VoLTE Phreaking

Haxpo Track, Hack in the Box Conference, 9 May 2019





© 2018. Proprietary & Confidential.

Who am I?

- Ralph Moonen
- Technical Director at Secura
- Old school phreak



Agenda

- A little history of telephony hacking (in NL/EU)
- The landscape now
- Intercepting communications in 2019
- Vulnerabilities discovered: some new, some old
- An app to monitor traffic on a phone



History









The Hacker Quarterly

VOLUME SIX, NUMBER THREE AUTUMN, 1989



History

- Signalling systems:
 - Like DTMF but with other frequencies
 - Could be heard whilst setting up call
 - Could/can also be injected by end-user (analog phreaking not completely 100% definitively dead yet)
 - Trick exchange into thinking end-user is also exchange
 - R1, R2, CCITT4, CCITT5
 - ftp://ftp.wideweb.com/GroupBell

History in NL

- 80's: a group in NL found that this also worked in for our phone network.
- Back then, 06-022XXXX were toll-free (now 0800-numbers)
- Often international lines: faxes, hotel reservations, modems, etc.
- Allowed phreaking!



History in NL

- Blue box, brown box, green box: the rainbow warrior
- Endless phun!
- Make phree phone calls, get connected to chatrooms, secret switchboards, operators in Korea, the White House, CIA, FBI, and lots of modems.
- Remember: dial-in lines were expensive

Play around yourself







Arduino-based Blue Box with CCITT #4 and 2600 pulse dialing

1.863 views

📫 17 🐠 0 🌧 SHARE 🎫 SAVE ...

Digital

- Late 80's, early 90's, we transitioned to ISDN, digital lines
- SS7 was introduced
- Still used and abused
- OOBSS



Mobile

GSM 2G Architecture



Mobile

3G rel99 Architecture (UMTS) - 3G Radios



Mobile





4G

• 4G has a new mode of voice transport: Voice over LTE, VoLTE.



- It is an implementation of VoIP using SIP and RTSP over 4G.
- Signalling is handled in the phone's software (the actual voice path is usually/mostly/always(?) handled by the baseband chip and not available within the Android kernel)
- Signalling therefore back again into the users hand and mistakes from the 70's & 80's also!

VoLTE

- Android allows interaction with rmnet0 and rmnet1: IP interfaces for data, and SIP (signalling) traffic
- Often rmnet1 is IPv6
- IPsec tunnel is used to connect to SIP proxy (a.k.a. PCFCS)



SECURITY DETAILS

root	t@a3y17lte:/ # ip xfrm poli <u>cy</u>				
src	:4/128 dst	:1:2:5789:931c/128	sport	32821 dpc	ort 6100
	dir in priority 0				
	tmpl src :: dst ::				
	proto esp reqid 4 mode tr	an <u>sport</u>			
src	:1:2:5789:931c/128 ds	t :4/128	sport	6100 dpor	rt 32821
	dir out priority 0				
	tmpl src :: dst ::				
	proto esp reqid 3 mode tr	ansport			



root@a	a3y17lte:/ # ip xfrm state	
src	:4 dst	:1:4:9d02:2e42
40	proto esp spi 0x000137f8 replay-window 4	reqid 4 mode transport
	auth-trunc hmac(md5) 0xcad enc cbc(des3 ede) 0x4abe8 sel src ::/0 dst ::/0	d19b13c583c94c8d975d83113aaf4a 96 f15fee3719adb5cf91c963cb41b4abe8f15fee3719a

MISCONFIGURATIONS

root	t@a3y17lte:/ # ip xfrm_state	
src	:4 dst	:1:4:9d02:2e42
	proto esp spi 0x000137f8	reqid 4 mode transport
	replay-window 4	
	auth-trunc hmac(<u>md5</u>) 0xca	ad19b13c583c94c8d975d83113aaf4a 96
	enc cbc(des3 ede) 0x4abe8	3f15fee3719adb5cf91c963cb41b4abe8f15fee3719a
	sel src ::/0 dst ::/0	

- 3DES Enc key: 192 bits (2/3 = 128 bits)
- 8 bits error correction per key each round (128 8*2 = 112 bits)
- Chosen/known-plain text attacks (80 bits, ≈ 1024 bit RSA keys)
- Radio layer also encrypted, but if that fails, then the voice layer is potentially accessible to sophisticated threat actors

MISCONFIGURATIONS

General			
Network IP version	IPv6	IPv4	IPv6
Downgrade IP version?	no	n/a	no
Network discovery	no	yes	no
IPsec			
Authentication type	$\mathrm{hmac}(\mathrm{md5})$	$\mathrm{hmac}(\mathrm{md5})$	$\mathrm{hmac}(\mathrm{md5})$
Authentication key length	128 bits	128 bits	128 bits
Encryption type	ecb(null)	cbc(aes)	$cbc(des3_ede)$
encryption key length	0 bits	128 bits	192 bits
Disable encryption?	n/a	no	yes
Disable authentication?	no	no	yes
Disable IPsec itself?	no	no	yes

VoLTE sniffing

Older Android versions use a database with IMS settings:

/data/data/com.android.providers.telephony/databases/
/data/data/com.sec.imsservice/databases/

 At least one provider allowed disabling of IPsec through hidden activity:

am start -n com.samsung.advp.imssettings/.ImsSettingsLauncherActivity



Sniffing traffic

- And if you are root on the phone you can easily extract the IPsec keys:
- 'ip xfrm state'



Sniffing traffic

Host: adb forward tcp:31337 tcp:31337 Device: tcpdump -i any not port 31337 -s 0 -w - | nc -l -p 31337 Host: nc localhost 31337 | wireshark -i - -k -S



A	oplica	tions 🕶	Place	s v	2 Wirest	hark 🔻															
																.pcap	ng				
EI	e <u>E</u>	dit <u>V</u> iew	Go (Capt	ture <u>A</u> nalyz	e <u>S</u> tati	istics Tele	phory	<u>Win</u>	eless	Tools	He	lp .								
	1	140	25	12		0		1 1-0		-		@		0 0	6						
-		0.00				~				_		~	~	~ 11							
	sip																				
No.		Time	So	De	Protocol	Length	Info														
	2	0.000025	-	-	SIP	115	Request:	REG	ISTER	t sip	:ims.	mnc	. 0	cc204	.3gpp	network	.org	(1 bind	ting)		
	3	0.231971			SIP	959	Status:	401	Unaut	hori	zed										
	5	0.348458			SIP	512	Request:	REG	ISTER	t sip	:ims.	mnc	. 1	ICC284	.3gpp	network	.org	(1 bind	ding)		
	6	0.457170			SIP	988	Status:	200	OK (1 bi	inding) [
	7	0.496938			SIP	1500	Request:	SUB	SCRIB	E si	p:+31	6		()ims	.mnc	.mcc2	84.3g	ppnetwor	rk.org		
	8	0.537530			SIP	880	Status:	200	OK												
	10	0.548194	-		SIP/XML	132	Request:	NOT	IFY s	ip:+	316		90					8917:fbb	d]:7000		
	11	0.556083			SIP	864	Status:	200	OK												
	13	20.63925	1 _	-	SIP/SDP	1080	Request:	INV	ITE s	ip:0	6		;pho	ne-co	ntext	=ims.mn	c .(mcc204.3	3gppnetwork	.org@i	ms.
	14	20.67208	4		SIP	588	Status:	100	Tryin	g											
	22	21.35883	5		SIP/SDP	656	Status:	183	Sessi	on P	rogre	55									
	23	21.37778	5 _	-	SIP	1420	Request:	PRA	VCK si	p:				11	11111	f-@ht-t	as-1-	vip-sip.			
	35	21.55414	5		SIP	768	Status:	200	OK												
	40	21.56991	8		SIP/SDP	800	Request:	UPD	ATE s	ip:				f	TTTTT	ff-@ht-	tas-1	-vip-sip	ð.		
	63	22.03777	4 _		SIP/SDP	156	Status:	200	OK												
	64	22.04611	9		SIP	1280	Status:	180	Ringi	ing											
	774	35.95614	3		SIP	1448	Status:	200	OK												
	775	35.97716	9		SIP	1320	Request:	ACK	sip:					1111	1111	(ht-tas	-1-vi	p-sip			: 5
	778	48.51118	3		SIP	872	Request:	BYE	sip:	+316	5	8][:891	7:fbbd]:	7000		
	779	48.52476	6 _		SIP	932	Status:	200	OK				-					-			
	781	56.67109	4		SIP/SDP	1172	Request:	INV	ITE s	ip:2	84			90				:8917:	fbbd]:7000		
	783	56.75218	2 _	-	SIP/SDP	340	Status:	183	Sessi	on P	rogre	55							-		
	784	57 11815	8		STP	836	Request	PRA	CK si	n:+3	16		16				-8	917 fhhr	11.7000		

MORE DIFFERENCES

Operator A	Operator B	Operator C	RFC 3261
INVITE	INVITE	INVITE	INVITE
100 Trying	100 Trying	100 Trying	100 Trying
200 OK	183 Session Prog.	183 Session Prog.	180 Ringing
ACK	PRACK	PRACK	200 OK
BYE	200 OK	200 OK	ACK
200 OK	UPDATE	180 Ringing	BYE
	200 OK	200 OK	200 OK
	180 Ringing	ACK	
	200 OK	BYE	
	ACK	200 OK	
	BYE		
	200 OK		

VoLTE data

- Some (non-NL) providers still allow internet access through rmnet1
 - No data charges
 - Tunneling through DNS potentially also an option
 - Infrastructure discovery over rmnet1



VoLTE authentication



VoLTE SIM sharing

- Send CHALL to other sim-card on other phone over other channel, and receive RESP, and authenticate as that one
- Multiple users can share SIM-card that way
- Lawful interception and attribution at risk
- Theoretical: not tested yet (confident in feasability through)





VoLTE SMS

- Not all providers use this
- But tricks were possible in at least one implementation:
 - Replay SMS (SIP MESSAGE) from other phone
 - Network thinks SMS is from original phone (and bills him/her)
 - Enumerate users (errors generated if recipient not known)



VoLTE Leakage

 In at least one implementation, SIP traffic revealed too much information: P-Access-Network-Info header has utran-cell-id-3gpp=20x0xabcd1234567 of call recipient.



VoLTE Leakage

The world's largest Open Database of Cell Towers

Locate devices without GPS, explore Mobile Operator coverage and more!



VoLTE Leakage

- Under certain conditions, called ID blocking is ignored:
 - #31# private calls are revealed anyway in SIP headers
 - Also IP addresses of call recipients
 - And IMEI of recipient
- When aborting call without other side ringing, this info is received (stealthy) in SIP PROGRESS message



VoLTE has a cousin

- VoWiFi
- Same functionality over WiFi





- Berry Busser wrote an app to monitor SIP traffic
- <u>https://github.com/SecuraBV/SIPWatcher</u>
- No guarantees, Open Source, As-is
- Under limited development, contributions welcome!
- Known to work on Samsung A3 (other models will follow)
- If you are able to run it in other countries on other providers, we are interested in the results!

- Uses tcpdump and tshark to sniff and decode from rmnet1
- armv8 version included in .apk
- Needs to be crosscompiled for other architectures (tbd)

0	¥E 🕾 .d 4% 🖻 21:	15
≡ sipw	/atcher	
	START CAPTURE?	
Inf rmnet1:	2a01:380:b00c:9c91:1:1:f83:1f4b	
tshark:	AVAILABLE	
tcpdump:	AVAILABLE	
IPsec SA count:	4	
IPsec protocol:	ESP	
IPsec mode:	TRANSPORT	
Auth cipher:	HMAC_MD5_96	
Auth key: 0x25f	fe280c9692e5d3030eaa2b23c1ece	
Encr cipher:	NULL	
Encr key: 0x		

0		₩8 19.41 4% 🖻 2	1:16	0
≡	SIPWatcher		8	≡
	CAPTURING.	(STOP?)		
				×
				~

6	📲 🞌 .// 5% 🖻 21:1			
≡	SIPWatcher :			
	CAPTURING. (STOP?)			
	↑ SIP/SDP Request: INVITE			
	SIP Status: 100 Trying \downarrow			
\sim	SIP/SDP Status: 183 Session Progress \downarrow			
	1 SIP Request: PRACK			
	SIP Status: 200 OK \downarrow			
	SIP/SDP Request: UPDATE			
\sim	SIP/SDP Status: 200 OK \downarrow			
	SIP Status: 183 Session Progress \downarrow			
	↑ SIP Request: PRACK			
	SIP Status: 200 OK \downarrow			
	SIP Status: 180 Ringing \downarrow			
	↑ SIP Request: PRACK			

0	¥≹ ∯.iil 7% @ 21:1	8 🖬 🕲
≡	SIPWatcher :	=
	CAPTURING (STOP?)	
phone>;ta -1a13d79	ag=mavodi-6-10b-1e9-1-ffffffff005056A1F442-320c-2c17e700 -5cd32b2a-cebdb	
Call-ID: bi	ksIGhD6-5ECR6DIJ4zX7A_@2a01:380:b00c:9c91:1:1:f83:1f4b	
CSeq: 1 If	NVITE	Internet
Require: p	precondition,100rel	Za01:380
RSeq: 3		Encapsu
Contact:	<sip:mavodi-6-10b-1e9-1-fffffff-@asd-tas-1-vip-sip.volte.nl.tele2.< td=""><td>Len: 878</td></sip:mavodi-6-10b-1e9-1-fffffff-@asd-tas-1-vip-sip.volte.nl.tele2.<>	Len: 878
SUGU;tran	isport=tcp>	Session
INVITE,AC	CK, OPTIONS, BYE, CANCEL, INFO, PRACK, NOTIFY, MESSAGE, UPDATE	INVITE
Record-R	oute: <sip:mavodi-8-10f-3fffffff-8-ffffffff-0-@[2a01:380:a060::4];< td=""><td>phone</td></sip:mavodi-8-10f-3fffffff-8-ffffffff-0-@[2a01:380:a060::4];<>	phone
6666,1r;m	avsipodi-8-11b-6f6e-8-713b65>	Via: SI 61001
P-Early-M	fedia: sendrecv,gated	Max-F
Server: M	lavenir UAG/v1.0 PCSCF/v1.0-14042501o	Route
Feature-C	Caps: *;+g.3gpp.srvcc;+g.3gpp.srvcc-alerting;+g.3gpp.ps2cs-srvcc- electing	Route

Content-Length: 0

1 SIP Request: PRACK

Internet Protocol Version 6, Src: 2a01:380:b00c:9c91:1:1:f83:1f4b, Dst: 2a01:380:a060::4

Encapsulating Security Payload

User Da SIPWatcher has been granted superuser permissions for an interactive shell

PRACK 5060;transport=tcp SIP/2.0

Via: SIP/2.0/UDP [2a01:380:b00c:9c91:1:1:f83:1f4b]: 6100;branch=z9hG4bK-524287-1---7860f276fc729bed;rport;transport=UDP

Max-Forwards: 70

A LANGUAGE C ANNOUNCE (A) I... I A

2.net:

e e	4	17 .레 6% 🗷 21:17
≡	SIPWatcher	4
	STOPPED, RESTART?	
~	↑ SIP/SDP Request: INVITE	E.
Internet	Protocol Version 6, Src: 2a01:380:b00c:9c91:1:1: 0:a060-4	f83:1f4b, Dst:
Encansu	lating Security Payload	
Transmit Len: 878	ssion Control Protocol, Src Port: 6169, Dat Port:	6666, Seq: 1407, Ack: 1,
Session	Initiation Protocol (INVITE)	
INVITE	sip:+31653251082@ims.mnc002.mcc204.3gpp SIP/2.0	network.org.user=
Via: SI 6100,t	P/2.0/TCP [2a01:380:b00c:9c91:1:1:f83:1f4b]: tranch=z9hG4bK-524287-1c9d656aa2ea4c8ce	rport,transport=TCP
Max-F	orwards: 70	
Route:	<sip:{2a01:380:a060::4}:6666dr></sip:{2a01:380:a060::4}:6666dr>	
Route:	<sip:asd-pcscf-2-volte.nl.tele2.net;lr;mpcftk=6-1< td=""><td>15-13c1-c-400950c8></td></sip:asd-pcscf-2-volte.nl.tele2.net;lr;mpcftk=6-1<>	15-13c1-c-400950c8>
Proxy	Require: sec-agree	
Requir	e: sec-agree	
Contai .instar -7%3A	ct: <sip:+31640582271@(2a01:380:b00c:9c91:1: ice="<um:gsma:imei:35311809-804899-0>";+g.3(3gpp-service.ims.lcsi.mmtel"</um:gsma:imei:35311809-804899-0></sip:+31640582271@(2a01:380:b00c:9c91:1: 	1:f83:1f4b]:6100>;*sip gpp.icsi-ref="urn%3Aum
To: «si	p:+31653251082@ims.mnc002.mcc204.3gppne	twork.org;user=phone>
From: 48384	<sip:+31640582271@ims.mnc002.mcc204.3gpp 154</sip:+31640582271@ims.mnc002.mcc204.3gpp 	network.org>;tag=
Call-ID	bkslGhD6-5ECR6DIJ4zX7A.@2a01:380:b00c:9	c91:1:1:f83:1f4b
CSeq:	1 INVITE	
Sessio	m-Expires: 1800	
Accep	t: application/sdp, application/3gpp-ims+xml	
Allow:	INVITE, ACK, OPTIONS, CANCEL, BYE, UPDATE,	INFO, REFER, NOTIFY,

Conclusions

- Phreaking is back in 2019, in a digital way
- Possible, because signalling back in the hands of the user
- Already weaknesses are being found:
 - SMS spoofing, card sharing, subscriber locating, privacy issues.



Some notes

- Legality: interaction with operator's network might be illegal.
- Simple observation of your own traffic is legal in most countries.
- Based in part on work by Berry Busser, Radboud Uni, that he did for Secura as his Master Thesis.
- Responsible disclosure was followed in all cases, mentioned issues have been mostly remediated in NL for relevant providers.

FOLLOW US ON



© 2018. Proprietary & Confidential.

