Effective SS7 protection

ITU Workshop on “SS7 Security”, June 29th 2016

Luca Melette <luca@srlabs.de>

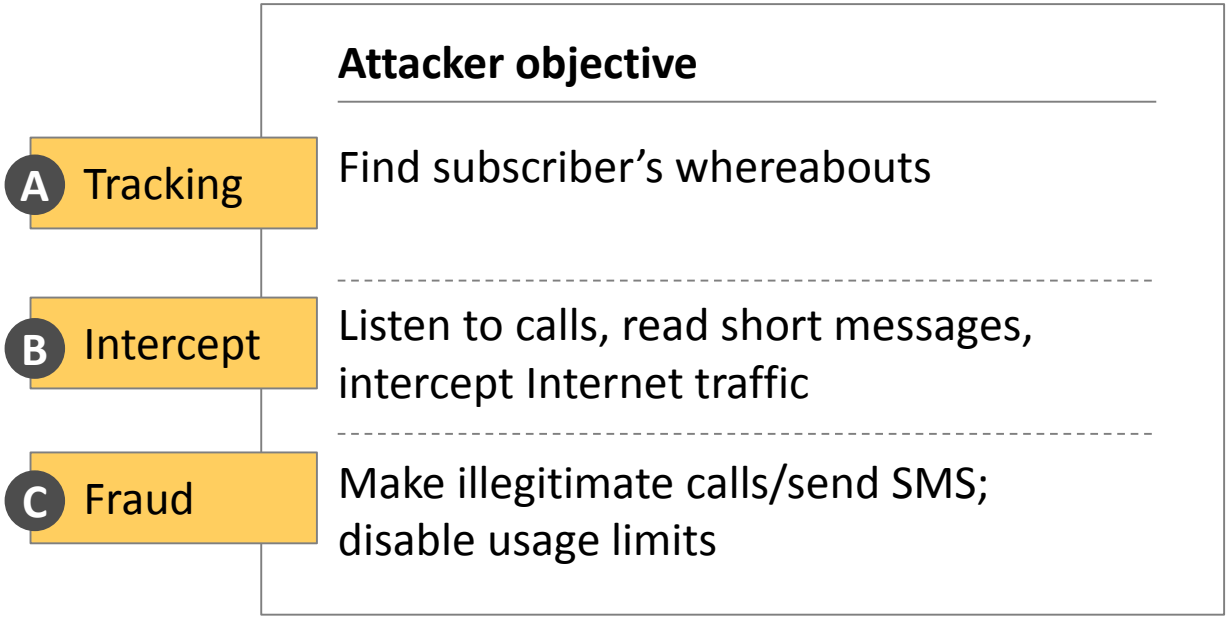
SECURITY
RESEARCH
LABS

Motivation: Operators and their users still vulnerable to SS7 attacks

Agenda

- **3 attack scenarios**
- 10 attack messages
- 4 defense measures

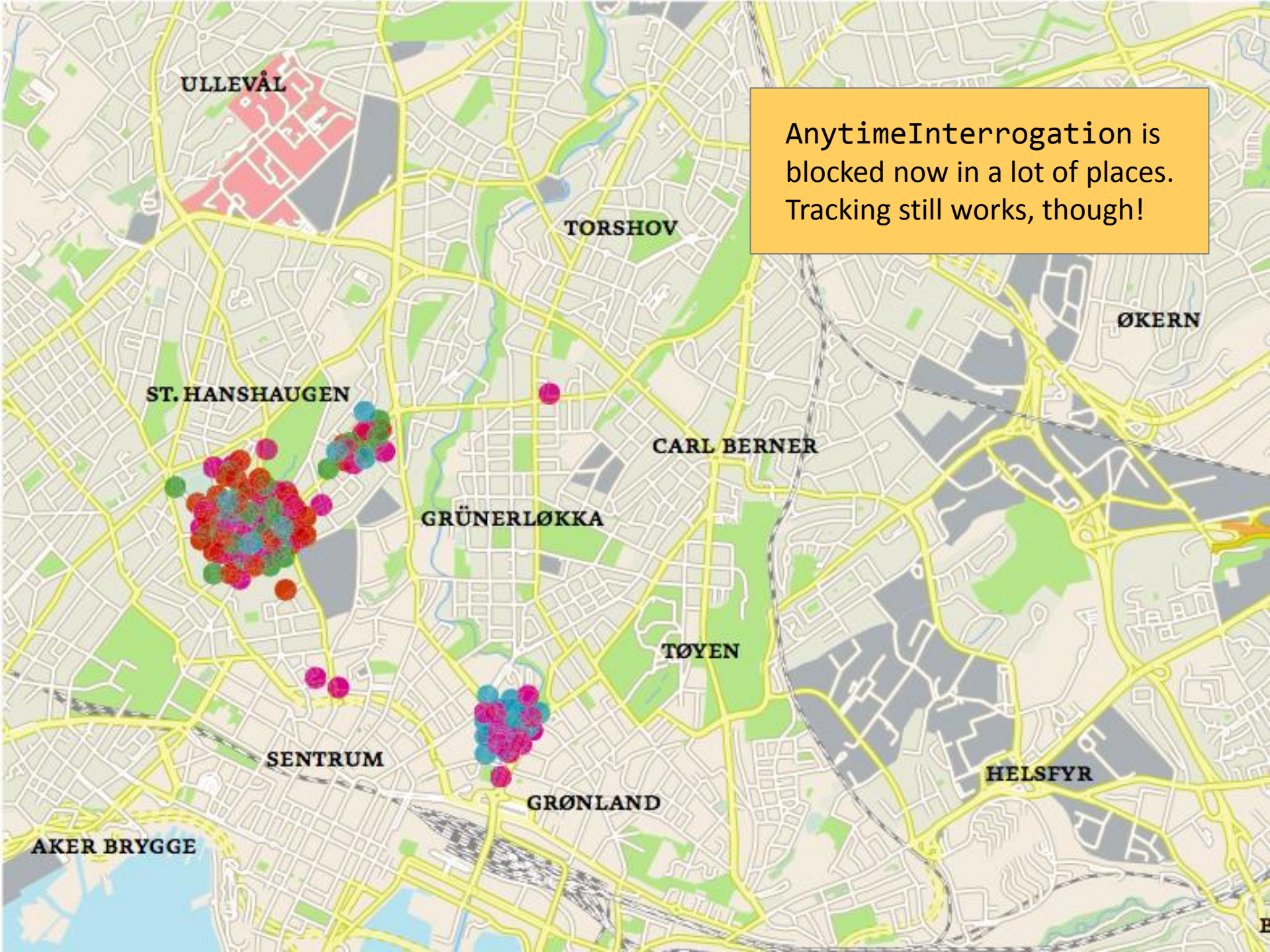
SS7 enables mobile abuse on different frontiers



A **Tracking** through ATI has become commonplace


The Washington Post

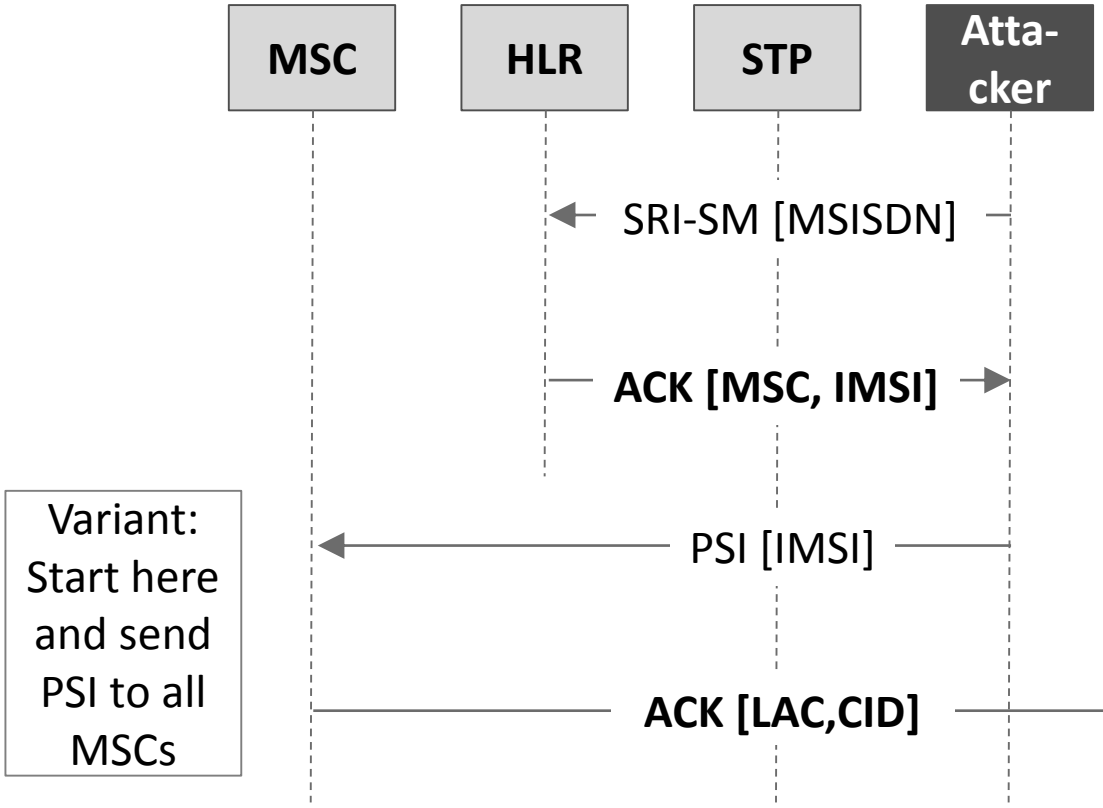
For sale: Systems that can secretly track where cellphone users go around the globe

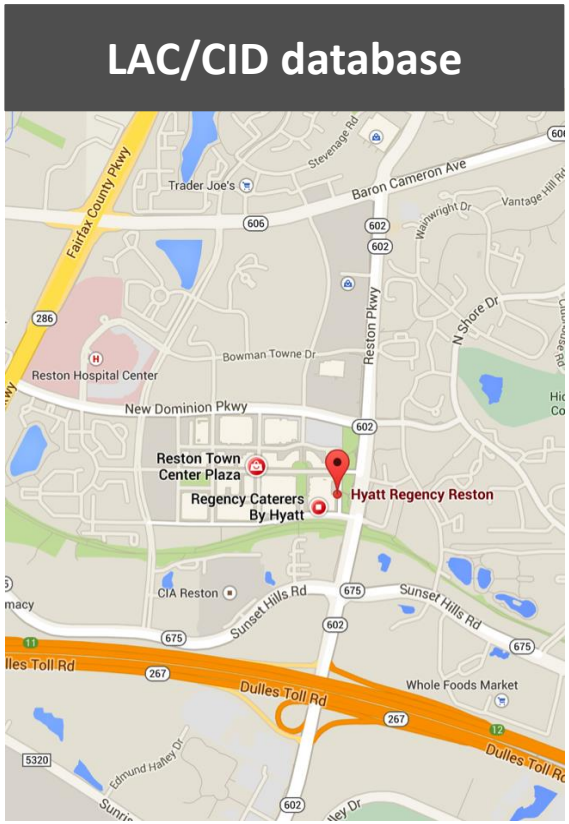

ULLEVÅL
TORSHOV
ØKERN
ST. HANSHAUGEN
CARL BERNER
GRÜNERLØKKA
TØYEN
SENTRUM
GRØNLAND
HELSFYR
AKER BRYGGE
AnytimeInterrogation is blocked now in a lot of places. Tracking still works, though!

A Accurate **tracking** is possible with standard messages

Shown in *60 Minutes*

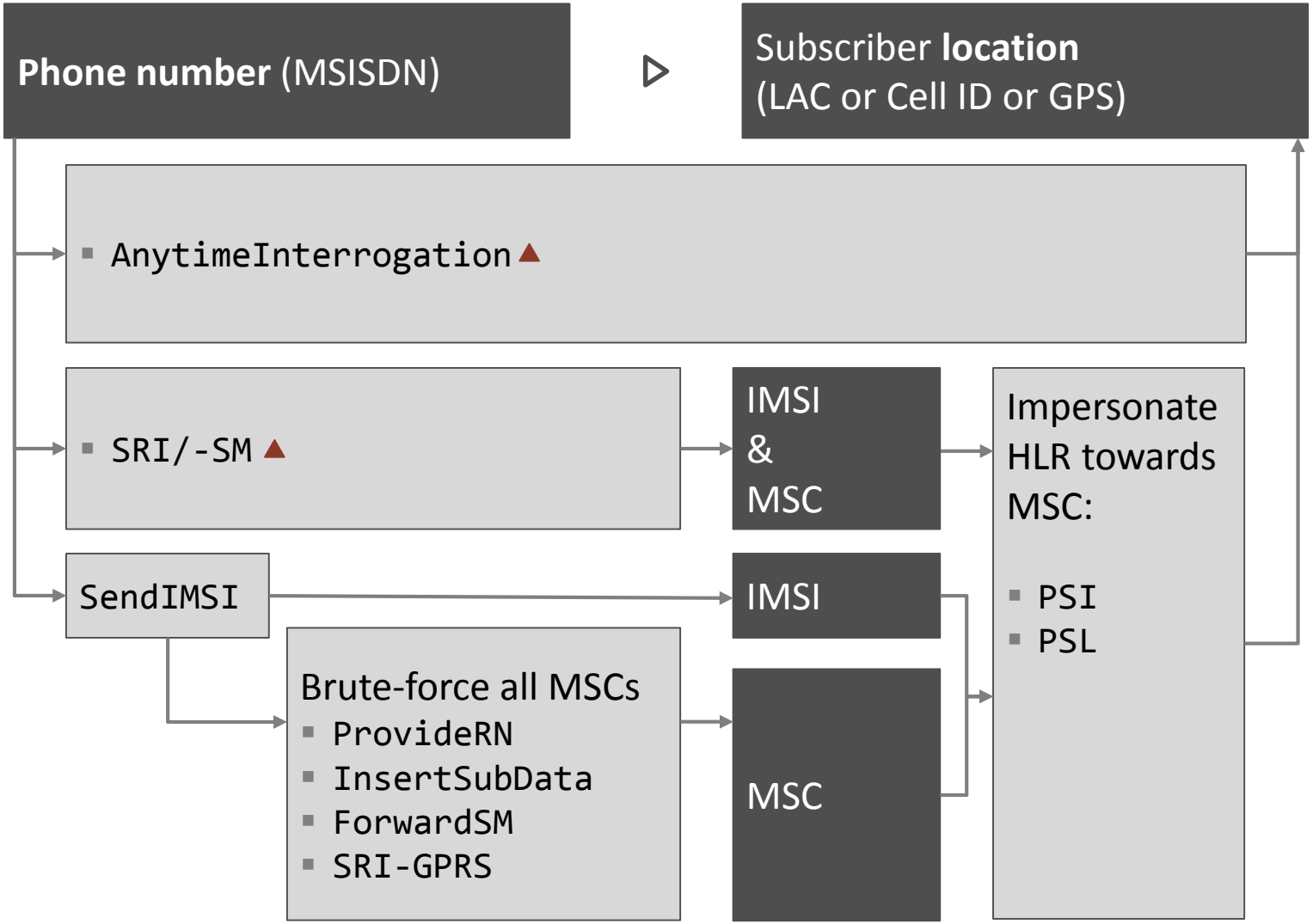
Attack – Probe MSC for subscriber location





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

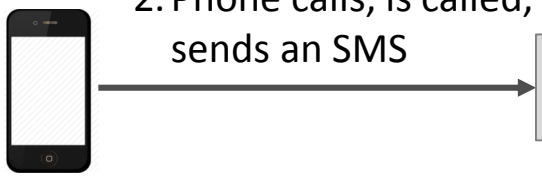
▲ Send to phone number or all HLRs or directly to MSC



B Remote **intercept** is possible through Camel

Shown in *60 Minutes*

Attack – Rewrite numbers over Camel



2. Phone calls, is called, or sends an SMS

MSC

1. `InsertSubscriber-Data(Camel server)` sets "triggering points"

3. Sends destination number to Camel server for verification

4. "Corrects" number

5. Connects call or sends SMS to attacker

Call out	✓
Call in	✓
SMS out	✓
SMS in	✗

Call intercept works for all Camel versions

SMS intercept requires Camel v3

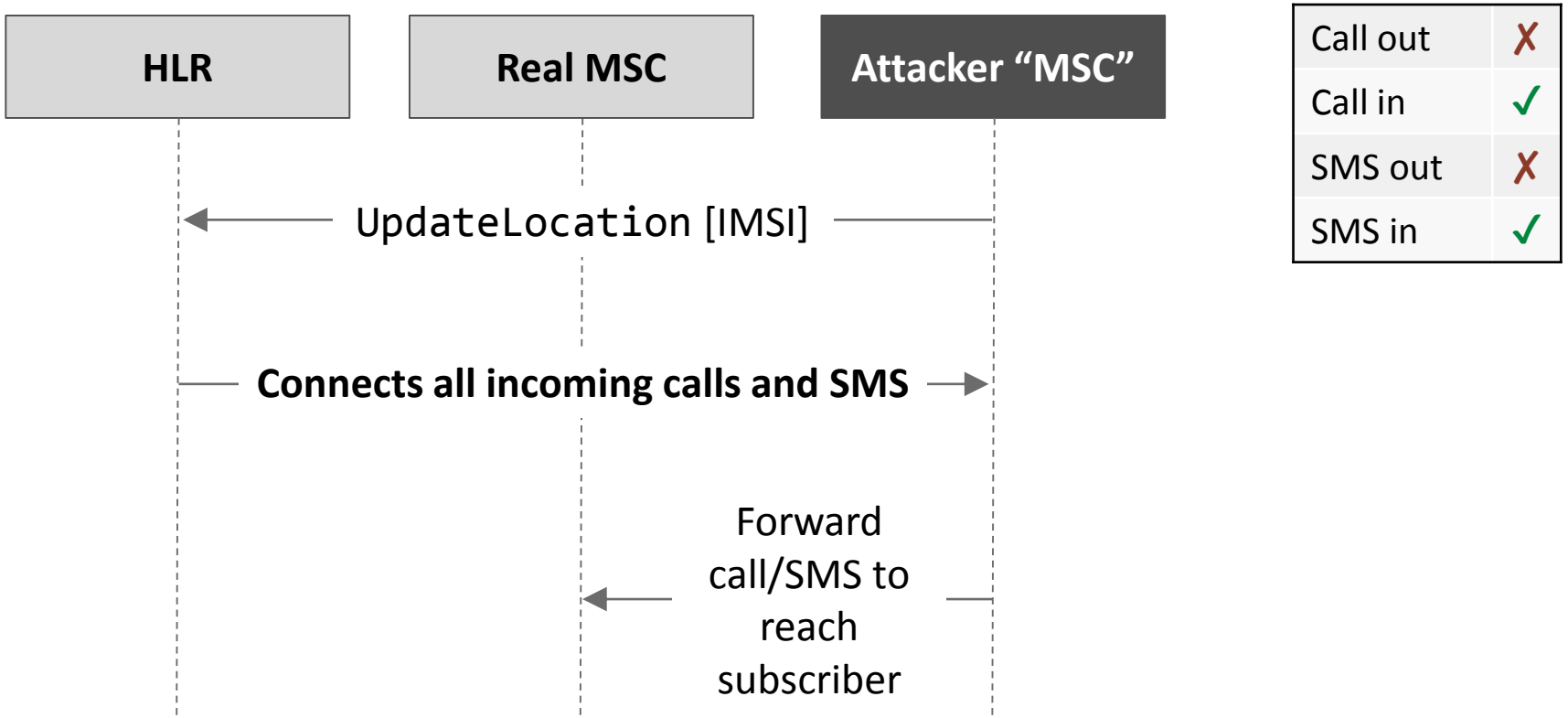
SS7 STP | **gsmSCF** | **MITM server**

Attacker

B Location update also achieves remote **intercept**

Shown in *60 Minutes*

Attack – Register as subscriber



C Selective **denial-of-service** is possible remotely

Signaling message	Send to	Effect
`CancelLocation`	MSC	For some phones: No service until reboot
`DeleteSubData`	MSC	Nothing works until next LU
`InsertSubData`	MSC	
`PurgeMS`	HLR	No Incoming SMS / Calls

Agenda

- 3 attack scenarios
- **10 attack messages**
- 4 defense measures

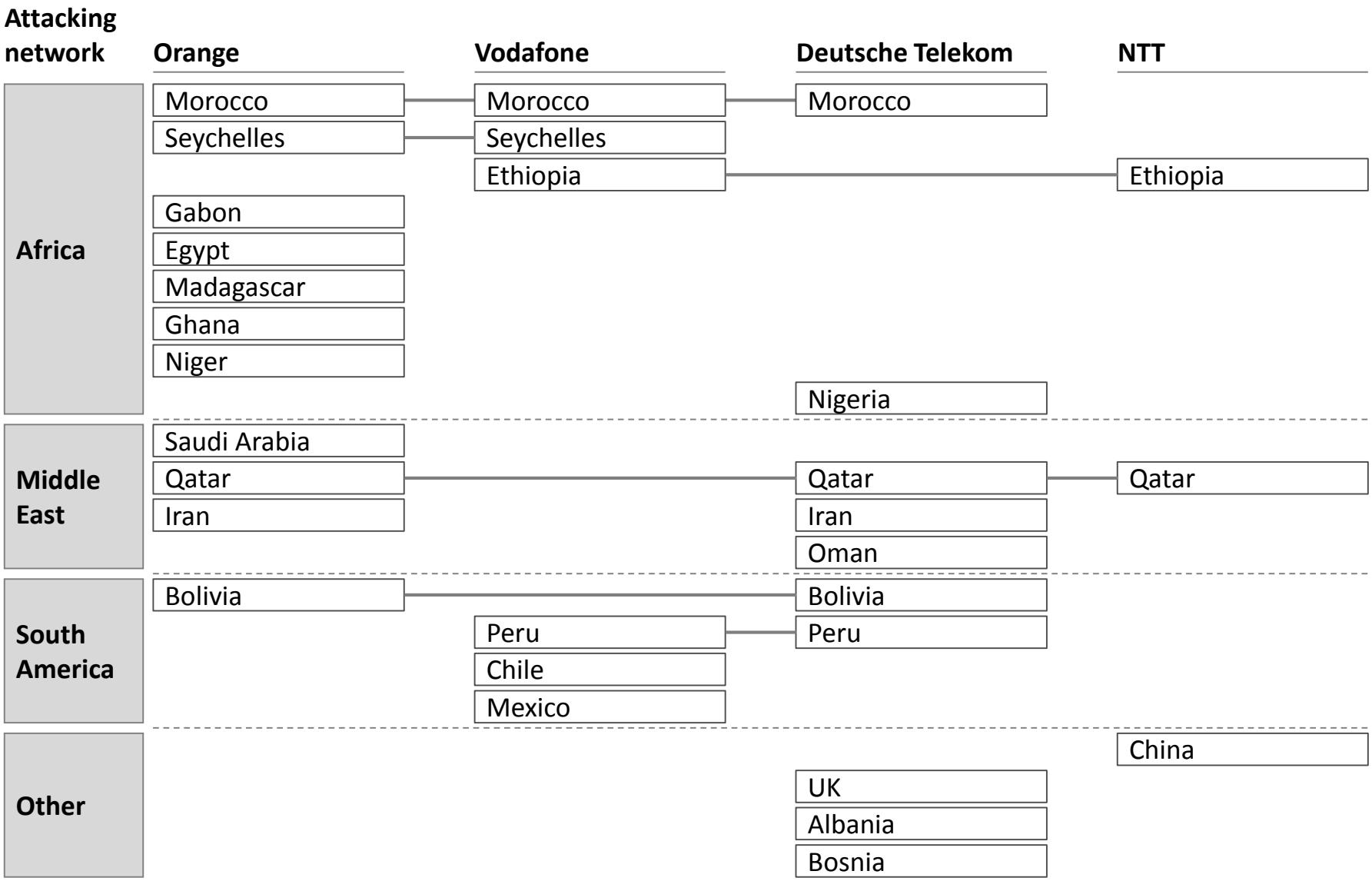
SS7 attacks are happening across the words

○ Some ○○ Thousands ○○○ Millions

		Observed attacks [GSMA FASG reports]			
	Attack message	**Orange** 22 countries	**Vodafone** 19 cntrs	**Deutsche Telekom** (Germany)	**NTT** (Japan)
Tracking	1. ATI	○○○	○○○	○○○	○○
	2. SRI-(SM)	○○○	○○	○	○○○
	3. PSI	○	?	○	○○○
	4. PSL	○	?	-	○○
	5. SendIMSI	○○	○○	○○	○○
Remote intercept	6. ActivateSS				
	7. Update location				
	8. ISD				
Fraud	9. DSD				
	10. SendID				

? No measurements reported to the FASG so far

Attacks originate in a diverse set of networks



Agenda

- 3 attack scenarios
- 10 attack messages
- **4 defense measures**

An SS7 firewall is necessary to defend from advanced attacks

	Defense	Messages	Where
Block	▪ Drop these messages	1. ATI 2. SRI 5. SendIMSI 10. SendID	1 **STP**
Re-route	▪ Home-routing + IMSI obfuscation	2. SRI-SM	2 **HLR**
Check origin	▪ Compare GT and IMSI: Is the operator asking about their own subscriber?	3. PSI 8. ISD 9. DSD	**Simple SS7 firewall**
Check location	▪ Compare GT with subscriber location: Is your subscriber in that country?	6. ActivateSS 7. UpdateLoc	3 **State-full SS7 firewall -or- simple firewall + ATI**

4 **+ Monitor, Monitor, Monitor!**

Take away

It's about time to solve 99% of the current SS7 problem by

- **… addressing 3 attack scenarios (Track, Intercept, Fraud) …**
- **… which rely on 10 SS7 messages …**
- **… that we can rejected using just 4 defense measures: STP, HLR, SS7 Firewall, and Monitoring!**

Questions?

Luca Melette <luca@srlabs.de>

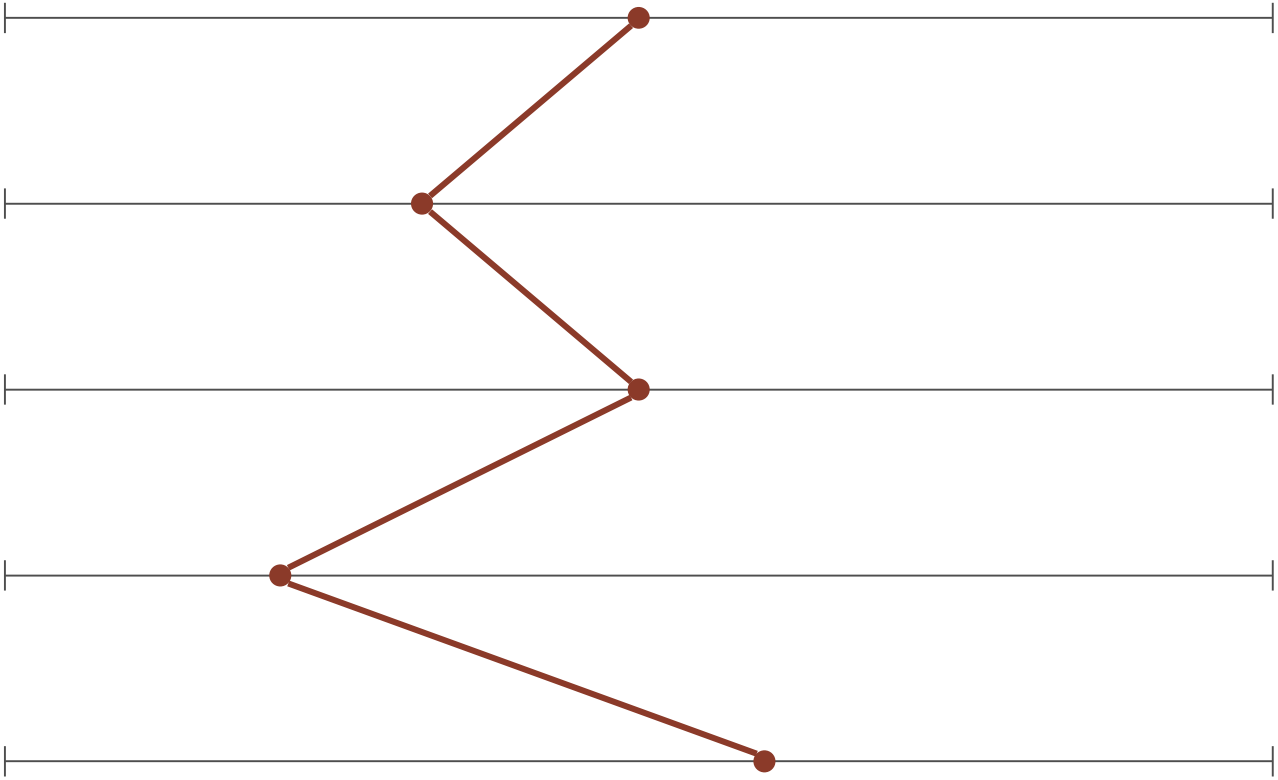
Protection from **SS7 threats** varies; can be improved

Exposure scan available from SRLabs

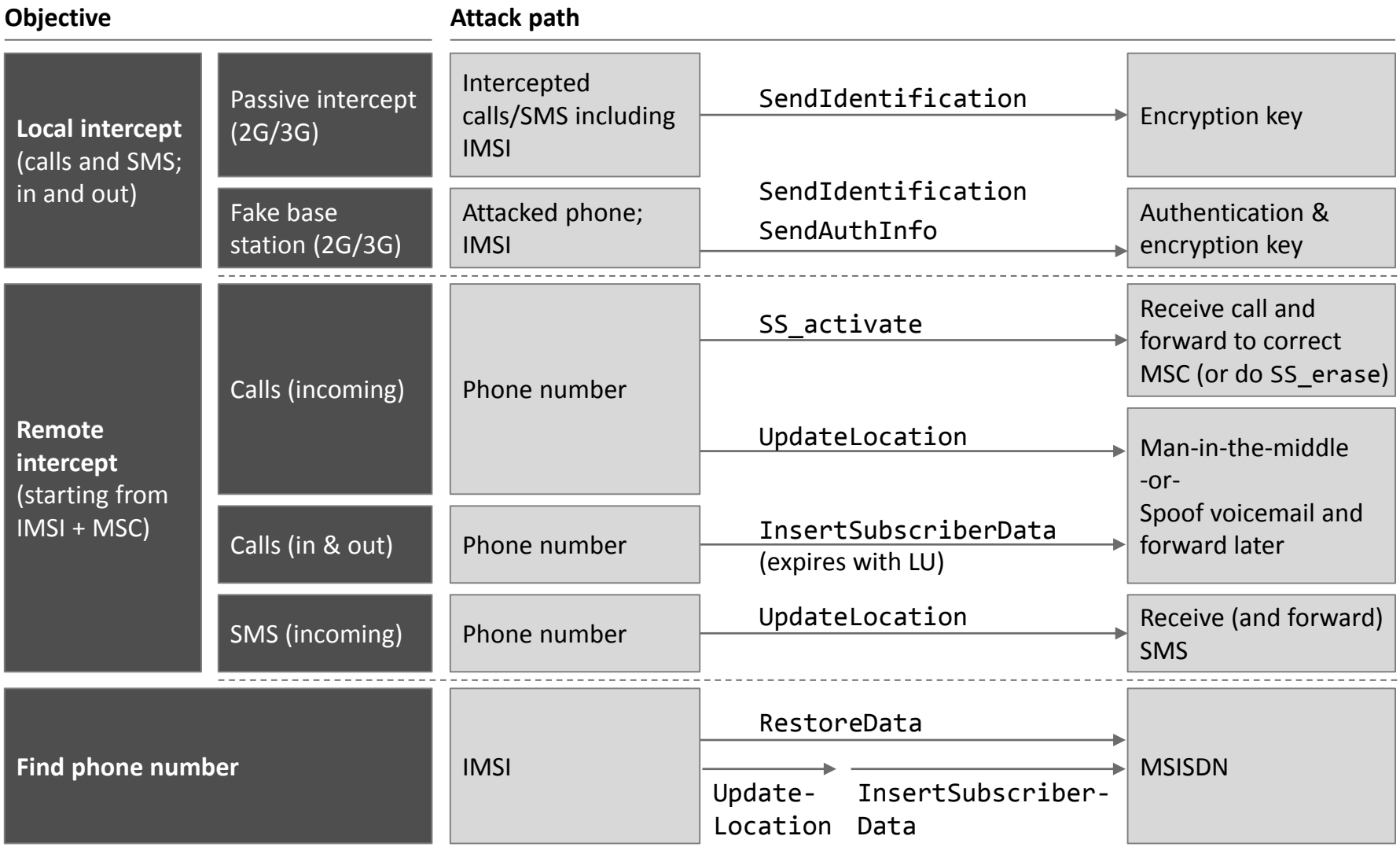
Illustrative

Threat category

		Unprotected	Standard attacks prevented	Advanced attacks prevented
A	**Tracking** – Remotely query subscriber location			
B	**Intercept** – Read SMS or listen to calls, locally or remotely			
C	**Denial-of-service** – Remotely disrupt subscribers service			
D	**Fraud** – Add premium number charges to bill			
E	**Spam** – Subscribers with SMS			



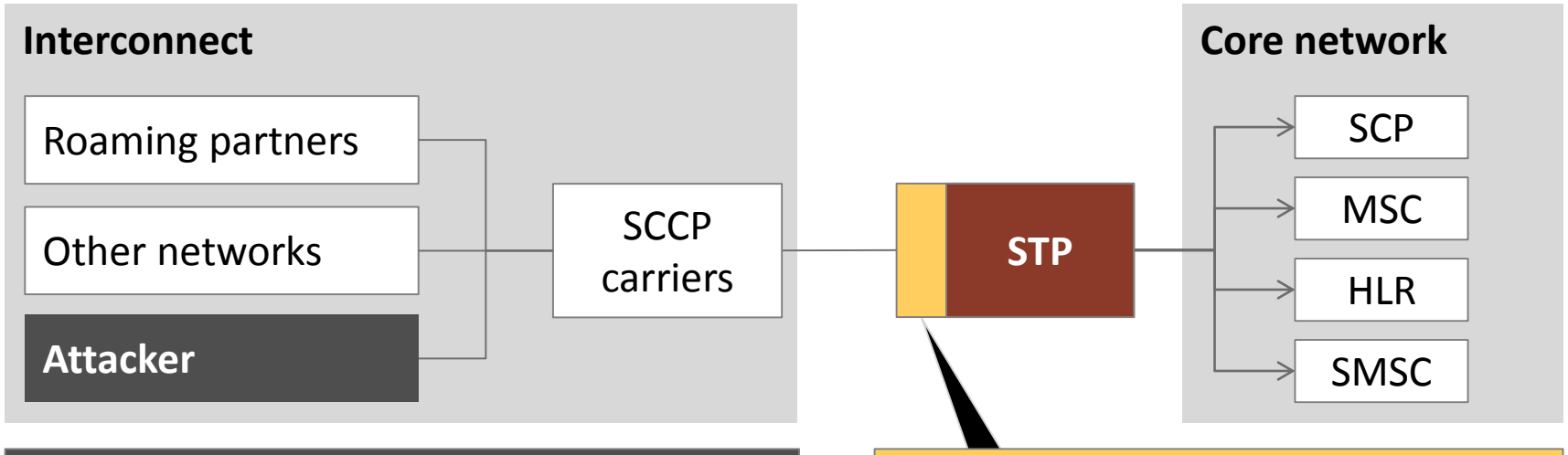
B Local and remote **intercept** is enabled through various signaling messages



Not all SS7 attacks can simply be blocked

Abuse scenario	Example SS7 attack 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)	

STP is the central instance for SS7 filtering



Attacker strategy

- Impersonate interconnect partners
- Address target elements by GT or SSN
- Issue unexpected MAP commands

STP defense

- **Block.** Verify that CgPA belongs to a trusted partner
- **L3 Firewall.** Enforce GT / SSN relationships
- **L7 Firewall.** Enforce MAP / GT relationships