Eavesdropping Attacks on High-Frequency RFID Tokens

Gerhard P. Hancke

July 11, 2008

UNIVERSITY OF CAMBRIDGE

Royal Holloway
University of London

What is the talk about?

- NOT presenting a new attack method
  - Overall eavesdropping is a straight forward attack
- NOT announcing that HF RFID can be eavesdropped
  - Already a recognised threat
- Look at issues around RFID eavesdropping
  - Ambiguities, perceptions and relevance (past and present)
- Discuss our eavesdropping experiment
  - Provide details method, observations and experiences
  - It is NOT all about the distance results (which can be affected by various variables)
- Some points in the talk might appear obvious:-)

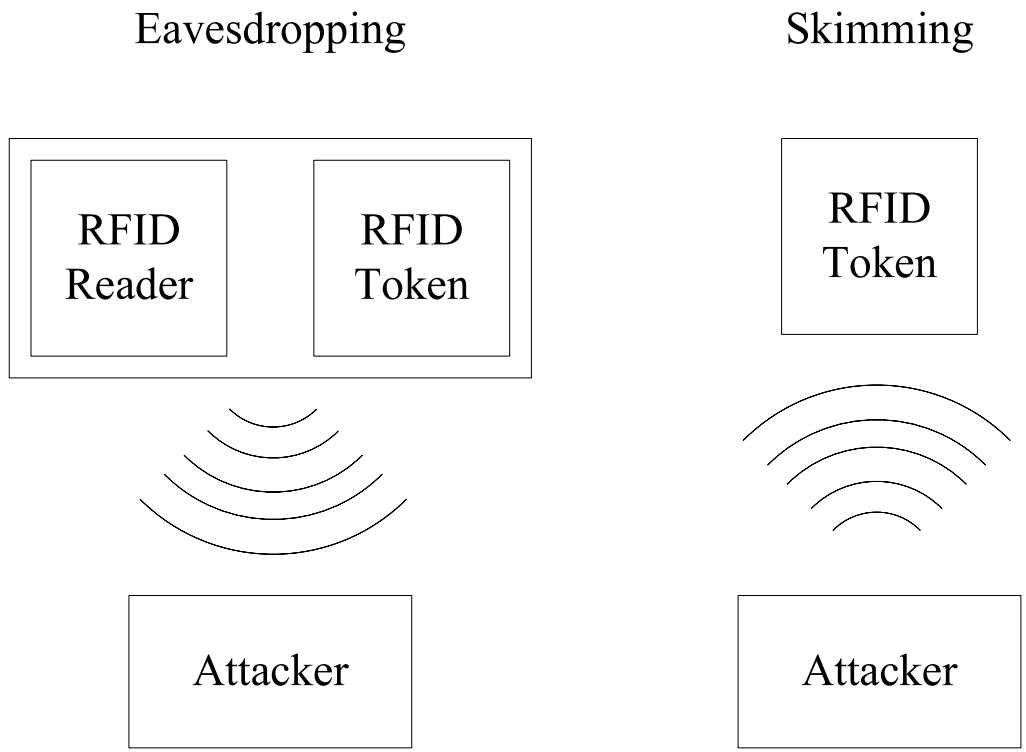
Why is eavesdropping still important?

- Credit Cards
  - Reported cases of personal information sent in the clear
- e-Passports
  - Some issues surrounding the entropy of the key
- Travel/Ticketing
  - Mifare Classic Crypto1 recently reverse engineered and shown to exhibit weaknesses
- Access Control
  - Some systems still use simple IDs or minimal crypto
- It seems that various end users still care...

Attack background

- Eavesdropping scenarios are well known
  - Government/public sector reports(e.g. NIST, DHS, BSI), academic papers, press report etc
- Practical results are limited to a few publications
  - T. Finke and H. Kelter(BSI). *RFID – Abhörmöglichkeiten der Kommunikation zwischen Lesegerät und Transponder am Beispiel eines ISO 14443-Systems*
  - J. Guerrieri and D. Novotny (NIST). *HF RFID Eavesdropping and Jamming Tests*
  - W. Tobergte and R. Bienert (NXP). *Eavesdropping and activation distance for ISO/IEC 14443 devices*
- Mains points of interest
  - Distance still an issue being debated/reported
  - Is it feasible in terms of cost and effort for an attacker?

Ambiguity: Type of attack?

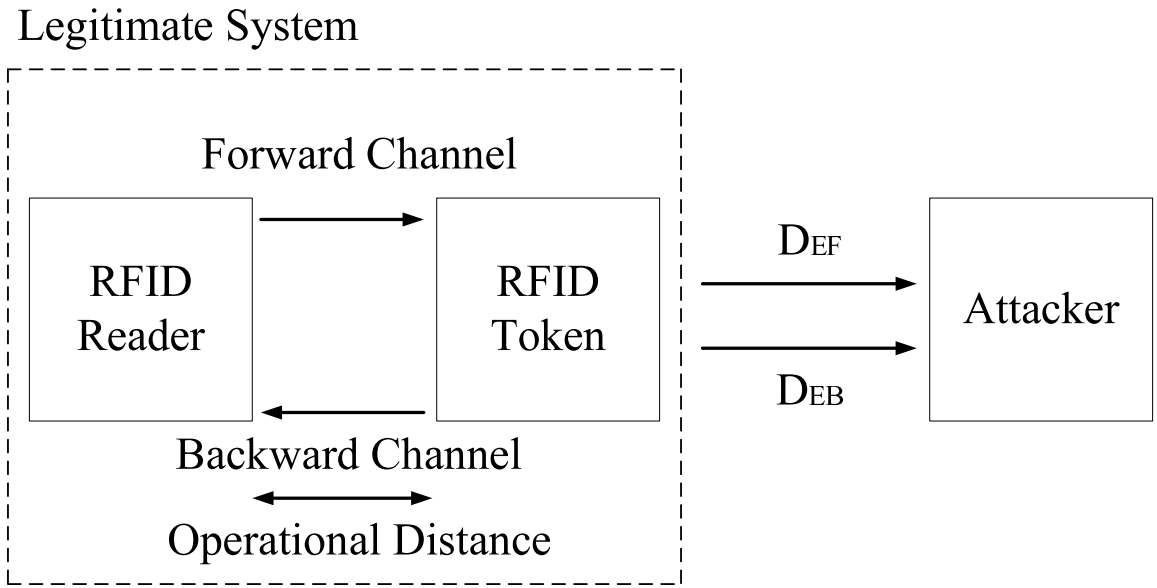


- Eavesdropping and skimming often listed as threats to RFID
- Some semantics: ‘Recovered’ or ‘Retrieved’ data sounds like eavesdropping while ‘Read’ should imply skimming

Ambiguity: What is ‘RFID’?

- Several technologies
  - ISO 14443 A/B
  - ISO 15693
  - ISO 18000
  - ISO 18092
  - EPC
- Different applications
  - product tags
  - tickets – single/multi-use
  - credit cards
  - travel documents

Ambiguity: What ‘distance’?

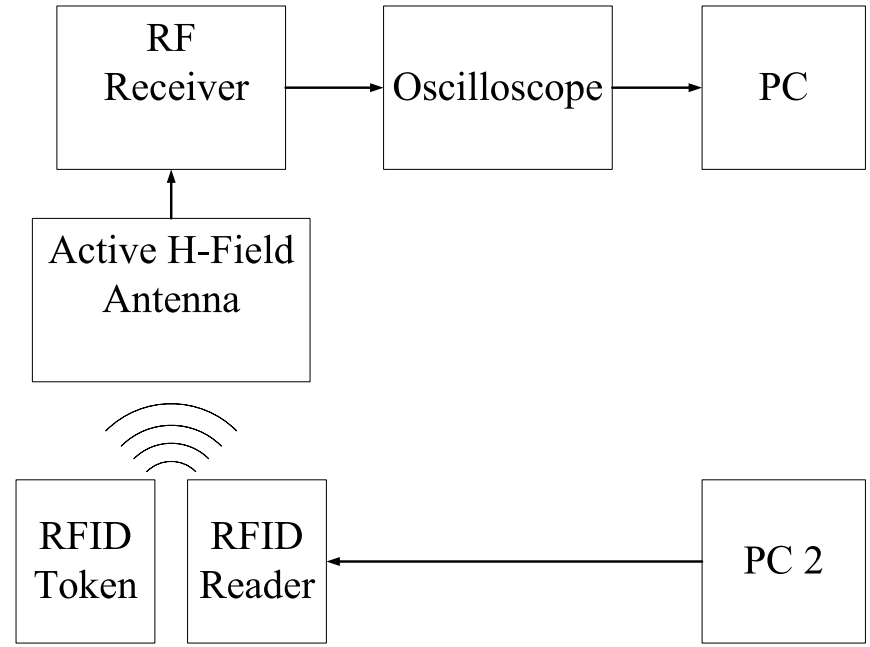


- The distance at which an attacker can detect a transaction
- The distance at which an attacker can reliably recover the data sent on the forward channel
- The distance at which an attacker can reliably recover the data sent on the backward channel

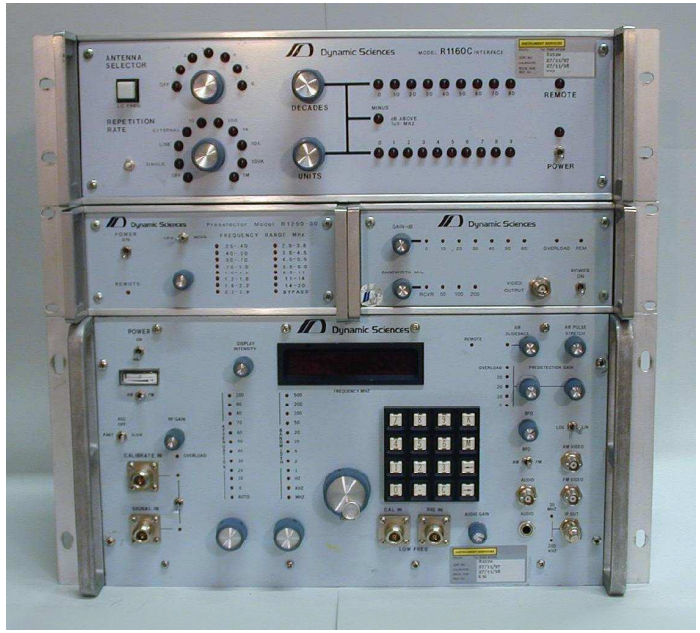
Other Issues

- Document the method – equipment, setup, data recovery?
  - Simulation/calculation still requires a well documented and substantiated model
  - Practical implementation and results probably more trusted
- What is the attack environment – in a field, noisy lab, shielded chamber?
- Put the report somewhere accessible – rumours are often worse than facts

Experimental Setup

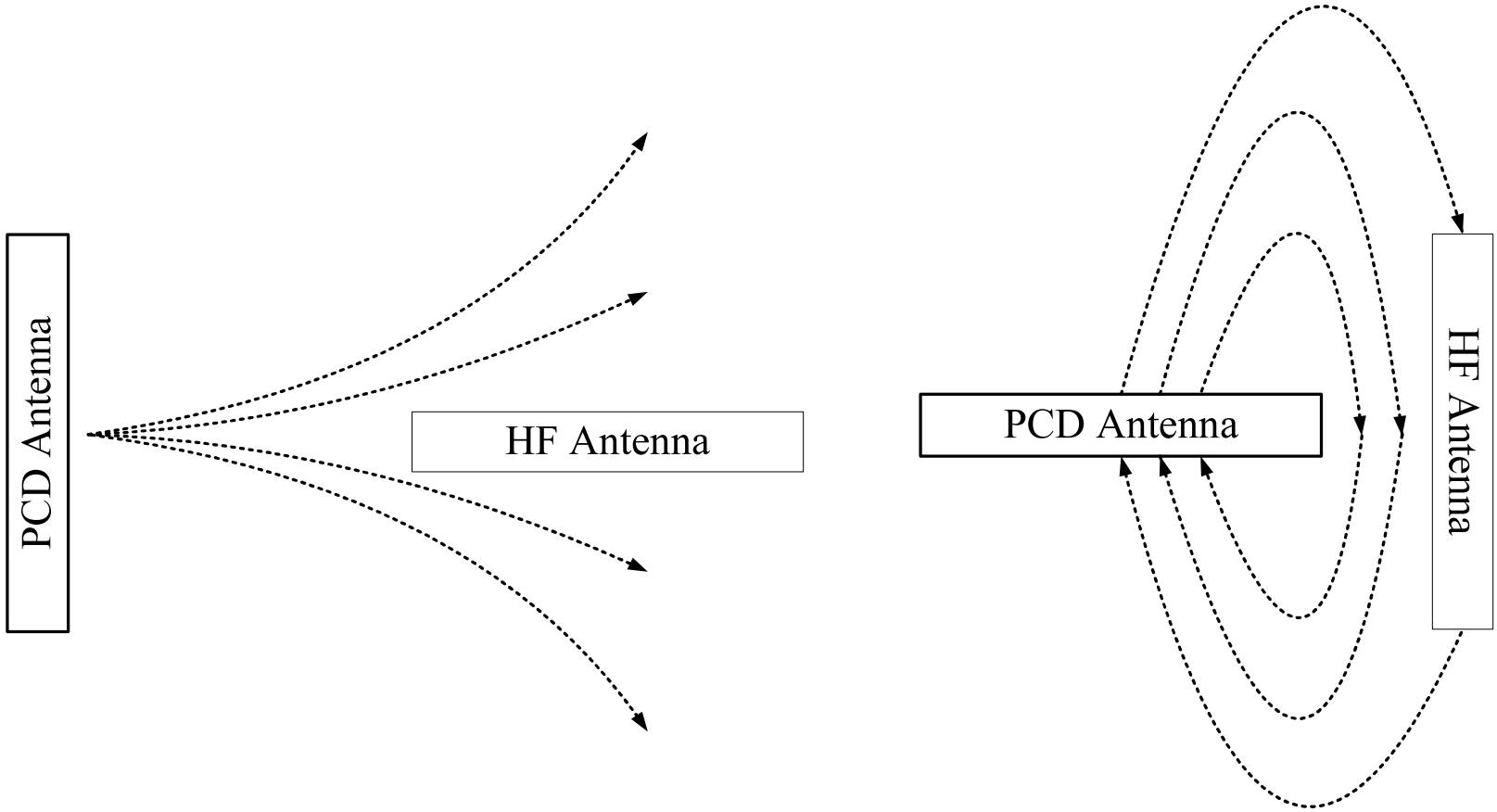


RF Equipment



- Dynamic Sciences R-1250 Wide Range Receiver (100 Hz to 1 GHz)
  - Selectable bandwidth (50 Hz to 200 MHz), AM/FM/IF output
  - RF and pre-detection gain (50 dB and 30 dB respectively)
- R-1150-10A Portable Antenna Kit
  - H-field ferrite core antenna (10 MHz to 30 MHz)

Antenna Orientation

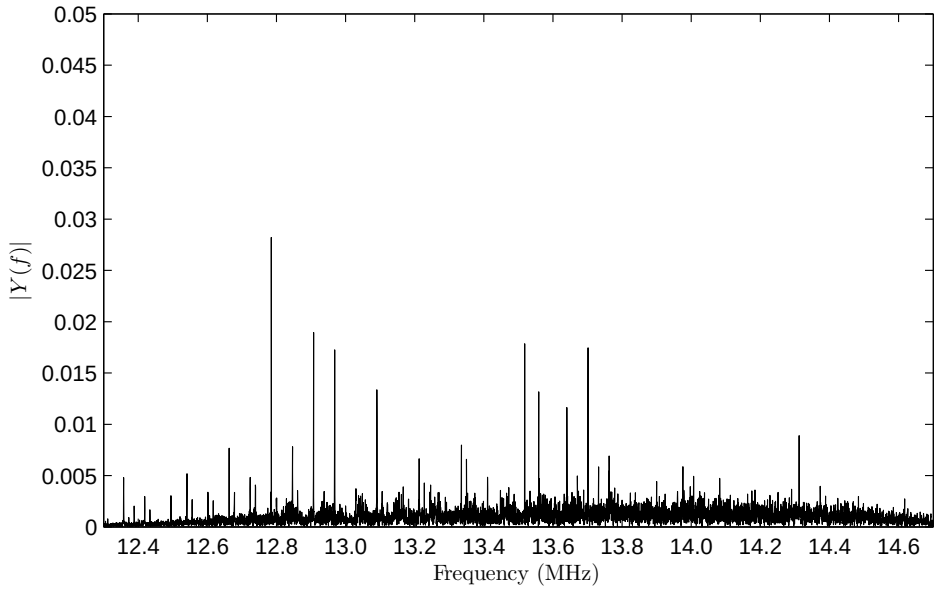


- Ideally H-field lines should go though the antenna...leads to decent directional effect

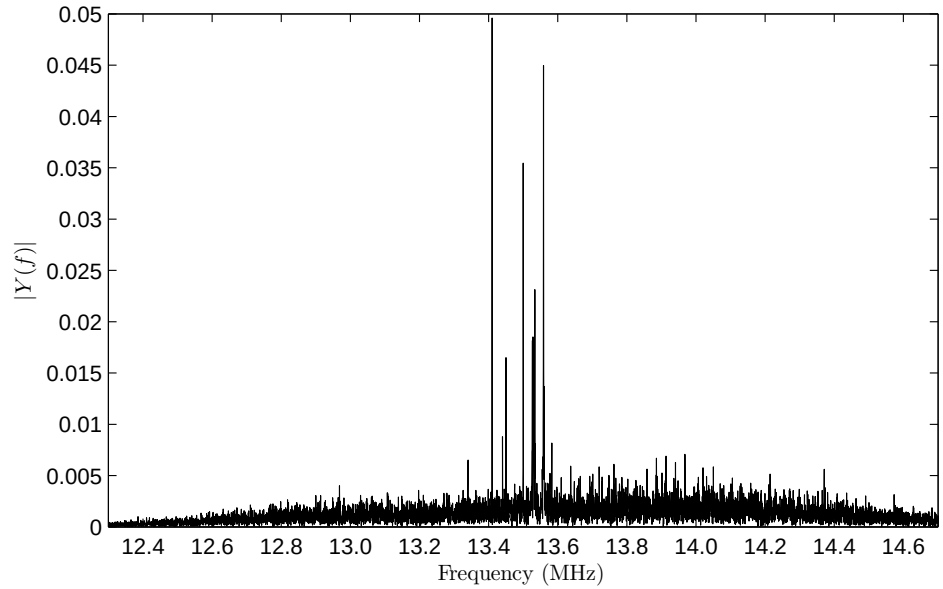
HF RFID Readers/Tokens

- Reader
  - ACG Multi-ISO RFID Reader
  - Antenna dimension: 9 cm $\times$ 6 cm
- Tokens
  - 14443A: NXP Mifare Classic
  - 14443B: Contactless payment card (unknown manufacturer)
  - 15693: NXP I-Code
- These specific products are not especially vulnerable – just what I had available

Environment



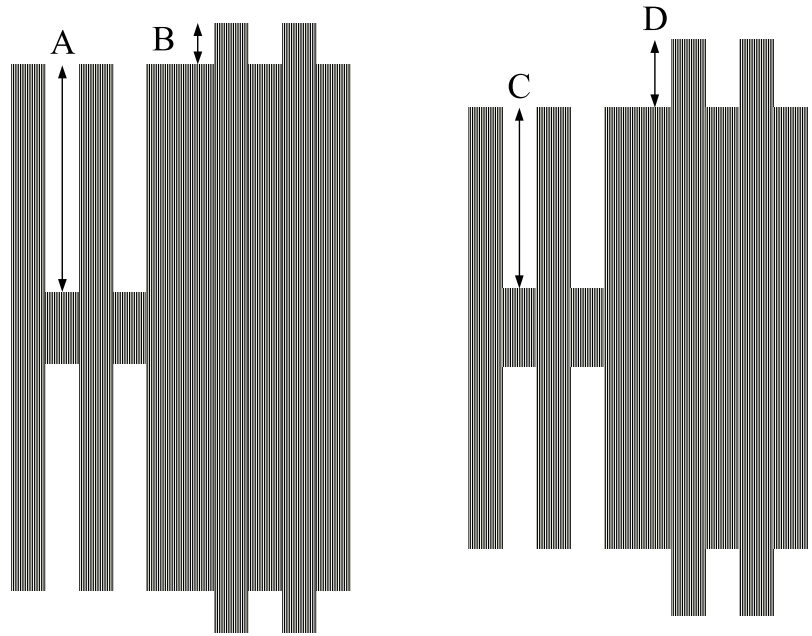
Hardware lab corridor



Main entrance hall

- Locations have different background noise profiles
- This effects eavesdropping success...

Additional experimental variation

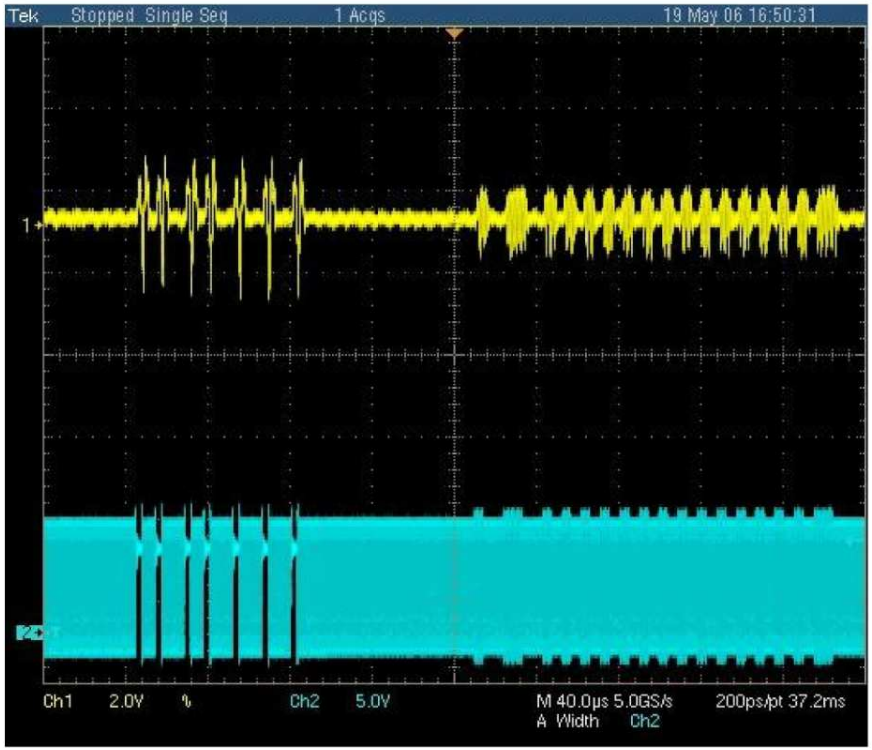


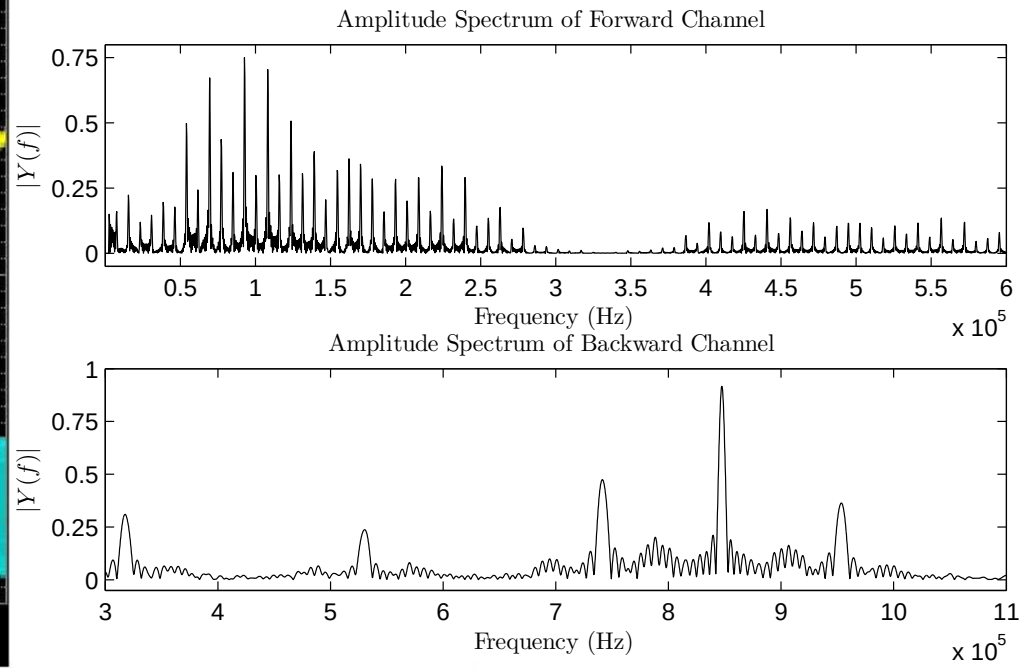
- Influences on carrier amplitude and modulation index/depth
  - Coupling – token orientation, antenna tuning
  - Power Consumption
- Parameters of the reader – antenna size, transmitted power
- Have not yet investigated this fully...

Method

- Generate reference data
  - Identify spectrum of interest
  - Determine whether the experiment was successful
- Calibration and signal capture
  - Set up the receiver
  - Capture and store output of the receiver
- Data recovery
  - Implement some signal processing

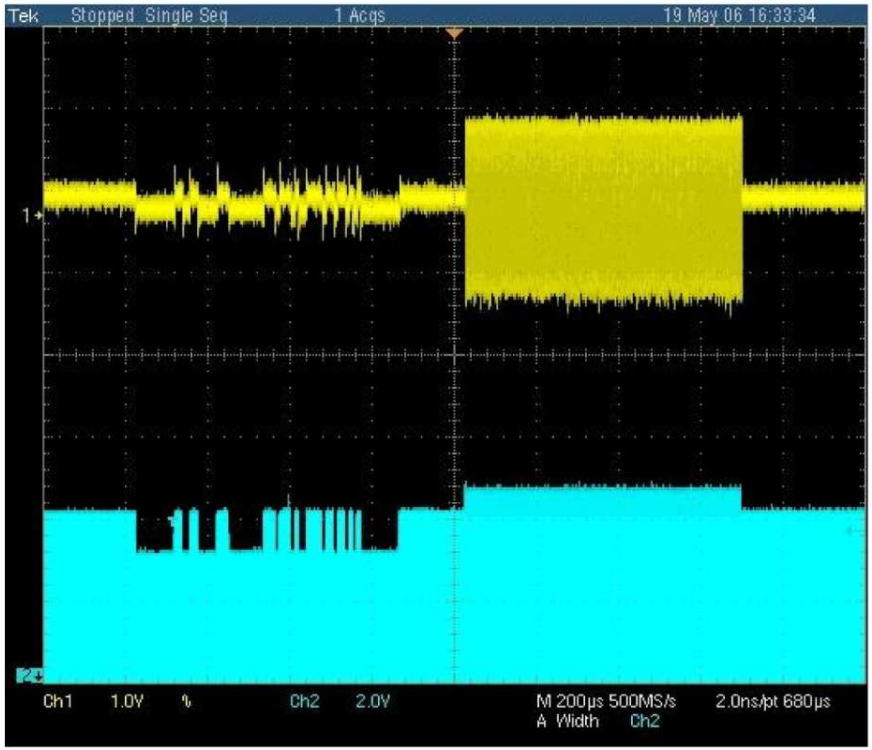
Reference Data: ISO 14443 A

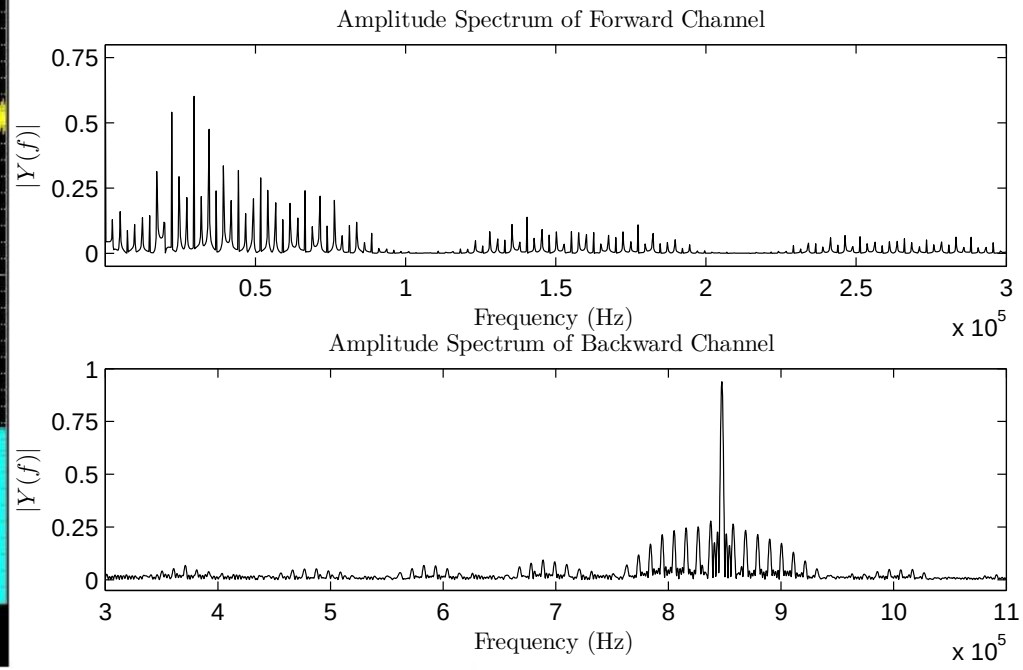




- Forward: 106 kbit/s Modified Miller (3μs pulses), 100% ASK
- Backward: 106 kbit/s Manchester, ASK onto 847 kHZ sub-carrier, carrier modulation index of 8–12%

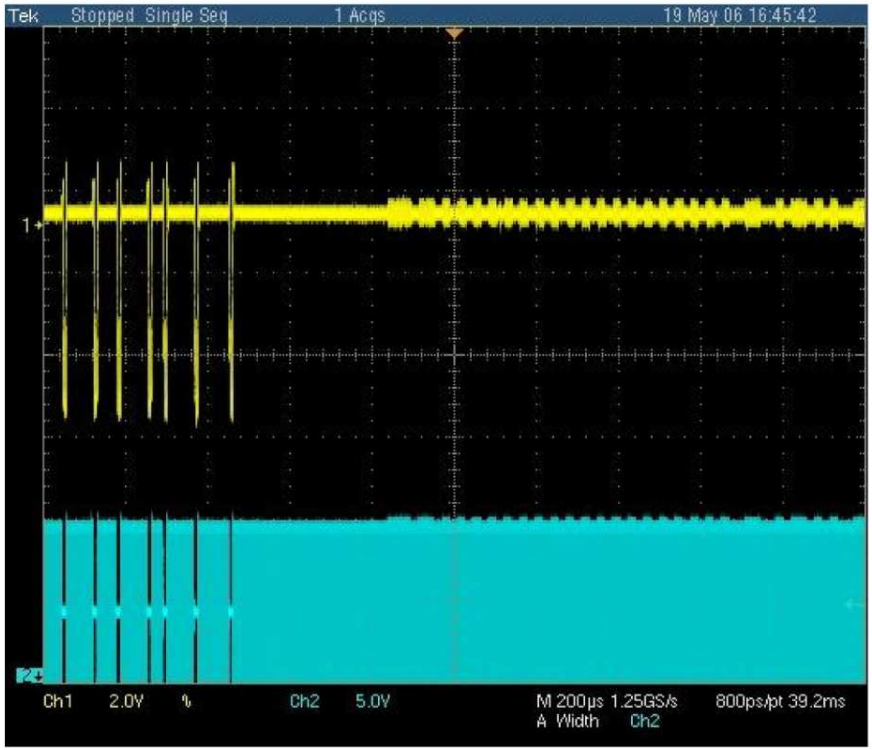
Reference Data: ISO 14443 B

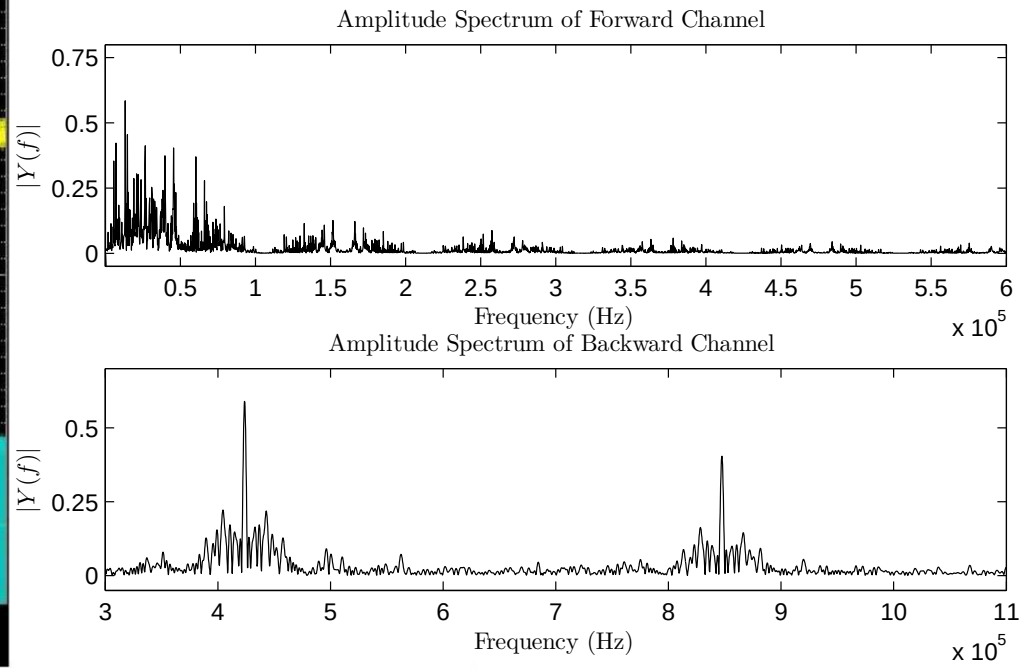




- Forward: 106 kbit/s NRZ, 10% ASK
- Backward: 106 kbit/s NRZ, BPSK onto 847 kHZ sub-carrier, carrier modulation index of 8–12%

Reference Data: ISO 15693





- Forward: 26.48 kbit/s ‘1 of 4’ PPM (9.44 µspulse), 100% ASK
- Backward: 26.48 kbit/s NRZ, ASK onto 423 kHZ sub-carrier, carrier modulation index of 8–12%

Capture and Calibration

- Oscilloscope Settings
  - Sample 30 MHz IF output at 100 MS/s for a duration of 320 ms
  - Manual trigger
- Receiver Settings
  - f_c = 13.56 MHz, BW = 2 MHz
    (try filter side-bands in software)
  - f_c = 14.4 MHz and 13.98 MHz, BW = 500 kHz and 200 kHz
- Calibration
  - Receiver gain adjusted with analog knob (gain therefore measured with a reference input signal)

Data Recovery

N correlators project the received signal $r(t)$ onto base functions $f_k(t)$

$y_k = \int_0^T r(t) f_k(t) d_t, \; k = 1, 2, \ldots, N$

Rectangular base function simplifies to integrator:

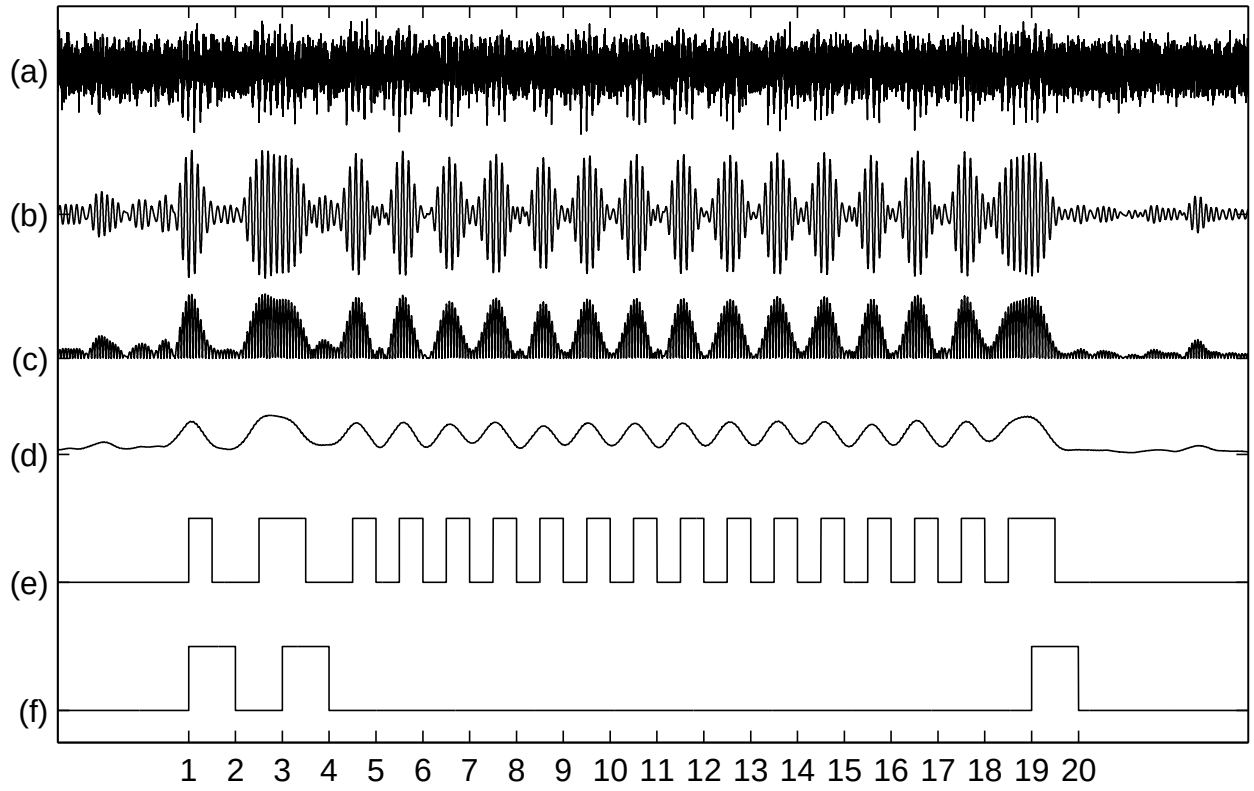
$y_k = \frac{1}{\sqrt{T}} \int_0^T r(t) d_t$

ISO 14443A: Forward channel $T = 3\ \mu\text{s}$, backward channel $T = \frac{1}{212\ \text{kHz}} = 4.72\ \mu\text{s}$

ISO 14443B: Forward channel $T = \frac{1}{106\ \text{kHz}} = 9.44\ \mu\text{s}$, backward channel $T = \frac{1}{106\ \text{kHz}} = 9.44\ \mu\text{s}$

ISO 15693: Forward channel $T = 9.44\ \mu\text{s}$, backward channel $T = \frac{1}{52.96\ \text{kHz}} = 18.88\ \mu\text{s}$

Data Recovery(2)



- Example of recovering data from a noisy signal

Results

	ISO 14443A	ISO 14443B	ISO 15693
Entrance hall			
1 m	FB	FB	FB
3 m	Fx	xB	Fx
5 m	Fx	xx	Fx
10 m[a]	Fx	xx	Fx
Lab corridor			
3 m	FB	FB	Fx
4 m	Fx	xB	Fx

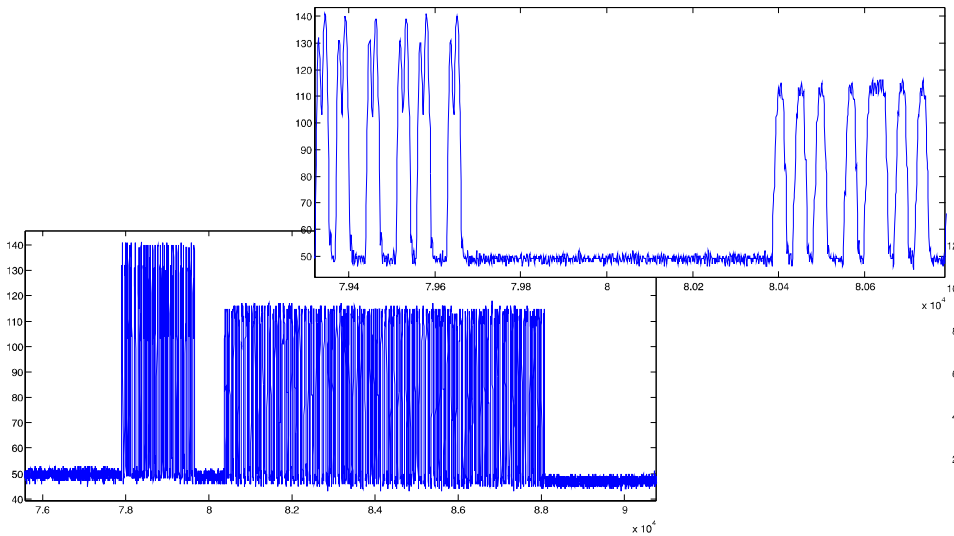
- F – Forward channel, B – Backward channel

a: Reader/Antenna in same horizontal plane

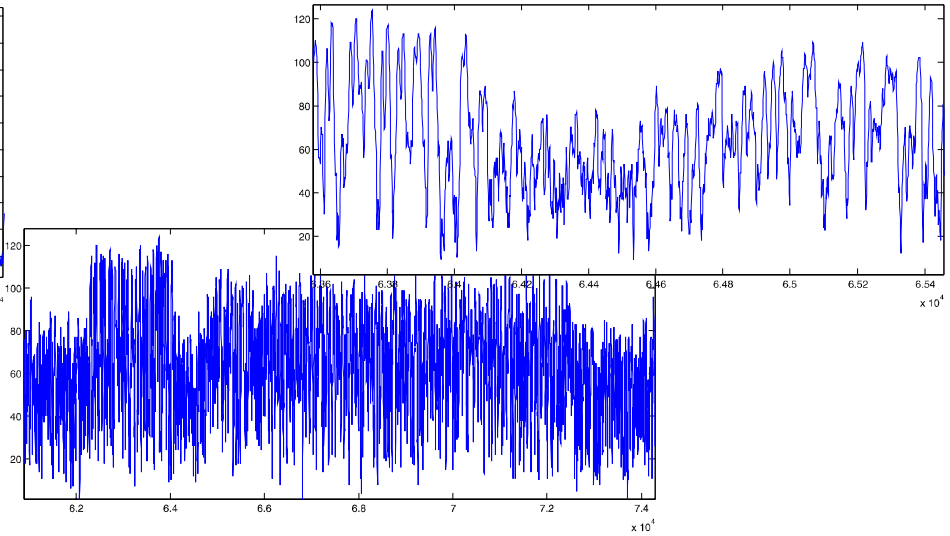
Finke and Kelter (2006)

- H-field loop, receiver ($f_c \approx$ 14.50 MHz, BW = 300 kHz)
- NXP Pegoda Reader, ISO 14443 A token
- Environment: Office/lab

Finke and Kelter (2006)



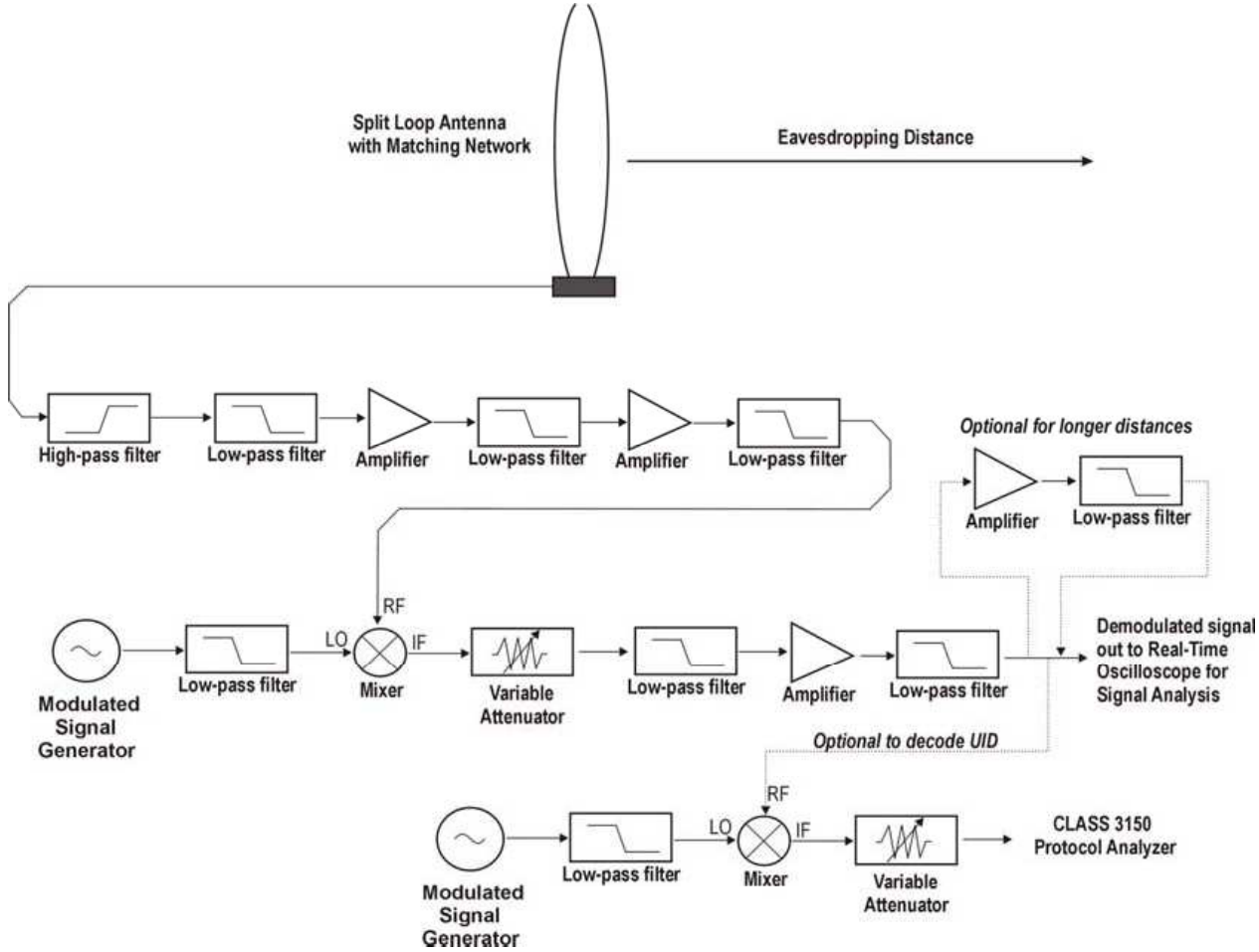
Trace 1m



Trace 3m

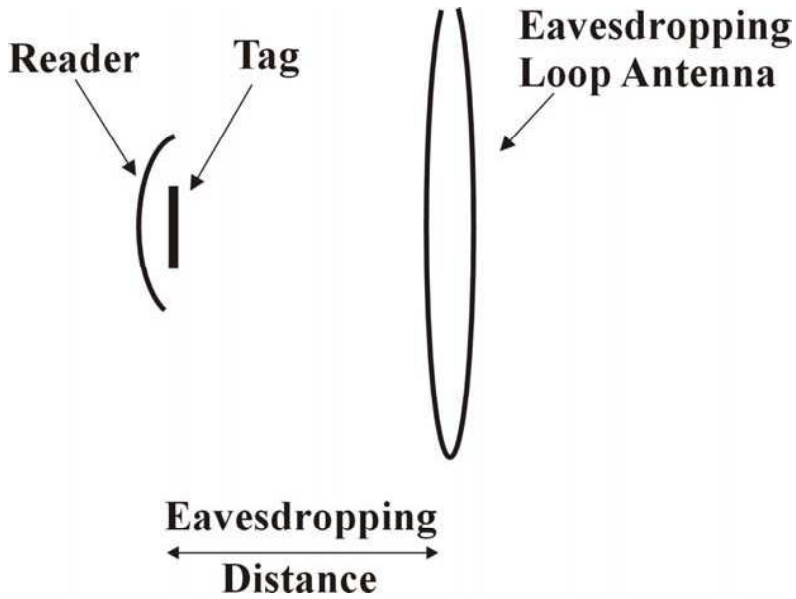
- Eavesdropping successful to 2 m
- If implemented additional data recovery could be 3 m?

Guerrieri and Novotny (2006)

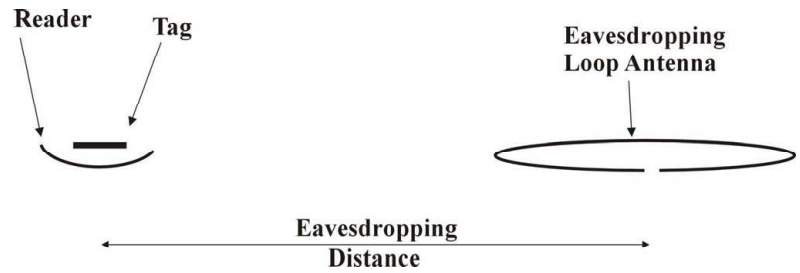


- Equipment is documented but not in too much detail

Guerrieri and Novotny (2006)



Close range



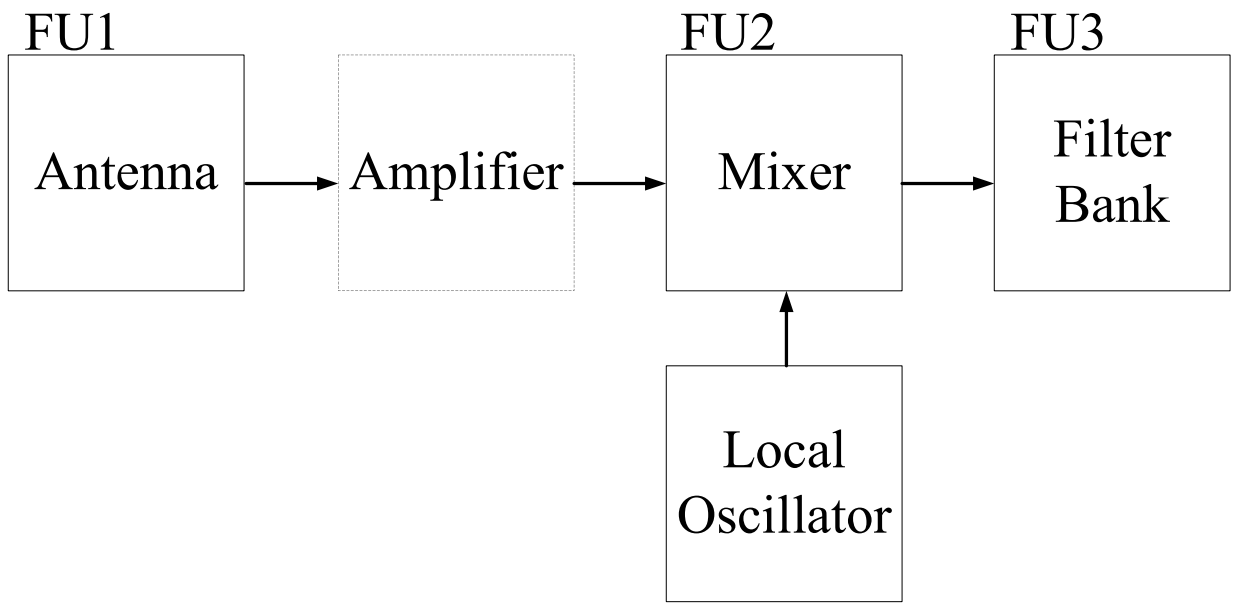
Long range

- Experimented with two antenna/reader orientations

Guerrieri and Novotny (2006)

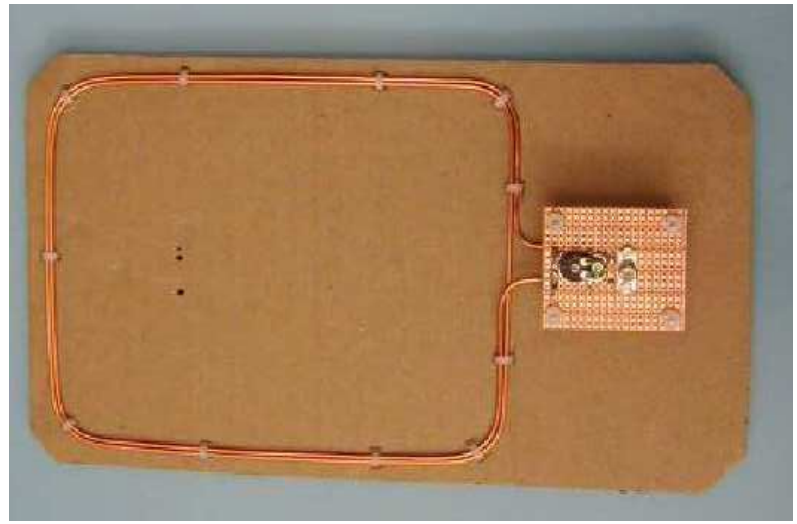
- RFID equipment
  - NXP Pegoda reader
  - Seven ISO 14443A tokens (4 manufacturers)
- Data recovery
  - Receiver connected to protocol analyser
  - Eavesdropping successful if SNR $>$ 6 dB
- Results
  - Close range setup: 6–6.5 m
  - Long range setup: 8–15 m
- Open questions
  - What is the environment? Noise figures very good...
  - What would the distance be with better data recovery?

Build your own receiver



- Is the attack really feasible for attackers?
- RFID at the easier side of the RF design space
- No need to spend much money on commercial receivers for simple experiments/attacks
- Building a receiver for 50–60cm range relatively simple

Making Antennas

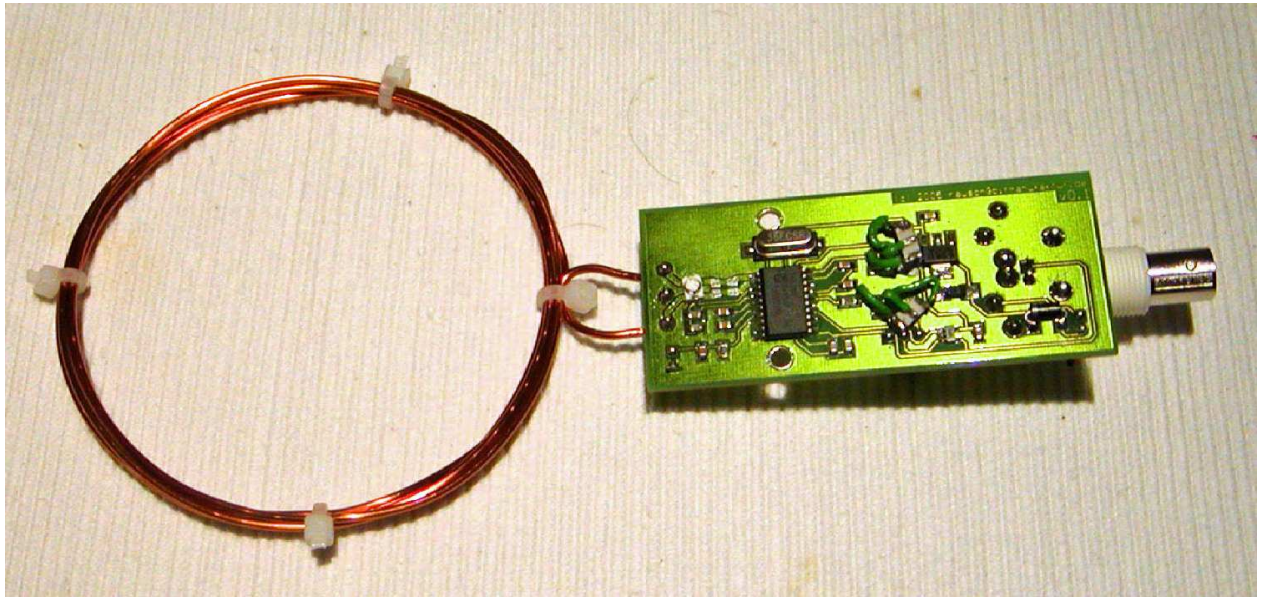


- Instructions
  - Books: J.J. Carr. Practical Antenna Handbook
  - Application notes: TI's Antenna Cookbook

Mixer and Filters

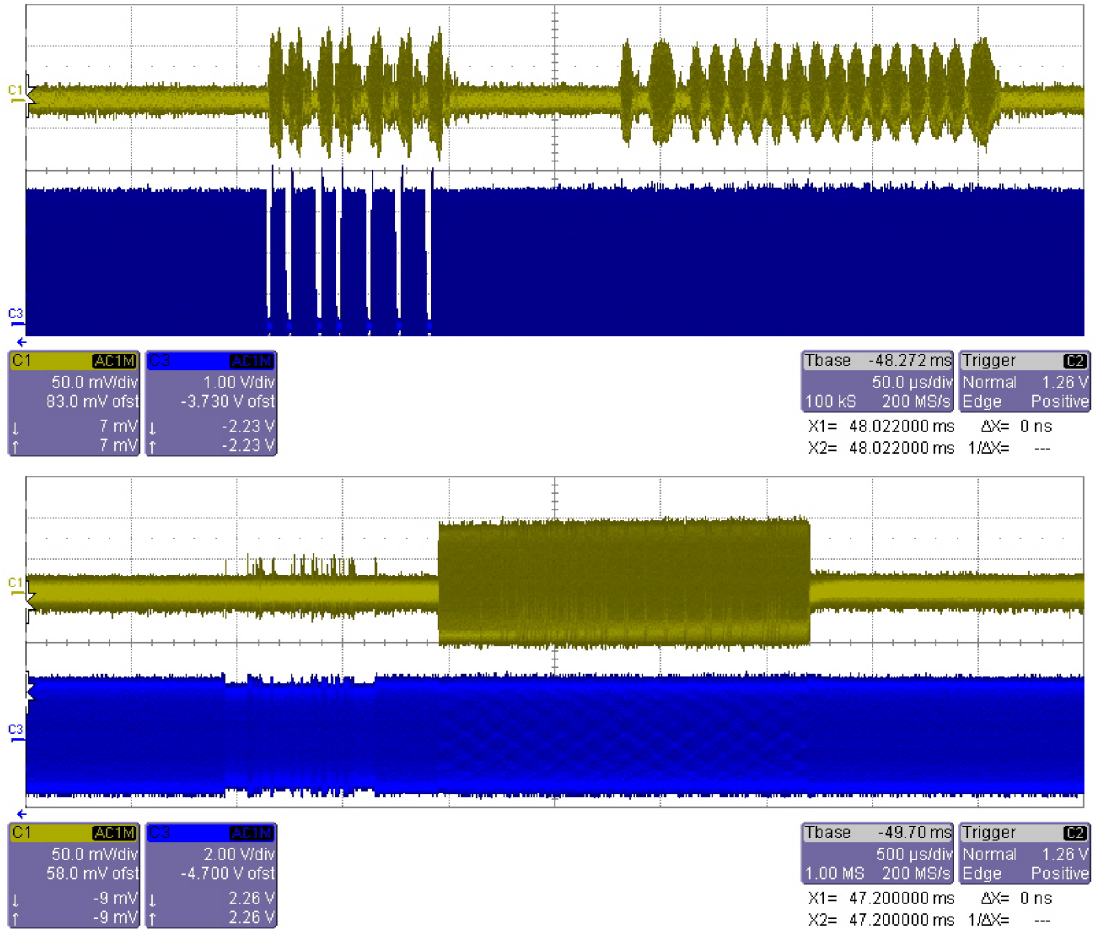
- RF Mixers
  - Buy a suitable IC, cheap and easy to use – e.g. NXP SA615
  - Mix to an IF suitable for filters
- Filters
  - Selection of off-the-shelf solutions – e.g. 10.7 MHz SAW filters
  - Else design and build your own, there are a number of free filter design tools

Reference Designs



- Last resort, use designs that are already available... for example Sniffer at www.opendpcd.org?

Sample Traces



- Backward channel for ISO 14443 A and B

Signal Capture and Data Recovery

- Sampling rate is dependent on the output of the receiver
  - Need to sample at least 2$\times$ IF
  - Directly influences the complexity and cost
    i.e. Cost 2 MS/s ADC $<$ 100 MS/s ADC
- Final signal processing to recover data
  - Store and process later, 8-bit samples at 2 MS/s for 10 s $\rightarrow$ 20 MB
  - 'Real-time' demodulator/decoder $\rightarrow$ How quick can it be done?
  - Basically a storage vs processing speed trade-off
- Hardware requirements are not unrealistic

Conclusion

- Presented details of a possible eavesdropping setup
  - Hope this helps understanding of the attack
  - Not claiming this is the best or only approach but provides a reference, which aid others to‘re-create’ similar experiments
  - I hope someone improves on it!
- Focus less on absolute distance
  - Just too many variables involved
  - Researcher with the best equipment wins
- Concentrate on feasibility and environmental parameters
  - Cost/size/skill required by attacker to practically implement
  - To what extent do external factors hinder or aid an attack?

Future Work

- Novel hardware implementation
  - Can you achieve the same performance as a commercial receiver in less space, for less money?
- Data recovery routines
  - Noise resistant receivers, hardware implementation, etc.
- Are E-field measurements useful?
- Eavesdropping for other RFID standards?
  - NFC Active mode $\rightarrow$ Effectively two forward channels
    Is this mode more vulnerable to eavesdropping?
  - Similar experiments for UHF (and other) RFID

Done

Thank you, and any questions?

gerhard.hancke@rhul.ac.uk