CORE SECURITY

Introducción a la ingeniería reversa de sistemas embebidos

Joaquín Rodríguez Varela
Senior Security Researcher
@insegar

18 de Mayo, 2016.

Temario

- **¿Qué son los sistemas embebidos?**
- **Hardware**
  - Microcontroladores, Microprocesadores y SoC (System on Chip)
  - Arquitecturas (ARM, MIPS, SPARC, x86)
- **Software**
  - Firmware/System Software
  - Sistemas Linux embebidos
    - Estructura del firmware
    - File System
  - ¿Cómo obtenerlo?
    - La Web
    - Hardware (UART, JTAG, Memoria Flash)
- **Análisis**
  - Estático
    - Herramientas
  - Dinámico
    - Herramientas (+ DEMO)
    - Emulación (+ DEMO)
- **Conclusión**

¿Qué son los sistemas embebidos?

¿Qué son los sistemas embebidos?

CORE SECURITY

¿Qué son los sistemas embebidos?

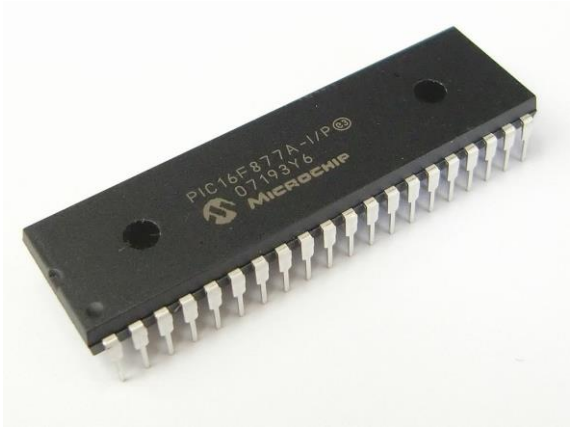
CORE SECURITY

Hardware

Microcontroladores, Microprocesadores y SoC

Microcontrolador (µC, UC o MCU):

- Circuito integrado programable
- Ejecuta órdenes grabadas en memoria
- Compuesto por bloques funcionales con tareas específicas
- Incluye CPU, memoria y periféricos I/O
- Utilizados normalmente en sistemas embebidos

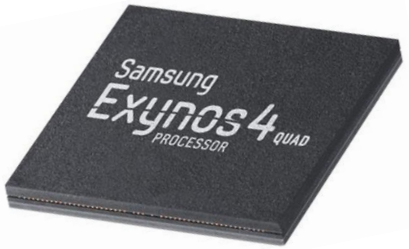


CORE SECURITY

Microcontroladores, Microprocesadores y SoC

Microprocesador:

- Circuito integrado central más complejo de un sistema
- Ejecuta instrucciones programadas en lenguaje de bajo nivel, realizando operaciones aritméticas y lógicas simples, lógicas binarias y accesos a memoria.
- Es un dispositivo multipropósito programable que recibe información digital como input, la procesa de acuerdo a instrucciones guardadas en memoria y provee resultados como outputs.



CORE SECURITY

Arquitecturas (ARM, MIPS, SPARC, x86)

Software

Firmware/System Software

Firmware:

- Conjunto de instrucciones esenciales que contienen y controlan las acciones específicas de los dispositivos.
- Se aloja en la memoria no volátil del dispositivo, como es la ROM, EPROM, o en una memoria flash.
- Actualmente incorporan interfaces sencillas de configuración del sistema, ya sea utilizando comandos o por medio de una interfaz web.

Sistemas Linux embebidos

Estructura del firmware:

- Firmware header (Magic Number, ej. TRXv1, TRXv2, BIN, etc.)
- Bootloader comprimido
- Bootloader de segunda etapa (Lilo, GRUB, etc.)
- Sistema Operativo comprimido
- Root File System

Sistemas Linux embebidos

Linux File Systems:

- ext2, ext3, ext4
- SquashFS (LZMA, LZO, LZMA2, LZ4)
- UBIFS (Unsorted Block Image File System)
- JFFS2 (Journalling Flash File System version) - OpenWrt
- YAFFS (Yet Another Flash File System)

¿Cómo obtenerlo?

La web:

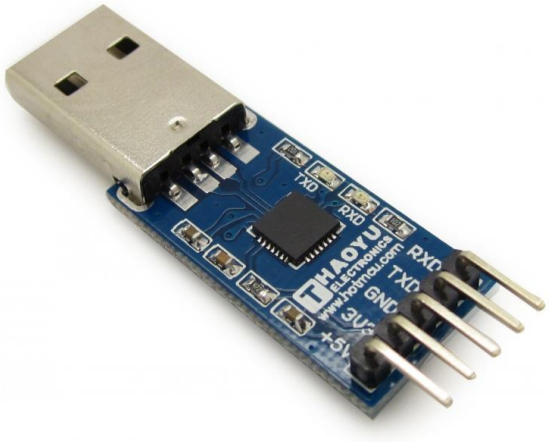
- Descarga sitio oficial
- ShodanHQ
- WorldOfVNC (nuevo) www.worldofvnc.net
  "On March 31st 2016, I scanned the whole internet for VNC servers, and took a screenshot of those without a password."
- Compra Online (nuevo o usado)

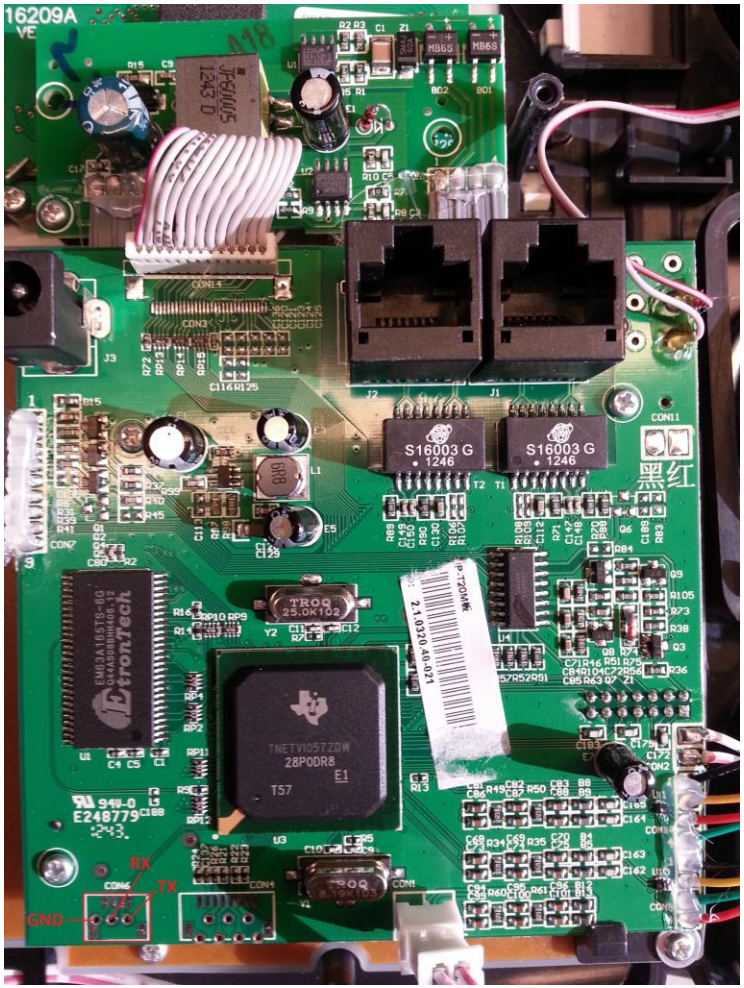
¿Cómo obtenerlo?

Hardware:

- UART

```
#cu -l /dev/ttyUSB0 -s 19200
```



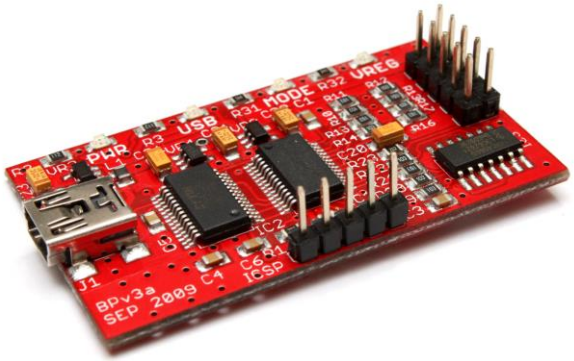


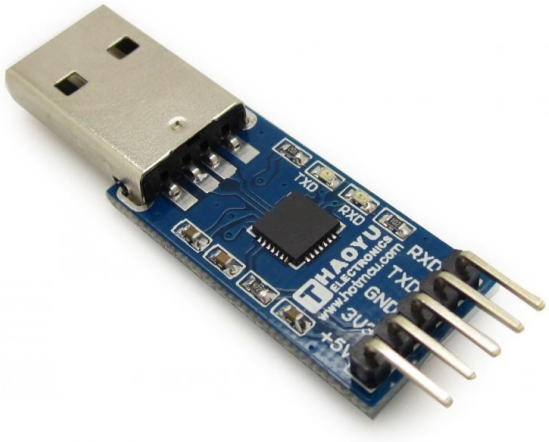
CORE SECURITY

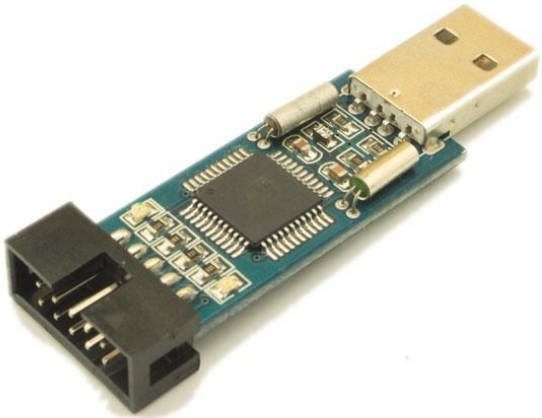
¿Cómo obtenerlo?

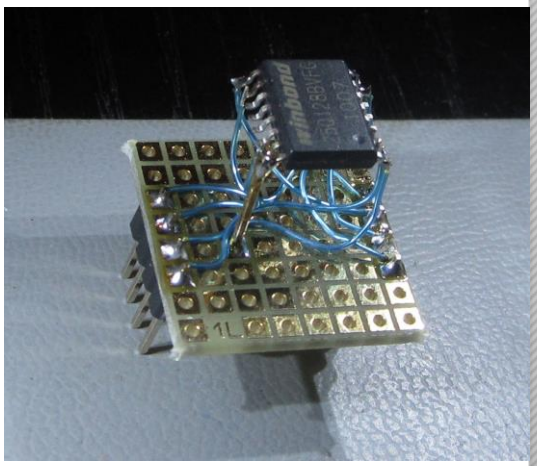
Hardware:

- UART
- JTAG (BusPirate)
- Dump o extracción de memoria flash









CORE SECURITY

Análisis estático

Herramientas:

- Binwalk (https://github.com/devttys0/binwalk/releases/tag/v2.0.1)
- dd
- Firmware ModKit (https://code.google.com/p/firmware-mod-kit/)
- HexDump
- IDA Pro (https://www.hex-rays.com/products/ida/)
- Radare2 (https://github.com/radare/radare2)

CORE SECURITY

Análisis dinámico

Herramientas:

- QEMU (http://wiki.qemu.org/Download)
- strace
- gdb (http://www.gnu.org/software/gdb/)
- lsof
- tcpdump

DEMO #1

MOXA®

HD, rugged, day-and-night box type IP cameras

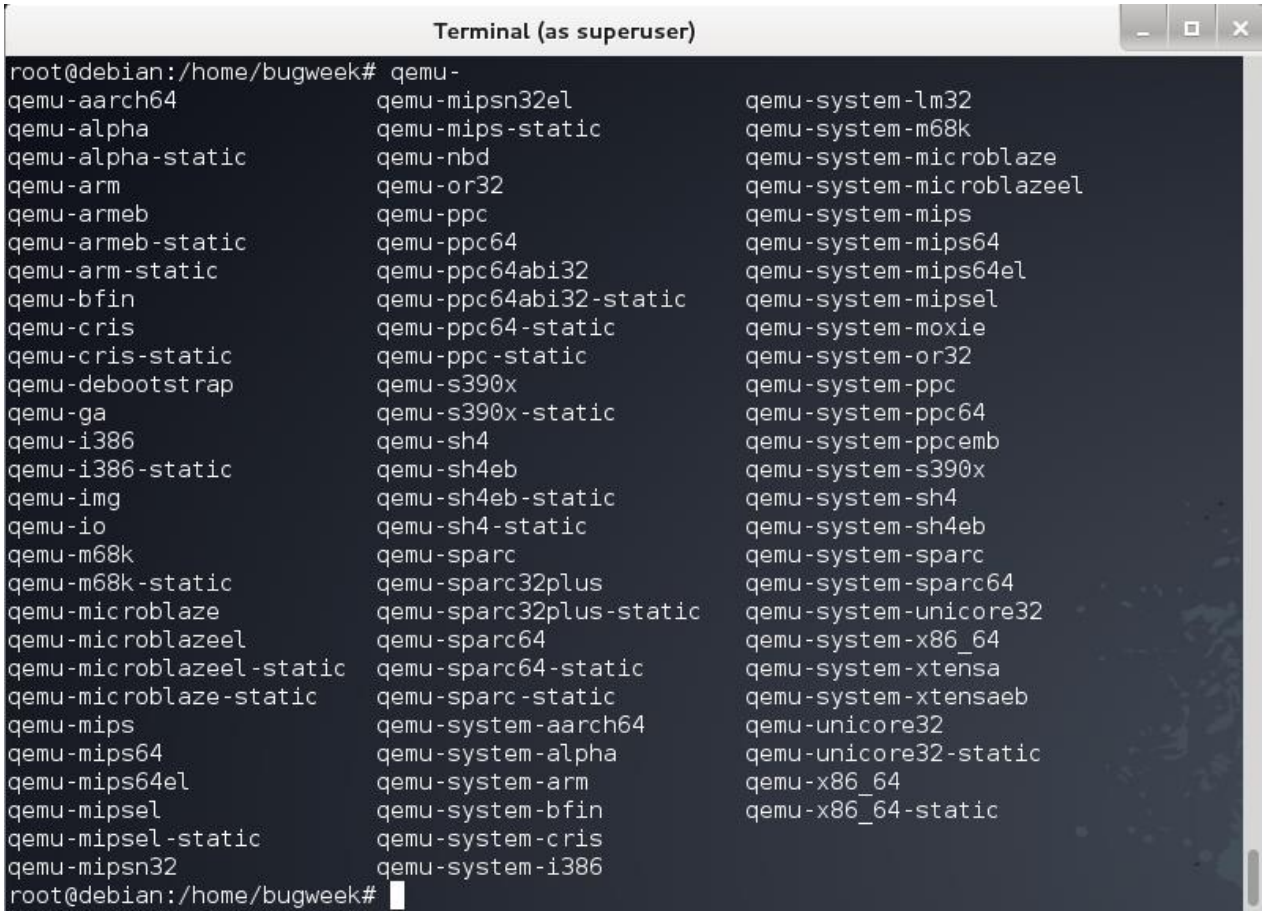
VPort 36-1MP Series

CORE SECURITY

Análisis dinámico

Emulación:

- QEMU
- chroot
- strace



CORE SECURITY

DEMO #2

Advantech EKI-6340

CVE-2014-8387

http://www.coresecurity.com/advisories/advantech-eki-6340-command-injection

Conclusión

```
0000a820  6d 65 6f 75 74 0a 00 00  52 65 63 65 69 76 65 20  |meout...Receive |
0000a830  46 69 6c 65 20 73 69 7a  65 3a 30 78 25 38 78 28  |File size:0x%8x(|
0000a840  25 64 29 0a 00 00 00 00  49 6d 61 67 65 20 4f 4b  |%d).....Image OK|
0000a850  21 0a 00 00 43 61 6c 6c  20 53 79 73 74 65 6d 20  |!...Call System |
0000a860  52 65 73 65 74 20 21 0a  00 00 00 00 3c 73 63 72  |Reset !.....<scr|
0000a870  69 70 74 20 6c 61 6e 67  75 61 67 65 3d 27 6a 61  |ipt language='ja|
0000a880  76 61 73 63 72 69 70 74  27 3e 3c 21 2d 2d 20 68  |vascript'><!-- h|
0000a890  69 64 65 00 3c 2f 68 65  61 64 3e 3c 62 6f 64 79  |ide.</head><body|
0000a8a0  3e 3c 62 6c 6f 63 6b 71  75 6f 74 65 20 63 6c 61  |><blockquote cla|
0000a8b0  73 73 3d 27 73 74 79 6c  65 31 27 3e 49 6e 76 61  |ss='style1'>Inva|
0000a8c0  6c 69 64 20 66 69 6c 65  2e 3c 2f 62 6c 6f 63 6b  |lid file.</block|
0000a8d0  71 75 6f 74 65 3e 3c 2f  62 6f 64 79 3e 3c 2f 68  |quote></body></h|
0000a8e0  74 6d 6c 3e 00 00 00 00  3c 73 63 72 69 70 74 20  |tml>....<script |
0000a8f0  6c 61 6e 67 75 61 67 65  3d 27 4a 61 76 61 53 63  |language='JavaSc|
0000a900  72 69 70 74 27 20 74 79  70 65 3d 27 74 65 78 74  |ript' type='text|
0000a910  2f 6a 61 76 61 73 63 72  69 70 74 27 3e 00 00 00  |/javascript'>...|
0000a920  3c 21 2d 2d 20 53 74 61  72 74 20 53 63 72 69 70  |<!-- Start Scrip|
0000a930  74 09 00 00 76 61 72 20  6d 61 78 63 68 61 72 73  |t...var maxchars|
0000a940  20 3d 20 35 30 3b 76 61  72 20 63 68 61 72 63 6f  | = 50;var charco|
0000a950  75 6e 74 20 3d 20 30 3b  00 00 00 00 66 75 6e 63  |unt = 0;....func|
0000a960  74 69 6f 6e 20 70 70 70  28 29 7b 76 61 72 20 63  |tion ppp(){var c|
0000a970  66 20 3d 20 64 6f 63 75  6d 65 6e 74 2e 66 6f 72  |f = document.for|
0000a980  6d 73 5b 30 5d 3b 69 66  20 28 63 68 61 72 63 6f  |ms[0];if (charco|
0000a990  75 6e 74 20 3c 20 6d 61  78 63 68 61 72 73 29 7b  |unt < maxchars){|
```

CORE SECURITY

Muchas gracias.

¿Preguntas?