



RFID Tags and Privacy

Dan Bailey, RSA Laboratories

August 26, 2004



Authentication

Access Management

Encryption

Digital Signatures

Early examples of consumer backlash



- 42% of Google results on “RFID” include word “privacy”
- CASPIAN (Consumers Against Supermarket Privacy Invasion and Numbering)
 - Group discovers Metro AG’s loyalty cards contain RFID tags without consumer disclosure...<http://www.foebud.org/rfid/index-gb.html>
 - ...leading Metro AG to remove RFID tags from future loyalty cards...<http://www.in-sourced.com/article/articleview/1396/1/1/>
 - National news coverage: NY Times, Time, etc.
- Even if the consumer hysteria is based on misperception, it’s still a major problem
- Most participants in this debate adopt one of two views. Let’s review them in detail

RFID Debate Part One: RFID is Good



- Proponents of this view tend to embrace the following:
 - RFID technology provides a major benefit to supply-chain efficiency, with the potential to save billions of dollars a year
 - Only “extremists” care about RFID privacy
 - Informal surveys of general consumer populations show little acknowledgement or concern about RFID privacy
 - Only the “misinformed” care about RFID privacy
 - some fears about tracking passive tags from satellites, or guns that shoot tags into people are misguided
 - People can already be tracked to some extent by their cellphones and credit card transactions
 - Building an infrastructure to create, store, and transport kill codes is a costly expenditure with questionable ROI for business

Authentication

Access Management

Encryption

Digital Signatures

RFID Debate Part Two: RFID is Bad



- Proponents of this view tend to embrace the following:
 - RFID technology provides a major new avenue for certain interest groups (government, big business, etc.) to create “dossiers” on average citizens’ locations and affinities
 - If you come near the DNC site with a copy of Adam Smith’s *The Wealth of Nations*, are you a threat?
 - This data can be harvested at a distance, without consumer knowledge or consent
 - Established RFID toll collection (Fast Lane, EZ-Pass, etc) systems collect data which already is subpoenaed by law enforcement or litigants, especially in child-custody lawsuits
 - The potential for abuse by special interests, or rogue insiders within data-collecting organizations is well documented

RFID Debate Part Three: Can Technological Safeguards Help?



- Rather than advocating either of these positions, we'd rather discuss technological safeguards which may provide a middle ground to solve this dilemma:
- Business benefits without consumer risks
- It all starts with a bit, but first a bit about consumer RFID applications...

Authentication

Access Management

Encryption

Digital Signatures

Consumer applications are coming

- Killing/removing tags stifles development of consumer apps
- “Smart” appliances
 - Refrigerators that automatically create shopping lists
 - Closets that tell you what clothes you have available, and search the Web for advice on current styles, etc.
 - Ovens that know how to cook pre-packaged food
 - **Medicine cabinets that can assist Alzheimer’s patients**
- “Smart” products
 - Clothing, appliances, CDs, etc. tagged for easy store returns
- “Smart” paper
 - Library books
 - Business cards

What's our goal here?

- To allow supply-chain infrastructure to provide business benefits while respecting consumer privacy
- The **privacy bit** allows supply-chain infrastructure to selectively communicate with **only those tags that are still in the supply chain**
- It also allows retailers an **auditable** way to assure customers that their privacy will be protected
 - Since anyone listening to the reader can hear its Query command
 - With a special tag for this purpose, anyone can tell if a reader is abiding by a policy that prevents it from scanning private tags

How does the privacy bit work?

- A tag is originated with Privacy bit set to 0
- The tag travels normally through the supply chain
 - Supply-chain readers issue Query commands specifying (say) Passive, Public tags
 - Note that ordinary supply chain operations aren't slowed down
- At point of sale, POS terminal can set the Privacy bit to 1, as an alternative to killing the tag
- Tag will now no longer reply to Supply-chain reader Query commands

How does the privacy bit work?

- After purchase, consumer can take tags home
- RFID readers for consumer applications issue PrivateQuery commands specifying Private tags
- This creates two classes of RFID reader, with two classes of policy and consumer disclosure:
 - Supply chain readers promise not to read Private tags
 - Consumer readers say they'll read Private tags
- Two very different policy and regulatory regimes are in effect
 - Could have a reader certification and branding process to indicate which readers/middleware are for which environment

What does this allow?

- Retailers have an auditable privacy policy that's "on by default" to protect consumer privacy
- Rogue readers can be thwarted by using a Blocker Tag
 - This Blocker Tag listens for PrivateQuery commands and simply mounts a Denial of Service attack on the reader

Questions?



Dan Bailey

RFID Solutions Architect, RSA Laboratories

<http://www.rsasecurity.com/go/rfid>

dbailey at rsasecurity dot com

+1 781 515 7253

Authentication

Access Management

Encryption

Digital Signatures