摩托罗拉 C118 基于 Osmocom-BB & OpenBTS 搭建小型短信基

站

0x00 写在前面

大家应该都听说过摩托罗拉 C118 配合 Osmocom-BB 实现 GSM 网络下的短信拦截功能

吧,在14年左右新出了一种玩法就是Osmocom-BB的 sylvain/testing 分支固件可以配

合 OpenBTS, , 借助周围信号强度较大的 ARFCN 伪造出一个新的基站信号。不过由于摩托

罗拉 C118 的问题,无法实现语音通话功能只可以发送短信(默认只可以发送英文短信,修

改源码可以实现发送中文短信)

以下内容将会指导你怎样用 Osmocom-bb 兼容的手机(如 c115,c118,c123 等)当作

OpenBTS 的无线收发机.

0x01 环境

已顺利编译运行过 Osmocombb 的可继续往下看,否则请参考官方链接或优秀文章

首先安装 libosmo-dsp 库

先下载

\$ git clone git://git.osmocom.org/libosmo-dsp.git

编译前需要安装 fftw3

\$ apt-get install libfftw3-3 libfftw3-dev libfftw3-doc

然后编译

\$ cd libosmo-dsp \$ autoreconf -i \$./configure \$ make \$ makeinstall

0x02 Osmocom-BB

采用 sylvain/testing 分支 (具体可看 WIKI)

先下载

\$ git clone git://git.osmocom.org/osmocom-bb.git

再切换分支编译

\$ cd osmocom-bb \$ git checkout sylvain/testing

默认编译出的版本发送信号相关的功能是被注释掉的,用 mobile 启动 layer23 后会一直于

搜信号的过程中,因为无法发送信号。

把 osmocom-bb/src/target/firmware 下的 Makefile 中的 DCONFIG_TX_ENABLE 宏打

开:

Uncomment this line if you want to enable Tx (Transmit) Support. #CFLAGS + = -DCONFIG_TX_ENABLE

然后到 src 目录下编译

\$ cd src make HOST_layer23_CONFARGS=--enable-transceiver

0x03 OpenBTS

这里使用的 OpenBTS 的版本是 OpenBts-p2.8 (嫌手动编译麻烦的可以找我要 DEB 安装

的教程),首先安装依赖

\$ sudo apt-get install autoconf libtool libosip2-dev libortp-dev libusb-1.0-0-dev g++ sqlite3 libsqlite3-dev erlang libreadline6-dev libncurses5-dev

下载源码

\$ svn co http://wush.net/svn/range/software/public (svn 版本必须 <= 1.7)

然后编译安装(有不懂的可以前往 WIKI 查看详细资料)

\$ cd a53/trunk \$ make install

\$ cd openbts/trunk
\$ autoreconf -i
\$./configure
\$ make
\$ make
\$ mkdir /etc/OpenBTS
\$ sqlite3 -init ./apps/OpenBTS.example.sql /etc/OpenBTS/OpenBTS.db ".quit"

\$ mkdir -p /var/lib/asterisk/sqlite3dir

\$ cd subscriberRegistry/trunk \$ make \$ sqlite3 -init subscriberRegistry.example.sql /etc/OpenBTS/sipauthserve.db ".quit"

\$ cd smqueue/trunk \$ autoreconf -i \$./configure \$ make \$ sqlite3 -init smqueue/smqueue.example.sql /etc/OpenBTS/smqueue.db ".quit"

安装 OpenBTS 后按照 WIKI 的说明配置/etc/OpenBTS/OpenBTS.db

首先安装数据库编译软件

\$ apt-get install sqlite3 sqliteman (ubuntu 系统安装 , Kali 自带 sqlitebrowser 无需安装)

然后在终端内输入 sqliteman 启动软件, 打开/etc/OpenBTS/目录下的 OpenBTS.db 文件

Control.GSMTAP.TargetIP = 127.0.0.1 GSM.Radio.NeedBSIC = 1 GSM.Radio.Band = 900 GSM.CellSelection.Neighbors =(留空) GSM.RACH.MaxRetrans = 3 GSM.RACH.TxInteger = 8 GSM.Radio.C0 = (发射的频点,数值1-124之间)

Control.LUR.OpenRegistration =.*

应用程序 ▼ 位置▼ 15:31 /etc/OpenBTS/OpenBTS.d File Edit View Help 🐻 New Database 🛛 👦 Open Database 🕆 Write Changes 🛛 🛱 Revert Changes SQL Log Database Structure Browse Data Edit Pragmas Execute SQL Show SQL submittee up represent ORDER BY 'rowid' ASC; SELECT 'rowid' ASC; LIMIT 0.50000; PRAGMA Aird yacum PRAGMA Airdy arcum Frage size PRAGMA Airdy arcum Frage size PRAGMA Airdy arcum Frage frage size Frage size Frage size Frage frage size Fra Show SQL submitted by Application V Table: CONFIG V 👸 New Record Delete Record VALUESTRING STATIC C KEYSTRING Filter /var/run/comm... 0 CLI.SocketPath 0 1 CLI.Sockettern 0 0 0 0 0 0 0 Control.Call.QueryRRLP.Late 3 Control.GSMTAP.GPRS 1 0 0 5 Control GSMTAP GSM 0 0 Control.GSMTAP.TargetIP 127.0.0.1 0 0 PRAGMA synchronous PRAGMA user, version PRAGMA vuser, version PRAGMA vasi, autorhekpoint PRAGMA vasi, autorhekpoint SELECT type name-sqliblin name FROM sqlite, remp. master: SELECT type name-sqliblin name FROM sqlite, remp. master: SELECT coUNT(*) FROM (SELECT ' rowid '* FROM ' CONFIG' DREBE RP 'unit' + SEC' 7 Control.LUR.AttachDetach 0 0 1 8 Control.LUR.FailedRegistration.Mes... Your handset is ... 0 0 9 Control.LUR.FailedRegistration.Sho... 1000 0 0 0 10 Control.LUR.NormalRegistration.M... 0 ORDER BY 'rowid' ASC); SELECT 'rowid',* FROM 'CONFIG' ORDER BY 'rowid' ASC LIMIT 0, 50000; < 1 - 12 of 222 > Go to: Plot SQL Log 😨 · 🖳 10

0x04 刷入固件

用 osmocon 程序将 trx.compalram.bin 刷入手机

命令 \$ sudo /dev/ttyUSB0 ./osmocon -р -*m* c123xor ../../target/firmware/board/compal_e88/trx.compalram.bin 应用程序 ▼ 位置 ▼ ^{\$}-终端 ▼ - 15 : 05 × ⊕) ⊕ -.... zh 🔻 root@h4ckOne: /opt/osmocom-bb2/src/host/osmoco 0 0 0 ion 2.0 root hub ated Products, Inc. CP210x UART Bridge / myAVR mySmartUSB light Virtual USB Hub Virtual Mouse Fion 1.1 root hub M# /osmocon -p /dev/ttyUSBO -m c123xor ../../target/firmware/board/compal_e88/trx.compalram.bin f6 02 00 4096 bytes (4096/62887) 4096 bytes (8192/62887) 🙀 🔚 📷 4- 🙃

0x05 开始执行

到 OpenBTS/apps 目录下,将 transceiver 重命名为 transceiver.bak 新建脚本文件

transceiver 内容如下

#!/bin/bash exec <your path to osmocom-bb>/src/host/layer23/src/transceiver/transceiver <ARFCN>

<your path to osmocom-bb>替换成你自己的路径, <ARFCN>替换成附近信号最强的

ARFCN 号

By:K1two2

摩托罗拉 C118 基于 Osmocom-BB& OpenBTS 搭建小型短信基站



赋予执行权限

chmod +x transceiver

然后开 4 个终端窗口分别执行

\$ cd openbts/trunk/apps

\$./OpenBTS



\$ cd subscriberRegistry/trunk

\$./sipauthserve(开启注册服务)

摩托罗拉 C118 基于 Osmocom-BB&OpenBTS 搭建小型短信基站

应用程序 ▼ 位置 ▼	- 15 : 10	_1 →≌ zh -	× × ∞) ⊙ -
root@h4ckOne: /opt/osmocom=bb2/src/host/osmocon	root@h4ckOne: /opt/OpenBTS-	-P2.8/openbts/trunk/apps	- 0 ×
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)	文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)		
Battery capacity is 100% Battery range is 31993999 mV. Battery full at 468 LSB . full at 585 LSB Charging at 239 LSB (204 mA). BCICTL2=0x3ff battery.info.flags=0x00000000 batt.compal_e88_chg_state=0 BAT-ADC: 664 6 0 0 1023 1023 1023 583 Charger at 51 mV. Battery at 4539 mV. Charging at 0 mA. Battery cange is 31993999 mV. Battery rull at 468 LSB full at 585 LSB Charging at 239 LSB (204 mA). BCICTL2=0x3ff battery.flags=0x00000000	<pre><011> trx.c: 512 TRX Data 2152407: 0: 0: 618bf <0011> trx.c: 512 TRX Data 2152408: 0: 0: 278f2 <0011> trx.c: 512 TRX Data 2152408: 0: 0: 3516 <0011> trx.c: 512 TRX Data 2152475: 0: 0: a606 <0011> trx.c: 512 TRX Data 2152458: 0: 0: 118a4 <0011> trx.c: 512 TRX Data 2152459: 0: 0: 40304 <0011> trx.c: 512 TRX Data 2152459: 0: 0: 40304 <0011> trx.c: 512 TRX Data 2152459: 0: 0: 40304 <0011> trx.c: 512 TRX Data 2152458: 0: 0: 618af <0011> trx.c: 512 TRX Data 2152458: 0: 0: 618af <0011> trx.c: 512 TRX Data 2152508: 0: 0: 63616 <0011> trx.c: 512 TRX Data 2152508: 0: 0: 63616 <0011> trx.c: 512 TRX Data 2152510: 0: 0: 0: 27874 <0011> trx.c: 512 TRX Data 2152510: 0: 0: 0: 27874 <0011> trx.c: 512 TRX Data 2152510: 0: 0: 0: 27874 <0011> trx.c: 512 TRX Data 2152559: 0: 0: a8415 <0011> trx.c: 512 TRX Data 2152569: 0: 0: 28294 <0011> trx.c: 512 TRX Data 2152569: 0: 0: a8415 <0011> trx.c: 512 TRX Data 2152569: 0: 0: a8415</pre>	bb007ffc0f38b52440fa87c70 ff0c4fb906604be6288b10310 cf902bf6a32f311c21810 48a43a104e000a010a56004e0 388440802e000a14281e80600 4a4020060740005c011800020 20420400a65ea138010216000 4272b9d407e30b44143d79a20 bb007ffc0f38b52440fa87c70 5f0c41b906604be6288b10310 c5f9010e6fe6a32f311c21810 51a314dc060907c410b055130 400ea1647e8ab7e003df5460	
root@h4ckOne: /opt/OpenBTS-P2.8/subscriberRegistry/trunk	 — — —	c70181285f07a0b57d681fe70	
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)	TRX Data 2152610: 0: 0: 816a8	0aa0221546952a45085401000	
<pre>root@MckOne: / opt//UpenBIS-P2.8/subscriberRegistry/trunk# ./sipau ALERT 3072866048 15:09:48.6 sipauthserve.cpp:277:main: ./sipauth ng EMERG 3072866048 15:09:48.6 ./SubscriberRegistry.cpp:173:init: / /sqlite3dir does not exist</pre>	thserve (re) starti TRX Data 2152612:0:0:14a01 serve (re) starti TRX Data 2152612:0:0:14a01 TRX Data 2152613:0:0:44214 var/lib/asterisk	22310244804803400424440 404481448700a10a010804aa0 20408540070a810001a212280	1
Broadcast message from systemd-journald@h4ck0ne (Mon 2016-06-13	15: 09: 48 CST):		
sipauthserve[2099]: EMERG 3072866048 15:09:48.6 ./SubscriberRegi t: /var/lib/asterisk/sqlite3dir does not exist	stry.cpp:173;ini		
Message from systopd@MckOhe at Jun 13 15:09:48 sipauthserve: EMERG 3072866044 IS:09:48.6 ./SubscriberRegistry. ar/lib/asterisk/sqlite3dir does not exist	cpp:173:init: /v		
\$ cd smqueue/trunk/smqueue/			
\$./smqueue(开启短信功能)			

应用程序▼ 位置▼	^{\$} -终端 ▼	- 15 : 10	1	12	zh 🔻	1 3	x =(0))	، گ
	root@h4ckOne: /opt/osmocom-bb2/src/host/osmocon	root@h4ckOne: /opt/OpenBTS-P2.8/openbt	:s/trunk/a	apps		Θ		
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)	文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)						
Broadcast message smqueue[2120]: EME //Lib/asterisk/sqli LOST 1877! LOST 1873! BAT-ADC: 687 7 Charger at Battery at Charging a Battery Ca Battery for Battery for	<pre>from systemd-journald@h4ckOne (Mon 2016-06-13 RG 3074483968 15:10:26.8 SubscriberRegistry.c te3dir does not exist 0 0 1023 1023 1023 582 60 mV. 4696 mV. 4696 mV. t 0 mA. pacity is 100% nge is 31993999 mV. U at 488 LSB full at 585 LSB t 239 LSB (204 mA). 3ff</pre>	$\begin{array}{llllllllllllllllllllllllllllllllllll$	042854 100a10a 10a8100 1000a01 1000a11 1000a11 140005c 15ea138 1e30b44 138b524 1604be6 1664be7 1664be7 1664be7 1664be7 1664be6 1664be7 1664	8042a 01080 01a21 0a560 281e8 01180 01021 143d7 40fa8 288b1 311c2 10b05 003df	4480 4aa0 2280 0600 0020 6000 9a20 7c70 0310 1810 5130 5460			
batterv-in	fo, flags=0x00000000 act@b4ckOpc:/opt/OpcpBTS=P2.8/cubscriberPagista/frupl	<0011> try_c: 512 TBY_Data_2160517* 0* 0* 042 ± 958b02511cf root@h4ckOne: /opt/OpenBTS=P2.8/smg	ueue/tru	nk/sm	8680 aueue		0	
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)	文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)			1			
ng Battery at EMERG 3072866048 19 /sqlite3dir does no	1999 ov 1993 86 / SubscriberRegistry.cpp:173:init: / t exist = 1995 fom systemd-journald@AdckOne (Mon 2016-06-13)	102 Poot@AckOng: /opt/OpenBTS-P2.8/smqueue/trunk/smqu Var/ALERT.9074483968 15:10:26:8 smqueue.cpp:2651:mail Smqueue Logs to syslogd facility UCAL7. So there EMERG 3074483968 15:10:26.8 SubscriberRegistry.cp 15; holita3dir does not exist	ieue# . n: smqu e's not op: 173:	/smqu eue (much init:	re) st to s / var	artinç ee hei /lib/a) re aster:	isk/s
sipauthserve[2099]: t: /var/lib/asteris	EMERG 3072866048 15:09:48.6 ./SubscriberRegi k/sqlite3dir does not exist	lstry Message from syslogd@h4ckOne at Jun 13 15:10:26 . smqueue: EMERG 3074483968 15:10:26.8 Subscriberf asterisk/sqlite3dir does not exist	 Registr	у. срр				/lib/
Message from syslog sipauthserve: EMEF ar/lib/asterisk/sql	jd@n4ck0ne at Jun 13 15:09:48 ∖G 3072866048 15:09:48.6 ./SubscriberRegistry. .ite3dir does not exist	Broadcast message from systemd-journald@h4ckOne (cpp: "Picture / smqueue[2120]: EMERG 3074483968 15:10:26.8 Subsci /lib/asterisk/sqlite3dir does not exist	Mon 20 riberRe	16-06 gistr	- 13 1 y. cpp	5: 10: 2 : 173: :		T): /var
Message from syslog smqueue: EMERG 307 asterisk/sqlite3dir	dd@n4ckOne at Jun 13 15:10:26 4483968 15:10:26.8 Subscriber∰is							

\$ cd openbts/trunk/apps

\$./OpenBTSCLI(打开 OpenBTS 控制台)

摩托罗拉 C118 基于 Osmocom-BB& OpenBTS 搭建小型短信基站

应用程序▼ 位置▼ ³ ─终端▼	— 15 : 15	1 💕 zh ∓ 💉 🕬 🕛 ∓
root@h4ckOne: /opt/osmocom=bb2	2/src/host/osmocon root@h4ckOne: /opt	:/OpenBTS-P2.8/openbts/trunk/apps - 🗉 🗴
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)	文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 青	将助(H)
Battery capacity is 100% Battery range is 31993999 mV. Battery full at 468 LSB full at 585 Charning at 239 LSB (204 mA)	 <0011> trx. c: 512 TRX Data 2220186: 0 <0011> trx. c: 512 TRX Data 2220187: 0 <0011> trx. c: 512 TRX Data 2220188: 0 <0011> trx. c: 512 TRX Data 2220188: 0 <00112 trx. c: 190 TRX (IX Indication 	: 0: 118a4388440802e000a14281e80600 : 0: 40a944a4020060740005c011800020 : 0: 0425020420400a65ea138010216000 _ 2220185
BCICTL2=0x3ff	root@h4ckOne: /opt/OpenBTS-P2.8/openbts/trunk/app	os 😑 🐵)b44143d79a20
battery-info.flags=0x00000000 bat compal a% sha state=0 文件(E) 编	蝸(F) 杏看(V) 搜索(S) 终端(T) 帮助(H)	052440fa87c70
BAT-ADC: 665 9 0 0 1023 1023 102 mot Ch4ck	One: / ont/ OnenBTS-P2_8/ openbts/trunk/apps#_/OpenBTSC	12 a51 bcc51 901 0 e61 a32 f 311 c 21810
Charger at 77 mV. OpenBTS C Battery at 4546 mV. OpenBTS C Charging at 0 mA. Licensed I Battery capacity is 00% Includes Battery range is 3199. 3999 m(command sy Battery full at 468 LSB fursponse i Charging at 239 LSB (204 mA). Remote In BCICTL2=0X3ff batterv.info.flags=0x000000000 "help".t	<pre>mand Line Interface (CLI) utility 2012, 2013 Range Networks, Inc. under GPLy2 libreadline, GPLy2 cocket path is /var/in/command socket bound to /tmp/OpenBTS.console.2151.575e5d37 serface Ready. 0 see .commands,</pre>	1220236 07-6410b055130 05-8842551821446000 07-6410b055130 05-28254600en1567745 97e0003475460 05-04251950012151140 7f15001178680 05-055460178680 4055746817470 05-055460178680 4055746817470 05-055460178680 4055746817470 05-051612457 4055746817470 05-051612457 2854804244480 05-0141464204 2854804244480 05-0141464204 104010864aa0
root@h4ckOne: /opt/OpenE "version	for version information, C * root@h4ckOne: /	pt/OpenBTS+P2.8/smqu e/trunk/smqueue - · · · ·
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助("quit" t	o exit console interface	(7) 招助(H)
Battery at 4703 mV. Charging at 0 mA. Battery capacity is 100%	/ opt/OpenBIS-P2.8/ 968 15:10:26.8 smg to syslogd facilit 968 15:10:26.8 Smi	emqueue/trunk/smque.##!/smqueue/ Meue.cpp:2651main/smqueue/(re)starting p.LOCAL7, so there notimuch to'see here scriberRegistry.cpp173:init: /var/lib/asterisk/s
<pre>root@h4ckOne:/opt/OpenBTS-P2.8/subscriperRegist</pre>		
ALERI 3072866048 15:09:48.6 sipauthserve.cpp:27.		Jun 13 15:10:26
EMERG 3072866048 15:09:48.6 ./SubscriberRegistry /sqlite3dir does not exist		U: 26.8 SubscriberRe istry.cpp:173:init: /var/lib/ Tist
Broadcast message from systemd-journal <u>d@h4-kOne</u>	(Mon 2016-06-13 15:09:48 CST):	journald@h4ck0ne (10 n 2016-06-13 15:10:26 CST):
sipauthserve[2099]: EMERG 3072866048 15:09:48.6 t: /var/lib/asterisk/sqlite3dir does not exist	./SubscriberRegistry.cpp:173:ini : EMERG 3074483968 /Lib/asteri /sqlite3dir does n	15:10:26.8 SubscriberRegistry.cpp:173:init: /var not exist
Message from syslogd@n4ck0ne at Jun 13 15:09:48	😭 🛄 🔳 🗐 🥃 🙌 🖻 📖 🗄	

如果一切运行顺利打开手机进入设置-移动网络-网络运营商即可看到我们创建的基站

15:14 🗖	0 % 🤶 📶 🗖 78
〈 网络运营商	0
运营商	
搜索网络 搜索所有可用网络	
自动 自动选择首选网络	
可用网络	
中国移动 4G 当前网络	
中国移动 3G 可用网络	
中国移动 2G 可用网络	
中国联通 4G 已禁止网络	
00101 2G 可用网络	
中国联通 2G 已禁止网络	

在 OpenBTSCLI 的终端窗口可以输入 help 查看命令帮助

输入 tmsis 可以查看当前基站用户的 IMSI

输入 sendsms IMSI 电话 短信内容 即可发送任意显示号码的短信

By:K1two2

摩托罗拉 C118 基于 Osmocom-BB&OpenBTS 搭建小型短信基站



0x06 结语

一入 GSM 深似海,作者不是学通信的,只是业余爱好,第一次写文章,文中不免纰漏和不 妥之处。有任何建议或意见欢迎留言!

0x07 参考资料

http://osmocom.org/projects/baseband/wiki/Transceiver

https://wush.net/trac/rangepublic/wiki/BuildInstallRun

https://wush.net/trac/rangepublic/wiki/DebOpenBTS

http://bb.osmocom.org/trac/blog/PHD2012

http://www.h-online.com/open/news/item/29C3-Budget-mobile-turns-into-GSM-

base-station-1775204.html

http://blog.0x7678.com/2014/03/osmocombbopenbtsgsmcalypso.html