Towards a Secured City:

The Contribution of the Smart City Physical Demonstrator in Threat

Marina Galiano[1,2]**,** Elvira Lara[2], Eduardo Ortega[2]

[1] *CSIRT-CV, Valencia (Spain)*
[2] *S2 Grupo (Spain)*
Contact email: csirtcv @gva.es

November 2023

- Master's degree in Biomedical engineering by UPV (Valencia, Spain)
- CSIRT-CV, Industrial Cybersecurity (Valencia, Spain)

What is CSIRT-CV?

ICT Security Centre of the Comunitat Valenciana, dependent on Generalitat Valenciana.

CSIRT-CV offers services within the Comunitat Valenciana (Alicante, Castellón and Valencia), with a non-profit public service vocation, so its services are offered free of charge.

Excellence Center of Industrial Cybersecurity

- Industrial Laboratory

  - Honeynet

  - Medical Image Unit

  - **SmartCity**

- Reducing consumption of resources
- Improving efficiency of management of services
- Improving quality of life
- Reducing pollution
- Safer cities and more livable

- **Internet of Things (IoT)**
  - Precise and instantaneous measurement
  - Make decisions based on highly accurate data

- Rapid transition to smart cities
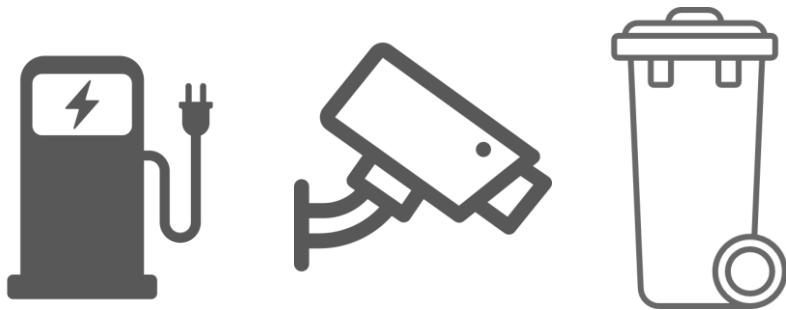- Rapid adoption without regard to the cybersecurity

**Cyberattack on Kansas town affects email, phone, payment systems**

- Need of understanding of the implicit risks
- Prepare to respond
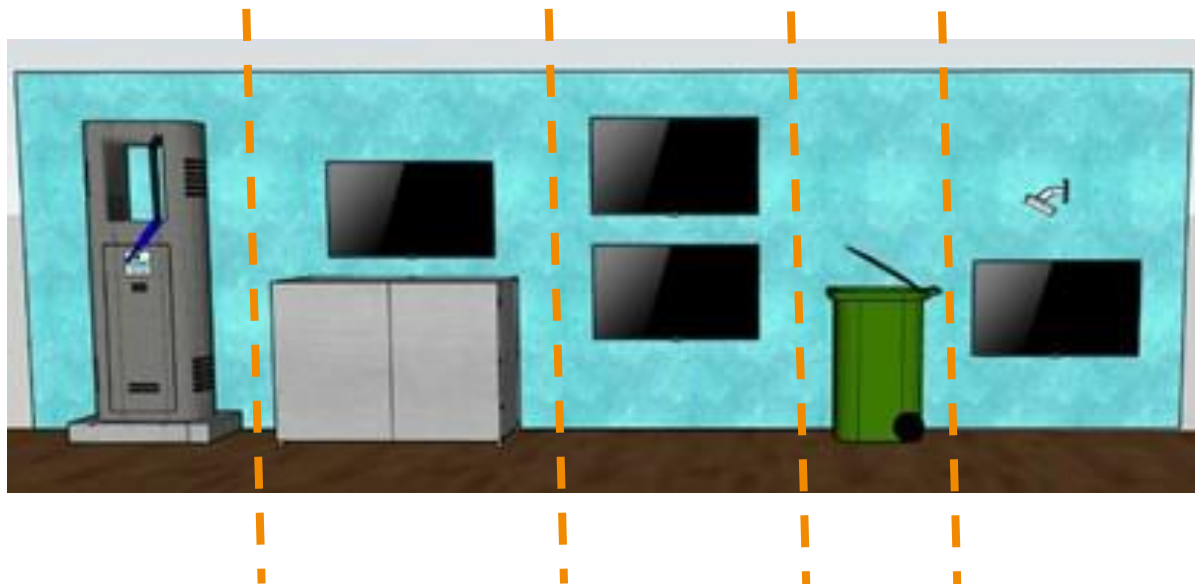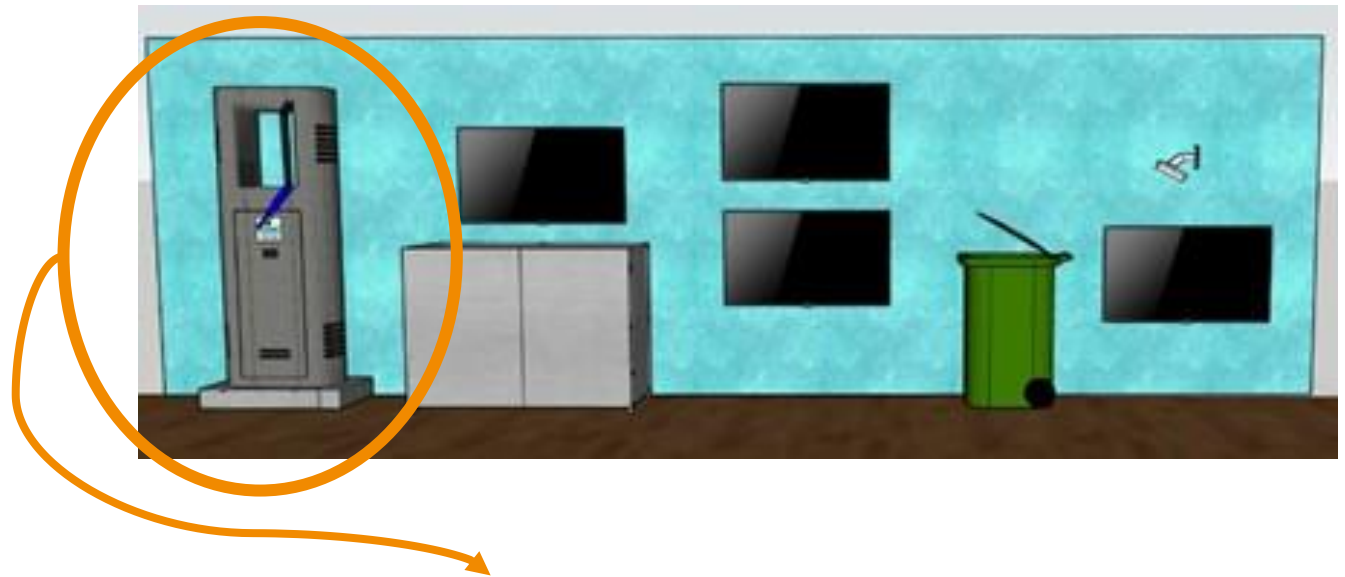- Securitization specialized

Objectives

- **Hybrid testbed: real systems & simulated**
- **Represent a Smart City**
  - conducting cybersecurity tests
  - observe the impacts of cyberattacks
  - raising awareness
  - investigate and analyze in depth the systems and threats
  - generate measures to reduce impact
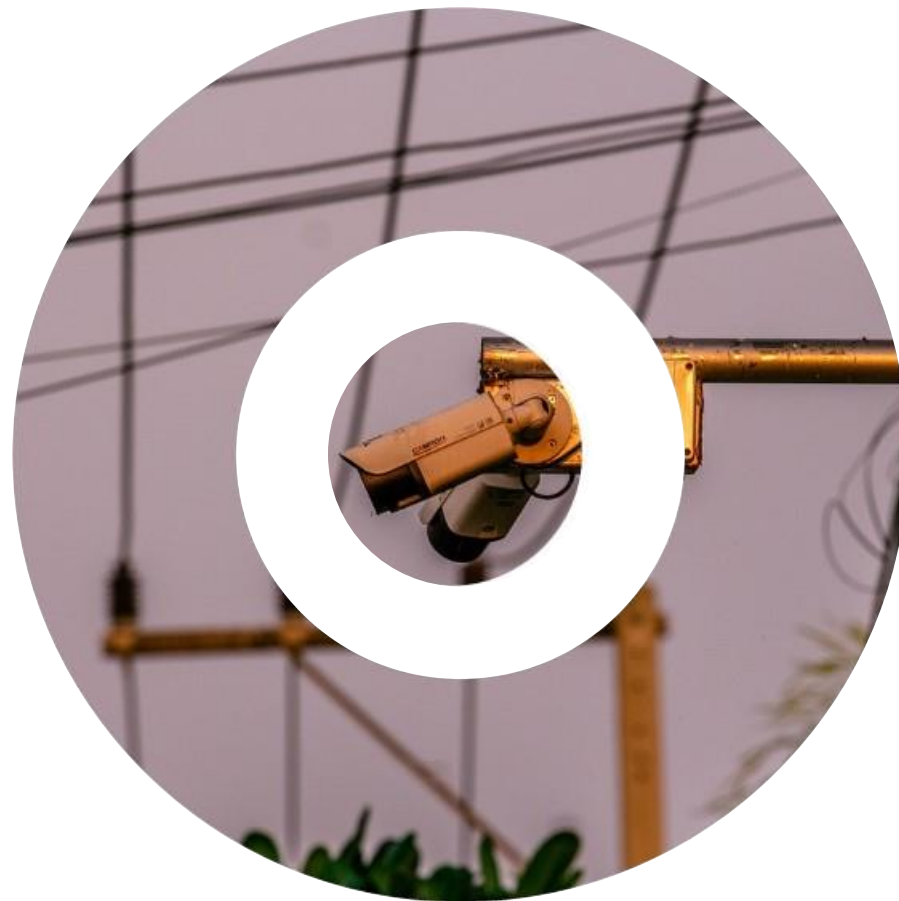
Ransomware attack on the charging infrastructure

- **Power down** the charger's sockets.
- Disable the charger and ask for a ransom
- It will be shown that an attempt is made to enable the charger, but it automatically reverts to the disabled state.

MitM in the charging system

- Show the customer that his vehicle is **charging when it is not**.
- Blue light indicating "charging" status will illuminate but the charging socket will actually be powered down.

Obtaining credentials from the waste management sensor

Method of **extracting authentication credentials** through tools against the MQTT protocol.

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.
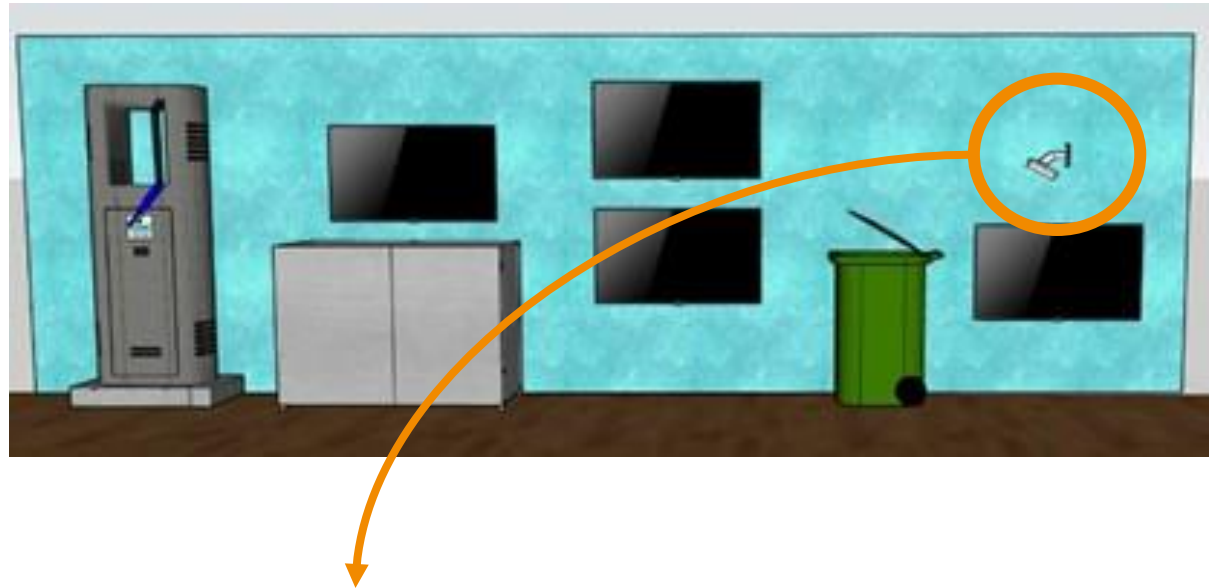
Obtaining camera credentials

Obtain the **camera's credentials** via Web cookie or via brute force by performing an attack on its sending protocol (RTSP).

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.

Ransomware attack & MitM on the charging infrastructure

- Removing the availability of charging devices
- Create significant logistical problem in the city
- Undermining the mobility capacity
- Complaints from the population
- Saturate certain citizen services
- Technical staff will not be able to cover the repair of lots of devices

Obtaining credentials & MitM from the waste management sensor and management platform

- Trash container is full or not
- Forcing a vehicle to travel to the site, when it is not necessary
- Wasting resources
- Pollution
- Trash container could be full, and no vehicle could appear
- Neighbors' discomfort
- Proliferation of pests

Obtaining camera credentials & attack on camera access token

- Having access to modify the credentials

- Restrict workers' access to them

- Power down the cameras

- Force technicians to go in person camera by camera to reset them

- Altering camera visual settings

- Workers or the camera cannot analyze the data correctly

- AI algorithms would include errors

- The Smart City physical demonstrator represents a **valuable tool** for cybersecurity teams.

- Improve **knowledge** of these Smart City environments.

- Test in a **real simulated environment** and conduct research.

- **Attack teams** can identify vulnerabilities and exploit them without the risk of causing damage to either facilities or users, gaining hands-on experience in a controlled environment.

- **Defense teams** can monitor the actions carried out by attack teams, learning about existing vulnerabilities in the system and improve their protection strategies.

- The detected abuse cases can be used in **conferences, lectures and trainings** to raise community awareness about the importance of cybersecurity in Smart Cities.

- Smart City systems are characterized by their large-scale complexity, making it impractical to acquire numerous physical devices for conducting real-scale testbeds → **need of virtualization**.

- Absolute fidelity to real-world configurations can prove **challenging**, given that each organization may have specific and **unique configurations.**

GENERALITAT VALENCIANA
Conselleria d'Hisenda, Economia i Administració Pública

CSIRT-CV
Centre Seguretat TIC de la Comunitat Valenciana

IARIA

- Incorporation of **luminaires**.

- Examination of **emerging attack vectors** and the development of use cases for training and awareness in the field of cybersecurity.

- Integration of a **3D model** representing a Smart City.

- Comprehensive evaluation of attack pathways and their real-world **impact** on an urban setting.

- Introduction of new technologies, particularly those involving **artificial intelligence (AI),** anomaly detection and countering attacks.

- This may also involve deploying **AI-driven monitoring systems**.

Thank you!
Questions?

CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana

C/ Ramiro de Maeztu Nº9 46022 Valencia, España
Teléfono: +34-96-398-5300 Email: csirtcv@gva.es

www.csirtcv.es | csirtcv@gva.es
www.csirtcv.gva.es | www.concientat.gva.es
Facebook.com/csirtcv | X.com/csirtcv

IARIA