Securing Smart Cities—Protecting Critical Urban Infrastructure

Introduction

Smart cities leverage IoT devices and interconnected systems to improve urban life—optimizing traffic, utilities, and public safety. However, this digital transformation introduces new vulnerabilities. Attacks on smart city infrastructure can disrupt essential services, threaten public safety, and undermine trust in technology-driven governance.

Scenario Overview

The city of "Urbania" has deployed a smart traffic management system and connected water supply sensors. Recently, a coordinated cyberattack caused traffic gridlock and manipulated water pressure, resulting in service outages and public panic. Urbania's city council must now assess vulnerabilities and develop a robust cyber resilience plan to protect its citizens and infrastructure.

Challenge Objective:

Students are expected to:

- Identify vulnerabilities in smart city IoT deployments and critical infrastructure.
- Propose a layered defence strategy for securing urban systems.
- Recommend incident response and public communication plans for cyber disruptions.

Main Deliverable:

- A 3-minute video (max) presenting your solution, including:

1. **Vulnerability Mapping:**
    a. Map out the attack surface of Urbania's smart systems (traffic, utilities, surveillance).
    b. Identify potential entry points and cascading risks.
2. **Defence Strategy:**
    a. Suggest technical and policy controls to secure IoT devices and networks (e.g., network segmentation, device authentication, regular patching).
3. **Incident Response:**
    a. Develop a crisis response playbook for city officials, including detection, containment, recovery, and public communication. Include key messages to the public, emphasizing transparency, timeliness, and use of multiple communication channels.
4. **Resilience & Trust:**
    a. Recommend strategies for building public trust and ensuring continuity of essential services during and after a cyber incident.

5th November 12:00 CET / 16:30 IST is the deadline for you to hand in a video of max. 3min to cyberschool@hcss.nl, in which you explain your Challenge solution and proposal. This is the final submission moment and from this submission, a Challenge-winning team will be determined. More information on this will be communicated via email.

Contributor

The contributor for this challenge is **NXP Semiconductors**.

As a global leader in secure connectivity solutions for embedded applications, NXP is at the forefront of enabling the technologies that power tomorrow's smart cities.

Our solutions help safeguard critical urban infrastructure—spanning traffic management, utilities, and public safety—by embedding security at every layer of connected systems.

By presenting this challenge to students, NXP aims to inspire the next generation of innovators to address the real-world cybersecurity risks facing modern cities. We believe that resilient, secure smart city infrastructure is essential for public trust and the continuity of essential services. Through this initiative, NXP is proud to support students in developing creative, practical solutions that protect urban environments and improve quality of life for all.

Guided by our vision of "Secure Connections for a Smarter World," NXP is committed to nurturing talent and fostering innovation. We encourage participants to think boldly, collaborate across disciplines, and help shape a safer, more connected future for cities everywhere.