we then discuss various privacy and security solutions, recommendations, and standards for smart cities and their services.

INTRODUCTION

Many cities around the world risk becoming barely livable within a few years as their infrastructures are stretched to their limits in terms of scalability, environment, and security while they adapt to support population growth (9.7 billion in 2050 according to the UN-Habitat United Nations [UN] program — http://unhabitat.org). Today, urban territories have complex economic and environmental crises. In fact, this urban evolution will convey both benefits and challenges. Economies will be under increased pressure; energy consumption will increase exponentially; the environment will be challenged; healthcare and education systems will demand new approaches; public safety will be further challenged; and the potential for future cyberattacks against cities is high. Without innovative solutions, this situation can lead to further environmental degradation and poverty. We need to rethink the models of access to resources, transport, waste management, and energy management [1]. Hence, smart, cost-effective, scalable, innovative solutions that can address the problems of urbanization are needed. There are six components that underpin most smart city models: government, economy, mobility, environment, living, and people. All these components help a smart city to achieve multiple benefits that include the following.

Efficient Urban Services: These provide improved transport conditions including comfort, shorter waiting times, better access to information, reduced travel time, reduced CO_2 emissions, optimized operations of municipal services (fast and effective response to the demands of citizens [users]), and reduced response times in case of failures of city services/systems or theft.

Smart Buildings Services: These offer reduced costs of electricity and water bills by providing information about an individual's consumption in real time, enabling buildings to make use of renewable energy, managing the energy consumption of buildings through a smart grid (e.g., anticipating consumption), and automating all building functions (heating and cooling, security, and lighting).

Cyberspace Services: These support timely and high-quality information to citizens, providing quick and efficient responses to the requests of citizens (e.g., through electronic operations), providing various types of services to citizens, including cloud computing and remote data storage.

As mentioned earlier, a smart city offers several solutions to the various problems faced by urban development and city management. However, the smart delivery of services depends on information and communication technology (ICT) as a critical component. In fact, there are risks and challenges invoked by introducing ICT into the infrastructure of a city. Citizens increasingly use unsafe WiFi networks to access their emails, e-banking, and so on, thereby exposing themselves to various types of cyberattacks such as man in the middle (MITM), cracking, and denial of service (DoS) attacks. On the other hand, new critical infrastructures of cities are likely to be exposed to attacks that could cause severe denial of service to cities and industrial sites, and impede the delivery of other services. Cybersecurity is one of the major distinguishing characteristics that can be used to classify safe cities around the world. The Safe Cities Index (SCI — http://safecities.cope.economist.com/wp-content/uploads/sites/5/2015/06/Safe_cities_index_2015_EIU_report-1.pdf) is often used, and it relies on an index comprising more than 40 quantitative and qualitative indicators relying on four facets: digital security, health security, infrastructure safety, and personal safety.

The actual supervisory control and data acquisition (SCADA) systems are based on old software platforms that can be susceptible to intrusions and attacks, thereby compromising these systems' security criteria. In 2010, the Stuxnet virus [2] targeted the SCADA systems of one of the Iranian nuclear centrifuges. The goal of Stuxnet was to intercept and modify the data sent from and to

The authors briefly present the fundamental design concepts of a smart city and review recent smart city initiatives and projects. After identifying several security vulnerabilities and privacy issues within the context of smart cities that must be addressed, they then discuss various privacy and security solutions, recommendations, and standards for smart cities and their services.

Rida Khatoun is with Telecom ParisTech; Sherali Zeadally is with the University of Kentucky.

Digital Object Identifier:
10.1109/MCOM.2017.1600297CM

The purpose of healthcare services is to help people live healthy by providing access to a range of facilities. In a smart city, public health professionals often need to access the medical information of patients at any time and from anywhere through connected devices, especially when circumstances do not allow for the physical presence of a specialist or in case of unforeseen disasters.

the programmable logic controllers (PLCs) in the nuclear reactors. Stuxnet was successful in causing real physical damage to the Iranian SCADA systems. By 2010 more than 90,000 Stuxnet infections were reported in 115 countries. According to the 2015 Dell Security Annual Threat Report (https://software.dell.com/docs/2015-dell-security-annual-threat-report-white-paper-15657.pdf), in 2014, the number of attacks on SCADA systems increased from 91,676 in January 2012 to 163,228 in January 2013, and 675,186 in January 2014. Intelligent vehicles are also vulnerable to serious cybersecurity attacks. In 2015, two cybersecurity researchers published a report (http://illmatics.com/Remote_Car_Hacking.pdf) showing how someone can wirelessly control a Jeep Cherokee after shattering the vehicle's Uconnect system. In 2014, Proofpoint Inc. (http://investors.proofpoint.com/releasedetail.cfm?ReleaseID=819799) published a report on Internet of Things (IoT)-based cyberattacks involving household smart devices. The report showed that 750,000 malicious emails (spam) were sent from more than 100,000 devices, including home networking routers, televisions, and refrigerators. In 2016, Dyn (a company that provides DNS services) suffered from a denial of service attack caused by tens of thousands of connected objects to saturate its infrastructure. The attack resulted in Dyn's inability to provide the DNS service (https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todaysmassive-internet-outage/). Hence, IoT networks are increasingly being used as an attack platform by malicious attackers.

These attacks and their impact show how seriously we should take security into consideration in critical infrastructures in order to protect data confidentiality, users' privacy, and the safety of human life. To address these aforementioned challenges, cities need to be "smart." As ICT is vulnerable to threats, the smart city should be immune against such attacks and vulnerabilities. In this work, we explore the security architecture of a smart city, and its requirements and challenges. We also highlight some cybersecurity challenges while exploring research opportunities that need more attention to enable the development and adoption of smart cities in the future.

The remainder of this article is organized as follows. In the next section, we describe the smart city design and its deployment. Following that, we present the cybersecurity solutions needed for different sectors of a smart city. Then we describe research works and challenges for privacy protection in smart cities. Finally, we conclude the article.

Smart City Design and Deployment

For its general foundation, a smart city's architecture must represent and consider the following components.

Government Sector

E-governance is the performance of a government through the electronic medium. E-government allows citizens to fulfill their civic and social responsibilities through a web portal. The main goals of e-government services include: providing access to all information services through official government websites; achieving efficient coordination among all government departments; providing flexible communication methods to citizens using various types of Internet applications such as email, SMS, chat, and social media; providing information on sentiments of citizens and giving early warnings when something is wrong [3]; and eliminating government paperwork. According to a recent report [4] of the UN, in 2014, all 193 UN member states had national websites, but most of them remain below the desired levels of e-government. In France, the digital France 2012–2020 project (France Numrique 2012–2020) [5] is a government initiative that aims to put France among the major digital nations through digital actions. In this context, the open government partnership (OGP — http://www.opengovpartnership.org/), an international organization supported by 69 countries, provides an international platform to encourage governments to be more open and responsive to citizens. Recently, OGP launched the International Open Data Charter that defines the best practices for the release of governmental open data.

Healthcare Sector

Healthcare services in a smart city can also benefit from smart connected devices. The purpose of healthcare services is to help people live healthy by providing access to a range of facilities. In a smart city, public health professionals often need to access the medical information of patients at any time and from anywhere through connected devices, especially when circumstances do not allow for the physical presence of a specialist or in case of unforeseen disasters. Remote healthcare can be realized through the utilization of smart devices wirelessly connected to health centers and a data analytics system. However, there are numerous challenges facing the implementation of healthcare services [6]: coordination among healthcare providers, insurance in case of mistakes or errors, high energy consumption by the new healthcare system, interactions among hospitals requiring common languages or new protocols, high-quality interoperable systems, and process standardization. The Health 2.0 (http://www.health2con.com/) project is a good example of a healthcare initiative that promotes and exchanges experiences of new technologies in healthcare. In this context, several health startups (http://tech.eu/features/1472/health-startup-europe/) are emerging that focus on digital health activity in Europe. To adopt smart healthcare systems, we need more clearly defined methodologies and guidelines to be implemented in hospitals and medical centers.

Critical Infrastructure Sector

A smart grid is a system built on advanced ICT-based infrastructures that manages electricity in a sustainable, reliable, and economic manner. It is an intelligent electricity network using computers and sensors placed in the grid. In the United Kingdom, more than 7 million smart meters will be installed during the next year in households under a new project called Smart Meters — Project Spark funded by the European Investment Bank and six other commercial banks. It is the largest existing smart meters installation project in Europe in this field to date. One of the world's most modern and intelligent electricity grids is

Project/location	Funding	Duration	Goals	Main partners
France Numrique/ France	French government	2012–2020	Facilitate the growth of digital small and medium-sized enterprises (SMEs). Introduce high-speed broadband and improve the quality of mobile access. Diversify uses and digital services. Renovate governance and ecosystem of the digital economy.	French Ministry of the Economy, Finance and Industry
Spark/United Kingdom	European Union via European Investment Bank (EIB)	2016–2020	Reduction of greenhouse gas	Department of Energy and Climate Change (DECC)
CenterPoint Energy Houston Electric (CEHE's) smart grid/ United States	Investment grant program		Reduce the following: greenhouse gas and pollutant emissions, meter-reading costs, maintenance costs, duration of outages, and theft costs	U.S. Department of Energy
Smart Grid Gotland (SGG)/Sweden	Swedish Energy Agency	2012–2015	Increase the hosting capacity for wind power, and participation in the electricity market.	ABB, Ventyx, Schneider Electric, Royal Institute of Technology (KTH), Svenska Kraftnt, GEAB, and Vattenfal
Yokohama Smart City Project (YSCP)/Japan	Ministry of Economy, Trade and Industry (METI)	2010–2015	Low-carbon city, hierarchical energy management systems (EMS), sensitive photovoltaic (PV) generation	Tokyo Institute of Technology, Toshiba, Mitsubishi, and Hitachi
SCOOP@F/France	Ministry of Sustainable Development and European Union	2014–2018 (parts 1 and 2)	Improve the safety of road users and road workers during maintenance projects. Traffic management.	PSA-Peugeot, Renault, Cerema, IFSTTAR, Telecom ParisTech, Orange
UR: BAN/Germany	Federal Ministry of Economics and Energy	2012-2015	Cognitive assistance, connected traffic systems, and human factors in traffic	Adam Opel, Audi, BMW, Volkswagen, and other companies. Fraunhofer Institute, TUM, Kassel University, other universities/ institutes.
AdaptIVe/Germany	European Union	2014–2017	Achieve real advances in safe automated driving. Legal context of automated driving in future cities and the classification of automated systems from a legal perspective.	Volkswagen, BMW, RENAULT, Volvo, Peugeot Citron, Ford R&A, and other companies. University of Trento, University of Leeds, and other universities/ institutes.
Green Vision/United States	State and federal funding	2007–2022	Ten goals have been defined, including reducing energy use by 50 percent, 100 percent energy from renewable sources, reuse of water, zero-emission lighting, and 100 percent public vehicles running on alternative fuels	Universities, private companies, and regional agencies

Table 1. Recent projects and initiatives related to smart cities around the world.

actually in progress on the Swedish island of Gotland. This project (http://www.smartgridgotland.se/), called Smart Grid Gotland (SGG), intends to integrate large amounts of renewable energy sources (RESs) into the network while maintaining reliability. SGG will increase the hosting capacity for wind power and test the sale of energy by households from solar or wind power under market driven conditions. In the United States, the results of CenterPoint Energy Houston Electric's (CEHE's) smart grid project (https://www.smartgrid.gov/project/centerpoint_energy_houston_electric_llc_smart_grid_project.html) show the benefits of the smart grid approach: improved distribution system reliability (avoiding dozens of millions of customer outage minutes), reduced meter reading costs, reduced operating and maintenance costs (decreased by approximately $55 million in 2013), reduced truck fleet fuel usage, and reduced costs from theft detection such as unusual consumption (a cost reduction of $2 million in 2013). To monitor and control distributed components in a power system, the latter needs a SCADA system.

In a smart city, an IT infrastructure underpins the design of buildings' control systems, including light and motion sensors, water heaters and coolers, escalators, gas and smoke detectors, water leak detectors, security and access systems. The integration and interconnection of these control systems with other systems will increase the security concerns for building operations, occupants and owners.

Smart Buildings Sector

In a smart city, innovative and smart buildings are required for various reasons: improving residents' comfort, efficient operation of the building's systems (i.e., elevators, water pipes, gas pipes), and reduction in energy consumption. In a smart building, a building automation system (BAS) automatically controls the heating, air conditioning, lighting, and other systems. In its report titled Global Smart Buildings Forecast 2013–2018, IDC Energy Insights expects that the smart building technology market will grow from $7.3 billion in 2014 to $21.9 billion in 2018. As for the promotion of technologies for smart buildings, it has been demonstrated that fuel cell technology [7] will enable smart buildings to provide their own electricity with 50 percent less CO_2 emissions. Fuel cell technology is currently being tested at various locations around the world such as Amsterdam's smart city projects and on environmentally friendly vehicles. Solar technology has also made significant strides (e.g., PV cells that convert light energy into electricity) in the past decade. Recently, new design approaches have emerged based on nanophotonics where nano-antennas are exploited for guiding and localizing light at the nanoscale [8, 9].

Transportation Sector

Half of humanity today lives in cities. Mobility in big cities leads to several problems, such as traffic congestion, and increased pollution and energy consumption. To alleviate these problems, one solution is intelligent transportation systems (ITSs). In a smart city, ITSs offer multiple services, such as reducing mobility by facilitating transport mode selection, optimizing trip planning and management, detecting drivers exhibiting malicious behaviors, improving driver and passenger safety, reducing CO_2, making available parking places information known on smartphones, and tracking cars. Hence, vehicular communication is a key technology in smart cities. ITS technologies and services have been developed over a number of years in research projects by different research communities and standardization organizations such as IEEE and the European Telecommunications Standards Institute (ETSI), the Car2Car Communication Consortium, or the U.S. National Highway Traffic Safety Administration (NHTSA). In Germany, 31 partners from industry and academia are working on the user-centric assistance systems and network management (UR: BAN) project (http://urban-online.org/en/urban.html — 2012–2015). This project's goal is to introduce human factors into the traffic system to receive information much earlier, which will help anticipate traffic situations, predict behavior, and detect hazardous traffic situations. Further, the European research project (https://www.adaptive-ip.eu/) Automated Driving Applications & Technologies for Intelligent Vehicles (AdaptIVe) in Wolfsburg, Germany, aims to improve safety for automated driving. In this project special attention is given to the legal aspects of automated driving in future cities and the classification of automated systems from a legal perspective.

In Table 1 we highlight specific developments related to smart cities in Asia, Europe, and North America.

Cybersecurity Solutions

For the many components of a smart city's design, we must also consider the cybersecurity solutions needed.

Critical Infrastructures

During the last few years, industrial control systems (ICSs) are increasingly connected to the Internet. ICSs can be found in various infrastructures, including nuclear power plants, chemical plants, oil refineries, railway signaling systems, wind turbines, and so on. Many supervising systems such as SCADA and communication protocols have been designed for ICSs. The SCADA system consists of multiple hardware modules and devices such as the front-end processors (FEPs), engineering workstations, servers, telephone lines, remote terminal units (RTUs), and programmable logic controller (PLC). These devices are controlled through specific SCADA system protocols such as Modbus/TCP, EtherNet/IP, and the Distributed Network Protocol (DNP). However, these protocols were originally designed without any security measures. Exploiting vulnerabilities in a SCADA system can cause significant disruption in the delivery of its services. In SCADA systems, the DNP3 and Modbus protocols allow the supervisory system to have remote devices (e.g., PLCs) that are used to control machines and processes, such as the flow of cooling water in a nuclear reactor, motors, and sensors. Actually, engineers need access to these PLC devices from diverse locations. DNP3 is a communication protocol standardized by IEEE for electric power systems. Modbus is the most widely rolled out industrial control communications protocol (designed in 1979 by Modicon). Unfortunately, security measures were not taken into consideration in the initial design of DNP3 and Modbus. Consequently, these protocols are often vulnerable to cyberattacks such as unauthorized command execution, MITM attacks, DoS, and replay attacks. For example, by default, DNP3 does not provide any authentication mechanisms between the master and the remote devices, which can lead to dangerous consequences in a critical infrastructure such as a water distribution system, a gas distribution system, or a nuclear reactor.

Recently, the open intrusion detection system (IDS) Snort, version 2.9.2, has added preprocessors to support the DNP3 and Modbus protocols in detecting intrusions and attacks against DNP3 and Modbus. A new design architecture of a firewall for systems that use the ModBus and DNP3 protocols using critical state distance (a metric to compute the distance between the current profile and a critical one) was proposed in [10]. However, critical states need to be described in advance, and the firewall does not automatically learn the configuration of the SCADA system. A lot of attention has been given to the data integrity, and some to authentication and confidentiality.

Smart Buildings

Cyber-attacks are threatening banks, companies, and government networks. In a smart city, an IT infrastructure underpins the design of buildings' control systems, including light and motion sensors, water heaters and coolers, escalators, gas

Characteristics	Description	Standards and recommendations
Organizational	• Develop a backup and recovery plan • Manage passwords • Open feedback sessions • Define the standards, tools, safety procedures and rules for the community • Develop policies regarding passwords and configurations	• Five Best Practices to Improve Building Management Systems (BMS), Schneider Electric • IET standards: Resilience and Cyber Security of Technology in the Built Environment • Frost & Sullivan's Cybersecurity in Smart Buildings, 2015 • Measurement Science Roadmap for Net-Zero Energy Buildings
Technical	• Provide physical security for equipment, network cable, and servers • Encrypt network traffic with robust symmetric algorithms such as AES and Blowfish • Use a secure connection such as a VPN for remote accesses • Secure any wireless network with WPA2 protocol • Deploy IDS in building • Use a centralized authentication, authorization, and accounting (AAA) server such as a RADIUS server • Deploy a firewall at every transition point • Use strong authentication methods such as biometric or smart cards	• ANSI/TIA-862, Building Automation Systems Cabling Standard • GSA Guide to Specifying Interoperable Building Automation and Control Systems Using ANSI/ASHRAE Standard 135-1995, BACnet • Security requirements of IoT-based smart buildings using RESTful web services • BSI Federal Office for Information Security • Schneider Electric
Human	• Comprehensive training program for developers and administrators. • Inform and raise awareness of safety issues • Alert and advise users where there are threats • Embed continuity plans and disaster recovery	–
Legal	• Respect legal aspects of security • Use safety standards and follow-up recommendations of the national cybersecurity agencies and actors of IT security • Good practices of ICT use • Performance standards	–

Table 2. Security standards and recommendations for cybersecurity of smart buildings.

and smoke detectors, water leak detectors, security, and access systems. The integration and interconnection of these control systems with other systems will increase the security concerns for building operations, occupants, and owners. In a smart building the threat could be the disruption of video surveillance, electrical distribution, lighting, emergency power, access control, elevators, fire systems, HVAC, climate control, monitoring, and so on. Any connected device using some software is vulnerable, and the hack can be performed remotely through the Internet. An attacker can easily hack a smart TV by using an MITM attack (https://iicybersecurity.wordpress.com/2015/07/07/how-to-easily-hack-your-smart-tv-samsung-and-lg/) because there are actually no anti-viruses or anti-malware solutions available for smart TVs, and for some TV brands the authentication procedure only needs an IP address, a media access control (MAC) address, and a hostname for authentication, which is easy to spoof. Cyberattacks can come from many sources: originating inside or outside a company, executed by terrorists, and so forth. Various communication protocols are actually used in smart buildings:

- BACnet is a communication protocol standardized by the American National Standards Institute (ANSI) and the International Standards Organization (ISO) (ISO 16484-5) since 2003 for building automation and control networks. It defines a number of data link/physical layers.
- KNX is standardized under EN 50090 and ISO/IEC 14543; it is an Open System Interconnection (OSI)-based network communications protocol for intelligent buildings.
- Factory Instrumentation Protocol (FIP) is a European standard (EN 50170-3) used for the interconnection of devices in automated systems. It defines several application/data link/physical layers.

However, all these protocols have no cybersecurity measures to protect buildings against cyberattacks or intrusions. Hence, strong security measures must be applied in smart buildings. These measures must be applied as part of a complete security architecture. Table 2 summarizes the security characteristics that must be applied in an intelligent building management system (BMS).

ITS

The IEEE 1609.2 standard proposed various methods of securing WAVE messages against eavesdropping and spoofing. These methods include public key cryptography, elliptic curve cryptography (ECC), specific WAVE certificates, and hybrid encryption. However, IEEE 1609.2 does not address the issue of user authentication and privacy. In [11] the authors showed a close correlation between the start and end points of a vehicle's trips and the vehicle owner's home address, which can lead to vehicle tracking. Current standardization efforts (http://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp1_security.pdf) focus on approaches based on asymmetric cryptography. Messages are authenticated with the Elliptic Curve Digital Signature Algorithm (ECDSA) and the public key certificate issued by a long-term certificate authority (LTCA). Each vehicle also has a pseudorandom certificate issued temporarily by a pseudorandom certificate authority (PCA). Changing pseudonyms frequently offers a good solution for location privacy [12]. However, if the pseudonyms are changed at an inappropriate time or position, such a solution might become inefficient.

E-health devices supporting healthcare applications face several constraints such as the computational limitations because of low-speed processors in sensors and smartphones, memory limitations, energy limitations, and concerns about mobility. Therefore, further research into novel, robust security algorithms is needed.

E-Government

As mentioned previously, e-governance is a modern system adopted by governments using ICT to link government institutions to each other and to private institutions. Several countries have tried e-government to offer high-quality e-government services to their citizens. However, according to the United Nations e-government survey (http://www.unpan.org/e-governme) in 2014, the majority of citizens are concerned about privacy and security when using e-government services. The main challenges e-government must overcome are privacy, trust, and availability in terms of security. In fact, the security of e-governance includes traditional security services (authentication, confidentiality, integrity, and availability), with more emphasis on data privacy and business continuity management. In the final report of the European project STOA, "Security of eGovernment Systems," 11 security policies were defined. More attention was given in this project to the privacy in e-governance such as building a "Privacy by Design" knowledge base, stimulating technical and legal solutions to enhance privacy, and making privacy impact assessments of e-government systems mandatory and public.

E-Health

E-health medical services are supported by electronic processes and communication. Also, healthcare professionals share patients' data among them and tele-monitor patients' health through smartphones, and patients can have e-prescriptions. E-health allows the public dissemination of medical information about a country's health situation and manages health crises through the use of information systems to measure, monitor, and make decisions. Actually, many research efforts have focused on the use of wireless medical networks to enable and improve the quality of care and remote medical monitoring. These networks, also called wireless body area networks (WBANs), are characterized by the mobility of their nodes, a network's easy deployment, and its self-organization, which allows elderly people, people at risk, and patients with chronic disease to be monitored. However, these networks open up new technological challenges in terms of security and privacy. For example, transmitting an electrocardiogram (ECG) signal without encryption will have a big impact on privacy. Commonly used methods include discrete cosine transform (DCT), wavelet transform, and adaptive Fourier decomposition (AFD) algorithms [13]. However, for e-health applications, the performance of these methods depends on the compression efficiency (i.e, the ratio between the original signal and the recovered one), reconstruction quality (the difference between the original signal and the recovered one), and computation complexity. Finding an efficient solution remains a serious challenge. On the other hand, shifting to the cloud environment and storing patient health data in third-party servers remains a serious threat to data privacy. Homomorphic encryption enables modification of the encrypted data without decrypting it. Homomorphic encryption is a very good candidate for e-health in the cloud as it makes the data hosted in the cloud incomprehensible to the provider and others during transmission or processing. The efficiency of Somewhat Homomorphic Encryption (SwHE) has been proven in medical and financial applications [14]. The ISO/TS 18308 standard defines security and privacy for medical records. E-health devices supporting healthcare applications face several constraints such as the computational limitations because of low-speed processors in sensors and smartphones, memory limitations, energy limitations, and concerns about mobility. Therefore, further research into novel, robust security algorithms that minimize resource consumption and maximize security performance (along with efficient energy use) is needed.

Internet of Things

According to [15], there are various key IoT challenges such as heterogeneity, interoperability, scalability, security and privacy, reliability, lack of understanding of new business models, and numerous competing technology standards — International Telecommunication Union Telecommunication Standardization Sector (ITU-T) Study Groups, Internet Engineering Task Force (IETF) Working Groups, ISO, International Electrotechnical Commission (IEC), ISO/IEC Joint Technical Committee 1 (JTC1), IEEE Working Groups, World Wide Web Consortium (W3C), Third Generation Partnership Project (3GPP), Object Management Group (OMG), Open Mobile Alliance (OMA), and others — that must be addressed in the future. In an IETF draft (https://tools.ietf.org/html/draft-ietf-dice-profile-17), the authors define the security architecture and security services (authentication, key exchange, and data integrity) of IoT, and its deployment model. They propose what is actually considered be the most suitable protocol for IoT, which is Constrained Application Protocol (CoAP) over Datagram Transport Layer Security (DTLS). CoAP is a lightweight application layer protocol particularly suited for constrained IP networks because of its low bandwidth requirements; it helps to increase reliability (by reducing fragmentation at layer 2) and reduce latency in low-power wireless networks such as IEEE 802.15.4. Along with IoT standardization perspectives, there is a need to integrate emerging technologies such as cloud computing, big data, software defined networking (SDN), and network functions virtualization (NFV) with IoT. However, this integration brings risks and vulnerabilities from a security perspective.

Generally, the introduction of ICT in smart cities leads to various security and privacy concerns, summarized in Table 3 along with possible countermeasures.

As shown in Fig. 1, we identified four main challenges for a cybersecurity architecture for smart cities: sophisticated attacks, software product bugs and vulnerabilities, legislation issues, and complexity. Sophisticated attacks are due to hardware capabilities, virtualization, and advanced cryptography techniques that are increasingly being used in network attacks. Software products with security vulnerabilities exist because of poor/defective software design, configuration errors, and/or unsecure isolation techniques. As for legislation issues, laws for smart cities cannot be developed and applied properly if existing laws are not reviewed in light of new demands (e.g., user privacy, smart cities leadership, and law

interoperability) in smart cities. Finally, security requirements, new attacks, and legislation issues together further increase the complexity of managing a smart city.

Privacy Protection in Smart Cities

For any technology, the rights of citizens should be guaranteed anywhere and anytime. Despite the benefits of smart cities services, privacy breaches are becoming worrisome within the context of smart cities. In fact, most services of a smart city are based on ICT. Sometimes users (especially adolescents and the elderly) are not familiar with security issues, and they become perfect targets for attackers when they interact with many smart cities services through their smartphones, tablets, and computers, revealing personal data such as gender, age, and location. Thus, this section focuses on privacy issues within smart cities. We first define privacy issues; then we present and compare different privacy models. Finally, we briefly discuss current privacy regulations in different countries.

Privacy Issues

To understand the significance of privacy challenges in smart cities, we use the following example. A vehicle's license plate can be connected to the vehicle owner's identity. Hence, the trajectory of a vehicle can easily be traced even if all communications between the vehicle and infrastructure are encrypted and each device is authenticated by others. This is against the common notion of privacy, which includes the right of people to lead their lives in a manner that is reasonably secluded from public scrutiny, whether such scrutiny comes from a neighbor's prying eyes, an investigator's eavesdropping ears, or a news photographer's intrusive camera. In a smart city, future vehicles will have various communication capabilities that include Internet access, GPS, an electronic tolling system, and RFID. Connected devices in a vehicle will store lots of personal information and have various communication capabilities. In a smart city, the number of connected devices will be very high. The data collected by IoT will allow data consumers to understand the behaviors of data owners or use the data to derive highly personal information, including daily habits.

Privacy Models

In an information system there are three main operations: data transfer, storage, and processing. Privacy concerns can occur during any of these operations, which can affect the user's behavior. Services may be associated with the user's location, which can raise privacy concerns. The authors in [16] proposed the Where, Who, What (W3) privacy model for location-based services (LBS). In [17], a three-layer model of user privacy was proposed to build privacy-friendly systems. For example, in a smart city, privacy-preserving techniques allow two companies to compare their activities without disclosing to each other their strategic or critical data. The authors in [18] proposed an approach based on linear algebra operations such as matrix multiplications to solve linear systems and compute the correlation between distributed datasets. The proposed solution is efficient and theoretically secure. However, on a large scale the performance of this solution is not reliable because it depends on a trusted initializer that must send data to the parties involved before protocol execution. Unfortunately, privacy-preserving techniques do not address constraints such as the frequent change of members and untrusted third parties (cloud providers). Hence, privacy preservation remains a significant challenge that requires further investigation.

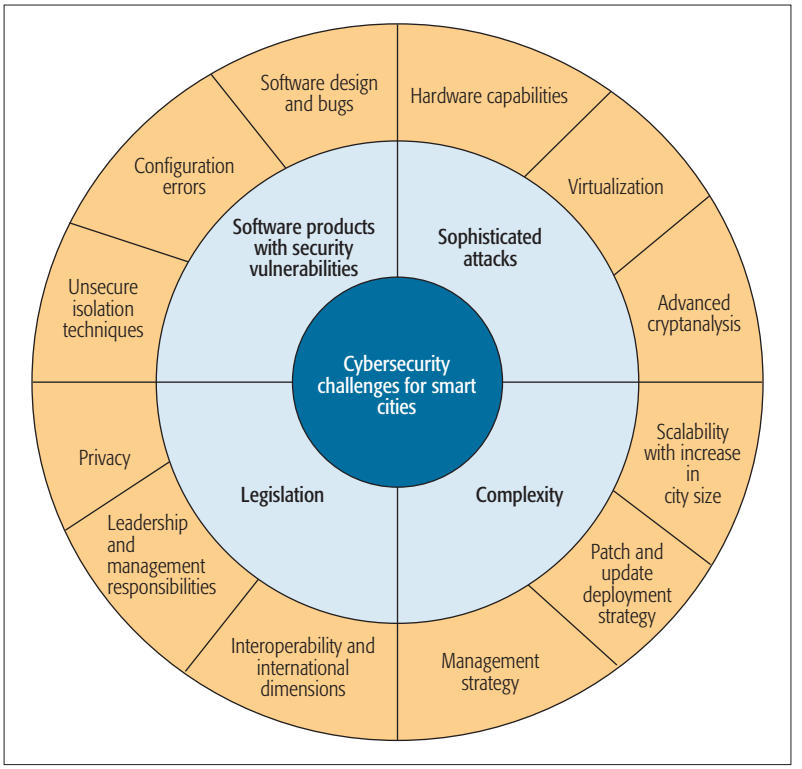

Figure 1. Cybersecurity challenges for smart cities.

Legislation is important to guarantee privacy within smart cities. Recently, the British Parliament initiated a bill [19] that would allow intelligence services to get unlimited access to users' Internet navigation data. Under this law, intelligence agencies can legally intercept and decrypt people's communications; service providers can store users' navigation data for 12 months; and police can also legally hack computers, networks, and mobile phones. However, Microsoft, Facebook, Google, Yahoo, and Twitter indicated their disapproval of this project. Human Rights Watch (https://www.hrw.org/news/2015/11/09/uk-surveillance-bill-threat-privacy) argued that this kind of project is dangerous and too intrusive because it threatens citizens' privacy in the United Kingdom. In France, a new surveillance law (Loi n° 2015-912 du 24 juillet 2015) was approved in July 2015. The new law allows intelligence agencies to monitor communications (emails and phone calls) of suspected persons.

Conclusion

The main objective of a smart city is to enhance the quality of services provided to citizens to improve their quality of life. However, ensuring security and privacy are significant challenges for our future cities. Here, we have described some of the basic concepts of smart cities, and highlighted recent major initiatives, developments, research, and industrial projects related to smart

cities in different countries. We then identify risks and challenges for smart cities in different sectors such as industrial control systems, intelligent transport systems, the Internet of Things, and e-health. In looking toward the future, we underscore that in smart cities, privacy and public safety remain a central concern that need more legal, scientific, and political consideration. To make this technology as beneficial and trustworthy as possible for public adoption, it is imperative to fight against cybercrime in smart cities. This will require ongoing efforts and support from all stakeholders including politicians, governments, legal institutions, energy providers, network operators, vehicle manufacturers, cloud providers, research laboratories, and industry.

Acknowledgments

We thank the anonymous reviewers for their valuable comments and suggestions, which helped us to improve the quality and presentation of this work.

Sector	Threats	Countermeasures
Smart buildings sector	• Infection by malware • Systems failure • Fraud by staff and unauthorized users • Controlling the fire system • Causing physical damage such as flooding • Disrupting building temperature (overheating or overcooling) • Damaging or controlling the lifts • Open windows and doors • Modifying smart meters • Opening parking gates • Disabling water and electricity supplies • Starting/stopping the irrigation water system • Stopping the renewable energy systems (RES)	• Two-factor authentication and one-time passwords for stronger authentication (Imprivata OneSign, Comodo Security Solutions, and STMicroelectronics Secure MCU) • IoT forensics (DigiCert IoT PKI Solutions, and Symantec solutions) • Threat and risk modeling • Data backup and recovery solutions to ensure reliability and continuity of services (CommScope solutions, Socomec solutions, Johnson Controls, and Newron System)
Transport sector	• Sending false emergency messages • Disrupting a vehicle's braking system • Stopping the vehicle's engine • Triggering false displays in the vehicle's dashboard • Disrupting the vehicle's emergency response system • Changing GPS signals	• Public key infrastructure (PKI), digital certificates (ECDSA) and data encryption solutions (ECIES and AES) • Misbehavior detection solutions • Pseudorandom identities
Government sector	• Preventing of cybercrime • Identity theft • Disrupting critical infrastructures • Fiscal fraud • Altered files	• Data leakage prevention (Symantec, Fortinet) • Risk assessment (MEHARI, EBIOS) • Insider threat analysis • Awareness training
Healthcare sector	• Modifying patients record or information • Exposing sensitive data unintentionally • Disrupting the monitoring system • Disrupting the emergency services • Sending false information • Jamming attacks • Sending an emergency alert • Eavesdropping sensitive information	• Secured WiFi networks to guarantee safe handling of confidential information and personal data (AirTight Networks solutions, Aerohive security solutions) • Risk assessment (Rapid7 solutions, Health Security Solutions, SafeNet's data security solutions, Stanley security solutions, Intel healthcare security solutions)
Energy sector	• Spoofing addresses and user names • Unauthorized access and controls • Zero day attacks • Botnets (Zeus, ZeroAccess, Conficker, etc.) • Denial of service and distributed denial of service (DDoS)	• Intrusion detection and prevention techniques (Radiflow, Snort) • Risk assessment (MEHARI, EBIOS) • Insider threat analysis • Cybercrime intelligence
Financial sector	• Loss of privacy • Accounting fraud • Disrupting business processes • Accessing confidential company information • Accessing confidential customer information • Damaging reputation(s) • Defacing websites • Financial and reputation concerns due to fraud and data leakage • Denial of service and DDoS • Phishing • Mobile banking exploitation • SQL injection • Trojan	• Anti-malware solutions (McAfee, Symantec) • Encrypted files and firewalling • Fraud detection and prevention techniques (NICE Actimize, Lexisnexis, Kount Complete, Signifyd, Fraud Guardian) • Risk assessment (MEHARI, EBIOS) • Insurance to mitigate cybercrime Risk • Cybercrime intelligence (RSA CyberCrime Intelligence Service, ThreatMetrix Advances Cybercrime Prevention, SurfWatch vC-Suite, IBM Enterprise Insight Analysis)

Table 3. Security and privacy concerns and countermeasures in smart cities.

References

[1] R. Khatoun and S. Zeadally, "Smart Cities: Basic Concepts, Architectural Issues, and Research Opportunities," *Commun. ACM*, vol. 59, no. 8, Aug. 2016, pp. 46–57.
[2] Symantec Security Response Report: W32.Stuxnet Dossier, v. 1.4, Feb. 2011.
[3] L. Berntzen, "Smart Cities, Smart Buildings, Smart Users," Keynote, DigitalWorld 2015, Lisbon, Portugal, Feb. 24th, 2015.
[4] UN E-Government Survey 2014, "E-Government for the Future We Want," http://www.un.org/desa
[5] France numérique 2012: bilan et perspectives, http://www.entreprises.gouv.fr
[6] H. Demirkan, "A Smart Healthcare Systems Framework," *IT Professional*, vol. 15, no. 5, Sept.–Oct. 2013, pp. 38–45.
[7] L. Valverde, C. Bordons, and F. Rosa, "Integration of Fuel Cell Technologies in Renewable-Energy-Based Microgrids Optimizing Operational Costs and Durability," *IEEE Trans. Industrial Electronics*, vol. 63, no. 1, Jan. 2016, pp. 167–77.
[8] G. Akselrod *et al.*, "Probing the Mechanisms of Large Purcell Enhancement in Plasmonic Nanoantennas," *Nature Photonics*, 2014.
[9] X. Zhou *et al.*, "Selective Functionalization of the Nanogap of a Plasmonic Dimer," *ACS Photonics*, vol. 2, no. 1, 2015, pp. 121–29.
[10] I. N Fovino *et al.*, "Critical State-Based Filtering System for Securing SCADA Network Protocols," *IEEE Trans. Industrial Electronics*, vol. 59, no. 10, Oct. 2012, pp. 3943–50.
[11] B. Hoh *et al.*, "Achieving Guaranteed Anonymity in GPS Traces via Uncertainty-Aware Path Cloaking," *IEEE Trans. Mobile Computing*, vol. 9, no. 8, Aug. 2010, pp. 1089–1107.
[12] R. Lu *et al.*, "Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in VANETs," *IEEE Trans. Vehic. Tech.*, vol. 61, no. 1, Jan. 2012, pp. 86–96.
[13] J. Ma, T. Zhang, and M. Dong, "A Novel ECG Data Compression Method Using Adaptive Fourier Decomposition with Security Guarantee in e-Health Applications," *IEEE J. Biomedical Health Informatics*, vol. 19, no. 3, May 2015, pp. 986–94.
[14] J. H. Cheon and J. Kim, "A Hybrid Scheme of Public-Key Encryption and Somewhat Homomorphic Encryption," *IEEE Trans. Info. Forensics Security*, vol. 10, no. 5, May 2015, pp. 1052–63.
[15] M. Carugi, "Considerations on the IoT Standardization Landscape and ITU-T Perspectives," Proc. IoT 360 Summit 2015, Technology Track, Session on "Standardization in IoT," 27 Oct. 2015, Roma, Italy.
[16] P. A. Prez-Martnez, and A. Solanas, "W3-Privacy: The Three Dimensions of User Privacy in LBS," *Proc. 12th ACM Int'l. Symp. Mobile Ad Hoc Networking and Computing*, May 2011.
[17] S. Spiekermann and L. F. Cranor, "Engineering Privacy," *IEEE Trans. Software Engineering*, vol. 35, no.1, Jan.–Feb. 2009, pp. 67–82.
[18] B. David *et al.*, "Unconditionally Secure, Universally Composable Privacy Preserving Linear Algebra," *IEEE Trans. Info. Forensics Security*, vol. 11, no. 1, Jan. 2016, pp. 59–73.
[19] Draft Investigatory Powers Bill, Nov. 2015.

Biographies

RIDA KHATOUN received his M. Sc in computer engineering and his Ph.D. from the University of Technology of Troyes (UTT), France, in 2004 and 2008. He is currently an associate professor at Telecom ParisTech. His research interests include DDoS attack detection and defense, intrusion detection systems, and mobile ad hoc network security.

SHERALI ZEADALLY received his Bachelor's degree in computer science from the University of Cambridge, United Kingdom, and his doctoral degree in computer science from the University of Buckingham, United Kingdom. He is an associate professor in the College of Communication and Information at the University of Kentucky. He is a Fellow of the British Computer Society and a Fellow of the Institution of Engineering Technology, United Kingdom.