Wireless ID Issues: Privacy, Efficiency and Security

Panelists

Kevin Fu
Frank Moss
Deirdre Mulligan
Charles Palmer
Sanjay Sarma
Panel Outline

- RFID introduction (Kevin Fu)
- e-Passports (Frank Moss)
- Privacy of e-Passports (Deirdre Mulligan)
- Human identification (Charles Palmer)
- Supply chain security (Sanjay Sarma)
Panel Format

- Short presentations by each panelist
- Q/A
- Final comments by each panelist
Wireless ID Issues:
Privacy, Efficiency and Security

Kevin Fu
UMass Amherst, Comp. Sci.
RFID tags in a nutshell

• Originally simple bar code replacement
• Now are mini, low-power computers
• Applications
  • E-commerce
  • Public transportation
  • Pharmaceutical anti-counterfeiting
  • Medical applications
What’s a Radio-Frequency Identification (RFID) tag?
Capabilities of basic RFID tags

- Often no tethered power
- Limited memory
- Limited computational power
- Debatable read ranges
Case Study: RFID Credit Cards
What are RFID Credit Cards?

- “No-swipe” credit card
- “fastest acceptance of new payment technology in the history of the industry.”

[VISA; As reported in the Boston Globe, August 14th 2006]
Video from ABC News not included in this PDF
Wireless ID Issues: Privacy, Efficiency and Security

Frank Moss
U.S. Dept. of State (ret.)

No slides available - see prepared remarks
Wireless ID Issues: Privacy, Efficiency and Security

Deirdre Mulligan
UC Berkeley, School of Law
Embedded RFID and Everyday Things: A Case Study of the Security & Privacy Risks of the e-Passport

Jennifer King
Marci Meingast
Deirdre Mulligan
University of California, Berkeley
An Interdisciplinary Approach

• Prof. Deirdre K. Mulligan - Director of the Samuelson Law, Technology, & Public Policy Clinic, Boalt School of Law

• Marci Meingast - Ph.D student, Dept. of Electrical Engineering & Computer Science

• Jennifer King - Information Scientist & Research Specialist, Samuelson Clinic
Talk Outline

• Traditional and new uses of RFID
• Privacy and security threats posed
• The e-Passport Case Study
  • Timeline
  • Issues posed by adoption process
• Recommendations for future embedded RFID implementations affecting the public
Terminology

- **RFID**: “Any technology that transmits specific identifying numbers using radio.” [Garfinkel ‘05]

- **Ubiquitous computing**: “Making many computers available throughout the physical environment, but making them effectively invisible to the user.” [Weiser ‘93]
Evolving Uses of RFID

• **Past:** livestock tagging, inventory management

• **Present:** proximity cards, library books, government issued ID, limited consumer products (Nike+iPod, car keys)

• **Future:** clothing, paper clips, money . . . ?
Concerns with evolution in RF applications

- **Ubiquity** - when the product is a payment card, ID card, etc., object is carried through public places
- **Data** - static, can be linked to individuals
- **User awareness** - user may not realize the object contains a transponder
- **Signaling** - object may not notify the user when data is read
Threats to Privacy

• Loss of control over personal data
  • Leak data without knowledge
  • Others can access your data without consent

• Context is important
  • What you wish to reveal about yourself is situationally dependent
  • Place (home vs. public place) matters
The e-Passport: A Case Study

- Result of the Enhanced Border Security and Visa Entry Reform Act of 2002
  - US chose to adopt the ICAO’s directive 9303
- First issued to the public Dec. ‘06
- Contains an ISO14443 compliant contactless smart card chip with 64K memory
Original Specifications

• Chip stores all data contained on identification page:
  • Name
  • Nationality
  • Gender
  • Date & place of birth
  • Issuing country & date
  • Expiration date
  • Passport number & type
  • JPEG of passport photo
• Data digitally signed but not encrypted
• No anti-skimming or eavesdropping countermeasures
ISO 14443

- Chips are 14443A or B compliant when they conform to:
  - Standardized physical architecture
  - Radio frequency power and signal interface (13.56mhz)
  - Initialization, anti-collision, and transmission protocols
- Passive chip, powered by reader
- Standard does not explicitly address:
  - Chip or reader OS (proprietary to each vendor)
  - Read range (generally assumed to be a max of 4cm/10in)
Security Vulnerabilities of Original Passport Design

• Eavesdropping
  • Intercept communications between the reader & the passport

• Skimming
  • Surreptitiously read data from the passport (esp. in public areas)

• These methods can be used to:
  • Identify passport holders (by name or nationality)
  • Hotlist/track individuals
  • Clone (done successfully by Lukas Grunwald in 2006)
US Dept. of State’s Initial Stance

• Passport data did not require protection because:
  • Identical to data currently printed on passport
  • Security measures cause longer read times
  • Encryption requires global coordination

• Overlooks fundamental change to passport
  • Document --> “technological artifact”
Changes to the e-Passport

- Late 2004 – incorporated anti-skimming material into outside cover of the passport
- Spring 2005 – commissioned NIST to conduct skimming vulnerability tests (results still not released)
- April 2005 – State admits passports can be read at one meter (3 feet) or more
- October 2005 – announces the adoption of Basic Access Control.

Changes driven by:

- Response to requests for comments by public:
  - 2,335 comments were received by the State Department:
    - 98.5 percent were negative
    - most focused on security and privacy concerns
- Negative press highlighting the lack of privacy protections in the original design
Problems with Process

- Privacy Impact Assessment failed to assess privacy concerns of passport holders
- Rule Making & Comment - conducted, but late in process, and info provided to public was minimal, lack of support
- No focus on needs of passport holders
- Lack of expert analysis and scientific assessment
  - No outside or expert assessments
  - No independent testing
Recommendations

- **If** RFID is an appropriate choice:
  - Employ user-centric design to ensure users’ security & privacy needs are met
  - Err on side of privacy: protect user data
  - Give users control - opt-outs should be possible, provide feedback, allow user to choose when transponder is activated
  - Engage with the public
  - Establish trust - develop policy guidelines outlining how data is collected and managed
Wireless ID Issues:
Privacy, Efficiency and Security

Charles Palmer
IBM Research
People can track RFID’s, but RFID’s can’t (reliably) track people
“The Use of RFID for Human Identity Verification” *

The Dec 2006 report from DHS’s Data Privacy & Integrity advisory committee provided advice on

- how to decide if RFID is a good choice to identify and/or verify the presence of an individual, and

- best practices on the use of RFID in such situations when they are selected or required by law.

Like most new technologies, RFID brings good news ... 

- Potential for better accuracy, speed, & efficiency
- Improved forgery prevention and tamper resistance
- Easier recovery of lost ID’s and detection of their fraudulent use
... and bad news

- Unauthorized access to data on the RFID or to the data when in transit to/from the reader
- Data gathered for one purpose might be reused for another
- Potential for surveillance of RFID-bearing individuals
Will children be playing RFID-Tag in the Future?
The real issue with using RFID for identity verification

RFID in a credential merely identifies the credential, not the individual bearing it.

Thus, RFID alone is insufficient to reliably verify identity.
Case Study: The Border Challenge

For non-citizens entering a country, the government want to know ...

- Who’s coming across, where are they going, and when do they plan to leave, and then
- When did they leave and where?
- All without impeding commerce
In 2005, 366,984 buses and trucks crossed the border into the US at Blaine, WA, or about 1000/day, not including private vehicles or cars.

Operating 24x7x365, this means 85 seconds per vehicle...

Adding a few seconds per vehicle could exceed 24 hours/day.
How RFID might help

- Each person entering the country is given an I-94 card with a unique RFID chip in it.
- On entry, the I94 # is stored with collected ID information (e.g., fingerprints).
- On exit, a simple scan of the I94 would bring up the record, including any new info since entry into the US. This could be done without exiting the vehicle.
- “Prepositioning” of this data is also a safety improvement for the border guards.
DHS began a pilot test at several US borders

They tried really hard to address privacy concerns

“... no personal information will be included on the RFID tag, and the serial number on the tag cannot be changed. Additionally, personal information is only processed within DHS databases and RFID technology tags are tamper-proof and difficult to counterfeit, with security features to prevent the misuse of information ...”

The problem here was that RFID wasn’t the right choice for the problem
Tracking the credential just isn’t the same

To speed up the exit process, all of the RFID-enabled I94’s in the vehicle would be read while the vehicle is moving (slowly).

If no reason to stop them came up, the vehicle would proceed without stopping.

*All* of the I94’s in the vehicle would be marked as having exited the US.
Who really left the country?

But there were some serious problems

- The RFID-enabled I94 could be read whether or not it was with the corresponding person

- Reading all the I94’s in a vehicle proved unreliable, and readers in different lanes read I94’s from vehicles in other lanes.

The pilot program was deemed “a failure”
RFID is good for tracking things that don’t mind being tracked.

For people, it seems RFID is only reliable when they gain a real benefit, or when it is combined with a second form of identity verification.

Otherwise, you can never be sure what you’re tracking.
Wireless ID Issues:
Privacy, Efficiency and Security

Sanjay Sarma
MIT, Mechanical Eng.

No slides available
Wireless ID Issues:
Privacy, Efficiency and Security

Question/Answer
Final Remarks

Wireless ID Issues: Privacy, Efficiency and Security