Known attacks on RFID systems, possible countermeasures and upcoming standardisation activities.

Klaus Finkenzeller
16.06.2009

Giesecke & Devrient

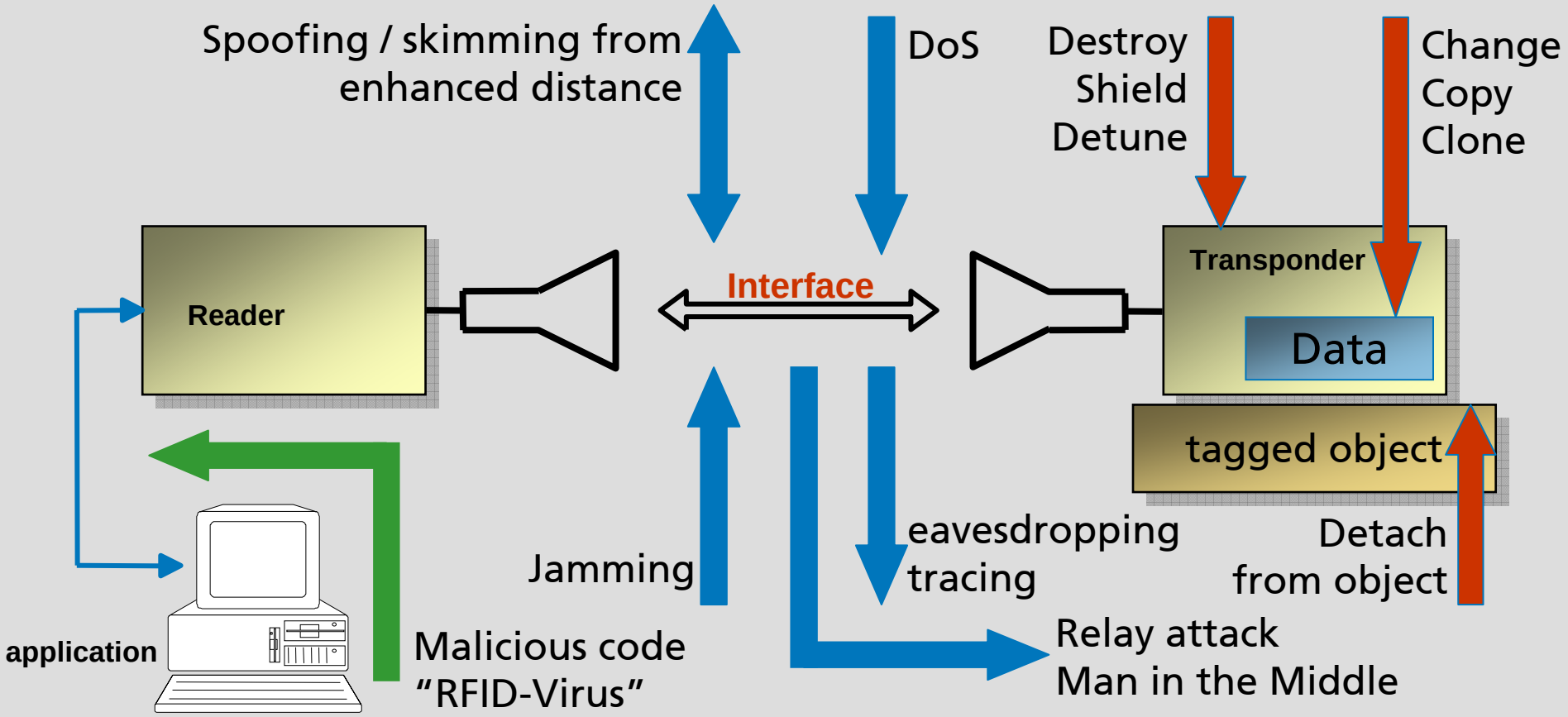
Creating Confidence.

Agenda

- **Attacks on RFID-Systems**
  - Part I: Attacks to destroy and disturb RFID-Systems
  - Part II: Attacks to collect, copy and modify data
  - Part III: Using a tag without physical access: relay attacks
- **Possible countermeasurements**
- **Standardisation activities**

Clustering attacks

Possible attacks on RFID-Systems



Part I: Attacks to destroy and disturb RFID-Systems

- Shielding:
  Use of mechanical means to disrupt function
- Jamming:
  Use of an electronic device to disrupt function
- Physical or electronic destruction of the tag

Attacks physically targeting the transponder

Detuning or shielding the transponder

- Metal foil around the antenna
- Dielectrically detuning of UHF-antennas (reduce reading range)

➔ Only temporarily. Can also be used to protect transponder against unknown or unrequested read attempts

Permanently destroying the Transponder

- Mechanical demolition of the microchip
- Chemical demolition of the transponder
- Clipping microchip off the antenna
- Exposure to strong magnetic fields (e.g., microwave oven)

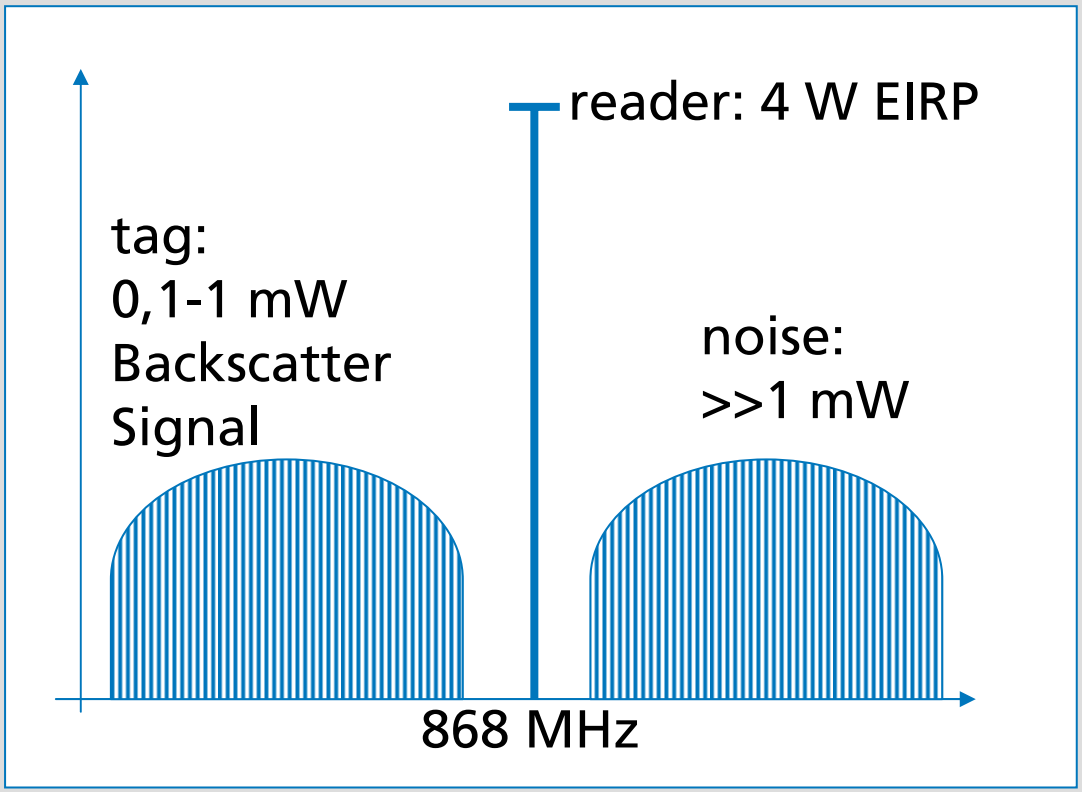
➔ Total lost of the transponder and probably of the stored data

Attacks targeting the RF-Interface: Noise & Jamming

Jamming is the use of an electronic device to disrupt the readers function

Jamming UHF (868 MHz)

- Jamming of sidebands
- Rough estimation of jamming range:
  60 mW 20 m
  250 mW 50 m
  1 W 100 m
- Short reading distance



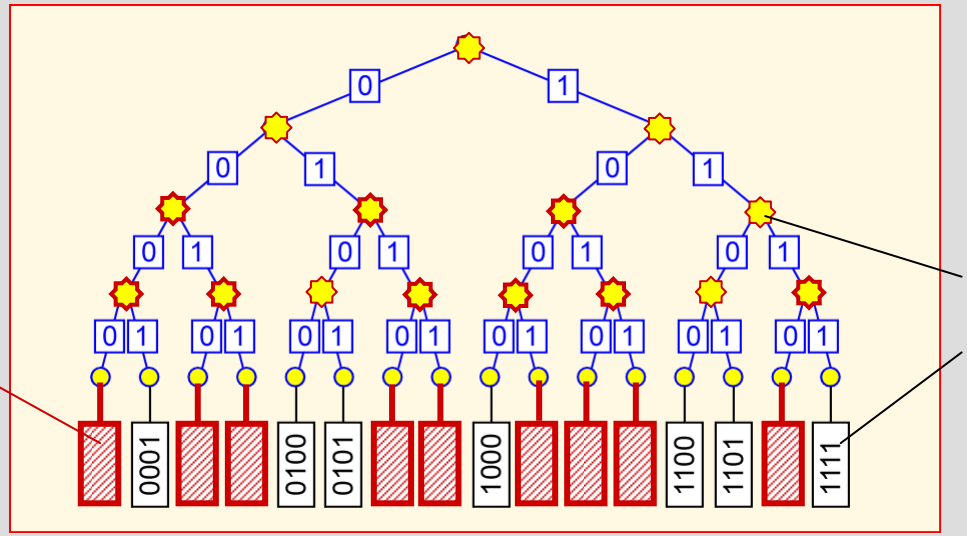
Jamming RF (13.56 MHz)

- Jamming of subcarrier sidebands
  (ISO/IEC 14443:
  13.56 MHz ± 848 kHz)
- At least 1m should be feasible (own measurements)
- Requires large antennas and huge power to gain more distance

Attacks targeting the RF-Interface: Anti-collision

Denial of Service occurs when specially-designed tags are used to overwhelm a reader's capacity to differentiate tags

- Use anti-collision algorithms to fake an infinite number of tags
- Tree walking „blocker tag" can fake a collision at each bit of the UID
- 48 bit Unique ID + 1 ms to read an UID
  ➔ 8925 years to read the whole number range of 2^{48} UIDs
- „Blocker Tag" shown by RSA



Attacks targeting to disturb & destroy: conclusion

Countermeasures?

- No countermeasures known against jamming, blocking, shielding and physical destruction.
- RFID systems have to deal with the potential risk of loss of communication and / or loss of data resulting from the above listed attacks

Part II: Attacks to collect, copy and modify data

- Spoofing:
  Duplicating tag data and transmitting it to a reader.
- Cloning:
  Duplicating data of one tag to another tag.
- Eavesdropping:
  Unauthorized listening / interception.
- Tracing/Tracking:
  Identify the parties that exchange messages (who, when, how often?). Possible attacks to location privacy.
- Skimming:
  Unauthorized access of reading of tag data.

Attacks targeting the Transponder Data: Spoofing

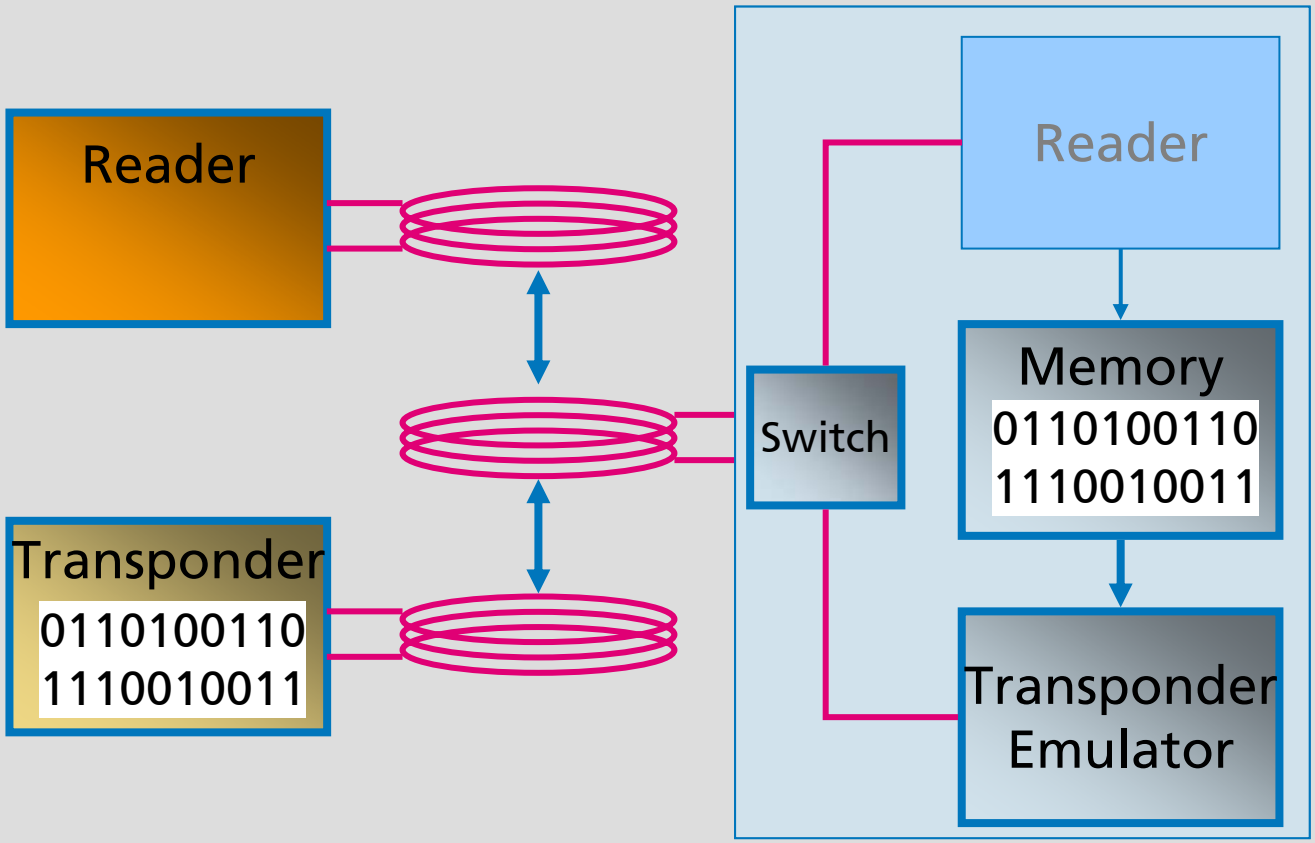
Spoofing is defined as duplicating tag data and transmitting it to a reader

Step 1

- Read and store UID + memory data from transponder

Step 2

- Emulate transponder using UID + memory data
- Change memory data as you like

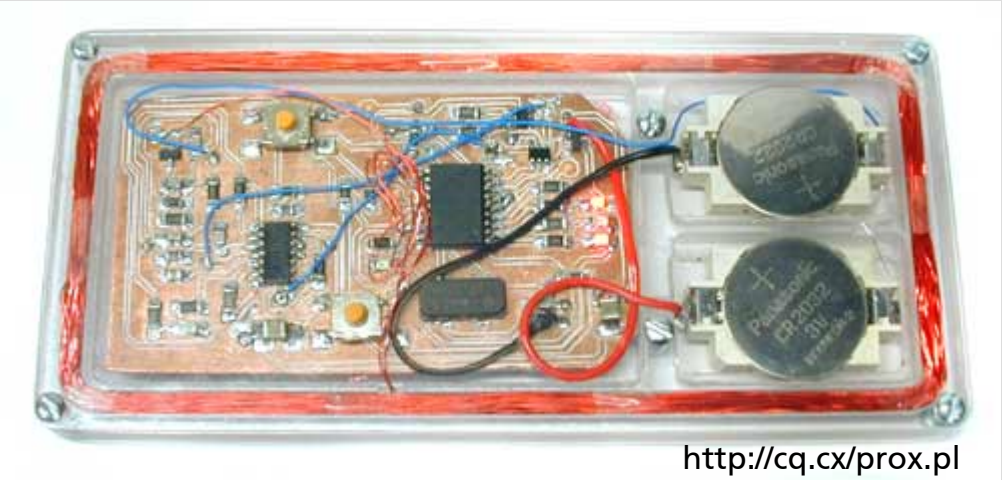


Attacks targeting the Transponder Data: Spoofing / Cloning

Spoofing (emulation and cloning) of a transponder

- Has been proved several times [Westhues 2003]
- All read-only and r/w-transponder (without encryption) are in danger
- Cannot be detected by the reader device

➔ Risks: Identity theft, restoring one time tickets; using someones access card, …



http://cq.cx/prox.pl

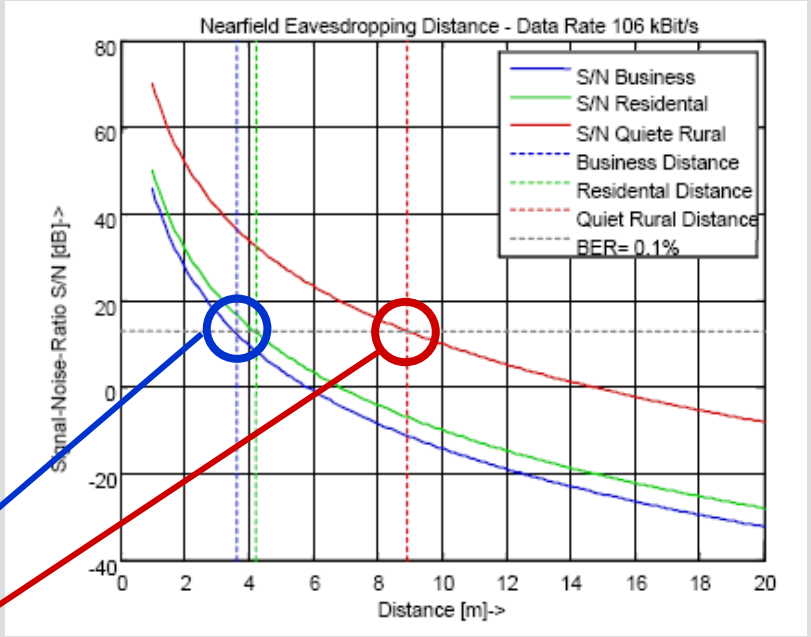
Attacks targeting Transponder Data: Eavesdropping 13,56 MHz

Eavesdropping: Unauthorized listening

- Collecting raw transmissions to determine protocols / encryption
- Determining traffic pattern
- Collecting the tag's data

Eavesdropping of uplink ISO 14443

- Detect Load Modulation Signal
- Several studies & successful attempts [BSI-MARS]
- Noisy Environment: 3 m
- Quiet Rural: 9 m



Picture source: "Messung der Abstrahleigenschaften von RFID-Systemen (MARS)", http://www.bsi.bund.de

Eavesdropping of downlink (reader signal) ISO 14443 even may work from a few 10 up to a few 100 meter

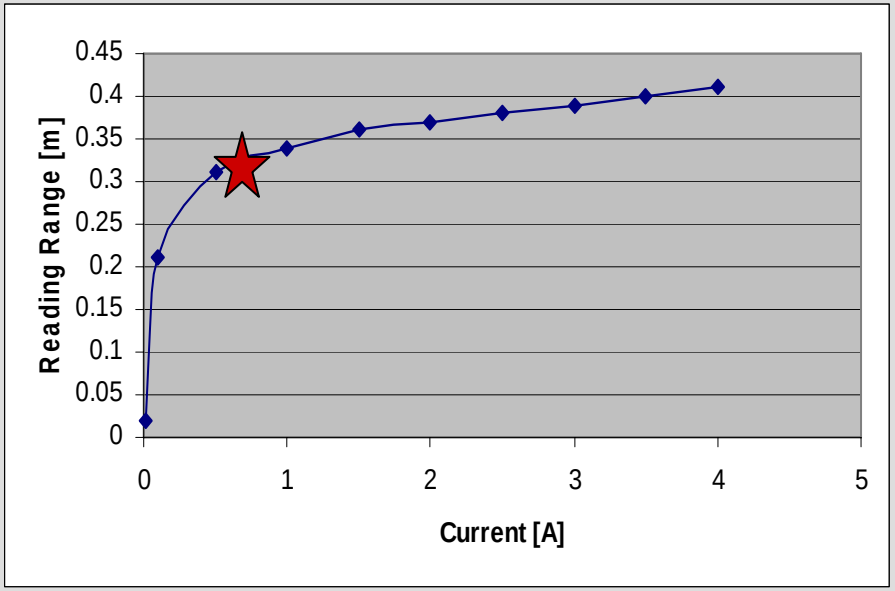
Attacks targeting Transponder Data: Skimming 13,56 MHz

Skimming: Unauthorized access of reading of tag data

Limitations in increasing the reading distance of ISO 14443 [Kirschenbaum 2005]

- Additional power adds additional noise to the load modulation side bands
- Increasing the antenna diameter decreases the coupling factor

Practical limit for ISO/IEC 14443 is around 40 cm!

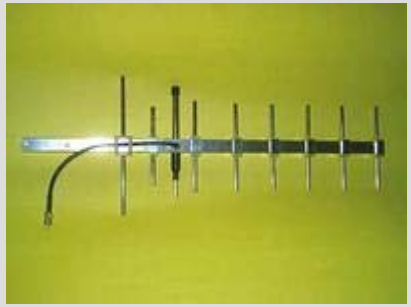


Property / Method	Max Distance	Extra Cost (beyond NFC)	Availability	Attacker Knowledge
Standard	~10 cm	0 $	High	Low
Current + Antenna	~40 cm	<100 $	High	Medium
Current + Antenna + Software	~50 cm	>100 $	Medium	High
Current + Antenna + Hardware	~55 cm	>5000 $	Low	Very High

Attacks targeting Transponder Data: Eavesdropping UHF 868 MHz

General issues

- Attacker may use directional antennas with 20 dB Gain and even more („long yagi“ or „grouped yagi“ antenna)
- Eavesdropping distance strongly depends on „line of sight“



Antenna with 10 dBi

Eavesdropping of uplink UHF (transponder ➔ reader)

- Typical backscatter power about 0,1 – 1 mW
- A rough estimation shows that a few 10 m should be no problem

Eavesdropping of downlink UHF (reader ➔ transponder)

- Typical reader power 2 W ERP (according to ERC 70-03)
- A rough estimation shows that several 100 m should be no problem

Attacks targeting the RF-Interface: Skimming UHF 868 MHz

Increase reading distance at UHF

- Increase power of reader?
  16 x power = 2 x distance!
  ➔ not feasible (adding noise)
- Increase antenna gain at reader?
  +6 dB = 2 x distance
  ➔ feasible with yagi antenna
- +20 dB = 10 x the distance
  ➔ proved by DEFCON [69 feet]
- +40 dB = 100 x the distance
  ➔ parabolic antenna with 15 m Diameter!

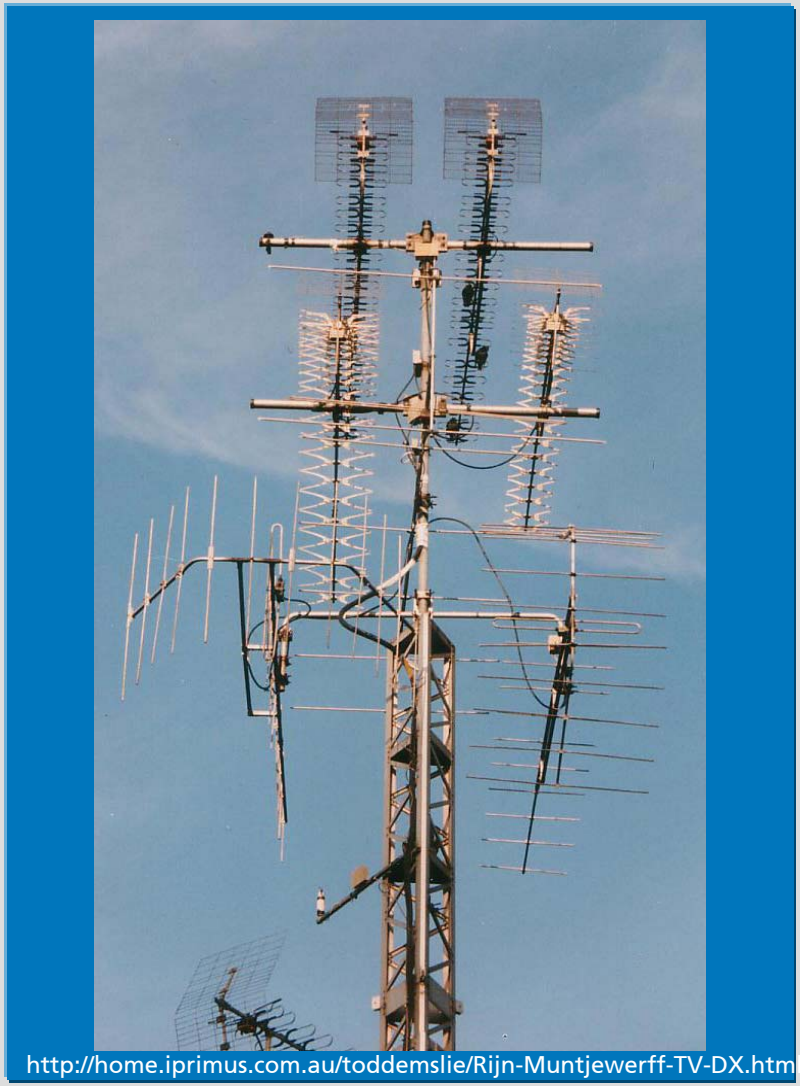
~ 40 dB antenna gain / 15 m ∅

Bild: http://www.baesystems.com/ProductsServices/radio_telescope.html

Attacks targeting the RF-Interface: Skimming @ 868 MHz

Increase reading distance at UHF

- Increase power of reader?
  16 x power = 2 x distance!
  ➔ not feasible (adding noise)
- Increase antenna gain at reader?
  +6 dB antenna gain = 2 x distance
  ➔ feasible with yagi antenna
- +20 dB antenna gain = 10 times the distance
  ➔ proved by DEFCON [69 feet]
- +40 dB antenna gain = 100 times the distance
  ➔ parabolic antenna with 15 m Diameter!
- Practical limit abt. 26 dB antenna gain = 20 times the distance
  ➔ huge antenna group


http://home.iprimus.com.au/toddemslie/Rijn-Muntjewerff-TV-DX.htm

Attacks targeting the Transponder Data

Countermeasures?

Yes! Cryptographic procedures protect against unauthorized eavesdropping, cloning, writing, modifying, reading (from distance)

- Mutual authentication between Tag and Reader
- Encryption of the data transfer between Tag and Reader
- Software countermeasures do exist (e.g., derived keys, use of session keys, periodical key updates)

Cryptographic security in contactless applications

	Cryptographic features	Threats
E-Passports (ICAO)	Passive authentication (stored data authenticity) Signature algorithms include RSA, DSA, ECDSA Optional security features: Active authentication (anti-cloning), BAC (confidentiality), keys have roughly 52 bits entropy, Secure Messaging (authenticating and encrypting passport-to-reader communications)	Tracking, hotlisting, scanning Passive eavesdropping Skimming Leakage of biometric data
MIFARE (NXB brand)	Security features: confidentiality of (proprietary) cryptographic algorithm, 48 bit keys, 16 bit random numbers (LFSR-based)	Stream cipher broken (CCC '07) attacks in minutes with limited material cost
EPC-C1G2 (ISO/IEC 18000-6C)	16-bit Pseudo-Random Number Generator, 16-bit Cyclic Redundancy Code Two 32-bit PINs: Kill and Access (uses Bitwise XOR with password); used to control memory lock states and tag kill operations Killing or discarding tags (enforces consumer privacy) No cryptographic primitives (hash functions, ciphers)	Cloning (EPC is copyable) EPC transmitted in plain text (-> Privacy, Tracking, Spoofing) PIN used in Access command can be disclosed (no real access control)
Secure UHF (ISO/IEC 18000-6)	Several **research projects**, proposals for new ciphers: Grain, Trivium, PRESENT-80 Products not yet available. Only HW implementations seem feasible.	new ciphers and algorithms => proofs outstanding => limited trust

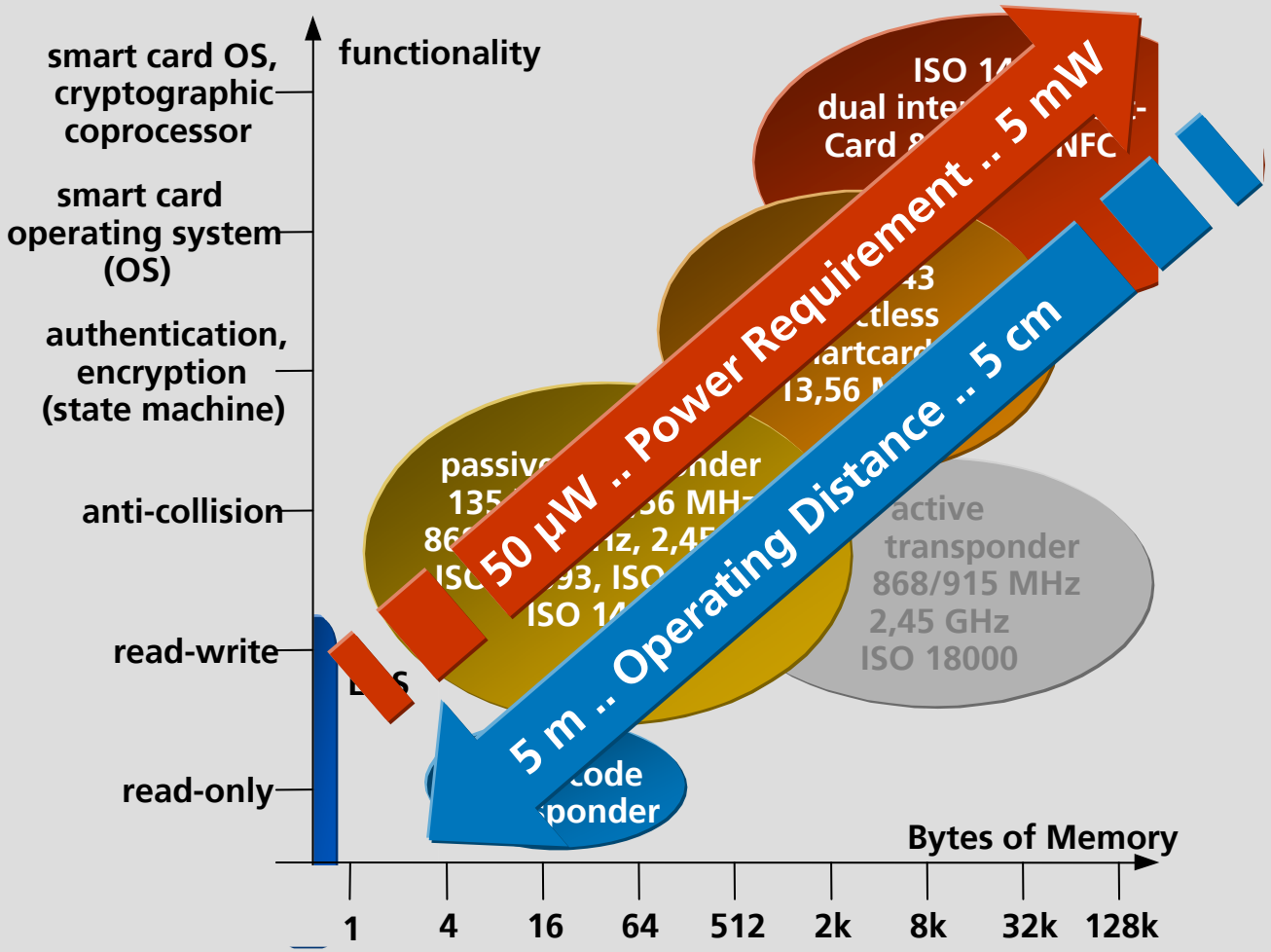
Attacks targeting the RF-Interface: Countermeasures

Cryptographic protocols are being used for high security applications:

- ePassport / eID
- Electronic payments
- Ticketing / Public Transport
- Medical / healthcare
- Access control

Problem: Cryptographic protocols increase power-consumption (bottleneck)

Result: Passive long range technologies do not (yet) provide cryptography



Part III: Using a tag without physical access ➔ relay attacks

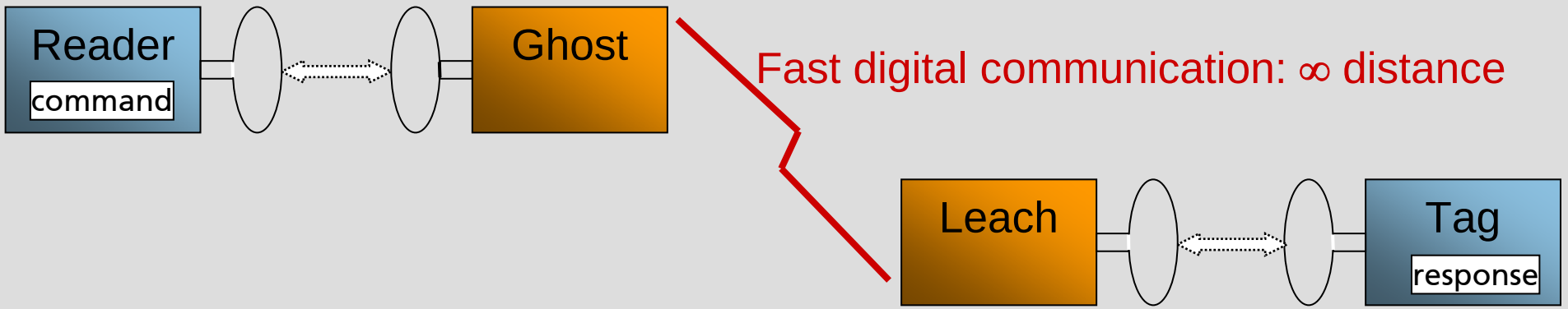
Relay attack

A Virtual Pick-Pocket System

- Ghost is the device that FAKES a Tag to the Reader
- Leach is the device that FAKES a Reader to the Tag
- Ghost to Leach distance is unlimited

Virtual Pick-Pocket allows

- Charging someone else's credit card for a purchase.
- Opening a secure door using someone else's key.

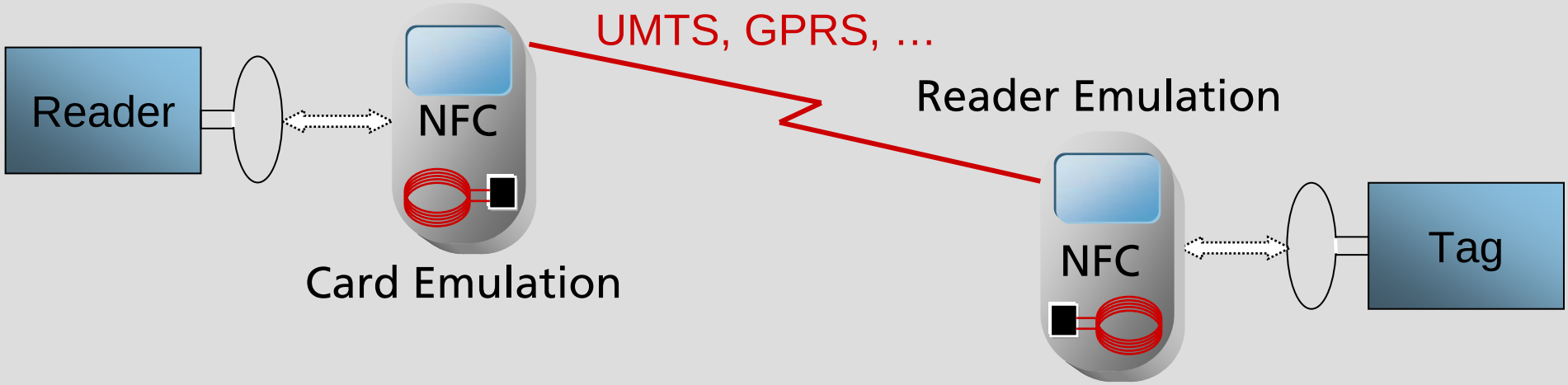


Relay attack

The real threat: relay attack using custom NFC phones

- Protocol stack implemented in mobile phone ➔ No detection by timing
- Transfer only APDU via data link between mobile phones
- Easy to handle, easy to copy, only Java-applet needed

High Risk: Easy to install (download NFC applet from internet), NFC phones available for low budget, NFC becoming a mass product!



Relay attack

Countermeasures against relay attack:

Additional information required to „confirm a transaction“:

- Press a button to confirm a required transaction (payment)
- „secret handshakes“, using movement sensor

- Basic Access Control (BAC) for electronic passports uses optical readable information from MRZ to derive an access key

Basic Access Control (BAC)

Protects against unauthorised access and eavesdropping.

Some limitations:

- **entropy of the derived session key**
- **MRZ ist static ➔ BAC key is static**

Optical character recognition

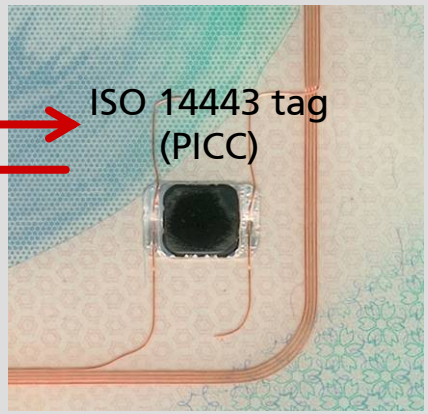
optically read MRZ

ISO 14443 reader (PCD)

send MRZ

receive additional info

➔ encrypted



Standardisation Activities

- Going to implement an RFID-system?

  ➔ Technical Recommendation (TR) and International Standards (IS) you should have a look at …

Technical Guidelines of German Federal Office for Information Security (BSI)

Technical Guidelines regarding RFID

With the publication of Technical Guidelines BSI pursues the objective to spread appropriate IT-security standards. Technical Guidelines address all parties involved in the installation or safeguarding of IT-systems. They complement the technical test specifications of BSI and provide criteria and practices for conformity evaluations ensuring the interoperability of IT-security components as well as the implementation of defined IT-security requirements.

http://www.bsi.de/literat/tr/tr03126/index.htm

Released:

- TR 03126-1 "eTicketing im ÖPNV„ (public transport), 181 pages
- TR 03126-2: "eTicketing für Veranstaltungen„ (event ticketing), 186 pages

Under Development:

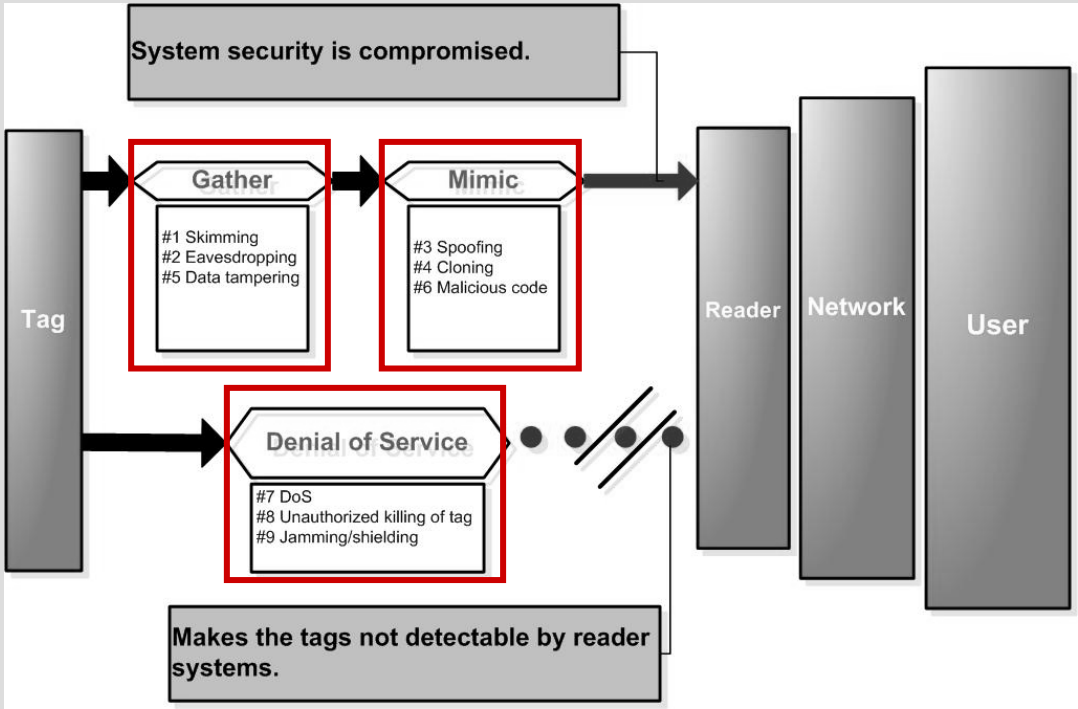
- *TR 03126-3: "NFC-basiertes eTicketing" (NFC ticketing)*
- *TR 03126-4: "Handelslogistik" (supply chain)*

RFID Security – ISO-IEC/JTC1/SC31/WG4

RFID for item management:

ISO/IEC TR 24729 – 4: RFID Implementation Guidelines – Tag data security

- Technical Report (TR)
- Based on ISO/IEC 18000-6C
- Provides guidance on potential threats to data security
- Threat scenarios and potential impact levels
- Provides Guidance on counter-measurements
- Looks at systemic solutions that prevent unauthorized access to data on an RFID tag.



RFID Security – ISO-IEC/JTC1/SC31/WG4

Under Development:

(Draft) ISO/IEC 24791-6: „RFIDfor item management – Software system infrastructure – Part 6: Security“

- Covers security issues for the RFID reader and back-end systems
- Will NOT cover the security issues in the air-interface between tag and reader

(Draft) ISO/IEC 29167: „Automatic identification and data capture techniques – Mobile item identification and management – Consumer privacy-protection protocol for Mobile RFID-Services“

- Conceal the original UII (unique item ID) and the original TID (tag ID)

RFID Security – ETSI

ETSI / TISPAN WG7:
New Work Item on RFID Security and Privacy – January 2009

- Scope of NWI
  - Develop a standard (EN) for the enhanced privacy & security of RFID & RFID networks
  - Supporting the Future Internet of Things (FIT)
  - Reader and network side: personalization and traffic analysis shall be addressed
- Technical investigation into the possibilities for RFID related crime
  - Evaluating the capabilities of passive RFID technologies UHF, HF and LF beyond regulatory limits
  - RFID technology supply chain threats
  - RFID counterfeiting

Questions?

References

- [69 feet] DEFCON RFID World record attempt, 2005 http://blog.makezine.com/archive/2005/07/_defcon_rfid_wo.html
- [A. Juels] The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy, http://www.rsa.com/rsalabs/staff/bios/ajuels/publications/blocker/blocker.pdf
- [BSI-MARS] Studie "Messung der Abstrahleigenschaften von RFID-Systemen (MARS)„ http://www.bsi.bund.de/fachthem/rfid/Mars_Teilbericht_1Therorie.pdf
- [Kirschenbaum 2005] How to Build a Low-Cost, Extended-Range RFID Skimmer, Ilan Kirschenbaum, Avishai Wool
- [Westhues 2003] A Card Simulator http://cq.cx/prox.pl