Practical Attacks on a Proximity Card

Jonathan Westhues
jwesthues@cq.cx
June 18 2005

Introduction

- How do RFID tags work?
- Signals sent over the air
- A naïve attack works perfectly
- Better-than-naïve attacks work even better
- Security is possible if you are willing to pay for it

How the tags work

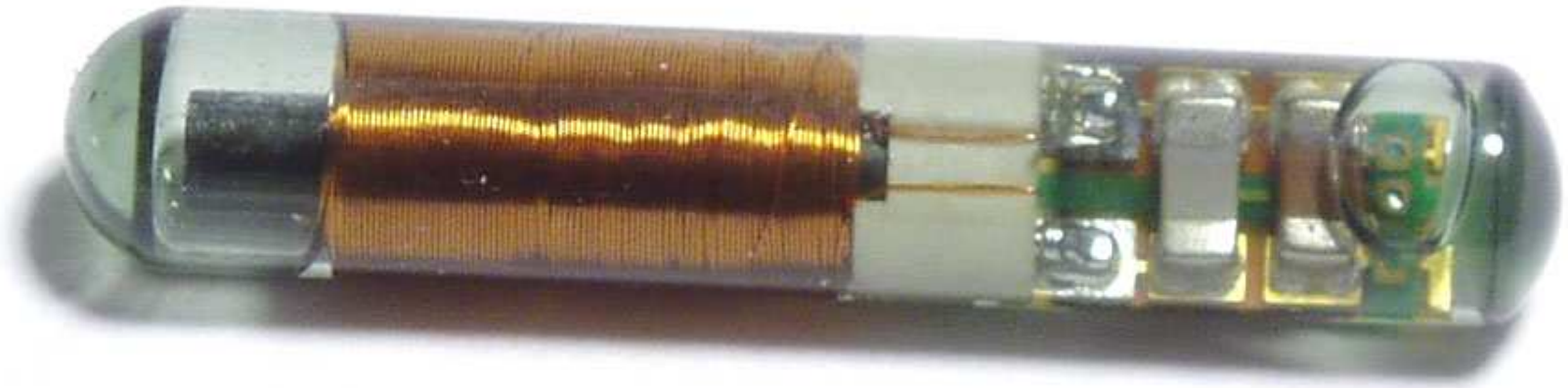
- The reader transmits a powerful carrier (a signal that carries no information)
  - Reader “excites” or “illuminates” tag
- This carrier powers the circuitry on the tag
  - So the tag does not need an internal power source (battery)

Information over the air

- Tag returns an information-bearing signal to the reader
  - Same frequency, same antenna
- Bi-directional communication also possible
  - e.g. to write information to a tag instead of just reading

Example: TI tag

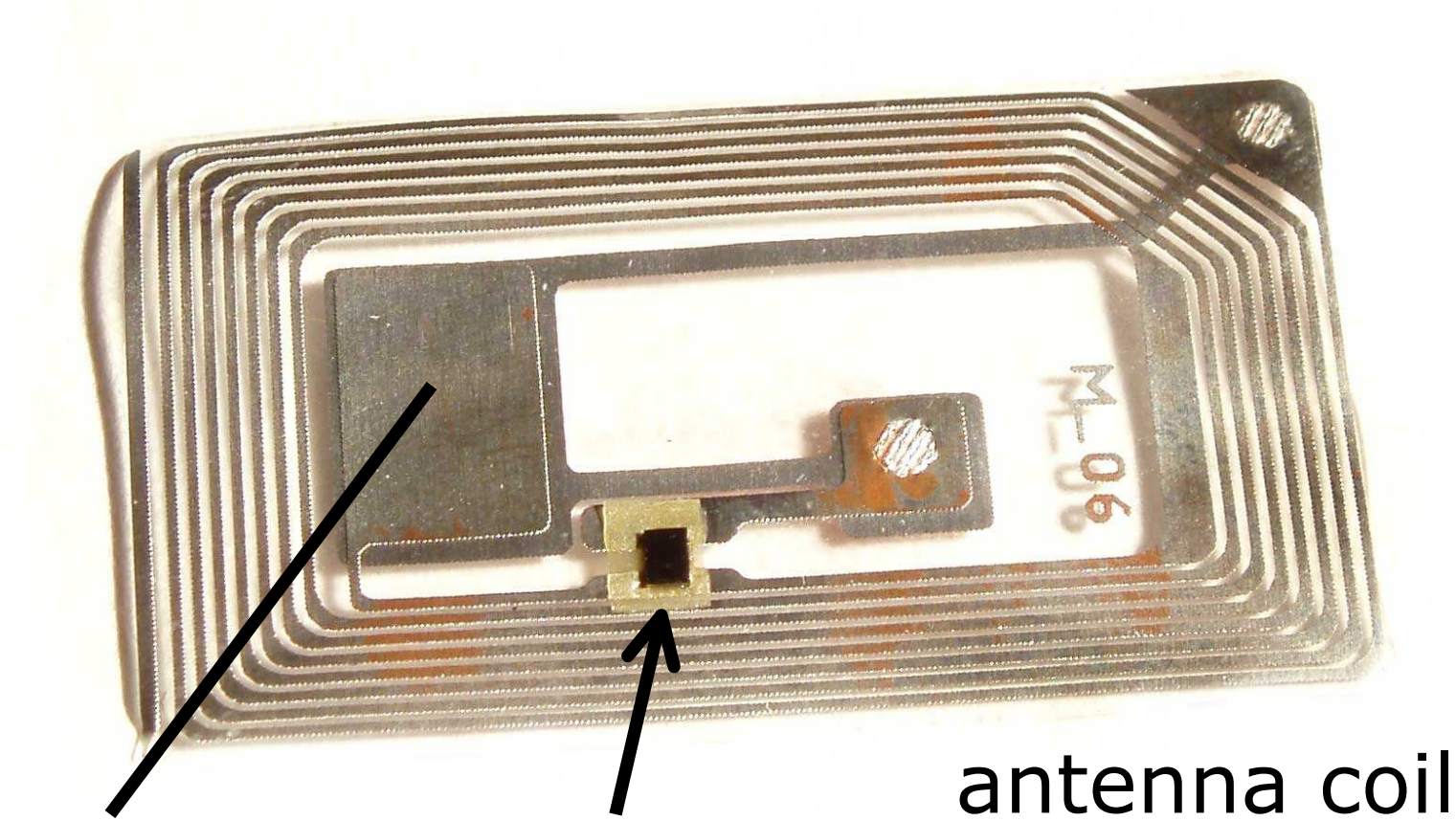
capacitor(s)



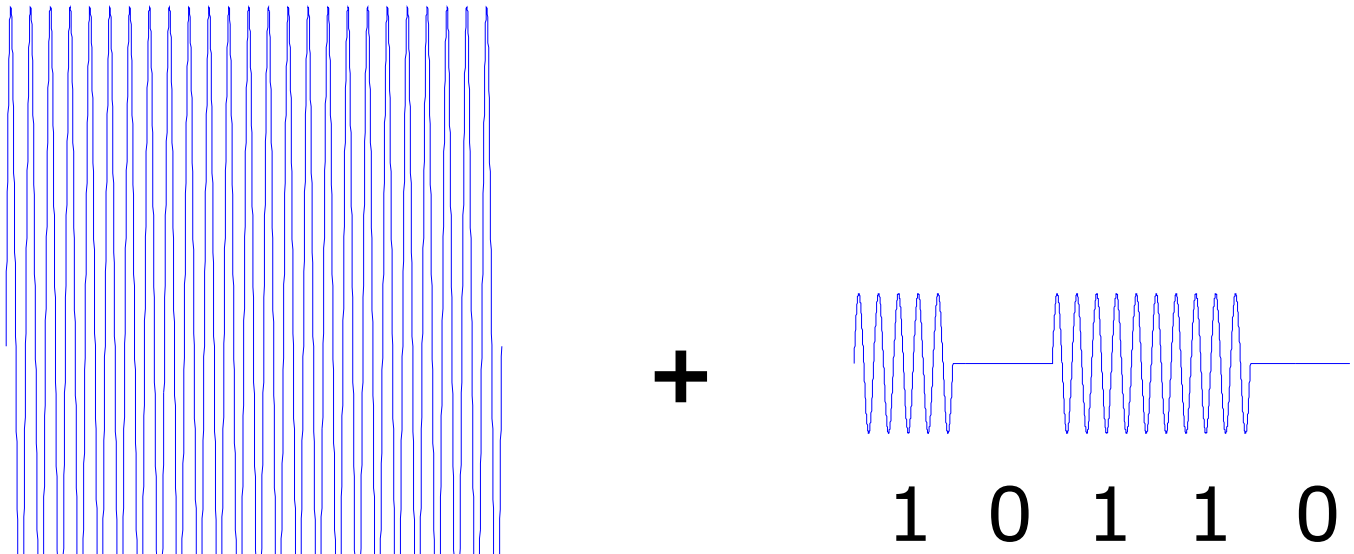
antenna coil

(microchip on other side)

Example: 13.56 MHz tag



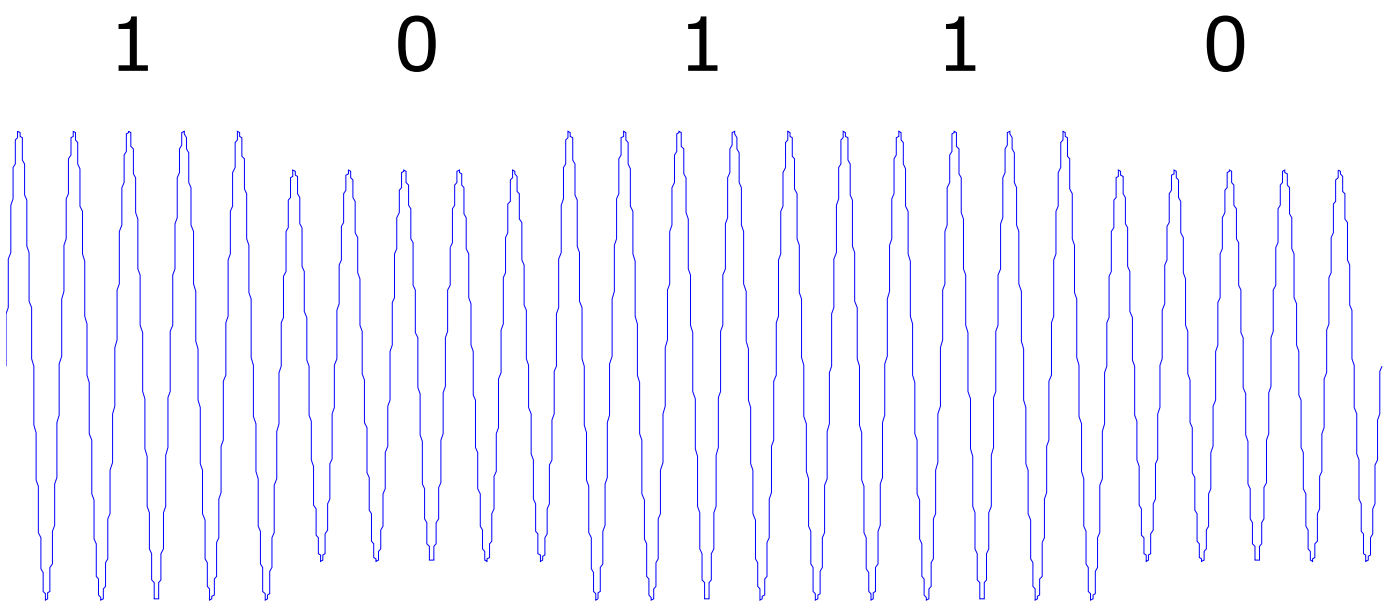
Signals over the air



reader: powerful, no information

tag: weak, carries information

Result: the signals add

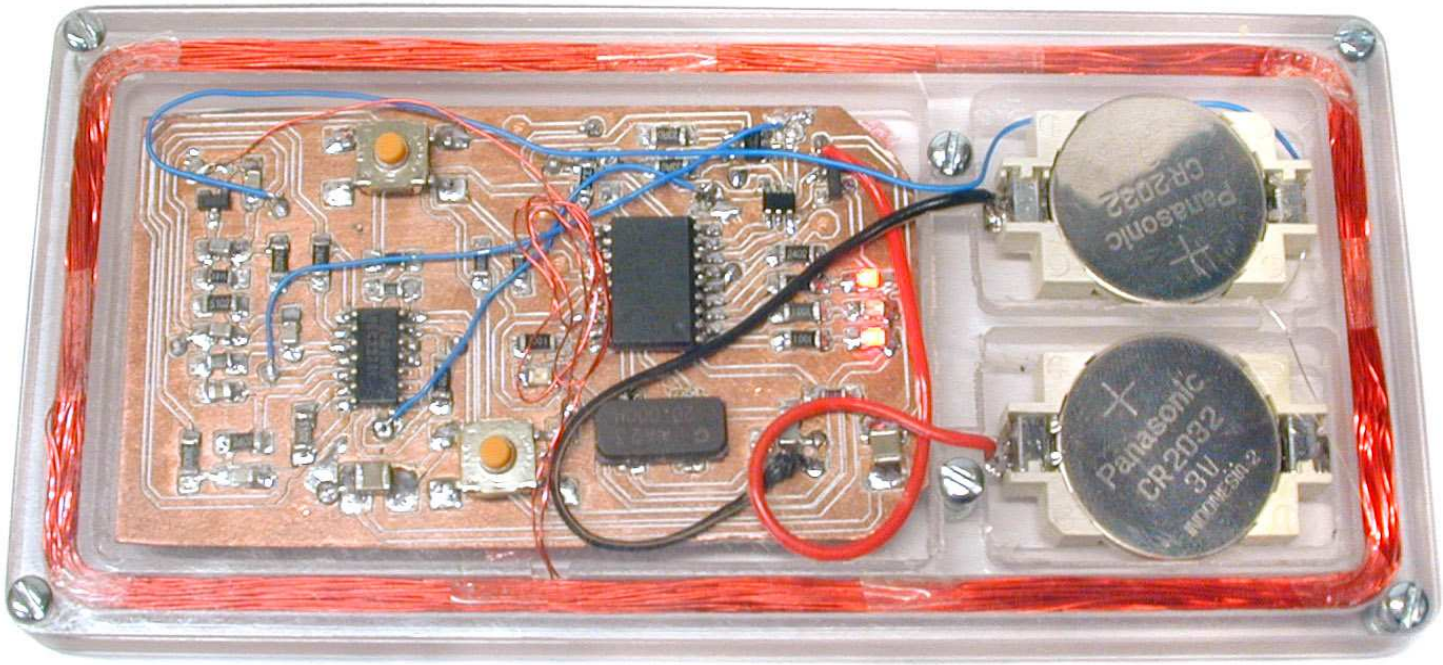


(signal seen at the reader)

Motorola/Indala Flexpass

- Card transmits its ID code to the reader
- Reader checks ID against its list to see if it should open the door
- That’s it; no attempt at security

Basic replay attack



Basic replay attack

- Read a legitimate card to get its ID code
- Store the ID in memory
- Replay the ID to a legitimate reader

Basic replay attack

- Hardware design: nothing fast, no need for anything custom
- Easy
- Other people have done this

What kind of read range?

- Depends on the power of the carrier that the reader transmits
- Practical limits:
  - TX power
    - Legalities (FCC, Industry Canada)
    - Input power
    - Technical limits (heat etc.)
  - Antenna size

Practical read range

- “A few feet”

Even better attacks

- The read range goes up when the card is already powered
  - Thus, even more vulnerable if the eavesdropper sets up near a legitimate reader
- The signal goes through sheetrock walls

DSP refinements

- FlexPass cards: repeat their ID over and over as long as they are powered
- Opportunity to use DSP techniques to “average together” multiple copies and improve sensitivity

Solution

http://members.core.com/~jeffp/

- But surely we can do better…

FlexPass FlexSecur

- Encrypt ID before programming it onto card
- Replay attack:
  - Doesn’t help, eavesdropper unlikely to notice that is present
- Not useless though

Challenge/Response

- Fixes everything, and cards are available that use it
- Drawbacks:
  - Complexity: crypto circuitry on the card
  - Bi-directional communication with reader is now required

Alternative: Rolling codes

- Also fixes everything
- Used e.g. in auto keyless entry
- Advantage:
  - No bi-directional communication required
- Disadvantage:
  - Needs non-volatile storage

Conclusion

- ID-only cards are not in any mathematical sense secure
- Secure alternatives exist
- Depending on the application, they might not be better
- It would be nice if the vendors would tell you what you’re getting

Thank you