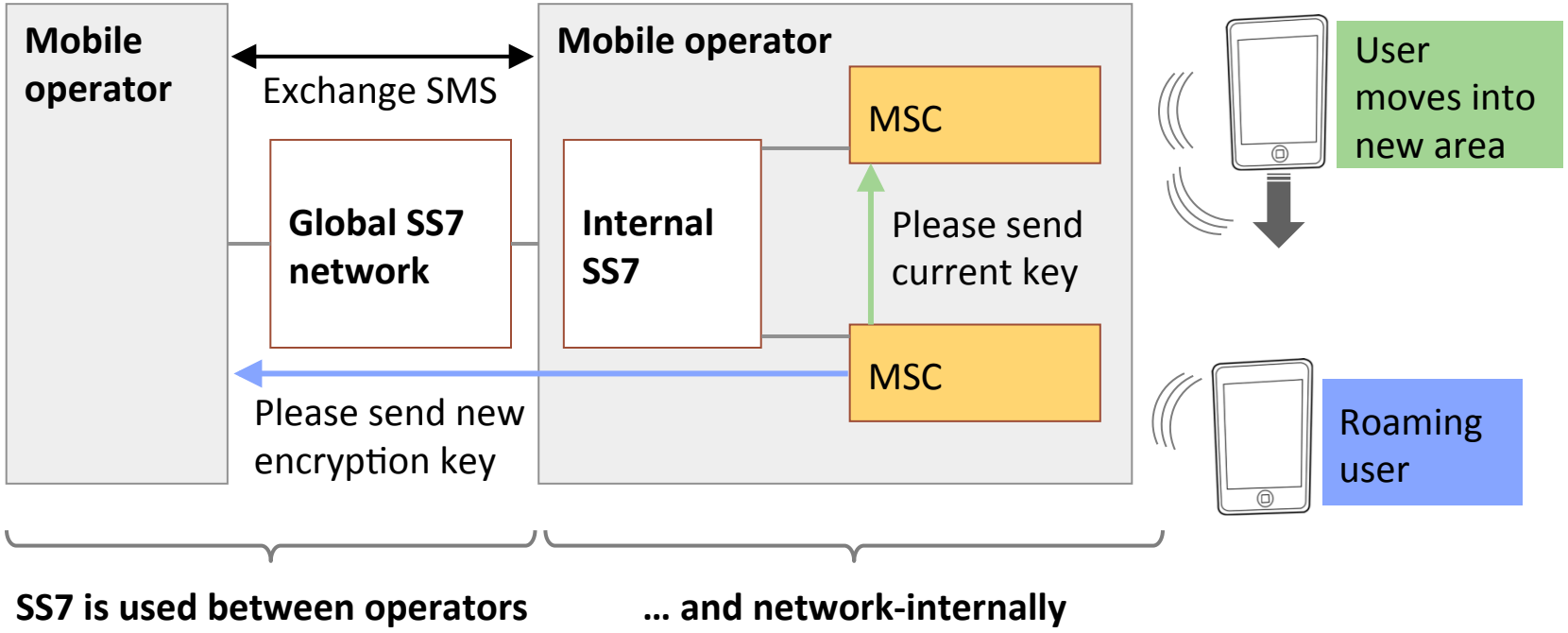
Mobile self-defense

Karsten Nohl <nohl@srlabs.de>

Agenda

- **SS7 attacks**
- 3G security
- Self-defense options

SS7 network enables exchange of SMS and cryptographic keys

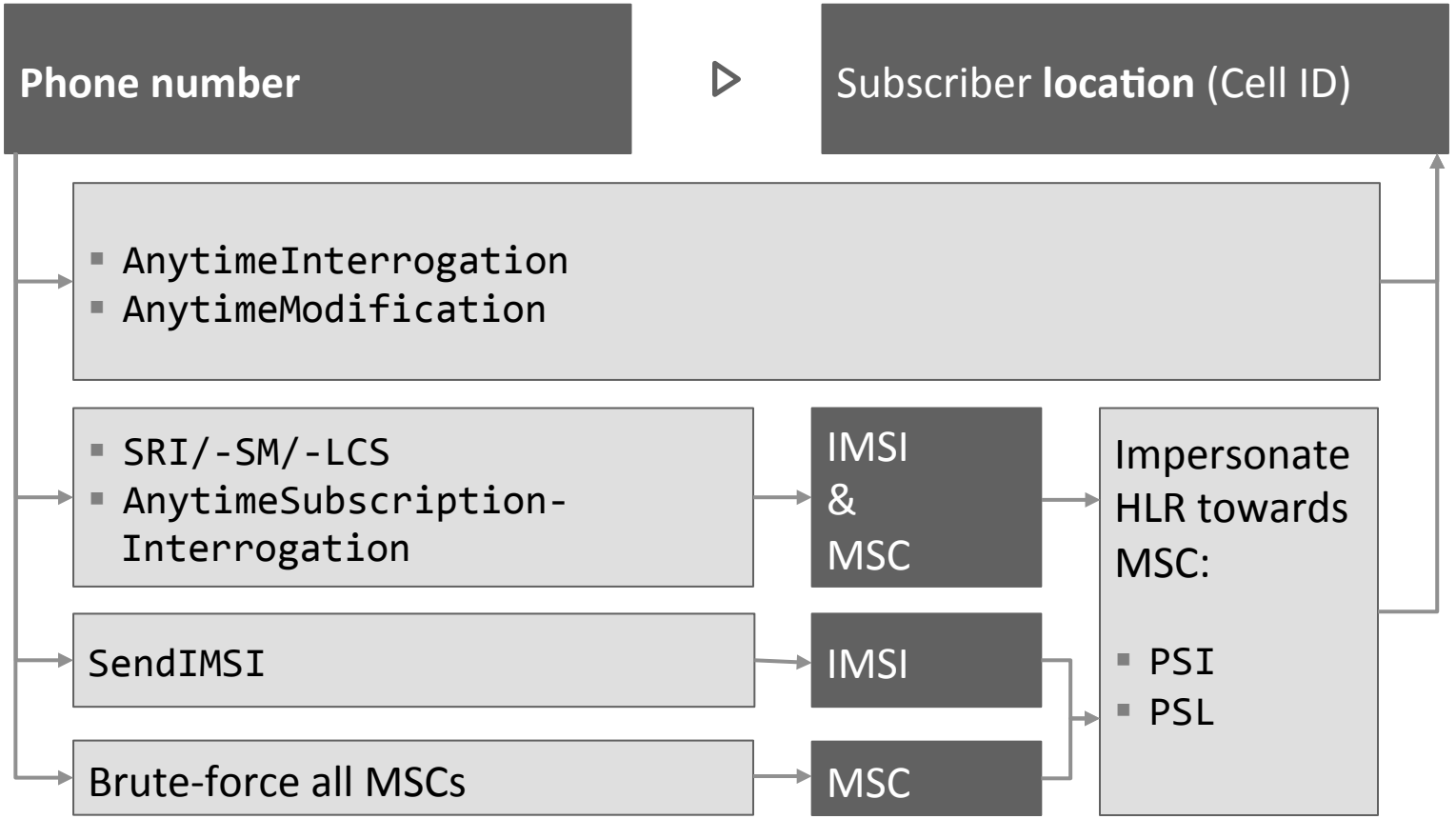


A **Tracking** over SS7 has become commonplace


The Washington Post

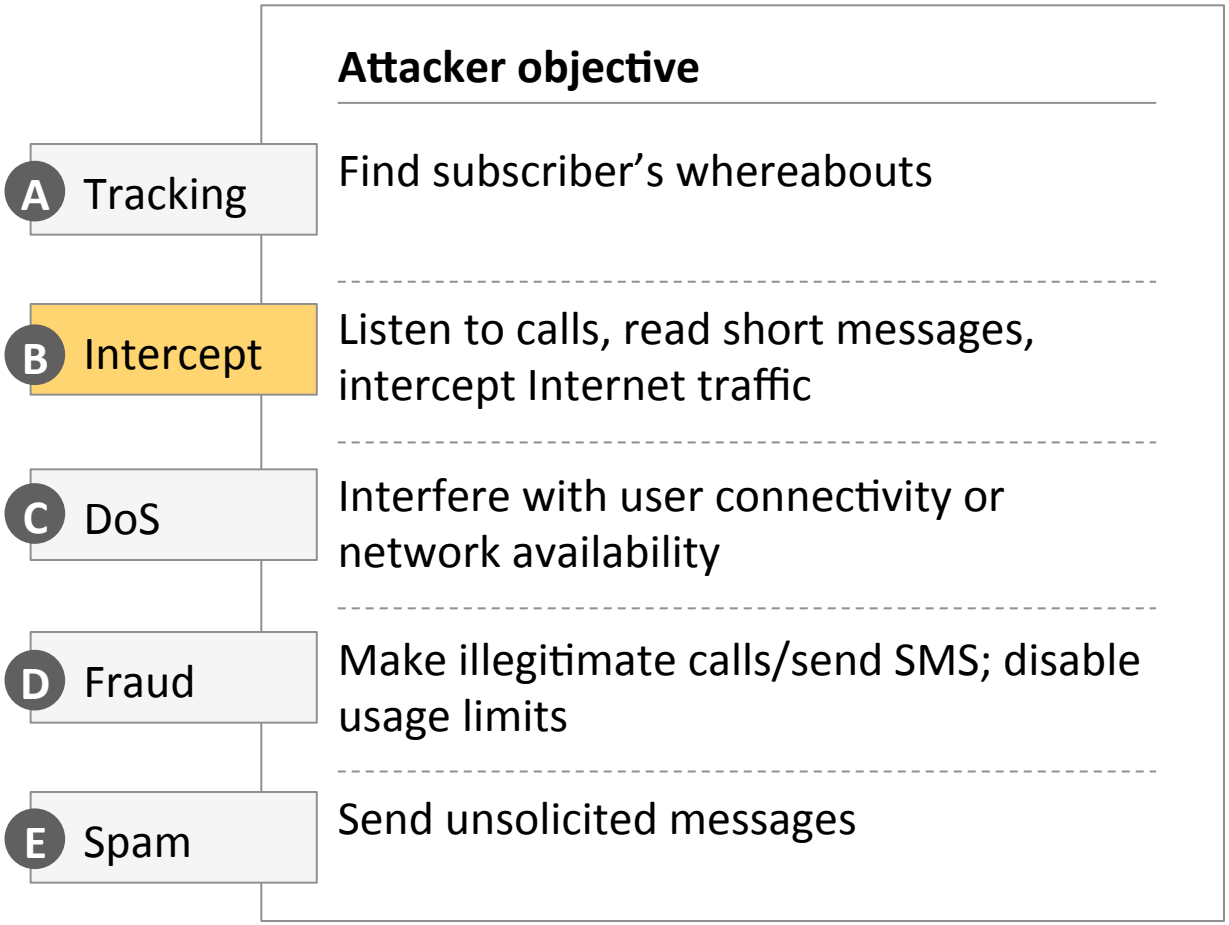
For sale: Systems that can secretly track where cellphone users go around the globe

A **Tracking** can happen using many more signaling messages

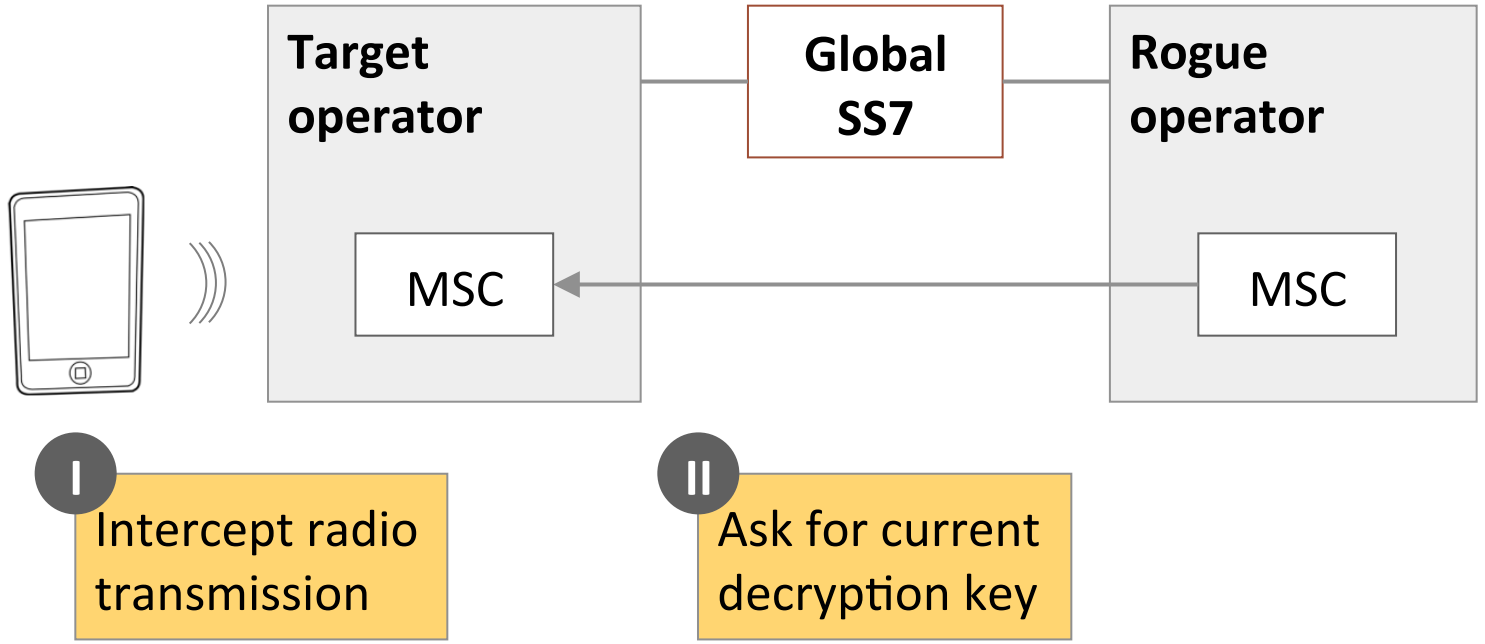


SS7 enables mobile abuse on five frontiers

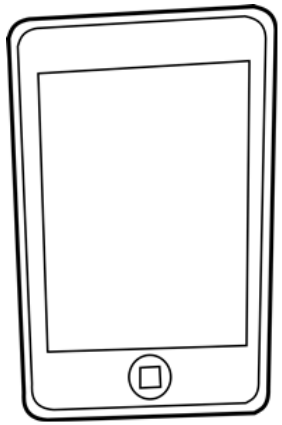
Focus of this presentation



1 2G + 3G transactions can be decrypted with help of SS7

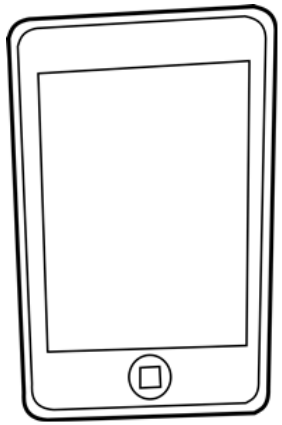


2 SS7 enables 3G IMSI Catcher



Here is my identity (IMSI), now prove that you are the real network

3G Fake Base Station ("IMSI catcher")



I. Prove your authenticity

III. Sends auth. proof

3G Fake Base Station

Global SS7

II. Request key

Mobile operator

3 Rerouting attacks over SS7 allow for remote intercept

SS7 Man-in-the-middle attacks

Capture incoming calls

Demo

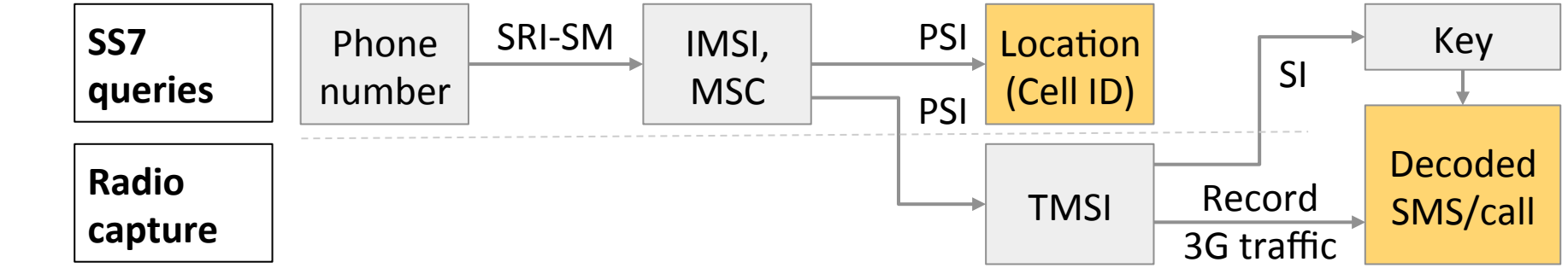
- Attacker activates call forwarding over SS7 for target number
- When a call is received, the attacker forwards it back to the original number

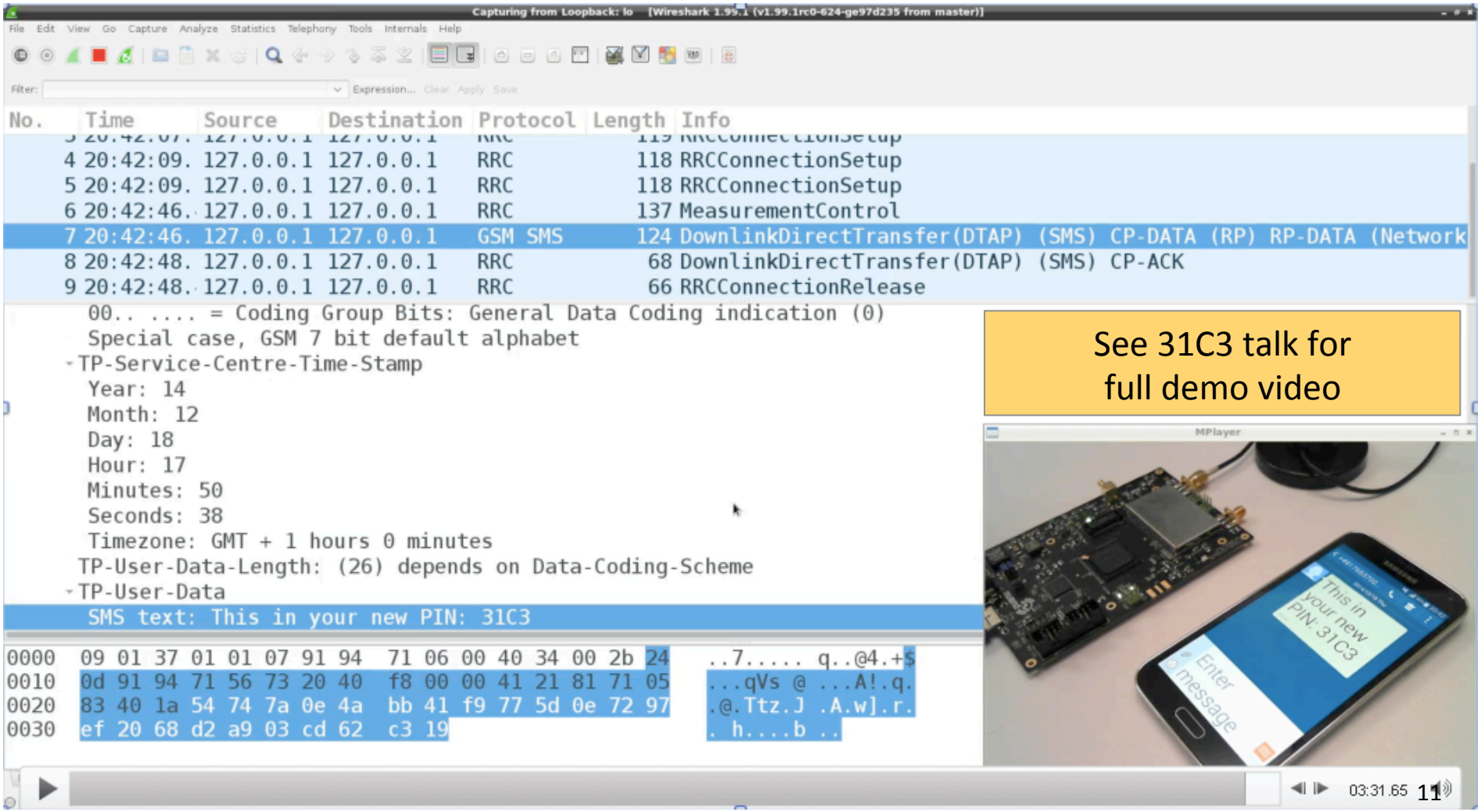
Capture outgoing calls

- Attacker adds a number rewriting rule for dialed numbers
- Called numbers are rewritten to reach attacker and are then forwarded to intended recipient

B Not all SS7 attacks can simply be blocked

Abuse scenario	Offending SS7 message	Mitigation effort
1 **Local passive intercept**	▪ `SendIdentification`	▪ **Easy –** Block message at network boundary
2 **IMSI Catcher**	▪ `SendAuthenticationInfo`	▪ **More complex –** Messages are required for operations, need to be plausibility-checked
3 **Rerouting attacks**	▪ `SS_activate/register` ▪ `UpdateLocation` ▪ Camel messages ▪ (Probably others)	


SS7 queries
Radio capture
Phone number
SRI-SM
IMSI, MSC
PSI
PSI
Location (Cell ID)
TMSI
SI
Key
Record 3G traffic
Decoded SMS/call


Capturing from Loopback: lo [Wireshark 1.99.1 (v1.99.1rc0-624-ge97d235 from master)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
No. Time Source Destination Protocol Length Info
4 20:42:09. 127.0.0.1 127.0.0.1 RRC 118 RRCConnectionSetup
5 20:42:09. 127.0.0.1 127.0.0.1 RRC 118 RRCConnectionSetup
6 20:42:46. 127.0.0.1 127.0.0.1 RRC 137 MeasurementControl
7 20:42:46. 127.0.0.1 127.0.0.1 GSM SMS 124 DownlinkDirectTransfer(DTAP) (SMS) CP-DATA (RP) RP-DATA (Network
8 20:42:48. 127.0.0.1 127.0.0.1 RRC 68 DownlinkDirectTransfer(DTAP) (SMS) CP-ACK
9 20:42:48. 127.0.0.1 127.0.0.1 RRC 66 RRCConnectionRelease
00.. .... = Coding Group Bits: General Data Coding indication (0)
Special case, GSM 7 bit default alphabet
TP-Service-Centre-Time-Stamp
Year: 14
Month: 12
Day: 18
Hour: 17
Minutes: 50
Seconds: 38
Timezone: GMT + 1 hours 0 minutes
TP-User-Data-Length: (26) depends on Data-Coding-Scheme
TP-User-Data
SMS text: This in your new PIN: 31C3
0000 09 01 37 01 01 07 91 94 71 06 00 40 34 00 2b 24 ..7..... q..@4.+$
0010 0d 91 94 71 56 73 20 40 f8 00 00 41 21 81 71 05 ...qVs @ ...A!.q.
0020 83 40 1a 54 74 7a 0e 4a bb 41 f9 77 5d 0e 72 97 .@.Ttz.J .A.w].r.
0030 ef 20 68 d2 a9 03 cd 62 c3 19 . h....b ..
See 31C3 talk for full demo video
MPlayer
This in your new PIN: 31C3
Enter message
03:31.65

Agenda

- SS7 attacks
- **3G security**
- Self-defense options

Remember? Intercepting GSM A5/1 calls and SMS is cheap

Intercept GSM call

- A reprogrammed EUR 20 phone captures 2G calls and SMS
- Multiple such phones could be clustered for wide-scale intercept

+

Crack A5/1 key

Standard server cracks key in seconds

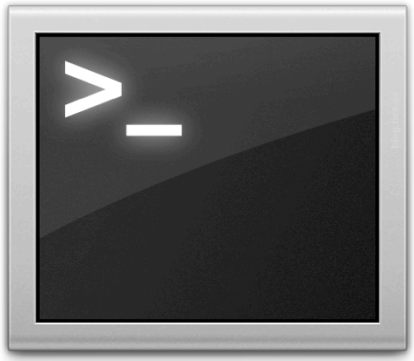
Intercepting 3G is also surprisingly cheap, thanks to SS7

Intercept 3G call

- Software-defined radio captures 3G transactions
- We use: **BladeRF** – USD 420
- Development took 3 months

+

Request decryption key

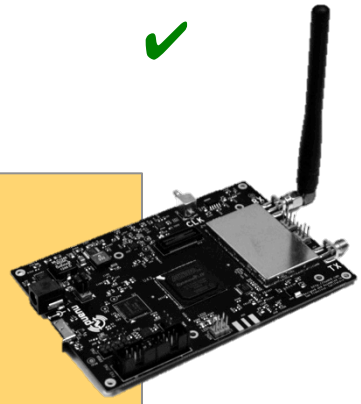


- SS7 query `SendIdentification` provides decryption key
- Also works for GSM A5/3

Some networks are so poorly configured that SS7 is not even needed to intercept their 3G transactions

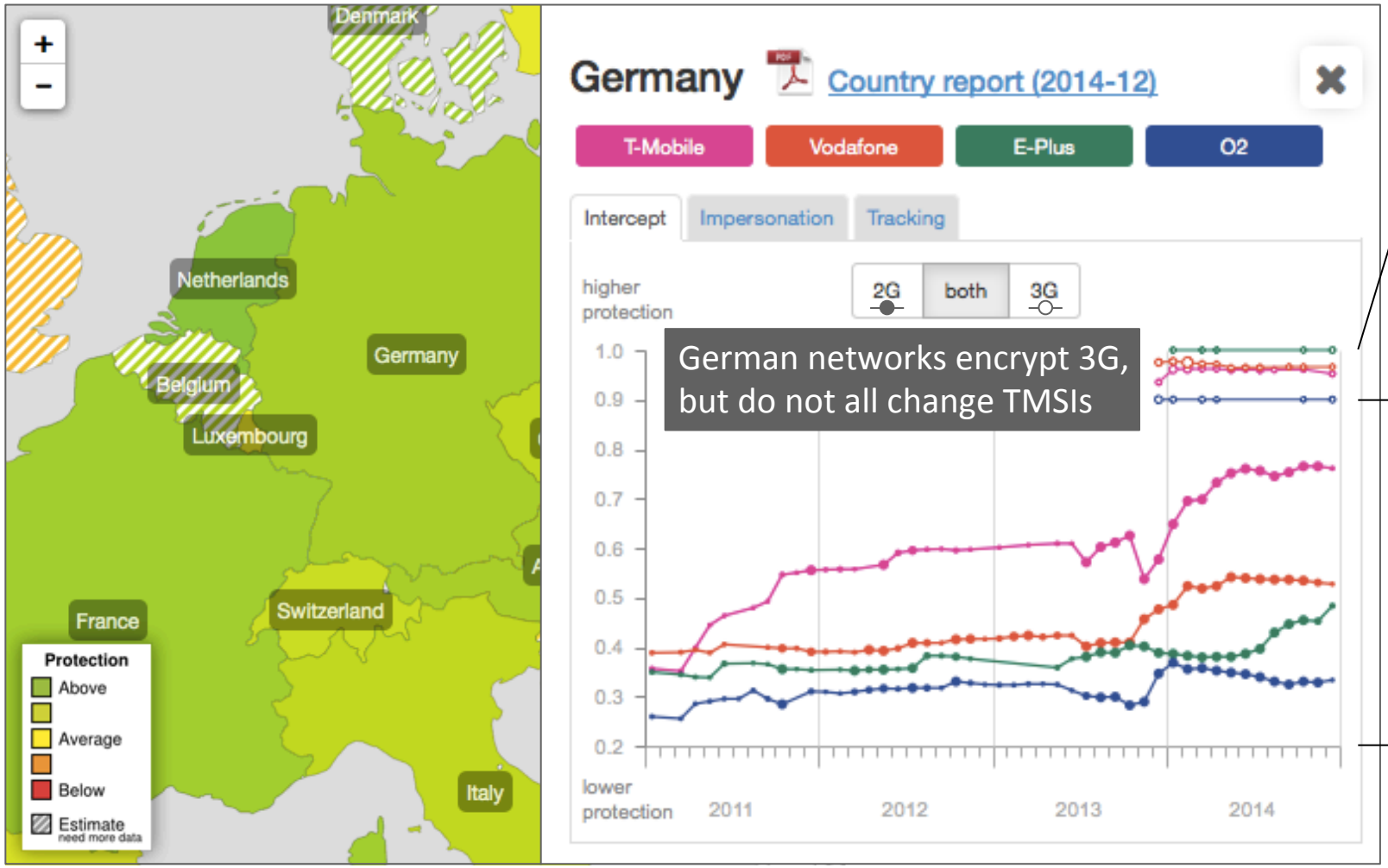
Network	Encrypts	Authenticates calls / SMS	Protects integrity
	✗	✗	✔
	✗	✗	✔
	✗	✗	✔
	✗	✗	✔
	✗	✗	✔

Risk – Calls, SMS, and Internet traffic on these networks can be intercepted passively with a programmable radio (but without SS7)



Protection status of 3G networks is tracked in online tool

gsmmap.org network security comparison



Initial 3G metric:

TMSI update [10%]

+

3G encryp-tion [90%]

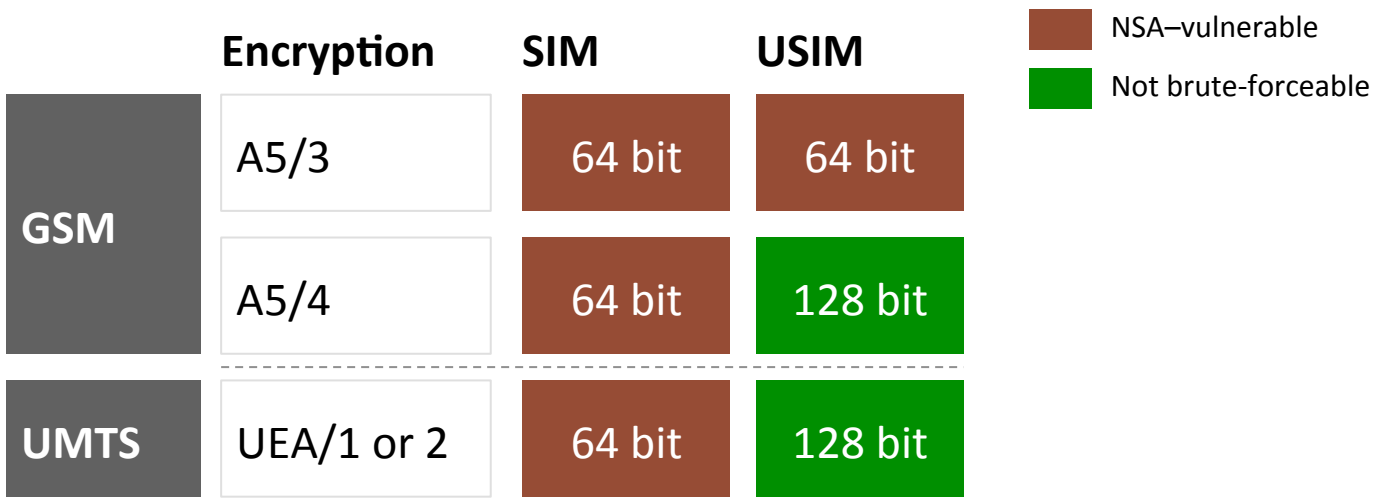
Networks without USIMs are vulnerable to brute-force attacks

NSA apparently broke 64-bit A5/3

DISCOVER ID 5100181 ANNEX A

Programme Outcomes	Target Capability deliveries for 2011/12
Respond to the roll out of the next Mobile OTA encryption standard for GSM (A5/3) by developing an attack with NSA, and for which there is significant SIA interest.	WOLFRAMITE R&D and definition.
Provide capability against Mobile encryption	• WOLFRAMITE – Definition and prototyping of GSM A5/3 decryption (funding decision to be made (of the order of £4m) probably in 2Q of 11/12)

Encryption keys are often too short to resist NSA



Source – *The intercept*: wolframite-encryption-attack.pdf

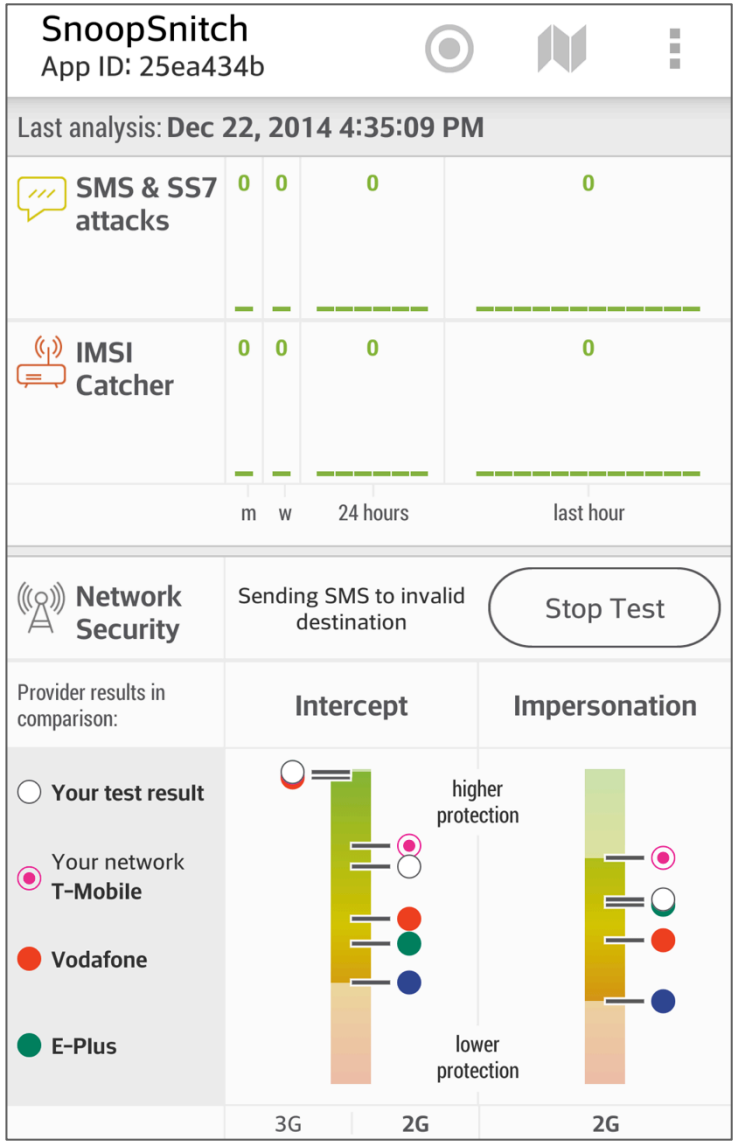
Agenda

- SS7 attacks
- 3G security
- **Self-defense options**

Many mobile network abuse scenarios can be detected

	Attack scenario	Detection heuristic
 **SMS Attacks**	▪ **SIM OTA attacks**	▪ Unsolicited binary SMS
	▪ Semi-lawful **Tracking** through silent SMS	▪ Silent SMS
SS7 Attacks	▪ SS7 abuse: **Tracking, Intercept**, etc.	▪ Empty paging
 **IMSI Catcher**	▪ **Tracking** or **Intercept** through 2G or 3G fake base station	▪ Unusual cell configuration and cell behavior (detailed later in this chapter)
 **Network Security**	▪ Insufficient encryption leads to **Intercept** and **Impersonation**	▪ Encryption level and key change frequency
	▪ Lack of TMSI updates enables **Tracking**	▪ TMSI update frequency

New tool detects common abuse scenarios



Tool name	**SnoopSnitch**
Purpose	▪ Collect network traces on Android phone and analyze for abuse ▪ Optionally, upload to GSMmap for further analysis
Require-ments	▪ Android 4.1 or newer ▪ Rooted, (but no CyanogenMod) ▪ Qualcomm chipset: Samsung S5/ S4/S3 Neo, Sony Z1, LG G2, Moto E, and many more
Source	Google Play: Search for *SnoopSnitch*

IMSI catcher detection analyzes a cell's configuration and behavior

SnoopSnitch combines a number of IMSI Catcher heuristics

Suspicious cell **configuration**

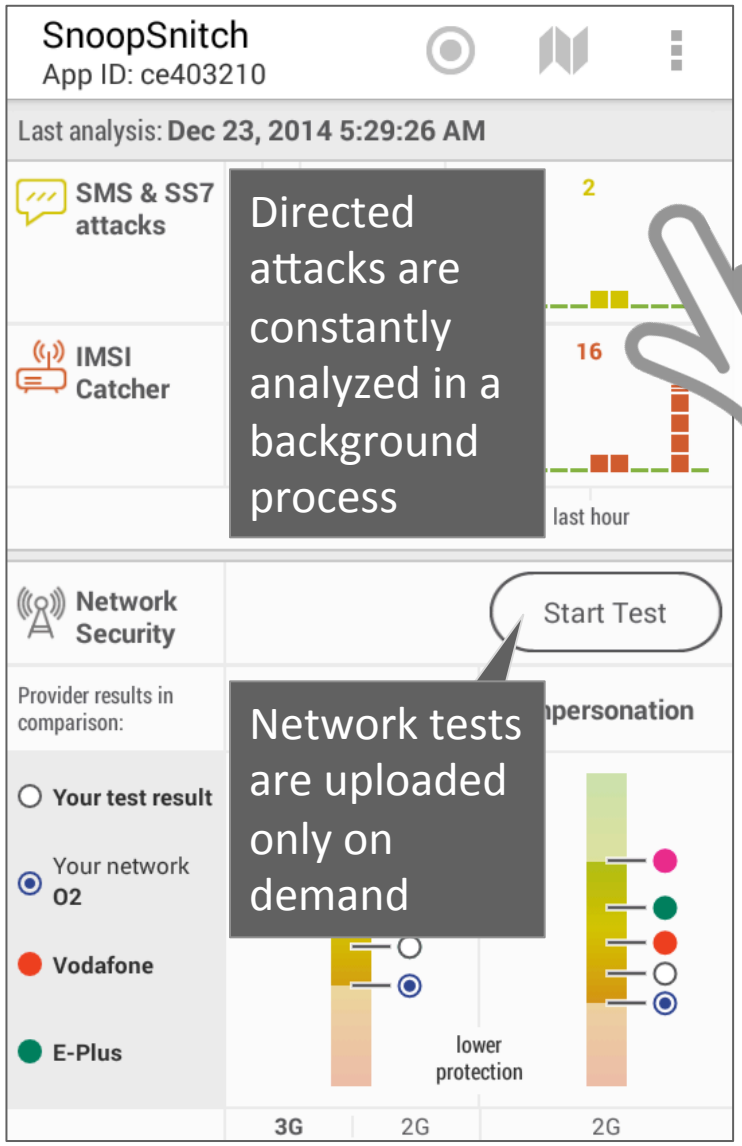
- Encryption downgrade / no encryption
- High cell reselect offset
- Large number of paging groups
- Low registration timer

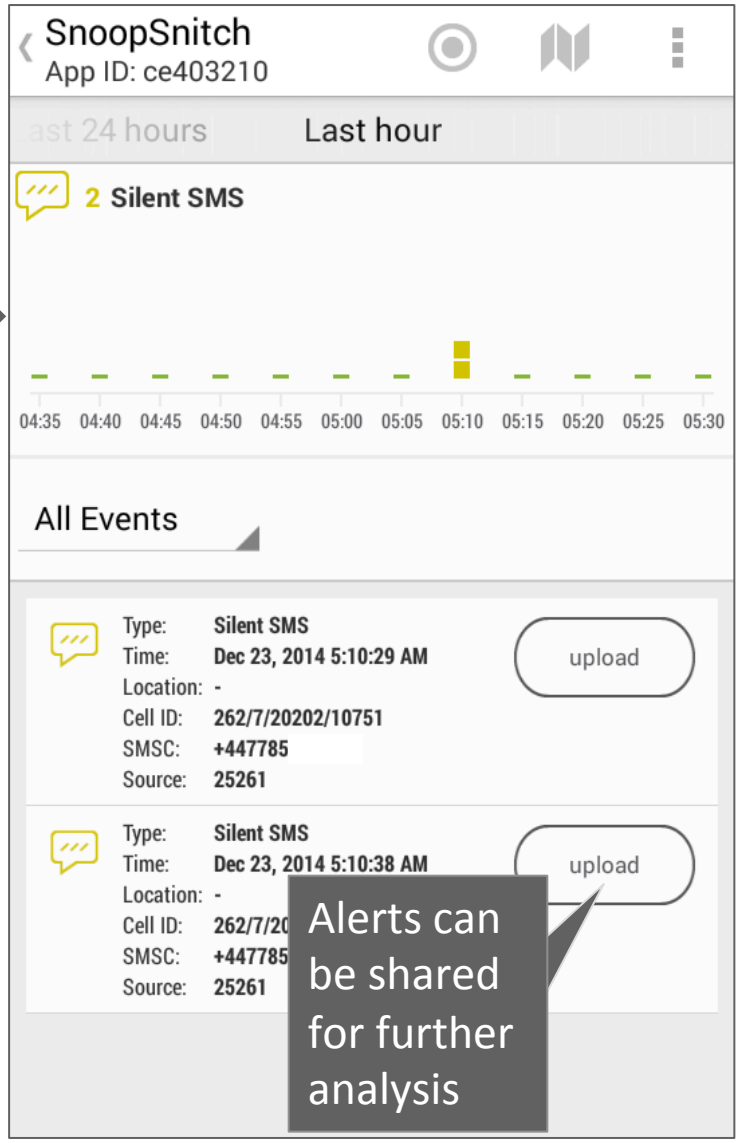
Suspicious cell **behavior**

- Delayed *Cipher Mode Complete* acknowledgement
- *Cipher Mode Complete* message without IMEISV
- ID requests during location update
- Paging without transaction
- Orphaned traffic channel

A number of other rules could not be implemented based on data available from Qualcomm chipsets. (Future work?)

SnoopSnitch collects data in the background and on request

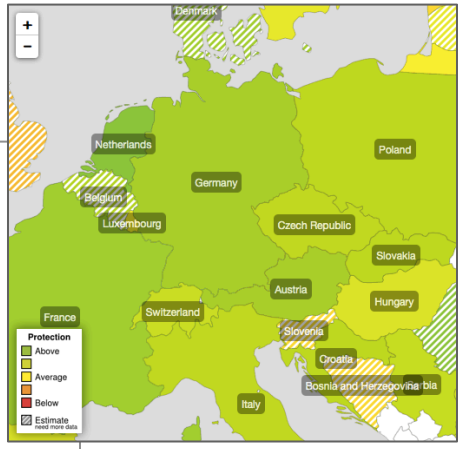


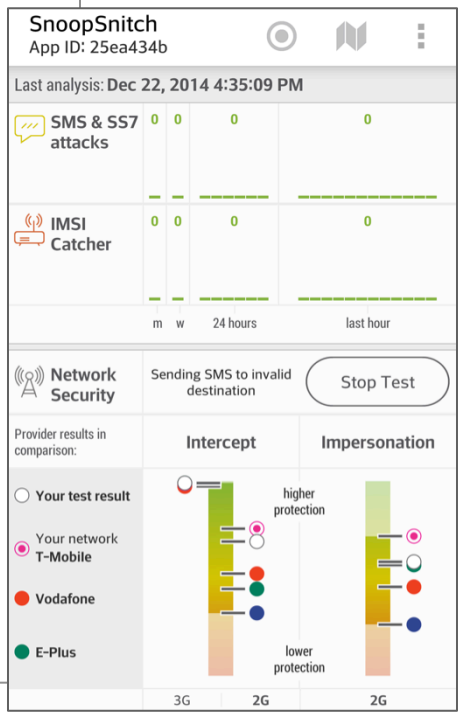


It’s now on you to contribute data and progress the toolbox of self-defense apps

Mobile self-defense strategy

1. Check your network operator on **gsmmap.org** for vulnerabilities; possibly switch to a more secure operator
2. Install **SnoopSnitch** from Google Play (needs Android 4.1+, Qualcomm chipset, root, but no custom ROM)
3. Conduct a network test and **upload any attack alarms** (SMS, SS7, IMSI catcher) for further analysis
4. Contribute to the SnoopSnitch code or use the source to build your own application based on raw 2G/3G/4G data





Thank you!

Research supported by

OPEN TECHNOLOGY FUND

Many thanks to **Alex Senier, Luca Melette, Lukas Kuzmiak**, **Linus Neumann**, **Jakob Lell,** and **dexter** for making this release possible!

Questions?

Karsten Nohl <nohl@srlabs.de>