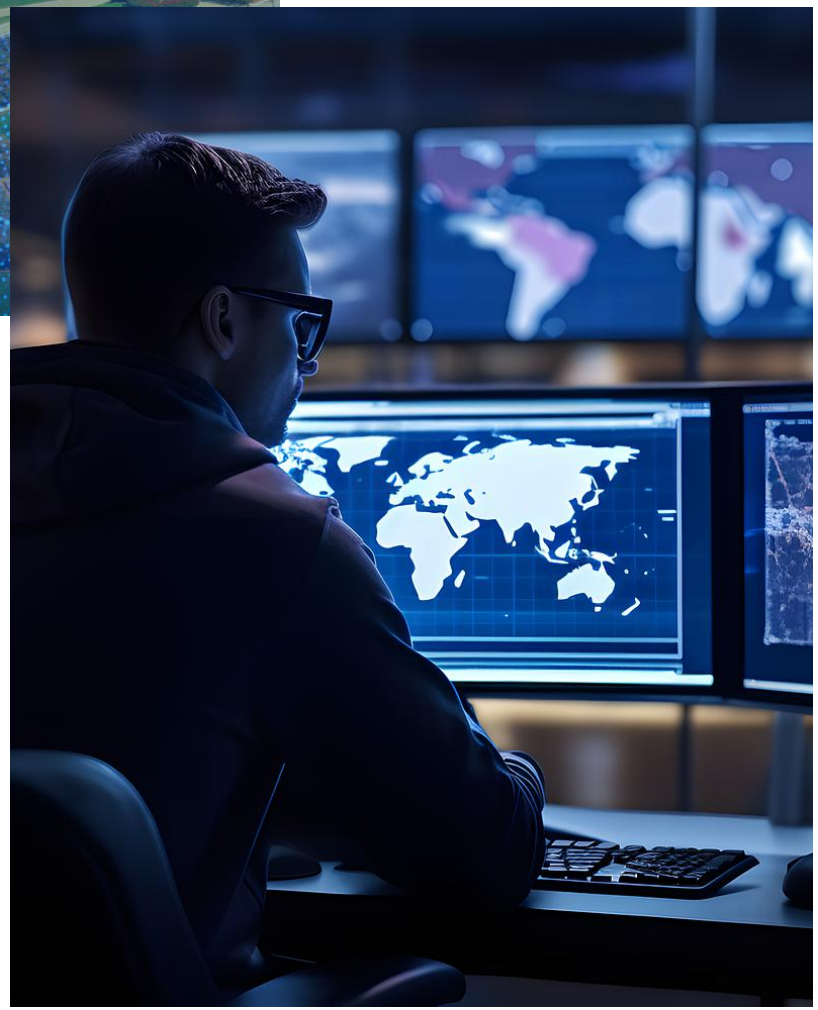
Capital Digital
MADRID

LABORATORIO DE INTELIGENCIA DE CIUDAD (COLABORACIÓN AYUNTAMIENTO-UNIVERSIDAD): CIBERSEGURIDAD

Collaboration between the Madrid City Council Cybersecurity Center (CCMAD) and research groups from the Technical University of Madrid (UPM): GB2S, RSTI

SMARTCITY EXPO WORLD CONGRESS

POLITÉCNICA UNIVERSIDAD POLITÉCNICA DE MADRID · GB2S · UPM RSTI · CMAD Centro de Ciberseguridad Ayuntamiento de Madrid



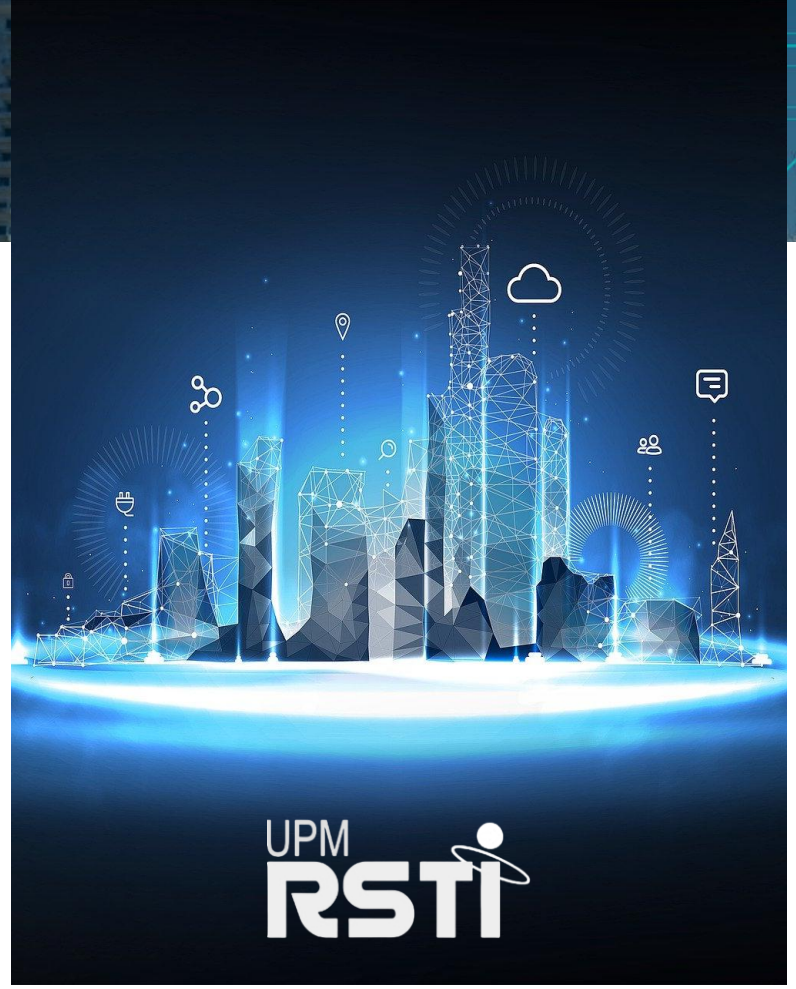
GLOBAL FOCUS

Address cybersecurity threats at each IoT layer of a Smart City

Determine the threat landscape in smart city services from their design to deployment.

Theoretical analysis and experimental validation of SUSs

Provide a theoretical framework and a testing and monitoring plan for Smart Urban Spaces (SUSs).



RSTI: RESEARCH GROUP ON TELECOMMUNICATION AND INTERNET NETWORKS AND SERVICES

Affiliation

- Department of Telematic Systems Engineering (DIT)
- Technical University School of Telecommunication Engineering (ETSIT)
- Polytechnic University of Madrid (UPM)

Projects

DESIRE6G, 6Green, SPEDIA, EUCINF, SPIDER 5G CYBER RANGE, Across, SecBluRed Ciberseguridad en el IoT Industrial

Interests

- Internet of Things
  - Sensor networks
  - Communication protocols
  - Smart Cities, mobility, transportation, etc.
- Advanced Wireless communication technologies
  - 5G/6G network cores
  - Traffic generation
  - Programmable data planes
- Cybersecurity
  - Dynamic risk management
  - Application of AI to Cybersecurity
  - Intrusion detection and response

GB2S: BIOMETRICS, BIOSIGNALS, SECURITY, AND SMART MOBILITY GROUP

Affiliation

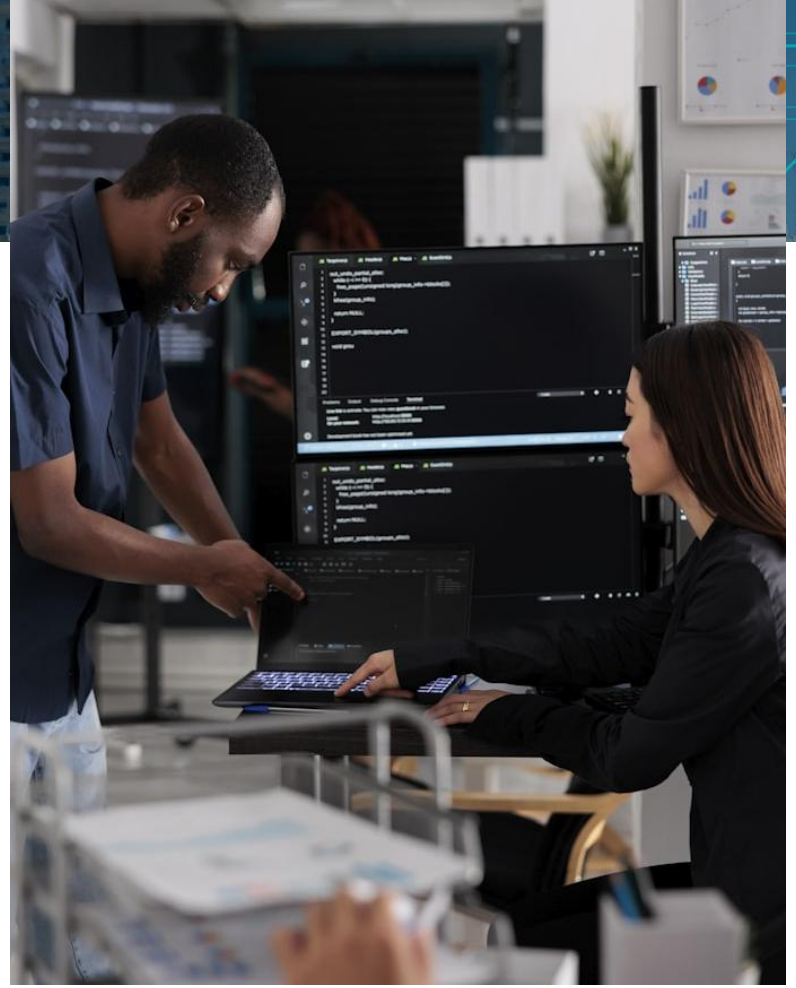
- Department of Applied Mathematics to Information and Communication Technologies (DMAT)
- Technical University School of Telecommunication Engineering (ETSIT)
- CeDInt-UPM Research Center
- Polytechnic University of Madrid (UPM)

Projects

- National and international, with numerous solutions developed, some patented and commercialized.

Interests

- Security and Cryptobiometrics
  - Classical symmetric and asymmetric cryptography
  - Post-quantum cryptography
  - Cryptanalysis
  - Cryptography in IoT
  - Cryptography in Blockchain
- Biometrics
  - Hand, iris, fase, veins ECG, typing patterns, airborne signatura, etc.
- Biosignals
  - EDA, ECG, EEG, PPG, stress, abnormal patient states, etc.
- Smart Mobility
  - Learning algorithms, AI, urban transportation and mobility, etc.



CYBERSECURITY GROUPS

LabCiber IoT

Cryptography (primitives, schemes, protocols)

Secure identification

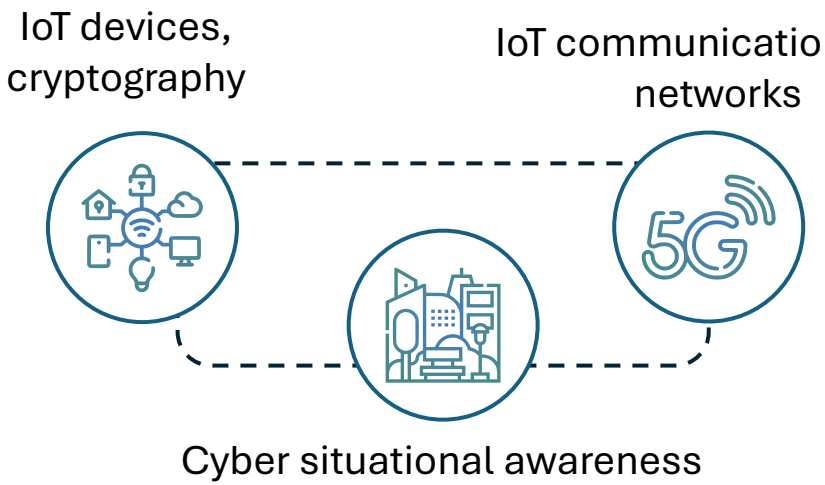
Cryptographic IoT Sensors and Devices

LabCiber 5G

Cybersecurity applied to IoT devices, protocols, and communications

Cybersecurity in advanced wireless networks (IoT, 5G)

Cyber situational awareness



REFERENCE CHECKLIST

Reference guide

The checklist is a document that serves as a high-level guide to determine the main security features and requirements that must be met in an IoT environment associated with a EUI.

It includes technical and strategic security requirements.

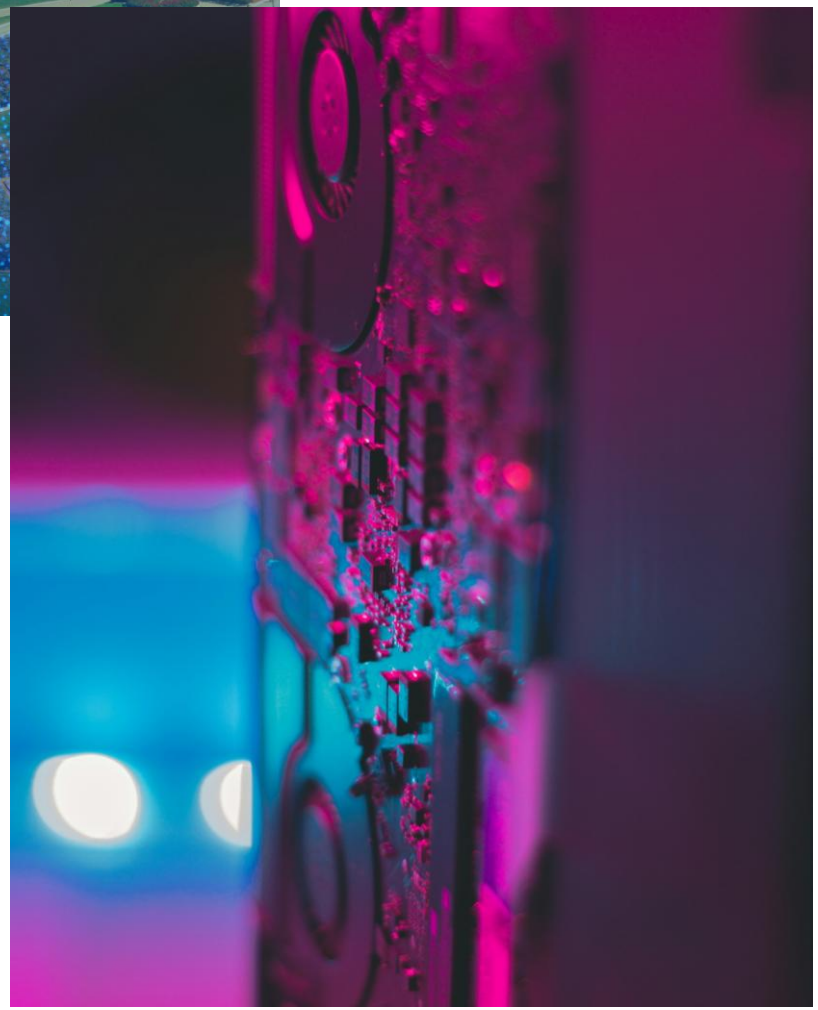
References

It is based on standards and recommendations such as the OWASP IoT Security Testing Guide, IoT Device Security Specification (CSA), the IoT Security Specification of the Open Connectivity Foundation (OCF), and ENISA Good Practices for IoT and Smart Infrastructures, among other documents.

Checklist usage

It serves as a basis for analyzing and testing the security of IoT proposals, designs, and deployments in urban environments.

It is kept up to date and continuously expanded according to the requirements and actions being implemented in the city.



SECURITY AND COMPATIBILITY ANALYSIS

Analysis of device security and their communications

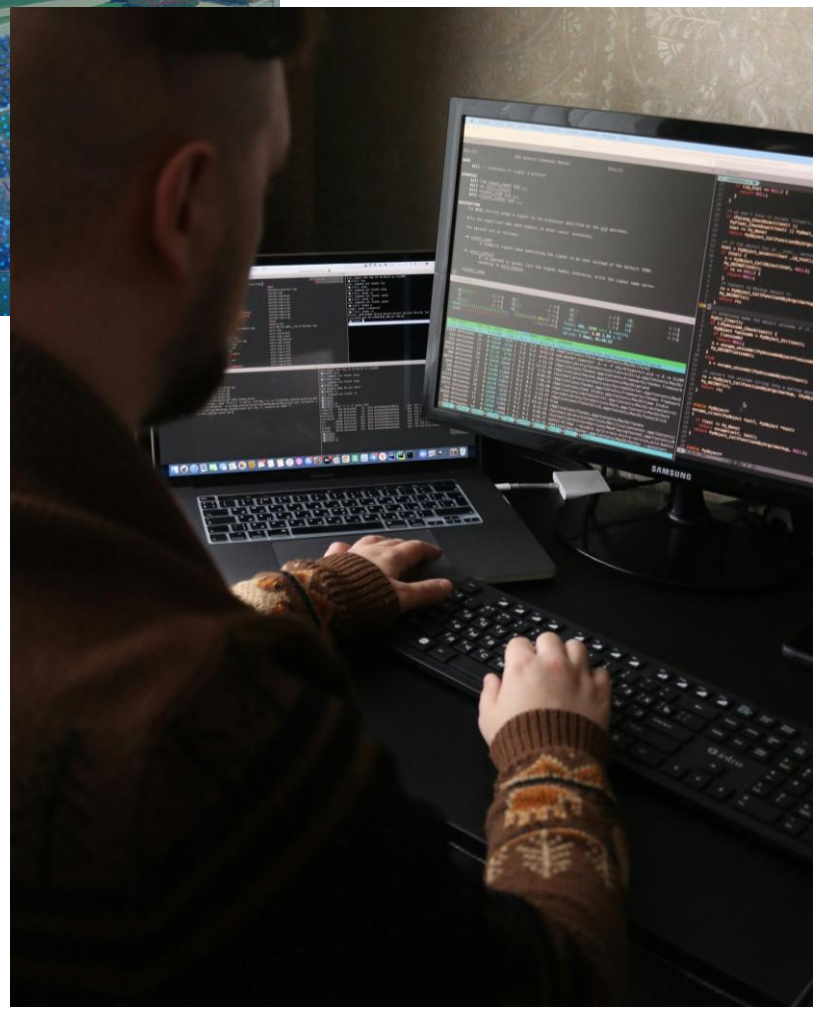
Study of the devices to be deployed/deployed..

Analysis of communication protocols.

Compatibility Analysis and Recommendations

Review of device information regarding cryptographic aspects and compatibility with recommendations, standards, and legislation.

Preparation of recommendations based on the analyses carried out.



SECURITY TEST DESIGN

Security testing plan

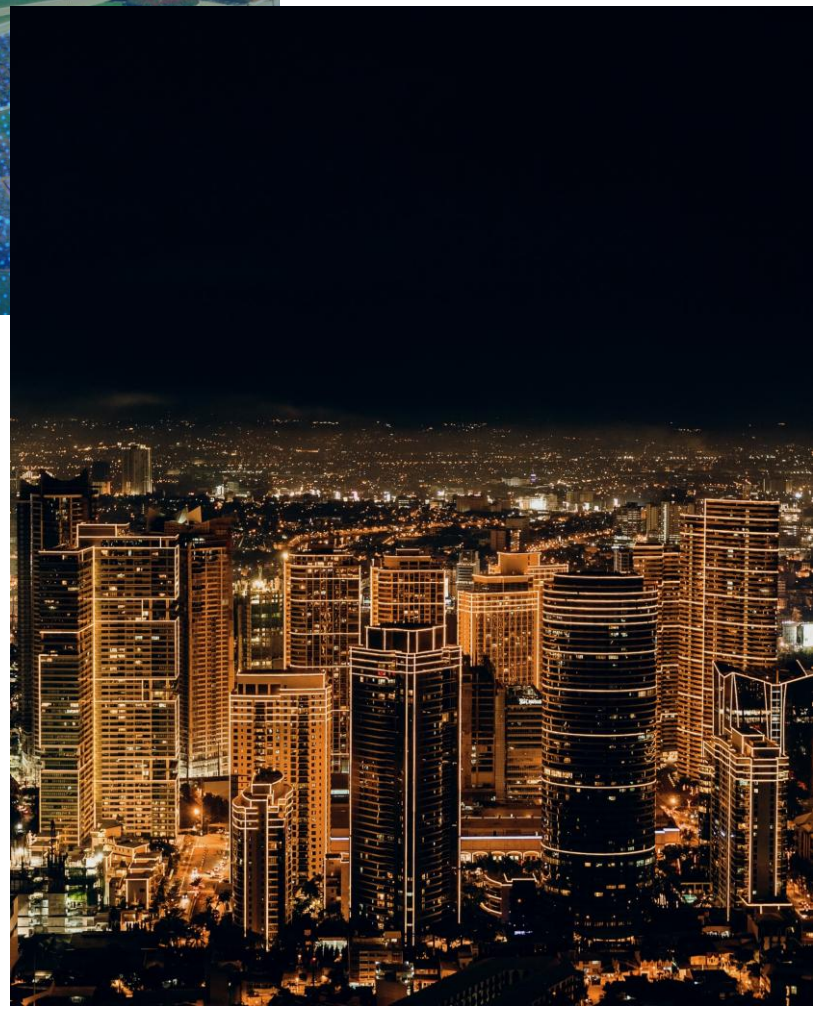
Based on the analysis work, development of a continuous security testing plan

Preparation of cryptographic black-box and white-box security tests at both individual and integrated levels.

Preparation of network security tests for device communications.

Security reports

Preparation of security reports based on the testing plan, including generation of recommendations and security improvement plans.



COLLABORATION IN SUS DESIGN

Security by design

Collaboration in the design and deployment of various Smart Urban Spaces (SUSs)

.
Provision of recommendations, plans, and security monitoring

- Firmware management and updates.
- Authentication, access control, encryption, and network segmentation.
- Continuous monitoring and anomaly detection.
- Compliance with regulations, recommendations, etc.

Collaboration with companies

Collaboration with supplier and partner companies

Partial audits of devices or deployments in collaboration with companies

Participation in projects and challenges promoted by the city council.

DISSEMINATION AND EVENTS

Participation in and Promotion of Events

Dissemination of the team's activities and results under the agreement

Promotion of security awareness in smart city services.

Cybersecurity events

Collaboration in organizing hackfest/hackathon-type events to promote cybersecurity activities within the smart city services environment.