

Privacy in a Networked World

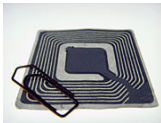
Instructor: Antonio R. Nicolosi

`nicolosi@cs.stevens.edu`



What's RFID?

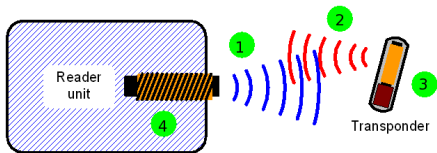
- Radio Frequency IDentification
- Tags



- Readers



How Does RFID Work?



1. Reader beams EM energy (& optional data)
2. Tag's antenna converts the EM wave into power
3. Tag's chip retrieves ID from its memory
4. Tag's antenna beams back reply to the reader
5. Reader receives answer/ID

Where Can RFID be Used?

Application Areas

- Identification
- Authentication

Sample Usages

- Supply-chain tracking (“barcodes on steroids”)
- Retail anti-theft system, libraries
- Toll payment & Mass transit
- E-Passport, Keyless car entry, TPMS, *etc.*

What Can Go Wrong?

Privacy Issues

- Remote tag activation
- Covert/stealthy tag activation

Security Issues

- “There’s no security, so there are no issues”
- Mostly proprietary schemes
 - Recently broken: *Mifare Classic*

Privacy Countermeasures

- Silencing (*Faraday cage*)
 - Wrapping tag with tin foil prevents activation
- Killing
 - Software lock to render tag silent
 - DoS?

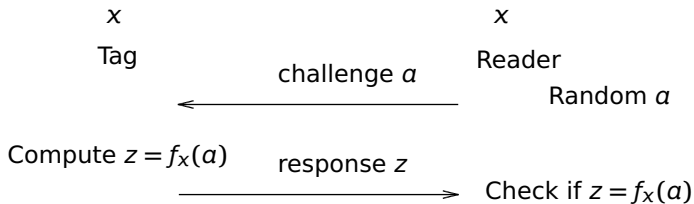
Can Crypto Help?

- Of course ;-)
But how?
- Main hurdles
 - “Dumb” tags (circuitry, power, memory)
 - Underspecified/unclear security/privacy goals
- Lightweight Authentication
- Lightweight Encryption

Lightweight Authentication

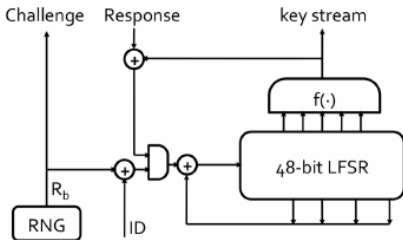
- Is it tag-to-reader authentication?
 - Payment, access control
- Or is it reader-to-tag authentication?
 - Tracking, sniffing
- Most secure “challenge-response” protocols incompatible with tags limitations

Challenge-Response Protocols



Challenge-Response Protocols (Cont'd)

- Existing systems follow “security by obscurity”



Mifare Classic's *crypto-1* [Credits: Karsten Nohl, UVa.]

Lightweight Encryption

- Tougher than authentication?

Identity Theft

 [Log in / create account](#)



WIKIPEDIA
The Free Encyclopedia

navigation

- [Main Page](#)
- [Contents](#)
- [Featured content](#)
- [Current events](#)
- [Random article](#)

interaction

article

[discussion](#)

[edit this page](#)

[history](#)

Identity theft

From Wikipedia, the free encyclopedia

Identity theft is a term used to refer to [fraud](#) that involves stealing money or getting other benefits by pretending to be someone else. The term is relatively new and is actually a misnomer, since it is not inherently possible to steal an [identity](#), only to use it. The person whose identity is used can suffer various consequences when they are held responsible for the perpetrator's actions. In many countries specific laws make the use of another person's identity for personal gain a crime.

Crimes



Classes of crime

[Infraction](#) · [Misdemeanor](#) · [Felony](#)

[Summary](#) · [Indictable](#) · [Hybrid](#)

Forms of Identity Theft

- Financial identity theft
 - Using another's identity to buy on credit, *etc.*
- Criminal identity theft
 - Posing as another upon arrest
- Identity cloning
 - Assuming another's identity in daily life
- Business/commercial identity theft
 - Using another business' name (reputation)

[Synovate ID Theft Survey]

Few Words on Terminology

Identity theft vs. Identity fraud

Identity fraud: Fraud in the 21st century

Using personal info about an individual to fraudulently create **new** fiscal entity (credit cards, loans, etc.)

+

Using said fiscal entity to acquire goods or services, passing debt back on to the victim.

Discussion

- What's so different w.r.t. classic fraud?
 - Impact on victim (limited liability/consequences)
- What's the root problem behind ID theft?
- Law focus: **Higher penalties** vs. **Victim's rights**
- Proposal: Build protections into the law
 - Burden of proof on financial institution responsible for creating the fiscal entity without proper checks

[Phishing, Spam and Id-Theft]

Misc On-Line Resources on Privacy

- Electronic Privacy Information Center
<http://www.epic.org/>
- Electronic Frontier Foundation
<http://www.eff.org/>
- Privacy Rights Clearinghouse
<http://www.privacyrights.org/>
- Center for Democracy and Technology
<http://www.cdt.org/>
- Privacy International
<http://www.privacyinternational.org/>

On-Line Privacy: Business Associations

- International Association of Privacy Professionals <http://www.privacyassociation.org>
- Privacy, Business and Law on-line newsletter <http://www.pandab.org>
- Network Advertising Initiative (self-regulation of Web Ad Businesses) <http://www.networkadvertising.org/>

Forums and Blogs

- Forum On Risks To The Public In Computers And Related Systems <http://catless.ncl.ac.uk/risks>
- Bruce Schneier's Crypto-Gram Newsletter <http://www.schneier.com/crypto-gram.html>
- Ed Felten's Freedom to Tinker <http://www.freedom-to-tinker.com/>
- Jennifer Granick's commentary on Wired <http://www.wired.com/commentary/circuitcourt>