CYBERSECURITY AND THE SMART CITY

Protecting the Smart City with CITISIM Platform

25/11/2019

BALUSIAN

BALUSIAN

Table of Contents

1 INTRO

Smart cities technology such as smart traffic control, smart energy management, smart parking, smart water management, smart street lighting, smart public transportation or security, bring (and will bring) an amount of improvements to the way cities are managed. In this context, CitiSim is an Intelligent Services Platform whose main goal is devoted to the design and implementation of a new generation platform for the smart city ecosystem.

Smart platforms do not only bring improvements, they also open new cybersecurity worries.

In this article we will explain what cybersecurity is and how it is related to Smart Cities. We'll have a look at the main dangers that can affect smart cities managed by Intelligent Services Platforms such as CitiSim, and how they can be carried out. And most importantly, we'll present the way we can face such threats.

2 WHAT IS CYBERSECURITY

Information security or cybersecurity is a discipline that comprehends different technologies and activities with **the objective of protecting technological infrastructures and the information** that is generated, processed, transmitted and stored in such infrastructures or computer networks. Protection focuses on the different dimensions of security, which are, at least, confidentiality, integrity, and availability. **Confidentiality** aims at protecting our valuable information (data on citizens, data generated by IOT sensors, information related to service platforms, sale reports, …) from unauthorized access, by means of encryption techniques and access control, or the use of firewalls. **Integrity** implies that data is not affected by mistakes or malicious modifications (modifications in payments and monetary transactions, changes in the content of emails, introduction of malicious codes within service applications), through the use of signatures, control of versions, antivirus systems and antimalware. Finally, **availability** refers to the necessity of the information being accessible for authorized parties who require it (citizens, IT administrators, providers), through redundancy systems and high availability, protection against external attacks and recovery systems in the case of failure.

Guaranteeing the information security of the infrastructures implies in setting up different prevention and protection measures or controls, along with detection and incident response to avoid and be protected against safety incidents. **There are different general security frameworks** that help identify the most adequate controls and measures (ISO 27001:2013, NIST Cybersecurity Framework, CIS Critical Security Controls). In the last years, more specific framework and best practices related to the IOT environment have been released, such as:

- ETSI TS 103 645 (2019-02): Cyber Security for Consumer Internet of things [1]
- ENISA Good practices for IoT and Smart Infrastructures Tool[2]
- NIST: Core Cybersecurity Feature Baseline for Securable IoT Devices. 3
- ISO/IEC 27030: Information technology — Security techniques —Guidelines for security and privacy in Internet of Things (IoT)[4]

[1] https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf
[2] https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/good-practices-for-iot-and-smart-infrastructures-tool
[3] https://csrc.nist.gov/publications/detail/nistir/8259/draft
[4] https://www.iso.org/standard/44373.html

- OWASP Internet Of Things Project[5]

A common characteristic in many of those ¡ standards is the focus on risk management, where risk is understood as the materialization of a system threat that can exploit the vulnerabilities (or weaknesses) offered by such systems, generating an impact.

RISK = THREAT x VULNERABILITY x IMPACT

3 RISK SCENARIOS IN SMART CITIES

We live in the early stages of a new kind of war against city governments and urban infrastructure. Some cities have capacities in place and can face them, but others are totally unprepared for the scale of cyberthreats.

3.1 Treats and resulting impacts

Let's first show several examples of cyberattacks that have taken place recently:

Date	Location	Asset affected	Attack description
December 2015	Ukraine	Power Grid	Attackers were able to compromise information systems of three energy distribution companies, affecting 30 substations and temporarily disrupt electricity supply to 230.000 end consumers. This is considered to be the first known successful cyberattack on a power grid.
March 2016	Undisclosed	Water treatment plant	Attackers changed the levels of chemicals used to treat tap water during an attack on the outdated IT network of the plant, exploiting its web-accessible payments systems and using it to access the company's web server.
April 2017	Dallas (USA)	Emergency alarms	Attackers turned on 156 of the city emergency alarms, initially designed to warn citizens about severe storms, tornados and other dangerous weather. Not only did it cause significance noise throughout the city, it also caused a surge in 911 calls (some who weren't calling about the sirens couldn't get through the emergency calls).
March 2018	Atlanta (2018)	City hall and airport	A ransomware cyberattack shuttered many devices at the City Hall for about five days in an extensive infection. It impacted law enforcement, and police had to temporarily write incidents by hand and costing the department access to nearly all its archived in-vehicle video. It also affected internal- and

[5] https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

			external-facing applications alike, forcing the manual processing of cases at Atlanta Municipal Court and stopping online or in-person payment of tickets, water bills, and business licenses and renewals. Out of caution, officials also disabled the Wi-Fi at Hartsfield-Jackson Atlanta International Airport until April 2.
June 2019	Riviera Beach (Florida, USA)	City's computer systems	A ransomware attack began after a police department employee opened an infected email attachment. Down went all of the city's online systems, including email and some phones, as well as water utility pump stations. The City Council unanimously agreed to have its insurance carrier pay the hackers 65 Bitcoin, a hard-to-trace digital currency, amounting to about $592,000.
October 2019	Johannesburg (South Africa)	City services	Key city systems including online services, bill payments and 112 emergency calls were shut down after a ransomware attack. Cybercriminals were demanding a ransom of 4 Bitcoins ($37,000) and threatened to upload the hacked data online (they claimed to have backed doors in the city systems).

As we can see, cyber criminals are launching ransomware, distributed denial of service attacks and other off-the-shelf hacker tools to interrupt and rob municipal infrastructure. Their digital weapons come from the Deep Web and they are fully automated, which means the attacks can run without interruption. The impacts of such attacks can be devastating.

Things can even turn worse due to technological acceleration and refinement of cybercrime. To date, most cyberattacks have taken place in cities that are not yet digitally wired, meaning the impact of the threats will be much more dramatic if cybercriminals are able to access and modify smart traffic control or smart street lighting infrastructures. In this context, the problem won't be monetary and will probably produce loss of life.

Let's summarize the main threats a smart city can face, according to the Threat Taxonomy defined by ENISA[6].
NOTE: not all the threats are due to cyberattacks. Many of them are due to unintentional accidents, so we'll also consider them in this list.

Category	Threat	Description
Nefarious activity / Abuse	Malware	Software programs designed to carry out unwanted and unauthorised actions on a system without the consent of the user, resulting in damage, corruption or information theft. Its impact can be high.
	Exploit Kits	Code designed to take advantage of a vulnerability in order to gain access to a system. This threat is difficult to detect and in IoT

[6] Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures – November 2017

Category	Threat	Description
		environments its impact ranges from high to crucial, depending on the assets affected.
	Targeted attacks	Attacks designed for a specific target, launched over a long period of time, and carried out in multiple stages. The main objective is to remain hidden and to obtain as much sensitive data/information or control as possible. While the impact of this threat is medium, detecting them is usually very difficult and takes a long time.
	DDOS	Multiple systems attack a single target in order to saturate it and make it crash. This can be done by making many connections, flooding a communication channel or replaying the same communications over and over.
	Counterfeit by malicious devices	This threat is difficult to discover, since a counterfeit device cannot be easily distinguished from the original. These devices usually have backdoors and can be used to conduct attacks on other ICT systems in the environment.
	Attacks on privacy	This threat affects both the privacy of the user and the exposure of network elements to unauthorised personnel.
	Modification of information	In this case, the objective is not to damage the devices, but to manipulate the information in order to cause chaos or acquire monetary gains.
Eavesdropping / Interception / Hijacking	Man in the Middle	Active eavesdropping attack, in which the attacker relays messages from one victim to another, in order to make them believe that they are talking directly to each other
	IOT communication protocol hijacking	Taking control of an existing communication session between two elements of the network. The intruder is able to sniff sensible information, including passwords. The hijacking can use aggressive techniques like forcing disconnection or denial of service.
	Interception of information	Unauthorised interception (and sometimes modification) of a private communication, such as phone calls, instant messages, e-mail communications
	Network reconnaissance	Passively obtain internal information about the network: devices connected, protocol used, open ports, services in use, etc.
	Session Hijacking	Stealing the data connection by acting as a legitimate host in order to steal, modify or delete transmitted data.
	Information gathering	Passively obtain internal information about the network: devices connected, protocol used, etc.
	Replay of messages	This attack uses a valid data transmission maliciously by repeatedly sending it or delaying it, in order to manipulate or crash the targeted device.
Outages	Network outage	Interruption or failure in the network supply, either intentional or accidental. Depending on the network segment affected, and on the time required to recover, the importance of this threat ranges from high to critical.
	Failure of devices	Threat of failure or malfunction of hardware devices.
	Failure of system	Threat of failure of software services or applications
	Loss of support services	Unavailability of support services required for proper operation of the information system.
Damage / Loss (IT assets)	Data / Sensitive information leakage	Sensitive data is revealed, intentionally or not, to unauthorised parties. The importance of this threat can vary greatly, depending on the kind of data leaked.
Disaster	Natural Disaster	These include events such as, floods, heavy winds, heavy snows, landslides, among others natural disaster, which could physically damage the devices.

Category	Threat	Description
	Environmental disaster	Disasters in the deployment environments of IoT equipment and causing their inoperability.
Physical attacks	Device modification	Tampering a device by for example taking advantage of bad configuration of ports, exploiting those left open.
	Device destruction (sabotage)	Incidents such devices theft, bomb attacks, vandalism or sabotage could damage devices

3.2 Vulnerabilities

Provided smart cities infrastructures can be attacked, causing serious consequences, let's now identify the vulnerabilities that can be exploited by such threats.

The main reason why cities have become targets for cybercriminals is because the underlying technologies running the critical infrastructure are obsolete, and city authorities often lack the skills to upgrade the systems.

Let's detail the main cybersecurity problems facing smart cities, according to the report "Smart Cities – Cyber Security Worries"[7]:

Vulnerability	Name	Description
1	Lack of cybersecurity testing	Most cities around the world are implementing new technologies without testing cybersecurity.
2	Poor or non-existent security	No basic security practices present on city technology development.
3	Encryption issues	Most technologies are wireless which are easier to hack is communications is not properly encrypted.
4	Lack of Computer Emergency Response Teams	Cities don't have Computer Emergency Response Teams to help coordinate security incidents response.
5	Large and complex attack surface	With so much complexity and interdependency, it is difficult to know what and how everything is exposed.
6	Patch deployment issues	It is common for cities to use vulnerable technology because vendors are slow to release security patches or patches are not applied.
7	Insecure legacy systems	Vulnerable and older systems are used, this adds complexity and increases in the attack surface.
8	Public sector issues	Cities have inadequate budgets, training and resources and on top of that there is bureaucracy.
9	Lack of cyber-attack emergency plans	Cities are not prepared against possible cyber-attacks.
10	Susceptibility to denial of service	With so many services dependent on technology, attackers have many methods to abuse them and cause Denial of Service (DoS)

[7] https://securingsmartcities.org/wp-content/uploads/2019/01/SmartCities-cybersecurity-worries.pdf

4 SECURITY MEASURES AND GOOD PRACTICES

4.1 How can cities protect themselves from threats defined in the previous sections?

Cities can no longer ignore cyberthreats, just as it does with traditional crime fighting, and must define a cybersecurity strategy. If cities such as Tokyo or San Francisco have prepared for many years now against natural disasters such as tsunamis and earthquakes, so too must cybersecurity become a core component of the city policy.

Defining a cybersecurity strategy is not only about hardware and software., a whole approach must be adopted, and cybersecurity must be conceived as an essential priority, taking into account since the design of smart services and not considered as an afterthought. Leaders must develop regulations, procedures and budgets in order to protect against attack and be able to respond once they will take place.

Baseline security recommendations from organizations such as ENISA[8] or NIST[9] provide a good starting point for implement cybersecurity measures which aim to mitigate the threats, vulnerabilities and risks identified in this document. They cover a wide range of security considerations, as we can see from the ENISA "Baseline Security Recommendations for IOT in the context of Critical Information Infrastructures":

Type of security measure	Control	Description of controls
Policies	Security by design	Consider the security of the whole IoT system from a consistent and holistic approach during its whole lifecycle across all levels of device/application design and development, integrating security throughout the development, manufacture, and deployment. Ensure the ability to integrate different security policies and techniques. Security must consider the risk posed to human safety. Designing for power conservation should not compromise security. Design architecture by compartments to encapsulate elements in case of attacks. For IoT hardware manufacturers and IoT software developers it is necessary to implement test plans to verify whether the product performs as it is expected. Penetration tests help to identify malformed input handling, authentication bypass attempts and overall security posture. For IoT software developers it is important to conduct code review during implementation as it helps to reduce bugs in a final version of a product.
	Privacy by design	Make privacy an integral part of the system. Perform privacy impact assessments before any new applications are launched.
	Asset Management	Establish and maintain asset management procedures and configuration controls for key network and information systems.
	Risk and Threat Identification and Assessment	Identify significant risks using a defence-in-depth approach. Identify the intended use and environment of a given IoT device.
Organisational, People and	End-of-life support	Develop an end-of-life strategy for IoT products. Disclose the duration and end-of-life security and patch support (beyond product warranty). Monitor the performance and patch known vulnerabilities up until the "end-of-support" period of a product's lifecycle.

[8] https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/good-practices-for-iot-and-smart-infrastructures-tool

[9] https://csrc.nist.gov/publications/detail/nistir/8259/draft

Type of security measure	Control	Description of controls
Process measures	Proven solutions	Use proven solutions, i.e. well-known communications protocols and cryptographic algorithms, recognized by the scientific community, etc. Certain proprietary solutions, such as custom cryptographic algorithms, should be avoided.
	Management of security vulnerabilities and/or incidents	Establish procedures for analysing and handling security incidents. Coordinated disclosure of vulnerabilities. Participate in information-sharing platforms to report vulnerabilities and receive timely and critical information about current cyber threats and vulnerabilities from public and private partners. Create a publicly disclosed mechanism for vulnerability reports, e.g. Bug Bounty programs.
	Human Resources Security Training and Awareness	Ensure the personnel practices promote privacy and security – train employees in good privacy and security practices. Document and monitor the privacy and security training activities. Ensure that cybersecurity roles and responsibilities for all workforce are established and introduce personnel assignments in accordance with the specifics of the projects and security engineering needs.
	Third-Party relationships	Data processed by a third-party must be protected by a data processing agreement. Only share consumers' personal data with third parties with express consent of the consumers, unless otherwise required and limited for the use of product features or service operations. For IoT hardware manufacturers and IoT software developers it is necessary to adopt cyber supply chain risk management policies and to communicate cyber security requirements to its suppliers and partners.
Technical measures	Hardware security	Employ a hardware-based immutable root of trust. Use hardware that incorporates security features to strengthen the protection and integrity of the device – for example, specialised security chips / coprocessors that integrate security at the transistor level, embedded in the processor, providing, among other things, a trusted storage of device identity and authentication means, protection of keys at rest and in use, and preventing unprivileged from accessing to security sensitive code. Protection against local and physical attacks can be covered via functional security.
	Trust and integrity management	Trust must be established in the boot environment before any trust in any other software or executable program can be claimed. Sign code cryptographically to ensure it has not been tampered with after signing it as safe for the device and implement run-time protection and secure execution monitoring to make sure malicious attacks do not overwrite code after it is loaded. Control the installation of software in operating systems, to prevent unauthenticated software and files from being loaded onto it. Enable a system to return to a state that was known to be secure, after a security breach has occurred or if an upgrade has not been successful. Use protocols and mechanisms able to represent and manage trust and trust relationships.
	Strong default security and privacy	Any applicable security features should be enabled by default, and any unused or insecure functionalities should be disabled by default. Establish hard to crack, device-individual default passwords.
	Data protection compliance	Personal data must be collected and processed fairly and lawfully, it should never be collected and processed without the data subject's consent. Make sure that personal data is used for the specified purposes for which they were collected, and that any further processing of personal data is compatible and that the data subjects are well informed. Minimise the data collected and retained. IoT stakeholders must be compliant with the EU General Data Protection Regulation (GDPR). Users of IoT products and services must be able to exercise their rights to information, access, erasure, rectification, data portability, restriction of processing, objection to processing, and their right not to be evaluated on the basis of automated processing.

Type of security measure	Control	Description of controls
	System safety and reliability	Design with system and operational disruption in mind, preventing the system from causing an unacceptable risk of injury or physical damage. Mechanisms for self-diagnosis and self-repair/healing to recover from failure, malfunction or a compromised state. Ensure standalone operation - essential features should continue to work with a loss of communications and chronicle negative impacts from compromised devices or cloud-based systems.
	Secure Software / Firmware updates	Ensure that the device software/firmware, its configuration and its applications have the ability to update Over-The-Air (OTA), that the update server is secure, that the update file is transmitted via a secure connection, that it does not contain sensitive data (e.g. hardcoded credentials), that it is signed by an authorised trust entity and encrypted using accepted encryption methods, and that the update package has its digital signature, signing certificate and signing certificate chain, verified by the device before the update process begins. Offer an automatic firmware update mechanism. Backward compatibility of firmware updates. Automatic firmware updates should not modify user-configured preferences, security, and/or privacy settings without user notification.
	Authentication	Design the authentication and authorisation schemes (unique per device) based on the system-level threat models. Ensure that default passwords and even default usernames are changed during the initial setup, and that weak, null or blank passwords are not allowed. Authentication mechanisms must use strong passwords or personal identification numbers (PINs) and should consider using two-factor authentication (2FA) or multi-factor authentication (MFA) like Smartphones, Biometrics, etc., on top of certificates. Authentication credentials shall be salted, hashed and/or encrypted. Protect against 'brute force' and/or other abusive login attempts. This protection should also consider keys stored in devices. Ensure password recovery or reset mechanism is robust and does not supply an attacker with information indicating a valid account. The same applies to key update and recovery mechanisms.
	Authorisation	Limit the actions allowed for a given system by Implementing fine-grained authorisation mechanisms and using the Principle of least privilege (POLP): applications must operate at the lowest privilege level possible. Device firmware should be designed to isolate privileged code, processes and data from portions of the firmware that do not need access to them. Device hardware should provide isolation concepts to prevent unprivileged from accessing security sensitive code.
	Access Control – Physical and Environmental security	Data integrity and confidentiality must be enforced by access controls. When the subject requesting access has been authorised to access particular processes, it is necessary to enforce the defined security policy. Ensure a context-based security and privacy that reflects different levels of importance. Measures for tamper protection and detection. Detection and reaction to hardware tampering should not rely on network connectivity. Ensure that the device cannot be easily disassembled and that the data storage medium is encrypted at rest and cannot be easily removed. Ensure that devices only feature the essential physical external ports (such as USB) necessary for them to function and that the test/debug modes are secure, so they cannot be used to maliciously access the devices. In general, lock down physical ports to only trusted connections.
	Cryptography	Ensure a proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of data and information (including control messages), in transit and in rest. Ensure the proper selection of standard and strong encryption algorithms and strong keys and disable insecure protocols. Verify the robustness of the implementation. Cryptographic keys must be securely managed. Build devices to be compatible with lightweight encryption and security techniques. Support scalable key management schemes.

Type of security measure	Control	Description of controls
	Secure and trusted communications	Guarantee the different security aspects -confidentiality (privacy), integrity, availability and authenticity- of the information in transit on the networks or stored in the IoT application or in the Cloud. Ensure that communication security is provided using state-of-the-art, standardised security protocols, such as TLS for encryption. Ensure credentials are not exposed in internal or external network traffic. Guarantee data authenticity to enable reliable exchanges from data emission to data reception. Data should always be signed whenever and wherever it is captured and stored. Do not trust data received and always verify any interconnections. Discover, identify and verify/authenticate the devices connected to the network before trust can be established, and preserve their integrity for reliable solutions and services. IoT devices should be restrictive rather than permissive in communicating. Make intentional connections. Prevent unauthorised connections to it or other devices the product is connected to, at all levels of the protocols. Disable specific ports and/or network connections for selective connectivity. Rate limiting. Controlling the traffic sent or received by a network to reduce the risk of automated attacks.
	Secure interfaces and network services	Risk Segmentation. Splitting network elements into separate components to help isolate security breaches and minimise the overall risk. Protocols should be designed to ensure that, if a single device is compromised, it does not affect the whole set. Avoid provisioning the same secret key in an entire product family, since compromising a single device would be enough to expose the rest of the product family. Ensure only necessary ports are exposed and available. Implement a DDoS-resistant and Load-Balancing infrastructure. Ensure web interfaces fully encrypt the user session, from the device to the backend services, and that they are not susceptible to XSS, CSRF, SQL injection, etc. Avoid security issues when designing error messages.
	Secure input and output handling	Data input validation (ensuring that data is safe prior to use) and output filtering.
	Logging	Implement a logging system that records events relating to user authentication, management of accounts and access rights, modifications to security rules, and the functioning of the system. Logs must be preserved on durable storage and retrievable via authenticated connections.
	Monitoring and Auditing	Implement regular monitoring to verify the device behaviour, to detect malware and to discover integrity errors. Conduct periodic audits and reviews of security controls to ensure that the controls are effective. Perform penetration tests at least biannually.

5 SECURITY MEASURES PROVIDED BY CITISIM PLATFORM

5.1 How can CitiSim platform help implement the cybersecurity strategy?

CitiSim has been concerned by cybersecurity issues since its beginning and helps implement some of the security measures defined in the previous section. The platform has to take into account the process of communicating data between the different entities that participate in the overall data flow, such as users, devices, services, sensors, actuators, etc., in a secure manner, such that communication channels are not infiltrated, and illegitimate date makes its way into the platform.

The security considerations that have been considered by CitiSim take into account those two main requirements:

- **The identity of an entity within CitiSim should be verifiable**: It is important to be able to verify and crosscheck the alleged identity of the entity within CitiSim, regardless of whether its publishing data or requesting it. In the case of the ammonia sensor, we must be able to ensure that the information regarding ammonia levels is in fact coming from a trusted source. If trust is not ensured in this scenario, an attacker could set up a "fake" ammonia sensor and send illegitimate values to the CitiSim platform in order to trigger some sort of emergency response when it was not necessary. In this regard, sensors, actuators, and services must be identifiable.
- **Actuator instructions must originate from trustworthy sources**: similar to the above example, sending a signal to an actuator that closes a water valve in a critical area of the city must come from an entity with the right authority to issue that action. If this is not the case and trust is not ensured in this context, an attacker may open and close valves or interact with other actuators without much effort, possibly jeopardizing lives and the stability of the system. Due to this, entities that request information or want to perform an action with an actuator must also be identifiable.

In order to assure this, Citisim project has implemented, among others, the following solutions:

- Secure communications
- A Public Key Infrastructure (PKI)
- Authentication and authorisation management for every service
- Platform hardening
- Software updates
- Logging and auditing

It's important to understand that the PKI infrastructure ensures a secure cryptosystem using digital certificates that prove an entity is who it claims to be. The PKI is composed of systems such as sensors, actuators, and services. Additionally, the role of the certification authority can be granted to the actual public authorities participating in the project such as local municipalities and city halls. In this regard, when a sensor, actuator, or service wishes to be incorporated into the CitiSim network, it must create a Certificate Signing Request and forward it to the corresponding governmental entity, in the hope of getting it validated and with it, obtain a digital certificate. Once the entity obtains the digital certificate, it will be able to participate in the network and communicate with other entities under the protection of the security layer via the use of the SSL protocol.

Apart from those cybersecurity controls, CitiSim can also help the client define the overall cybersecurity approach after the CitiSim platform has been connected to the client's infrastructure and understand how it can be included in the existing cybersecurity strategy.

6 CONCLUSIONS

Cities will have to define their priorities taking into considerations the threats that will have to face their networked urban landscape. While the improvements they will benefit are quite clear, they must be confronted carefully against the new risks we have identified in this document. As it is very likely any city can be attacked, cybersecurity strategy must be a priority for leaders and policymakers, given the available resources.

Identifying the dependency of metropolitan services with technology is the first step to detect the cybersecurity measures needed, most of which can be taken from the recognized organizations seen (ENISA, NIST, OWASP).

Councils and public organizations adopting CitiSim platform will benefit from its smart services, but they will have to implement a smart city cybersecurity strategy. As we have seen, CitiSim guarantees secured features in their different modules, and can also help define a Smart City cybersecurity strategy.