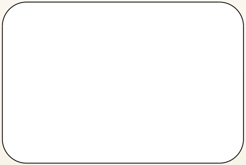
RFID Hacking

23rd Chaos Communication Congress
"Who can you trust?"

Henryk Plötz <henryk+23C3@ploetzli.ch>

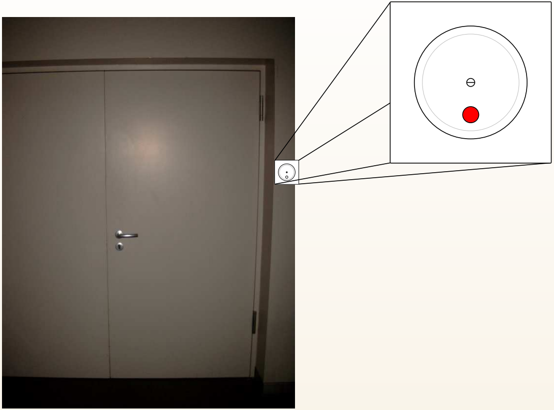
2006-12-28

Analyzing an unknown access control system



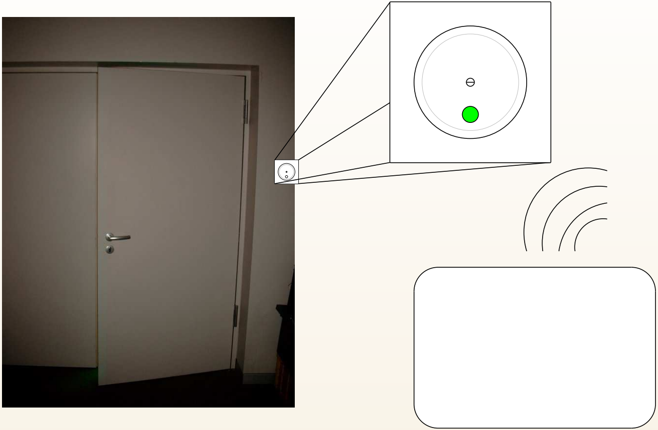
Card

Analyzing an unknown access control system



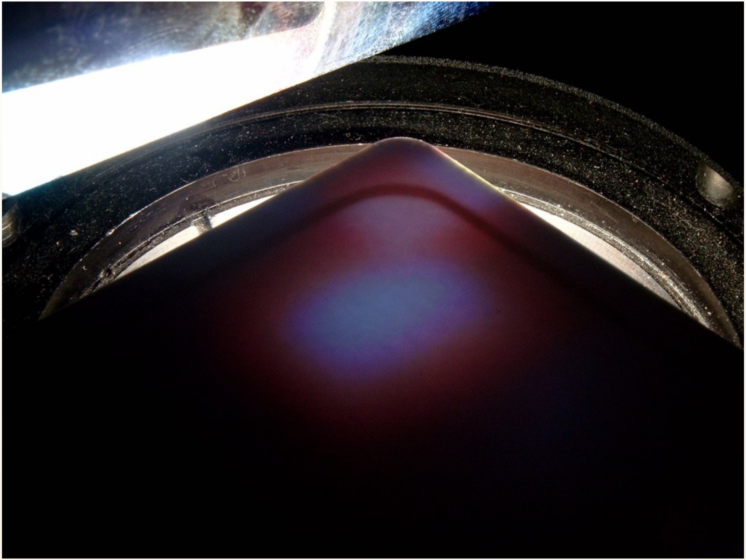
Door

Analyzing an unknown access control system



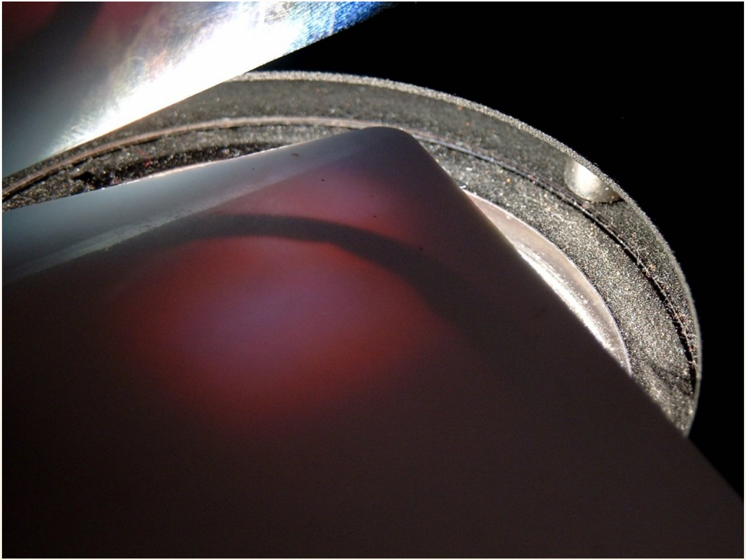
Card opens door

Step 0: Preliminaries



For comparison: 13.56MHz card

Step 0: Preliminaries

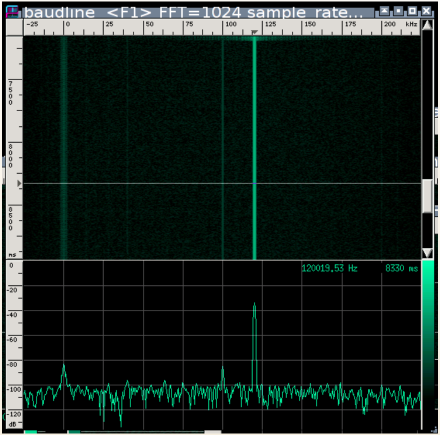


Unknown card: lots of windings → probably low frequency

Step 1: Find the carrier

gnuradio/USRP to the rescue!

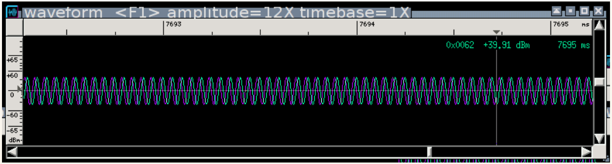
1. Position an antenna next to the door transceiver
2. Look at the lower end of the radio frequency spectrum
   → powerful carrier at 120kHz



Step 1: Find the carrier

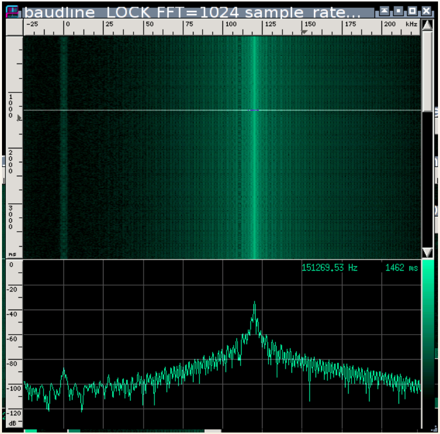
gnuradio/USRP to the rescue!

1. Position an antenna next to the door transceiver
2. Look at the lower end of the radio frequency spectrum
   → powerful carrier at 120kHz



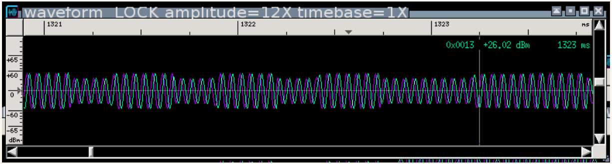
Step 2: Capture the identification

1. Hold a card next to the door transceiver
2. Look at the signal
   → load modulation from the card (as expected), no signal other than the carrier from the door



Step 2: Capture the identification

1. Hold a card next to the door transceiver
2. Look at the signal
   → load modulation from the card (as expected), no signal other than the carrier from the door

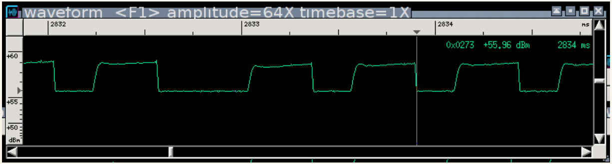


Step 3: Demodulate the signal

1. Amplitude demodulation with gnuradio (gr.pll_carriertracking_cc and gr.complex_to_mag)
2. Look at the recovered data signal:

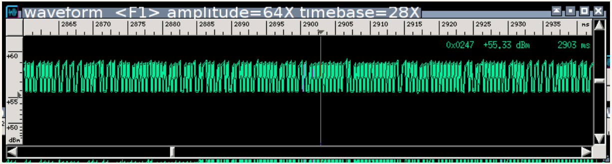
   $\longrightarrow$

   - Seems to be manchester encoded
   - Probably periodic (period length ca. 68ms)



Step 3: Demodulate the signal

1. Amplitude demodulation with gnuradio (gr.pll_carriertracking_cc and gr.complex_to_mag)
2. Look at the recovered data signal:
   →
   - Seems to be manchester encoded
   - Probably periodic (period length ca. 68ms)



Preliminary summary

What we have up to here:

- Door transceiver transmits carrier at 120kHz
- Card transmits its ID with load modulation as soon as it is in the field
- ID is looped as long as the transponder is in the field
- Especially: no challenge/response!
- Should be easy to replicate

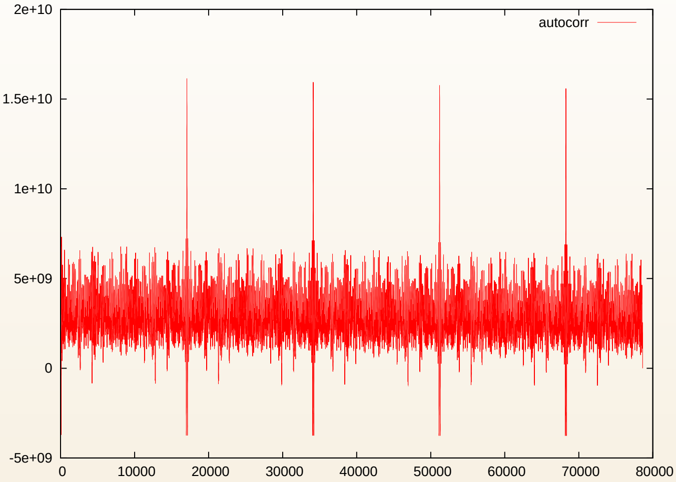
Step 4: Find the exact period length

1. Autocorrelation over the data using program in C

$$\text{autocorr}(i) = \sum_{t=0}^{n-i} \left(x\left(t\right) - \overline{x}\right) \cdot \left(x\left(t+i\right) - \overline{x}\right)$$

Step 4: Find the exact period length

2. Graph the result in Octave:



Step 4: Find the exact period length

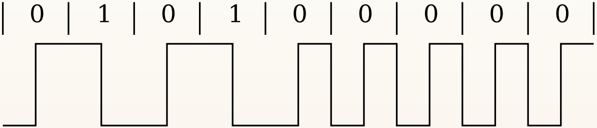
1. Autocorrelation over the data using program in C

$$\text{autocorr}(i) = \sum_{t=0}^{n-i} (x(t) - \overline{x}) \cdot (x(t+i) - \overline{x})$$

2. Graph the result in Octave
3. Maxima at 17067, 34133, 51200, ... samples
   $\rightarrow$ periodic signal, period length 68.266... ms $\equiv$ 8192 periods of the 120kHz carrier $\rightarrow$ looks about right
4. Might perform periodic averaging to enhance the signal

Step 5: Find the bit length

1. Assume manchester encoding. Bit length is two times the shorter time between two edges or equal the longer time between two edges.



2. Measure in the data signal: $\approx 533.3\,\mu s \equiv 64$ periods of the 120kHz carrier $\rightarrow$ looks about right
3. Result: 128 bits @ 1875 bits/s

Step 6: Decode the ID

1. Get some additional samples and use a manchester decoder on the data.
2. Use the long low-frequency sequence as synchronization signal (in manchester code: 1010101010)
   →Doesn't look right: 4 samples: A and B identical except for about 40 bits, C and D identical except for about 40 bits, A and C nearly complementary

New Theory: Differential Manchester Encoding

1. Transform manchester decoded signal to differential manchester decoded signal (easy: just xor all consecutive bits)
   → Looks better: All samples identical except for about 50 bits
2. Try to find the printed number somewhere in the ID.

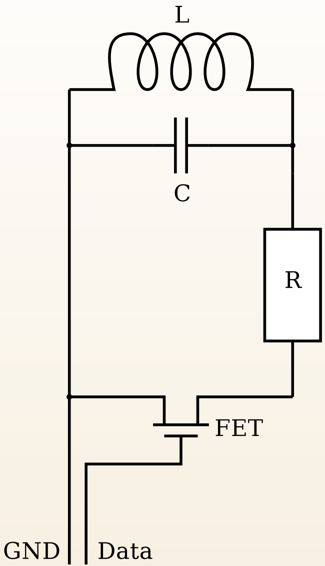
   523: 1111 1111 1000 1011 0110 0100 0010 0001
   0011 0011 0100 1010 1010 0011 0000 0101 0
   0010 0011 0 **0000 0101** 0 0000 0000 0011
   1000 1001 0000 0000 1101 0100 0000 11000

Replaying

Remember:

- ID transmitted with load modulation
- . . . in a loop . . .
- . . . without challenge/response
- "Should be easy to replicate"

Load modulation

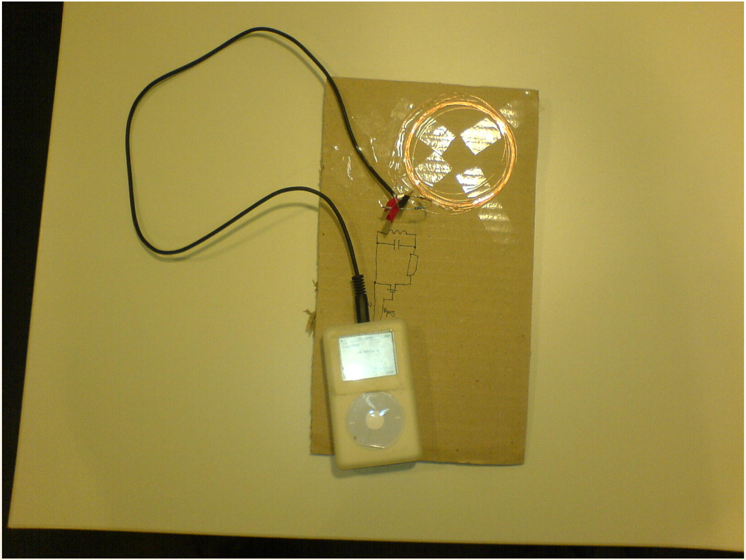


For example:

radius of coil	3.25 cm
diameter of wire	0.2 mm
C	22 nF
number of windings	$\approx$ 15.7

For the full formula see: RFID Handbook, Klaus Finkenzeller

Replayer



video

Outlook

- Maybe find out more about the data encoded in the ID
- Have a look at Mifare (they use a stream cipher and CRC → confidentiality without integrity) when the OpenPICC+OpenPCD hardware is available.

Thanks for listening.