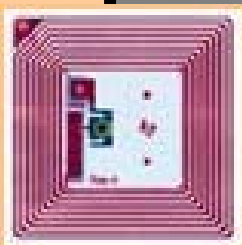




RFID Security & Privacy: Long-Term Research or Short-Term Tinkering?



The cast of characters:

- | | | |
|--------------------------|----|---|
| ▪Mike Burmester, USF | as | Academic Crypto Researcher |
| ▪Roberto Di Pietro, Rome | as | Academic Security + Applied Crypto Researcher |
| ▪Melanie Rieback, Vrije | as | Academic RFID Enthusiast and Security Researcher |
| ▪Alfred Kobsa, UCI | as | Academic Usability of Security/Privacy Researcher |
| ▪David Molnar, Berkeley | as | Academic Security + Applied Crypto Researcher |
| ▪Ari Juels, RSA | as | Industrial RFID Evangelist and Crypto Researcher |
| ▪Gene Tsudik, UCI | as | Panel Chair, “jack of all trades, master of none” |

Gee, Brain, what are we going to do tonight?

The same me thing we do every night, Pinky. Try to take over the world
(with the help of RFID technology)



Variety of RFID Technologies



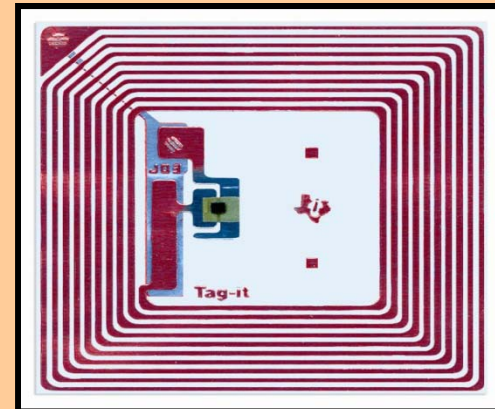
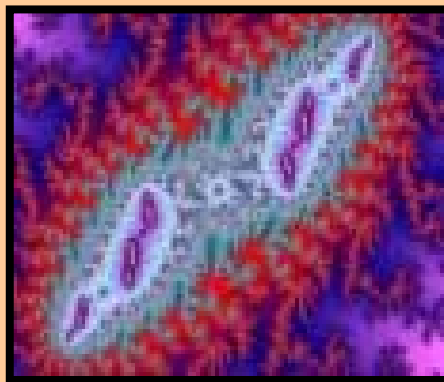
Security Issues:

- Espionage + Personal Privacy
- Forgery
- Sabotage (DoS)

RFID security/privacy challenge

How to obtain maximum security & privacy with minimal resources?

An RFID tag is a computational Amoeba



Thus far...

- RFID security/privacy dates back to 2002/3
- Lots of small results since then
- Many are broken
- Many are utterly impractical:
 - computation- and/or communication-hungry
- Three PhD-s on the topic
 - maybe more?
- Is the problem “deep”? Is it long-term?
 - I have doubts

- 6 panelists
 - Rieback, Burmester, Di Pietro, Kobsa, Molnar, Juels
- 9 mins (max) each
- Questions to follow