RFID Tags

• Radio frequency devices that transmit information (e.g., serial numbers) to compliant readers in a contactless manner

• Classified in the literature as:
  – Passive: transmission power is derived from reader
  – Active: energy comes from on-board battery
  – Semi-passive: battery powered chips, but transmission powered by reader

• Electronic Product Code (EPC) tags
  – Main kind of low-cost tags in use on today’s RFID supply chain applications
  – Passive UHF RFID tags
  – EPCglobal inc: Main organization controlling EPC development
Sample representation of an EPC number

35 • 006A13A • 012B5F • 000034DA0

Header    Manager number    Object class    Serial number

RFID Tag
Security Problems

- Threats to and from front-end components (i.e., tags and readers)
- Privacy concerns during the receiving of information
  - Lack of authentication between readers & tags
  - Necessity of a fine grained access control for the interaction of principals
Threat Analysis Methodology

- Based on a methodology proposed by the European Telecommunications Standards Institute (ETSI)
  - Risk Factors: Likelihood of threat occurrence & Impact on user or system
  - Likelihood Assessment Factors: Motivation of attacker & Technical difficulty
  - Overall Risk Assessment: Critical, Major, Minor
EPC Inventory Protocol

- Lack of authentication between readers & tags
  - 16-bit random sequences (denoted as RN16) to acknowledge the process
- Any compatible reader can obtain the code
  - Illicit readers can impersonate legal readers
Rogue Scanning

- Powering the tag to obtain tag ID
  - The use of special hardware (e.g., highly sensitive receivers and high gain antennas) can ease the attack.

<table>
<thead>
<tr>
<th>Motivation</th>
<th>Difficulty</th>
<th>Likelihood</th>
<th>Impact</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Solvable</td>
<td>Possible</td>
<td>High</td>
<td>Critical</td>
</tr>
</tbody>
</table>
Eavesdropping Reader Channel

- Passive observation or recording of the communication
  - The distance at which an attacker can eavesdrop the signal of an EPC reader can be much longer than the operating environment of the tag.
  - Some data items (e.g., 16-bit random sequences) can be eavesdropped at long distances.

<table>
<thead>
<tr>
<th>Motivation</th>
<th>Difficulty</th>
<th>Likelihood</th>
<th>Impact</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Solvable</td>
<td>Possible</td>
<td>High</td>
<td>Critical</td>
</tr>
</tbody>
</table>
Cloning of Tags

- Using the codes eavesdropped or scanned, an attacker may successfully clone the tags.

<table>
<thead>
<tr>
<th>Motivation</th>
<th>Difficulty</th>
<th>Likelihood</th>
<th>Impact</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Moderate</td>
<td>Solvable</td>
<td>Possible</td>
<td>Medium</td>
<td>Major</td>
</tr>
</tbody>
</table>
Location Tracking

- Adversaries can distinguish any given tag by just getting the EPC.
- Correlating reader’s position, adversary can trace location of bearers.
- It can also provide useful data for fingerprinting and profiling.

<table>
<thead>
<tr>
<th>Motivation</th>
<th>Difficulty</th>
<th>Likelihood</th>
<th>Impact</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Moderate</td>
<td>Solvable</td>
<td>Possible</td>
<td>Medium</td>
<td>Major</td>
</tr>
</tbody>
</table>
Tampering of Data (1/3)

- Gen2 tags are required to be writable
- Although this feature can be protected with a 32-bit password, bypassing the protection is solvable
Tampering of Data (2/3)

- Gen2 tags are required to be writable
- Although this feature can be protected with a 32-bit password, bypassing the protection is solvable
Tampering of Data (3/3)

- Gen2 tags are required to be writable
- Although this feature can be protected with a 32-bit password, bypassing the protection is solvable

<table>
<thead>
<tr>
<th>Motivation</th>
<th>Difficulty</th>
<th>Likelihood</th>
<th>Impact</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Moderate</td>
<td>Solvable</td>
<td>Possible</td>
<td>High</td>
<td>Critical</td>
</tr>
</tbody>
</table>
Denial of Service

- Tag data destruction or interference by attacks such as (1) attacks targeting writing or self-destruction routines and (2) use of jamming or strong electromagnetic pulses.

<table>
<thead>
<tr>
<th>Motivation</th>
<th>Difficulty</th>
<th>Likelihood</th>
<th>Impact</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Moderate</td>
<td>Solvable</td>
<td>Possible</td>
<td>Medium</td>
<td>Major</td>
</tr>
</tbody>
</table>

(1) Tag write/kill command to Illicit Reader

(2) Tag jamming by Jamming device
### Evaluation of Threats (Summary)

<table>
<thead>
<tr>
<th>Threats</th>
<th>Motivation</th>
<th>Difficulty</th>
<th>Likelihood</th>
<th>Impact</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eavesdropping, Rogue Scanning</td>
<td>High</td>
<td>Solvable</td>
<td>Possible</td>
<td>High</td>
<td>Critical</td>
</tr>
<tr>
<td>Cloning of Tags, Location Tracking</td>
<td>Moderate</td>
<td>Solvable</td>
<td>Possible</td>
<td>Medium</td>
<td>Major</td>
</tr>
<tr>
<td>Tampering of Data</td>
<td>Moderate</td>
<td>Solvable</td>
<td>Possible</td>
<td>High</td>
<td>Critical</td>
</tr>
<tr>
<td>Destruction of Data, Denial of Service</td>
<td>Moderate</td>
<td>Solvable</td>
<td>Possible</td>
<td>Medium</td>
<td>Major</td>
</tr>
</tbody>
</table>
How to deal with these threats?

• Shielding or jamming the signal
  – It may work on some other RFID applications, but not on EPC setups

• Third party blockers or guardians
  – Requires the management of new components

• Use of lightweight countermeasures, such as:
  – Message Authentication Codes
  – Lock-based Access Control Schemes
  – Random Pseudonyms
  – Threshold Cryptography
  – Physically Unclonable Functions
Message Authentication Codes

- Tags & readers share a secret that allows the verification of the integrity and authenticity of exchanged messages
Lock-based Access Control Schemes

- Simplified Scheme:
  - Readers and tags share a common secret
  - When a tag receives a proof ownership of the secret (e.g., a hash of it), it locks itself
    → when interrogated, it only answers with this pseudo ID
  - Tag unlocks itself when it receives the secret
Random Pseudonyms

- Tags storing a pseudonym, or a list of pseudonyms, instead of the real object or tag identifier (i.e., EPC number)

- To handle the location tracking threat, pseudonyms must be generated at random and they must change frequently

- Authorized readers must know how to match the pseudonyms to the real tag identifiers
Threshold Cryptography

- Exploit the natural movement of tag populations on the supply chain to distribute secrets and enforce privacy

$k$ out of $n$ tags can reconstruct the secret
Physically Unclonable Functions (1/2)

- Originated from optical mechanisms for generating unique secrets in the form of physical variations

- E.g.:
Physically Unclonable Functions (2/2)

• Promising for the implementation of challenge-response protocols in low-cost EPC tags.

• Optical designs have been improved towards new schemes exploiting other physical random variations
  – Delays of wires and logic gates of integrated circuits
  – SRAM startup values as origin of randomness

• Can be used to handle the authentication threat, as well as the cloning and location tracking threats