

# 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
- Benefits: document security, "improved port of entry performance"



# 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



► The contactless chip can be integrated into either the cover page or the data page.



# 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)



# Usability Issues with the Original Passport Design

- No user feedback – user has no idea when or by whom the chip was accessed
- Lack of agency (AG)
  - “I didn’t mean to engage the system.”
  - “I wasn’t aware of the system.”
  - “I don’t want to use the system.”
- Lack of boundedness/boundaries



# 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.



# Motivations for change

- 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
    - Samuelson Clinic submitted comments on behalf of eight computer scientists and engineers
  - 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
- No focus on needs of passport holders
- Lack of expert analysis and scientific assessment
  - No outside or expert assessments
  - No independent testing
  - No security testing until public outcry



# 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

