Chronicle Journal of Engineering Science

Review Article

The role of IoT in Smart Cities: Security and Privacy in Smart World

Christos Beretas[1*]

[1]PhD Candidate (full scholarship) in Cyber Security at Innovative Knowledge Institute, Paris, France.

[*]Corresponding author: Christos Beretas. PhD Candidate (full scholarship) in Cyber Security at Innovative Knowledge Institute, Paris, France. (+30) 693-890-9477 | e-mail: cberetas@ikinstitute.org

Received: 1st August 2020
Accepted: 17th August 2020
Published: 24th August 2020

Abstract

Smart devices, or Internet of Things in other world, are a concept that applies to the electronic objects around us, that is, devices that use built-in sensors to collect data and take action on it within a network. As smart devices collect data about its users, smart cities, they are primary targets for hackers. There are several reports on the web about how vulnerable smart devices are to intrusion and loss of privacy, those online reports also provides details on how routers can be hacked. If the router that connects a smart device is hacked, all smart systems and devices connected to it can be controlled remotely. Hackers will attack anything, from routers, webcams, security systems, sensors, actuators, data storage places and databases, to try to do things like locate their users, and monitor their conversations as much as possible. It is clear that today we know better. But, how long will it be before we see a smart city locked by hackers in demand for ransom? It is not far from happening, it is a matter of time before it happens. Most of smart devices are heavily dependent on Wi-Fi, which remains directly compromised by a person with average hacker skills. This means, that a smart device could easily be compromised through this point, so that someone could enter the internal computer system, could enter at smart device management console, have access to personal data, and application management system. Smart users should ask if smart devices provide authentication ad what kind of authentication, if the username and password can be changed, if customer support is provided, if the device collects their personal data and if yes in what level, if the manufacturer has compromised data and if encrypts stored data and automatically updates software. In the U.S, some smart devices sold with the promise of a subscription became useless after the company's decision to shut down the central servers used by the devices to operate, therefore, Before a city can be transformed from a classic to a smart one, all the parameters must be taken into account

Keywords: smart cities; IoT; smart devices; networks; security; privacy

Introduction

In last years, smart devices have been widely used, from smart parking devices, smart lighting and watering trees, to intelligent ways of informing and involving citizens in various activities. The installation and use of such smart devices by both organizations and citizens does not necessarily mean that they have the knowledge is need about the safe installation and use of such devices. Smart devices have antennas and emit wireless radiation to communicate with the central device. Examples of smart devices are: smart lamps, smart car parking, smart relays, door-window sensors, movement sensors, and so on. Most smart devices emit high-frequency electromagnetic fields at 2.4GHz such as Wi-Fi and Bluetooth. The central unit of the systems constantly emits, respectively with a Wi-Fi modem / router. Connected devices emit radiation even in standby mode, so they maintain communication with the central unit. Smart cities have significantly higher wireless radiation rates, as smart devices use antennas that emit 24 hours a day.

On the opposite side, biological effects may be present in a few minutes, at levels related to exposure to smart cities

antennas, wireless modems cause full body exposure. Many of these biological effects can reasonably be considered to have adverse health effects when the exposure is prolonged or chronic. This is because they interfere with the body's normal processes, prevent the repair of damaged **DNA**, cause imbalances in the immune system, metabolic disorders and reduced resistance to multiple diseases. Necessary body functions can eventually be disabled due to incessant external pressures and lead to diffuse dysfunction of metabolism and reproductive functions. Several thousand scientific studies over the past decades have shown serious biological effects and damage to health from low- and high-frequency electromagnetic fields. Financial interests allow for easy licensing of creating new smart cities without prior research about data security, privacy, encryption, communication security and the effects on human health.

Analysis

The installation of a smart device does not imply knowledge of the security of communications and data, from this point the problems begin. A faulty installation of a smart device or with incomplete configuration is capable of affecting not only the internal network to which it is connected, but also directly endangering the personal data of citizens who have an interface with this device. A recent study on smart device threats states that most of the attacks targeted digital video recorders, IP cameras at **63%** while, **20%** of the attacks targeted network devices, including routers and DSL modems. **China, Vietnam, and Russia**, were the top three countries in attack on smart devices, each with a large number of "infected" smart devices. Over time, the attacks will rise dramatically, the reason behind the rise is simple: Smart Devices are fragile and exposed to digital criminals. The vast majority of "smart" devices run Linux-based operating systems, that means with few words **Linux Kernel**, making it easier to attack them because criminals can write a general malicious code that simultaneously targets a huge number of smart devices from different manufacturers. There are already more than **5** billion "smart" devices in the world which most of them do not have a security method installed, and their manufacturers usually do not release security updates, new firmware, or patches. This means that there are millions of vulnerable smart devices in operation, some of which may have already been compromised.

There are no smart cities, but there are smart cities in the eyes of the public and only as it is impossible for the average user to know the level of security of a smart device nor is it able to know the level of protection of their personal data. Recent analysis have shown that developed countries have developed statistics on the level of security of smart devices and security vulnerabilities after a virtual attack by scanning IP address zones performed by external factors and in several cases showed vulnerabilities and access in the internal network. Smart devices use and transmit a significant amount of personal data related to their narrow private functionality, on the one hand, they come from their users, on the other hand, they concern the same users, such as contact information, geolocation data, financial transactions, searches and various user features. In addition, smart devices can store or log real-time data from many sensors, such as microphones, parking sensors, license plates, and other devices used to operate for the purpose for which they were installed. Although service designers want to provide new and innovative services, these services can pose serious risks to the privacy and reputation of smart device users, smart devices do not always comply with European privacy law, the reason is that the supply of a smart device can be done through the internet and the specific device maybe does not comply by the European Union privacy law, Smart device users should not feel completely secure, as personal data loss is in any way in last years is very popular.

The issue of security and privacy is very important and unfortunately those who propose such projects do not realize it, since they are interested in the outcome, not the security, they are all sacrificing themselves on the altar of state publicity advertising, ignoring the fact that there are private companies that either operate on behalf of private interests or are funded by governments to scan smart devices to detect vulnerabilities for accessing the internal network and extracting information. The lack of security policies will simply be here to constantly remind us of mistakes and omissions while the citizens will in turn be the ones here to always collect the losses of their personal data and the violation of their privacy. A number of smart devices send the user's location and IP address to various servers that are often unrelated to the smart device manufacturer. Sensitive user data leaks to various companies, smart devices where installed in smart cities, leak personal data, even when they are inactive, these data can be channeled to third companies for any purpose, from statistic analysis to tracking specific people. Depending on the manufacturer of the smart device and the software it uses, the data sent could include the user's location, device type and terminal, as well as what services the user uses depending on the time.

The installation and configuration of smart devices installed in various cities to provide various services to citizens should be performed by people who know about smart devices, network and application security. It is no coincidence that several times in the past and several times in the future, smart devices have fallen and will fall victim to attacks that several times have been and will continue to be, since these devices have been shown to be vulnerable to various types of attacks, hackers scanning smart devices to detect vulnerabilities. Attackers can try everything to carry out an attack, for example to use the "weak" default credentials that have not been changed, to take possession of the weak passwords that are circulated in plain text, or to brute force accounts that have access to the admin web management console. Lack of encryption when transferring data, storing data or to view data transferred over the network. Those who could carry out such an attack may be internal or external attackers

who have access to the network to which a smart device is connected. Lack of Transport Encryption in smart devices is a security vulnerability that is common and easily detectable. Such a weakness leaves the attacker who "transferred" through the network or the Internet exposed to the attacker. The consequences of such a lack of protection are serious, as data loss is possible. Depending on the data that has been exposed, there is a possibility that will be exposed to a complete exposure of users' devices or user accounts. Privacy Concern, is something that is common in smart devices. This is due to the collection of personal data and in addition to the lack of proper protection. Smart device administrators may reviewing the data collected during the activation of a device and apply the appropriate privacy policy.

Attacks on smart devices will increase in the future as their technology evolves and the cost of acquiring such a device decreases significantly. Also reduce the complexity of installing a smart device, but unfortunately there is no automated security model, mistakenly believing that the necessary security settings have been activated by the manufacturer. Illegal access to such smart devices can lead to economic and social disaster. For example, unauthorized access to a smart device that handles the amount of water pumped through a pump could damage the pump, changing its timing frequency, the damage or flooding of the water tank or even shutting down the pump resulting in a city water supply being cut off. There are many ways to compromise a smart device. To compromise the security of a smart device, it is not necessary to violate the smart device first and then the internal network. Vulnerable services are running, backdoor viruses have been created or the network is being monitored by IP packet monitoring programs (sniffers). Remote control viruses can be installed either on the internal network by a user by mistake or intentionally, or at some point where the network is compromised, also, such viruses can be installed by violating the smart device to some extent in order to provide access to the internal network where to escalate rights with administrator capabilities or with a user who has increased permissions that allow the installation of applications. A smart device that is able to perform large-scale services, any breach will cause a major blow as the losses will be severe. Sometimes the selfishness and prestige of some people rushing to advertise to the citizens that a city from classic moves to smart and modern, therefore bypasses security protocols to show superiority to their opponents hastily proceeds to the disclosure of smart services, ignoring the security factor and personal data protection. Organizations they are unaware that the more popular the services they offer, the greater the security risk as the services offered become attractive to would-be intruders. The organizations do not understand the dangers of denial of service (DOS) attacks and automated attacks through BOT that will be accepted by smart devices with negative effects on citizens and of course with disgruntled citizens.

The design and study of data security, storage and validity of data and communication is what will really create a smart and secure city, a city where citizens will not be afraid to use smart devices, feel confident and trust the people behind smart devices. Experienced human resources are the ones that should support operation, upgrade and in early detection of threats to prevent them, the scanning of entire IP ranges from external sources to find vulnerabilities should not be tolerated and not be captured as a threat because there was no successful access. The integration of smart devices into access control systems certainly leads to some challenges that need to be addressed. Smart city managers, depending on the rate of integration of services offered to citizens in conjunction with digital security planning, can confuse design jurisdiction between engineers involved in the installation process and security design managers. This new element brings a set of needs, requirements and concerns for these two teams. The old philosophy that just connect something and it works was the sole responsibility of the installation's engineers, it is now a hub for the IT network, which leads to many challenges as both the challenges and the electronic threats have multiplied. Nowadays we have to be responsible for the maintenance of the physical security provided by the smart device, also add the competence of the ownership of the information. Also, human resources are the ones that need to know, configure, and control access points and the level of these access points. While the process of backup and designing Disaster Recovery is essential. It is worth noting here that the selection of the appropriate manufacturer to create a smart city with electronic medium that will meet the needs and requirements of both today's era and the citizens is a key element. There are many smart device components that someone can choose from, but it is important to remember that in this case, it is not just a product option but an approach that has been previously studied and designed properly. Usually the choice of sensors is made after a series of proposals for the various needs of creating a smart city.

It is taken for granted that software should not be installed from unreliable sources and no attachments should be open to the internal mail of personnel who are on the same network as smart devices, the validity of the sender via e-mail should not only be confirmed by e-mail address but also by e-mail headers. Informatics has changed a lot in last years, due to the great technological development of electronics. Smart devices belong to this field, over time smart devices will become even smarter by performing more complex processes, on the other hand, the more complex smart devices become, the greater their risk against electronic attacks. Data is at risk, as added new sensors and new devices to the network, possibly creating more risks. The greater the use, the greater the probability of a problem, the data transfer across networks has an impact on their reliability. Data availability is very important for Internet security as it ensures that users can access information resources in both normal and disastrous situations. Data availability also ensures uninterrupted flow of information. Data Integrity protects useful information from being stolen by cybercriminals (hackers) during

communication. There are a number of issues, such as denial of service attack (DoS) or power outages that can affect data integrity. The purpose of data confidentiality is to protect the confidentiality of sensitive information using certain mechanisms and to prevent unauthorized access. For smart devices such as sensors and nodes, data confidentiality means that the data collected by the sensors and nodes should not be transmitted to a single authorized entity. Encryption is a mechanism that ensures the confidentiality of data. Encrypted data is converted to encrypted text. Therefore, unauthorized users do not have easy access to the data.

Specialized personnel with knowledge of security and personal data protection combined with information security study will convince a smart city. Smart city is not the city that will install sensors and provide electronic services to the citizens, smart city is the one that the citizens will trust the electronic services it offers as they will know that their personal data is secure, encrypted while the communications re also protected, the citizens also may feel their transaction security with Smart devices are a given, and finally the smart electronic device system will continue to work under attack that means a mitigation plan is applied. Focusing on evolving technologies, smart device applications, and in particular the security and privacy issues that arise during their use, the ever-evolving development of smart devices is about to change the daily lives of ordinary people. There are many benefits to different areas of life. Health, smart travel, parking solutions, smart lighting are some realistic examples. But along with all these benefits, there are certain risks, as the increase in connected devices and the many vulnerabilities that exist, provide more opportunities for malicious users and cybercriminals to attack. Smart devices that use outdated security protocols that do not support encrypted communication, as well as the huge amount of data generated, incomplete authentication and authorization processes, and the small importance given to security issues, are only few of the key issues that lead to critical personal data and protection problems. As smart devices expands, citizens need to demand better levels of protection regarding their security and personal data, so that they are not vulnerable to third-party surveillance and data leaks. The biggest danger for smart cities is that citizens are slowly giving up their private lives without realizing it, because they do not know what data is being collected and how it is being used. Thus, they may fall victim to the detection, monitoring, loging, and configuration of their character, which implies the continuous violation of the privacy of their personal data. In order to avoid this risk, in addition to the need to adopt security mechanisms, the application of European legislation on the processing of personal data by smart devices should be taken into account. Smart devices are not safe smart phones are not safe too, always we must have on our minds **4** things:

1. Surveillance software does not appear in installed applications list. You will never find surveillance software installed by the eye of view, surveillance software running in the background and is difficult to locate, a smart device packed with pre-installed surveillance software can be delivered to an interested party.

2. Resetting to factory settings may not permanently eliminate the surveillance software. The reason is that this type of software has the ability to copy itself in different locations of the partitions of the operating system, thus activating the smart device the surveillance software run again.

3. Scrambled applications are easily localized, while well- designed applications run on Stealth Mode and extremely difficult to detect even with anti-malware protection.

4. A smart device including smart phones surveillance software can be downloaded to smart devices and smart phones through another applications.

Smart Devices divided in 3 levels:

1. Interaction with its sensors.

It deals with how a smart device interacts with sensors to collect information where this information then will be transmitted over the network to other locations for evaluation, processing, or decision making.

2. Interaction with the Internet or other local networks and devices.

It is about the process of interacting with smart devices, that is, how they talk to the rest of the network, which may not only consist of smart devices but of classic information systems. This level also includes the modes of transmission of the sensors for processing, for example, the transmission methods, such as the use of specific data transmission protocols.

3. The level of data publishing, whether it is a cloud application. A device that perform functions in conjunction with the data processed by the smart device, that means actuators.

Of course, it is about making decisions, since the useful information has now been collected and the smart devices will simply execute the result that came from analyzing the information that received from the sensors. There must be a secure connections between the sensor and the smart devices to prevent fake sensor combinations, this involves applying an appropriate security policy to ensure that the specific sensor is the one to be and that through it the sensor will interact with the IoT data in a secure manner. It should be borne in mind that the guarantee of the data that will interact with IoT with the sensor should be ensured because, on the basis of

these data, decisions will be made. Smart devices can have a wired or wireless connection. As for the wireless connection, there are many different communication technologies and protocols that can be used to connect these devices. Some of these are ZigBee, Bluetooth Low Energy, Z-Wave, and NFC (or Near Field Communication).

Storing the data is very important, and their perception could feed users with false data. The IoT should use secure and encrypted data transfer methods, storage space must also be safe, any tampering of the storage site poses a risk to both the data and the IoT itself. Creating a secure parallele storage system could control and restore fake files and let users know about it. When transferring the data, some kind of attack on the smart device network, whether can be a man in the middle attack or can also come from the internet. Therefore, an algorithm for self-protection of the smart device network is needed. There are some algorithms that are used for data accurancy, but without the right security policies they can not do much. Attackers include smart devices that operate in smart cities in botnets to attack them. Due to the limited security offered by smart devices, hackers can easily include and use such devices as they use zombie computers in botnets, building and maintaining even larger botnets. Having armies of botnets and command and control servers at their disposal, have more power to launch even more effective and efficient attacks. The kernel of an smart device is a red flag for attackers, it could hide a malware and loging forever the habits, data, and peculiarities of each user, giving the possibility to external attackers to create an online user profile and be able to know everything from its transitions, lifestyle, transactions, payment methods, habits, and personal data, that means an incorrect security policy, a wrong software, a vulnerable sensor, a vulnerable smart device including actuators, could burn the whole project. It is worth noting at this point, that only last year the attacks on smart devices exceeded **48%**.
Unauthorized users should not have access to smart device data management, policy management, firewall, operation, and publishing, the metadata often revealing important data sources. Authorized users should be granted partial access per level and not full access everywhere. Providing full access management everywhere at all levels then a DDOS attack could give complete access. Most of the security techniques that have been created are mainly aimed at the accuracy of the information transferred to the smart device network (for example point to point encryption, firewall policies). Thinking that in case of set-up elements are the sensors and the storage media, the possibility of contamination of the operating system remains second degree, a malware could work for years and log user habits, it will be a back door for the attackers, a back door of violation of human privacy.

The use of default features by the manufacturer itself for example usernames and passwords, makes it a vulnerable smart device network structure including the privacy, anyone who has physical or remote access and knows the IoT model is easy to try to access by identify for its factory settings and factory usernames and passwords. This is a very serious attack, the first thing people have to do is change the default usernames and passwords and in some cases the default settings. User accounts with incorrectly restricted permissions, no password, access to services without user authentication, are red flag for smart device security, can easily break the security of the smart device network that depending on the type of installation in a home will also have consequences. When an smart device is installed in a public place in which there is a computer network that interacts with the smart device, other smart devices, or decision support systems, should be ensured the harmonic communication with each other. If the computing network is unsafe then easily can break an smart device security. An smart device can not protect a vulnerable computing network, and a vulnerable computing network can not protect an smart device. It is important that where they store the data either if they will be stored locally on the premises, so there should be a way of data accurancy and backup, while in the case of Cloud the physical access is not permitted, should be ensured encryption of data information stored over there, while is important to creating a recovery plan in the case of data lose, data breach or in the case of something goes wrong.

The management of an smart device through a web environment is the backdoor of the network mainly through Wi-Fi networks. The violation of a Wi-Fi and then access to the entire network of the infrastructure allows external attackers to try illegally entering the smart device through its web console, where any successful access, the attackers would have full control over the functions through the sensors throughout the whole smart device infrastructure.

Conclusion

Smart devices will evolve even more, will be everywhere in our lives and will automatically perform many processes, but the evolution of smart devices does not go hand in hand with its security. It takes generations of change and design of systems and security methods to have truly secure smart devices, and this is not something that can automatically change from one day to the next, it takes time and study. Some solutions to the security problems of smart devices are:

1. Smart Device Updates

Manufacturers of smart devices should regularly release patches or firmware upgrades to the hardware they offer, and manufacturers should also allow users to report to the company any security vulnerabilities and securty issues.

2. Blockchain

blockchain is essentially a ledger in which information and data are stored and verified, which are usually included in a block, using cryptographic methods and in such a way as to create a continuous data chain, while modifying any recorded information. in the register to necessarily affect all subsequent entries. A blockchain platform can be public (open) or private (closed), respectively with public (via) networks (such as the internet) and internal networks (intranets) . Blockchain technology is coming to radically change this security status.

Using mathematics and cryptography, provides an open and decentralized database in any transaction. Creates a record for each transaction that can be verified by the entire community. Combining cryptography and distributed computing systems, blockchain provides secure, peer-to-peer transactions, blockchain technology can also provide a solution to the problem of security and privacy on smart devices, providing a new computing layer where data can be processed. be analyzed safely, remaining private. Implementing these features is expected to ensure a more efficient allocation of resources.

3. Staff Training

The human factor remains one of the most important threats, employees must recognize, understand, and implement the security policies that have been created and must be followed, Citizens' personal data must be secured in any way and must stored encrypted. Any attempt to violate any part or the entire network should be identified immediately a*nd neutralized.*

References

1. Christos Beretas. Smart Cities and Smart Devices: The back door to privacy and data breaches, 2020 Biomed J Sci & Tech Res | BJSTR. MS.ID.004588.

2. Christos Beretas. Internet of Things and Privacy, 2018.

3. Brian Russell, Drew Van Duren. Practical Internet of Things Security, 2016.

4. Nitesh Dhanjani. Abusing the Internet of Things: Blackouts, Freakouts, and Stakeouts, 2015.