RFID Privacy

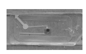
Presented by Leonid Bolotnyy

February 26, 2004 @ UVA

Squealing Euros: Privacy Protection in RFID-Enabled Banknotes

Ari Juels and Ravikanth Pappu

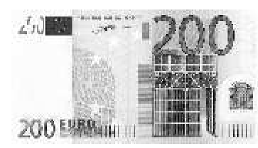
Primer on RFID



- RFID – Radio Frequency ID
  - Have small storage ~1K bits
  - Use small frequency (125KHz – 2.45GHz)
  - ID can be read over a short distance using RFID reader
  - Passive – use power supplied by the reader
  - Cheap and getting cheaper
- Consequences:
  - Infeasible to implement complicated encryption (too few bits and very little power)
  - RFID can be obtained and ID forged easily

Introduction to the problem

- In an attempt to prevent counterfeiting of money, ECB has decided to install RFID devices into high value banknotes to enable tracking of the money by 2005.
- What are some of the problems that such an action may bring?



Potential Problems

- Gathering purchasing habits of consumers without their consent
- Illegal tracking of banknotes
- Illegal tracking of people’s activities
- Illegal alteration of banknotes
- Making banknotes unusable by invalidating information recorded on the chip

Solution Goals

- Consumer privacy
  - Only police can trace banknotes
- Strong Tracing
  - Police can determine serial # (without physical contact)
- Minimal infrastructure
  - Consumers should not need anything. Merchants need very little
- Forgery resistance
  - Forger needs physical contact to forge, unable to forge unseen serial numbers
- Privilege separation
  - Banknotes should only be alterable given physical contact
- Fraud detection
  - Should be easy to detect if invalid information is recorded

Solution Approach

Need to alter the RFID tag to prevent unauthorized tracing

- Use re-encryption to change the information recorded on the RFID to evade illegal tracing.
- Re-encryption changes the appearance of the ciphertext leaving the plaintext unchanged.

Note: Current RFID devices do not support write.

Two important problems surface from the solution approach

- Need to ensure that re-encryption is performed by authorized entities at the right times
- Need to ensure that valid new information replaces the old one

Banknote Creation

S: serial number, (PK, SK): keys,
den: denomination, r: random number,
h: collision avoiding hash function

- Digital signature ∑ = Sig(SK, [S || den])
  - Used to hide serial number on the banknote
- Key D = h(∑)
  - Used to protect the information readable/writable by RFID reader
- Ciphertext C = Enc(PK, [∑ || S], r)

Solution Scheme

RF	cell γ : ciphertext	cell δ : encryption factor
	$C = \mathrm{Enc}(PK_L, [\Sigma \| S], r)$	r
	keyed write under $D = h(\Sigma)$	keyed read/write under $D = h(\Sigma)$
Optical	serial number	signature
	S	$\Sigma = \mathrm{Sig}(SK_B, [S \| den])$

Banknote Verification

- Merchant optically reads S, and ∑
- Computes D = h(∑)
- Reads RFID fields C and r using key D
- Computes C* = Enc(PK, [∑ || S], r)
- Checks if C equals C*
- Picks a new r’ and computes C’=Enc(PK, [∑ || S], r’)
- Writes C’ and r’ onto the banknote

Solution Scheme Questions

- Why do we need encryption factor r?
- Why do we need to read protect r?
- Why do we compute D = h(∑) and not D = h(S)?
- Why do we need ∑?
- Why do we need to separate RFID and optical data?

More Solution Scheme Questions

- Once an individual receives a banknote from a merchant, what should he do?
- What is the likelihood of RFID malfunction or that the note authenticity fails at one of the steps?

Are goals achieved?

- Consumer privacy
- Strong Tracing
- Minimal infrastructure
- Forgery resistance
- Privilege separation
- Fraud detection

	cell γ : ciphertext	cell δ : encryption factor
RF	$C = \mathrm{Enc}(PK_L, [\Sigma \| S], r)$	r
	keyed write under $D = h(\Sigma)$	keyed read/write under $D = h(\Sigma)$
	serial number	signature
Optical	S	$\Sigma = \mathrm{Sig}(SK_B, [S \| den])$

Possible attacks

- Many keys (D) are known. Try brute force attack (RFID properties to the rescue)
- Use RFID reader to detect presence of RFID tags to disclose the possession of money by people
- Attacker may place correct note information from some other banknote avoiding tracing
- Attacker may transmit legal ID even though he caries an illegal banknote, avoiding tracing
- Attacker may shield RFID tag to avoid detection

10 second break

Other Approaches to Protect Privacy

- The "Kill Tag"
- The Faraday Cage
- The Active Jamming
- The Regulation
- The "Smart" RFID Tag
  - The "Hash-lock"
  - The re-encryption (we just looked at it)
  - Silent Tree-Walking
    - Blocker Tags

The Regulation Approach

- Consumer should know if an item is tagged
- Consumer should be able to remove or deactivate the tag
- Consumer should have access to the tag data
- Consumer should have access to services without the tag
- Consumer should know when where and why the tag is being accessed

"Hash-lock" Approach

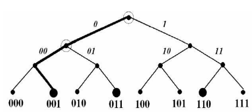
- The tag is unlocked while the store uses it for inventory tracking and is locked at the counter when a consumer purchased the item.
- Consumer unlocks the tag when s/he gets home.
- What are the problems with this approach?

Silent Tree Walking

- When a reader reads tags within its access zone, it may receive responses from several tags at once.
- To avoid collisions a Tree Walking Protocol is used.
  - A binary tree of nodes with tags at the leafs
  - A node corresponds to an id prefix with a root being empty string, left tree corresponds to n||0 and right node corresponds to n||1 where n is an id prefix of the node

Silent Tree Walking Continues

- Reader traverses the tree using DFS requesting one bit at a time pruning subtrees that are not needed.



Blocker Tag

- Blocker tag is used to simulate a number of tags. It will possibly have several antennas and will send 0 and 1 when a reader requests the next bit.
  - Reader friendly blockers
  - Privacy zones
  - Malicious Blocker Tags
    - How to deal with them?