Mini Review

BIOMEDICAL
Journal of Scientific & Technical Research

ISSN: 2574 -1241

DOI: 10.26717/BJSTR.2020.28.004588

Smart Cities and Smart Devices: The Back Door to Privacy and Data Breaches

Christos Beretas*

PhD Candidate (full scholarship) in Cyber Security at Innovative Knowledge Institute, France

***Corresponding author:** Christos Beretas, PhD Candidate (full scholarship) in Cyber Security at Innovative Knowledge Institute, France

ARTICLE INFO

Received: May 21, 2020

Published: June 01, 2020

Citation: Christos Beretas. Smart Cities and Smart Devices: The Back Door to Privacy and Data Breaches. Biomed J Sci & Tech Res 28(1)-2020. BJSTR. MS.ID.004588.

Keywords: Smart Cities; IoT; Smart Devices; Networks; Back Doors; Privacy

Abstract

The technological innovation has led societies to the need to design and create smart applications that are combined with smart devices that interact either automatically or after some action by their operators, Such devices range from automatic temperature gauges and active watering in public trees with tree planting to locating empty parking spaces on city streets with the help of smart sensors. All of the above seems nice and harmonious if there were no questions such as: is personal data collected by users? Is this data able to create a personal profile of the user regarding his/her daily habits including the location? to what extent is the meta-data collected are capable of violating the privacy of personal life? data related to users of this services where is stored and to what extent is there their encryption? if there is, of course, encryption, which if it does not exist is a tragic lack of security. Are the data collected by users then forwarded to government or private companies for statistical analysis? how are personal data ensured that they will not be forwarded to others for other purposes in the future? How does the use of such services by users, which may include money transactions, ensure that users will not be subject to further financial monitoring? Smart devices are part of a network, which means that an incomplete configuration of a smart device or install a smart device that offers incomplete security features and does not meet security standards is capable of providing remote access to the internal network that is connected, if there is illegal remote access to the internal network to the extent that it will be able to affect the integrity of the data but also the change of use of the operation of the smart device. All of the above are key questions about the integrity of smart devices, but also the level of security they offer that they are called upon to answer in this article.

Mini Review

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. 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. So 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 zonesperformed by external factors and in several cases showed vulnerabilities and access in the internal network, then what smart cities are they talking about? 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.

Analysis

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 outside from the country where smart devices operate, since these devices have been shown to be vulnerable to various types of attacks, which is why technologically advanced countries are scanning ranges of IP addresses of other countries to detect smart devices and detect vulnerabilities. As mentioned above, 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 [1].

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 auser 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 [2].

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 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. Finally, 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 [3].

Conclusion

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. 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, their transaction security with Smart devices are a given, and finally the smart electronic device system will continue to work when it’s raining and won’t be out of order.

References

1. Christos Beretas (2018) Internet of Things and Privacy. Current Trends in Computer Sciences & Applications 1(1): 1-2.
2. Brian Russell, Drew Van Duren (2016) Practical Internet of Things Security. pp. 336.
3. Nitesh Dhanjani (2015) Abusing the Internet of Things: Blackouts, Freakouts, and Stakeouts.

ISSN: 2574-1241

DOI: 10.26717/BJSTR.2020.28.004588

Christos Beretas. Biomed J Sci & Tech Res