HOWTO sniff RFID

“rfiddump” Project presentation

Milosch Meriac
mailto:22c3@bitmanufaktur.de

Hard copy of presentation:
http://rfiddump.org/rfid-22c3.pdf

HOWTO sniff RFID

Who am I ?

- Milosch Meriac
- freelance hard & software developer
- focused on deeply embedded systems
- custom-tailored embedded linux platforms
- linux and windows kernel drivers
- lowlevel/realtime programming
- reverse engineering

HOWTO sniff RFID

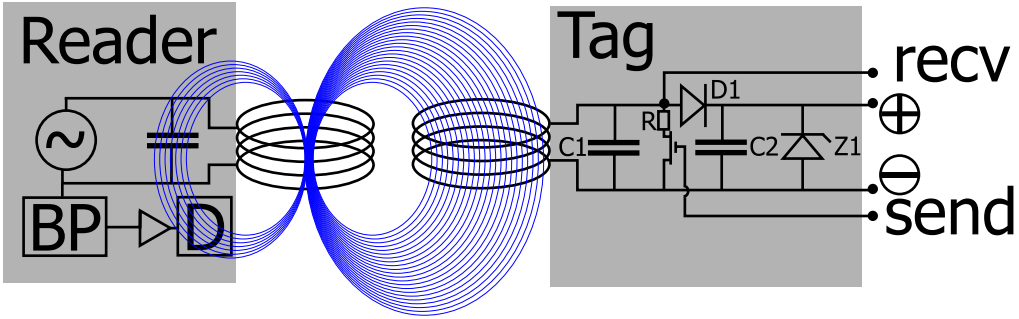
What do we need ?

- a generic approach for sniffing RFID transponders at 13,56MHz
- “cheap” says the budgie: affordable
- device built from freely available parts
- as few as possible expensive equipment needed to build one: home-brewn devices must be possible

HOWTO sniff RFID

Short introduction into Tag-Reader communication at 13,56MHz (I)

- applies to ISO14443
- can be compared with an air coupled transformer: inductive coupling



HOWTO sniff RFID

Short introduction into Tag-Reader communication @13,56MHz (II)

- Reader transmits a 13,56Mhz carrier
- carrier is used as tag power supply (rectifier D1, capacitor C2 & Zener diode Z1)
- Reader->Tag by AM-modulated carrier
- Tag -> Reader by changing the load of the carrier (like carrier AM)

HOWTO sniff RFID

Sniffing problems (I)

- we need an antenna that is capable to "see" the magnetic field portion.
- solution: Magnetic Loop Antenna
  Example calculation for 13,56MHz:
  300/13,56MHz = 22,12m is one wave
  22,12m / 4 = 5,53 is 1/4 wave
  5,53m / pi = 1,76m optimal diameter

HOWTO sniff RFID

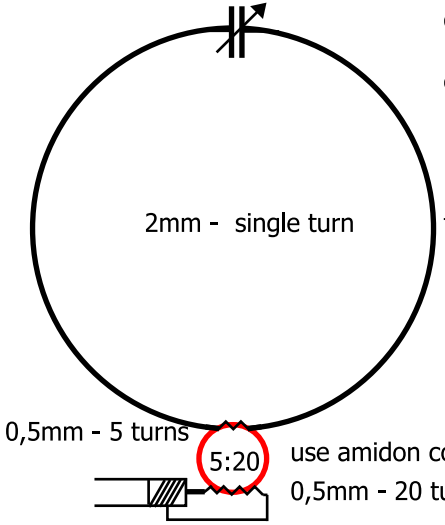
How do you build a cool loop antenna easily for less than €10 ?

- get a plastic Hula Hoop®
- get thick copper wire (2mm or thicker is fine)
- get a low cost adjustable capacitor (1,6-15pF, 250V)
- Amidon torodial core (T50-2)
- 50 ohm coaxial cable

Milosch Meriac <rfiddump@bitmanufaktur.de> - http://rfiddump.org/

HOWTO sniff RFID

How does a “Hula Loop” look like?

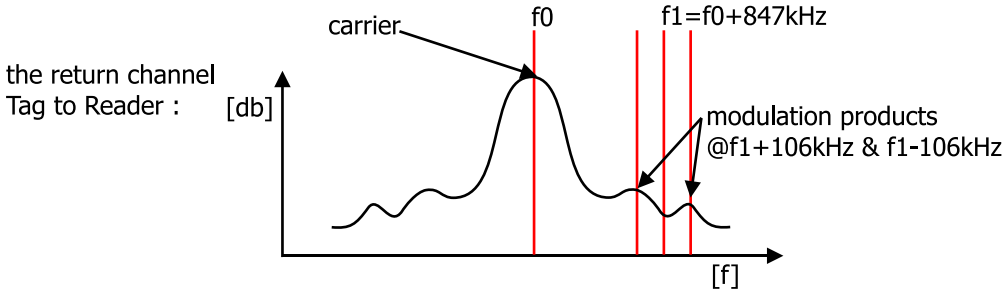


Milosch Meriac <rfiddump@bitmanufaktur.de> - http://rfiddump.org/

HOWTO sniff RFID

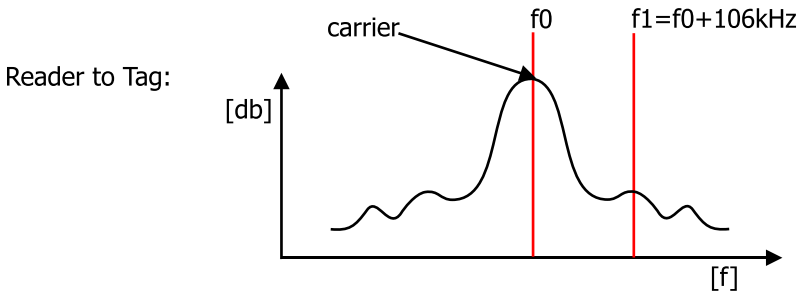
Sniffing problems (II)

- more than 50db carrier-to-sideband signal ratio for return channel (Tag->Reader)
- must filter signal before amplifier



HOWTO sniff RFID

Sniffing (Reader->Tag)
- tune receiver to carrier +/- baud rate frequency



HOWTO sniff RFID

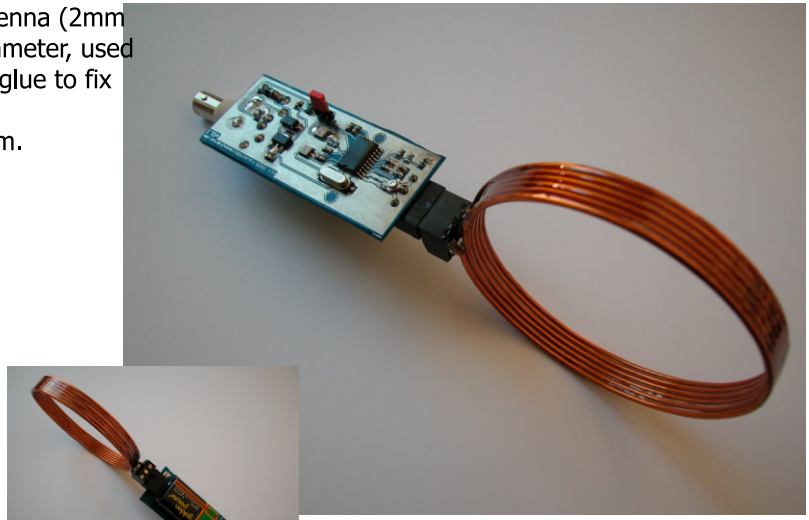
High sensitive Tag->Reader sniffer:

- use common SA615 RF-IC
- downmix upper sideband
  13,56MHz+847kHz with
  common 3,6864Mhz crystal.
  13,56+0,847-3,6864=10,7206MHz
- 10,7206MHz allows usage of common
  ceramic 10,7Mhz filters !

HOWTO sniff RFID

How does our mini sniffer look like

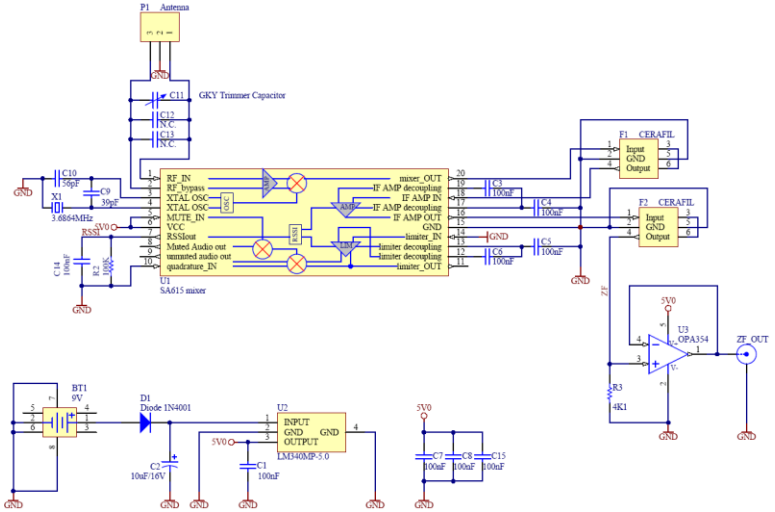
5 turns loop antenna (2mm CU, ~90mm diameter, used two component glue to fix the wire.
Current range 1m.



Milosch Meriac <rfiddump@bitmanufaktur.de> - http://rfiddump.org/

HOWTO sniff RFID

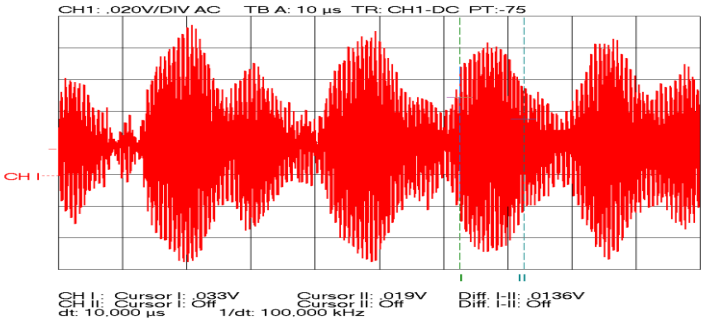
Mini sniffer HF-Frontend



HOWTO sniff RFID

What does the sniffer currently provide:

- buffered clean intermediate frequency at 10,7Mhz with Reader ->Tag data



HOWTO sniff RFID

What do we want to achive in near future (release on march 2006):

- full duplex sniffing of RFID R->T and T->R traffic at distances of 3 to 5 meters
- GPL'ed toolset with tcpdump-like functionality and protocol decoding
- **RFID Tag emulation mode: can emulate any given ISO14443 Tag**

HOWTO sniff RFID

What can it be used for ?

- for replacing "lost" RFID tags
- reverse engineering of readers, protocols and tags without physical access to a reader or a tag.
- offline RFID key cracking
- validate RFID RF interfaces
- collect passively statistics of persons passing a RFID reader

HOWTO sniff RFID

Questions ?