David M. N. Bryan, Trustwave SpiderLabs

I pwned your router. Oops.

- @_videoman_
- dbryan@trustwave.com
- dave@drstrangelove.net

David M N Bryan

- Trustwave SpiderLabs
- Senior Security Consultant and Penetration Tester
- Hacker Space President
- Electronics
- Hacking
- Metal working, etc....

Review of Embedded Security

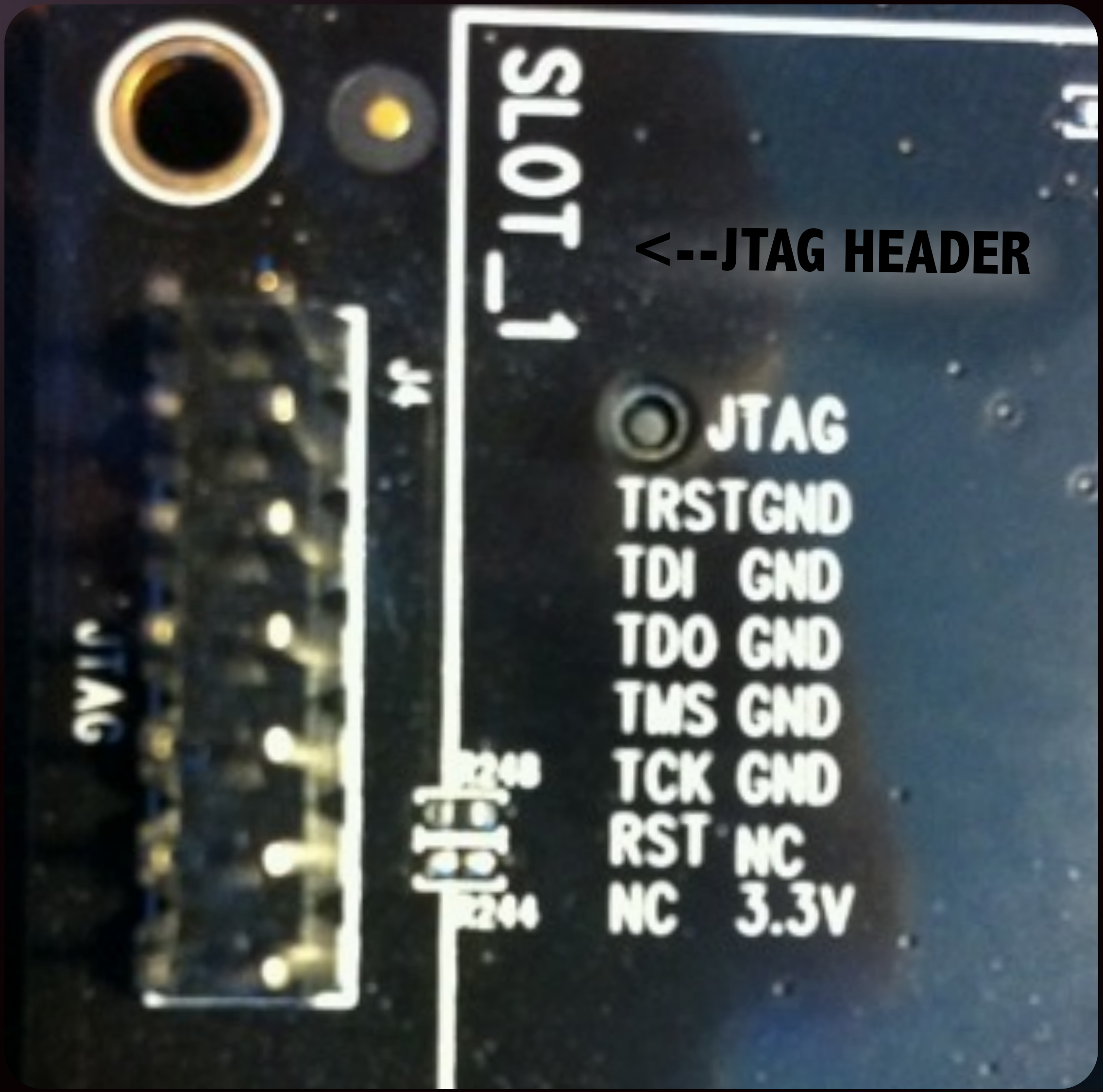
- Security is not the goal
- Small memory foot print
- Low cost hardware
- Little or no disk storage
- Cost....

Remember the 1990's

- The dream is alive in Embedded Hardware
- Sleep till 11
- Based on BusyBox
- Anyone here remember having to disable services? System hardening?
- inetd.conf
- SSH config - disable root login

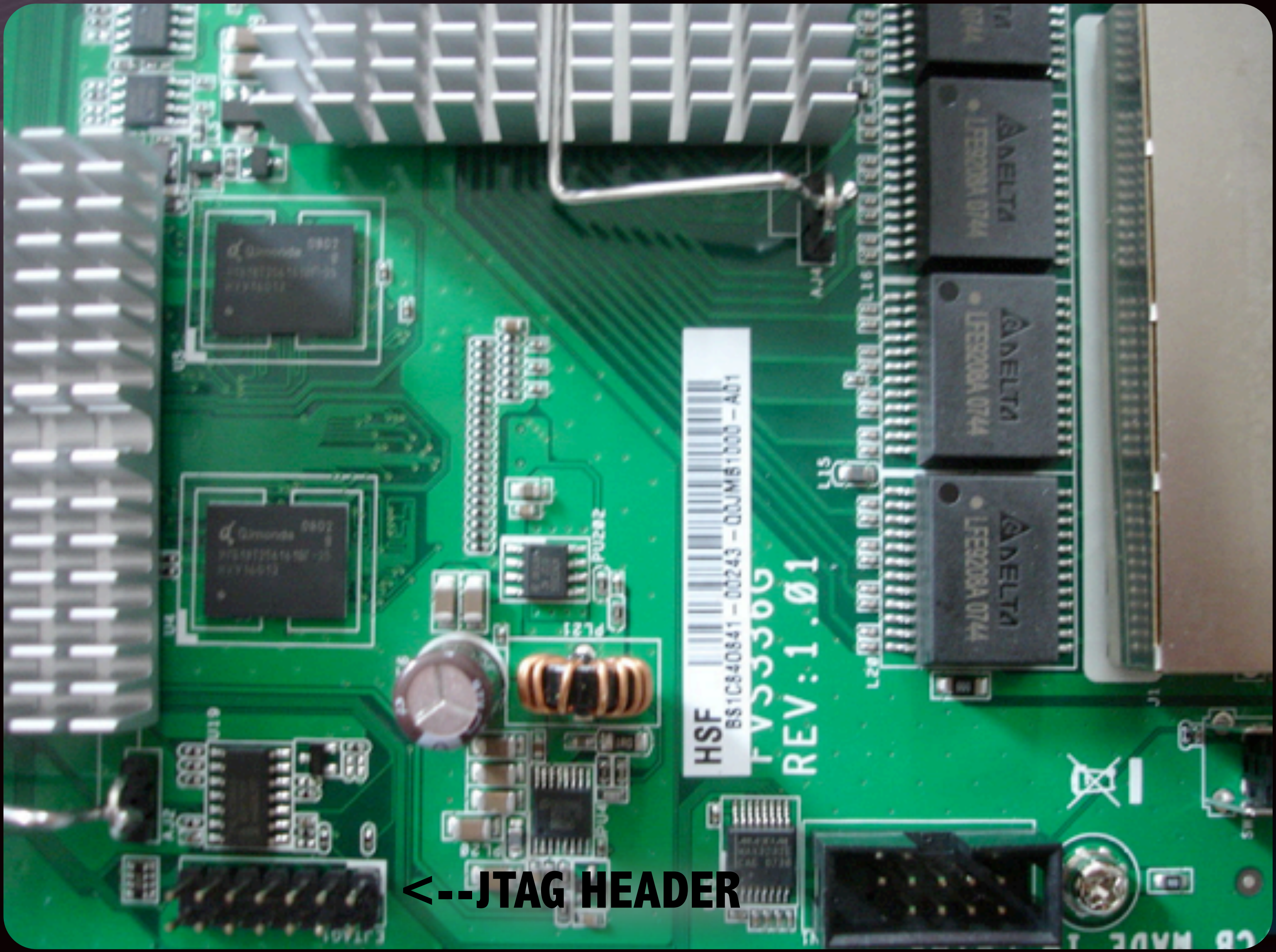
JTAG is our friend

- Joint Test Action Group - JTAG
- Allows in-circuit debugging
- Flash firmware
- Read/Modify memory registers
- Halt
- Reset
- OpenOCD



<--JTAG HEADER

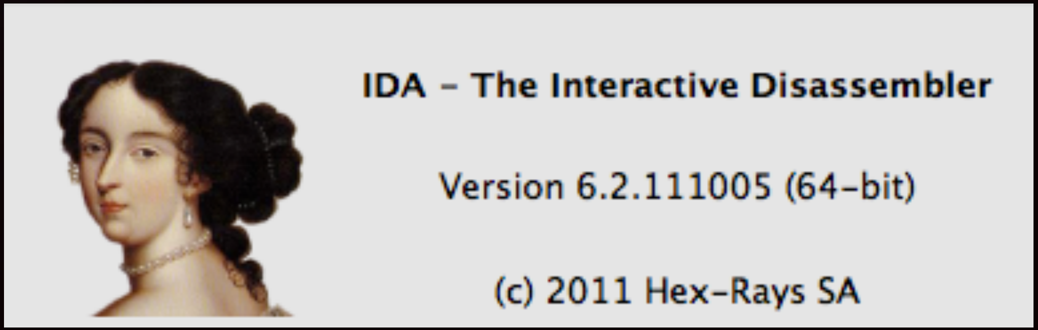
SLOT_1
J4
JTAG
JTAG
TRST GND
TDI GND
TDO GND
TMS GND
TCK GND
RST NC
NC 3.3V
R248
R244



<--JTAG HEADER

IDA Pro

- Awesome!
- Decompiler tool
- Proximity View Rocks....



IDA – The Interactive Disassembler

Version 6.2.111005 (64-bit)

(c) 2011 Hex-Rays SA

Where did security go?

- No sudoers
- No shadow
- One user to rule them all
- Snmp, telnet, and ssh?
- Using the device to restrict network access, not the network
- BusyBox still?

What things could we get to?

- SNMP?
- SSH?
- TELNET?
- Webserver….

What to do to pwn?

- If only we could add an account
- We can list it's gateway up stream
- Crash the thing
- Get a root shell

Options for Root Shells…

- Option 1

  I can Haz Password Hashes, plz?

- Option 2

  STRCPY FTW!

Option 1 - I can Haz HASHES?

- Dump firmware - Either JTAG or BIN image
- Find the partitions – binwalk/hexedit/hexdump
- dd offset=x if=file.bin of=file.img count=50 bs=1
- mount virtual filesystems or grep
- grab password hashes
- Crack password with John The Ripper

Option 2 - STRCPY!

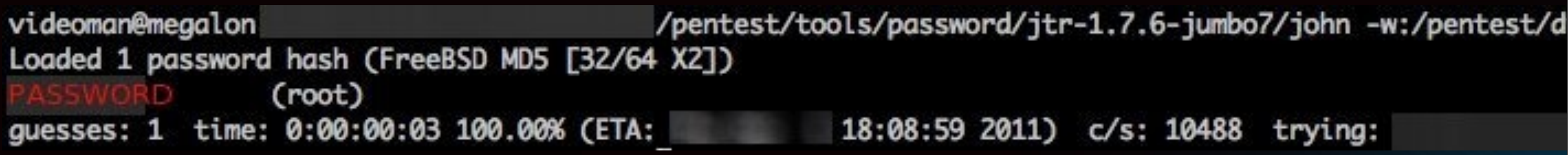
- Dump firmware
- Find and mount the partition
- Find web interface binaries
- Use IDA Pro on Binaries
- Reverse engineer and identify strcpy & mallocs

Option 2 - STRCPY! Continued...

- Grab raw data pusher (MSF and ARM binary in this case)
- Push that data onto C++ App

Option 1 - Hashes Exploit

- mount -o loop firmware.img /mnt
- cd /mnt/etc
- more passwd
- Crackme....

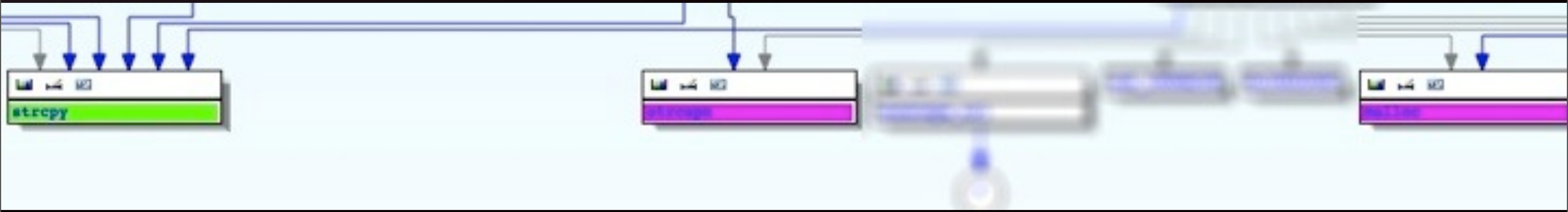


```
videoman@megalon [redacted] /pentest/tools/password/jtr-1.7.6-jumbo7/john -w:/pentest/d
Loaded 1 password hash (FreeBSD MD5 [32/64 X2])
PASSWORD         (root)
guesses: 1  time: 0:00:00:03 100.00% (ETA: [redacted] 18:08:59 2011)  c/s: 10488  trying: [redacted]
```

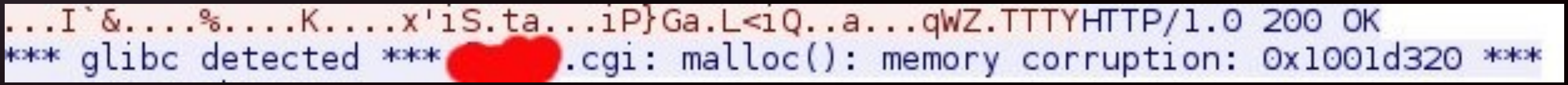
Option 2 - STRCPY Exploit

- Find vulnerable code on web service...
- Use MSF module linksys_apply_cgi.rb
- Appended shellcode payload from "Linux/MIPS - reboot() - 32 bytes"

Option 2 - STRCPY Exploit Continued...



Who needs strlcpy?



```
...I`&....%....K....x'iS.ta...iP}Ga.L<iQ..a...qWZ.TTTYHTTP/1.0 200 OK
*** glibc detected *** [redacted].cgi: malloc(): memory corruption: 0x1001d320 ***
```

- Watch app fail and dump core – entry point identified.
- Followed by a Backtrace and a Memory Map.
- Pwn'd

Option 3

- You didn’t mention option three.

  Modify the image and flash it via the JTAG interface

  That’s what it’s for..

- Time however… it’s kind of slow.

Trustwave SpiderLabs

DEMO TIME!

- Lets how the demo gods work with us.
  - JTAG Tools Demo (quick start)
  - Data finding demo
  - IDA Pro Demo

Review

- What could we do better
  - Sudoers
  - Separate accounts
  - Shadow file
  - No passwords, each system gets a key-pair or a trusted public key

Review

- What could we do better
  - Code review
  - Do not allow debug symbols to be pushed into prod
  - Assume that the system is owned

Conclusions

- Do security reviews of products internally before buying
- Don’t use shared passwords on client systems
- Code/hardware in the users hands is hardware/code you don’t really control
- Make things with security in mind not as an after thought
- Why can’t we run full OSes anymore on these things? Ditch Busybox?

Links

- http://en.wikipedia.org/wiki/Joint_Test_Action_Group
- https://dev.metasploit.com/redmine/projects/framework/repository/entry/modules/exploits/linux/http/linksys_apply_cgi.rb
- http://www.exploit-db.com/exploits/18227/

David M. N. Bryan, Trustwave SpiderLabs

I pwned your router. Oops.

- @_videoman_
- dbryan@trustwave.com
- dave@drstrangelove.net