

Instructional Scenario

The Smart City

IoT Security Crisis



Course/Duty Area: Cybersecurity Fundamentals/Exploring Emerging Technologies and Related Security Concerns

Scenario:

The city of Techville has launched a "Smart City" initiative, deploying thousands of Internet of Things (IoT) devices, including smart traffic lights, public safety cameras, and utility meters. During a pilot phase, an attacker successfully compromised a non-essential smart thermostat in a municipal building and used it as a foothold to launch a Denial-of-Service (DoS) attack against the city's public information display system. The city government has paused the entire project and hired your team, the Emerging Tech Security Task Force, to prevent future breaches. Your task is to perform a security analysis focused on IoT vulnerabilities and create a mandatory security framework for all future smart city devices.

Big Question:

How do the unique characteristics and inherent vulnerabilities of interconnected, emerging IoT devices introduce new attack vectors, and what proactive security frameworks are required to mitigate these risks in a large-scale deployment?

Focused Questions:

- What are three specific vulnerabilities unique to IoT devices (e.g., default credentials, lack of updates, physical access) that traditional IT security may overlook?
- What is the concept of network segmentation, and how would implementing a segmented network for IoT devices have prevented the compromised smart thermostat from launching an attack against the city's public display system?
- Based on industry standards (e.g., NIST, OWASP), what are the top five mandatory security requirements (e.g., encryption, MFA, patching schedules) that must be included in the city's new security framework for all smart devices?
- How can the concept of Zero Trust be applied to a large, diverse network of IoT devices to manage and restrict access in this smart city environment?

Student Project or Outcome:

Students will create a formal Smart City IoT Security Policy and Executive Brief consisting of

- a two-page policy document outlining the mandatory security framework
- a five-slide executive presentation that explains the initial breach, the unique security risks of IoT, and justifies the proposed security framework.

Project-Based Assessment:

Grading rubric will be used to evaluate the policy's comprehensive nature and technical accuracy. Special focus will be placed on the students' ability to identify current, realistic emerging technology threats and propose industry-standard protective measures.

Teacher Resources:

- [NIST Cybersecurity Framework](#)
- [NIST Cybersecurity for IoT Program](#)

- [CSA IoT Security Controls Framework](#)
- [Virginia Cyber Range](#)
- [Cisco Networking Academy](#) (Packet Tracer for IoT network diagramming/troubleshooting)
- [Cisco Small Business Network Security Checklist](#)

Scenario submitted by Lowell Mathis, Jr., Blacksburg High School, Montgomery County Public Schools