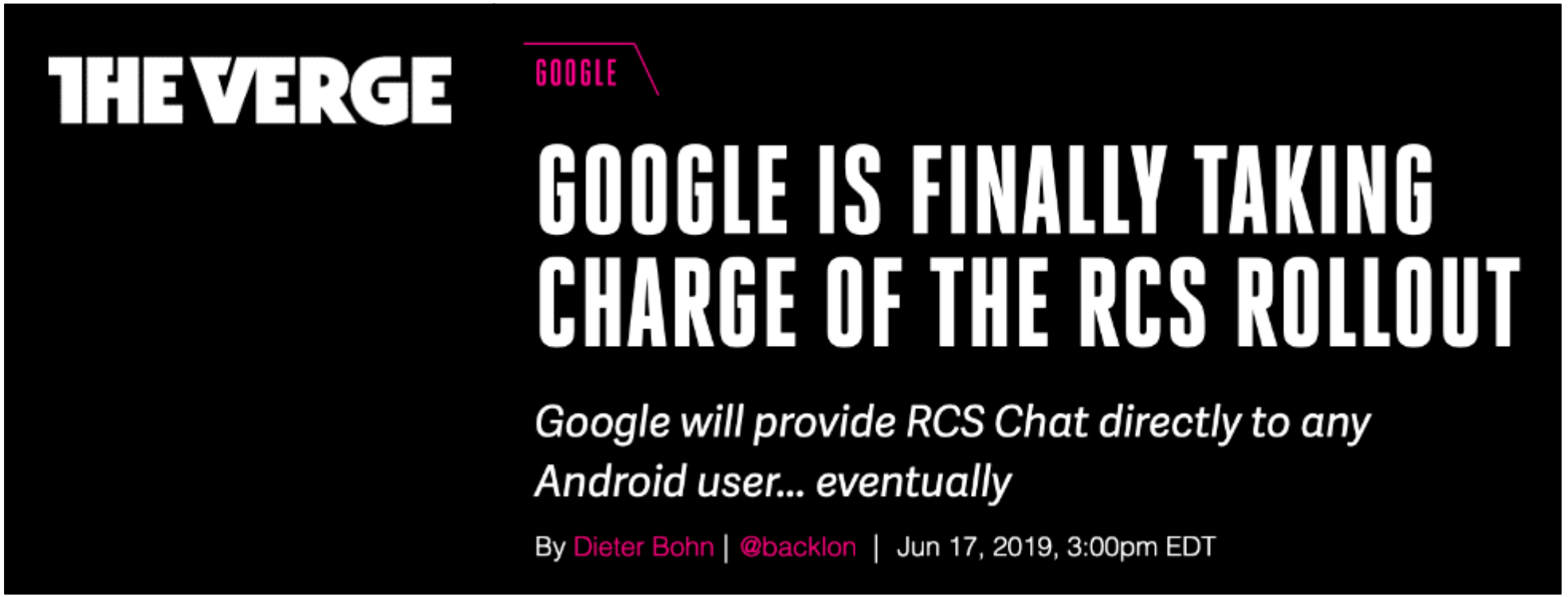
Mobile network hacking – All-over-IP edition

DeepSec, Nov 29 2019, Vienna

Luca Melette <luca@srlabs.de>
Sina Yazdanmehr <sina@srlabs.de>

Security
Research
Labs

Mobile networks are evolving, and research is hardly keeping up



THE VERGE

GOOGLE

GOOGLE IS FINALLY TAKING CHARGE OF THE RCS ROLLOUT

Google will provide RCS Chat directly to any Android user... eventually

By Dieter Bohn | @backlon | Jun 17, 2019, 3:00pm EDT

Research question

After several decades of intercept attacks (A5/1, SS7, IMSI catchers), **will RCS finally protect text messages?**

AT&T, Verizon, Sprint, and T-Mobile have finally agreed to replace SMS with a new RCS standard

There will be a new app

By Dieter Bohn | @backlon | Oct 24, 2019, 7:19pm EDT

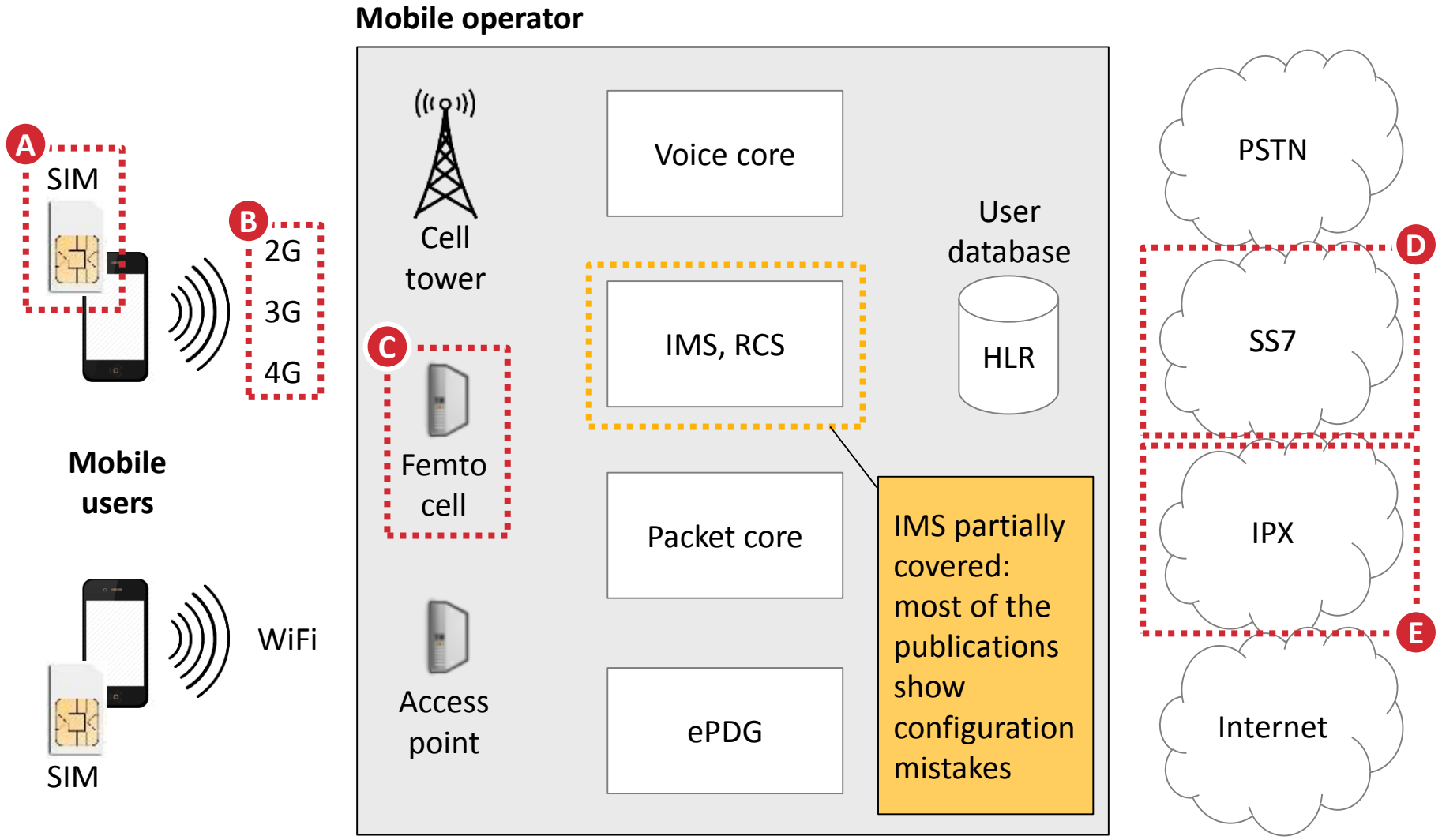
Agenda

1. **Mobile attack recap**
2. Attacks on new technologies
3. Mitigations

Known mobile network attacks can be categorized in 5 classes

Attack impact	Attack scope	Attack details
I Intercept calls and texts	Local	▪ Passively sniff and crack weak encryption (A5/1, A5/2), run IMSI catcher
	Remote	▪ Reroute voice flows enabling call forwarding via SS7
II Impersonate user identity	Local	▪ Grab TMSIs over-the-air, spoof originating call or SMS via radio interface
	Remote	▪ Send SMS or USSD code on behalf of another user via SS7
III Track users	Local	▪ Collect IMSIs from the radio interface, verify user presence with silent SMS
	Remote	▪ Globally locate mobile subscribers by requesting serving tower via SS7
IV Conduct fraud	No charge	▪ Disable call barrings and prepaid data limits via SS7
	Charge others	▪ Spoof calls and SMS to premium numbers, steal bank OTP codes in SMS
V DoS users or network	Subscriber	▪ Make users unreachable via detach message (radio) or cancel location (SS7)
	Network	▪ Exhaust MSC/HLR resources via SS7 requests (RESET, PRN, ATI, PSI)

Only some parts of a telco networks have been publicly dissected by security researchers



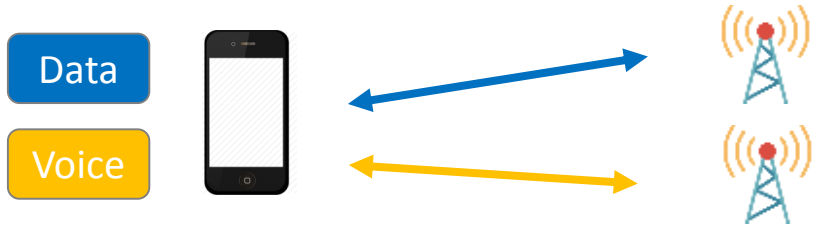
Several vulnerabilities have been identified in these telco components:

A. Malicious applications can be remotely installed in SIM cards
B. Weak radio encryption allow call/SMS and data to be intercepted
C. Devices in user hands can provide privileged access to core nodes
D. Hackers can remotely intercept calls/SMS and track users because of missing authentication
E. Like point D, but for data connections

New technologies are replacing legacy standards: IMS (VoLTE, VoWiFi) and RCS

Voice calls are moving from dedicated channels to voice-over-IP (VoIP)

Dedicated voice channels (CSFB)

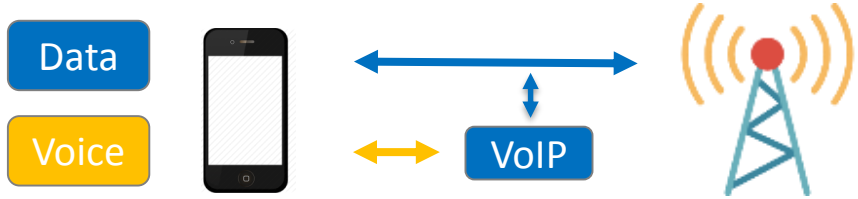


4G/5G

3G

The mobile uses legacy networks to transmit voice, the fast 4G link is only used for internet traffic

Basic VoIP (IMS)



4G/5G

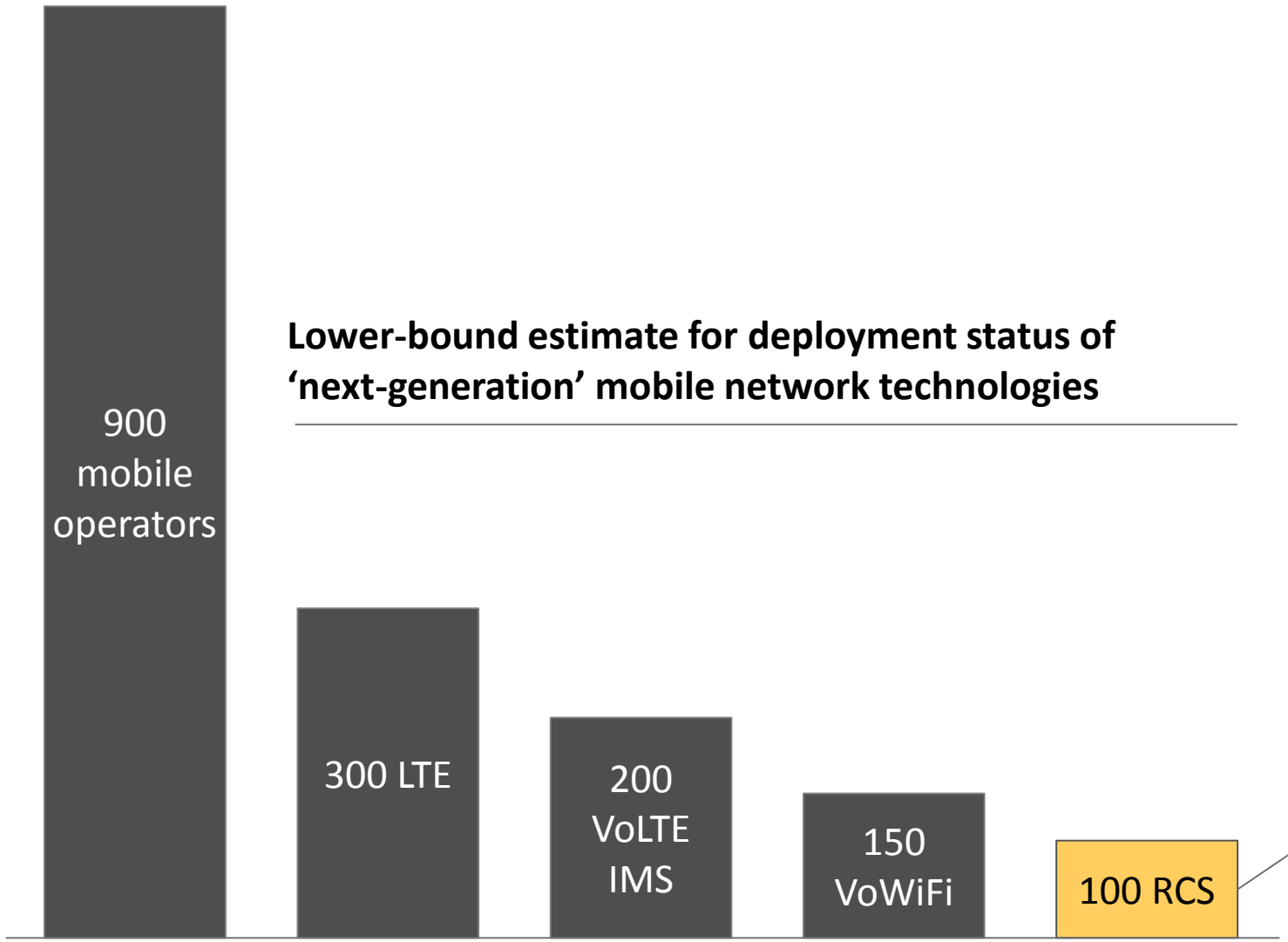
IMS makes the fast LTE interface usable for both internet and voice traffic

Advanced VoIP (IMS+RCS)

RCS messaging is similar to WhatsApp, iMessage

RCS is supported by an increasing number of networks

RCS is already implemented by at least 100 mobile operators

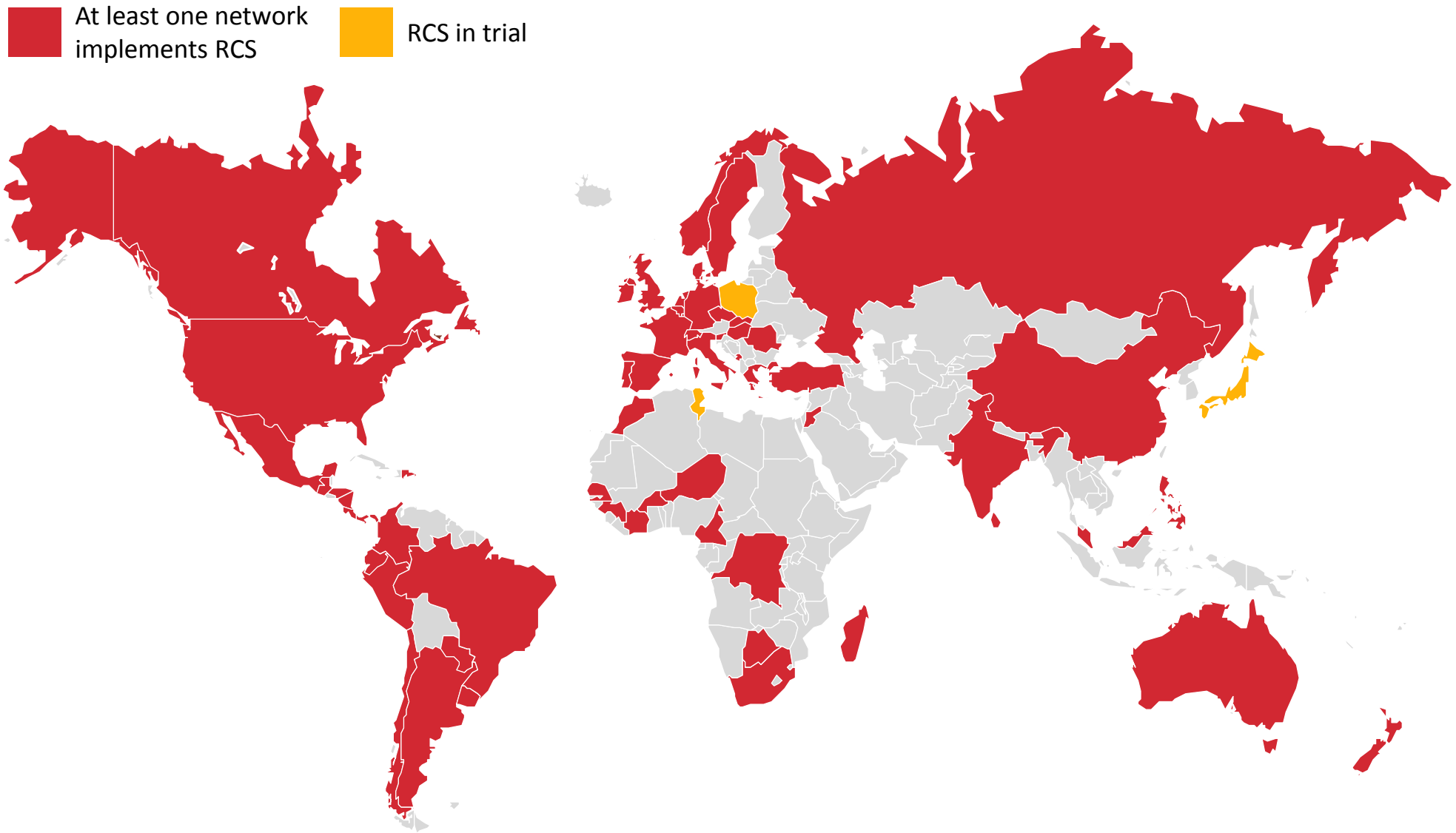


Lower-bound estimate for deployment status of 'next-generation' mobile network technologies

- Functional RCS deployments were identified through DNS and HTTP queries towards RCS-related domains [1]
- European telco groups constitute a large part of the current RCS deployments:
  - Orange (17 countries)
  - Vodafone (16 countries)
  - T-Mobile (9 countries)

[1] config.rcs.mncYYY.mccXXX.pub.3gppnetwork.org, where XXX and YYY are valid MCC and MNC values

Active RCS deployments span 67 countries, while a few others are conducting trials

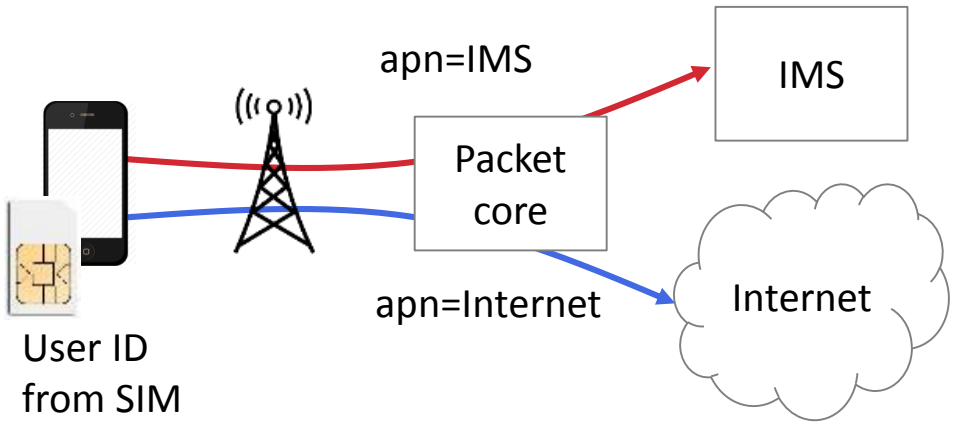


Agenda

1. Mobile network attack recap
2. **Attacks on new technologies**
3. Mitigations

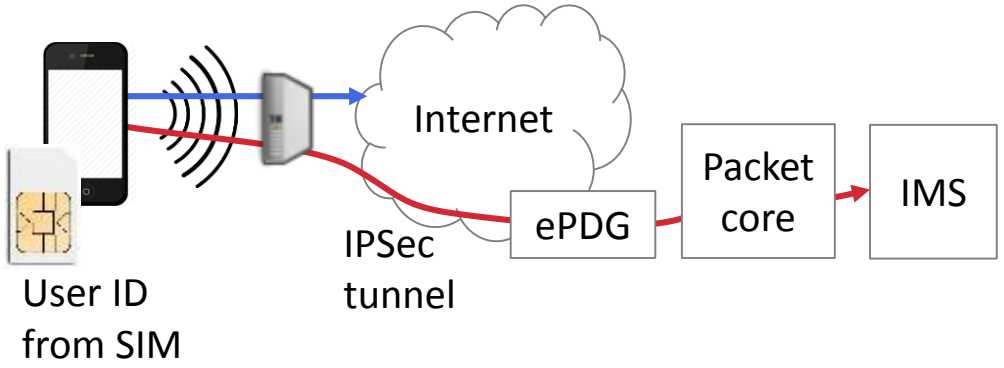
IMS security background: VoWiFi should be more secure than VoLTE thanks to additional IPSec authentication and encryption

VoLTE – Assumes trusted internet uplink



- Device connects to IMS PDN through LTE network
- All traffic goes through an IPSec tunnel that usually **does not have encryption**
- SIP signaling packets are encapsulated in ESP packets for integrity protection

VoWiFi – Assumes untrusted internet connection



- Device connects to ePDG to get access to packet core and IMS PDN
- All traffic goes through an **encrypted** IPSec tunnel
- SIP signaling packets are encapsulated in ESP packets that provides an **additional encryption** and integrity protection layer

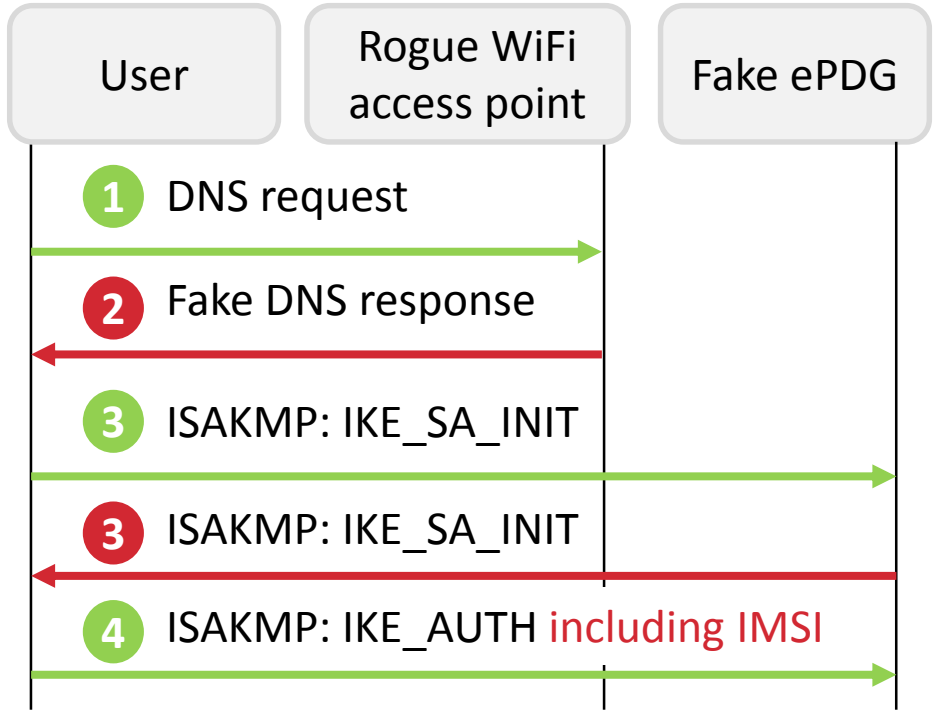
All authentication, encryption and, integrity keys are generated based on shared secret key on the SIM card by AKA

VoWiFi: Smartphones disclose their IMSI automatically when connecting to the ePDG

Smartphones that support VoWiFi (aka “WiFi-calling”) automatically attempt to establish a secure tunnel to the ePDG (IPSec endpoint) hosted by the mobile operator to offload voice traffic from radio channels

IMSI catcher attack scenario

1. After the victim connects to a rogue AP, the mobile automatically tries to connect to epdg.ims.mncXXX.mccYYY.3gppnetwork.org
2. The rogue AP fake the DNS reply, pointing the mobile to an ePDG controlled by the attacker
3. The phone negotiates and accepts IPSec capabilities suggested by the fake ePDG
4. The phone starts the authentication process sharing the victim’s IMSI



- The attack outcome is similar to IMSI catchers based on WiFi-EAP (BlackHat 2016, Piers O'Hanlon), but more powerful in 3 ways:
  1. Easier to implement since it only relies on DNS
  2. More generic because it works on uplinks other than WiFi
  3. Works against a larger number of phones since WiFi-EAP-SIM is less common than VoWiFi
- This new attack can be easily implemented using a Raspberry PI to create a rogue WiFi access point and running a modified version of StrongSWAN to emulate an ePDG and capture IMSIs

What attacks are possible in RCS?

Example hacking goal		Example method using RCS	Attack scope
Track users	A	Get IP address of victim / verify if user is online	These hacks should work against many RCS deployments as they do not require secret information about the victim; they do rely on configuration issues in the network
Impersonate users	B	Caller-ID spoofing in calls / messages	
Conduct fraud	C	Inject traffic / hijack session if victim is behind the same NAT	
Website DDoS	D	Send file attachment forcing auto-preview on victim	
Intercept texts	E	Connect to RCS with user credentials	Requires victim's config file

A User presence and coarse location can be disclosed by replies to SIP OPTIONS requests

Once connected to RCS, a malicious user can collect information about other users by sending the SIP OPTIONS request to sequential mobile numbers

In addition to presence, the response message discloses the local IP of the victim, potentially revealing its location

Attacker

SIP OPTIONS +4917xxx001

SIP OPTIONS +4917xxx002

SIP reply: user not found

SIP OPTIONS +4917xxx003

Mobile operator A

IMS RCS

SIP reply: user available

001

SIP/2.0 200 OK
CSeq: 1 OPTIONS
Contact:
<sip:+49xxx01@111.22.33.44:5060;
transport=tls>

Mobile operator B

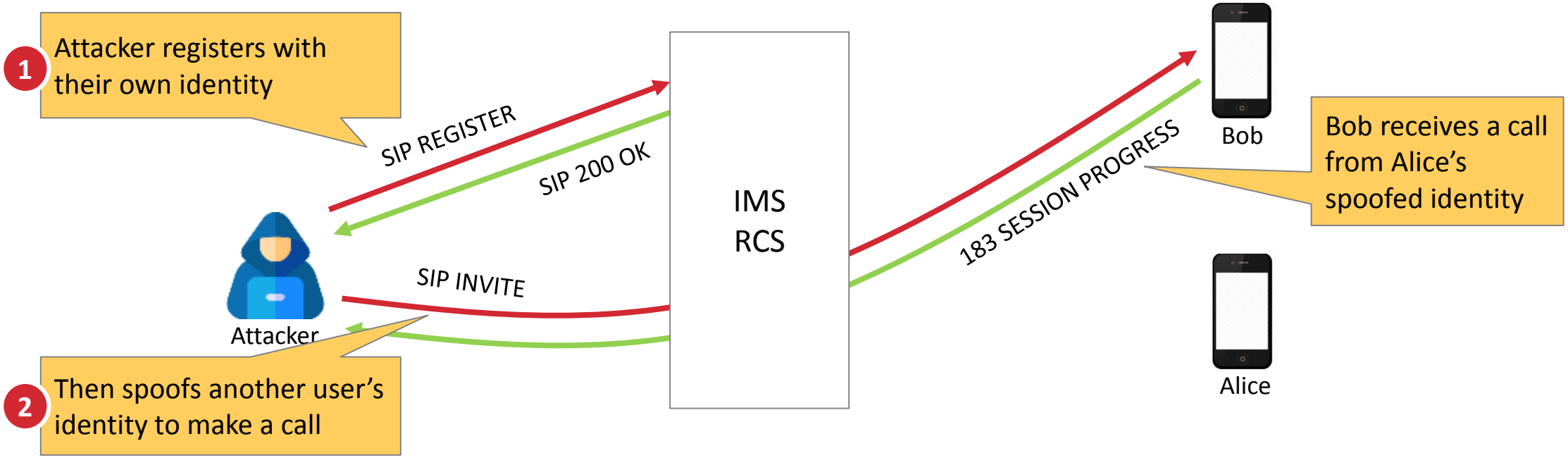
IMS RCS

SIP reply: user available

003

Thanks to number portability and commercial agreements between operators, users in other networks can be also paged and later attacked

B Caller-ID spoofing in calls / messages



1 SIP REGISTER

```
REGISTER sip:mno.net SIP/2.0
From:
<sip:+4917...@mno.net>;tag=291412310
To: <sip:+4917...@mno.net>
.....
```

2 SIP INVITE

```
INVITE sip:bob@mno.net;phone-context=mno.net SIP/2.0
To: <sip:bob@mno.net;phone-context=mno.net>
From: <sip:1337@mno.net>;tag=291412310
P-Preferred-Identity: <sip:1337@mno.net>
.....
```

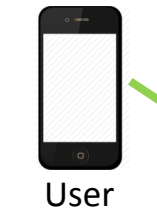
C Traffic injection is possible if victim and attacker share the same public IP address

Attack scenario 1

The attacker and victim are behind the same NAT

Attack scenario 2

The attacker manipulates user traffic using a rogue AP



1a User and attacker connect behind the same NAT and share an external IP

VPN

WiFi NAT

X

Internet

403 forbidden

200 successful

PCSCF 1

PCSCF 2

RCS core

User	IP	PCSCF
user-1	[Ext IP]	pcscf 2

-Demo-

2 Attacker identifies the correct PCSCF by trying all options

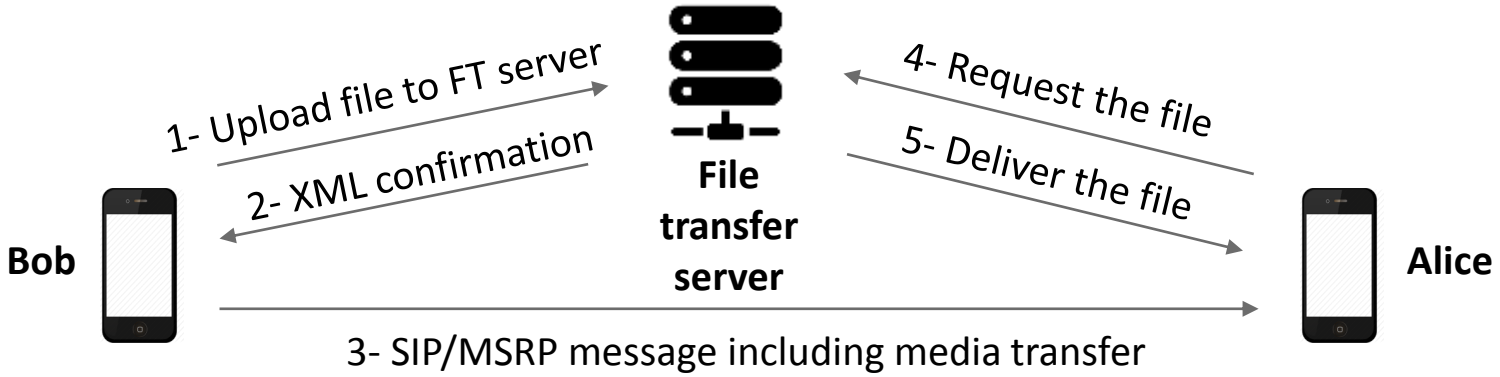
3 In some implementations, attackers can inject messages into the RCS core because users are solely identified by their mobile number and public IP

1b Attacker controls Internet uplink of victim

D File transfer uses unauthenticated XML files that enable abuse

RCS can send media content

The Message Session Relay Protocol is used to share files (images, videos, audio) between RCS users. This protocol is similar to SIP and HTTP, and carries content metadata in XML format.



Scenario 1 – **Leverage RCS clients to DDoS a website**

1. Attacker identifies a large file on a target website
2. Attacker crafts an XML message where the thumbnail URL (indicated as a small file) points to target large file
3. Attacker sends the crafted XML message as a SIP/MSRP message to many thousands of subscribers
4. Each RCS client automatically attempts to download the file overloading the target website

Scenario 2 - **User tracking**

1. The attacker starts a web server on a public IP
2. The attacker sends an RCS messages including previewable contents hosted on that server
3. The victim attempts to download the content disclosing their IP address

Scenario 3 - **Account takeover**

1. The attacker conducts the attack as in scenario 2, and collects headers sent by the victim
2. If an RCS session token is included, the attacker can impersonate the victim sending messages and starting calls

E Intercept can be achieved abusing RCS signaling in multiple ways

Attack scenario 1

Set call forwardings abusing the XCAP interface

Implementation issues (vendor dependent)
We found some buggy XCAP implementation that does not validate properly the identity when interacting with the server, thus enabling XCAP settings manipulation

Configuration issues (network dependent)
If the XCAP server uses password authentication instead of the secure SIM-based authentication, the password could be brute-forced

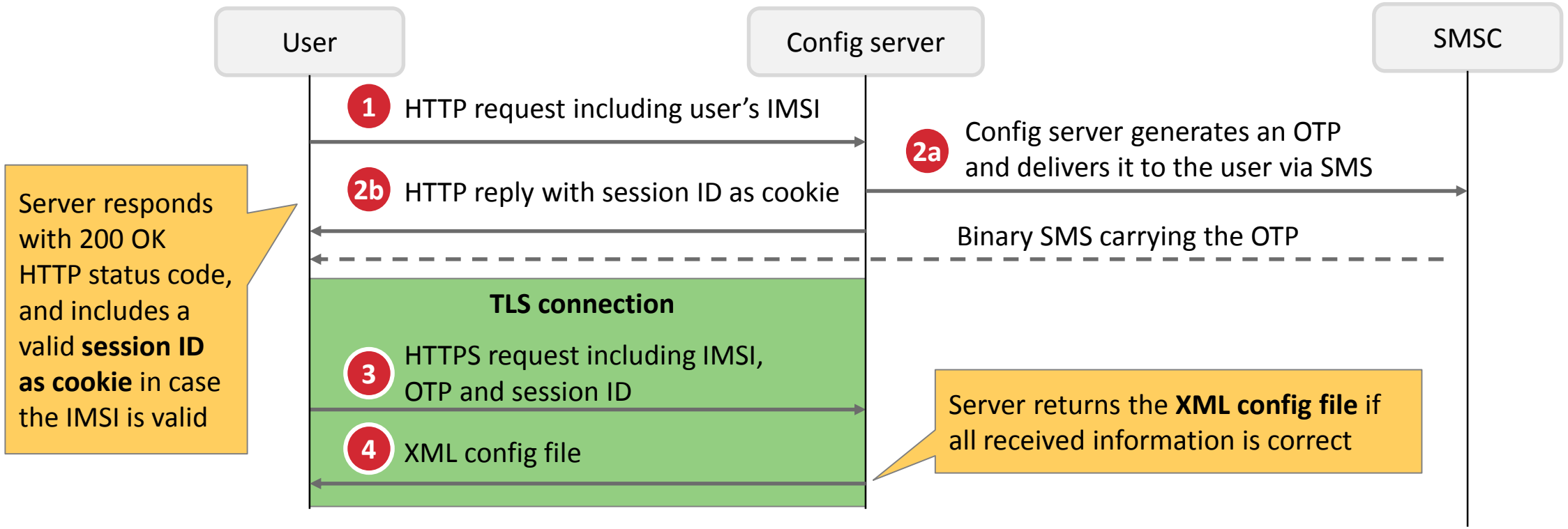
Attack scenario 2

Steal the config file so you can provision on behalf of the victim

1. Malicious apps
2. Mobile hotspot sharing
3. Malicious open WiFi with captive portal
4. Brute force identity/OTP via web

Details in the next slides

E 1+2 Malicious app or rogue hotspot can get in the middle of RCS provisioning



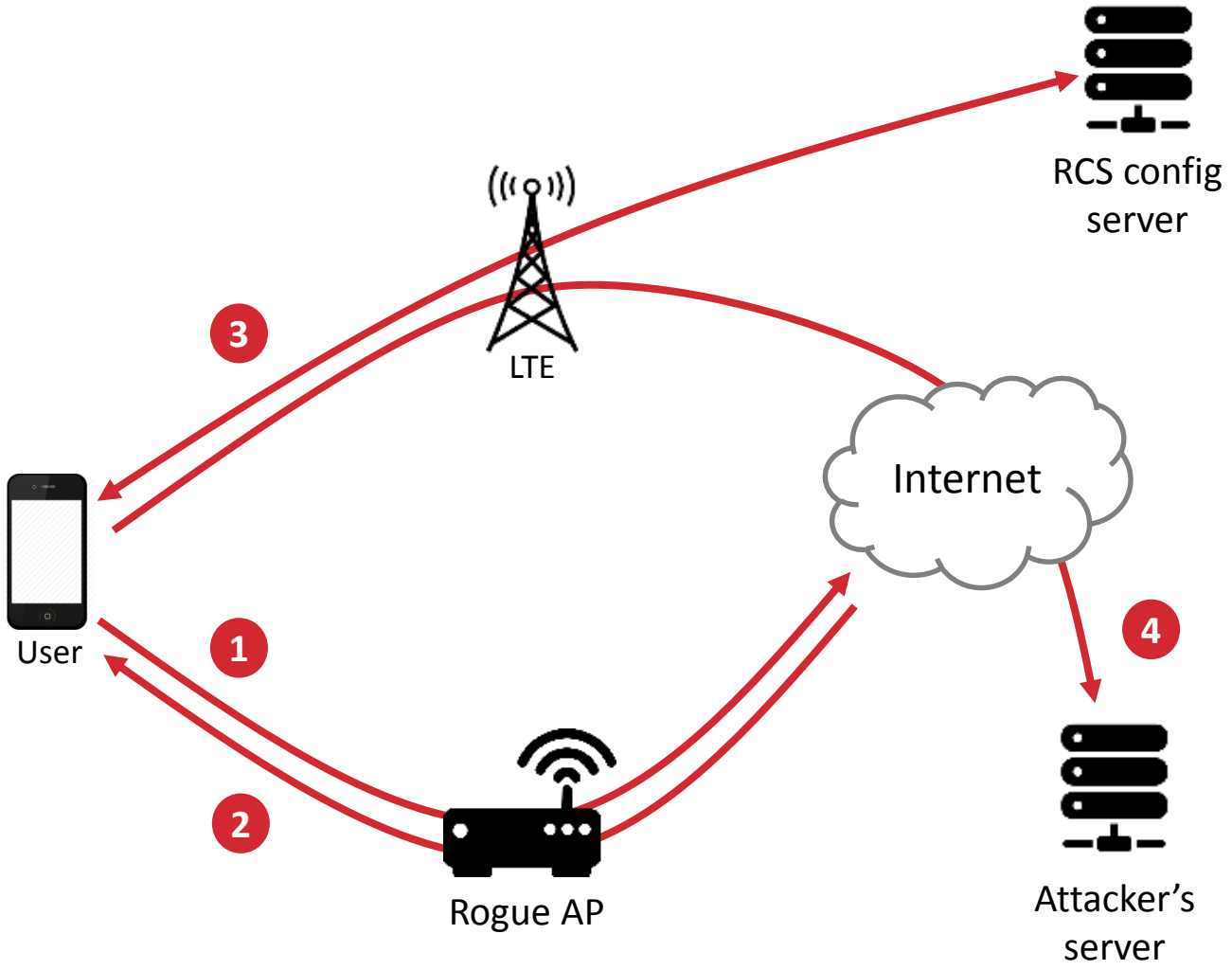
Attack scenario 1 Malicious app

- The app is installed on victim's device
- The app uses victim's LTE connection to fetch config file
- If the app has SMS_READ permission, it can retrieve even OTP code, for networks that require it

Attack scenario 2 Mobile hotspot sharing

- Attacker uses victim's LTE connection via hotspot sharing
- Attacker can request config file through victim's connection, and retrieve it

E3 Rogue WiFi can steal victim's config file injecting JavaScript code



Attack sequence

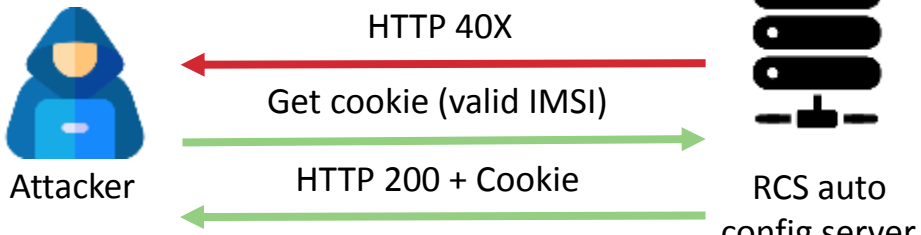
1. Victim tries to access a website through a rogue AP
2. The rogue AP retrieves the content of the website requested by the victim and forwards it back injecting malicious JavaScript. Immediately after, the AP pushes back the victim to LTE, terminating the WiFi access
3. The malicious JavaScript code retrieves the RCS config file via LTE connection
4. The malicious JavaScript code uploads the retrieved XML config file to the attacker's server on the internet

-Demo-

E4 Some networks requiring OTP verification are prone to user account brute force

Enumerate IMSIs. Perform GET over HTTP supplying a random IMSI until a 200 is returned

1

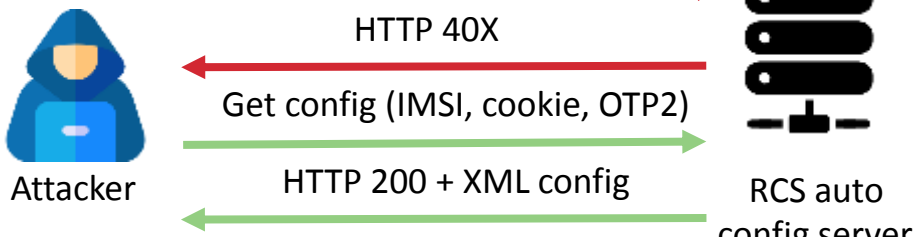


Valid IMSIs found

Request	Payload	Status
618	2006926662	200
416	2306619324	200
274	9905718604	200
1000	2339995484	403
999	5301958639	403
998	3019582052	403
997	6318945582	403
996	2346086272	403
995	9642808511	403
994	9233382889	403

Brute force OTP. Quickly perform GET over HTTPS trying all possible OTP values (up to 6 digits)

2



Correct OTP found

Request	Payload	Status ▲
47	364188	200
46	321886	400
45	860405	400
44	605306	400
43	980066	400
42	807303	400
41	525721	400
40	201573	400
39	070424	400
38	601133	400

E 1-4 Intercept first step: Login using victim's RCS account, activate SMS-over-IP in HSS

1. Steal victim's RCS config file (using any of the 4 methods described in the previous slides)

User

eNB

2. User attaches to the LTE network

3. Attacker registers to the RCS, announcing the SMS over IP capability in the SIP 'Contact' header

Attacker

Internet

EPC

MME

HSS/HLR

User	SMSoverCS	SMSoverIP
12345678	Yes	Yes

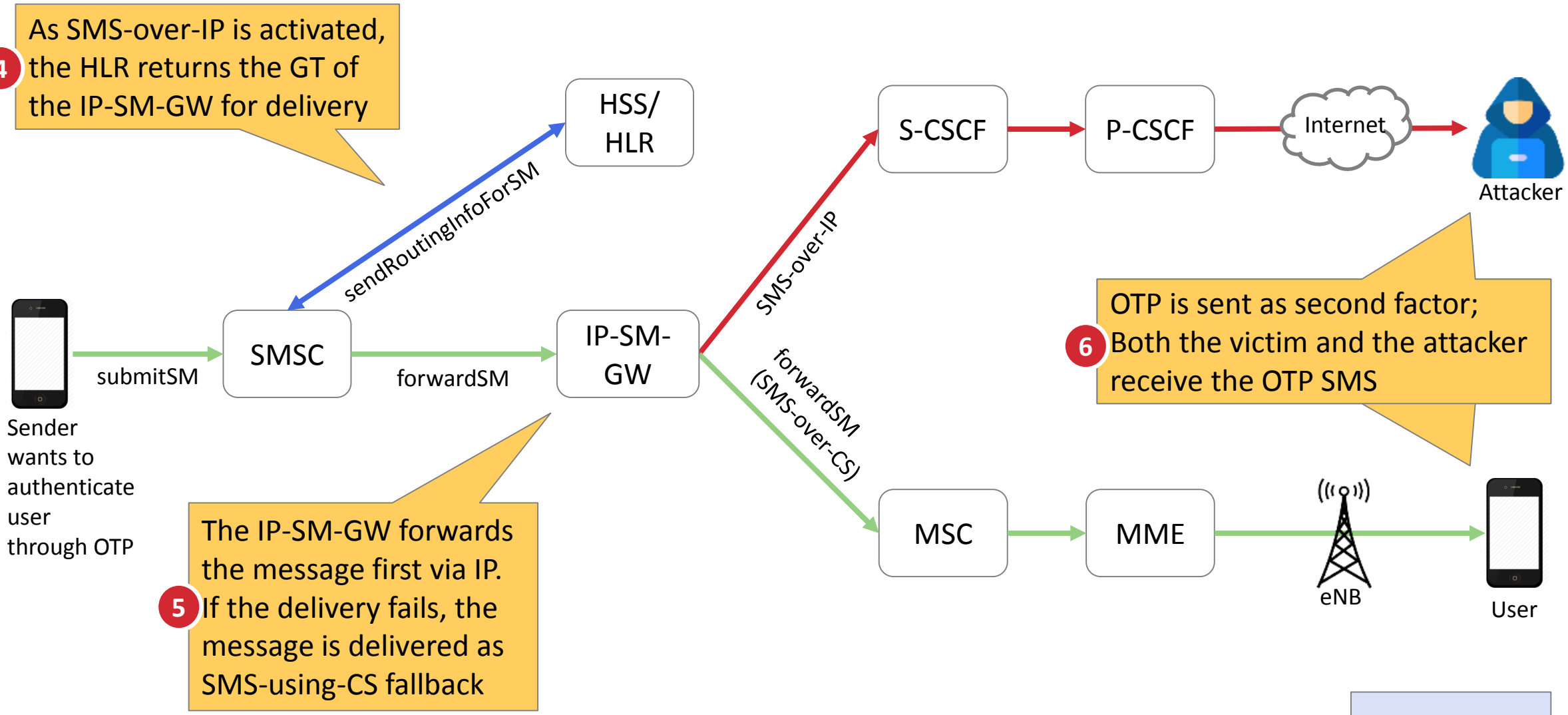
IMS

P-CSCF

S-CSCF

User	Capabilities	Connection
12345678	[+g.3gpp.smsip]	tcp:1.1.1.1:5060

E 1-4 Intercept second step: Wait for SMS delivery



Agenda

1. Mobile network attack recap
2. Attacks on new technologies
3. **Mitigations**

RCS issues can be mitigated by applying 6 best practices

- Not all RCS deployments are vulnerable to all attacks discussed in this presentation
- We found some vulnerable networks for each of the attacks
- To mitigate attacks, six countermeasures can improve RCS deployments

Area		Best practice	Implementation details	Affected components
Client provisioning		Authenticate using SIM / secure element	User authentication should be GBA/BSF based	RCS configuration server
	or	Use strong OTP verification codes	OTP should be at least 8 alphanumeric characters	RCS configuration server
		Apply rate limiting	Limit OTP validity to 5 minutes and 3 HTTP request attempts	RCS configuration server, SBC/P-CSCF
RCS services		Validate client identity	Validate SIP session using state (e.g. source IP, cookie, …)	SBC/P-CSCF
		Avoid information leakage	Strip sensitive information from SIP requests	SBC/P-CSCF, RCS client
		Filter uploaded contents	Check/restrict content-type and size provided by clients	SBC/P-CSCF, FT server

Take aways

1	Telcos and mobile vendors are moving all communications to IP protocols
2	New technologies are often poorly implemented, and are vulnerable to old attacks
3	Weak user authentication can expose RCS clients to intercept and impersonation risks
4	Security best practices should be applied and verified to new telco technologies

Questions?

Luca Melette <luca@srlabs.de>, Sina Yazdanmehr <sina@srlabs.de>