


**ETH**  
 Eidgenössische Technische Hochschule Zürich  
 Swiss Federal Institute of Technology Zürich

## RFID and Privacy

Marc Langheinrich  
 Institute for Pervasive Computing

www.vs.inf.ethz.ch



**ETH**  
 Eidgenössische Technische Hochschule Zürich  
 Swiss Federal Institute of Technology Zürich

## No Shortage of Public Fears





Dr. Katherine Albrecht  
 C.A.S.P.I.A.N. Founder

- „The risk [RFID] poses to humanity is on a par with nuclear weapons.”
  - Katherine Albrecht, C.A.S.P.I.A.N. as quoted in Larry Downes: "Don't fear new bar codes", USA Today, Sep. 25, 2003
- “Up until now, no one thought [RFID] could themselves be infected with **computer viruses**. Now researchers have discovered that computer viruses in animals, supermarket products, airline baggage and other physical objects are a **real threat**.”
  - Financial Facts Online commenting on Rieback, Crispo, and Tannenbaum: "Is Your Cat Infected With a Computer Virus", Proc. of Percom 2006

**ETH**  
 Eidgenössische Technische Hochschule Zürich  
 Swiss Federal Institute of Technology Zürich

## RFID: Essentially just a wireless license plate

(Ari Juels, RSA Labs)



- Reader scans for tags in vicinity
- Tag that enters reader-range replies (maybe)
- Reader is pretty much „blind“
  - If tag does not reply, reader does not know about it
  - Tags typically „promiscuous“ (reply to any reader)
  - Can be coupled with secondary channel
    - e.g., optical reader (e-passport)

**ETH**  
 Eidgenössische Technische Hochschule Zürich  
 Swiss Federal Institute of Technology Zürich

## RFID Application Areas

- Alerting** => Denial of Service
  - Paid/Not paid privacy relevant
- Identification** => **Sniffing**
  - „Barcodes on steroids“ (more data, faster to process)
- Monitoring** => **Tracking**
  - Automation makes tracking feasible (i.e., much easier!)
- Authentication** => **Forgery**
  - E-Passport, Car Immobilizer, Credit Cards, ...

**ETH**  
 Eidgenössische Technische Hochschule Zürich  
 Swiss Federal Institute of Technology Zürich

## Silencing

- Tin Foil**
  - Prevents tag activation
  - Effective, cheap




DIFRWEAR: RFID Passport Sleeve

- Only for small stuff!

**ETH**  
 Eidgenössische Technische Hochschule Zürich  
 Swiss Federal Institute of Technology Zürich

## Killing

- Kill-Command**
  - Part of EPCGlobal/AutoID standard
  - Software lock that renders tags silent

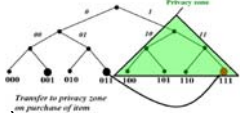


Metro RFID De-Activator

- Prevents future use!
- Requires encryption to prevent DoS

**ETH**  
 Eidgenössische Technische Hochschule Zürich  
 Swiss Federal Institute of Technology Zürich


## Hiding



- **Blocker tag** (Juels, Rivest, Szydlo, 2003)
  - Simulates all possible tag IDs (trillions!)
  - Cheap, effective (implementable on simple RFID tag)
- **Requires tree-walking protocol**
- **Requires configuration**
  - only my personal tags should be hidden (otherwise DoS on lawful RFID systems, e.g., checkout systems)
  - to prevent misuse (e.g., hiding supermarket items for theft) this must be password controlled

**ETH**  
 Eidgenössische Technische Hochschule Zürich  
 Swiss Federal Institute of Technology Zürich

## Protecting



RFID Guardian  
 (Rieback, Crispo, Tanenbaum, 2005)

- **Guardian** (Rieback et al.) **or**  
**Enhancer Proxy** (Juels et al.)
  - Monitors reader communication and selectively jams tag replies as needed
- **Works only with deterministic protocols (ISO 15693)**
- **Cannot suppress tag replies entirely, only jam**
- **Cannot suppress reader commands**

**ETH**  
 Eidgenössische Technische Hochschule Zürich  
 Swiss Federal Institute of Technology Zürich

## Encryption

- „The Siren Song of Encryption“ (Juels, 2007)
- **Powerful stuff**
  - „Secured“ tags could talk only to „authorized“ readers
  - would only disclose the „right“ information to the „right“ recipients
- **Lots of proposals, very active field of research**
  - G. Avoine's Web Page: <http://lasecwww.epfl.ch/~gavoine/rfid/>
- **The Solution?!**


**ETH**  
 Eidgenössische Technische Hochschule Zürich  
 Swiss Federal Institute of Technology Zürich

## Achilles Heel: Key Exchange

- **Reader must know password**
  - Unless only one password (which is bad), reader needs to know which tag it is ☹
  - => Reader must „try“ hundreds of passwords!
- **How does the reader know about the password?**
  - Needs to be fed into reader system
  - From where? When?
- **Consumer Use vs. Controlled Environments**
  - Chewing gum vs. Car immobilizer

**ETH**  
 Eidgenössische Technische Hochschule Zürich  
 Swiss Federal Institute of Technology Zürich


## Usage Scenario



September 29, 2007 11

**ETH**  
 Eidgenössische Technische Hochschule Zürich  
 Swiss Federal Institute of Technology Zürich

## Usage Scenario



**Does Your Solution Work Here?**

September 29, 2007 12

**ETH**  
 Eidgenössische Technische Hochschule Zürich  
 Swiss Federal Institute of Technology Zürich

## Keyless Encryption

- **Delay, not Deny!**
- **Juels „Minimalist Crypto“**
  - Simply store a few dozens (random) IDs per tag
  - Disclose one ID at a time, e.g., every 30 seconds
- **Effective against sniffing and tracking**
  - Only owner knows ID->item resolution (no sniffing)
  - ID changes often (hard to track, big gaps)
- **Effectiveness drops sharply with more items**

September 29, 2007 14

**ETH**  
 Eidgenössische Technische Hochschule Zürich  
 Swiss Federal Institute of Technology Zürich

## Shamir Tags

### An Example for Zero-Management Privacy Protection

September 29, 2007 14

**ETH**  
 Eidgenössische Technische Hochschule Zürich  
 Swiss Federal Institute of Technology Zürich

## Shamir Tags

### An Example for Zero-Management Privacy Protection

- **Unknown Tags Take Long Time To Read Out**
  - Bitwise release, short range (e.g., one random bit/sec)
  - Intermediate results meaningless, since encrypted
  - Decryption requires all bits being read
  - Complicates Tracking & Unauthorized Identification

September 29, 2007 15

**ETH**  
 Eidgenössische Technische Hochschule Zürich  
 Swiss Federal Institute of Technology Zürich

## Shamir Tags

### An Example for Zero-Management Privacy Protection

- **Unknown Tags Take Long Time To Read Out**
  - Bitwise release, short range (e.g., one random bit/sec)
  - Intermediate results meaningless, since encrypted
  - Decryption requires all bits being read
  - Complicates Tracking & Unauthorized Identification
- **Known Tags Can be Directly Identified**
  - Initial partial release of bits enough for identification from a limit set of known tags
  - Allows owner to use tags without apparent restrictions

September 29, 2007 16

**ETH**  
 Eidgenössische Technische Hochschule Zürich  
 Swiss Federal Institute of Technology Zürich

## Secret Shares (Shamir 1979)

$p(x) = s + a_1x + a_2x^2$

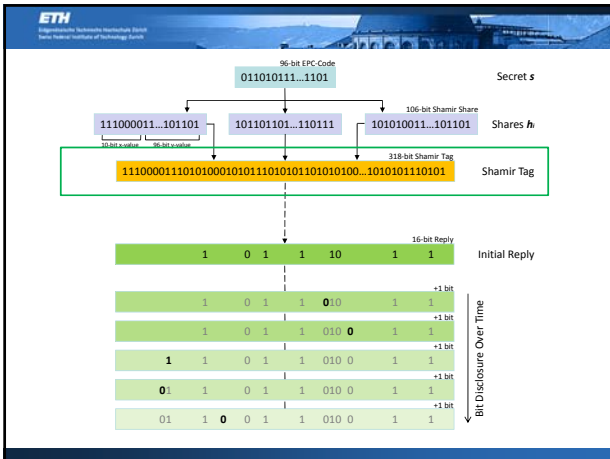
September 29, 2007 17

**ETH**  
 Eidgenössische Technische Hochschule Zürich  
 Swiss Federal Institute of Technology Zürich

## Secret Shares (Shamir 1979)

$p(x) = s + a_1x + a_2x^2$

September 29, 2007 18



### More Privacy Through Less Security?

- **Shamir Tags Require No Consumer Effort**
  - Delay upon first use, but ownership transfer trivial
  - Not useful for „important“ items (passports, authenticity, ...), this still requires strong crypto
  - Not able to alleviate customer concerns (when in doubt, better to remove/clip tag)

### More Privacy Through Less Security?

- **Shamir Tags Require No Consumer Effort**
  - Delay upon first use, but ownership transfer trivial
  - Not useful for „important“ items (passports, authenticity, ...), this still requires strong crypto
  - Not able to alleviate customer concerns (when in doubt, better to remove/clip tag)
- **Building Block for Comprehensive Solution**
  - Strong crypto for passports, drug-authenticity, ...
  - Clipping/killing for concerned consumers
  - Unconcerned consumers get at least basic protection

### Policy!

- **Transparency protocols** (Floerkemeier et al., 2004)
  - Reader queries include detailed P3P-like privacy policy
- **RFID Bill of Rights** (Garfinkel, 2002)
  - Demands industry transparency & control guidelines
- **EU Directive 95/46/EC**
  - „Data-protection law also applies to RFID“  
Resolution on radio frequency identification. 25th International Conference of Data Protection and Privacy Commissioners (2003)

### Summary

- **Simple principle, complex implications**
  - Core problem: Access Control!
- **Still much potential for security research**
  - Resource-constrained security algorithms
- **Encryption is NOT the panacea for RFID privacy!**
  - Key exchange problem often not considered!
- **Usable Security!**
  - Keyless Protocols, Policy, Physical Restrictions