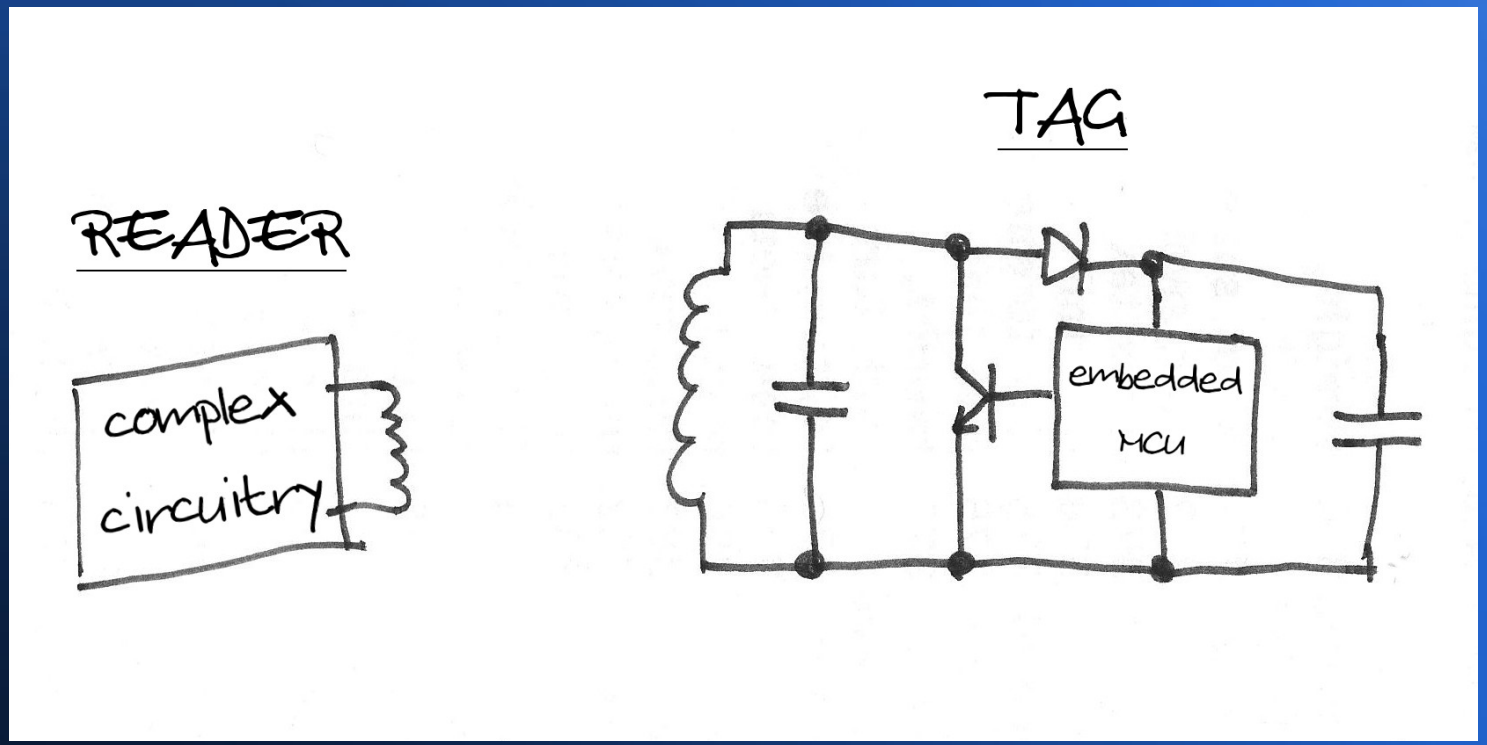
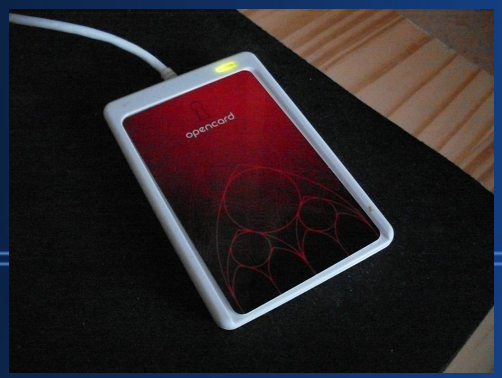
RFID (in)security primer

Jan Hrach

WTF RFID

(Radio Frequency IDentification)



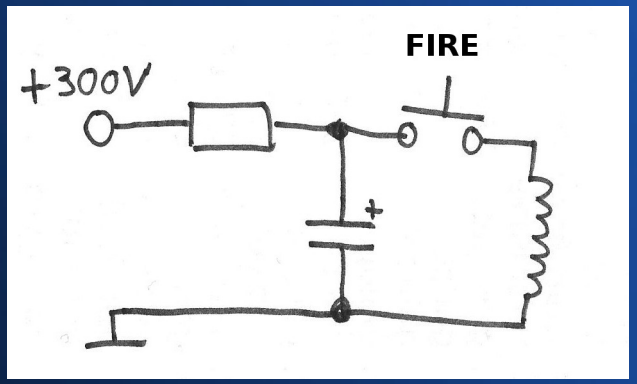


Tag types

- Dumb (and cheap) – UID transponders
- Crypto tags

Basic attacks

- **All attacks through-the-pocket**
- DoS: RFID Zapper

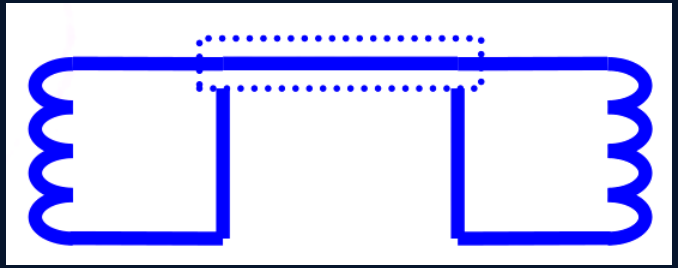


- Cloning attack

Crapto-1 story

- First tag in 1994
- Security-by-obscurity
- Reverse-engineered in 2008
- 48b keys allow brute-force, “random” number generator
- Can be broken in ~15 minutes on better computer or ~1 second on FPGA
- But still widely used (ISIC, Plzeňská karta, openkrad before 9/2008)

Relay attack



(credit: Tomáš Rosa, http://www.smartcardforum.cz/)

Relay attack - defense

- Distance-bounding

Typical #fail scenario

- Using UID as a “trusted” element
  - **lots** of MACs (incl. brmdoor), school cantens, single-use tickets……
  - → CLONE
- Storing values on card for offline checking
  - (phone cards), public transportation tickets (Plzeň, San Francisco), micropayment systems…
  - → TAMPER
- Weak crypto → CRACK
- Other → RELAY

Real-life examples

- brmdoor
- Pilsen Card
  - “Plzeňské městské dopravní podniky (PMDP) totiž manipulovanou kartu během několika dní zablokují.”
  - → DoS :-P
- openkrad
- BART
- ePassport

Links

http://brmlab.cz/project/freakcard#links

UAG

(the end)