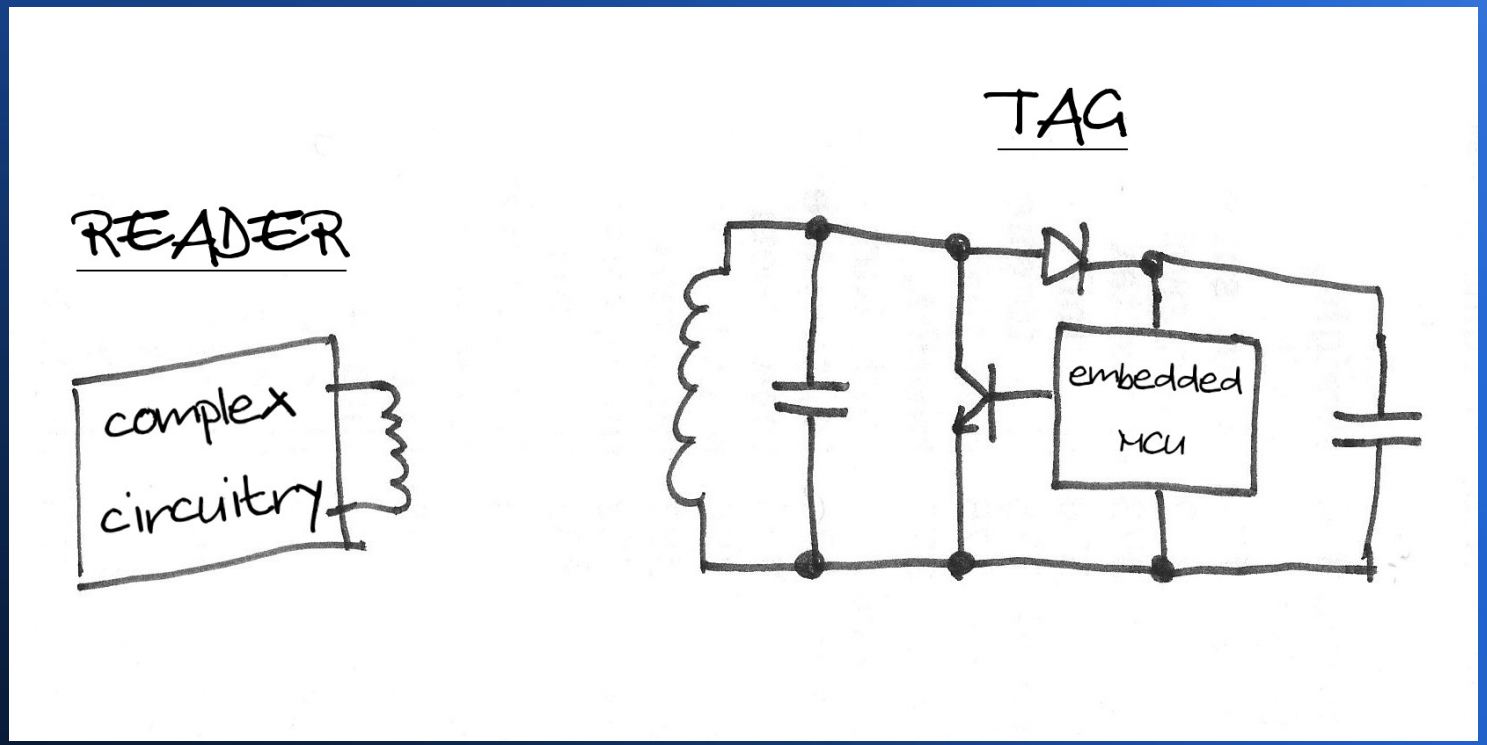
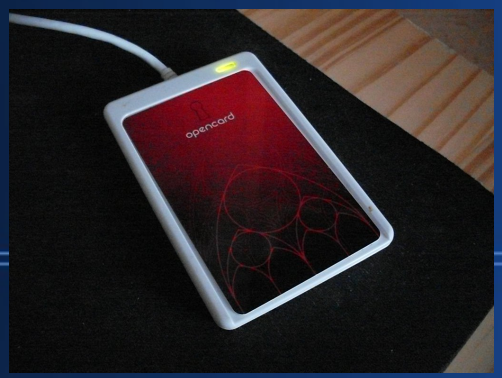
RFID (in)security primer

Jan Hrach

WTF RFID

(Radio Frequency IDentification)



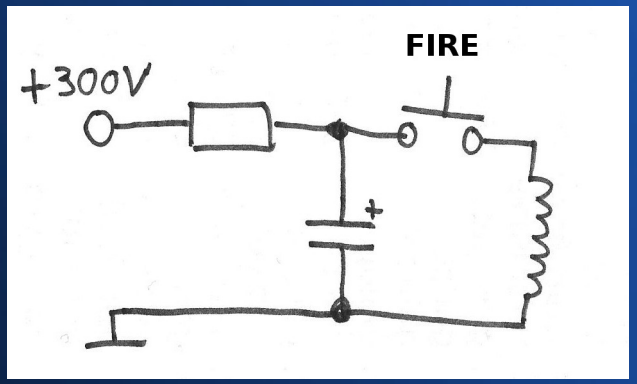


Tag types

- 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)

Breaking Mifare DESFire MF3ICD40: Power Analysis and Templates in the Real World — Extended Version*

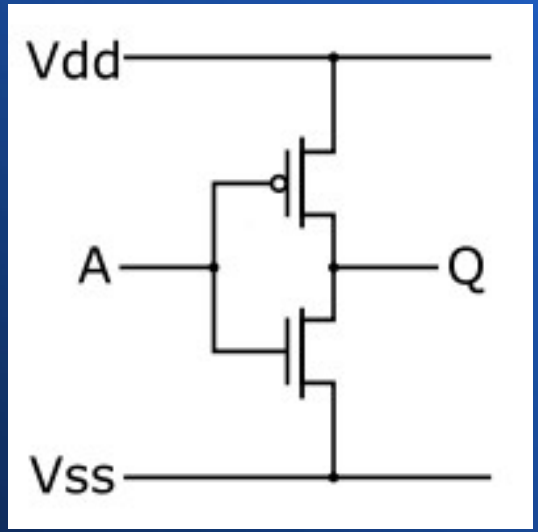
David Oswald and Christof Paar

Horst Görtz Institute for IT Security
Ruhr-University Bochum, Germany
david.oswald@rub.de, christof.paar@rub.de

Abstract. With the advent of side-channel analysis, implementations of mathematically secure ciphers face a new threat: by exploiting the physical characteristics of a device, adversaries are able to break algorithms such as AES or Triple-DES (3DES), for which no efficient analytical or brute-force attacks exist. In this paper, we demonstrate practical, non-invasive side-channel attacks on the Mifare DESFire MF3ICD40 contactless smartcard, a 3DES-based alternative to the cryptanalytically weak Mifare Classic [9, 25]. We detail on how to recover the complete 112-bit secret key of the employed 3DES algorithm, using non-invasive power analysis and template attacks. Our methods can be put into practice at a low cost with standard equipment, thus posing a severe threat to many real-world applications that employ the DESFire MF3ICD40 smartcard.

Keywords: contactless smartcard, side-channel analysis, templates, DESFire

Side channel - Power analysis



KEY transfer to crypto coprocessor (DESFIRE)
substitution, XOR… (AES S-box)

or jusr read the key directly (AFM - $ much)

…isn't symmetric cryptography for these purposes defective by design?

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
  - and planned turnstiles…
- BART – nice presentation in links
- ePassport

Links

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

UAG

(the end)