Untraceable RFID Tags via Insubvertible Encryption

Giuseppe Ateniese, Jan Camenisch, Breno de Medeiros

Presented by Michael Lin
The RFID Future...

- EZ-Pass, gas payment, smart keys
- Pay for your groceries by walking through an RFID reader
- RFID tags will be everywhere... is this good?
The RFID Future...

- Why do we even want RFID tags on everything?
  - Inventory (warehouses, stores)
  - Product information (expiration dates, post-sale consumer updates)
  - Checking out groceries takes a long time...
RFID and Privacy

• Passive RFID tags can be read from a remarkable distance...

• If everything has an RFID tag...

• What does this imply?
The Not-Quite Privacy Problem

• How do we prevent tracking of RFID tags over a long period of time by bad guys but allow good guys to do it?

How would you like it if, for instance, one day you realized your underwear was reporting on your whereabouts?

California State Senator Debra Bowen
Protecting Privacy

• RFID tags can’t perform any operations
• How do you protect the privacy of a storage device that you assume can be read and written by anyone?
• Plain encryption doesn’t solve this problem

Cryptography is like a picket fence around your house that consists of one picket ninety miles tall - Neal Stephenson
Adding Randomness

- “Random” data
- Instead of storing an ID, store data that changes
- The trick is being able to understand the ID through changes
- Crypto people have seen this requirement somewhere before...
Mixnets

- A mixnet solves the traffic analysis problem
  - it hides who is talking to whom
- Universal re-encryption - changes ciphertext BUT it can still be decrypted with the original (private) key
- How does this relate to RFID privacy?
Mixnet => RFID
Is this really private?

• Contents of the tag change every time it’s read and an attacker can’t decrypt the message to track it

• But an attacker can store his own encrypted data and use that to track the RFID tag

• If you were clever you could say the attacker subverts the encryption
Insubvertible Encryption

- Same as universal re-encryption, except now we can tell if the data has been tampered with
- We can remove an attacker’s tracking data (note we lose the original data)
Is this really private?

- Still allows tracking by “good guys”
- Covers a pretty specific case - if no one reads your RFID tag it’s going to keep the same “random” value forever
Privacy in RFID tags is a big issue...
this doesn’t quite solve it
(but the math is really cool)