IOActive™

COMPREHENSIVE COMPUTER SECURITY SERVICES

RFID for Beginners++

Chris Paget, Director of R&D, IOActive
chris.paget@ioactive.com

20 minutes?

- 20 minutes to cover:
  - Theory
  - Design
  - Operation
  - Mathematics

  Of RFID systems? Not freaking likely.

- Include design and operation of Cloner 2.0?
  - Uhhh….

What happened in DC?

- Legal nastiness, ACLU, DHS, US-CERT
- yadda yadda patents yadda yadda.
  - Look it up if you’re interested

- Where did it all end up?
  - $10m of patent attorney time is a lot, no matter how 1337 you are
  - Couldn’t risk it ☹

- No schematics
- No PIC source code
- No singling out specific (nameless) vendors….

So what then?

- <Insert talk about theory, design, operation, and mathematics of RFID here>
  - <Explain vehemently that ALL prox systems are vulnerable – Indala, Motorola, Hitachi, “others”>
- If you’re using 125KHz Prox, your doors are highly insecure.
- Demo time!

OK, so you didn’t fake it then?

- Nope.

- RFID shields do *NOT* protect you at 125KHz.
  - You mean my tinfoil wallet is worthless?

- Research continues…

IOActive™
COMPREHENSIVE COMPUTER SECURITY SERVICES

Cloner 2.0

- In development
- Massively improved capabilities
  - Improved read range
  - Multiple RF frontends for different modulations
  - Enhanced microcontroller s/w for different data formats
  - Passive mode
    - Let someone else power the card, sniff at a distance
    - Aiming for 10 feet
    - Drop it in a bush, come back the next day
  - Display and keypad for retrieval / entry of codes

- Blackhat 2008?

I can has schematics?

- Mine? No.

- Others? Sure!
  - Jonathan Westhues' VeriChip cloner
    - http://cq.cx/vchdiy.pl
  - PIC16F628A datasheet:
    - http://ww1.microchip.com/downloads/en/DeviceDoc/40044E.pdf
  - Microchip reference design for an RFID reader
    - http://pe.ece.olin.edu/projects/proxcard/51115e.pdf
  - Protocol documentation
    - http://pe.ece.olin.edu/projects/proxcard/prox.html

- Those links, high-school level electronics, and a week or so.
  - Maybe a month if you don't know anything beyond V=IR

IOActive™

COMPREHENSIVE COMPUTER SECURITY SERVICES

Questions?

(And yes, I can answer technical stuff over email)

chris.paget@ioactive.com