Context Aware IoT Security

Lecture 6: Context Aware Security in IoT

Instructor: Mehmoona Jabeen (mehmoona.jabeen@au.edu.pk)
Course: Internet of Things Security — Spring 2025
Department: Cyber Security, Air University

Lecture Outline

- What is Context Awareness?
- Motivation
- Context Awareness in Cyber Security
- Recent Work on Context Aware Cyber Security
- Hybrid Model: Machine Learning + Context Awareness

What is Context?

> **Definition:** Any information that characterizes a situation or event.

Examples of context in a lecture:

- Speaker bio
- Topic
- Schedule & duration
- Participants
- Date & venue
- Anything describing the situation

Context Awareness

> **Definition:** A system is context-aware if it uses context to provide relevant services or information.

Features:

- Dynamically adapts to user situations
- Example:
  - A tablet auto-rotating screen or adjusting zoom
  - Smart AC adjusting temperature when user is asleep

Context Awareness Cycle

Phases of Context Handling:

1. Context Acquisition

Techniques for collecting context:

- Push & Pull methods
- Direct sensor hardware
- Middleware infrastructure
- Context servers
- Physical, virtual, logical sensors
- Manually entered, sensed, or derived

---

2. Context Modelling Techniques

Model	Description
Key-Value	Context as key-value pairs in text or binary format.
Object-Based	Uses classes and relationships (OOP).
Markup Scheme	Uses tags to store context (e.g., XML).

Model	Description
Logic-Based	Uses facts/rules; can integrate with ontologies.
Graphical	Visual relationships, e.g., UML, ORM.
Ontology-Based	Uses semantic standards (RDF, RDFS, OWL) for structured context.

3. Context Reasoning

> **Goal:** Deduce new knowledge from context.

Technique	When Used
Supervised Learning	Known outcomes, large datasets
Unsupervised	Unknown outcomes
Fuzzy Logic	Converts low-level data into high-level natural info
Ontology-Based	For knowledge-critical cases (numerical + textual)
Rules	Converts raw data into high-level context; defines events
Probabilistic Logic	When data is uncertain; combines evidence from different sources

4. Context Distribution

> **How context is delivered to consumers:**

- Query-based
- Publish/Subscribe (push updates)

Motivation for Context Awareness in IoT

- Traditional security uses **static** parameters
- IoT is **dynamic and large-scale**
- Rapid increase in **IoT-specific attacks**
- Users unaware of **attack consequences**

Context Aware Security (Definition)

> “A set of information from user and app environment relevant to security infrastructure.”
> — Mostefaoui and Brezillon

Why it matters:

- Uses context to provide **dynamic security**
- Crucial for IoT environments

Security Applications of Context Awareness

- **Access Control:** Auth differs by location (e.g., New York ≠ London)
- **Anomaly Detection:** Uses contextual info
- **Firewalls:** Behavior-aware rule adaptation

Why Context Matters in Security

> Without context:

- Can’t verify if alert is real or false
- Hard to compare or prioritize signals
- May miss relevant factors like:
  - Known false positives
  - Event frequency or source history

- Related events
- Traffic reputation (e.g., blacklists)

Real-World Attack Stats (Motivation)

- **1.5+ billion IoT attacks** in first half of 2021 (Kaspersky)
- **66 hospitals in South Africa** affected by DDoS
- **FNB South Africa** hit by malware
- **1.7 million accounts** hacked at **Nedbank**

Limitations of Existing (Non-Context) Methods

Supervised IDS in Smart Homes

> Anthi, Williams, Burnap – *IEEE IoT Journal, Oct 2019*

- **Approach:** 3-layer IDS with ML
- **Issue:** High false positives, static method
- **Future Work:** More complex attack scenarios

Limitations of ML Approaches

- Expensive labeled datasets
- Privacy limits data collection
- High variability in devices/sensors

Limitations of Semantic (Ontology) Approaches

- Domain data collection is costly
- Ontologies get complex with scale
- Reasoning becomes slow & resource-heavy

Hybrid Model: Context + ML

> Combines machine learning with ontology-based context.

- Example figures:
  - User ontology
  - UPnP device context
    (Refer to slides for visualizations)

Context Aware Security: Use Cases

Use Case 1: Ransomware (Kia Motors, Feb 2021)

- Affected systems: Mobile apps, payments, IT, dealership tools
- Malware: **DoppelPaymer**
- Cause: Likely phishing email
- Kia denied "ransomware" due to having backups
- **Contextual insight:** Email context awareness could prevent attack

---

Use Case 2: IoT Botnet (BotenaGo)

- Discovers **30 exploits** for routers/IoT devices
- Exploits target:
  - D-Link: CVE-2015-2051, etc.
  - Netgear: CVE-2016-1555, etc.
  - Realtek, Zyxel, Tenda, ZTE
- **Attack Method:** Gains access → runs remote shell → joins botnet
- **Solution:** Context-aware filtering could stop access commands

---

Conclusion

- Context Awareness enhances IoT security by adapting to real-time environmental and behavioral data.
- ML alone or Ontologies alone are not enough — hybrid models are the way forward.
- Security systems must consider dynamic, situation-based inputs to remain effective against evolving threats.
