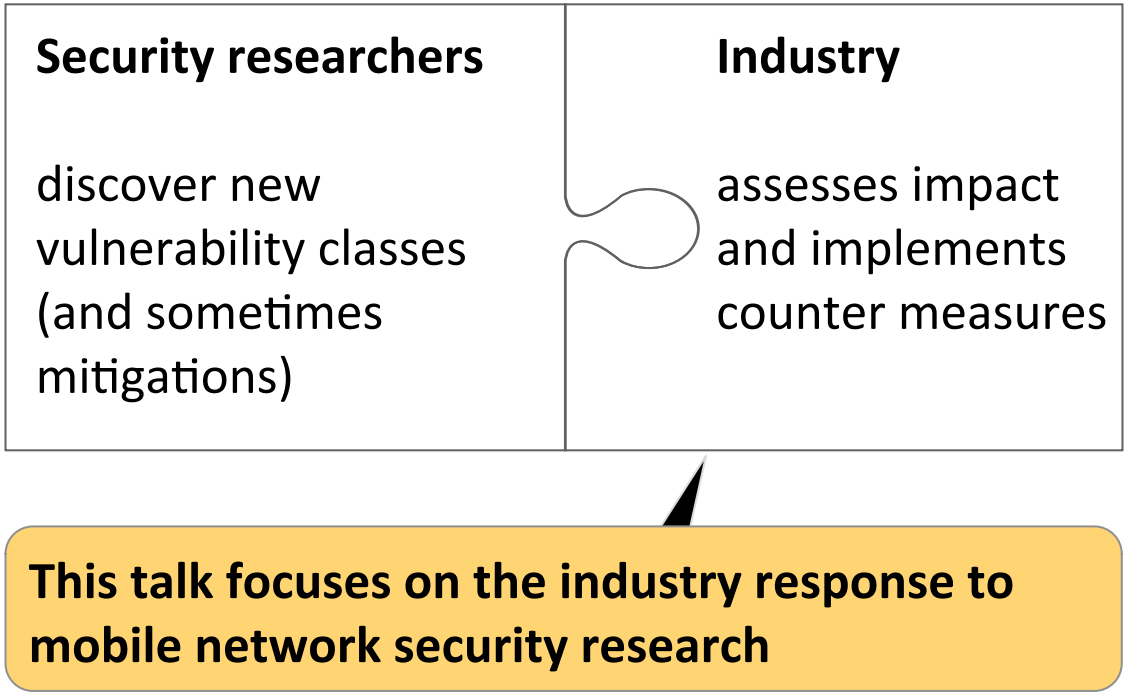
Mobile Network Attack Evolution

Karsten Nohl <nohl@srlabs.de>
Luca Melette <luca@srlabs.de>

SECURITY
RESEARCH
LABS

Security research is successful if vulnerabilities get removed



Agenda

- **Advanced SIM card attacks**
- Advanced GSM intercept
- Keeping network operators honest

SIM security research motivated some technology upgrades

Security researchers published several **SIM card attacks**

Industry reacted swiftly but **not thoroughly**

Finding	Response
1 Anybody can send management SMS to SIM cards	Many networks started filtering the most obvious attack messages
2 The OTA app mgmt interface is not always protected with good crypto	Some operators phased out DES keys in favor of 3DES
3 SIM applications can break out of their JavaCard sandbox	The vulnerability has not been addressed yet in affected cards

1 Binary SMS can take many forms to circumvent filters

		SMS field			
		PID	**DCS**	**UDHI**	**User data**
Best practice filters	**Several message types may go to the SIM**	127	*	*	*
		*	246 or 22	*	*
		*	*	1	027000…
	Some phones also forward other types	*	*	0	027000…
vs.					
Imple-mented filters	**Many networks only filter one type**	127	*	*	*

2 Misconfigurations in SIMs go well beyond DES keys

ILLUSTRATIVE

SIM configurations need to be assessed in two dimensions

2. Verify that all SIM applications enforce cryptography

1. Verify that all keys are 3DES or AES

		Application (TAR)			
Keyset		**000000**	**000001**	**…**	**FFFFFF**
1:	3DES	Sign + encrypt	Unprotected (MSL=0)		…
2:	3DES	Sign + encrypt	Sign		…
…					
16:	DES	Sign	Sign		…

Demo – Persistent infection of modern SIM card

Target —
New nano-SIM (October 2013) in iPhone 5s from major US carrier

Attack steps

- **A** Lure the phone onto fake base station to circumvent network filters
- **B** Scan the SIM remotely for configuration issues (on the SIM in this demo: discover TAR with MSL=0)
- **C** Install Java virus through vulnerable TAR
- **D** Let phone connect back to normal network, maintain persistent access through SMS-C&C

Tool release: SIM card configuration security assessment

Tool name	**SIMtester**
Purpose	▪ Find cryptographic attack surface: – Signature disclosure – 3DES downgrade ▪ Enumerate logical attack surface: Detect hidden application TARs and test their security level ▪ Upload traces to gsmmap.org for further analysis (Thank you.)
Requirements	PC/SC smartcard reader –or– Osmocom phone
Source	opensource.srlabs.de

Agenda

- Advanced SIM card attacks
- **Advanced GSM intercept**
- Keeping network operators honest

GSM intercept attacks are still under addressed

The majority of mobile phone calls worldwide still uses 2G GSM frequencies

To protect customers, mobile networks must support and harden two encryption standards

1

Older phones only support **A5/1 encryption**

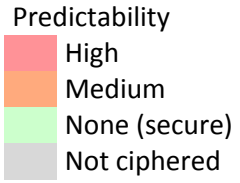
Protection status: Available strengthening measures are rarely seen

2

A5/3 protects much better

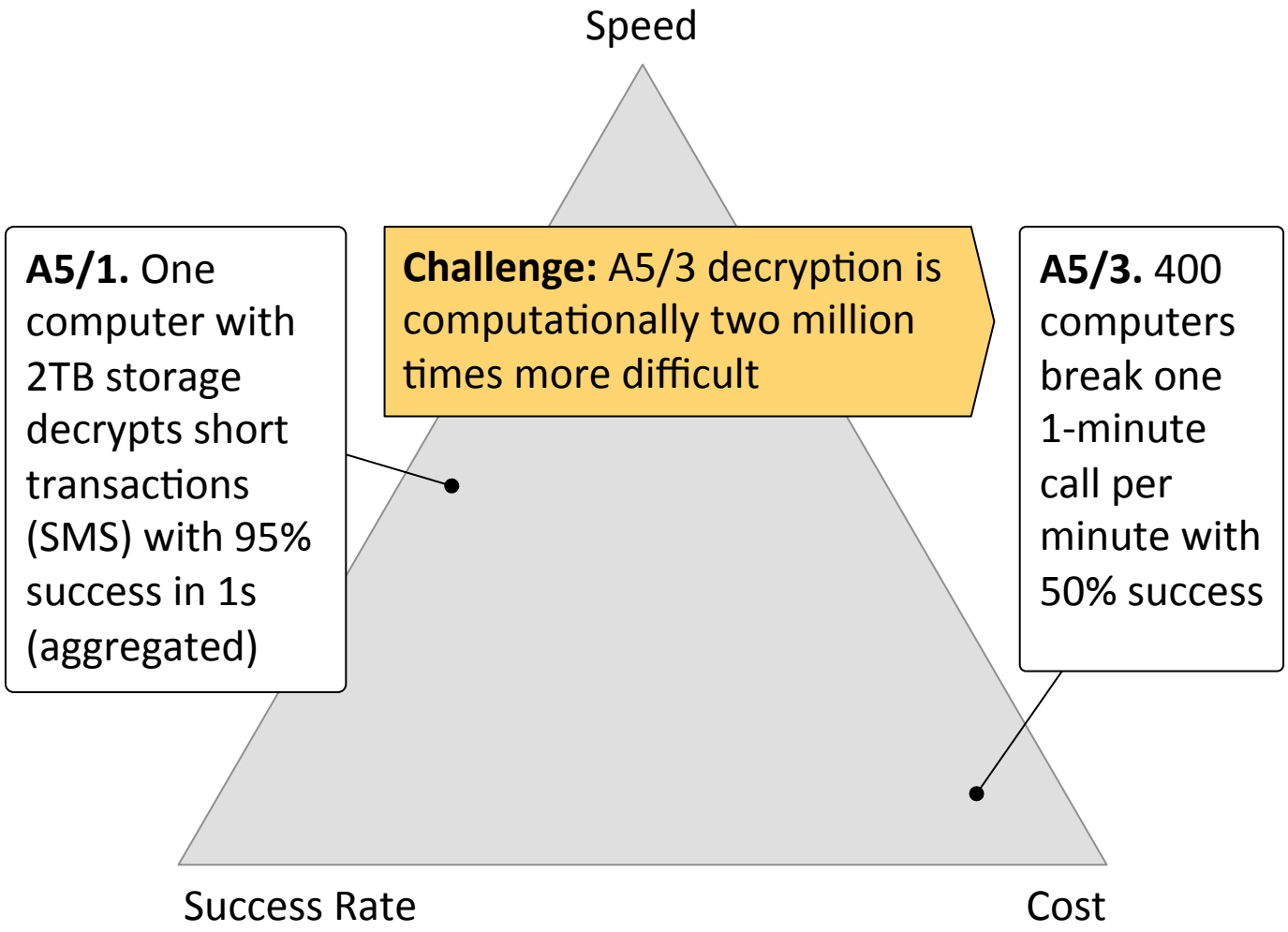
Protection status: Still only a minority of networks support A5/3

1 A5/1 decryption can mostly be prevented through randomization



		Features to decrease cryptographic attack surface	
Example call setup trace	**Unprotected**	**Padding randomization**	**+ SI5 randomization**
Ciphering Mode Cmd			
TMSI Reallocation Cmd			
Null Frame			
System Information 5			
Call Proceeding			
System Information 6			
Null Frame			
Fragment			
Assignment Command			
System Information 5ter			

2 A5/3 makes intercept much harder, but decryption is still possible for well-funded spy agencies



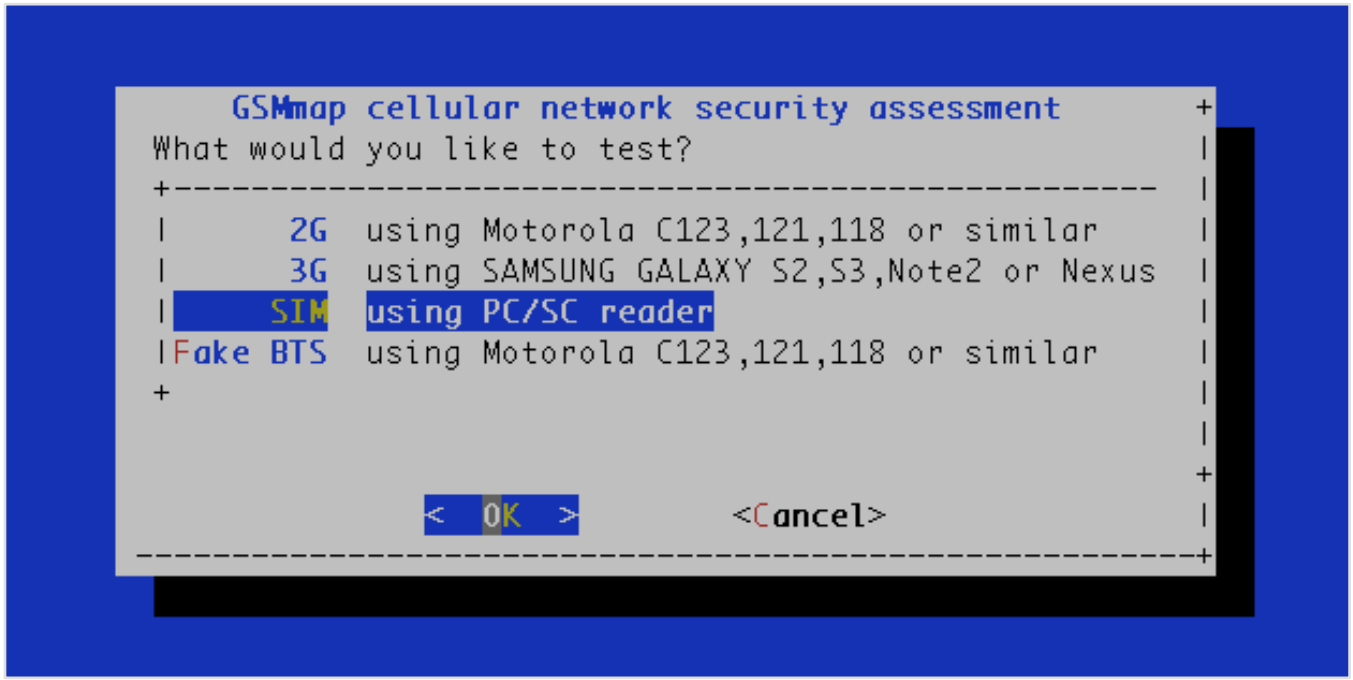
Tools release:
Measuring mobile network security from Android or Linux

Tool name	GSMmap.apk	xgoldscanner	OsmocomBB
Purpose	Collect network traces on Android phone and upload for analysis to gsmmap.org	Record network traces for analysis in Linux	Update to Sylvain's burst_ind setup to capture network traces for analysis in Linux
Requirements	Rooted Samsung Galaxy S2/S3	Samsung Galaxy S2, S3, Note 2, or Nexus	An older Motorola phone (C123, …)
Source	Google Play: GSMmap	opensource.srlabs.de	OsmocomBB git: *gsmmap* branch

Agenda

- Advanced SIM card attacks
- Advanced GSM intercept
- **Keeping network operators honest**

Live ISO puts mobile security tools on ready-to-use USB stick

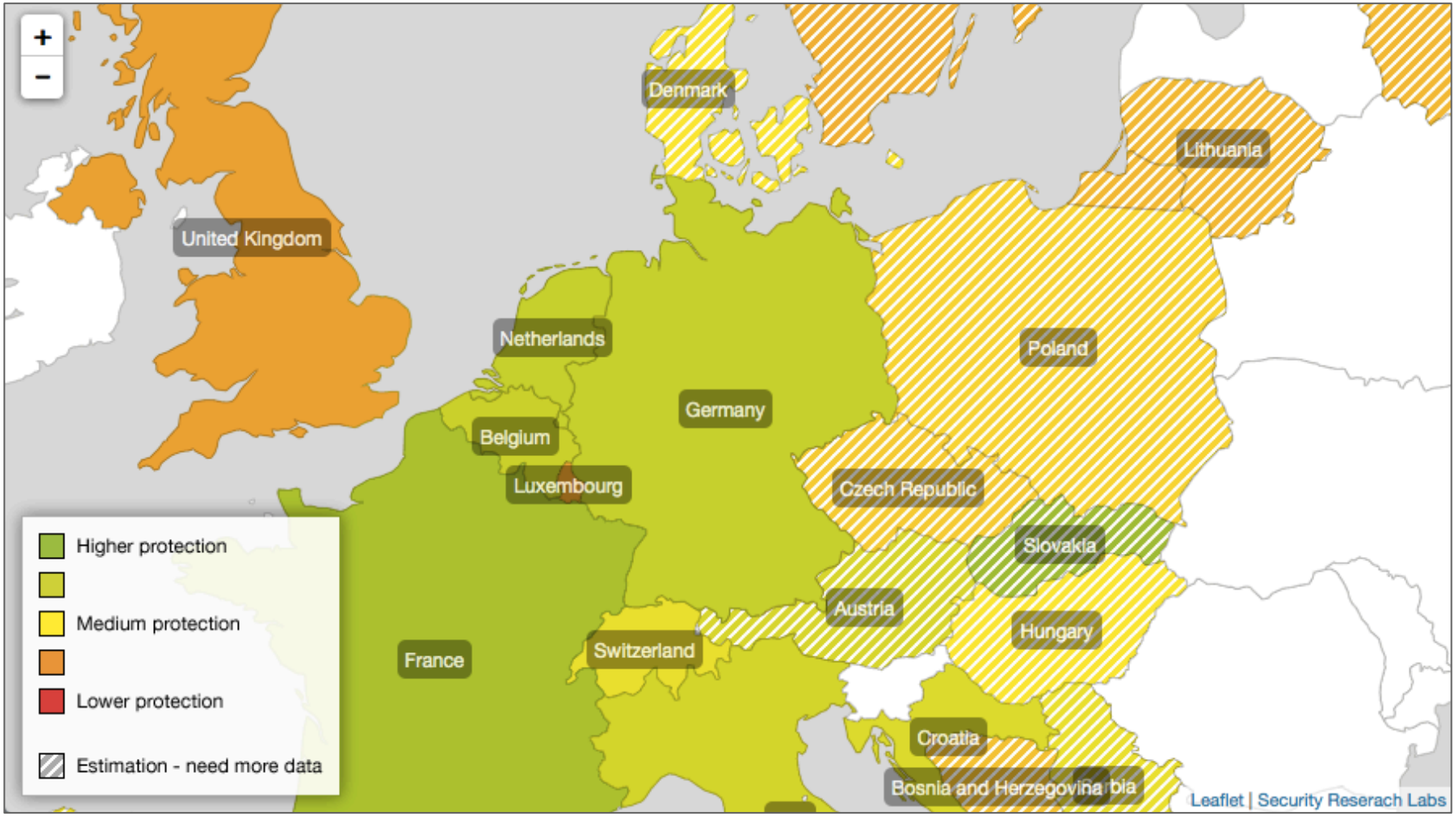


GSM map live ISO bundles mobile security tools

Network measurement with Galaxy S2/S3	Network measurement & IMSI catcher detection with Osmocom BB phone	SIM card assessment with PC/SC reader or Osmocom BB phone

Download and How-Tos	opensource.srlabs.de

gsmmap.org – Tracking mobile network evolution online



Thank you!

Research supported by

OPEN TECHNOLOGY FUND

Many thanks to **Lukas Kuzmiak** and **Linus Neumann** for creating and supporting the research tools released today!

Questions?

Karsten Nohl <nohl@srlabs.de>
Luca Melette <luca@srlabs.de>