RFID Privacy: An Overview of Problems and Proposed Solutions

Simson L. Garfinkel, Ari Juels, and Ravi Pappu

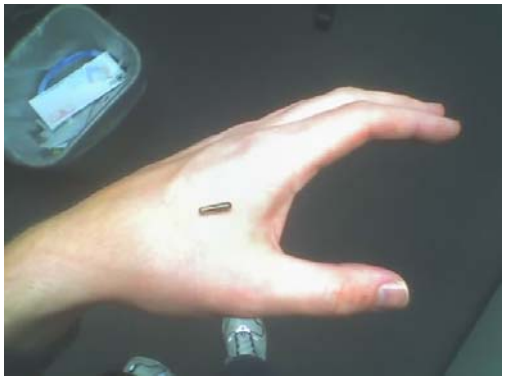
George Boulos
gwf5@pitt.edu

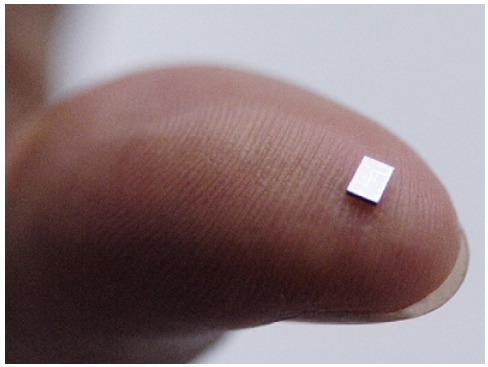
Motivation

- RFID tags has the potential for tracking consumers without their knowledge or consent. It is a great threat for user privacy.
- RFID has already been massively deployed.
- Propose solutions for safely using RFID.

RFID

- replacement for the Universal Product Code bar codes. Each RFID tag has 96-bit number that is both globally unique and unreusable.
- *RFID readers can read tags remotely. The range depends on the RFID tag design, it varies from 5 cm to 10 m.*





RFID Applications

- Automobile immobilizers
- Animal tracking
- Payment systems
  - used as creditcard-like payment tokens that contain a serial number
- Automatic toll collection
- Inventory management

RFID Potential

- Many suppliers have recently begun embedding RFID tags.
- RFID tags will be embedded in automobile tires.
- Zebra Technologies developed A print engine that can embed an RFID transponder directly into a product label.
- Hitachi has developed 0.4mm-square RFID tag called the “µchip”. Designed for photocopier papers.

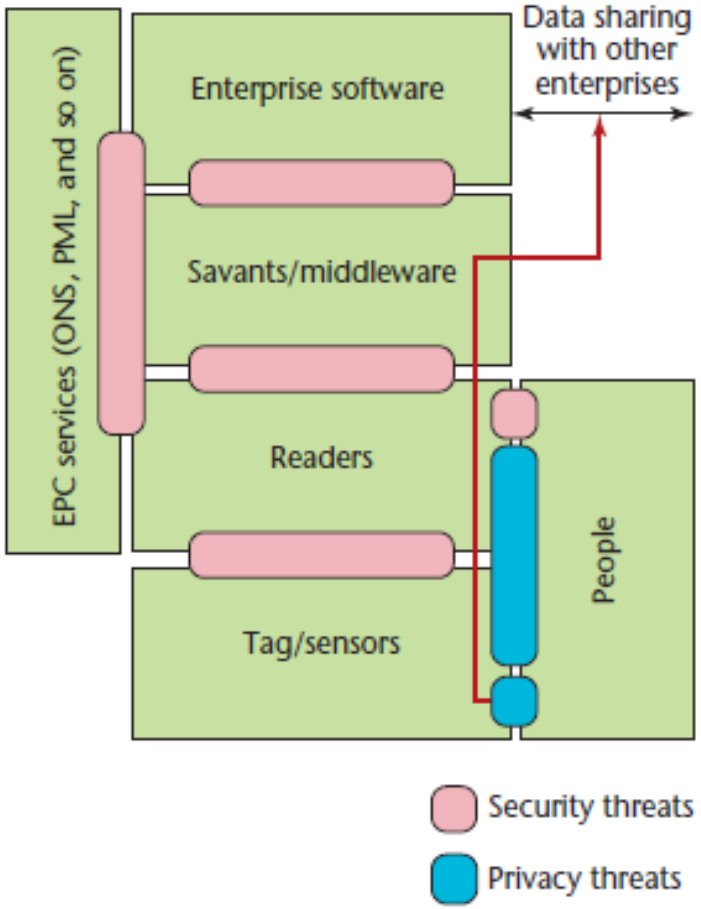
EPC RFID Tags

- Electronic Product Code, developed mainly to be simple and cheap.
- EPC is being promoted as a single, open worldwide RFID standard that will dramatically lower costs and increase adoption.
- 96 bits divided into sections identifying the tagged item’s manufacturer, product, version, and serial number.

EPC RFID Tags (Cont.)

- On avg. RPC tags contain 250 to 1,000 gates.
- No support for encryption algorithms or other traditional security features.
- tags contain a *kill (self-destruct)* feature.
- Or could be used as a pointer to a database entry for the tag that contains a detailed transactional history for the associated object.
- Universally accessible Object Name Service (ONS) database.

EPC RFID Tags (Cont.)



Corporate data security threats

- *Corporate espionage threat*
  - it easier for competitors to remotely gather supply chain data
- *Competitive marketing threat*
  - gain unauthorized access to customer preferences
- *Infrastructure threat*
  - Corporate would depend on easily jammed radio frequency signals
- *Trust perimeter threat*
  - larger volumes of data electronically

Personal privacy threats

- Action threat
  - individual's behavior (or possibly his or her intent) is inferred by monitoring the action of a group of tags.
- Association threat
  - customer's identity can be associated with the item's electronic serial number
- Location threat
  - carrying unique tags can be monitored and their location revealed

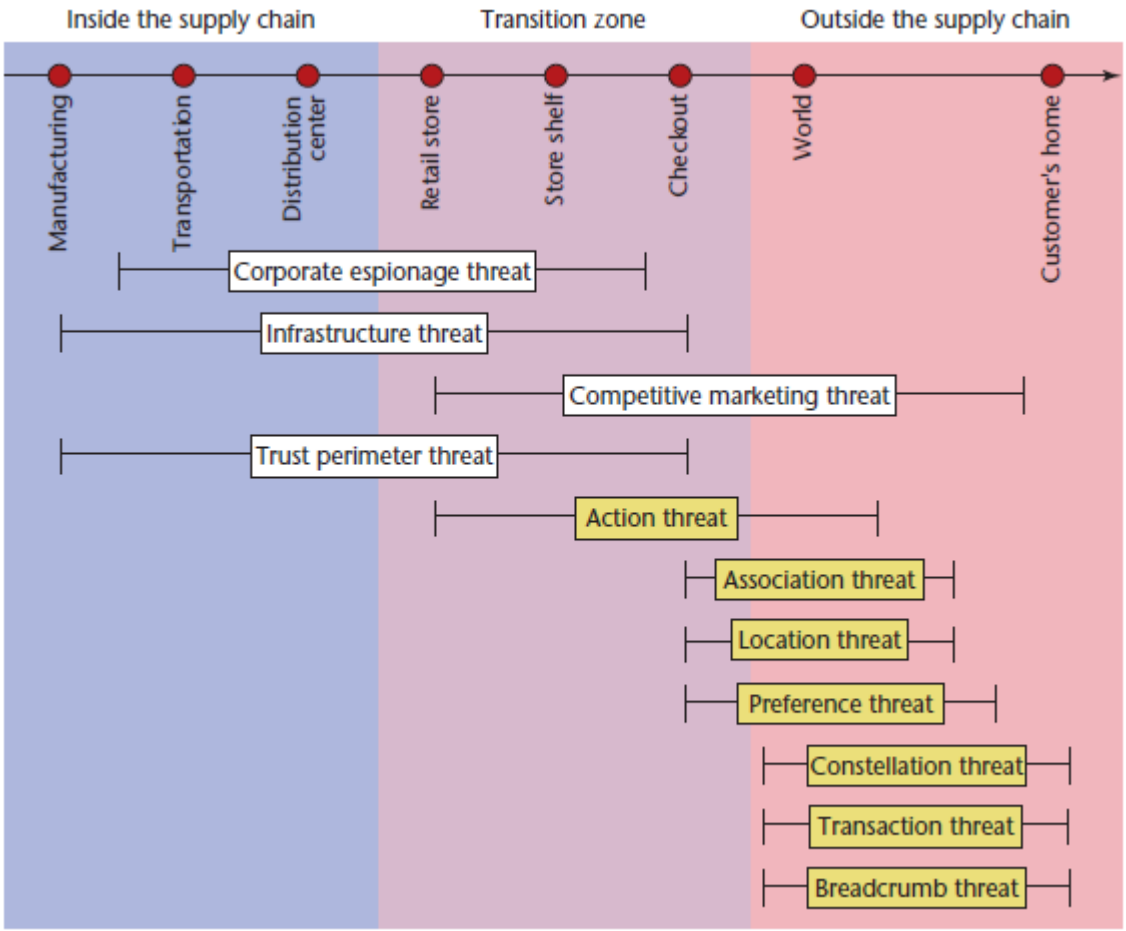
Personal privacy threats (Cont.)

- Preference threat
  - exposes customer preferences to competitive forces
- Constellation threat
  - tags form a unique RFID shadow or constellation that can be used to track people
- Transaction threat
  - tagged objects move from one constellation to another

Personal privacy threats (Cont.)

- Breadcrumb threat
  - individuals collect tagged items that are associated with them. When they discard these electronic breadcrumbs, the association between them and the items isn't broken.
- The cloning threat
  - Speedpass devices tags could be cloned, which leads to possibilities of payment fraud and new modes of automobile theft.

EPC Deployment threats



TECHNICAL SOLUTIONS

EPC Killing

- EPC tags contains self destruct feature.
- When an EPC tag successfully receives the kill command (associated with a 32 bit password), it renders itself permanently inoperable.
- Killing is not enough?
  - EPC tags has some post-sale applications
  - Other than EPC, live RFID tags are already proliferating in everyday life

Encryption

- Cheap Encryption:
  - key management problem
  - Does not solve privacy problems
- Performing onboard encryption
  - Would increase the tag cost

Tag Password

- Each tag has a password, and replies with the correct data only if the correct password is provided.
  - How to find out which password to transmit without knowing the tag id.
  - Yet this solution could be used if all tags have the same password.

Tag Pseudonym

- Each tag change his id, and has n pseudonyms.
- Whenever scanned it returns a different pseudonym.
- Unauthorized tag tracking would be more difficult, attackers could repeatedly scan the same tag, thereby forcing it to cycle through all available pseudonyms.
- tag might release a new pseudonym only every five minutes.
- The tag id must be reprogramable.

Blocker Tags

- blocker tag creates an RF environment that is hostile to RFID readers. The blocker tag is a specially configured, ancillary RFID tag that prevents unauthorized scanning of consumer items.
- Simply interrupts the communication between the reader and the RFID tag.
- For Example: Any tag with a leading 1 bit would be protected by the blocker.

Blocker Tags (Cont.)

- An adversary might well be able to design or configure a reader that sometimes defeats blocker tags.
- impolite or even malicious blockers impose a denial-of-service threat. *How?!*

Soft Blocking

- a blocker tag can confer privacy protection merely by informing a reader of its presence.
- Enforce polite reader behavior by ensuring that they always adhere to a “blocker-compliant or “polite” policy.
- Accomplish this by requiring that polite reader ***firmware*** be the commercial default, as well as using ***auditing procedures*** and ***legislative regulation***.

Soft Blocking (Cont.)

- Soft blocking is similar to the P3P.
- Relies on a carefully regulated privacy enforcement environment.
- Soft blocking would not provide protection against rogue readers.
- Soft blocking could be used with full blocking.

How?!

Antenna-energy Analysis

- Reader signal's signal-to-noise ratio decreases measurably with distance.
- RFID tag might be able to obtain a rough estimate of the querying reader's distance and change its behavior accordingly.
- Distance could be ***combined*** with traditional ***access-control techniques*** such as a challenge-response protocol.
- This approach is complementary to both blocker tags and pseudonyms.

Policy Solutions

- Simson Garfinkel has proposed the following policy.
- Users of RFID systems and purchasers of products containing RFID tags have:

Proposed Policy

1. The right to know if a product contains an RFID tag.
2. The right to have embedded RFID tags removed, deactivated, or destroyed when a product is purchased.
3. The right to first-class RFID alternatives. Consumers should not lose other rights (such as the right to return a product or travel on a particular road) if they decide to opt-out of RFID or exercise an RFID tag's kill feature.
4. The right to know what information is stored inside their RFID tags. If this information is incorrect, there must be a means to correct or amend it.
5. The right to know when, where, and why an RFID tag is being read.

Proposed Solution (Cont.)

- To comply with item 1, organizations might include a prominently displayed logo on any RFID-tagged product.
- organizations could post a sign wherever RFID readers operate (similarly an RFID readers free zone)
- readers could emit a tone or flash a light when a reading occurs.
- the tag itself could emit a tone or flash a light.
- a tag equipped with memory could count the numberof times it has been read.

Proposed Solution (Cont.)

- Most of these options would add to the tag's cost.
- We could instead develop RFID reader detectors for concerned consumers.

What do you think about this idea?

Another proposed Policy

- Consumers should be notified when items they purchase contain RFID tags.
- RFID tags should be disabled by default at the checkout counter.
- RFID tags should be placed on product packaging instead of on the product when possible.
- RFID tags should be readily visible and easily removable.

Strength and Weaknesses

- Strengths:
  - Present broad dangers and threats caused by the deployment of RFID tags.
  - Presents several solutions.
- Weaknesses:
  - In my opinion, it tries to find the perfect solution, one that is 100% threat proof, cheap and easy to deploy. It is not possible.

Q&A

Richard Stallman presenting RFID badge wrapped with a tin foil

Thank you