Radio Frequency Identification and Radio Networks

Advanced Internet Security

Adrian Dabrowski, Christian Kudera, Georg Merzdovnik
inetsec@seclab.tuwien.ac.at

Overview

InetSec

- Basics
- Attack methods
- Freq/Time domain
- SDR / USRP
- GSM, UMTS, LTE
- GPS

Adv.InetSec

- Basics (rep)
- RFID
- NFC

OPINION

GPS jammer to stop tracking messed up airport navigation, driver fired, fined $32,000

What happens if you take steps to insure a bit of privacy by jamming a company vehicle's GPS tracker to hide your location from your boss? A New Jersey man found out after his GPS jamming disrupted a "pre-deployment testing of a ground-based augmentation system (GBAS) at Newark Liberty International Airport;" he was fired from his job as a driver for engineering company Tilcon and fined almost $32,000 by the FCC.

Jamming devices "have no lawful use," according to the FCC [pdf], and can legally only be marketed "to the U.S. federal government for authorized, official use." The GBAS being tested at Newark Airport is supposed to provide "enhanced navigation signals to aircraft in the vicinity of an airport for precision approach, departure procedures, and terminal area operations." On August 3, the FAA complained of interference during testing. On August 4, an officer used "direction finding techniques" to determine the GPS jamming was emanating from a red Ford F-150 pickup truck.

MORE LIKE THIS

Spoofed! Fake GPS signals lead yacht astray

Homemade GPS jammers raise concerns

Civilian drones vulnerable to hackers, can be hijacked, used as missiles

VIDEO
Tech Talk: Apple's home speaker, HomePod, arrives

Wireless

- The so called “air-interface” is a shared medium
- To access the “interface” you can either just be within the vicinity or in a galaxy far far away...

http://ironic1.com/ https://defcon.org/html/links/dc_press/archives/12/esato_bluetoothcracking.htm

Radio is strange...

- Does not stop at walls.
- Is a shared medium
  - Everything is a broadcast
  - Unicast is a “filter”
- Distance mainly depends on:
  - Transmit power
  - Antenna gain (“focusing”)
    - Send and receive side
  - Receiver sensitivity
  - Obstructions, noise, and modulation

Example

Modern Car Keys

Immobilizer (RFID)

Makes sure, original key is in ignition lock.

Securing techniques:

- Encryption

- Challenge Response

Remote Control

Opens/Close car from remote

Security techniques:

- Rolling Code

- Encryption

Example

Modern Car Keys

Immobilizer (RFID)

Makes sure, original key is in ignition lock.

Securing techniques:

~~**- Encryption**~~

~~**- Challenge Response**~~

Remote Control

Opens/Close car from remote

~~**Security**~~ **techniques:**

- Rolling Code

- Encryption

Used wrongly

Usenix Security 2016

Lock It and Still Lose It – On the (In)Security of Automotive Remote Keyless Entry Systems

Flavio D. Garcia[1]
School of Computer Science, University of Birmingham, UK.
f.garcia@bham.ac.uk

David Oswald[2]
School of Computer Science, University of Birmingham, UK.
d.f.oswald@bham.ac.uk

Timo Kasper[2]
Kasper & Oswald GmbH, Germany.
info@kasper-oswald.de

Pierre Pavlidès[1]
School of Computer Science, University of Birmingham, UK.
pierre@pavlides.fr

Abstract

While most automotive immobilizer systems have been shown to be insecure in the last few years, the security of remote keyless entry systems (to lock and unlock a car) based on rolling codes has received less attention. In this paper, we close this gap and present vulnerabilities in keyless entry schemes used by major manufacturers. In our first case study, we show that the security of the keyless entry systems of most VW Group vehicles manufactured between 1995 and today relies on a few, global master keys.

to create a duplicate. In addition, mechanical tumbler locks and disc locks are known to be vulnerable to techniques such as lock-picking and bumping that allow to operate a lock without the respective key. Finally, for most types of car locks, locksmith tools exist that allow to decode the lock and create a matching key.

1.1 Electronics in a Car Key

With electronic accessories becoming available, ad-

Main Attack Modes

Intercept

- Sniff, Decrypt

Suppress

- Jamming
- Blackholeing

Forge

- Spoofing

Replace

- In-place
- Suppress and Forge

Replay

- Record once, replay later

Relay

- Tunnel communication to another location (out-of-range device)

Intercept

- Radio waves are usually not contained (except SCIF, EMC Testing)
- Easy to sniff traffic
- Gather and analyze from a safe distance
- Depends on antenna gain/performance

- In a smaller scale: Side Channel Attacks on embedded systems
  - Every circuitry receives and emits electro-magnetic radiation
  - A radio is build to maximize this capability

Suppression: e.g., Jamming

- Interrupt or prevent communication
  - Single unrecoverable bit-error could be enough for the receiver to silently drop the data packet
- Ranges from simple overloading the RF frontend to sophisticated network attacks
  - Specific jamming (e.g., only one device)
  - Blackholing (let other devices believe, you are a shorter/ better route, don't forward traffic)
- Jam a single frequency or a wide band
- Energy requirements for a wide band are high
  - Receivers are made to cope with noise
- Can simply be brute force

Spoofing, ...

- Shared interface
  - Forging receiver and sender address/id
- Intercept, jam, and spoof
  - Change/replace content
- Relay
  - Send communication to a device, that should not receive the signals
- Replay
  - Record, and playback later
- Optional Man-in-the-Middle (MitM)
- Data processing and transmitter necessary

RFID and NFC

RFID is not a standard

NFC is … kind of...

RFID is a concept, with many diverse implementations.
NFC specifies data formats and partly how to fit them onto specific cards.

RFID, some properties

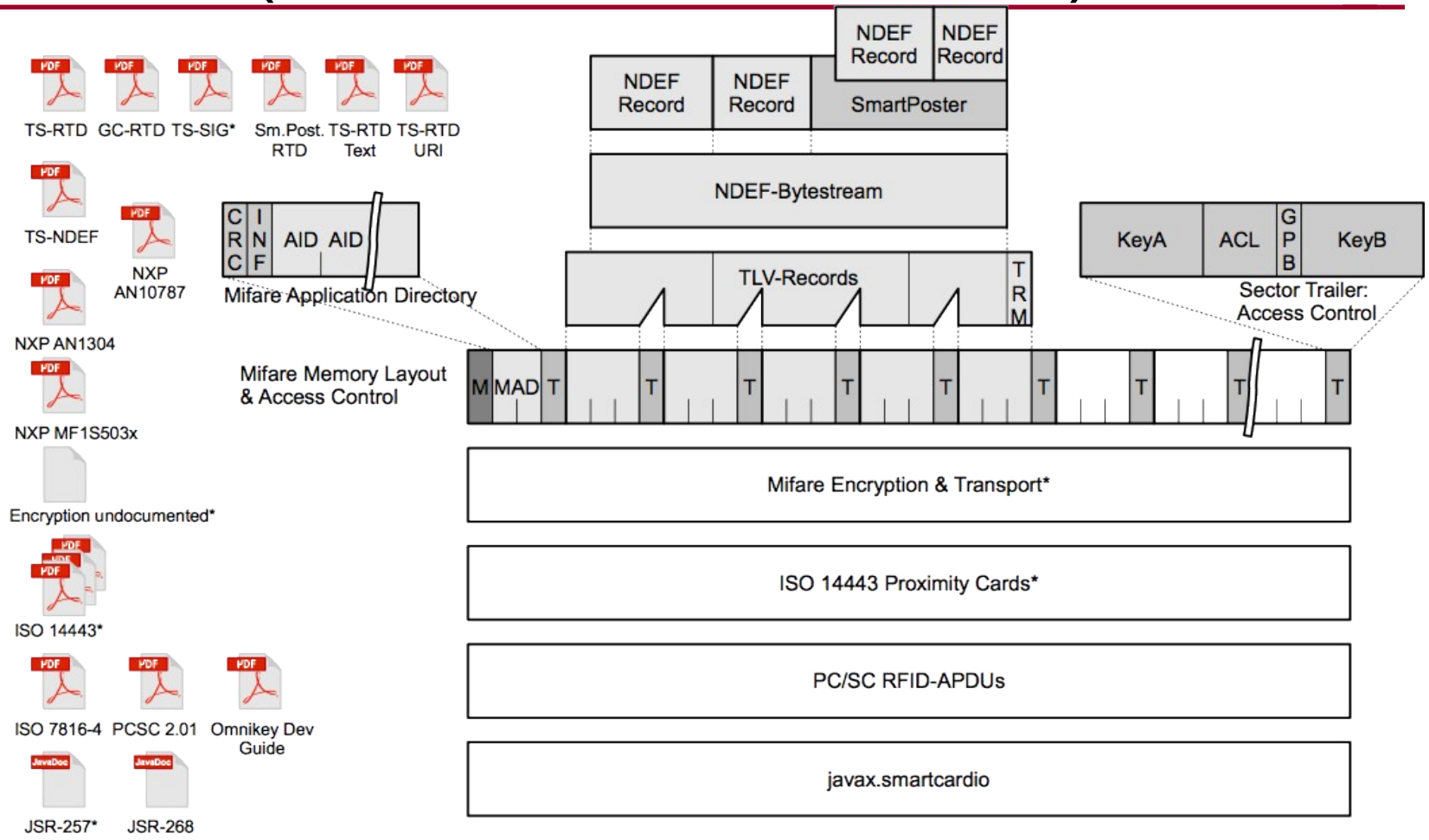
Tag

- Mostly “dumb” device
  - ID
  - (crypto) memory
- Mostly passively powered
- Inactive, when outside of a reader field

Reader

- Active
- Supplies tag with power
- Has most of the logic and application
- Might be online

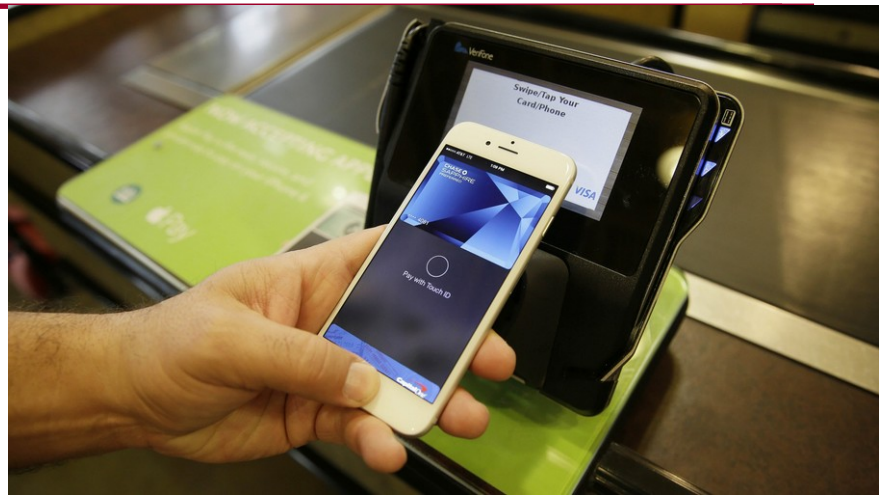
NFC Stack Example (NFC NDEF on Mifare)



What Marketing is selling to us...

- eg. Wiener Linien, ÖBB, …
- Buy tickets with your mobile NFC phone
- Passive NFC stickers

What Marketing is selling to us...



- Touch two phones to transfer images, music, ….
  - Real transfer is done via Bluetooth or WiFi Direct
- Touch to pay
  - Payment services

Radio Frequency Identification

- Many origins
  - eg. 2nd world war: radar reflection pattern for "friend or foe" detection
- Most developments started in logistics
  - As Barcode replacement
- Later adopted as memory
  - As Magstripe replacement
- Later adopted as smart card
  - As T0/T1 contact protocol replacement

- **Function and application creep at its best...**

Overview: How does RFID work

- Radio Frequency Identification
    - Near field communication
- Frequency
  - 125 kHz, 13.56 MHz, 433 MHz, 900 Mhz, 2.45 GHz
- Power
  - Passive, semi-passive, active
- Coupling
  - Inductive, Backscatter, Capacitive
- Return Channel
  - Load Modulation, Sub-carriers, Harmonic carriers
- Carrier is...
  - Power supply
  - Clock supply
  - Downstream
  - Base for upstream signal

Underline: predominant in consumer applications

Power

- Passive
  - All power for the function of the tag is derived over the air
  - No active transmitter
  - Typ. small plastic cards and tags
  - Found in alarms, id-systems, key cards, payment
- Semi-passive
  - Battery powered
  - Might be only activated with a button press – or – sensor values
  - No active transmitter (uses the same transmit method like passive tags)
  - e.g. found in temperature sensors (food logistics)
- Active
  - Active Transmitter, can transmit on its own.
  - Battery powered
  - e.g. Bluetooth LE

Frequency

- 125 kHz
  - LF tags
  - Typ. inductive coupling, passive
- 13.56 MHz
  - HF tags
  - Typ. inductive coupling, passive
- 433 MHz
  - Seldom used
- 900 Mhz
  - UHF Tags
  - Backscatter return channel
- 2.45 GHz
  - Microwave tags
  - Typ. Capacitive or backscatter

Consumer Tags

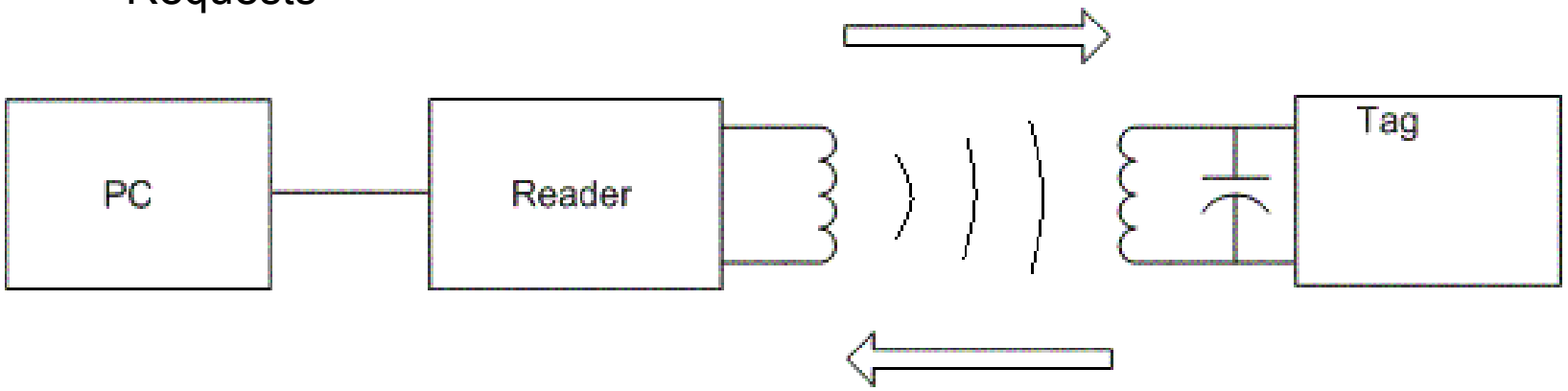
Logistics

Coupling & Return Channel

- Coupling
  - Inductive (or magnetic coupling)
    - Similar to transformer
    - Works only in the “near field” of an antenna
    - Limits range most
  - Backscatter
    - Changes harmonics or reflects energy, e.g. on a different frequency
  - Capacitive
- Return Channel
  - Load Modulation
  - Sub-carriers
    - Typ. An integer fraction of the main carrier
  - Harmonic carriers

So the carrier is...

- **>>>** Power supply **>>>**
  - For operating
- **>>>** Clock supply **>>>**
  - No power for independent clock
  - Perfectly synchronized with reader
- **>>>** Downstream data / modulation **>>>**
  - Requests

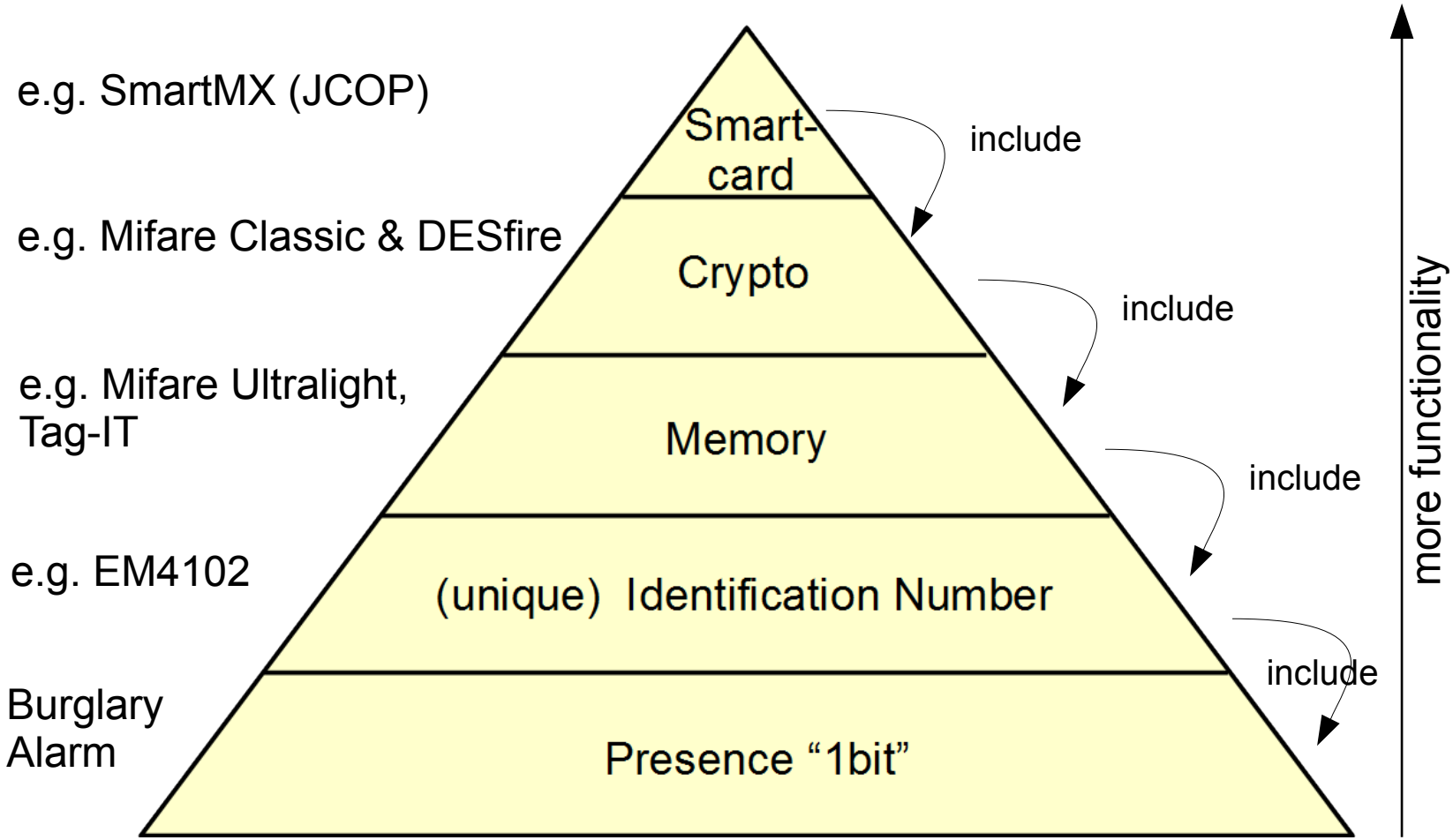


- **<<<** Base for upstream signal **<<<**
  - return/response

Modulation

- Downstream and upstream modulation often very different
  - Downstream
    - very easy: amplitude modulation (ASK)
  - Upstream:
    - Typically FSK on sub-carriers
    - Much slower
- High/Lowspeed modes (for extended range)
  - e.g. ISO 15693 has 8 combinations of up/downstream modulations and speeds.

Functionality Pyramid



Most widespread Card Systems

- ISO14443
  - NXP Mifare
    - Ultralight
    - Classic
    - Classic Plus
    - Desfire / EV1
- ISO15693 (div)
  - eg. skipass

- EM 4102
- EM 4150
- HID (div)

- Felica
  - eg. Suica, PASMO

Card system architecture

- **Online** Systems
  - Card only stores ID
  - Every transaction needs a (networked) **database** lookup
  - Often uses the (insecure) Unique ID (UID / serial number) of the card
- **Offline** Systems
  - All transaction information is **stored on the card** or processed on the card (e.g. deduction of funds)
  - No extra database needed

Hybrid Online/Offline Systems

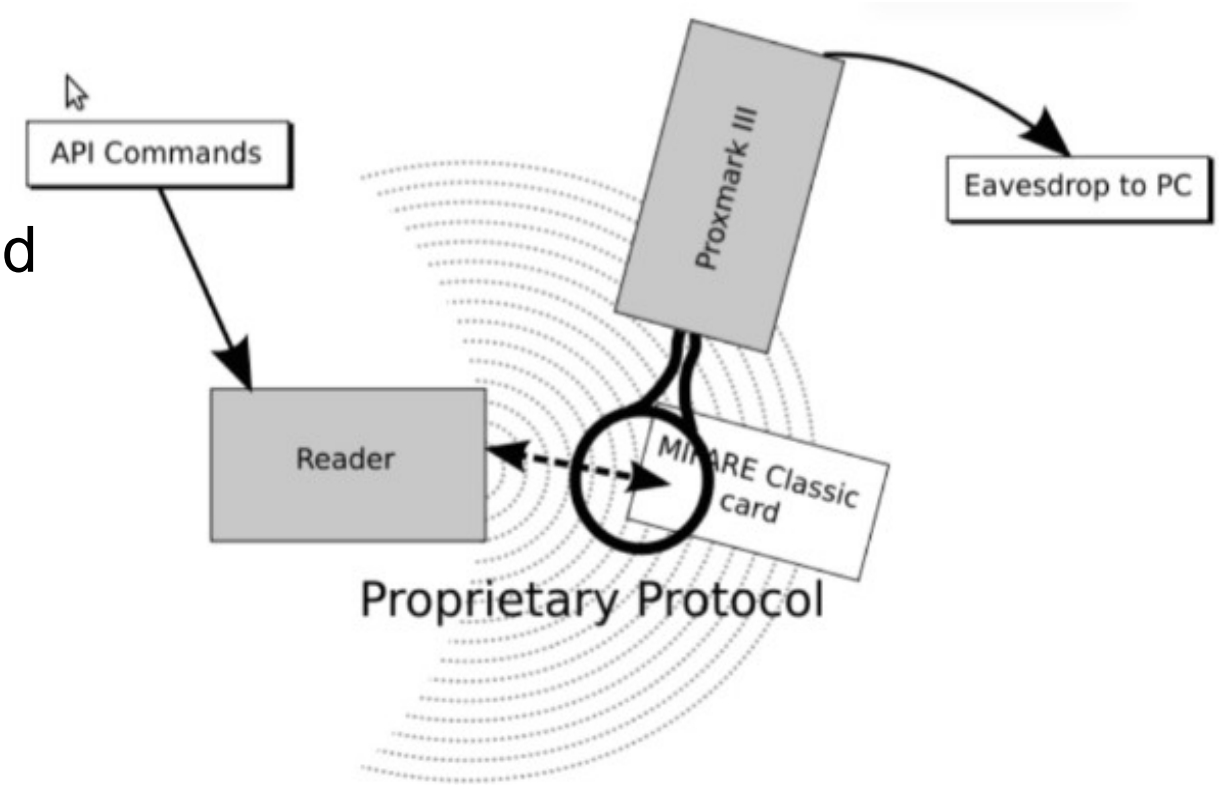
- Hybrid access control
  - Doors are offline, main entrance is online
  - Cards get an day-by-day update at the main entrance, expires the next day
  - Doors need an RTC
- Hybrid risk control
  - Transactions are offline, but are stored and synchronized/matched afterwards to check for consistency
  - Detects and locks out manipulated cards after e.g. a few days

Main Attack Types

- **Retrieve card key(s)**
  - Copy content of card
  - Backup/clone/restore old state of card (e.g. after an deducting transaction)
- **Clone UID**
  - UID is a very low level protocol information; typically not changeable
  - Some Chinese knockoff cards or card simulators are able to simulate arbitrary UIDs
- **Replay attack**
  - Non randomized cryptographic transaction
- **Relay attack**
  - Build a “bridge/tunnel” that simulate physical presence of real card over large distance

Sniffing (& Replay)

- Used for Mifare and other protocols
- Sniffing: important tool for analyzing unknown protocols
- Replay only possible with non-randomized encryption

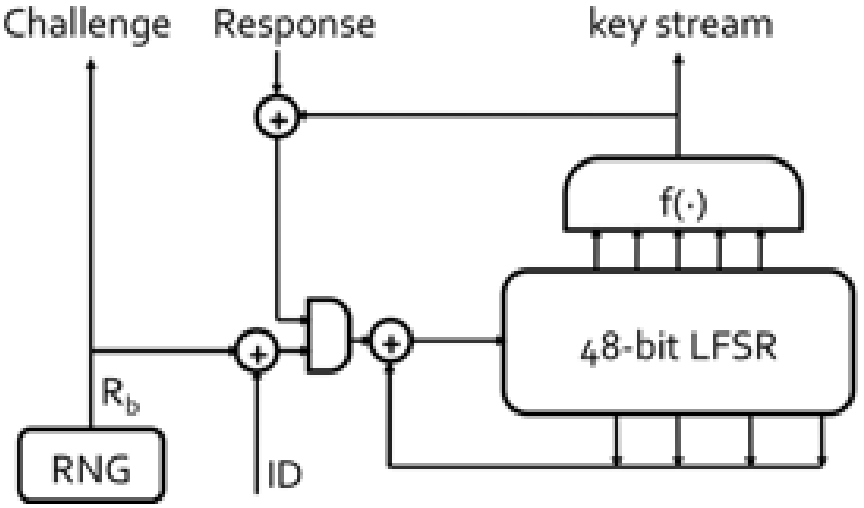


Card key reconstruction

- **Mifare Classic**
  - By NXP/Phillips
  - Used a proprietary non-public cipher: CRYPTO1
  - Reader hardware had to use NXP chip as well
  - Until 2007, 3.5 billion cards were produced
  - CCC 2007: Nohl & Pöltz, partial reverse engineered Crypto-1 (by optical reconstruction of IC)
  - March 2008: Group at Radbound University completely reversed crypto-1 and intended to publish it.
  - NXP tried to used lawyers, started judicial process
  - July 2008: court decides in favor of researchers

Mifare Classic (cont)

- Keys only 48 bits
- LFSR for RNG is predictable
  - Constant init cond.
  - Only dependent on clock
  - For attacks, timing is important
  - Since the reader (=attacker) controls the timing, he/she can control the RNG
-



Mifare classic format

		Key A	Access Bits	Key B
Sector	Block	Data		
0	0	33bd9d3f2c980200648f841441502212		
	1	090f1808000000000000003010000400b		
	2	00000000400c400c400c000400040005		
	3	a0a1a2a3a4a5787788c17de02a7f6025		
1	0	418d50c98d7f962462004c800000ffcc		
	1	1fa1014100d101c060000000049a2a9f		
	2	1fa1014100d101c060000000049a2a9f		
	3	2735fc18180778778800bf23a53c1f63		
2	0	3065061730077220296012505b74c05d		
	1	68c701da24c027ece0ee9a99c0caadb1		
	2	c82591842f0b8304a2a068d1f4e016e7		
	3	2aba9519f574787788ffcb9a1f2d7368		
3	0	6c135ade77c0f7a11f09ad059d45720c		
	1	3c0dc85010e3ef723bfad584c4ad509d		
	2	040e821625f14168040ed8ee61a8f635		
	3	84fd7f7a12b6787788ffc7c0adb3284f		
4	0	420d53f9dbd3362461004c800000bc18		
	1	1f51014100d101c0900004240280bdce		
	2	1f51014100d101c0900004240280bdce		
	3	73068f118c13787788002b7f3253fac5		
5	0	00000000000000000000000000000000		
	1	01770000907222029653352020202020		
	2	00000000000000000000000000000000		
	3	186d8c4b93f908778f029f131d8c2057		

- Sector = 4 x 16 byte pages
  - Page 0-2: user data
  - Page 3 contains 2 keys + permission bits (W only)
- Sector 0 page 0:
  - UID & config (RO)
- Sector 0 page 1+2:
  - MAD: Mifare Application Directory (not mandatory)
- Sector 0 page 3: RO key usually public, if MAD present

Mifare card only attacks (most popular)

- "Nested Attack" **MFOC**
  - Needs one sector with known key
  - Try to re-authenticate, determine timing distance and computes LFSR timing distance
  - Retry at different block
  - 2 to 10 min to reconstruct all keys of a card
- "Dark-side Attack" **MFCUK**
  - Card checks parity bits before checking correctness of message
  - If parity is correct, but message not, sends error code encrypted; otherwise silent
  - Reconstructing four keystream bits in this step.
  - Reconstructing one sector key takes around 1 hour, then switch to MFOC

Mifare Classic breakdown

- In 2009/2010 London Transport had to change to Mifare Desfire
  - 17 million cards
- Reports say, 700 million cards had to be replaces worldwide
- Other cities still use Mifare Classic (e.g. Los Angeles)

- Big image problem for NXP, big business success
  - Most companies transitioned for Mifare Desfire, some use Mifare Plus as intermediate step

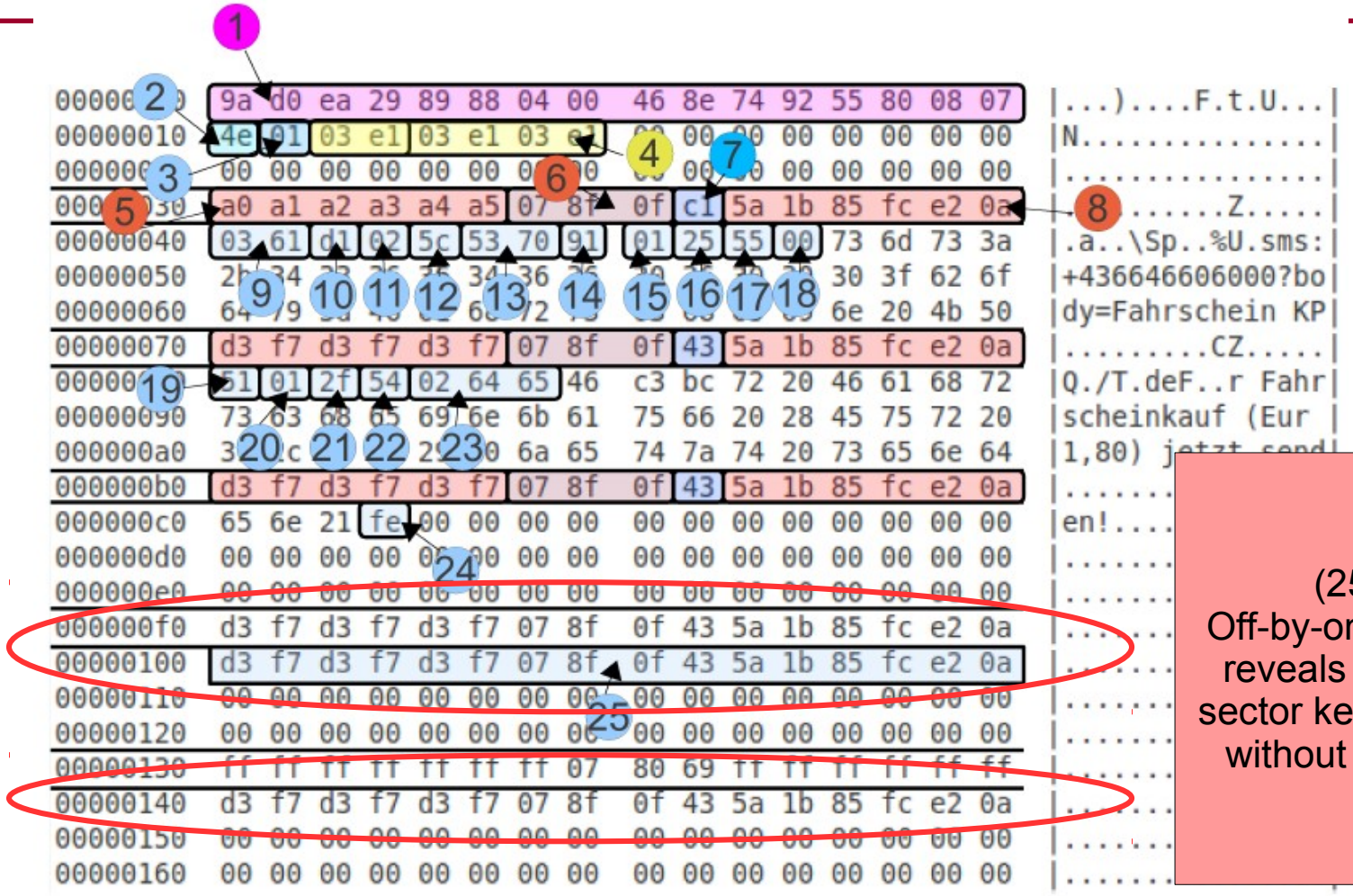
Mifare Plus and Mifare DESfire

- Mifare PLUS
  - Bridges gap, because can reuse Mifare classic readers, Mifare DESfire has higher hardware needs.
- Original Version used DES
  - Also vulnerabilities found, but much harder to exploit (> 5000 USD per card/key)
- Mifare DESfire EV1 also supports AES
  - Allows “applications” to be installed without knowing the master key → finally a real multi-application multi-vendor solution
  - NXP forces developers to sign multiple NDAs
  - Hardware emulators available

Mifare at Wiener Linien (2011)

- Buy tickets with your mobile NFC phone
- Passive NFC stickers

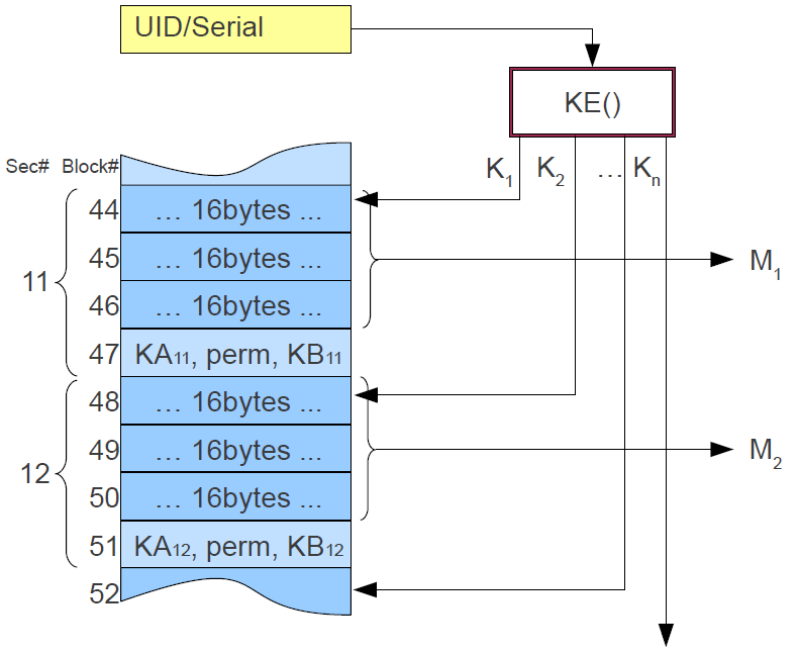
Mifare at Wiener Linien (2011)



Coffee anyone?

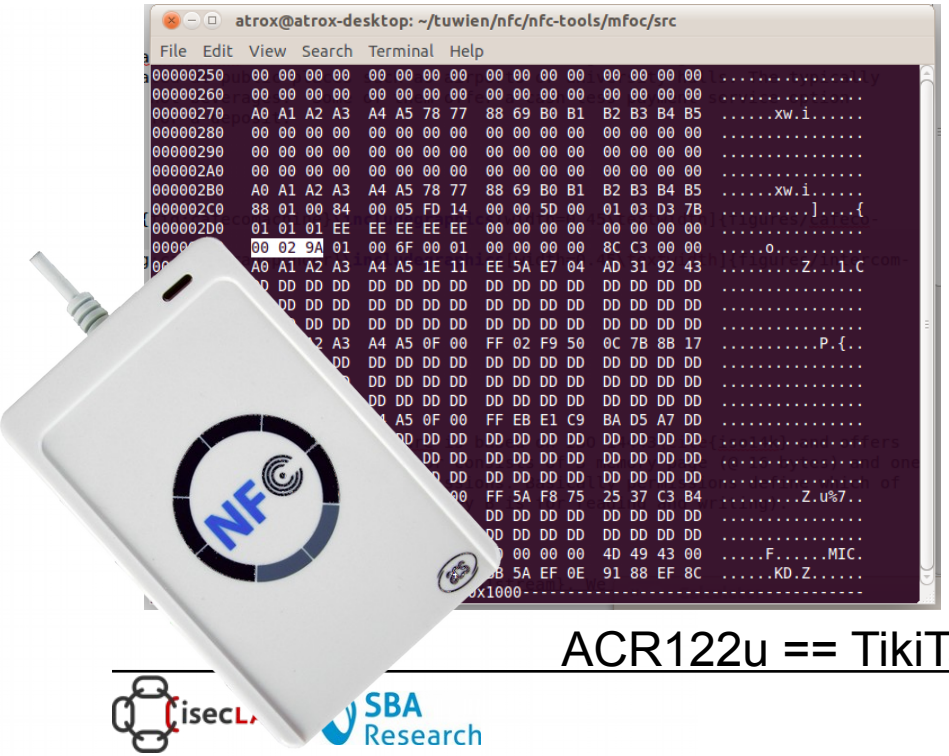
12

Good Idea:
Use key diversity
i.e. keys are dependent on card UID



Coffee anyone?

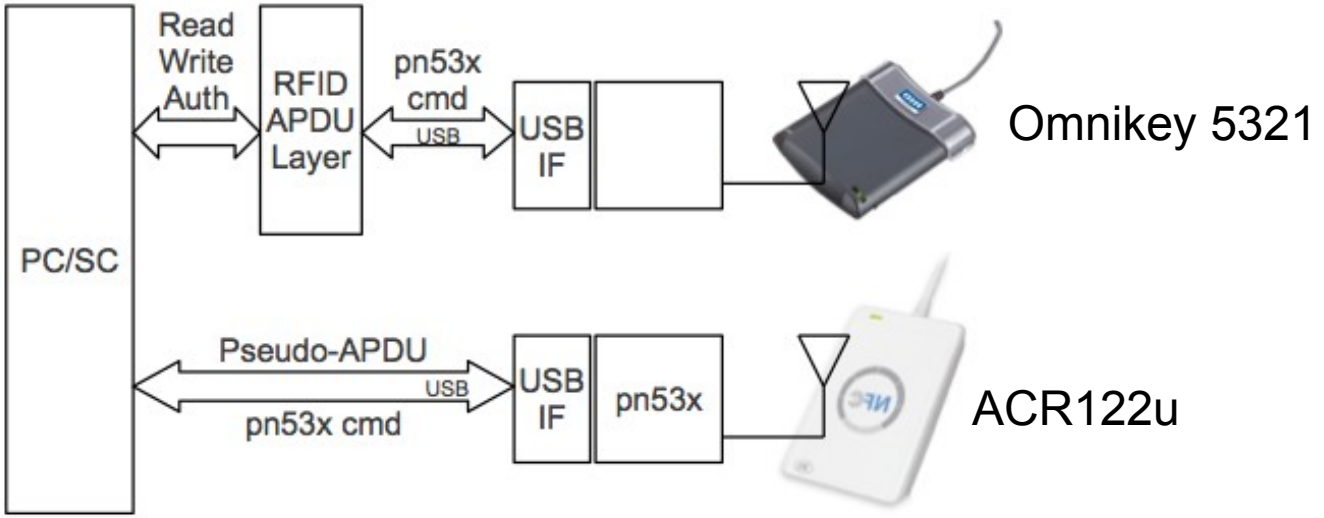
a) crack Mifare keys
b) create dump, make transaction, create 2nd dump
c) create difference
d) find monetary value



ACR122u == TikiTag == Touchatag + libnfc (mfoc)

Protocol Level Tools

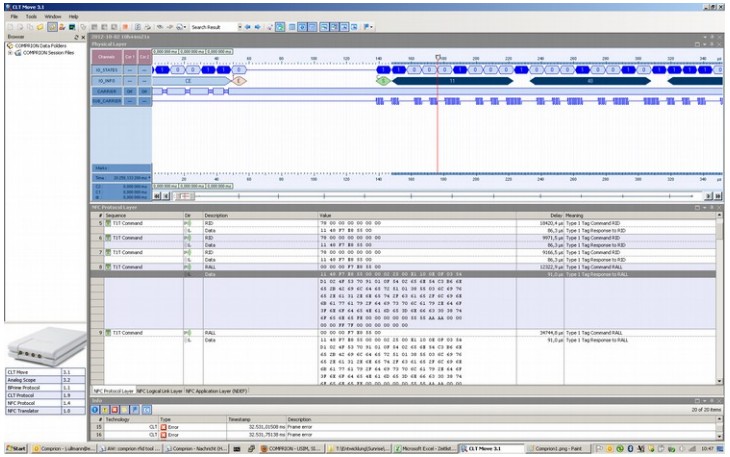
- PC/SC
  - Software Interface
  - APDU-Commands
  - Originally for wired smart cards
  - Packs everything into APDU frames (can be cumbersome)



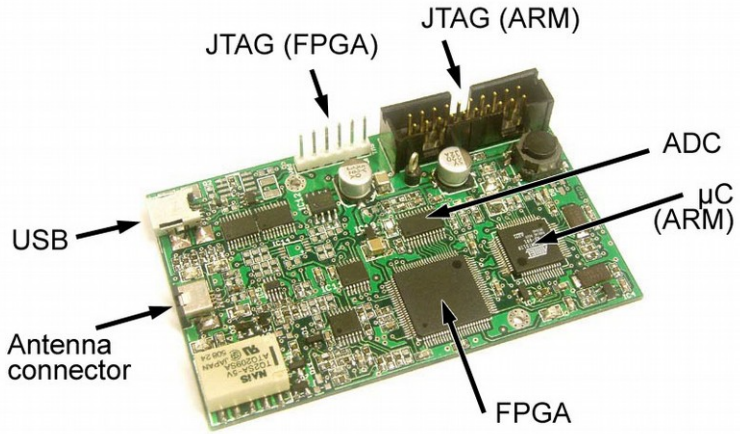
More Tools (expensive!)

Comprion

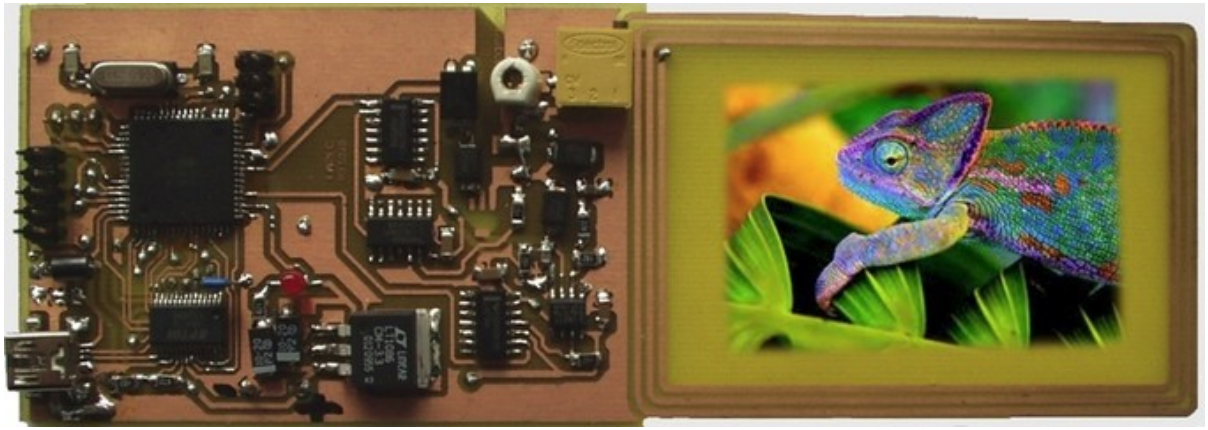
IAIK DemoTag



Proxmark III



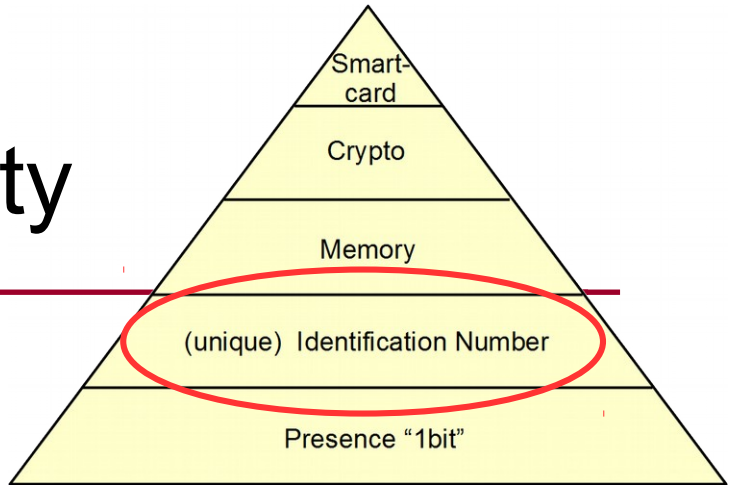
Chameleon Mini



~€100 (Kickstarter)

https://github.com/emsec/ChameleonMini/wiki

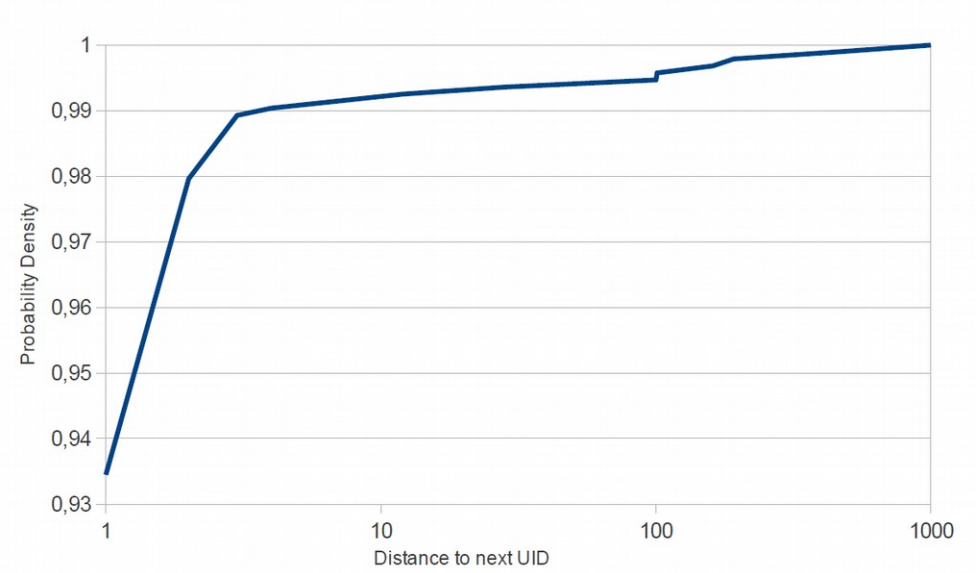
On UID safety



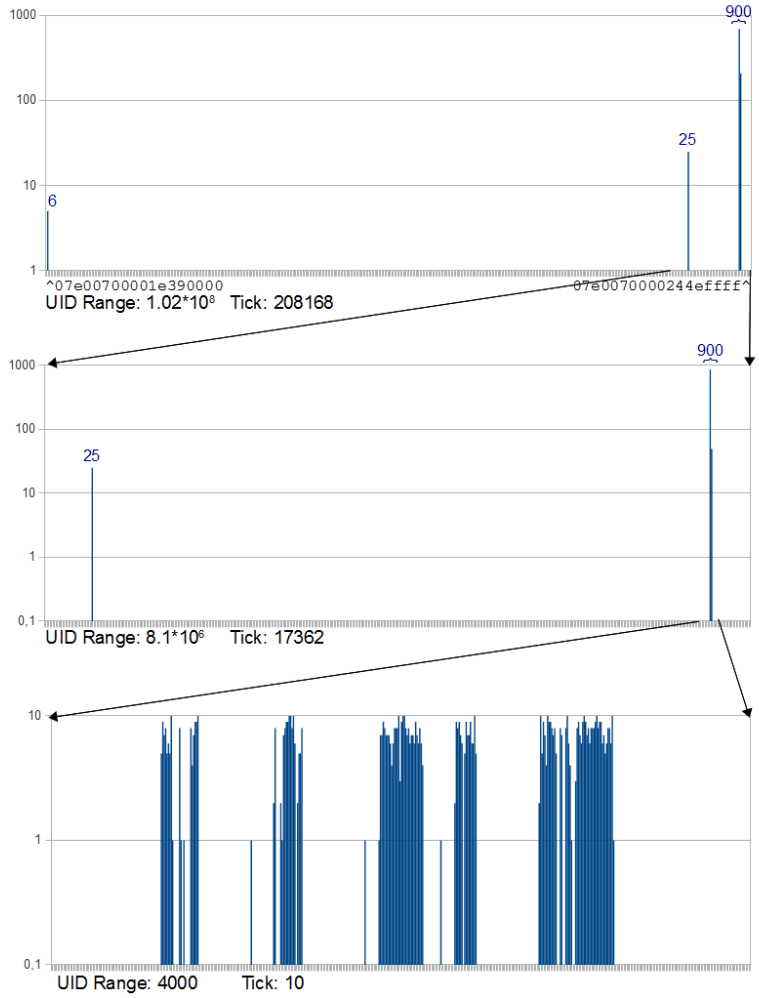
- Easy to get "serial number"
- Typically 32-64 bit … sufficient large space, or is it?
  - They become predictable, because not randomized
  - eg. one stolen/lost card gives away information about other cards from the same lot
- Sniffable

- Simulateable with custom hardware
- Special UID rewritable cards for various systems
  - eg. Chinese Mifare clones
  - EM4102

UID-Based Security: TI-LAB

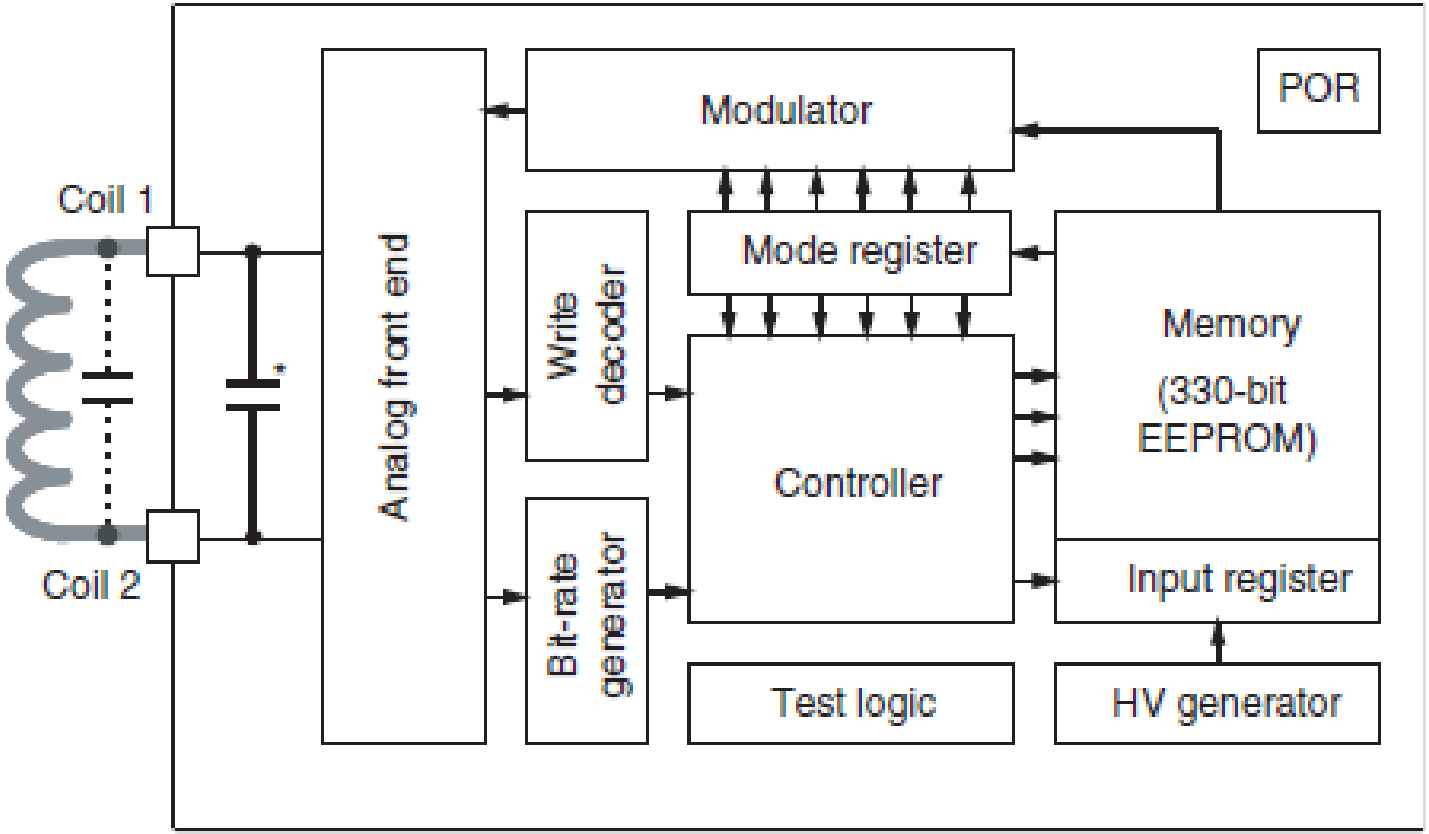


Cumulative distribution function



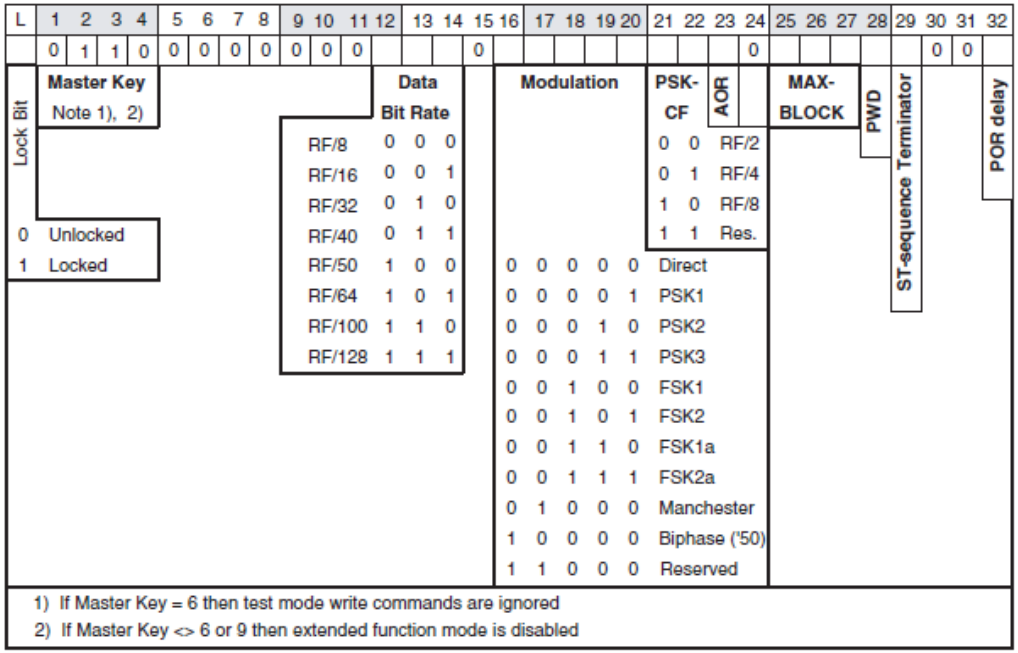
EM4102 & co.

Atmel T5557 T5567 T5551



Atmel T5557 T5567 T5551

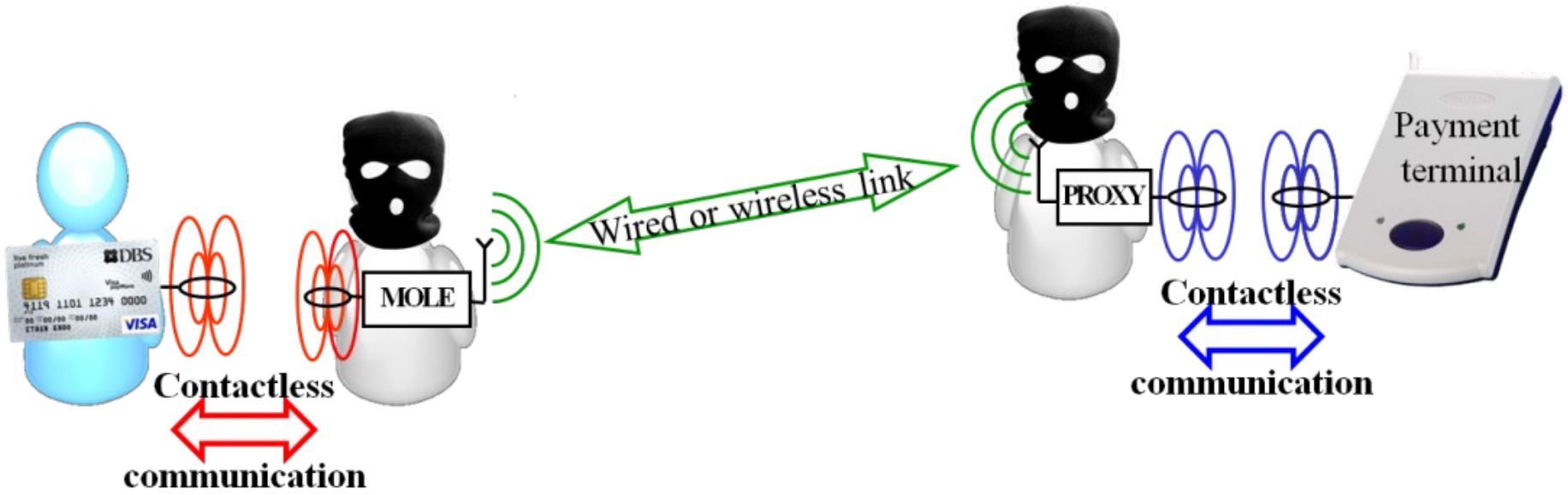
- Basically, an fully programmable signal generator
  - Running on 125 khz, powered by carrier
  - Different encodings and bit patterns possible
- Very popular EM4102 simply repeats its ID endlessly
  - Easy to simulate with an T5557



EM4102 cloning

Relay Attack

- “tunnel” cryptographic data over large distances
- Works also with unknown or unbroken cryptography
- Hard to combat, partly success with strict timing



Questions?


Oleg Šelajev
@shelajev
Follow
The S in the IoT stands for Security.
RETWEETS
3,302
LIKES
3,472
1:08 PM - 10 Nov 2016
27
3.3K
3.5K