SDR

Introduction

Maarten Pentinga

Junior-pentester & teacher. Big interest in breaking things, creating hacking challenges & organizing CTF events.

Roald Nefs

DevOps Engineer at DUO. Big interest in Site Reliability Engineering, Python, RF and more...

GitHub: <u>roaldnefs</u> E-mail: <u>roald@warpnet.nl</u>

E-mail: mp@warpnet.nl



Agenda

Introduction **Exercise:** Listen up! Regulations **Example:** Passive IMSI Catcher **Example:** Fixed Code **Example:** Rolling Code Hello Barbie! **Exercise:** Ring the Doorbell

Exercise: Listen up!

Exercise

- Work in groups of 4,
- Listen very carefully, they might broadcast twice.

Goal

- Listen at least to one radio station,
- Choose whether you would want to receive messages from the P2000 network or monitor air traffic.

30m

Extra

- Try and receive weather satellite images with your RTL-SDR. (Google required)

Frequency regulations

Countries have different regulations. Within the **Netherlands**, sending signals on common frequencies is **illegal**. Therefor a permit is required. For equipment with **limited reach** and **low transmitting powe**r no permit is needed.



Hmh, please do clarify!

Product Model: XD-RF-5V



Transmitter:Technical parameters ofProduct Model: XD-FSTLaunch distance :20-200 meters (different voltage, different results)Operating voltage :3.5-12VDimensions: 19 * 19mmOperating mode: AMTransfer rate: 4KB / STransmitting power: 10mWTransmitting frequency: 433MPinout from left \rightarrow right: (DATA; VCC; GND)We legal (:

Tabel 1Algemene toepassingen zoals bijvoorbeeld
telemetrie, telecommand, alarmering, data

		Frequentieband	Vermogen/Veldsterkte	Kanaalraster	Duty-cycle
	A	6765 - 6795 kHz	42 dBµA/m op 10 m afstand	-	-
	В	13,553 - 13,567 MHz	42 dBµA/m op 10 m afstand	-	-
	с	26,957 - 27,283 MHz	42 dBμA/m op 10 m afstand of 10 mW e.r.p.	-	-
	D	40,660 - 40,700 MHz	10 mW e.r.p.	-	-
┛	Е	433,050 - 434,790 MHz	10 mW e.r.p.	-	< 10 %
	E1	433,050 - 434,790 MHz	1 mW e.r.p. ¹	-	-
	E2	434,040 - 434,790 MHz	10 mW e.r.p.	25 kHz	-
	F	863,000 - 865,000 MHz	25 mW e.r.p.	-	< 0,1 % ³
	G	865,000 - 868,600 MHz	25 mW e.r.p.	-	< 1,0 % ³
	Н	868,700 - 869,200 MHz	25 mW e.r.p.	-	< 0,1 % ³
	1	869,300 - 869,400 MHz	10 mW e.r.p.	25 kHz	-
	К1	869,400 - 869,650 MHz	500 mW e.r.p.	25 kHz ²	< 10 % ³

Example: Fixed Code (1/3)

Devices using a fixed code are vulnerable to a replay and bruteforce attack. The attacker can simple record and replay the signal.

Using a bruteforce approach requires knowledge about the modulation type (FFCID).



Example: Fixed Code (2/3)

Instead of using an SDR to record the signal you can also use a cheap receiver to listen to the fixed codes.

For more popular devices such as *Klik Aan Klik Uit* you will even find libraries:

kakuarduino



Example: Fixed Code (3/3)

Most devices will repeat the fixed code several times.

Instead of repeating them, you can simple send each code once.

You might want to check of the <u>De Bruijn sequence</u>...



Example: Passive IMSI Catcher (1/5)

The passive International Mobile Subscriber Identity (**IMSI**) catcher works by capturing an IMSI number when a phone **initializes a connection to a base station**. To protect the privacy of the user all subsequent communication is done with a random Temporary Mobile Subscriber Identity (**TMSI**) number.

Active IMSI catchers perform a man in the middle attack and are definitely illegal!



Example: Passive IMSI Catcher (2/5)

Scan for nearby base stations:

File E	dit Vie	w Searc	h Termin	al He	elp										
19:27	\$ sudo	grgsm_	scanner												
linux;	GNU C	++ vers	ion 7.3.(9; Во	ost_106	501; U	HD_003	.010.0	003.0	90-0-u	ו <mark>kno</mark> י	//n			
ARFCN:	976,	Freq:	925.4M,	CID:	10353,	LAC:	210,	MCC:	204,	MNC:	4,	Pwr:	-39		
ARFCN:	978,	Freq:	925.8M,	CID:	60563,	LAC:	210,	MCC:	204,	MNC:	4,	Pwr:	-43		
ARFCN:	1022,	Freq:	934.6M,	CID:	60564,	LAC:	210,	MCC:	204,	MNC:	4,	Pwr:	-44		
ARFCN:	5,	Freg:	936.0M,	CID:	46836,	LAC:	3220,	MCC:	204,	MNC:	8,	Pwr:	-27		
ARFCN:	16,	Freq:	938.2M,	CID:	46837,	LAC:	3220,	MCC:	204,	MNC:	8,	Pwr:	-38		

Frequency

Power

Example: Passive IMSI Catcher (3/5)

Using <u>github.com/Oros42/IMSI-catcher</u> to sniff IMSI numbers (*will automatically scan and select a base station*):

File Edit	View Search	Terminal Help				
sudo pytl	hon simple_IM	SI-catcher.py				
Nb IMSI	; TMSI-1	; TMSI-2 ;	IMSI ;	ntry ; brand ; operator ; MCC ; MNC	; LAC ; CellId	
1	i		204 08 ;	herlands (Kingdom of the Netherlands) ; KPN ; KPN Mobil	e The Netherlands B.V. ; 204 ; 08	; 3220 ; 46836
2	;		204 08 ;	herlands (Kingdom of the Netherlands) ; KPN ; KPN Mobil	e The Netherlands B.V. ; 204 ; 08	; 3220 ; 46836
			204 08 ;	herlands (Kingdom of the Netherlands) ; KPN ; KPN Mobil	e The Netherlands B.V. ; 204 ; 08	; 3220 ; 46836
	;		204 08 ;	herlands (Kingdom of the Netherlands) ; KPN ; KPN Mobil	e The Netherlands B.V. ; 204 ; 08	; 3220 ; 46836
3	;		262 02	many ; Vodafone ; Vodafone D2 GmbH ; 204 ; 08	; 3220 ; 46836	
4	i		204 09 ;	herlands (Kingdom of the Netherlands) ; Lycamobile ; Lycamobil	e Netherlands Limited ; 204 ; 08	; 3220 ; 46836
5			260 06 ;	.and ; Play ; P4 Sp. z o.o. ; 204 ; 08	; 3220 ; 46836	
6	;		204 08 ;	herlands (Kingdom of the Netherlands) ; KPN ; KPN Mobil	e The Netherlands B.V. ; 204 ; 08	; 3220 ; 46836
	;		204 08	herlands (Kingdom of the Netherlands) ; KPN ; KPN Mobil	e The Netherlands B.V. ; 204 ; 08	; 3220 ; 46836
7	;		204 08 ;	herlands (Kingdom of the Netherlands) ; KPN ; KPN Mobil	e The Netherlands B.V. ; 204 ; 08	; 3220 ; 46836
8			204 12 ;	herlands (Kingdom of the Netherlands) ; Telfort ; KPN Mobil	e The Netherlands B.V. ; 204 ; 08	; 3220 ; 46836
9	;		204 08 ;	herlands (Kingdom of the Netherlands) ; KPN ; KPN Mobil	e The Netherlands B.V. ; 204 ; 08	; 3220 ; 46836
10			204 08 ;	herlands (Kingdom of the Netherlands) ; KPN ; KPN Mobil	e The Netherlands B.V. ; 204 ; 08	; 3220 ; 46836
11			238 02 ;	mark (Kingdom of Denmark) ; Telenor ; Telenor Denmark	; 204 ; 08 ; 3220 ; 46836	
12	;		204 08 ;	herlands (Kingdom of the Netherlands) ; KPN ; KPN Mobil	e The Netherlands B.V. ; 204 ; 08	; 3220 ; 46836
13	;		204 08 ;	herlands (Kingdom of the Netherlands) ; KPN ; KPN Mobil	e The Netherlands B.V. ; 204 ; 08	; 3220 ; 46836
	;		260 06 ;	.and ; Play ; P4 Sp. z o.o. ; 204 ; 08	; 3220 ; 46836	
	;		204 08 ;	herlands (Kingdom of the Netherlands) ; KPN ; KPN Mobil	e The Netherlands B.V. ; 204 ; 08	; 3220 ; 46836
	;		204 08	herlands (Kingdom of the Netherlands) ; KPN ; KPN Mobil	e The Netherlands B.V. ; 204 ; 08	; 3220 ; 46836
	;	; ;	204 08	herlands (Kingdom of the Netherlands) ; KPN ; KPN Mobil	e The Netherlands B.V. ; 204 ; 08	; 3220 ; 46836

Example: Passive IMSI Catcher (4/5)

The GSM traffic can be viewed in Wireshark, the !icmp && e212.imsi filter will only show packets that contain IMSI numbers.

									0	-						
			QQ		* * *	2 💻		Đ Đ		ш						
	icmp && gsmtap!											X		Expre	ssion.	
No.	Time	▼ Source	D	estination		Protoco	I Leng	gth Info								
	1135 1359.0802	889 127.0.0.1	1	27.0.0.1		LAPDm	1	81 U, fun	c=UI(C	CCH)	(RR) S	ystem I	nformat	tion T	ype 5	
1	1135 1359.0837	639 127.0.0.1	1	27.0.0.1		LAPDm	1	81 I, N(R)=0, N	I(S)=0	(Frag	ment)				
	1135 1359.1316	673 127.0.0.1	1	27.0.0.1		LAPDm		81 I, N(R)=0, N	I(S)=1						
	1135 1359.1361	507 127.0.0.1	1	27.0.0.1		GSMTAP		81 (CCCH)	(RR)	Syste	m into	rmation	Type 3	3		
	1135 1359.1400	165 127.0.0.1	1	7.0.0.1		CEMTAD		81 1, N(R)=0, N	Tmmod	into A	ccianmo	nt			
:	1135 1359.1454	002 127.0.0.1	1	27 0 0 1		I ADDm		81 T N/R	1-2 M	1(S)-0	(Eran	mont)	inc.			
	1135 1359 1868	895 127.0.0.1	1	7.0.0 1		GSMTAD		81 (CCCH)	(RR)	Pagin	n Requ	est Tyn	e 1			
	1135 1359,1869	518 127.0.0.1	1	7.0.0.1		LAPDm		81 T. N(R)=2.	(S)=0	(Frag	ment)				
	1135 1359.1946	464. 127.0.0.1	1	27.0.0.1		GSMTAP		81 (CCCH)	(RR)	Pagin	a Reau	est Tvp	e 1			
	1135 1359.1947	912 127.0.0.1	1	27.0.0.1		LAPDm	-	81 Ì, N(R)=2, N	I(S)=0	(Frag	ment)				
-	1135 1359.2034	049 127.0.0.1	1	27.0.0.1		LAPDm		81 U F, f	unc=UA	(DTAP) (MM)	Locati	on Upda	ating	Reque	st
1	1135 1359.2067	102 127.0.0.1	1	27.0.0.1		LAPDm	1	81 I, N(R)=0, N	I(S)=3	(Frag	ment)				
4																
*	SSM A-I/F DTAP Protocol Disc 00= S	- Location Upda criminator: Mob Sequence number	ating Request pility Managem :: 0	ent mess	ages (5)											
È I	<pre>SSM A-I/F DTAP > Protocol Disc 00</pre>	Location Upda riminator: Mob equence number DTAP Mobility M y Sequence Numb ting Type - No Identification n Classmark 1	ating Request pility Managem : 0 Management Mes per prmal pn (LAI)	ent mess sage Typ	ages (5) ne: Locatio	n Updati	ing Re	equest (0:	<08)							
•	SSM A-1/F DTAP > Protocol Disc 00= S 00 1000 = I > Ciphering Key > Location Upda > Location Area Mobile Static > Mobile Ident	Location Upda riminator: Mob Sequence number TAP Mobility N r Sequence Numb tting Type - No a Identification n Classmark 1 tty - IMSI (204 80 00 00 00 00	ating Request ility Managem : 0 anagement Mes per ormal on (LAI) 10 0 0 0 0 0 0 0 0 0 0 0 0 0	ent mess sage Typ 00 45 00	ages (5) ne: Locatio	n Updati	ing Re	equest (0:	(08)							
000	Link Access pro SSM A-1/F DTAP > Protocol Diss 00	- Location Upda riminator: Mob sequence number DTAP Mobility M / Sequence Numb ting Type - No 1 Identificatio n Classmark 1 Lty - IMSI (204 00 00 00 00 00	Ating Request ility Managem : 0 ber ormal on (LAI) 102 0 00 00 00 08 4 07 7f 00 00	ent mess sage Typ 00 45 00 01 7f 00	ages (5) He: Locatio	n Updati	Lng Re	equest (0;	(08)							
000	Link Access Fio SSM A-1/F DTAP > Protocol Diss 00s 00 1000 = 1 > Ciphering Key > Location Area > Mobile Stati > Mobile Ident 0 00 00 00 00 00 43 58 a0 0 00 10 9 c5	Location Upda riminator: Mob sequence number DTAP Mobility M / Sequence Numb ting Type - No A Identification n Classmark 1 (ty - IMSI (204 00 00 00 00 40 00 40 11 e4 12 79 00 2f fe	ating Request ility Managem : 0 Management Mess per prmal in (LAI) 00 00 00 00 00 00 4 07 7f 00 00 4 2 02 04 01	ent mess sage Typ 00 45 00 01 7f 00 01 00 05	ages (5) e: Locatio CX @ @	n Updati	ing Re	equest (0:	(08)		_		_			
000	Link Access Fro SSM A-1/F DTAP > Protocol Disc 00	- Location Upda riminator: Mob sequence number NTAP Mobility M v Sequence Numb tring Type - Not a Identificatio n Classmark 1 ty - INSI (204 00 00 00 00 00 40 00 40 11 e ² 12 79 00 2f ff 80 4a 08 00 05 r a constantion	ating`Request sility Managem :0 tanagement Messer ormal on (LAI) 102 000 00 00 08 4 07 7f 00 00 4 202 04 01 5 bd 01 73 49	ent mess sage Typ 00 45 00 01 7f 00 01 00 05 05 08 70	ages (5) e: Locatio	n Updati E	ing Re	equest (0:	(08)						_	
000	Link Access From SGM A-1/F DTAP Protocol Diss 00	- Location Upda criminator: Mobiequence number DTAP Mobility M v Sequence Numb tting Type - No a Identificatio on Classmark 1 1ty - IMSI (204 60 00 00 00 40 00 40 11 e4 12 79 00 2f fe 80 4a 08 00 05 fe 53	ating Request signal and a second se	ent mess sage Typ 00 45 00 01 7f 00 01 00 05 05 08 70 a3	ages (5) e: Locatic CX @ @ y. J.	n Updati	Lng Re	equest (0:	(08)							
000 001 002 003 004	Link Access From SGM A-1/F DTAP Protocol Disc 60= S 00 10000 = I Ciphering Key Location Upda Location Upda Location Aree Mobile Identi 00 00 00 00 00 43 58 a0 00 00 49 c5 10 00 274 80 ff 8c	Location Upda priminator: Moli requence number TAP Mobility W Sequence Numb ting Type - No Identificatio n Classmark 1 ty - INSI (204 00 00 00 00 40 00 40 11 e4 12 79 00 2f fc 80 4a 08 00 05 fe 53	ating Request bility Managem : 0 lanagement Mes- ber ormal in (LAI) 000 00 008 4 07 7f 00 00 4 22 02 04 01 5 bd 01 73 49	ent mess sage Typ 00 45 00 01 7f 00 01 00 05 05 08 70 a3	CX @ @ S	n Updati	Eng Re	equest (0:	(08)							
0000 001 002 003 004 005	Link Access Fro SSM A-I/F 0TAP > Protocol Diss 00s Ciphering Key Location Updie Location Updie Location Ares Mobile Static Mobile Gent Mobile Gent 00 00 00 00 00 00 00 00 00 00 00 00 00 00	Location Upda riminator: Mobi Mobility Mobility Mobilitation Identification Classmark 1 ty - IMSI (200 00 00 00 00 00 00 40 00 40 11 ec 40 00 40 10 ec 40 00 40 00 40 00 40 10 ec 40 00 40 00 40 00 10 ec 40 00 00 00 00 00 00 00 00 00 00 00 00 0	ating Request jility Managem : 0 lanagement Mes- er ormal in (LAI) 00 00 00 00 00 4 07 77 00 00 4 20 20 4 01 5 bd 01 73 49	ent mess sage Typ 00 45 00 01 7f 00 01 00 05 05 08 70 a3	e: Locatio	n Updati	E.	equest (0:	(08)							
000 001 002 003 004 005	Link Access Fro SSM A-1/F DTAP 9 Protocol Diss 00	Location Upda riminator: Mot sequence number titing Type - No titing Type - No titing Type - No titing Type - No titing Type - No 00 00 00 00 00 00 00 00	ating Request jlity Managem : 0 lanagement Mes- er yrmal in (LAI) 102 00 00 00 00 00 4 07 7f 00 00 4 40 7 7f 00 00 4 42 02 04 01 5 bd 01 73 49	ent mess sage Typ 00 45 00 01 7f 00 01 00 05 05 08 70 a3	ages (5) e: Locatio CX @ @ 	n Updati '-B sI+	Ling Re	equest (0:	(08)		_	_				
0000 001 002 003 004 005	Link Actess Fro SSM A.T/F DTAP Protocol Diss 0	Location Upda riminator: Mob sequence number VAP Mobility N / Sequence Numb I Identificatio n Classmark 1 Lty - INSI (204 00 00 00 00 00 00 00 00 00 12 79 00 27 fe 80 4a 08 00 00 fe 53	ating Request julity Managem : 0 danagement Mes er or mal on (LAI) 100 00 00 00 08 4 07 77 00 00 4 20 20 40 01 5 bd 01 73 49	ent mess sage Typ 00 45 00 01 7f 00 01 7f 00 01 2f 00 05 08 70 a3	e: Locatio	n Updati	Ling Re	equest (0)	<08)							
0000 0001 0002 0003 0004 0005	Link Actess Fro SSM A-T/F DTAP 9 Protocol Diss 08	Location Upda Triminator: Mot Sequence number ITAP Mobility M / Sequence Numb Ling Type - No Lidentificatio no Classmark 1 (1990) 100 000 000 00 000 000 00 000 000 00 000 000 00 000 00 000 00 00 00	ating Request jility Managem : 0 tanagement Mes per prmal on (LAI) 10: 0 00 00 00 8 407 77 00 08 407 77 00 08 407 70 00 8 407 74 00 8 5 bd 01 73 49	ent mess sage Typ 00 45 00 01 7f 00 01 00 05 05 08 70 a3	ages (5) e: Locatio -CX-@ @ 	n Updati	Lng Re	equest (0:	(08)							
000	Link Access Fro SSM A-I/F 0TAP > Protocol Diss 00	Location Upda riminator: Mob Bequence number 7AP Mobility M / Sequence Numb Indentification n Classmark 1 Lty - INSI (204 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	ating Request jility Managem : 0 tanagement Mes yer ymal on (LAI) 000 00 00 00 000 00 00 00 407 77 00 00 407 77 00 00 42 02 04 01 5 bd 61 73 49	ent mess sage Typ 00 45 00 01 7f 00 01 00 05 05 08 70 a3	ages (5) e: Locatio CX @ @ 	n Updati	ing Re I P	equest (0:	(08)			_				

Example: Passive IMSI Catcher (5/5)

Problems occur when you can associate an IMSI number with an individual.

Mobile apps can access a device's IMSI number, e.g. getSubscriberId on Android...



Example: Rolling Code (1/3)

Rolling code is used in keyless entry systems to prevent replay attacks. The car and keyfob use a pseudorandom number generator.



Example: Rolling Code (2/3)

Jam the vehicle's frequency and intercept two codes. Stop jamming an Immediately send the first received code so the owner won't notice anything...



The second captured code is still usable and can be used as long as the owner doesn't (un)lock the vehicle.

Example: Rolling Code (3/3)

Used hardware: two **YARD Stick One's** (Yet Another Radio Dongle), which can transmit and receive digital wireless signals at frequencies below 1 GHz.

The YARD Stick One come with <u>RfCat</u> firmware tnstalled. RfCat allows you to control the wireless transceiver from an interactive **Python** shell.

YARD Stick One != SDR



Hello Barbie! (1/3)

Let's take a closer look at Barbie...



Hello Barbie! (2/3)

FCC ID: PIYDKF74-15A5W

Operating Frequencies

Searchable FCC ID Database: <u>fccid.io</u>

Document	Туре	Available
User manual-2	Users Manual Adobe Acrobat PDF (237 kB)	2015-10-16 2015-10-20
User manual-1	Users Manual Adobe Acrobat PDF (4139 kB)	2015-10-16 2015-10-20
Tune up procedure	Parts List/Tune Up Info Adobe Acrobat PDF (25 kB)	2015-10-16 2015-10-20
Letter MCL	Cover Letter(s) Adobe Acrobat PDF (32 kB)	2015-10-16 2015-10-20
Confidential letter	Cover Letter(s) Adobe Acrobat PDF (64 kB)	2015-10-16 2015-10-20
Channel statement	Cover Letter(s) Adobe Acrobat PDF (32 kB)	2015-10-16 2015-10-20
Authority letter	Internal photos	2015-10-16 2015-10-20
Setup photos		2015-10-16 2015-10-20
SZEM150800520001-revised		2015-10-16 2015-10-20
SZEM150800520002 -rev2	External photos	2015-10-16 2015-10-20
Label	AUUVE AUUVALPUF (2140 KD)	2015-10-16
Internal photos	Internal Photos Adobe Acrobat PDF (1999 kB)	2015-10-16 2015-10-20
External photos	External Photos Adobe Acrobat PDF (1418 kB)	2015-10-16 2015-10-20
5200CR PBA	Cover Letter(s)	2015-10-16

Frequency Range	Power Output	Rule Parts	Line Entry
2.412-2.462 GHz 📭	79 mW	15C	1

Hello Barbie! (3/3)



Exercise: Ring the Doorbell



Exercise

- Work in groups of 4,
- Finish assignment 1 till 7 from chapter 3.

Goal

- Ring the doorbell by recording the signal, demodulation in Audacity and writing your own doorbell script.



