RFID Payment Systems

free drinks and all you can eat

PRESENTED BY:

Gerhard Klostermerier

@iiiikarus · www.icaria.de · contact@icaria.de

Me

- Gerhard / ikarus
- Pentester, hacker, researcher, IT/HW/RF security enthusiast
- Especially interested in hardware hacking and wireless systems

Agenda

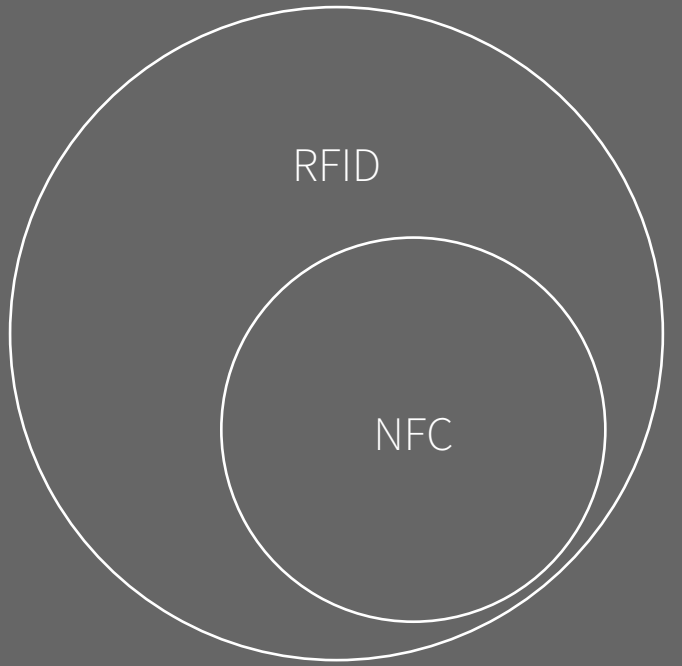
- What is this talk about and what not
- RFID/NFC basics
- Some details about MIFARE Classic and Legic Prime
- Examples and anecdotes of broken systems

What is this talk about

- What is it about
  - RFID/NFC hacking
  - Broken and old technologies
  - Stories and lessons learned from analyzing proprietary systems
- What is it NOT about
  - New and complicated hacks
  - EMV (credit cards, giro cards, Google/Apple Pay, etc.)

RFID/NFC basics

- RFID
  - Radio-Frequency Identification
  - Everything related to wireless identification
- NFC
  - Near Field Communication
  - Collection of standards and technologies (passive 13.56 MHz RFID tags, typically ISO 14443, ISO 15693, FeliCA)



Some fundamental differences

- Frequency
  - 13.56 MHz
  - 125 kHz (+/-)
  - ...
- Power
  - Passive
  - Active

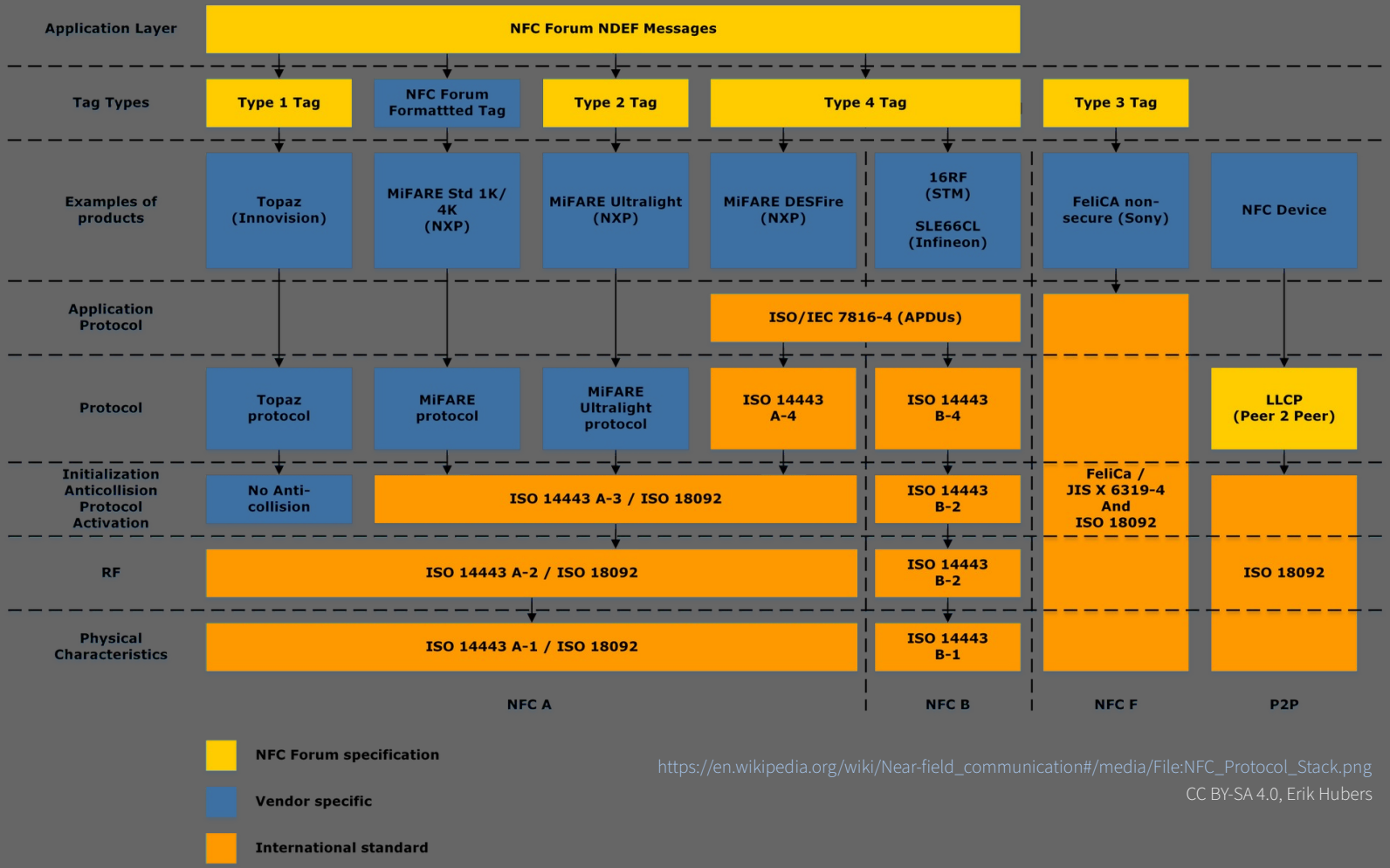
RFID/NFC technologies (extract)

13.56 MHz

- MIFARE Classic
- MIFARE DESFire EV1 / EV2
- MIFARE Ultralight / C
- Legic Prime / Advant
- NTAG 203
- Sony FeliCa
- ...

125 kHz (+/-)

- EM4xxx
- HID Prox
- Hitag 1 / 2 / S
- T55xx
- Viking
- FDX-B
- ...



https://en.wikipedia.org/wiki/Near-field_communication#/media/File:NFC_Protocol_Stack.png

MIFARE Classic
&
Legic Prime

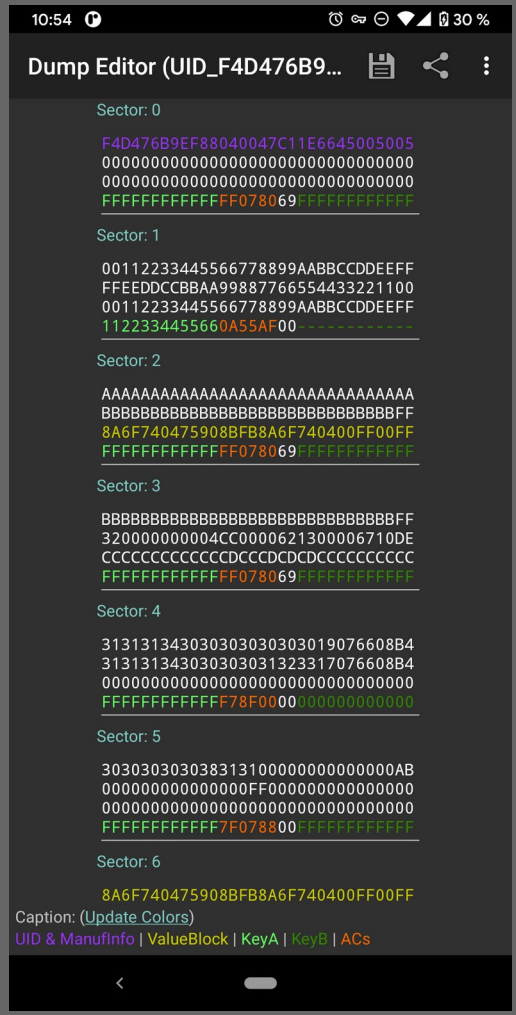
MIFARE Classic

- MIFARE is a series of chips by NXP (Classic, DESFire, Ultralight, etc.)
- Memory is divided into sectors and blocks
- Data can be protected with keys
- MIFARE Classic security is broken (since 2007!)
- MFC security got an updated around 2010 and was broken again around 2013/2015
- Proxmark3 (and other tools) can recover the keys

MIFARE Classic

97	7B	93	42	3D	88	04	00	43	28	2C	E6	00	0C	02	08	.{.B=...C(,.....
01	02	03	04	05	00	00	00	09	0A	0B	0C	0D	0E	80	79	...............y
11	09	09	20	01	12	01	6F	41	24	9F	09	11	66	08	3F	... ...oA$...f.?
E2	51	A9	DA	73	4D	63	C7	89	00	32	2C	9C	BB	E5	3F	.Q..sMc...2,...?
00	00	00	00	FF	FF	FF	FF	00	00	00	00	00	FF	00	FF	....
00	00	00	00	FF	FF	FF	FF	00	00	00	00	00	FF	00	FF	....
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	FF	....
38	41	56	08	19	0C	40	F7	8B	00	92	48	F9	4B	91	22	8AV...@....H.K."
12	01	0B	09	07	D9	0E	1D	00	00	00	00	00	00	00	23	.... #
12	01	0B	09	07	D9	0E	1D	00	00	00	00	00	00	00	23	.... #
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	FF	....
D2	B5	01	9A	33	56	72	D7	88	00	81	54	3A	CE	34	33	....3Vr....T:.43
31	08	20	15	30	00	00	00	0E	00	00	00	00	30	00	FD	1. .0........0..
31	00	00	00	21	05	40	30	30	00	00	00	00	67	91	5C	1...!.@00....g.\
01	03	20	15	34	F8	B8	B4	93	00	00	00	00	00	00	9B	.. .4...........
2A	31	66	C2	5A	1B	70	F7	88	00	E4	24	51	AB	0C	44	*1f.Z.p....$Q..D
31	30	34	35	30	31	32	30	30	30	30	09	11	66	08	BA	10450120000..f..
31	30	34	35	30	31	32	30	30	30	30	09	11	66	08	BA	10450120000..f..
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
85	1D	E7	BC	5B	A4	70	F7	88	00	27	48	A4	D9	E1	7A	....[.p...'H...z

Type	Mifare
Size	1024 Bytes
UID	977B9342
SAK	88
ATQA	0400
Name	Mifare Classic 1K



Legic Prime

- Legic is a series of chips (Prime, Advant)
- Not compatible with NFC/smartphones, but 13.56 MHz
- Memory is divided into segments
- Legic Prime security is broken (since 2008!)
- Proxmark3 (and other tools?) can read/write data

Legic Prime

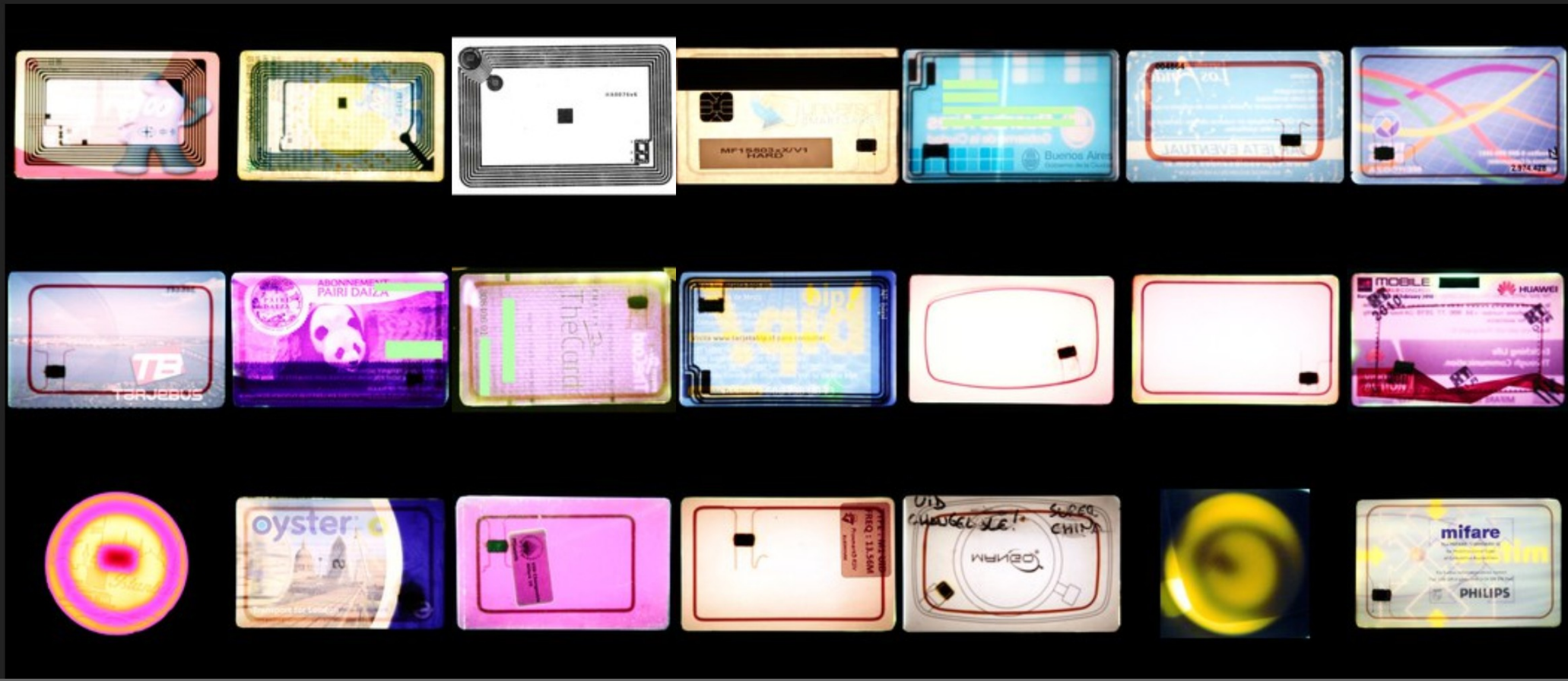
```
[=] --- Tag Information ---------------------------------------

[+]  CDF: System Area
[=] ------------------------------------------------------------
[+] MCD: 41 MSN: 8B 23 9B  MCC: CE ( ok )
[+] DCF: 60000 (60 ea) Token Type = IM-S (OLE = 0)
[+] WRP = 15 WRC = 1 RD = 1 SSC = FF
[+] Remaining Header Area
[+] 00 00 00 11 04 89 C0 04 C0 DD 83 00 00
[=] ------------------------------------------------------------
[=]
[+] ADF: User Area
[=] ------------------------------------------------------------
[+] Segment....... 01
[+] Raw header.... 0x16 0x40 0x0A 0x30
[+] Segment len... 22  Flag: 0x4 (valid:1 last:0)
[+]                WRP: 10 WRC: 03 RD: 0 CRC: 0xAF ( ok )
[=]
[+] WRC protected area:   (I 27 | K 0| WRC 3)
[=]
[=] ## | data                                            | ascii
[=] ---+------------------------------------------------+----------------
[=] 00 | FB 0A 01                                        | ...
[=] ---+------------------------------------------------+----------------
[=]
[+] Remaining write protected area:  (I 30 | K 30 | WRC 3 | WRP 10  WRP_LEN 7)
[=]
[=] ## | data                                            | ascii
[=] ---+------------------------------------------------+----------------
[=] 00 | 02 02 00 67 58 01 6D                            | ...gX.m
[=] ---+------------------------------------------------+----------------
[=]
[+] Remaining segment payload:  (I 37 | K 37 | Remain LEN 7)
[=]
[=] ## | data                                            | ascii
[=] ---+------------------------------------------------+----------------
[=] 00 | 00 00 00 00 00 00 00                            | .......
[=] ---+------------------------------------------------+----------------

[+] Segment....... 02
[+] Raw header.... 0xBA 0x40 0x04 0xC0
[+] Segment len... 186  Flag: 0x4 (valid:1 last:0)
[+]                WRP: 04 WRC: 04 RD: 1 CRC: 0xF0 ( ok )
[=]
```

Demos

- Identifying a tag
- Cracking MIFARE Classic keys
- Reading Legic Prime

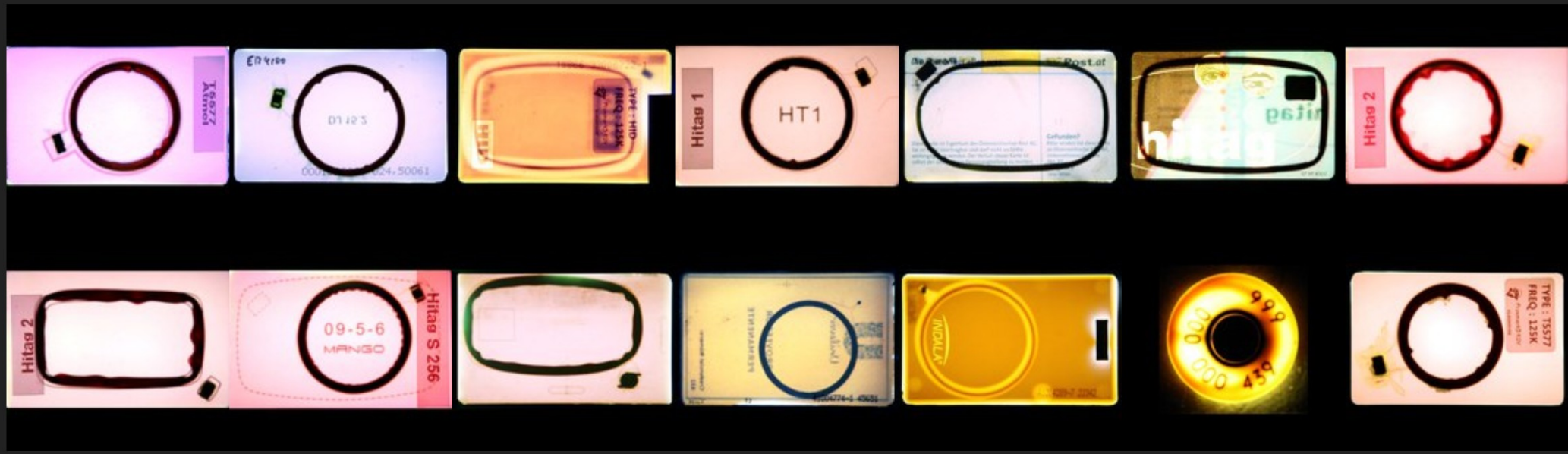
https://lab401.com/en-de/collections/rfid-tools
https://play.google.com/store/apps/details?id=com.nxp.taginfolite

NFC/RFID Gone Wild Gallery » See-through HF



https://doegox.github.io/rfidpics/#!/see-through_lf 150%

NFC/RFID Gone Wild Gallery » See-through LF

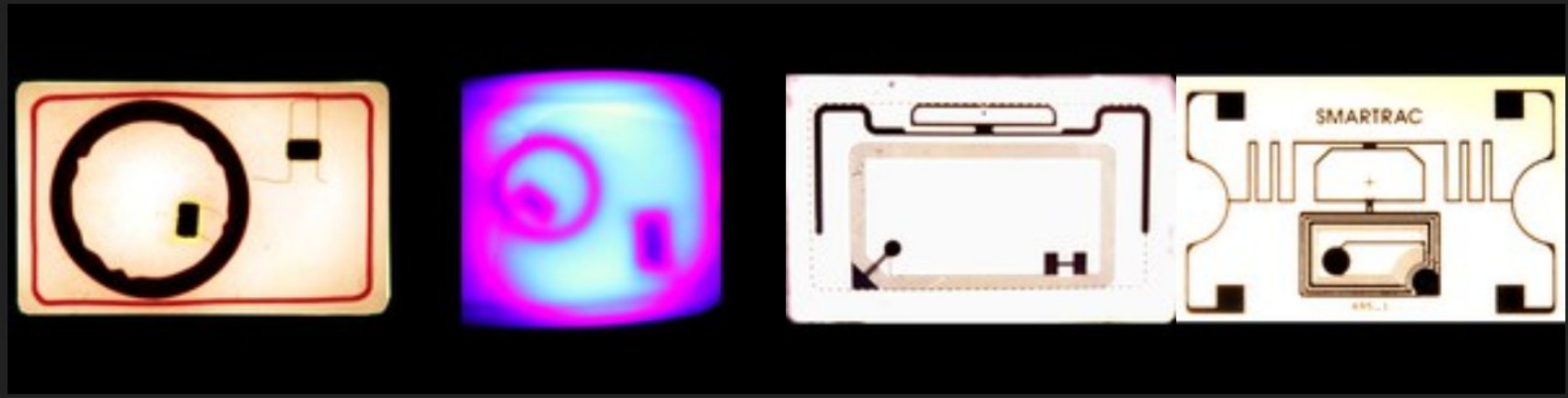


You want to contribute to this gallery? Just make a PR! See https://github.com/doegox/rfidpics

Powered by PhotoFloat

https://doegox.github.io/rfidpics/#!/see-through_dual

NFC/RFID Gone Wild Gallery » See-through Dual



You want to contribute to this gallery? Just make a PR! See https://github.com/doegox/rfidpics

Powered by PhotoFloat

Broken systems

- There will be no company names
- There will be no detailed instructions

- Fraud is illegal!
  Don’t try this at your university/company without consent!

System #1: (old) student ID cards

System #1: (old) student ID cards

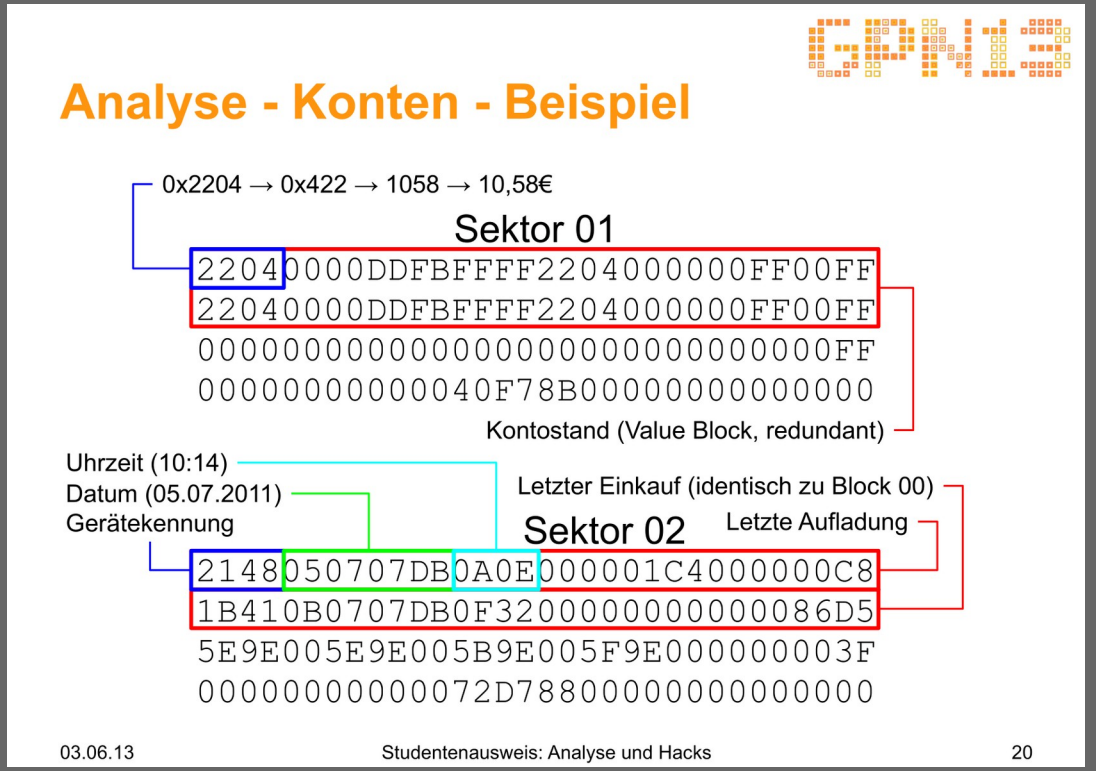
- A lot of universities/colleges have systems by the same company
- They were based on MIFARE Classic
  (now widely replaced by MIFARE DESFire)
- Money is stored in Value Blocks
- Most other data is only protected by a simple checksum
- Balance is not compared live with back end systems when shopping

System #1: (old) student ID cards

- Did a talk on the student ID cards back at GPN13

  https://entropia.de/GPN13:Analyse_des_Studentenausweises_und_daraus_resultierende_Hacks

- Yes, it was possible to get free drinks and access to every room



System #2: popular system/vendor

- “Wide spread” solution found in many companies
- Available with different card technologies
  - The one I checked used Legic Prime
- Some systems don’t compare the balance live when shopping
- Some systems are offline (e.g. vending machines)

System #2: popular system/vendor

System #3: infinite money without top up

- Legic Prime-based system
- There is a one byte checksum
  - Find the checksum algorithm: Legic CRC8
  - Find the data that are used in the checksum, e.g.
    `LegicCrc8(MCD, MSN0, MSN1, MSN2, WRC protected area, Remaining write protected area)`
  - Manipulate data at will
- Creating a card with high balance was possible

System #3: infinite money without top up

- Better: Program the card to a cost center

infinite money glitch

Privacy, simplified.

All | Images | Videos | News | Maps | Shopping | Chat | Settings

NEW! Explore DuckDuckGo's latest updates

France | Safe search: moderate | Any time | All sizes | All colors | All types | All layouts | All Licenses

1280 × 720
GTA V : INFINITE MONEY GLITCH !! (100k eve...
youtube.com

1280 × 720
"Infinite Money Glitch" - YouTube
youtube.com

1280 × 720
INFINITE Money Glitch Tutorial | Unlimited Monkey...
youtube.com

1280 × 720
Infinite Money Glitch IRL (FREE $$$) - YouTube
youtube.com

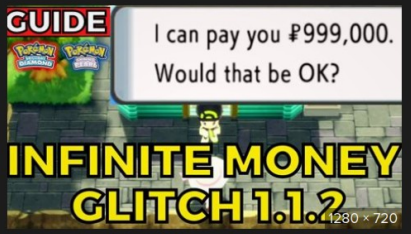
1125 × 1800
Infinite Money Glit...
goodreads.com

696 × 479
Cyberpunk 2077 Infinite Money Glitch G...
respawnfirst.com

1280 × 720
GTA 5 Infinite Money Glitch (Single Player) - YouTube
youtube.com

800 × 450
How to do an Easy GTA 5 infinite money glitch
sportskeeda.com

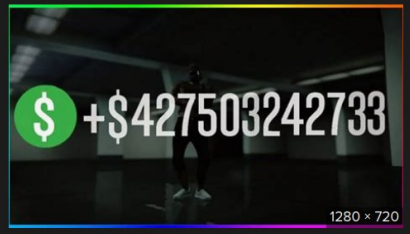
1280 × 720
GTA 5 : INFINITE MONEY Glitch "FREE MONEY" GTA...
youtube.com



1280 × 720
How to make Infinite Money Glitch 1.1.2. Guide Poke...
youtube.com

1280 × 720
Infinite Money Glitch in Borderlands 2 (2019) - YouTu...
youtube.com

1280 × 720
The QYLD Infinite Money Glitch Explained - YouTube
youtube.com

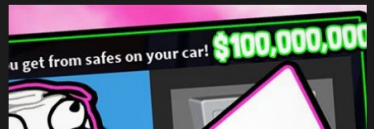


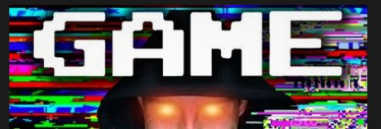
1280 × 720
UNLIMITED MONEY GLITCH In GTA 5 Online - (PS4, ...
youtube.com

1280 × 720
INFINITE MONEY GLITCH | BLOONS TD 6 - YouTube
youtube.com

1280 × 720
Infinite money GLITCH in Multiversus - YouTube
youtube.com

1280 × 720
Brand New Unlimited Money Glitch In Jailbreak?!! | H...
youtube.com





Share Feedback

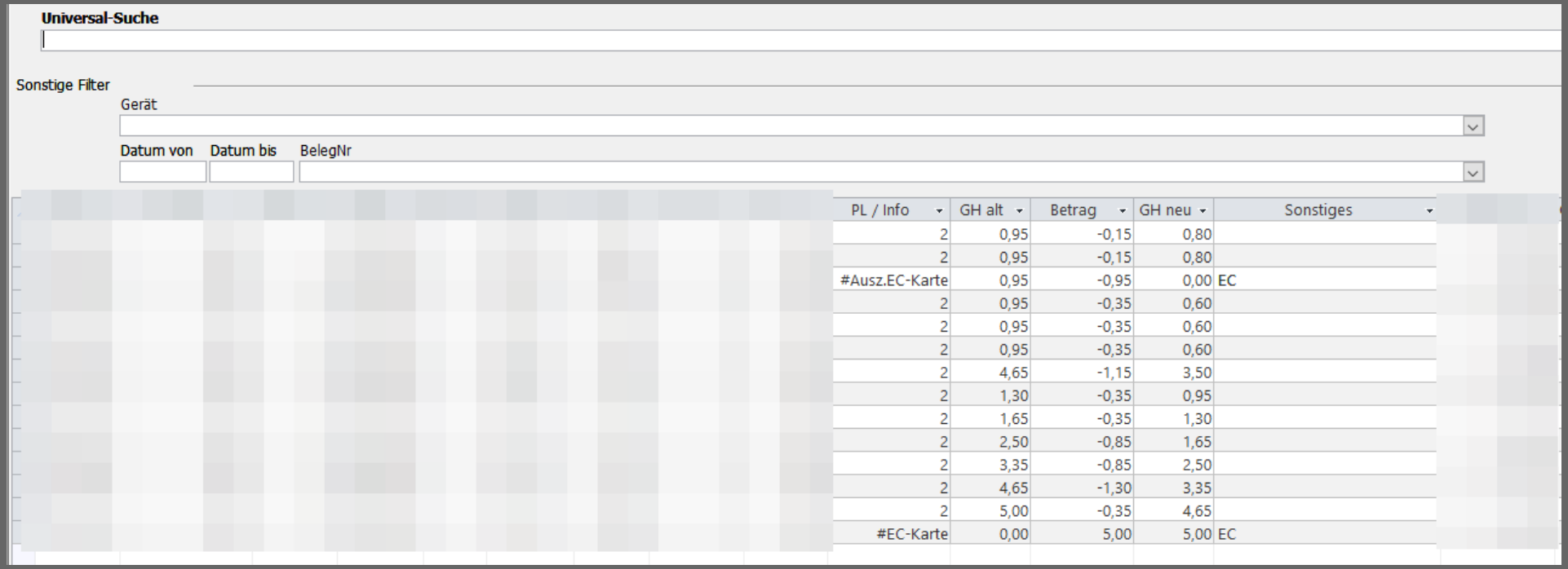
System #4: don’t know, don’t care

- MIFARE Classic-based system
- No time to analyze it: don’t know, don’t care
  1. Top up the card with 50€
  2. Read the card & make a backup
  3. Spend all the money
  4. Restore the backup
  5. Goto 3. & repeat

System #5: give me back “my” money

- MIFARE Classic-based system
- Guest card can be obtained from an “vending machine”
- Card can be toped up with money from an EC card
- After the visit the remaining balance can be payed out to the bank account of the EC card
- Back end system does not throw an error when the payout is higher than the amount initially loaded onto the card

System #5: give me back “my” money



PL / Info	GH alt	Betrag	GH neu	Sonstiges
2	0,95	-0,15	0,80	
2	0,95	-0,15	0,80	
#Ausz.EC-Karte	0,95	-0,95	0,00	EC
2	0,95	-0,35	0,60	
2	0,95	-0,35	0,60	
2	0,95	-0,35	0,60	
2	4,65	-1,15	3,50	
2	1,30	-0,35	0,95	
2	1,65	-0,35	1,30	
2	2,50	-0,85	1,65	
2	3,35	-0,85	2,50	
2	4,65	-1,30	3,35	
2	5,00	-0,35	4,65	
#EC-Karte	0,00	5,00	5,00	EC

System #6: the gift of free money

- Gift cards at an Irish Pub
- Can be toped up with freely a choosable amount before gifting
- MIFARE Classic-based system
- POS system does not track the gift cards and their balance

System #6: the gift of free money

Free drinks and all you can eat!

Lessons learned

- Don’t use insecure RFID/NFC technologies
- Use online systems (check balance with back end systems)
- Be responsible! Get consent!

Questions?

CONTACT:
𝕏 @iiiikarus · www.icaria.de · contact@icaria.de