Practical Attacks on Proximity Identification Systems

Gerhard P. Hancke

May 26, 2006

UNIVERSITY OF CAMBRIDGE

RFID Devices

- Applications
  - Logistics
  - Access control
  - ICAO e-Passport
  - Europay/Mastercard/Visa
- Standards
  - Frequency
  - Data encoding
  - Range

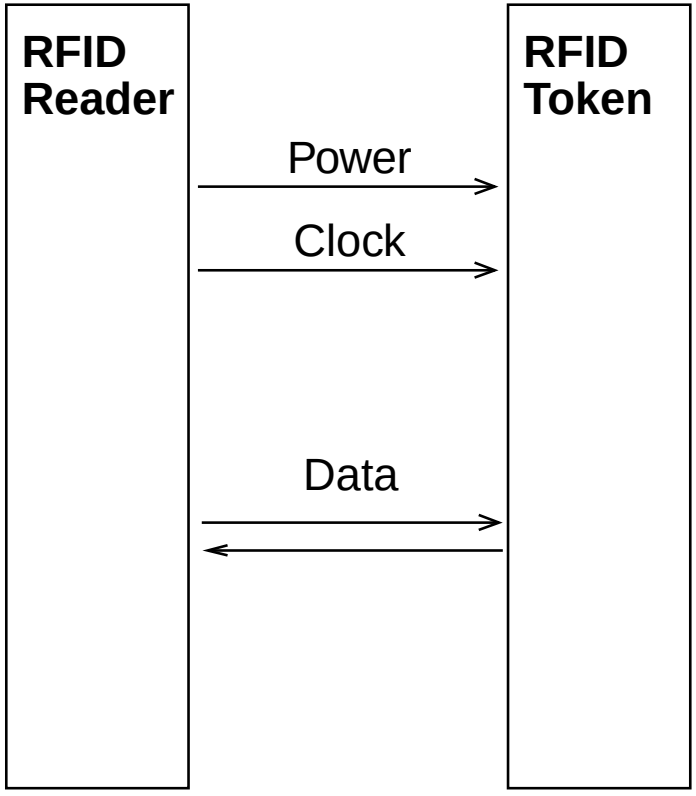
Security Concerns

- Various attacks proposed
  - Kfir and Wool (2005)
- Prominent media claims
  - ACLU – read ‘similar’ RFID to e-passport at 1 m
  - NIST – read e-passport RFID at 9 m
  - DEFCON – eavesdropped RFID at 20 m
- Confusion ??
  - RFID type
  - Definition of distances
  - Experimental setup

Attack Overview

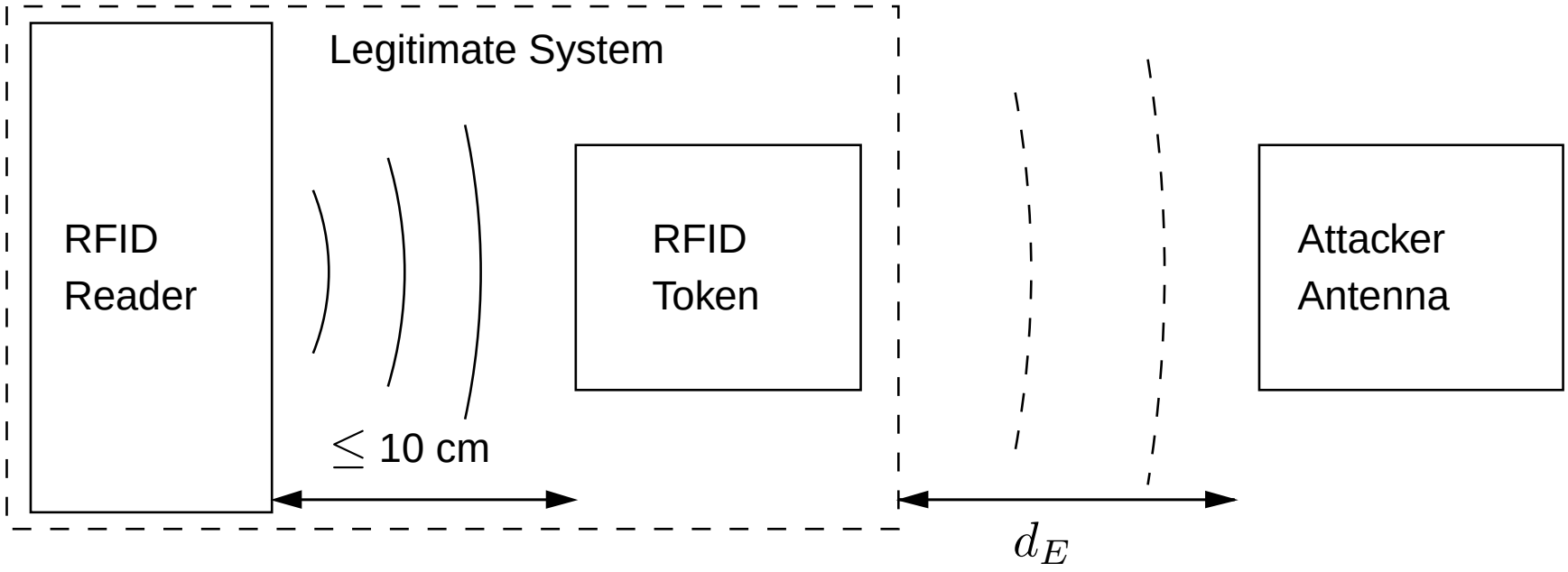
- Proof of Concept
  - What can actually be implemented?
  - Left room for improvement...
- Attacks
  - Passive Eavesdropping
  - Active Scanning (or skimming)
  - Relay Attacks

“Proximity” Identification



- ISO 14443 A (and B)
- 13.56 MHz
- Reader → Token
  - Modified Miller, 106 kbps
  - 100% ASK
- Token → Reader
  - Manchester, 106 kbps
  - ASK modulated subcarrier
  - Load modulation

Passive Eavesdropping



- An attacker can eavesdrop a two-way communication sequence from distance d_E
- Further considerations
  - $d_{R \to T}$, Reader $\to$ Token communication
  - $d_{T \to R}$, Token $\to$ Reader communication

Passive Eavesdropping: Setup

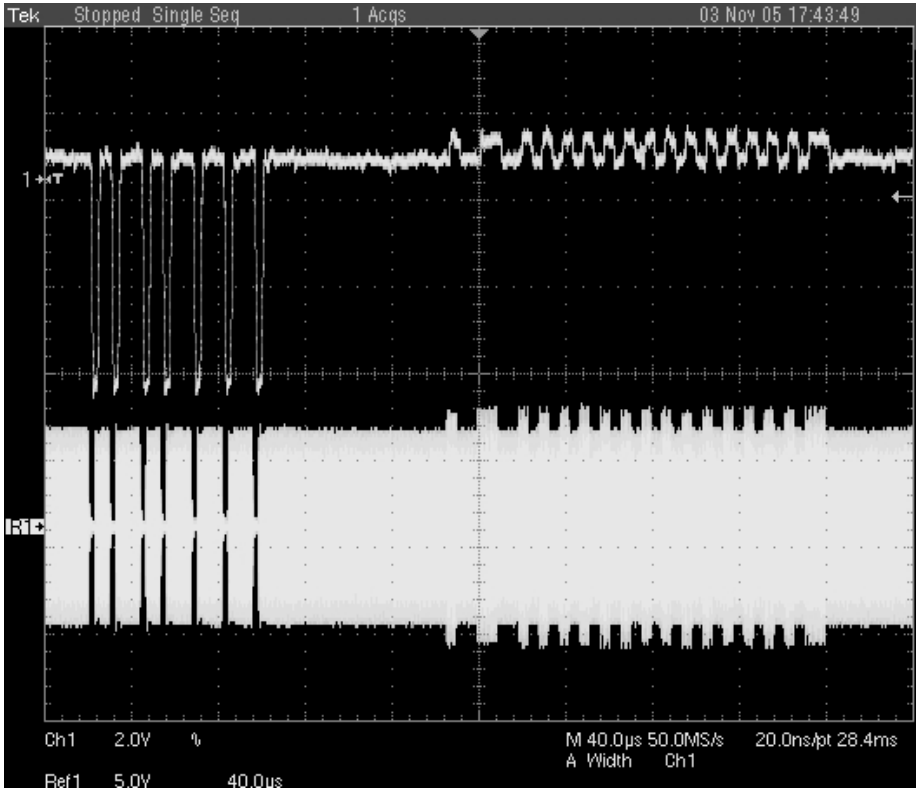
RFID Reader

- 14443 A compatible reader
- Philips MF RC530
- 60x45 mm loop antenna

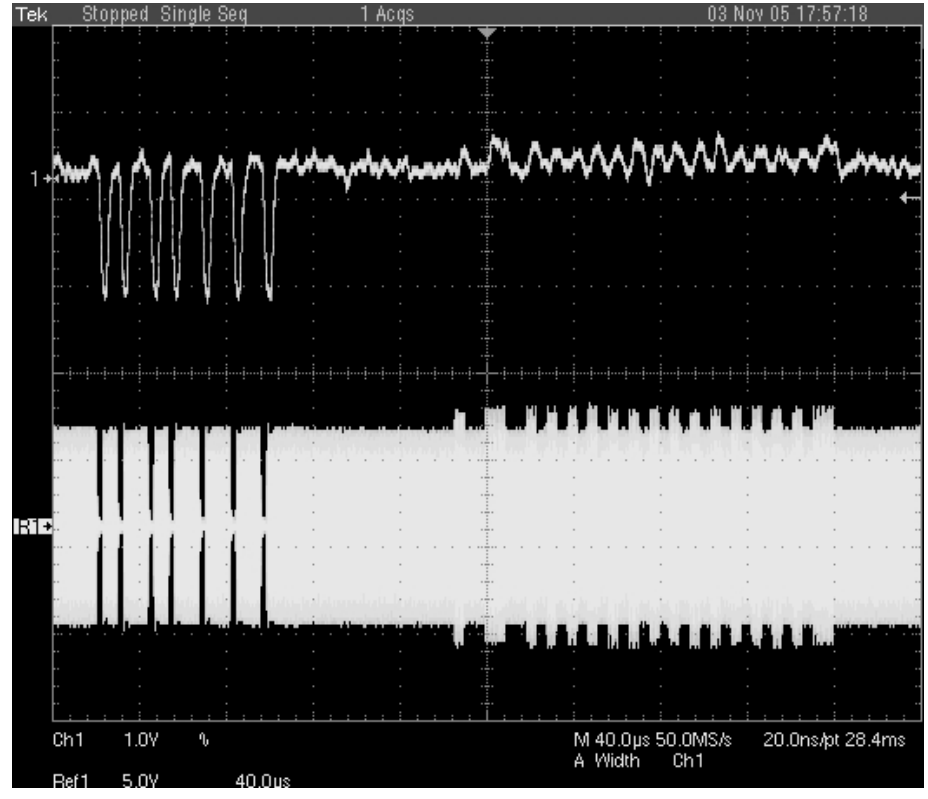
H-field Antenna

- Dynamic Sciences R-1250 Wide Range receiver
- Antenna: 10 MHz – 30 MHz

Passive Eavesdropping: Results

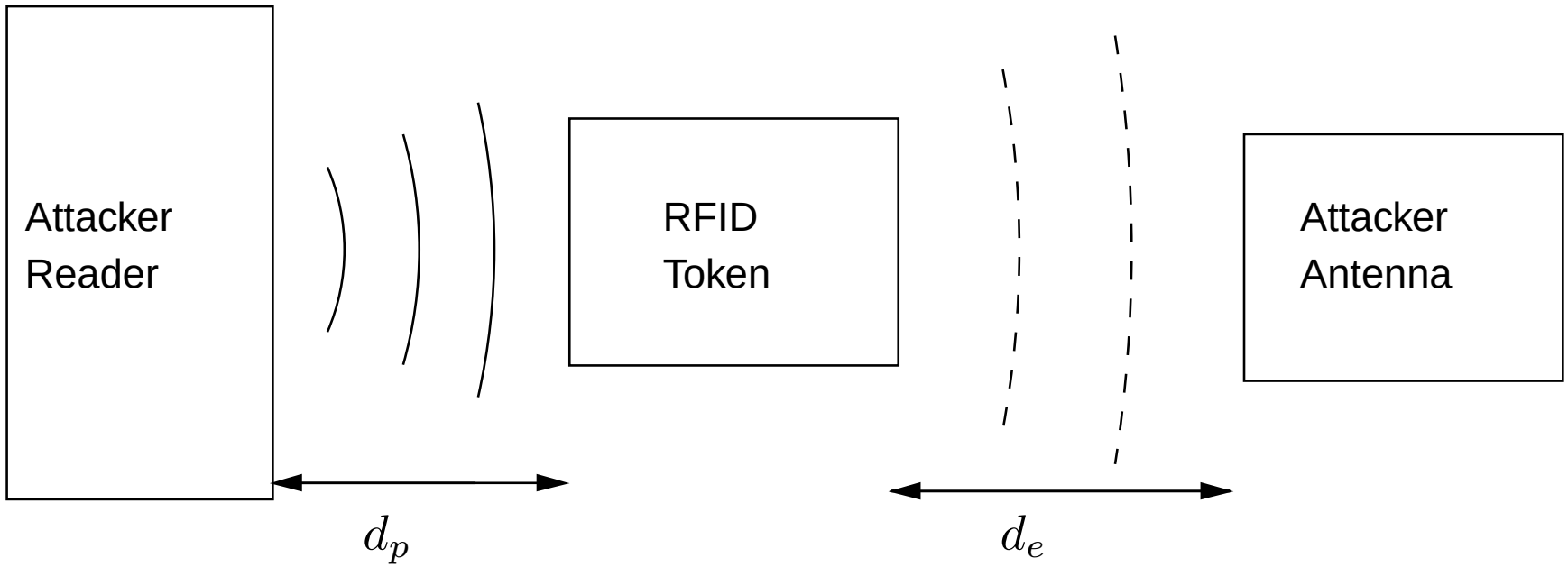


- $d_E = 110$ cm
- Limited by Token $\rightarrow$ Reader
- Simple comparator used



- $d_E = 400$ cm
- Bit errors in data. $d_E > 400$ cm

Active Scanning



- d_p, power and communicate with the token
- d_e, recover the token's response
- The attacker controls Reader $\rightarrow$ Token communication

Active Scanning: Setup

- Same reader as passive eavesdropping
- Simple matched loop antennas (A5, A4, A3)
- E-type amplifier (0.5 W, 1 W, 2 W, 4 W)
- Attacker's antenna same system used for passive eavesdropping

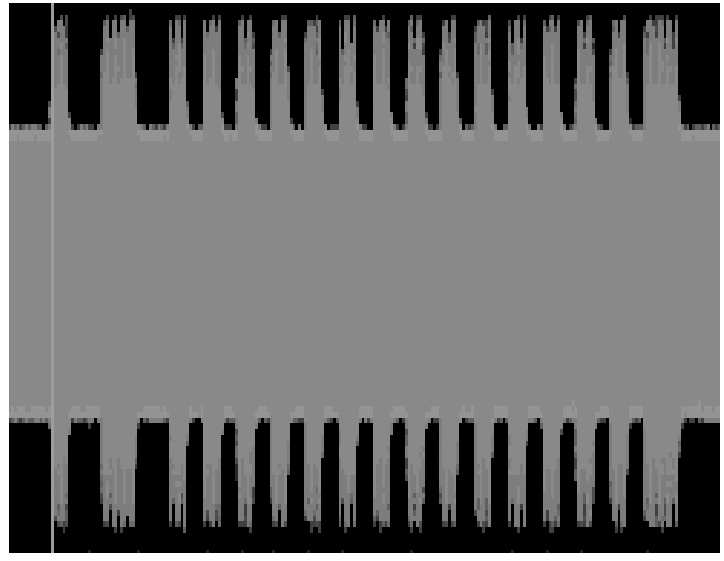
Active Scanning: Reader to Token

	0.5 W	1 W	2 W	4 W
A5 (1/32 m^2)	15 cm	16 cm	17 cm	19 cm
A4 (1/16 m^2)	20 cm	23 cm	23 cm	25 cm
A3 (1/8 m^2)	22 cm	25 cm	26 cm	27 cm

- Used a pick-up coil close go token to verify that it was responding
- d_p is proportional to the antenna radius/transmitted power
- Just increasing the power for a given antenna will eventually yield no additional distance

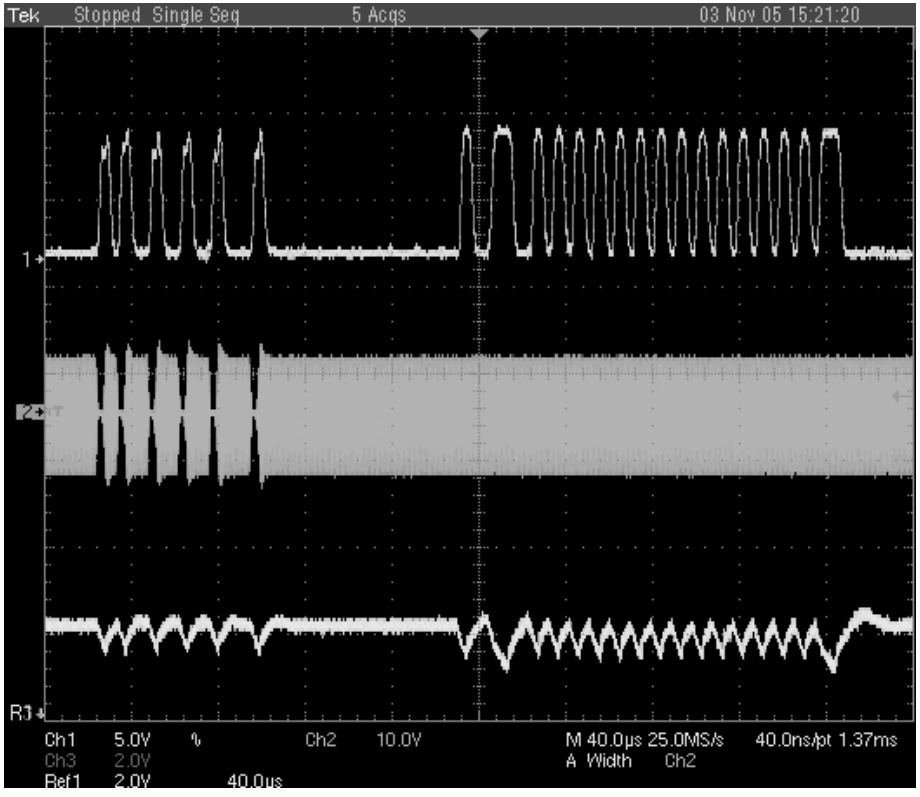
Active Scanning: Token to Attacker

Example of load modulation



- Best result not given by largest antenna and amplifier
  - Increased carrier amplitude complicates recovering the token's response
  - Load modulation amplitude not proportional to carrier

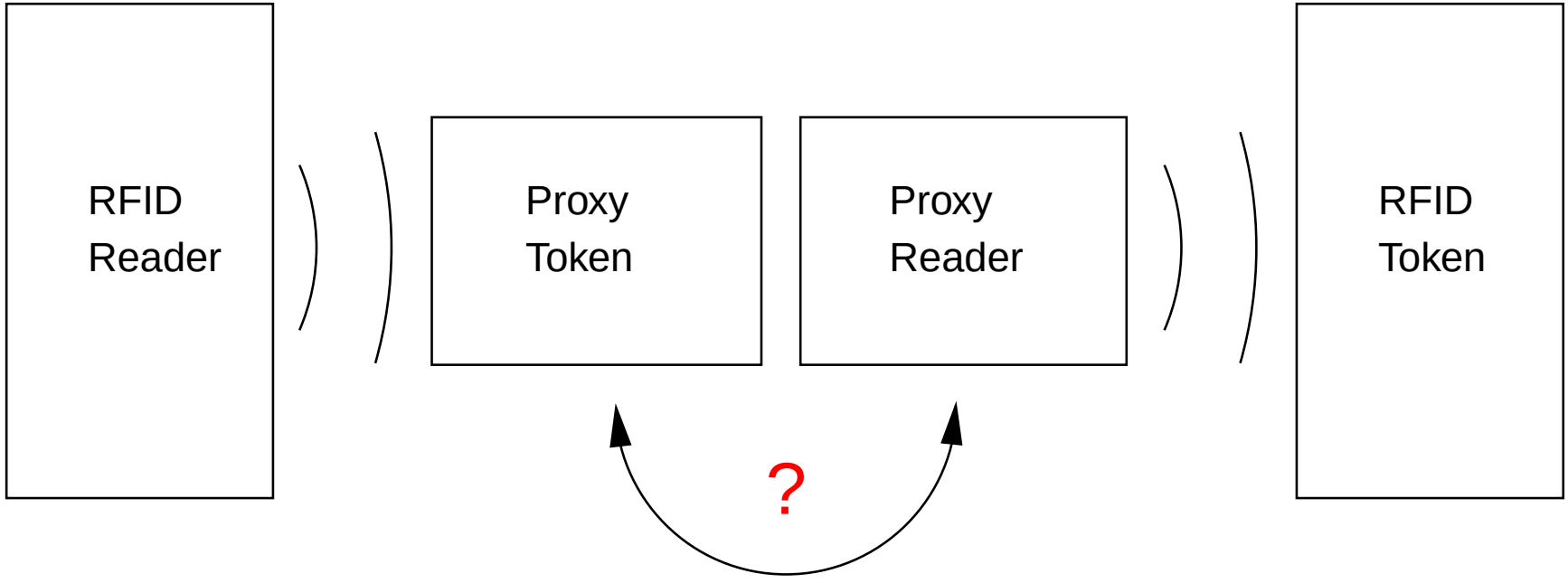
Active Scanning: Results



- A5 antenna with 1 W amplifier
- $d_p = 15$ cm and $d_e = 75$ cm
- Active scanning not as simple

- A5 antenna with 1 W amplifier
- $d_p = 15$ cm and $d_e = 145$ cm
- Still viable attack

Relay attack



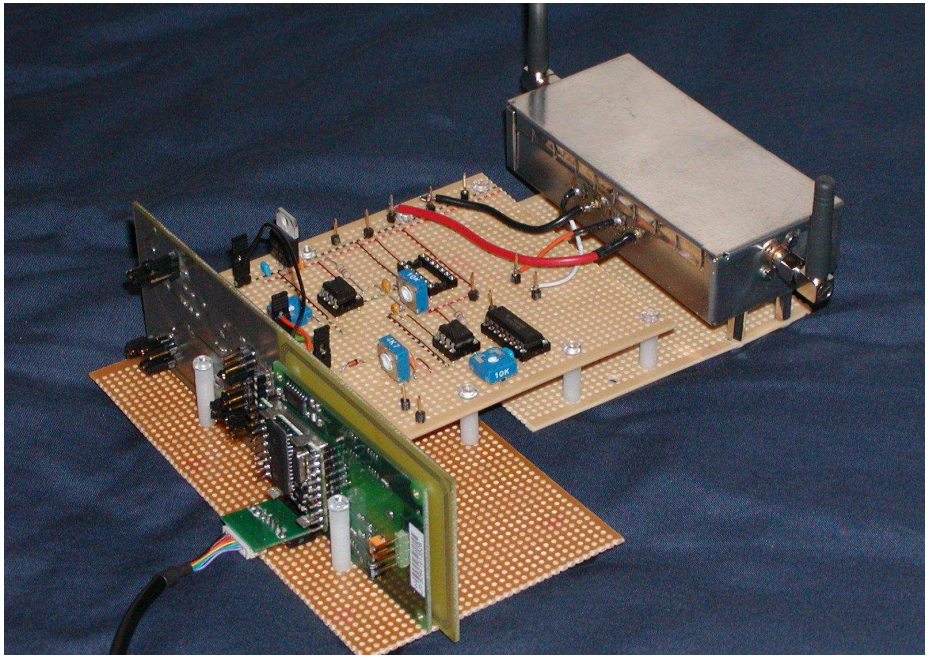
- Data passes through attacker's hardware en route between token and reader

Relay attack implications

- Location Spoofing
  - Attacker uses a valid token in a remote location to gain services
  - Circumvents application layer security protocols
- Data Modification
  - Data is altered on its way between the token and reader

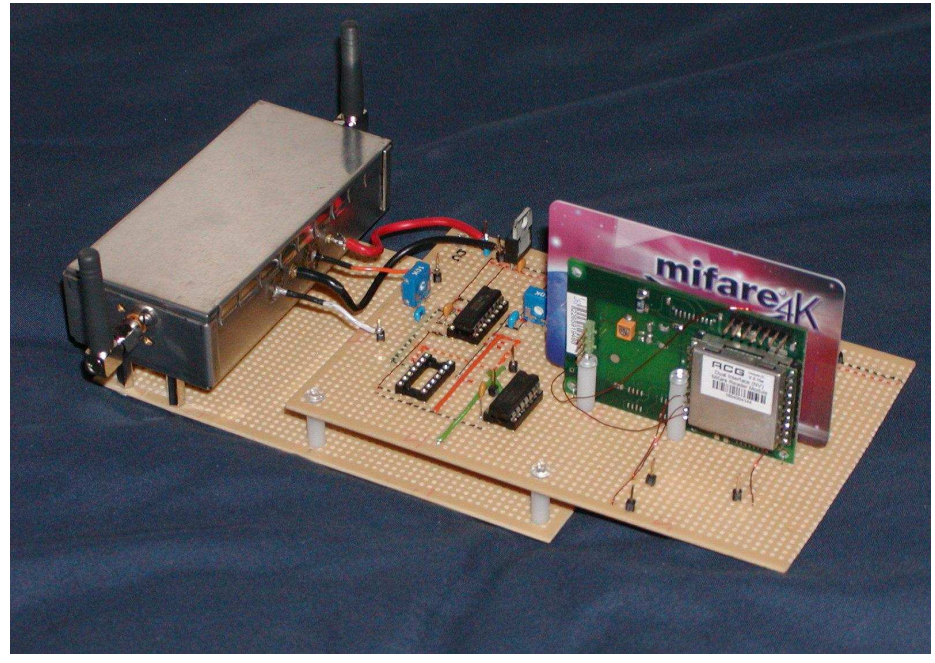
Relay attack: Setup

Proxy Token



- 14443 A/B test card circuit
- Signal processing with discrete components
- Duplex RF link

Proxy Reader



- Commercial reader module
- Reprogrammed with our firmware
- Price $\approx$ $ 100

Relay attack: Results

- Location Spoofing
  - Data relayed over a distance of 50 m
- Data Modification
  - Same experimental setup as before except RF link substituted with FPGA development board
  - Modification of plaintext data, e.g. Token ID
  - Modification of encrypted data
    - One commercial product had an interesting result
    - 1 bit error in ciphertext $\rightarrow$ 1 bit error in plaintext
    - Integrity provided by a CRC which could be modified

Conclusion

- Passively eavesdropped up to 4 m without much effort
  - Token $\rightarrow$ Reader communication the limiting factor
  - Not enough data yet to refute or confirm media claims
- Active scanning, powered token from 15 cm and retrieved response from 145 cm
  - Two antenna attack yield better results
  - More power and larger loop antennas not the solution
- Relay attacks very effective
  - Current mechanisms cannot prevent location spoofing
- More work is needed!

Future work

- Investigate other standards
  - ISO 14443 B
  - ISO 15693
- Improvement of results
  - Application specific receivers, antennas etc
  - Signal processing