Extra Reading 08

IoT – Internet of Threats Survey

1. Purpose of the Paper

The document is a **survey of real-world security vulnerabilities** discovered in commercially available IoT devices. Its goal is to:

- Provide **practical examples** of weaknesses across consumer IoT.
- Highlight **common design flaws** that attackers exploit.
- Show how poor implementation and configuration create risks.

2. Categories of IoT Vulnerabilities

2.1 Lack of Physical Hardening

IoT devices often have:

- Exposed debugging ports
- USB interfaces
- Accessible SoC pins

This enables attackers to:

- Extract firmware
- Bypass authentication mechanisms
- Access full system privilege levels

→ Many devices rely on the assumption that an attacker cannot physically access the hardware, which is often false.

2.2 Firmware Vulnerabilities

Firmware is frequently:

- Unencrypted
- Unsigned
- Stored in plain memory chips

This allows:

- Firmware dumping
- Reverse engineering
- Identification of hardcoded passwords
- Discovery of outdated libraries

The paper highlights that firmware is the **root of trust**, yet often the least protected component.

2.3 Poor Authentication

Many IoT devices use:

- **Default usernames/passwords**
- **Weak or guessable credentials**
- **Backdoor accounts**

Effects:

- Easy compromise of devices
- Large-scale botnets (e.g., Mirai-like attacks)

Even HTTPS login pages can be bypassed if the **device trusts all certificates**.

2.4 Communication Protocol Weaknesses

IoT devices rely on many insecure protocols, such as:

- Telnet
- Unencrypted HTTP
- Weak proprietary radio protocols

Common findings include:

- No encryption or integrity checks
- Replay attack vulnerabilities
- Lack of mutual authentication

2.5 Outdated and Vulnerable Components

Many IoT devices run:

- Old Linux kernels
- Obsolete libraries
- Unsupported SDK versions

Risks:

- Publicly documented CVEs remain unpatched
- Remote code execution (RCE) opportunities

3. Case Studies Highlighted

The document includes real devices and what was found in them:

3.1 Smart Cameras

Common vulnerabilities:

- Hidden UART interfaces
- Plaintext Wi-Fi credentials stored in firmware
- Weak cloud API authentication

Attackers could:

- Stream live video
- Control device remotely

3.2 Smart Home Hubs

Findings:

- Outdated OpenSSL
- Root access available via UART
- Hardcoded private keys

Impact:

- Full compromise of the smart home ecosystem
- Lateral movement within the home network

3.3 Wearables and Smart Health Devices

Issues:

- BLE connections without pairing security
- Harvestable health data
- Exposed debug logs

Impact:

- Privacy breaches of sensitive user data

4. Systemic Root Causes

4.1 "Security as an Afterthought"

Manufacturers prioritise:

- Cost
- Time-to-market

Result:

- No secure-by-design principles
- Minimal penetration testing

4.2 Lack of Standardisation

IoT lacks:

- Industry-wide secure protocols
- Mandatory update policies
- Hardware security certifications

→ This leads to inconsistent and often poor protection.

4.3 Difficulty in Updating IoT Devices

Many IoT devices:

- Cannot be updated at all
- Receive updates irregularly
- Use insecure update channels (HTTP, unsigned firmware)

This leads to:

- Long-term exposure to known exploits
- Persistently vulnerable deployments

5. Key Takeaways

- IoT devices frequently share **the same core weaknesses**, especially bad authentication and insecure firmware.
- Even large vendors release products with **trivial bypasses and exposed debug functions**.
- Lack of encryption—both in transit and at rest—is widespread.
- Attackers can easily escalate from **device compromise → cloud compromise → full ecosystem takeover**.
- Better industry standards and secure development lifecycles (SDL) are required.