

The Modern Hacker – From Insight to Impact

Karsten Nohl <nohl@srlabs.de>



Security
Research
Labs

Nice to meet you



Karsten Nohl

Chief Scientist at
SRLabs and
Autobahn Security

Trained
cryptographer from
a time when crypto
meant 'encryption'

Passionate white hat
telco hacker

The Hacking Community has come a long way

Companies
vs
Hacking



Companies
fear & respect
Hackers



Joining forces
against
Criminals

The Hacking Community has come a long way

Companies
vs
Hacking



Companies
fear & respect
Hackers



Joining forces
against
Criminals

- 1 Feuding at a distance
- 2 Clashing mindsets

- 3 Demanding change
- 4 Co-working solutions

- 5 Driving change
- 6 Co-piloting evolution

The Hacking Community has come a long way

Companies
vs
Hacking



Companies
fear & respect
Hackers



Joining forces
against
Criminals

- 1 Feuding at a distance
- 2 Clashing mindsets

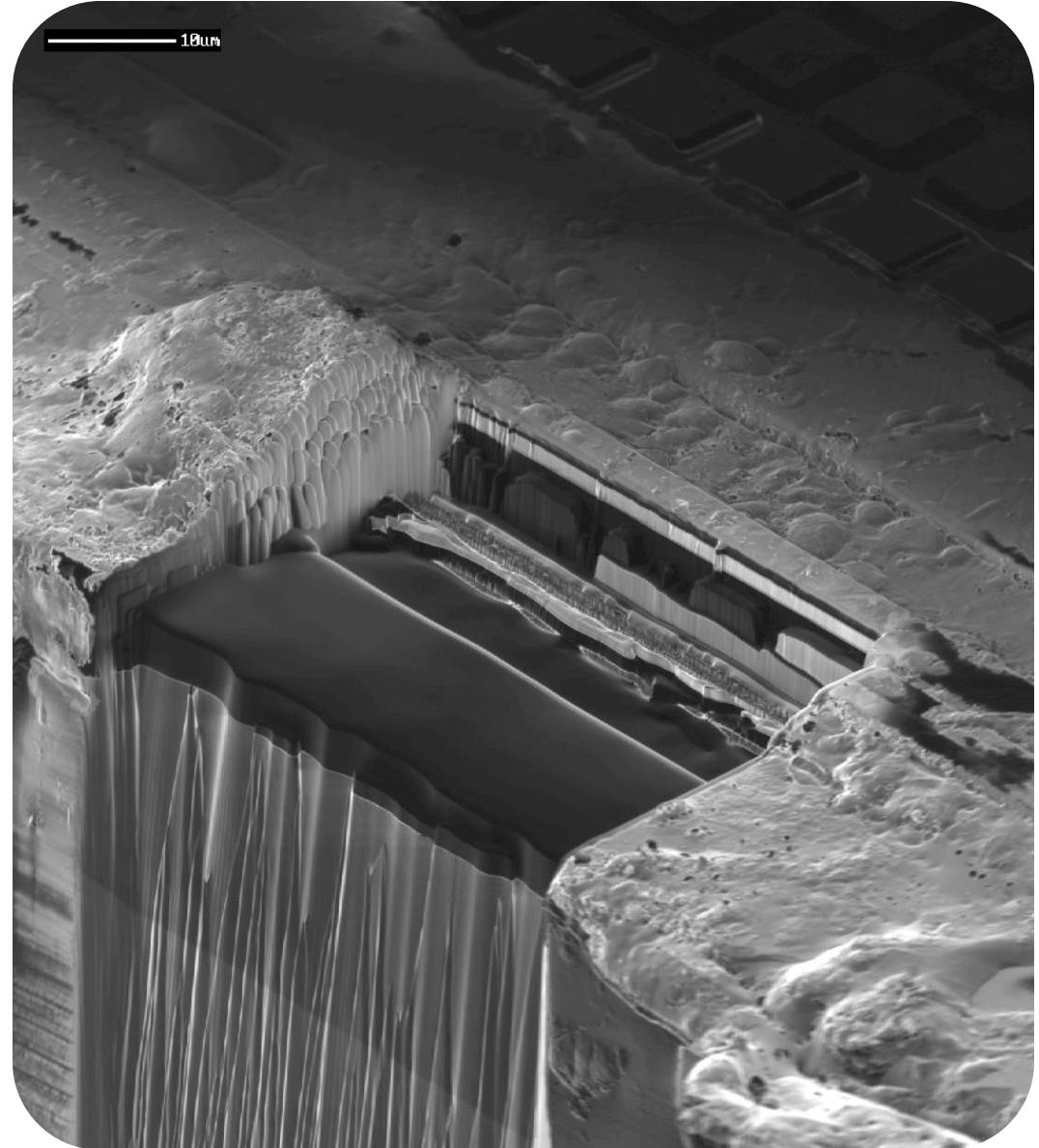
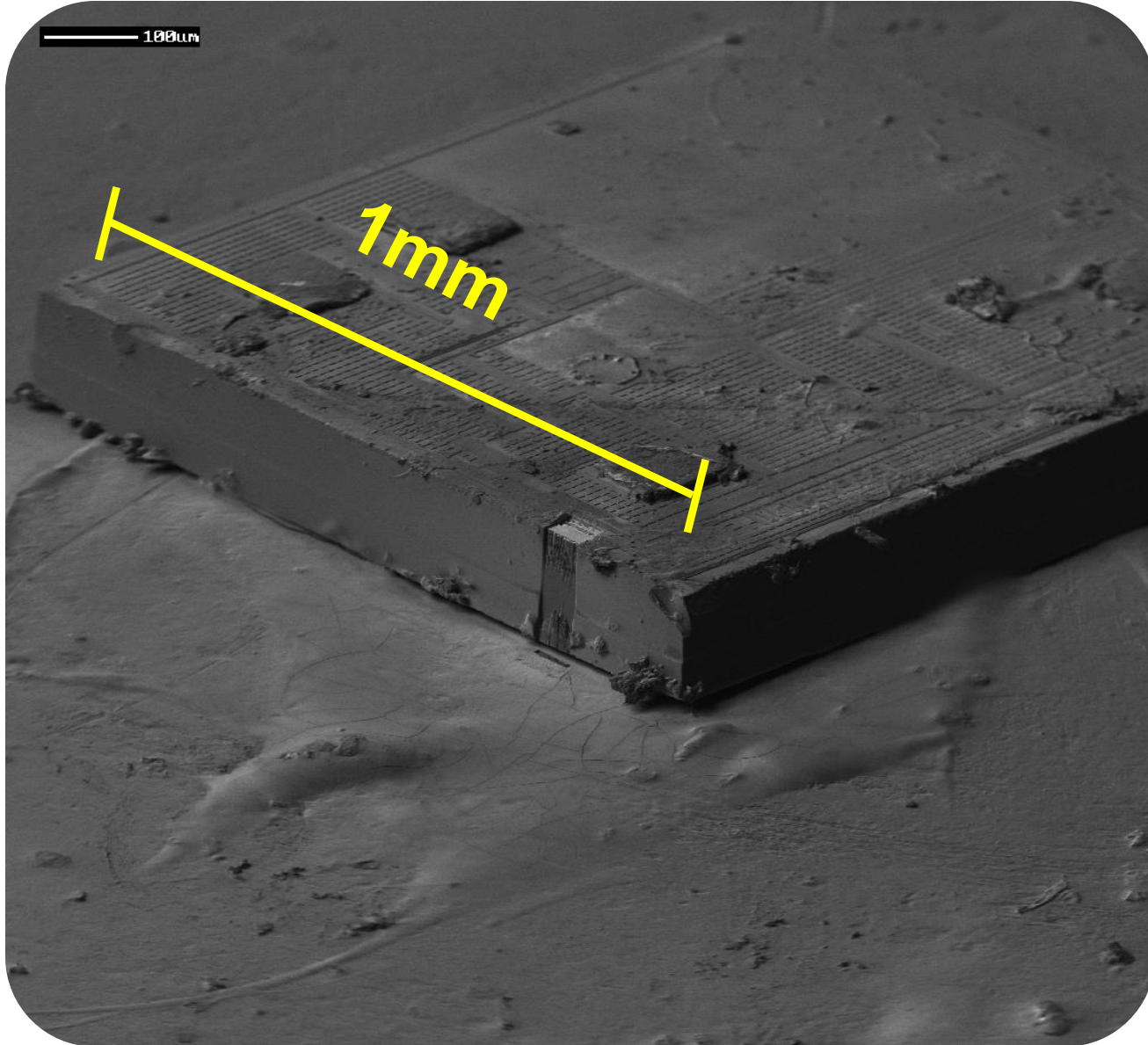
- 3 Demanding change
- 4 Co-working solutions

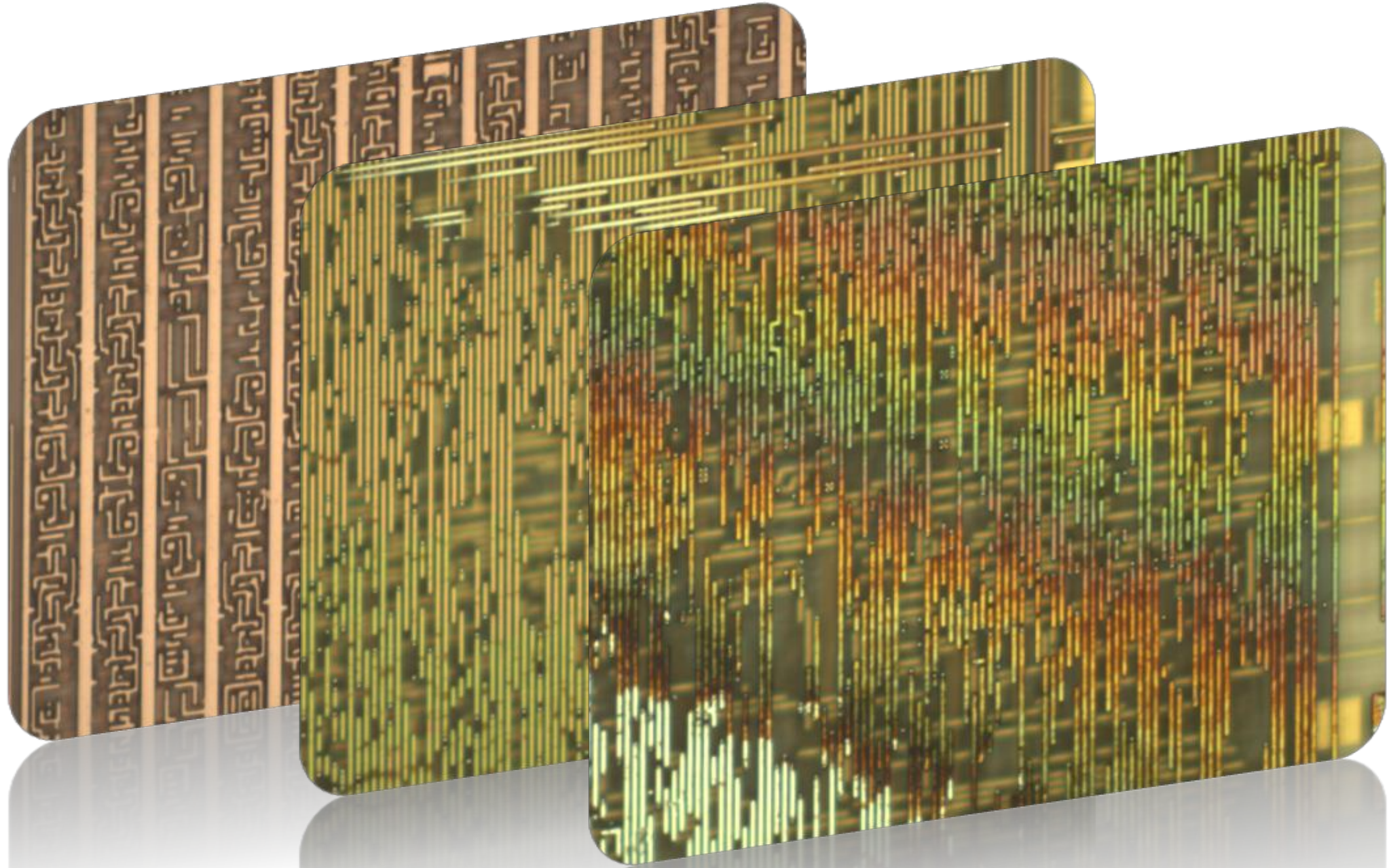
- 5 Driving change
- 6 Co-piloting evolution

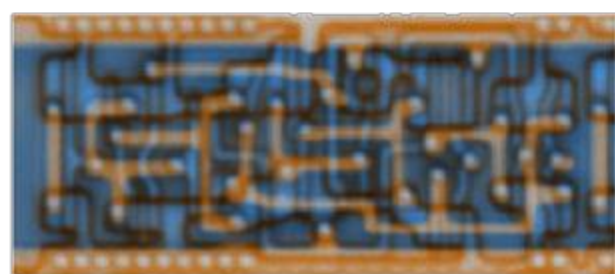
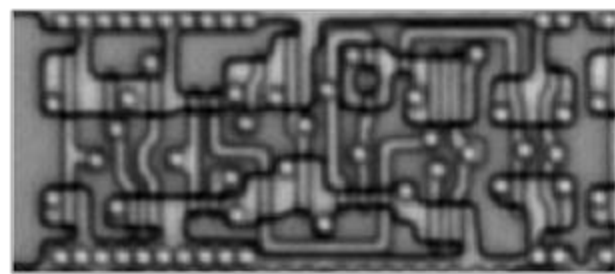
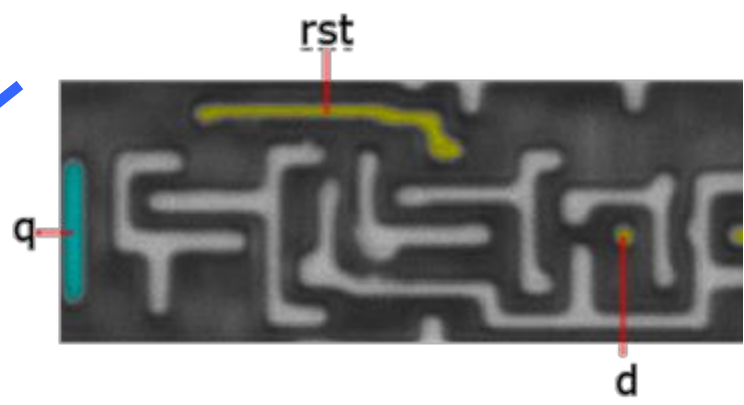
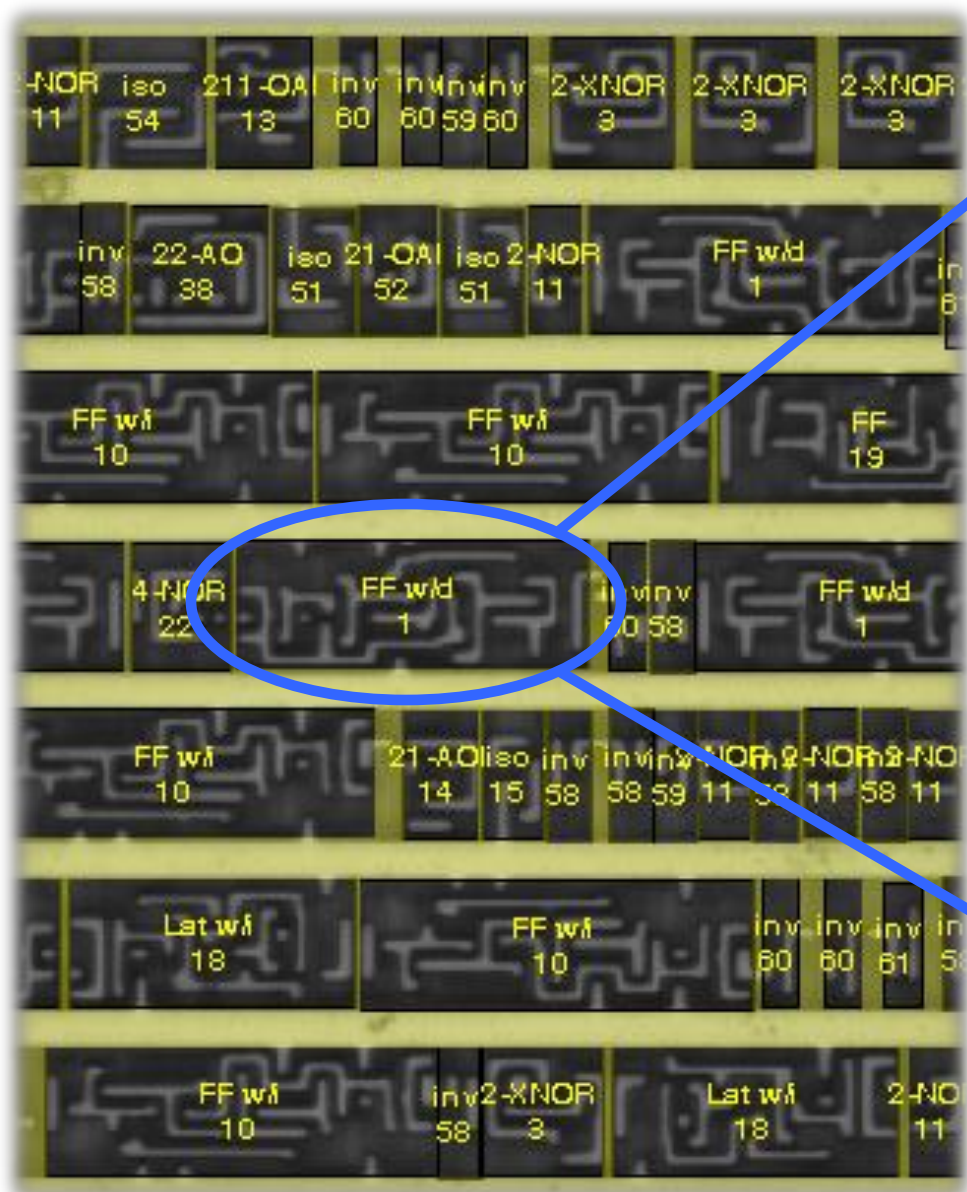
- 1 Feuding at a distance:**
Spending 3 years just to make a point

Hacking is perpetual curiosity
about how things work & how
you can influence them to
work differently

Mifare Classic RFID tags tried to hide secret cipher in silicon die







degate - [~/home/martin/Development/degate3/2011-02-06_0045_degat*] [1/3]

Project View Tools Layer Logic Gate Recognition Help

5300 5400 5500 5600 5700 5800 5900 6000 6100 6200 6300 6400 6500 6600 6700 6800 6900 7000

Logic gates

| Short Name | # | Width | Height | Fill color | Frame color | Description |
|------------|----|-------|--------|------------|-------------|-----------------------|
| 01-FF | 58 | 272 | 134 | | | D-Q-FlipFlop |
| 02-FF | 11 | 343 | 134 | | | D-Q-FlipFlop with rst |
| 03-FF | 17 | 343 | 133 | | | D-Q-FlipFlop with rts |
| 04-BUF | 5 | 226 | 128 | | | |
| 05-3XOR | 13 | 249 | 133 | | | |
| 06: 2-XNOR | 12 | 133 | 133 | | | |

Edit Add Remove Close

Edit gate

Entity Behaviour Layout

Short name: 02-FF

Description: D-Q-FlipFlop with rst

Logic Class: flipflop (generic)

| Port ID | Port Name | Port Description | In | Out |
|---------|-----------|------------------|-------------------------------------|-------------------------------------|
| 2384 | !Q | !Q | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 2380 | Q | Q | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 2388 | clk | clk | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| 2386 | D | D | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| 2382 | rst | rst | <input checked="" type="checkbox"/> | <input type="checkbox"/> |

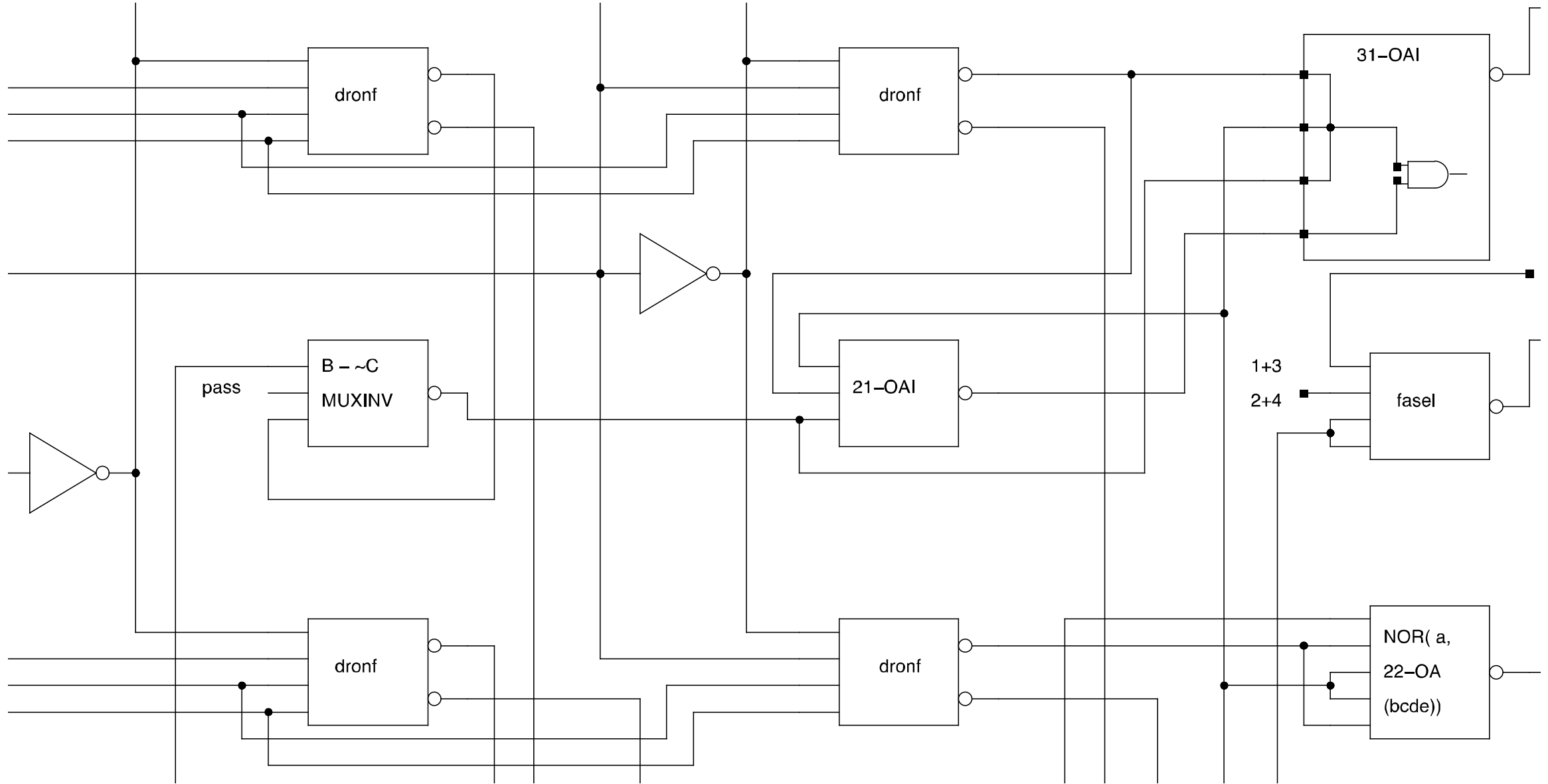
Fill color: Reset Color

Frame color: Reset Color

Cancel OK

Autosaving project data ... done.

The result of a three-year journey: Fully understanding the algorithm inside the “secret” chip





Home > Mobile > Mobile Apps

NEWS

RFID hack could crack open 2 billion smart cards

Analyst: One European government sent armed guards to protect facilities using the card



Responsibly disclosure requires some level of mutual understanding



Knee jerk by the company

Media reports: “NXP executives have downplayed the severity: The attack defeats only a single layer of security and **additional security layers prevent misuse.**”



Knee jerk by us

Double down: **Find and publish exploits** for Mifare Classic – a tradition that continues until today



Slow relationship building

Working together to understand the problem and the solution
... and to **understand each other** (Thank you, Matthias!)
=> The essence of **responsible disclosure**

2 Clashing mindsets:
"Can we buy your silence?"

Some companies lack the base understanding of what drives hackers



Knee jerk by the company

- “Sign a contract so you will never tell anyone about the vulnerabilities you discovered”
- “Only then will we consider looking into to vulnerabilities” (Several remain open.)

The Hacking Community has come a long way

Companies
vs
Hacking



Companies
fear & respect
Hackers



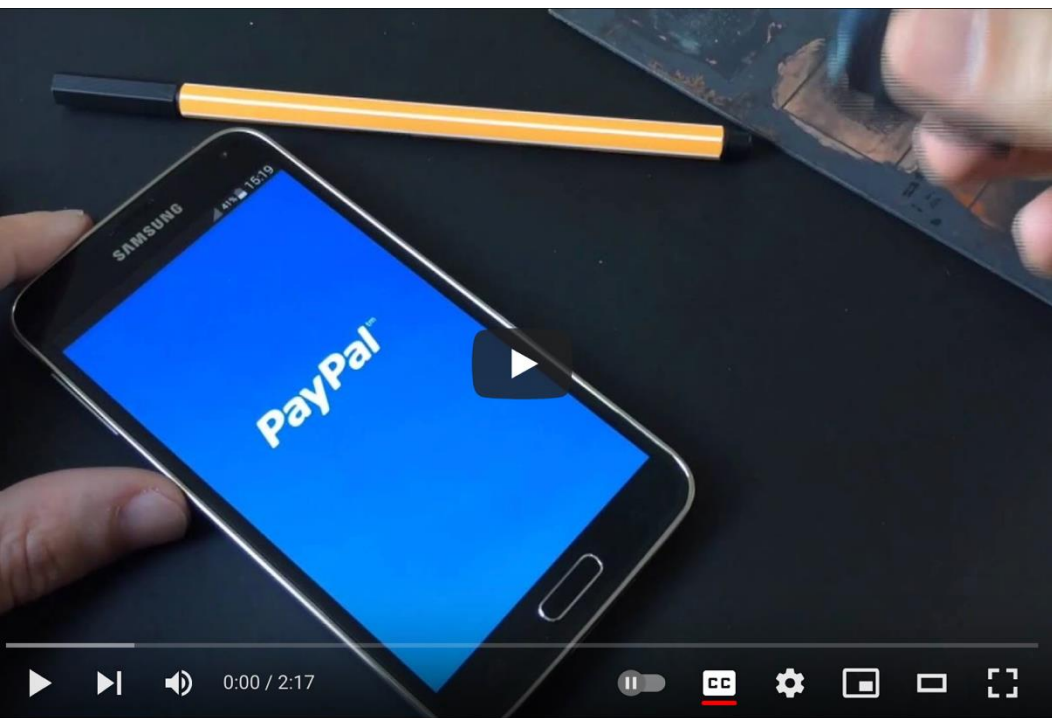
Joining forces
against
Criminals

- 1 Feuding at a distance
- 2 Clashing mindsets


- 3 Demanding change
- 4 Co-working solutions


- 5 Driving change
- 6 Co-piloting evolution


3 Demanding change:
Instant product feedback




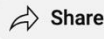
Samsung Galaxy S5 Finger Scanner also susceptible to ordinary spoofs


 Security Res...
3.19K subscribers

 Subscribed

 1.6K

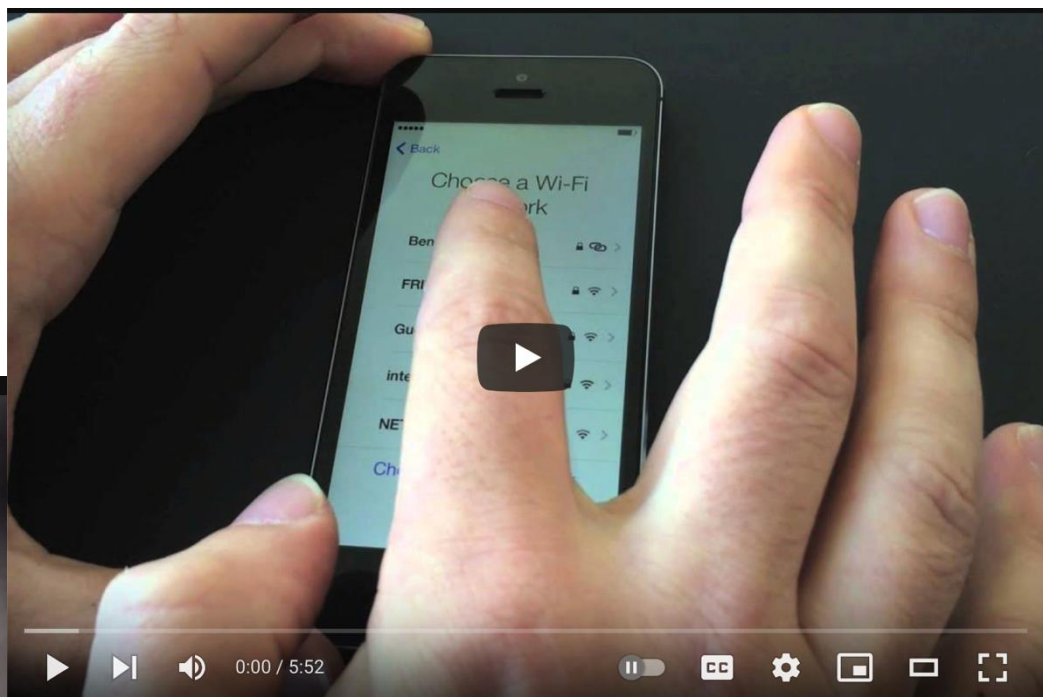
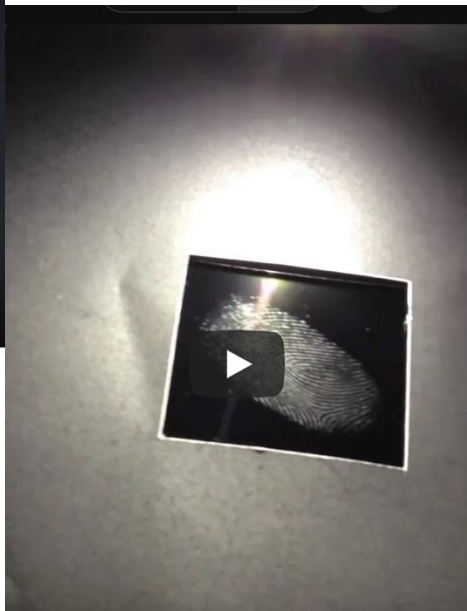


 Share





1.2M views 10 years ago


This video demonstrates how flaws in the implementation of fingerprint authentication in the Samsung Galaxy S5 expose users' devices, data, and even bank accounts to thieves or other attackers.




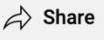
Flaws in iOS 7 allow stolen iPhone to hijack Apple ID despite remote wipe


 Security Res...
3.19K subscribers

 Subscribed

 2.8K



 Share




1.3M views 10 years ago


<https://srlabs.de/spoofing-fingerprints/>


The iPhone 5s's fingerprint sensor does not only appear to provide no additional protection, its use even undermines other security mechanisms. This video demonstrates how other flaws in iOS and iClo...more





iPhone 5s Touch ID susceptible to fingerprint spoofs


 Security Res...
3.19K subscribers

 Subscribed

 284



 Share



113K views 10 years ago

Published on Sep 24, 2013, More info: <https://srlabs.de/spoofing-fingerprints/>

The Apple iPhone 5s's Touch ID fingerprint authentication system can be bypassed using information gathered from latent prints left on the victim phone's display using the camera on the iPhone 4S, ...more

Co-working solutions:

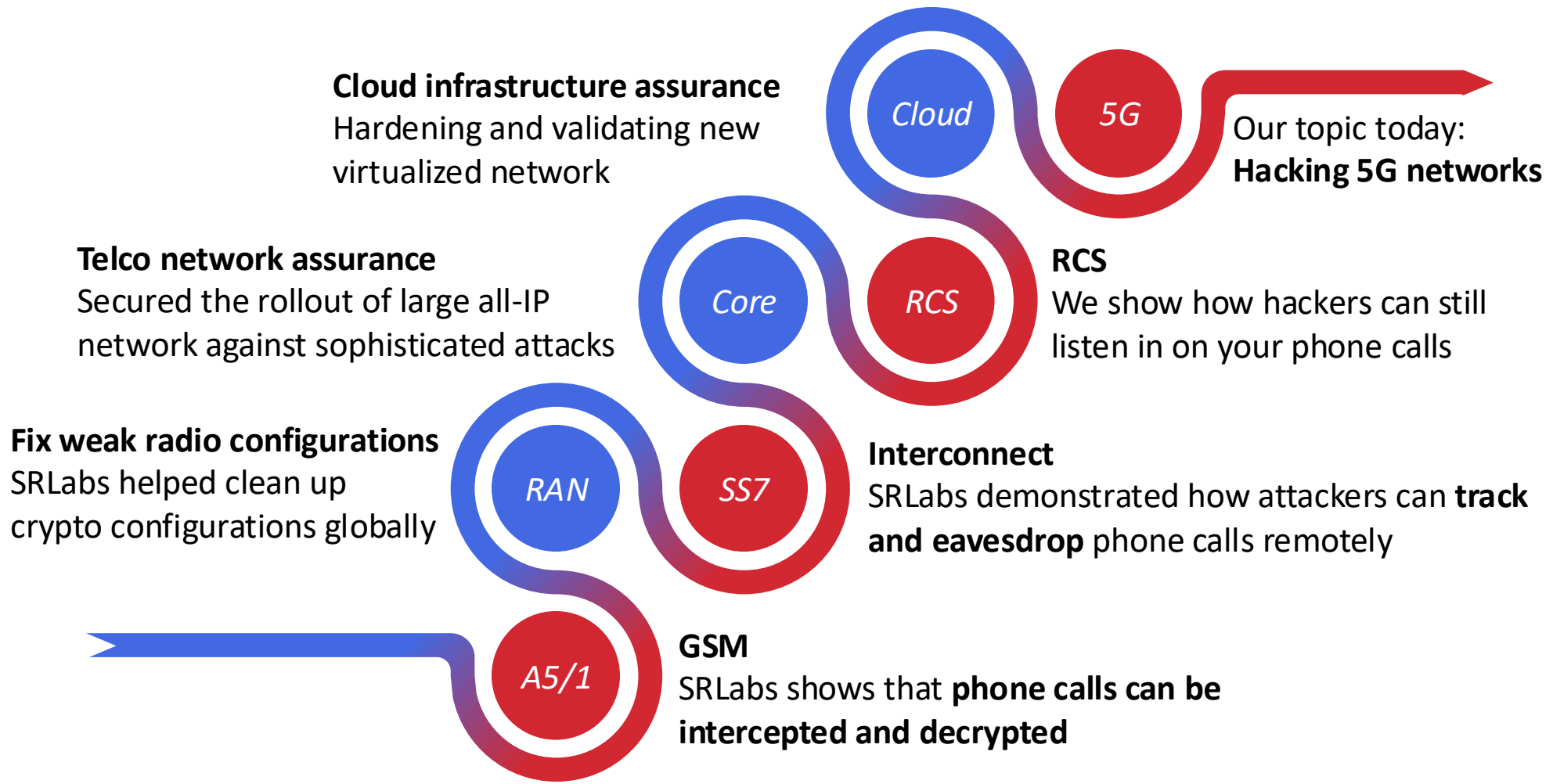
- 4** Staying engaged until the path forward is cleared

Hacking telcos since before it was cool.



We have been finding security issues in mobile networks for over a decade, and regularly help to fix them

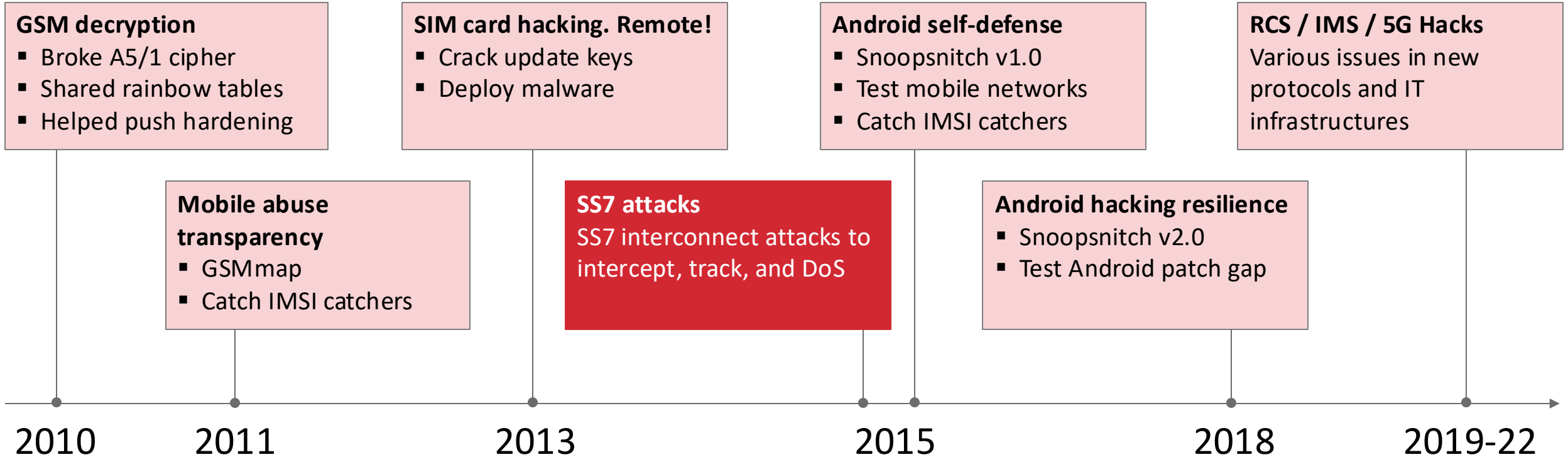
The symbiosis of mobile network hacking **research** and **risk management** for mobile networks



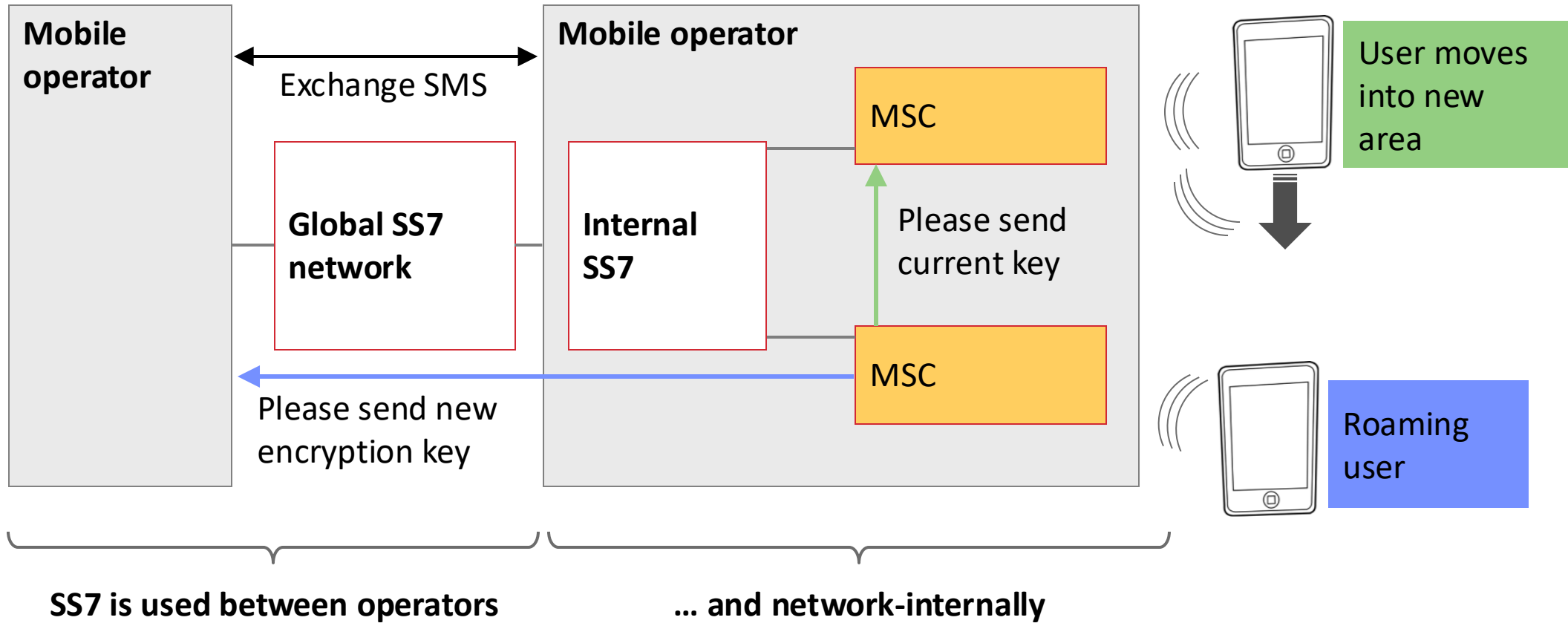
Telco hacking heros

- | | |
|---|------------------------|
|  | Luca Melette |
|  | Jakob Lell |
|  | Sina Yazdanmehr |
|  | Linus Neumann |

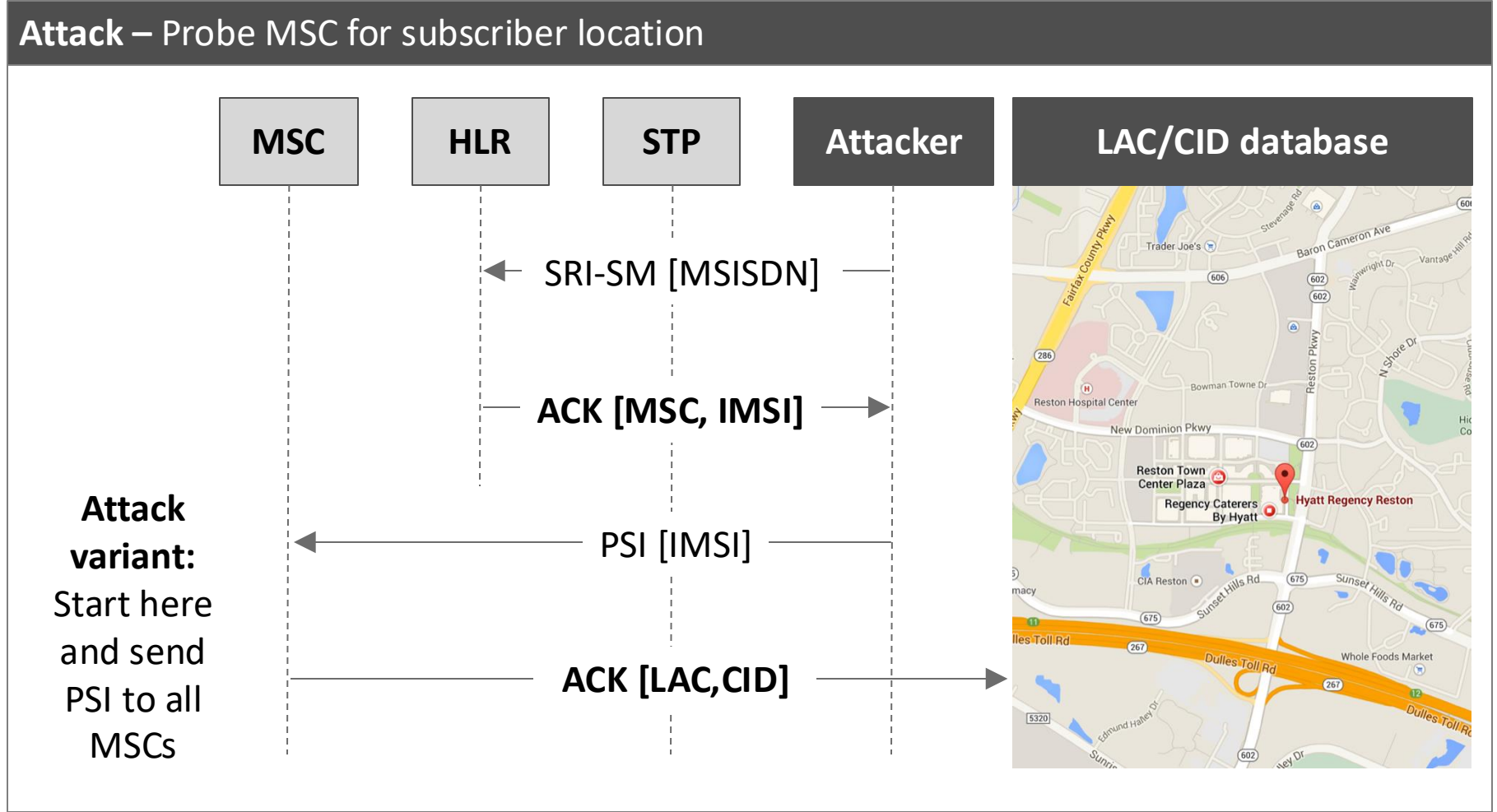
Mobile hacking journey at SRLabs



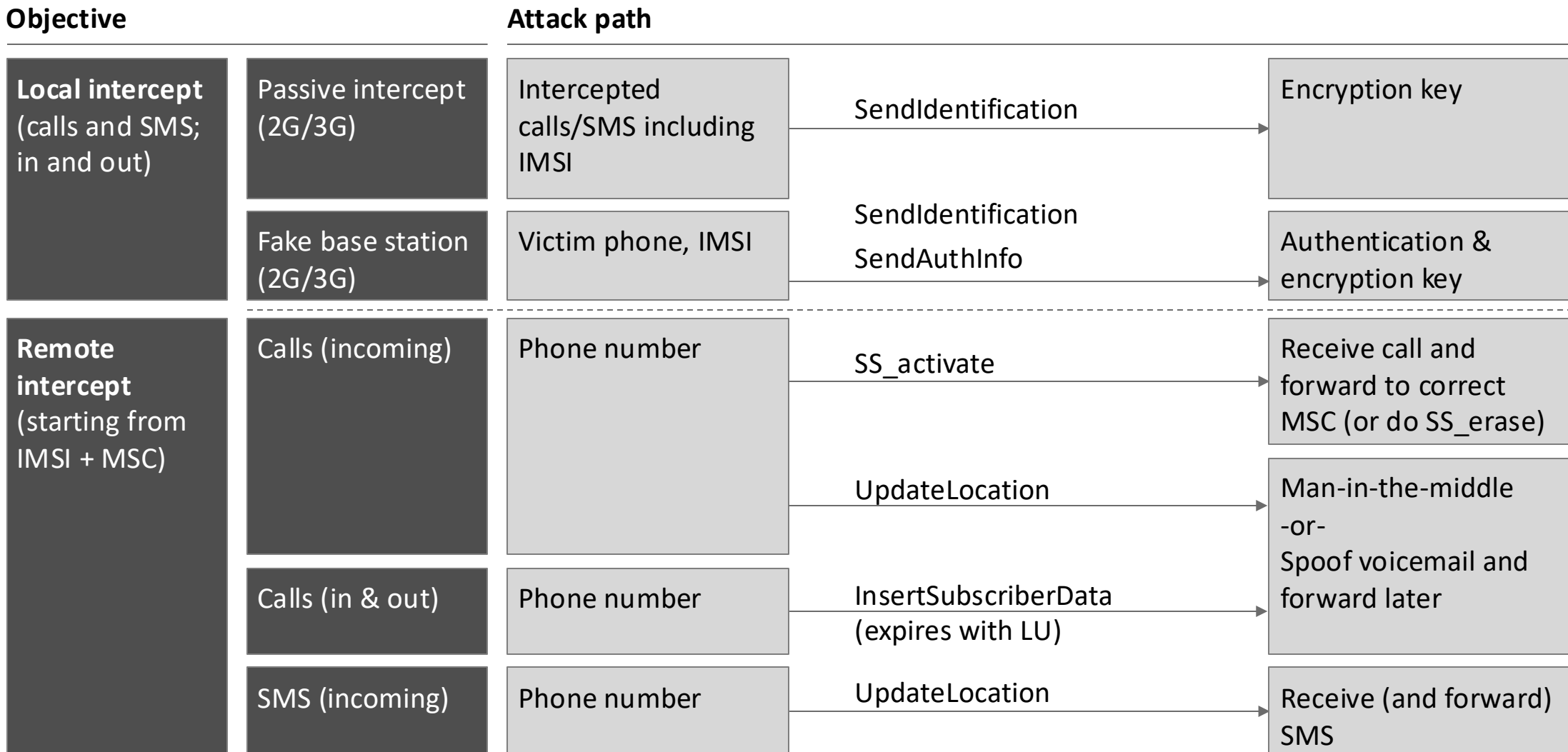
SS7 network enables exchange of SMS and cryptographic keys



Most common abuse case: Subscriber location is retrieved over SS7



Various signaling messages enable local and remote **intercept** attacks



Three GSMA standards provide advice on how to protect from SS7 attacks

FS.07 - SS7 and SIGTRAN Network Security

- 8 Recommendations and Countermeasures**
- 8.1 SCCP Global Title Anti-Spoofing
- 8.2 MAP Screening Policy Guidelines
 - 8.2.1 Category 1
 - 8.2.2 Category 2
 - 8.2.3 Category 3
 - 8.2.4 Filtering Considerations

FS.11 - SS7 Interconnect Security Monitoring and Firewall Guidelines

- Annex B SS7 Firewall Recommendations**
- B.1 Introduction
- B.2 Definitions
- B.3 SS7 Firewall Rules
 - B.3.1 SS7 Firewall Rules for MAP
 - B.3.1.1 MAP Category 1
 - B.3.1.2 MAP Category 2
 - B.3.1.3 MAP Category 3
 - B.3.1.4 Specific Handling of Mixed Category MAP Messages
 - B.3.1.5 MAP GroupCall / CUG
 - B.3.1.6 MAP CCBS
 - B.3.1.7 MAP gsmSCF
 - B.3.1.8 MAP Handover
 - B.3.1.9 MAP 'Reasonableness' / 'Velocity' Check
 - B.3.1.10 Application Context and MAP versions
 - B.3.2 SS7 Firewall Rules for CAMEL
 - B.3.2.1 CAMEL Category 2
 - B.3.2.2 CAMEL Category 3

IR.82 - SS7 Security Network Implementation Guidelines

- 3 Possible Solutions for SS7 Vulnerabilities**
- 3.1 Common Filtering Features
- 3.2 Filtering Features per Category
 - 3.2.1 MAP- Category 1
 - 3.2.2 MAP - Category 2
 - 3.2.3 MAP - Category 3
 - 3.2.4 CAP - Category 2
 - 3.2.5 CAP - Category 3
- 3.3 Filtering Features Description
 - 3.3.1 MAP screening (Op, CgGT)
 - 3.3.2 MAP screening (Op, GT, IMSI)
 - 3.3.3 Compare current VLR and Cg SCCP
 - 3.3.4 Compare IMSI and HLR
 - 3.3.5 Compare IMSI and gsmSCF
 - 3.3.6 SMS Home Routing
 - 3.3.7 Check CgGT spoofing
 - 3.3.8 Check Location
- 3.4 Passive monitoring

Interconnect security might still be the weakest link of most telcos today

Threat

- Interconnect hacking is possible since the adoption of the global SS7 network around 30 years ago
- **Public awareness of the hacking technique has been raised since at least 2014**
- One main risk today is intercept of SMS 2-factor codes, which has led to online identify theft and online banking fraud

Australian senator hacked over SS7 in 2015

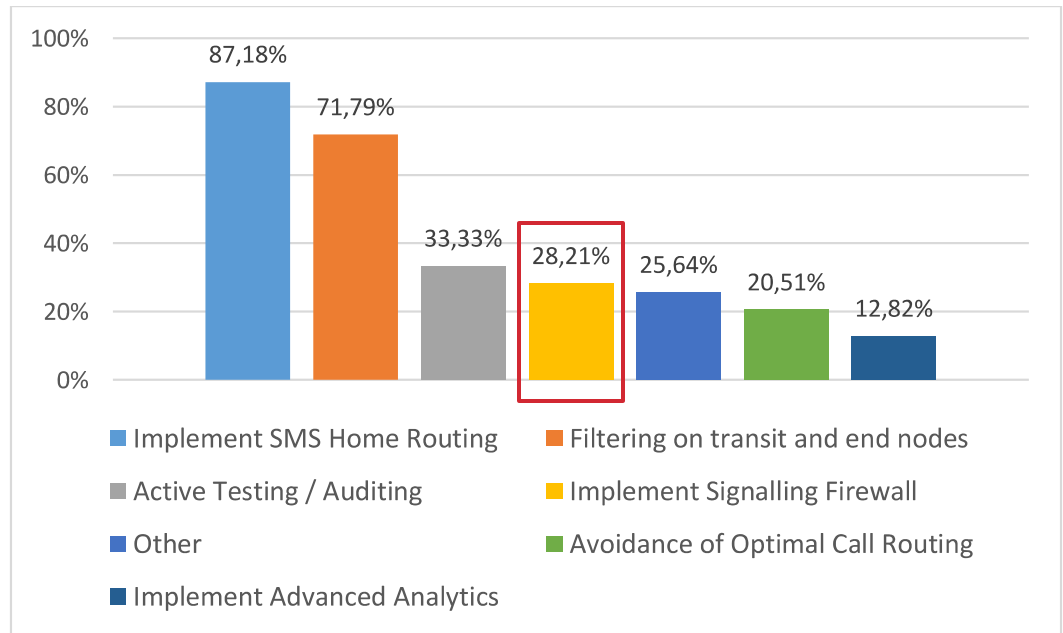


Defenses

- Most SS7 hacking can be prevented with an interconnect/signaling firewall
- **Most telcos do not have this protection**

2.1.2 Security measures in place

Several questions were asked about the available measures in place. Pls. find below the answers provided.



Source: ENISA report *Signalling Security in Telecom*, covers 39 EU telcos, prepared for the EU Commission, **March 2018**

The Hacking Community has come a long way

Companies
vs
Hacking



Companies
fear & respect
Hackers



Joining forces
against
Criminals

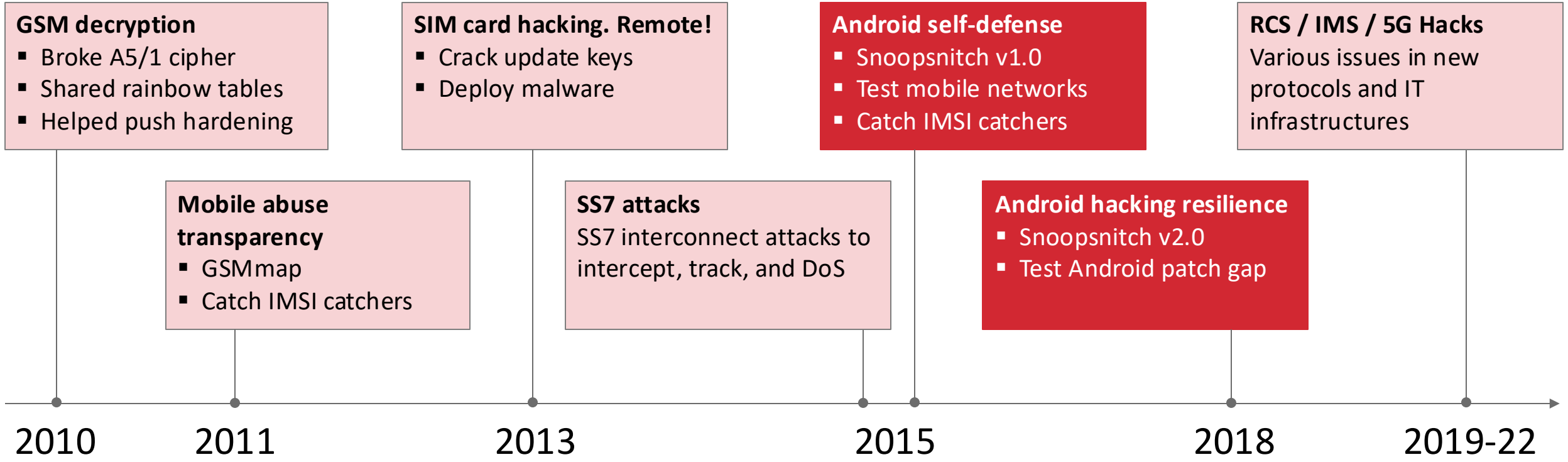
- 1 Feuding at a distance
- 2 Clashing mindsets

- 3 Demanding change
- 4 Co-working solutions


- 5 Driving change
- 6 Co-piloting evolution

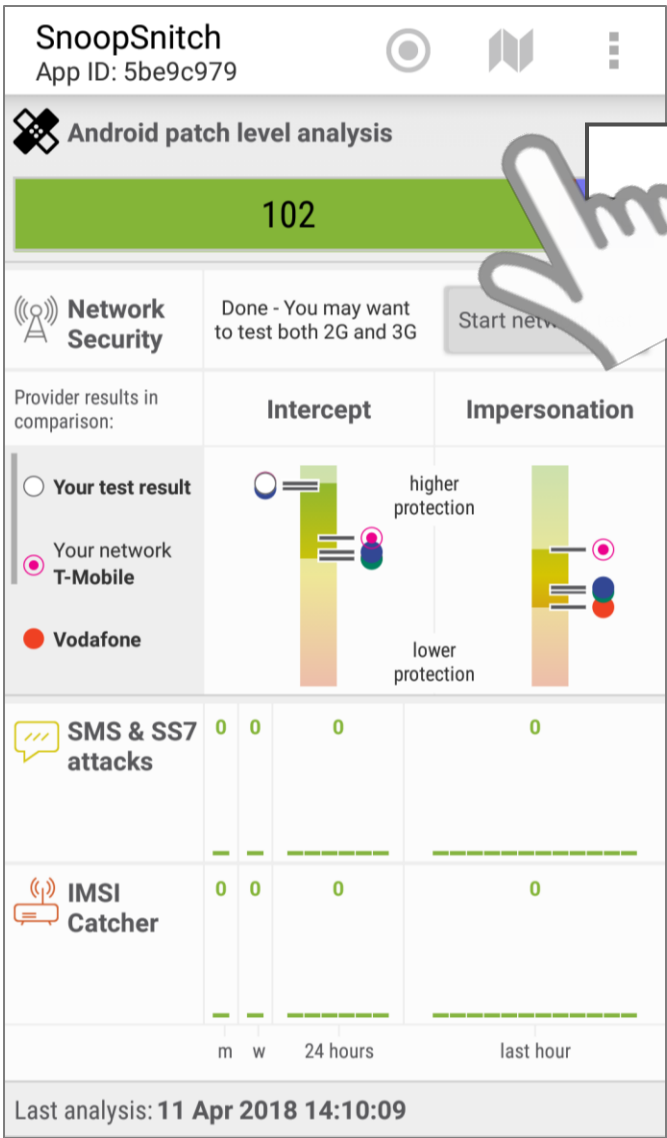
5 **Driving change:**
Community-driven Security “KPIs”

Mobile hacking journey at SRLabs



SnoopSnitch provides patch analysis for Android users

| |
|--|
| Tool name |
| SnoopSnitch |
| Purpose |
| <ul style="list-style-type: none"> ▪ Detect potentially missing Android security patches ▪ Collect network traces on Android phone and analyze for abuse ▪ Optionally, upload network traces to GSMmap for further analysis |
| Requirements |
| <ul style="list-style-type: none"> ▪ Android version 5.0 ▪ Patch level analysis: All phones incl. non-rooted ▪ Network attack monitoring: Rooted Qualcomm-based phone |
| Source |
|  Search: <i>SnoopSnitch</i> |



SnoopSnitch
App ID: 5be9c979

Android patch level analysis

102

Network Security Done - You may want to test both 2G and 3G Start net...

Provider results in comparison:

Your test result

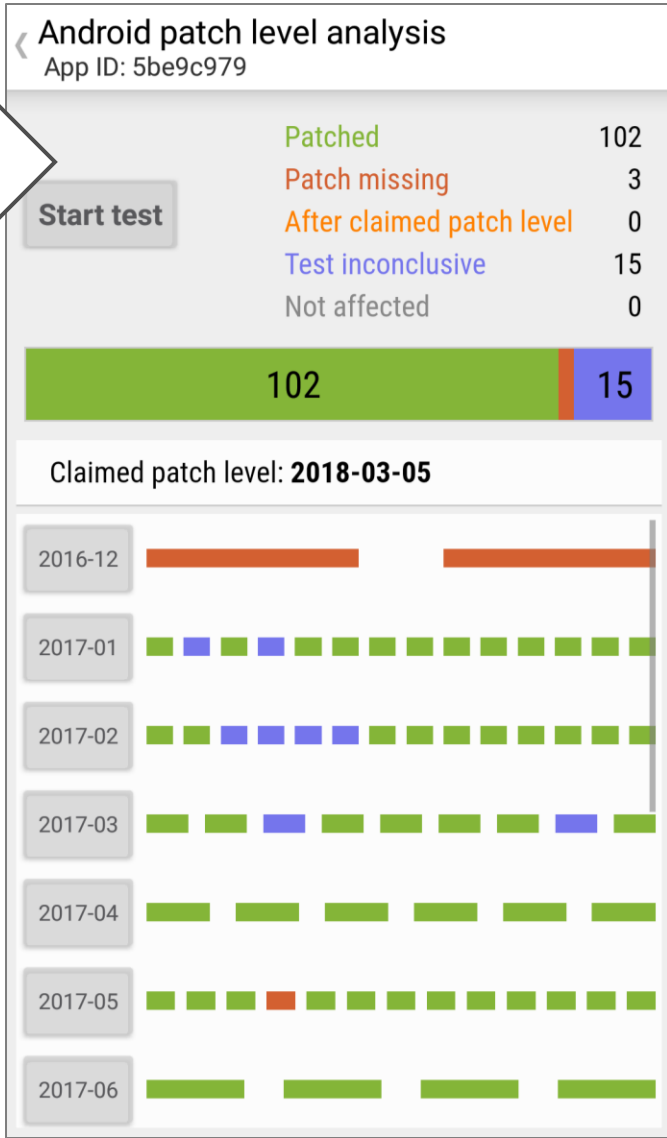
Your network T-Mobile

Vodafone

| | Intercept | Impersonation |
|------------------------------|-----------|---------------|
| SMS & SS7 attacks | 0 0 0 | 0 |
| IMSI Catcher | 0 0 0 | 0 |

m w 24 hours last hour

Last analysis: 11 Apr 2018 14:10:09



Android patch level analysis
App ID: 5be9c979

Start test

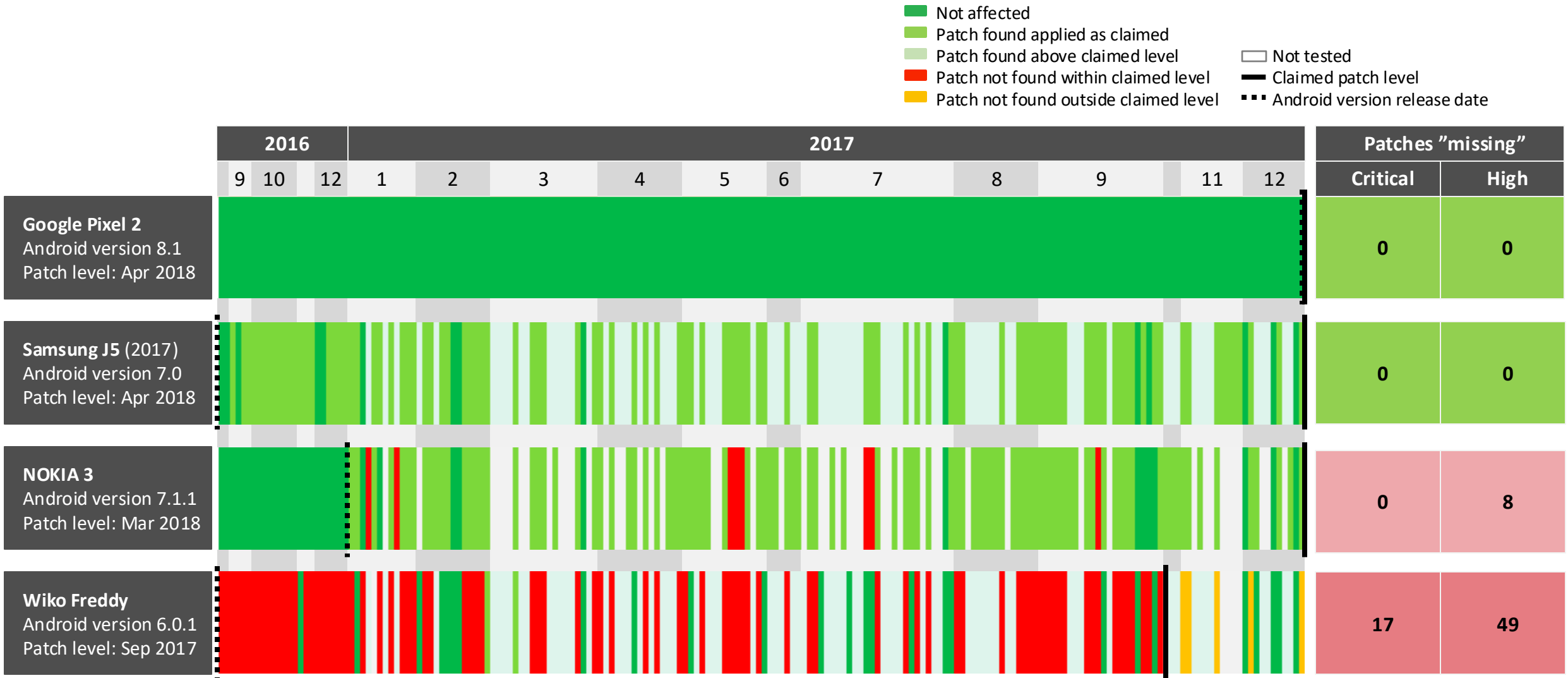
| | |
|---------------------------|-----|
| Patched | 102 |
| Patch missing | 3 |
| After claimed patch level | 0 |
| Test inconclusive | 15 |
| Not affected | 0 |

102 15

Claimed patch level: **2018-03-05**

| | |
|---------|----------------------------|
| 2016-12 | Orange bar |
| 2017-01 | Green bar |
| 2017-02 | Green bar |
| 2017-03 | Green bar |
| 2017-04 | Green bar |
| 2017-05 | Green bar with red segment |
| 2017-06 | Green bar |

The Android patch gap in 2018: Patching completeness varied widely for different phones



Patch gap started closing
in response to our research

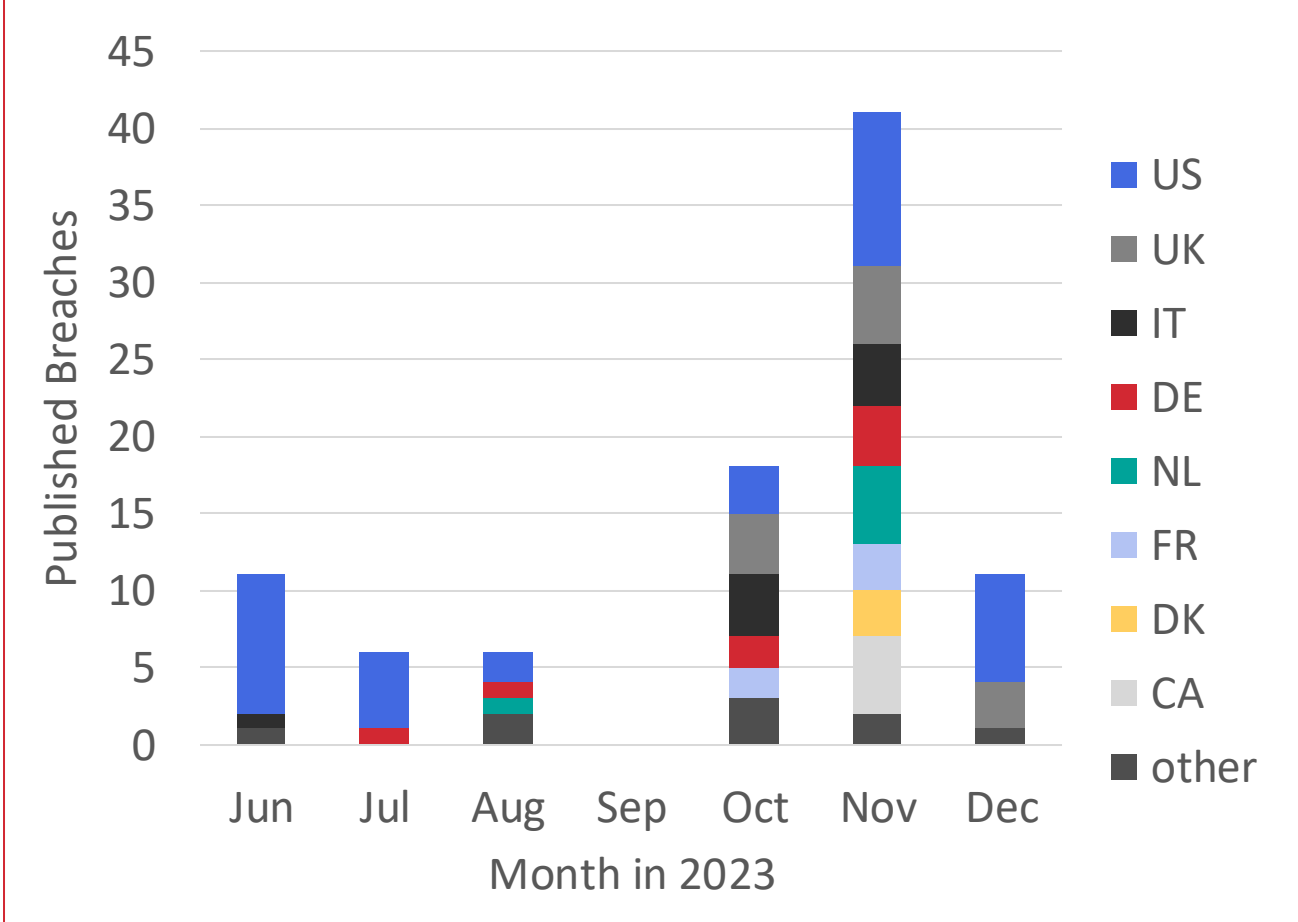
| Patch delay [days] | Vendor | Missed Patches | | Samples* |
|--------------------|----------|----------------|----------|----------|
| | | 2018 | 2019 | |
| Immediately | Google | 0 to 0.2 | 0 to 0.2 | many |
| | Sony | 0.2 to 1 | 0.2 to 1 | lots |
| | Nokia | 0.2 to 1 | 0.2 to 1 | lots |
| Within 2 weeks | Huawei | 0.2 to 1 | 0.2 to 1 | lots |
| | LGE | 0 to 0.2 | 0 to 0.2 | lots |
| | Samsung | 0 to 0.2 | 0 to 0.2 | lots |
| Within 1 month | Motorola | 0 to 0.2 | 0.2 to 1 | lots |
| | BQ | 0.2 to 1 | 0.2 to 1 | many |
| | ZTE | 2 to 4 | 0 to 0.2 | lots |
| | Oppo | 4 or more | 1 to 2 | few |
| | Wiko | 2 to 4 | 0 to 0.2 | few |
| | Verizon | 0.2 to 1 | 0 to 0.2 | few |
| | Lenovo | 4 or more | 0 to 0.2 | few |
| | TCL | 2 to 4 | 0.2 to 1 | few |
| | Asus | 0.2 to 1 | 0.2 to 1 | many |
| | OnePlus | 0 to 0.2 | 0.2 to 1 | many |
| | Vivo | 1 to 2 | 0.2 to 1 | lots |
| | htc | 1 to 2 | 1 to 2 | many |
| Xiaomi | 0.2 to 1 | 0 to 0.2 | many | |

6 **Co-piloting evolution:**
Fighting the real enemy: Criminals

Black Basta is a major threat actor since 2022

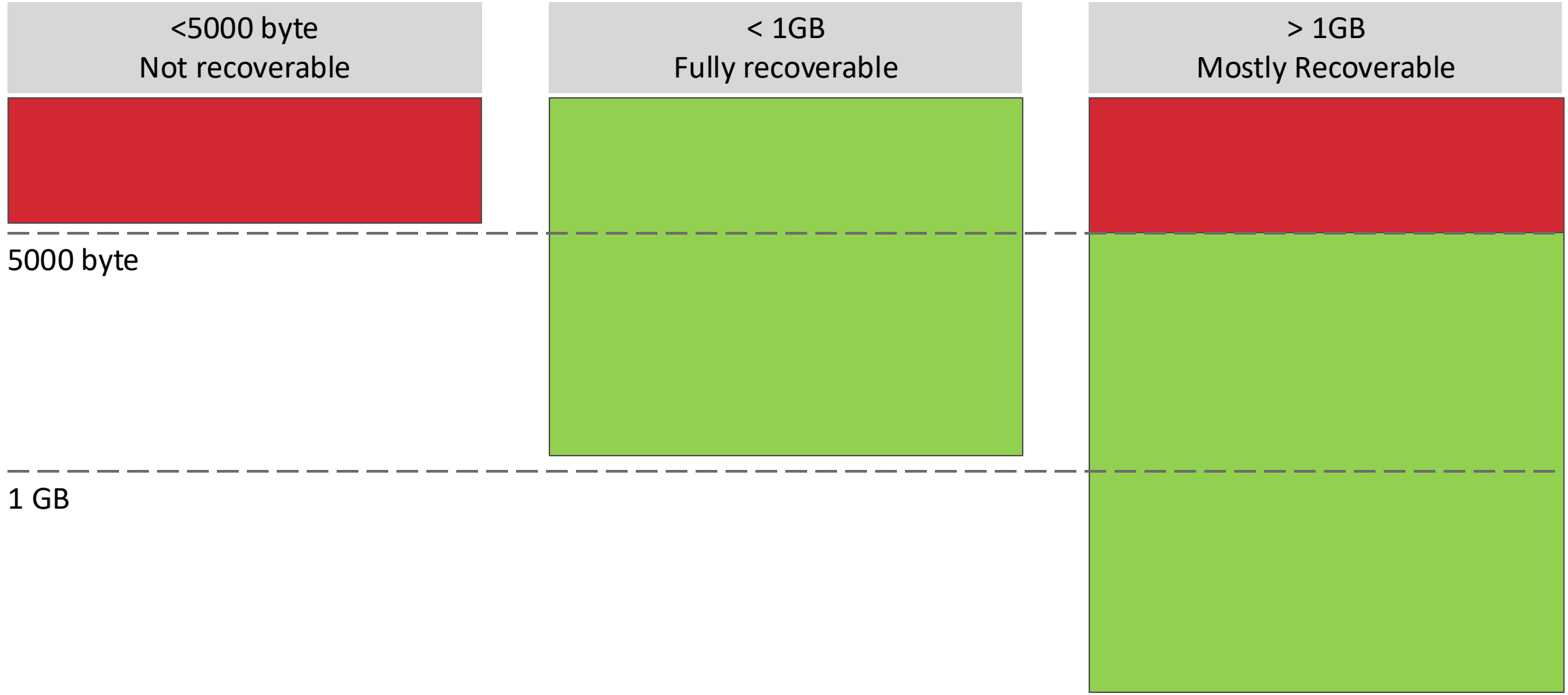
Black Basta ransomware gang

- Started in **2022-04** as Conti offspring
- Published about **320 breaches**, averaging 13 per month
- Extorted **USD 100+ Mio** from 90 victims
- Was the “**second most used ransomware** in Germany”
- Targets **ESXi** servers
- **Changed their encryption** to ECC in 2022-11



Many files encrypted by Black Basta are recoverable

Recoverable
Not recoverable



We can successfully decrypt and recover the original file

```
fish /tmp/decrypt
87% 32.68MB/s 6 seconds remaining, ETA: 2023-10-10T10:56
WARNING:decryptblocks:Looking at 4718592 905969472 (1073741824): 84.3
75% 33.28MB/s 4 seconds remaining, ETA: 2023-10-10T10:56
WARNING:decryptblocks:Looking at 4980736 956301120 (1073741824): 89.0
62% 32.01MB/s 3 seconds remaining, ETA: 2023-10-10T10:56
WARNING:decryptblocks:Looking at 5242880 1006632768 (1073741824): 93.
750% 40.31MB/s 1 seconds remaining, ETA: 2023-10-10T10:56
WARNING:decryptblocks:Looking at 5505024 1056964416 (1073741824): 98.
437% 50.06MB/s 0 seconds remaining, ETA: 2023-10-10T10:56
INFO:magic:Renaming file to remove magic suffix: /tmp/myfile.vmdk.sah
28vut5 /tmp/myfile.vmdk
Decrypted: /tmp/myfile.vmdk
✂ /t/decrypt xxd -a /tmp/myfile.vmdk 10:56:53
00000000: 0000 0000 0000 0000 0000 0000 0000 0000 0000 .....
*
3fffffff0: 0000 0000 0000 0000 0000 0000 0000 0000 0000 .....
✂ /t/decrypt 10:57:43
```

We automated the decryption, shared it with victims, and then with everyone

Recovering an encrypted file

- Knowing 64 plaintext bytes allow file **recovery**
- **If >1GB**, the first 5000 bytes are lost
- Fortunately, ESXi disk images have:
 - **zero-bytes**, and
 - **re-creatable** MBR or GPT structure (in multiple locations)

Automatic recovery of files

- We developed **scripts** to
 - detect encrypted zeros, and
 - **decrypt** the file
- Caveat: Malware can encrypt files multiple times, requiring **manual investigation**

Sharing insights

- We contacted **affected organisations** and shared the documentation
- We disseminated the tools through **law enforcement** and **CERTs**
- Released at **37C3** (2023-Dec)
- <https://github.com/srlabs/black-basta-buster>
- <https://nomoreransom.org>

The awesome team behind this release

Tobias Müller, Jakob Rieck, Florian Wilkens, Luca Glockow, Nick Farnham, Jannes Quer, Matthias Marx, Dominik Oepen

In summary: All three modes of engagements are needed for technology evolution

Companies
vs
Hacking



Companies
fear & respect
Hackers



Joining forces
against
Criminals

Independent
oversight



Keep
companies
engaged



Drive
technology
evolution

Questions?

Your journey continues.

How do I become ...

... an Ethical Hacker?

1. Find a hack that excites you
2. Try to re-create it
3. Play “boxes” on ‘Hack the Box’
4. Play CTFs
5. Get OSCP-certified
6. **Always stay curious**



... a Security Professional?

YouTube
Hacking Matters
@hackingmatters · 7.32K subscribers · 10 videos
Welcome to Hacking Matters, your ultimate ...more

Learn from practitioners.

- THE RIGHT WAY TO SLOW DOWN HACKERS a little bit (6:47)
- Vulnerability management: the worst understood (6:35)
- Network segregation done right - Hacking Matters (2.5K views · 2 weeks ago)
- Vulnerability management done right - Hacking Matters (6.6K views · 3 weeks ago)
- Your tool to prevent 80% of hackers from breaking in (9:51)
- 5 baseline security processes (12:38)
- Patching done right - Hacking Matters (4.4K views · 4 weeks ago)
- 5 baseline security processes - Hacking Matters (2.8K views · 1 month ago)

Stay in touch:



linkedin.com/in/karsten-nohl/

@ nohl@srlabs.de