Physical Intrusion Detection Using RFID

Trends, Technology, Problems

Benjamin Fabian

Institute of Information Systems, HU Berlin
bfabian@wiwi.hu-berlin.de
Classical Divide: Physical vs. Logical Security

- **Physical**: Fire alarm, burglar alarm systems, door locks, badges and access cards, video cameras, etc.

- **Logical**: Server logs, Router security, Firewalls, IDS / IPS, Honeypots, Network AAA services (Authentication, Authorization, Accounting), etc.
Convergence of Logical and Physical Security

- **Convergence**: Physical and logical security systems start to cooperate.

- Integration into **Enterprise Security Management** systems.

- In the field of **Intrusion Detection**, existing detection and analysis infrastructure can be upgraded to deal with physical events: **Physical Intrusion Detection (PHIDS)**.
Physical Intrusion Detection (PHIDS)

• **Monitoring access** to buildings, rooms, devices.
• **Tracking**: Detailed tracking of employees and devices in high security areas.
• **Asset management**, including verification of change requests.
• Identification and tracking of (infected) **mobile devices** inside of the company perimeter.
• **Global RFID tagging** of items could create a new quality of physical monitoring.
• Automated **detection and exact interpretation of physical objects** (e.g., cameras, weapons), unauthorized use of company property, theft.
RFID & EPC: Further Bridging the Gap

- **Electronic Product Code (EPC):** RFID Tags on objects transmit a **globally unique serial number** - via radio.
- Reading range depends on model, frequency and surroundings (absorbing materials).
RFID: The Impact of Item-level Tagging

- First pilot deployment of **item-level** RFID-tagging in logistics and shops today.
- Tagging of consumer items is expected by many business experts within the next decade - caveat: **Privacy concerns**.
- Item-level tagging could also enable **after-sale services**.
- Example home applications: "**Smart** shelves and fridges** know their inventory, enabling delivery or recommendation services."
The Future Office?
Ubiquitous Computing and Smart Buildings

• RFID is a key enabling technology for "Smart" Environments (Ambient Intelligence, Ubiquitous Computing).

• Even if other sensor technology and image recognition advances, RFID will stay simple, effective and cheap.

• Examples: Gator Tech Smart House, METRO Future Store.
PHIDS Method 1: Using RFID Readers

- RFID readers can in principle read all tags in their vicinity via radio communication. These directly collected EPCs could then be analyzed for patterns of misuse.

- Cost reduction for tag and reader infrastructures: Readers could be already in place for a primary business function.

- Placing of additional readers at critical locations, like elevators, stairs, exits could increase monitoring coverage.
PHIDS Method 2: Investigating Network Traffic

• Using RFID in an enterprise will generate huge amounts of **EPC-related network traffic** between readers, middleware, applications. This can be investigated using normal **Network IDS**.

• **EPC Network**: A global distributed information storage and retrieval system for object information and history.

• Its **lookup** service called **Object Naming Service** (ONS) will be based on **DNS**.

• The **actual data sources** are called **EPC Information Services** (EPCIS): They use **Web Services** communication (e.g., XML-RPC, SOAP).
The EPC Network

1. RFID Tag-to-Reader Communication

2. ONS Resolution (using partial EPC coded in DNS)

3. EPC-IS Access
Physical Markup Language - From Supply Chains to PHIDS Signatures?

- PHIDS signatures will need to "understand" parts of the physical topology, as well as item categories, and how they relate to corporate security policy.
- This information will already be needed for many business processes, and could be adapted to PHIDS. PHIDS could be used to audit and verify these processes.
- This information will be formulated using the Physical Markup Language (PML). PML is based on XML, created to describe RFID and sensor data, as well as object properties.
Detection and Correlation Problems

- Data Storage, Aggregation and Transfer: How to cope with anticipated **data masses** to be investigated and generated by PHIDS, e.g. in smart environments?
- Integration and correlation of **heterogeneous physical and logical security systems** will not be easy (e.g., event logging).
- **False positives**! What are the **implications** of errors, i.e., would building doors stay shut, or police be constantly alarmed?
- **False negatives**! Tag removal, radio **transmission problems** and emerging **RFID protection measures** (though corporate policy may forbid protected tags).
Backlash on Corporate Privacy: EPC Resolving

• One problem in classical intrusion analysis: Reverse DNS lookup of attacker IP addresses can inform attackers of who and when someone follows their actions.

• PHIDS using RFID (actually every EPC Network application): Resolving EPCs can create traces on networks and servers outside of the company.

• Corresponding potential profiling of item flows could constitute valuable business intelligence, and in turn increase corporate risk.
Risks for Individual Privacy

- Ubiquitous reading out of **personal assets**?
- **Tracking people**.
- **Profiling** of individuals (employees, customers, visitors).
- Creation of **global surveillance infrastructures** by linking local PHIDS (e.g., outsourcing using third party **Managed & Monitored Security Services**)?
- What **Privacy Enhancing Technologies** could be used? Protecting the tag, protecting the EPC, the collected data and preventing inferences by **data mining**?
Conclusion

• RFID, EPC Network, PML: New and systematic approach for identifying, interpreting and tracking of physical objects by IT systems.
• High demand: RFID in supply chains and asset tracking.
• PHIDS using RFID could be used as an independent audit trail of core business processes ("... are my smart objects really moving where my ERP system tells me?") and corporate security policy.
• Privacy: Where will this convergence lead us to? Are the negative effects on personal privacy controllable at all? Which PET could be implemented to reduce these threats?