Information Security Audit and Assurance

Course Code : [CS8.402]

Security Flaws in IOT and Smart Cities Initiatives

Team No. – 9
Ankit Mishra (2024201047)
Disha Jain (2023202002)
Lakkireddy Sai Chaitanya Reddy (2023202023)

1. Introduction

"The Internet of Things (IoT) is a network of physical objects ('things') embedded with sensors, software, and other technologies that enable them to collect and exchange data with other devices and systems over the internet."

Examples of IoT Applications:

- **Consumer IoT:** Smartwatches that monitor heart rate and detect abnormalities.
- **Industrial IoT:** Predictive maintenance sensors in manufacturing plants.
- **Public Sector IoT:** CCTV cameras that **transmit live feeds** to smart surveillance hubs.

Overview of India’s Smart Cities Mission

India's Smart Cities Mission, launched in 2015 by the Ministry of Housing and Urban Affairs, aims to develop 100 smart cities across the country. The mission focuses on leveraging technology to improve urban living standards, enhance infrastructure, and promote sustainable development.

Key Smart City Technologies & Examples:

- **Smart Traffic Management:** AI-driven traffic signals adjust based on real-time congestion data (*Example: Delhi’s Adaptive Traffic Control System*).
- **Smart Energy Grids:** Automated grids optimize electricity distribution, reducing **power outages** (*Example: Smart grid pilot in Bangalore*).
- **Digital Healthcare:** IoT-enabled **remote patient monitoring** and AI-based **predictive diagnostics** (*Example: Telemedicine platforms in Chennai*).
- **Smart Waste Management:** Sensors in waste bins optimize collection routes to improve efficiency (*Example: Indore’s IoT-based waste tracking*).

Security Flaws in IoT Systems

Common Vulnerabilities in IoT Devices

Poor vulnerability testing

- Many IoT devices are developed with a focus on functionality instead of security. So vulnerability testing critical for identifying weaknesses before deployment is often neglected or poorly executed.

Default passwords and weak authentication:

- A standard (yet dangerous) practice is for IoT devices to ship with default passwords, which users frequently neglect to change. Even if passwords are updated, they are often weak and easily compromised.

Unpatched vulnerabilities

- Too many IoT devices run unpatched vulnerabilities due to a lack of available updates or the complexity of applying patches. IoT devices often remain used for extended periods, with no updates being applied or available.

Security Flaws in IoT Systems

Outdated firmware and software:

- Once deployed, IoT devices are often left running on outdated firmware or software, which makes them vulnerable to newly discovered exploits.

Poor device management and visibility::

- IoT devices are frequently deployed outside the purview of IT departments, leading to a lack of visibility and control over them. This is another example of Shadow Iot, which complicates efforts to secure networks as IT teams struggle to manage and protect assets they're unaware of.

Legacy assets:

- Many industries rely on legacy IoT devices designed and deployed years ago. These older devices often lack the security features of more modern technology, and organizations are reluctant to move on from them due to the cost and complexity of upgrading or replacing them

Large attack surface emerges from interconnection:

- **Smart cities connect thousands of IoT devices.**Each device—sensors, cameras, lights—expands the network's vulnerability points.A single breach in one device can compromise the entire system, like a city's traffic network.

Case Studies of IoT Security Breaches

Mirai Botnet (Global, 2016):

- Hackers used default passwords to hijack IoT devices like cameras and routers.
- Created a botnet for a massive DDoS attack, disrupting internet services globally.
- Relevant to India, where smart city devices often retain factory settings.

Ring Camera Breach (USA, 2019):

- Attackers hacked Ring smart cameras using reused credentials.
- Accessed live feeds and harassed users, highlighting privacy risks.
- siimilar IoT surveillance systems in Ahmedabad or Delhi could be targets.

Implications of IoT Security Flaws in Smart Cities

1.Risks to Public Safety and Infrastructure

- **Breaches can disrupt utilities:** Hackers targeting IoT devices could shut down water,electricity systems.
  For example, tampering with smart meters in Pune might cut electricity supply.

- **Traffic systems are vulnerable:** A hacked IoT traffic network could cause gridlock or accidents.In Surat, altered signal timings might endanger commuters.

2. Economic and Operational Impacts

- **Financial losses pile up:** Repairing breaches costs millions in damages and fixes.
  A single DDoS attack on a smart grid could drain municipal budgets.

Implications of IoT Security Flaws in Smart Cities

Limited cybersecurity awareness is a gap:

- Many citizens and officials don’t grasp IoT risks.
- In smaller smart cities, users may ignore default password changes.

Resource constraints limit defenses:

- Funding for security upgrades is often tight.
- Cities like Bhubaneswar struggle to afford robust IoT protection.

Rapid rollout outpaces security:

- India’s rush to deploy IoT skips thorough testing.
- Jaipur’s smart grids might run outdated firmware due to haste.

Risk Assessment Methodology: Step-by-Step Application

1. System Characterization
Input: Bhubaneswar's smart streetlights (hardware: motion sensors; data: energy consumption logs).
Output: Boundaries (streetlight network), criticality (HIGH—30% energy savings), sensitivity (location data).
2. Threat Identification
Sources: Hackers exploiting default passwords (e.g., 2020 Airtel router flaw), natural disasters disrupting sensors.
Output: Threat statement for Delhi's traffic cameras: "Unauthorized access due to weak credentials."
3. Vulnerability Identification
Tools: OpenVAS scans detected unencrypted data in Pune's water meters.
Output: Vulnerability list: "Lack of TLS encryption in data transmission.
4. Control Analysis
Existing: Jaipur's smart grids use AES-256 encryption.
Planned: Blockchain integration for Indore's waste management audit trails.
5. Likelihood Determination
Rating: HIGH for Surat's traffic sensors (exposed to unsecured MQTT protocols).
6. Impact Analysis
Criticality: HIGH if Jaipur's grid is breached (city-wide blackout affecting 2 million residents).
7. Risk Determination
Matrix: Prioritize Mirai botnet risks to 10 million IoT streetlights nationwide.
8. Control Recommendations
Technical: Mandate MFA for all ICCCs (e.g., Hyderabad's facial recognition systems).
Operational: Train Bhubaneswar's staff to patch vulnerabilities using CERT-In guidelines.
9. Results Documentation

Case Study 1: Mirai Botnet Attack (Global, 2016 – Relevance to India)

Background

- **What Happened:**

  Mirai Botnet emerged in August 2016, targeting IoT devices like cameras, routers, and DVRs.

- **How It Worked:**

  Exploited default passwords (e.g., “admin/admin”) to hijack over 600,000 devices globally.

- **Key Attacks:**
  - September 2016: Launched a 1-terabit-per-second DDoS attack on OVH, a French hosting provider.
  - October 2016: Hit Dyn DNS, crashing internet services (e.g., Twitter, Netflix) for millions.

- **Code Release:**

  Hackers made Mirai’s source code public on GitHub in October 2016—anyone can reuse it.

- **India Relevance:**

  Surat’s traffic cameras, part of India’s Smart Cities Mission, are at risk if unsecured—could join a botnet and disrupt cities.

Risk Management Analysis

System Characterization (Surat ITMS)

- IoT devices: traffic cams, streetlights, linked to the Integrated Command and Control Centre (ICCC).
- Data: Real-time traffic feeds, logs.
- Criticality: High—system disruption impacts safety and economy.

Threat Identification

- Actors: Mirai creators and copycats.
- Method: Scanning ports, default credential brute-force, malware install, DDoS.
- India reference: CERT-In alerts (2016), GitHub code access.

Vulnerabilities

- Default passwords (e.g., admin/12345).
- Unsecured Telnet/HTTP protocols.
- Outdated firmware (unpatched).

cont.

Control Analysis

- **Current**: Weak passwords, minimal firewall.
- **Planned**: **MFA**, secure protocols (e.g., **MQTT**), firmware updates (not yet implemented).

Likelihood & Impact

- **Likelihood**: **High** – easy to exploit, widespread impact.
- **Impact**: **High** – traffic gridlock, $1M/hour loss, emergency delays.

Risk Level

- **Risk = Likelihood × Impact = High (100)**
- **Controls inadequate**—urgent mitigation needed

Business Continuity Planning (BCP)

initial Planning

- **SMC buy-in**, $300K budget, 4-month timeline.
- **Backup servers**, DDoS mitigation tools, IoT security training.

Risk & Impact Analysis

- Risk: DDoS leads to **ITMS shutdown**.
- Impact: $1M/hour loss, emergency and public safety disruption.
- RTO: 24 hrs | RPO: 1 hr.

BC Plan Design

- **Objective**: Maintain ITMS uptime post-attack.
- **Notify CERT-In** within 1 hr; activate plan if downtime > 2 hrs.
- Offsite data storage in Ahmedabad.

Implementation

- Emergency isolation of compromised devices.
- Failover to backups, MFA on restored devices.
- SLAs with vendors for patches; procure spares and DDoS tools.

cont..

Testing & Maintenance

- Annual tabletop test and biannual failover.
- IoT security training for staff (credential & botnet awareness).

Disaster Recovery

- Hot site in Ahmedabad.
- Hourly data backups.
- Encrypted communication (MQTT), MFA.
- Cyber insurance to offset downtime losses.

Conclusion:the Mirai attack highlights critical gaps in IoT security. Indian smart cities like Surat must proactively implement robust controls, continuity plans, and staff training to mitigate similar threats