Security and Privacy of Postal RFID Systems

Joan Melià-Seguí
Jordi Herrera-Joancomartí
Joaquín García-Alfaro

1 Universitat Oberta de Catalunya, 2 Universitat Autònoma de Barcelona

KISON Group
http://kison.uoc.edu
Index

• Introduction to EPC
• RFID in the supply chain
• RFID projects in postal environments
• RFID postal model
• Postal RFID threat context
• Suitable security measures for postal RFID
• Conclusions
Introduction to EPC

Electronic Product Code:

De facto standard for supply chain applications

Source: www.epcglobalinc.org
Introduction to EPC

- **Electronic Product Code (EPC):**
  - 10 m.
  - ID = 96 bit
  - Security:
    - Kill passwd. (32 b)
    - CRC-16
    - PRNG 16 bit
    - XOR
RFID in the supply chain

RFID in the supply chain

Open loop

RFID in the supply chain

- Open loop

- Closed loop

RFID Postal Model

- **Open-loop based projects**
  - ETRI in South Korea
  - Correos (Spanish postal company)
  - Saudí Post

- **Closed-loop based projects**
  - China Post
  - Correos (Spanish postal company)
EPC for postal?
EPC for postal?
RFID Postal Model
RFID threat context

• Wireless channel is potentially insecure.
RFID threat context

• Wireless channel is potentially insecure.
• There is not secure authentication between tag and reader.
RFID threat context

- Wireless channel is potentially insecure.
- There is not secure authentication between tag and reader.
- Confidentiality is not granted for transferred data.
RFID threat context

- Supply chain *
  - Inside the supply chain
  - Transition zone
  - Outside the supply chain

RFID threat context

• Supply chain *
  • Inside the supply chain
  • Transition zone
  • Outside the supply chain

Postal Sector

Postal RFID threat context

- RFID
- stamp

Mr. Receiver Name and Surname
Address, Postal Code, City
Country
Postal RFID threat context

Example of postal RFID application

- Sender PC
- Receiver PC
- Date sent
- Stamp value

- RFID
- stamp

Mr. Receiver Name and Surname
Address, Postal Code, City Country

Example of postal RFID application
Postal RFID threat context

Example of postal RFID application

- Sender PC
- Receiver PC
- Date sent
- Stamp value

Mr. Receiver Name and Surname
Address, Postal Code, City, Country

- RFID
- Stamp

Diagram showing the flow of a shipment from origin to destination through post offices and distribution centers.
Postal RFID threat context
Postal RFID threat context

- Non legitimate reader
- Obtaining RFID info
- Scanning

Shipping from origin
Postal RFID threat context

Spoofing

Non legitimate reader

Obtaining RFID info

scanning

SHIPMENT FROM ORIGIN
Postal RFID threat context

Non legitimate reader → tampering

- Sender PC
- Receiver PC
- Date sent
- Stamp value
Postal RFID threat context

Counterfeiting

- Non legitimate reader
- Tampering

- Sender PC
- False PC
- Impossible date
- Stamp value + $
Postal RFID threat context

Counterfeiting

Non legitimate reader → tampering

POST OFFICE 1 PICK UP → classification → wrong destination

- Sender PC
- False PC
- Impossible date
- Stamp value + $
Postal RFID threat context

- Legitimate reader
- Non legitimate reader

POST OFFICE 1
PICK UP
Postal RFID threat context

- Legitimate reader
- Scanning
- Non legitimate reader

POST OFFICE 1 PICK UP
Postal RFID threat context

- **Legitimate reader**
- **Non legitimate reader**

- **Scanning**
  - Obtaining RFID info

- **Eavesdropping**
  - POST OFFICE 1 PICK UP
Postal RFID threat context

Ch. 1 Jamming
Ch. 2 Jamming
Ch. 3 Jamming
Ch. .... Jamming

Non legitimate reader
Postal RFID threat context

Non legitimate reader

Kill ID1
Kill ID2
Kill ID3
Kill ID...

LOGISTICS
DISTRIBUTION CENTRE's
Postal RFID threat context

Non legitimate reader

DoS
Postal RFID threat context
Suitable security measures for postal RFID

- Kill (EPC)
  - Disables the tag performance permanently
- Relabeling or ciphered ID
- Shielding
- Active Jamming
- Trusted Tag Relation
- Printed Support Redundancy
- ID with MAC

Due to the postal model uniqueness, there are threats both at the beginning and the end of the postal chain.
Suitable security measures for postal RFID

- Kill (EPC)
- Relabeling or ciphered ID
- Shielding
- Active Jamming
- Trusted Tag Relation
- Printed Support Redundancy
- ID with MAC
Suitable security measures for postal RFID

Kill (EPC)
Relabeling or ciphered ID
Shielding
Active Jamming
Trusted Tag Relation
Printed Support Redundancy
ID with MAC

- A part of the ID is used to store a message authentication code

\[ ID_{96\text{bits}} = ID_{50\text{bits}} | H_k(ID_{50\text{bits}} \oplus k)_{46\text{bits}} \]

- The aim is to improve the integrity of the stored information in the tag
- Partially solves some postal RFID threats
Suitable security measures for postal RFID

<table>
<thead>
<tr>
<th>Security Measures</th>
<th>Threats in postal model</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Eavesdropping</td>
</tr>
<tr>
<td>Kill</td>
<td>-</td>
</tr>
<tr>
<td>Shielding</td>
<td>-</td>
</tr>
<tr>
<td>Active Jamming</td>
<td>-</td>
</tr>
<tr>
<td>Rewrite / ID encryption</td>
<td>X</td>
</tr>
<tr>
<td>TTR</td>
<td></td>
</tr>
<tr>
<td>PSR</td>
<td>X</td>
</tr>
</tbody>
</table>

(-) Solves specific threat, but is not applicable to a postal model.
(X) Solves the threat and is compatible with a RFID postal implementation.
Conclusions

• Definition of an EPC-RFID postal model
• Definition and classification of security and privacy known threats for the EPC-RFID postal model.
• Proposed solutions for specified threats in the EPC technology context.