Reverse Engineering a Cryptographic RFID Tag

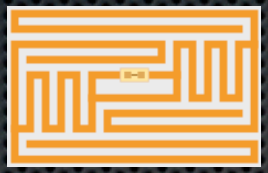
Karsten Nohl, David Evans, Starbug Plötz, Henrik Plötz

Presented by Avani Wildani

Radio Frequency IDentification

- All RFID tags are essentially radio transponders with memory.
  - Can be either passive (no power) or use relfective power (modulated backscatter) with a battery.
- Two components: IC and antenna

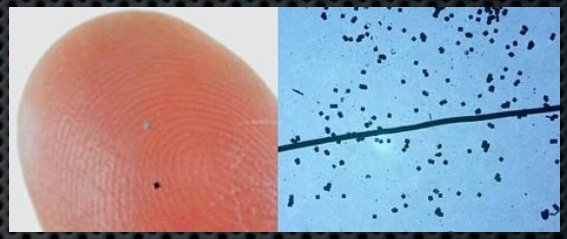
Where are RFIDs used?



- UCSC (and most corporate) ID Cards
- Passports
- Clothing/Books/CDs (EPC tags)
- BART Passes
- Animal Tracking
- Paying for drinks if you're a VIP (!)

Image: WalMart EPC RFID tag; courtesy of Wikipedia

RFID Errata



- Smallest tag is 150 x 150 x 7.5 microns
  - Can store 38 digit numbers using 128-bit ROM.
- Initiative to reduce per-tag price to 5¥, or about a nickel.
- Typical frequencies are 0.125–0.1342, 0.140–0.1485, 13.56, and 868–928 Mhz.
  - Optical “RF”ID uses 333 THz. It also can’t be read without line of sight, which makes it slightly less vulnerable.

Image courtesy of http://www.pinktentacle.com/tag/hitachi/

Security Issues

- RFID manufacturers love “Security through Obscurity”
- Many RFID tags send and receive data in clear text, leaving themselves open to man in the middle attacks (more later)
- Cost of reconstructing cipher from the hardware implementation is less than manufacturers think.

MIFARE Classic RFID Tag

- Primarily for ticketing, transportation, and access control / identification.
- Widespread: Costs under .5€ in small quantities.
- 1sq mm: 1/4 for 1K flash, 1/4 for antenna, 1/2 for logic + cryptography
- Crypto functions make up 400 2-NAND gate equivalents, whereas small AES takes 3400: very simplistic.

MIFARE Cipher

- Uses a 48-bit symmetric stream cipher.
  - This is already crackable: remember how easy it was to crack 56-bit DES.
- Data is divided into two sections with different access rights and correspondingly different keys.
- To ease key-distribution, different tags in a system frequently have the same read key, leaving it open to impersonation.

Physical Reverse Engineering

- Step 1: Dissolve cards with acetone to get access to the chip.
  - Step 1.5: Place chip in a medium to limit tilting
- Step 2: Polish off micrometer-thin layers of the chip using .04μm thick sandpaper or polishing solution.
- Step 3: Image all 6 layers (transistors are on the bottom).
  - Some tilting is unavoidable. Use a tool to average several images.

Physical Reverse Engineering

- Step 4: There are several thousand logic gates on a chip, but only about 70 types. Identify these gates.
- Step 5: Use MATLAB image processing to automatically identify these gates given the templates you've identified.
  - Use normalized cross-correlation to overcome the variation in color/brightness across your chip images.
  - This is <10 minutes for the entire chip.

Physical Reverse Engineering

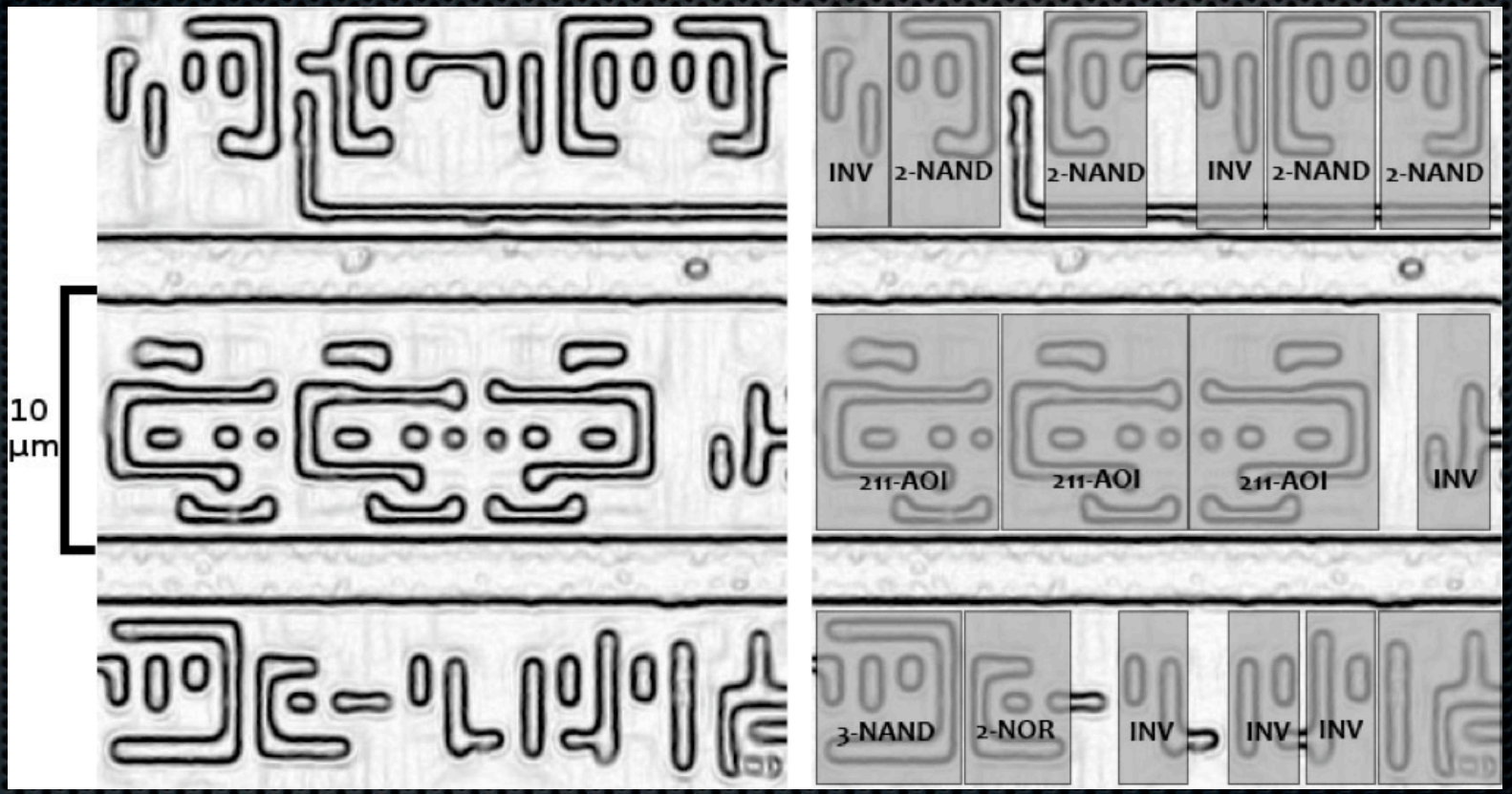


Image from Nohl et al., 2008

Physical Reverse Engineering

- Now that you know how the gates are laid out, you can find the cryptographic area of the chip by looking for a 48+ bit register and a set of XOR gates.
- RNG is an area with output but no input.
- Examine the area by hand, but don’t over-do it: you can fill in holes in your knowledge by analyzing the protocol.

Protocol Analysis

- Use the OpenPCD Open Source RFID Reader to poke the chip. This lets you control timing, which is important to discovering vulnerabilities.
- First test: Are the key and the (known) tag ID shifted together sequentially? They tried shifted combinations and found many worked.
  - This also told them the structure of the 48-bit linear shift register that holds the cipher.
    - Entirely deterministic register that just cycles through a set of values by XOR-ing.

Protocol Analysis

- Cipher contains no non-linearity. This means everything is easy to derive once you know something.
- Recap: Authentication protocol is taking a shared secret key and a unique ID tag as input and using those to establish a shared session key for the stream cipher.

Random Number Generation

- Random numbers generated by a 16-bit linear feedback shift register initialized to a constant value.
- This means that the “random” number is purely a function of the amount of time the tag has been powered up!
- The number is also very short. Even if you can’t control the timing, you only have 65,535 possibilities.

Vulnerabilities

- Key is small enough to brute force.
  - Takes about 50 minutes on 64 FPGAs.
- Since you control “random” numbers and know the shifting patterns, you can create a codebook of recorded authentication outputs and the corresponding keys. Rainbow tables let you trade computation for space and store information for all keys.
- Each session key/ID pair has exactly one corresponding secret key and all shifts are linear: Thus, if you compute codebook for one secret key, you can use it anywhere...

Summary

- Attacker scans public RFID ID.
- Use a reader to record just two timed challenge-response interactions with the card.
- Use codebook to compute the key.
- Read all data on the card in the clear.
- Game over.

Fixing MIFARE Classic

- Better RNG: exploit the fact that memory cells are initially “random.” Start the cipher area in a random state and evolve using feedback loop until the random number is needed.
  - This also saves space since you don’t need a separate RNG: Use this to make a bigger cipher.
- Break the key-ID mapping by using a non-linear feedback on one of the two for the register shift.
- Make the output function non-linear to protect against statistical attacks.

General Defense

- Don’t rely on secrets! Use something like 3-DES and implement it properly.
- Use fraud detection to detect unusual access patterns.
  - Even worse for privacy than straight RFID.
- Obfuscate at least the cipher part of your physical circuit design.

Just in case you feel safe...

- Many large companies don't bother with encryption at all.
- For access-passes, you can just grab and replicate the authentication code from a correct RFID: This is known as a relay attack.
- Passport cards and drivers' licenses can be easily cloned as well as having the data stolen off them.
  - You can download apps off the Internet to "back-up" any actual modern US passport.

Further Reading

- http://www.dexlab.nl/ (Passport Backup)
- http://hackaday.com/2009/02/16/shmoocon-2009-chris-pagets-rfid-cloning-talk/ (Great talk!)
- http://hackaday.com/2009/02/02/mobile-rfid-scanning/ (Passport RFID Cards)
- http://www.schneier.com/blog/

Questions?

Amal Graafstra's hands. Image courtesy of http://www.amal.net/rfid.html