Towards a Secure City: The Contribution of the Smart City Physical Demonstrator in Threat Assessment

Marina Galiano Botella
CSIRT-CV
Valencia, Spain
e-mail: csirtcv@gva.es

Eduardo Ortega Serrano
S2 Grupo
Valencia, Spain
e-mail: csirtcv@gva.es

Elvira Lara Maudos
S2 Grupo
Valencia, Spain
e-mail: csirtcv@gva.es

Abstract- **Smart Cities are susceptible to cyberattacks due to the large amount of data being collected and shared in real time across networks and connected systems. Cyberattacks on Smart Cities can have serious consequences, such as unauthorized access to sensitive information, sabotage of critical infrastructure, and disruption of essential services. Prior studies have developed testbeds in the context of Smart Cities, but these have not been primarily focused on cybersecurity. Furthermore, existing research on cybersecurity within Smart Cities often comprises literature reviews rather than practical experimentation in a test environment. In this paper, we propose a Smart City physical demonstrator. It aims to investigate and analyze in depth these systems to know the scope of the different attacks and generate measures to mitigate the risks and impact. In addition, the demonstrator seeks to raise awareness of Smart City users and organizations involved in its development. The physical demonstrator of a Smart City serves as an invaluable resource for cybersecurity teams, empowering them to enhance their understanding of Smart City environments.**

Keywords*- *Smart City; cybersecurity; traffic; waste; electrical vehicles.

I. INTRODUCTION

Smart Cities are born with the aim of reducing the consumption of resources and improving the efficiency of the management of services, as well as improving the quality of life of citizens, reducing pollution and making cities safer and more livable. On the other hand, the revolution brought about by the Internet of Things (IoT) has made feasible the precise and instantaneous measurement of many variables that affect the environment of cities, making it possible for the first time to make decisions based on instantaneous, highly accurate data.

The rapid transition to smart cities has led to the rapid adoption of the devices being used without regard to cybersecurity. This is reflected in some cyberattacks on smart cities that leave the city without the software necessary for city management, resulting in loss of police records or other court documents [1]. For these reasons, it is evident the need to have a thorough understanding of the implicit risks of this digital transformation and to be prepared to respond effectively to the possible risk scenarios to which a Smart City may be subjected. In short, a correct transition towards a Smart City model must be accompanied by a correct securitization specialized in cybersecurity.

Among the systems that can be found in Smart Cities, traffic management, waste management and electric vehicle charging systems, are of particular interest. These systems are the ones that have been selected to make a physical demonstrator of a Smart City, based on the city of Valencia, Spain. The components used in the environment can be found in real Smart City locations, as well as with the same configurations.

A. *Traffic management*

Traffic management is represented by the use of a camera. Cameras play an important role in traffic management in modern cities. They enable traffic operators to monitor and control vehicle flow, detect traffic violations and generally improve road safety. Cameras can be used to monitor traffic lights and crosswalks, detect vehicles in bus lanes or exclusive lanes, as well as to detect traffic violations, such as speeding, red light violations or using a cell phone while driving. In addition, cameras can be used to collect traffic data, which helps to plan and improve city infrastructure [2].

B. *Waste management*

Waste management in the demonstrator is represented by an urban waste sensor installed inside a container. These sensors are an important tool for improving waste collection efficiency, as they allow city operators to monitor container filling and plan waste collection more effectively. Sensors can also help reduce collection costs, as operators can collect containers only when they are full, rather than on a defined schedule. In addition, some of these sensors can be used to measure air quality, providing valuable data for urban planning and environmental management [3][4].

C. *Electric vehicle charging systems management*

In this case, electric vehicle charging is represented by an outdoor charging station. Electric vehicle chargers are essential in Smart Cities because they enable the transition towards a more sustainable and cleaner mobility. These chargers are important for urban planning, as they enable energy demand management and optimization of power grid usage [5]-[7].

The objectives of the demonstrator are to investigate and analyze in depth the systems and threats to which Smart Cities are exposed, raise awareness among people and organizations using the systems, and perform tests on these systems to know the scope of the different attacks and thus be able to generate measures to reduce or eliminate the impact.

Within the paper's structure, in Section 2, the related work concerning testbeds, digital twins and cybersecurity in Smart Cities will be presented. In Section 3, the testbed setup and the proposed cybersecurity investigation methods for Smart Cities will be outlined. In Section 4, the outcomes and consequences of the conducted attacks will be presented. In Section 5, conclusions are summarized, project challenges are discussed, and future work is highlighted.

II. STATE OF ART

Significant technological advancements in replicating environments have occurred, as we have witnessed a noticeable shift from traditional testbeds to what we now refer to as digital twins [8]. These digital twins are highly detailed digital representations of physical products and even entire environments, playing a pivotal role in various applications, including Smart Cities [9]-[12]. While there are numerous testbeds specializing in Smart Cities [13]-[15], it is less common to find initiatives that integrate these testbeds with digital twins. Additionally, these approaches often overlook the aspect of cybersecurity.

However, it is important to note that, on occasion, potential applications in the field of cybersecurity that these digital twin models offer are mentioned [11]. Cybersecurity stands as a critical element in Smart Cities, and the capability to simulate and analyze cyber threats in virtual environments can be essential for protecting critical infrastructure and intelligent systems within the city.

Conversely, the continuous increase in cyberattacks directed at the Smart Cities sector has spurred the creation of studies that analyze trends and types of attacks that have occurred or could potentially occur within these smart cities [16]-[19]. Some of them apply new technologies such as Deep Learning or other kinds of Artificial Intelligence (AI) [20][21]. Nevertheless, it is relevant to mention that most of these studies tend to consist of literature reviews or compilations of existing data, rather than conducting actual attacks in a controlled testing environment. For this reason, the project focuses on creating a hybrid testbed that combines real systems with typical elements of a digital twin. The goal of this testbed is to represent a Smart City and be useful for conducting cybersecurity tests on a small and large scale, allowing us to observe the impacts of cyberattacks. It also serves as a means of raising awareness about these environments.

III. MATERIALS AND METHODS

The Smart City demonstrator mainly represents three management systems: traffic, waste and electric vehicle chargers. For each of these systems, a traffic camera, a waste sensor and an electric vehicle outdoor charging station have been used as main elements, respectively. In addition, there are several PCs for the management of the devices. It should be noted that the connection of all devices is wired directly to the managed switch except for the waste management sensor, which communicates with a router to provide Internet connection and to communicate with a real pre-production platform.

The environment has been designed with the aim of making the training and demonstrations as visual as possible. For this purpose, there are different visualization screens where the consequences of an attack on one of these systems can be shown. To play the role of an external attacker, there is a laptop from which some of the malicious behaviors can be simulated in order to affect the infrastructure of a Smart City.

When monitoring the environment, a port mirror is used on the switch to study attacks from a defensive perspective.

Figure 1 shows the pre-construction design of the Smart City. The laboratory consists of five assemblable parts (racks).

- Main rack: The electrical cabinet containing the switchgear, network electronics and device control elements is located in this rack. In addition, there is a display at the top for the management of the devices in the environment.
- Rack 1: Contains the electric vehicle charging station.
- Rack 2: The waste management system has been installed, which includes a trash container and the sensor installed inside it.
- Rack 3: It contains the traffic camera system. The camera is installed in the upper part and the display screen in the lower part.
- Rack 4: Contains two screens showing the city's pre-production platform and viewing environment.

The abuse cases will be developed in Python 3, compiled into a single script that can be launched automatically, making it unnecessary for the attacker to have technical knowledge to compromise the different components of the Smart City. For attacks on the charger and camera, the attacker's PC will be connected via an ethernet cable, while attacks on the debris sensor will be done wirelessly.

The abuse cases proposed for development are described below:

A. *Ransomware attack on the charging infrastructure*

The goal of the attack is to power down the charger's sockets. In this way, the attacker would disable the charger and ask for a ransom to restore the charger to its normal state. During the attack, it will be shown that an attempt is made to enable the charger, but it automatically reverts to the disabled state.

B. *Man in the Middle (MitM) in the charging system*

The purpose of the attack is to show the customer that their vehicle is charging when it is not. Thus, the blue light indicating "charging" status will illuminate but the charging socket will actually be powered down.

C. *Obtaining camera credentials*

The purpose here is to obtain the camera’s credentials via web cookie or via brute force by performing an attack on its sending protocol Real-Time Streaming Protocol (RTSP).

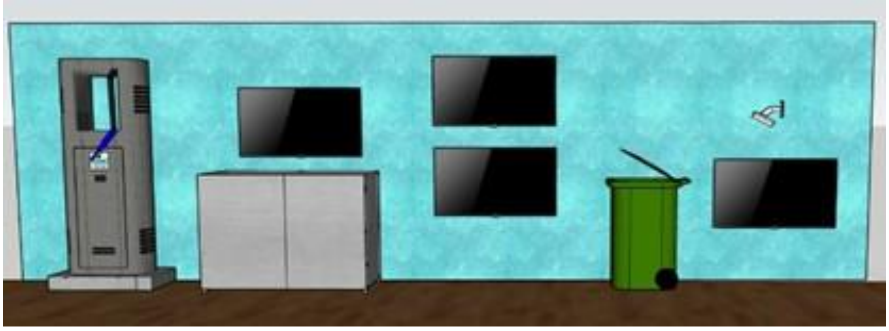

Figure 1. 3D design of the physical demonstrator of the Smart City. The 3D design consists of 5 racks with various displays and real systems of a Smart City.

D. *Attack on the camera access token*

By means of the user's access token, different configuration elements such as zoom, brightness or intensity can be changed so that the image displayed does not correspond to the real image.

E. *Obtaining credentials from the waste management sensor*

This represents a method of extracting authentication credentials through tools against the Message Queuing Telemetry Transport (MQTT) protocol.

F. *MitM between the waste management sensor and the management platform*

Tampering in the middle of the communications between the sensor and the sensor management web page to steal information or enter modified information.

IV. RESULTS

The Smart City demonstrator consists of several modules. Figure 2 shows the visualization of the Smart City racks. The image illustrates the structure of racks 2 and 4 in the Smart City prototype with the displays and the waste management sensor. Also, it shows the racks 1 and 3 where the charger of the electric vehicle charging management system and the camera of the traffic management system are located, respectively.

The abuse cases are currently under development. However, an analysis of the implications of each of the attacks in case of success has been carried out.

A. *Ransomware attack on the charging infrastructure*

Removing the availability of charging devices can create a significant logistical problem in the city. If the problem extends to several systems and for an extended period of time, it could create a sense of discomfort and dissatisfaction in the population by not being able to use the electric vehicle charging services of their city, undermining the mobility capacity of its inhabitants.

B. *MitM in the charging system*

The spoofing of a charge may cause complaints from the population to increase and saturate certain citizen services or even if this extends to several devices, the technical staff will not be able to cover the repair of all of them.

C. *Obtaining camera credentials*

Obtaining the credentials of traffic cameras may involve having access to modify the credentials and restrict workers' access to them or even power down the cameras. This would force technicians to go in person camera by camera to reset them.

D. *Attack on the camera access token*

Altering camera visual settings means that traffic control center workers cannot do their job properly or the camera cannot analyze the data correctly. If one of the cameras records videos and uses AI algorithms to count vehicles but the zoom has been changed, this data would include errors.

E. *Obtaining credentials from the waste management sensor*

Obtaining passwords via MQTT would be an initial step in order to be able to modify data emitted by the sensor. These consequences are explained in the following abuse case.

F. *MitM between the waste management sensor and the management platform*

The data that can be manipulated is whether the trash container is full or not, forcing a vehicle to travel to the site, when it is not necessary, wasting resources. On the other hand, the trash container could be full, and no vehicle could appear, causing the neighbors' discomfort and the proliferation of pests.

In the future, luminaires will be incorporated into one of the racks. In addition, the different abuse cases for each of the systems will be implemented, while in parallel we will analyze how to detect these attacks defensively, while analyzing the repercussions of each of the abuse cases.

Finally, these abuse cases can be used in new research on industrial cybersecurity, conferences, lectures and trainings for cybersecurity awareness in Smart Cities environments, as well as, to train new professionals in attack and defense of such facilities for ethical purposes.

V. CONCLUSIONS

The Smart City physical demonstrator represents a valuable tool for cybersecurity teams, allowing them to improve their knowledge of these Smart City environments, test in a real simulated environment, and conduct research. Thanks to this technology, attack teams can identify vulnerabilities and exploit them without the risk of causing damage to either facilities or users, giving them the opportunity to gain hands-on experience in a controlled environment.

On the other hand, defense teams can monitor the actions carried out by attack teams, which allows them to learn about

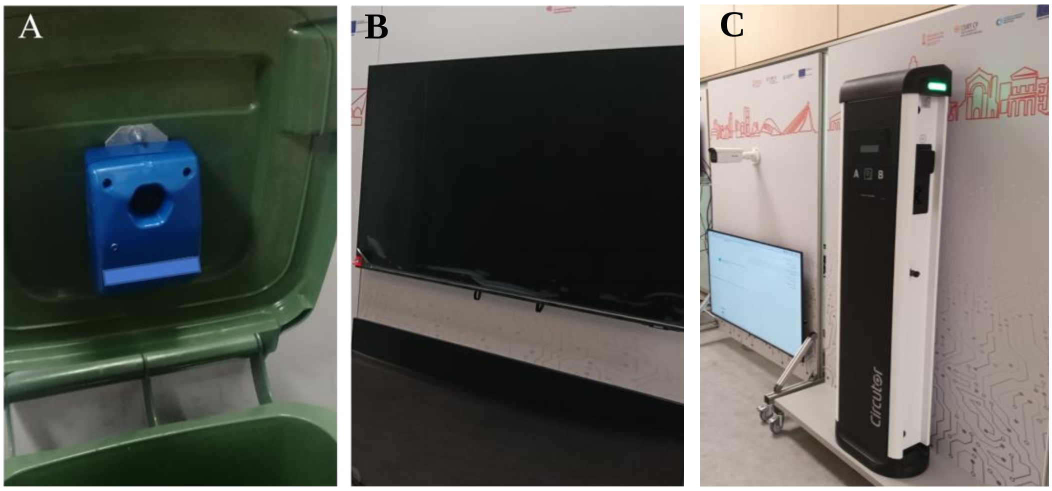

Figure 2. Representation of the SmartCity. A - Waste management system sensor. B - Display screens. C - Traffic management camera and electric vehicle charger.

existing vulnerabilities in the system and improve their protection strategies. In addition, the detected abuse cases can be used in conferences, lectures and trainings to raise community awareness about the importance of cybersecurity in Smart Cities.

In short, the Smart City physical demonstrator is presented as a fundamental tool for teaching and training new professionals in the field of Smart Cities cybersecurity. This technology allows users to learn how to defend and attack such facilities for ethical purposes, thus contributing to the construction of a safer and more secure environment.

Smart City systems are characterized by their large-scale complexity, making it impractical to acquire numerous physical devices for conducting real-scale testbeds. As a result, virtualization of these systems becomes a crucial avenue for experimentation. Furthermore, the rapid proliferation of new devices in the Smart City landscape necessitates ongoing vigilance to identify and integrate these devices into testbeds effectively.

In addition, achieving highly realistic configurations for these testbeds is a primary objective, as it allows for more accurate experimentation. However, achieving absolute fidelity to real-world configurations can prove challenging, given that each organization or municipal body may possess specific and unique configurations that deviate from the initial design parameters. This divergence can necessitate adjustments in testbed setups to accommodate these variations.

Furthermore, in addition to the incorporation of luminaires, there is a need to conduct a comprehensive analysis of the systems currently deployed within Smart Cities that hold the potential for integration into the testbed environment. This necessitates an examination of emerging attack vectors and the development of use cases for training and awareness in the field of cybersecurity.

Expanding the testbed environment is achievable through the integration of a 3D model representing a Smart City. This model facilitates the scalability of attacks across multiple devices, enabling a comprehensive evaluation of attack pathways and their real-world impact on an urban setting. Additionally, the introduction of new technologies, particularly those involving AI, holds promise for enhancing anomaly detection and countering attacks. This may also involve deploying AI-driven surveillance systems, which, it is important to note, can be vulnerable to manipulation by potential attackers, adding an additional layer of complexity to the research.

REFERENCES

[1] “SAMSAM Ransomware Suspected in Atlanta Cyberattack - Noticias de seguridad - Trend Micro ES”. https://www.trendmicro.com/vinfo/es/security/news/cybercrime-and-digital-threats/samsam-ransomware-suspected-in-atlanta-cyberattack (accessed Sep. 01, 2023).

[2] A. M. de Souza, C. A. Brennand, R. S. Yokoyama, E. A. Donato, E. R. Madeira, and L. A. Villas, “Traffic management systems: A classification, review, challenges, and future perspectives”, *International Journal of Distributed Sensor Networks*, vol. 13, no. 4, p. 1550147716683612, Apr. 2017, doi: 10.1177/1550147716683612.

[3] B. Esmaeilian, B. Wang, K. Lewis, F. Duarte, C. Ratti and S. Behdad, “The future of waste management in smart and sustainable cities: A review and concept paper”, *Waste Management*, vol. 81, pp. 177–195, Nov. 2018, doi: 10.1016/j.wasman.2018.09.047.

[4] A. Hussain *et al.*, “Waste Management and Prediction of Air Pollutants Using IoT and Machine Learning Approach”, *Energies*, vol. 13, no. 15, Art. no. 15, Jan. 2020, doi: 10.3390/en13153930.

[5] M. S. Mastoi *et al.*, “An in-depth analysis of electric vehicle charging station infrastructure, policy implications, and future trends”, *Energy Reports*, vol. 8, pp. 11504–11529, Nov. 2022, doi: 10.1016/j.egyr.2022.09.011.

[6] A. Khaksari, G. Tsaousoglou, P. Makris, K. Steriotis, N. Efthymiopoulos, and E. Varvarigos, “Sizing of electric vehicle charging stations with smart charging capabilities and quality of service requirements”, *Sustainable Cities and Society*, vol. 70, p. 102872, Jul. 2021, doi: 10.1016/j.scs.2021.102872.

[7] B. P. Rimal, C. Kong, B. Poudel, Y. Wang, and P. Shahi, “Smart Electric Vehicle Charging in the Era of Internet of Vehicles, Emerging Trends, and Open Issues”, *Energies*, vol. 15, no. 5, Art. no. 5, Jan. 2022, doi: 10.3390/en15051908.

[8] R. Vrabič, J. A. Erkoyuncu, P. Butala, and R. Roy, “Digital twins: Understanding the added value of integrated models for through-life engineering services”, Procedia Manufacturing, vol. 16, pp. 139–146, 2018, doi: 10.1016/j.promfg.2018.10.167.

[9] L. Deren, Y. Wenbo, and S. Zhenfeng, “Smart city based on digital twins”, Comput.Urban Sci., vol. 1, no. 1, p. 4, Dec. 2021, doi: 10.1007/s43762-021-00005-y

[10] G. White, A. Zink, L. Codecá, and S. Clarke, “A digital twin smart city for citizen feedback”, Cities, vol. 110, p. 103064, Mar. 2021, doi: 10.1016/j.cities.2020.103064.

[11] M. Jafari, A. Kavousi-Fard, T. Chen, and M. Karimi, “A Review on Digital Twin Technology in Smart Grid, Transportation System and Smart City: Challenges and Future”, IEEE Access, vol. 11, pp. 17471–17484, 2023, doi: 10.1109/ACCESS.2023.3241588.

[12] H. Xia, Z. Liu, M. Efremochkina, X. Liu, and C. Lin, “Study on city digital twin technologies for sustainable smart city design: A review and bibliometric analysis of geographic information system and building information modeling integration”, Sustainable Cities and Society, vol. 84, p. 104009, Sep. 2022, doi: 10.1016/j.scs.2022.104009.

[13] M. Zaman, N. Puryear, N. Zohrabi, and S. Abdelwahed, “Development of the OpenCyberCity Testbed: Smart City Research Innovation and Opportunities”, in Proceedings of the ACM/IEEE 14th International Conference on Cyber-Physical Systems (with CPS-IoT Week 2023), San Antonio TX USA: ACM, May 2023, pp. 233–234. doi: 10.1145/3576841.3589612.

[14] R. Sell, R.-M. Soe, R. Wang, and A. Rassõlkin, “Autonomous Vehicle Shuttle in Smart City Testbed”, in Intelligent System Solutions for Auto Mobility and Beyond, C. Zachäus and G. Meyer, Eds., in Lecture Notes in Mobility. , Cham: Springer International Publishing, 2021, pp. 143–157. doi: 10.1007/978-3-030-65871-7_11.

[15] L. Sanchez *et al.*, “SmartSantander: IoT experimentation over a smart city testbed”, Computer Networks, vol. 61, pp. 217–238, Mar. 2014, doi: 10.1016/j.bjp.2013.12.020.

[16] V. Garcia-Font, C. Garrigues, and H. Rifà-Pous, “Attack Classification Schema for Smart City WSNs”, Sensors, vol. 17, no. 4, p. 771, Apr. 2017, doi: 10.3390/s17040771

[17] A. A. Elsaeidy, A. Jamalipour, and K. S. Munasinghe, “A Hybrid Deep Learning Approach for Replay and DDoS Attack Detection in a Smart City”, IEEE Access, vol. 9, pp. 154864–154875, 2021, doi: 10.1109/ACCESS.2021.3128701.

[18] M. Alamer and M. A. Almaiah, “Cybersecurity in Smart City: A Systematic Mapping Study”, in 2021 International Conference on Information Technology (ICIT), Amman, Jordan: IEEE, Jul. 2021, pp. 719–724. doi: 10.1109/ICIT52682.2021.9491123.

[19] M. Kalinin, V. Krundyshev, and P. Zegzhda, “Cybersecurity Risk Assessment in Smart City Infrastructures”, Machines, vol. 9, no. 4, p. 78, Apr. 2021, doi: 10.3390/machines9040078.

[20] C. Ma, “Smart city and cyber-security; technologies used, leading challenges and future recommendations”, Energy Reports, vol. 7, pp. 7999–8012, Nov. 2021, doi: 10.1016/j.egyr.2021.08.124.

[21] Md. M. Rashid *et al.*, “Adversarial training for deep learning-based cyberattack detection in IoT-based smart city applications”, Computers & Security, vol. 120, p. 102783, Sep. 2022, doi: 10.1016/j.cose.2022.102783.