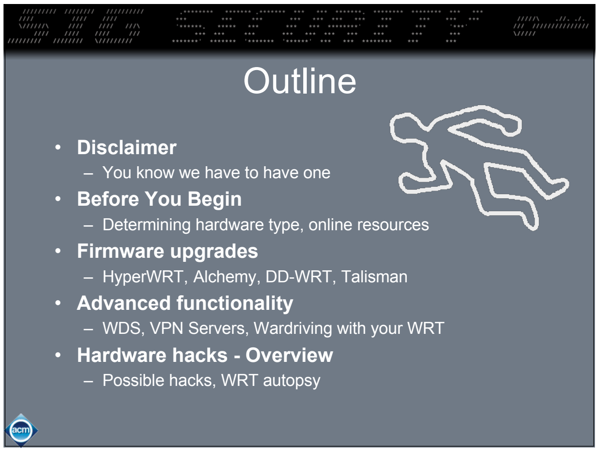
If You Bought It, You Might As Well ØwN It!

Hacking Your WRT into Complete Obedience

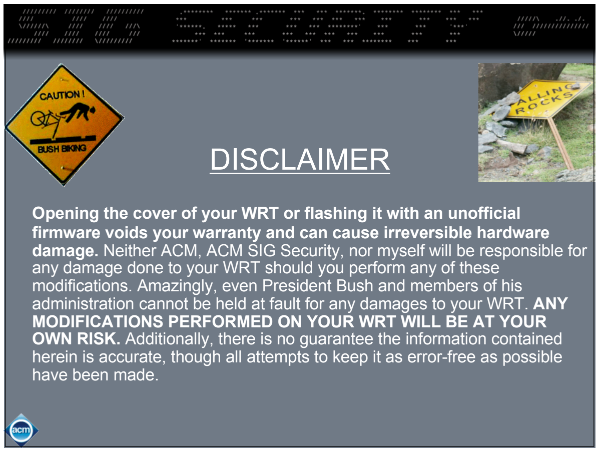
8 February 2006

Presented by William Atkins <wda8rd@umr.edu>



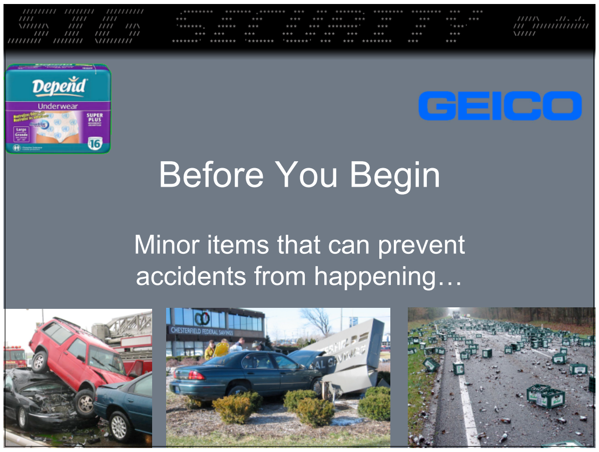
Outline

- **Disclaimer**
  - You know we have to have one
- **Before You Begin**
  - Determining hardware type, online resources
- **Firmware upgrades**
  - HyperWRT, Alchemy, DD-WRT, Talisman
- **Advanced functionality**
  - WDS, VPN Servers, Wardriving with your WRT
- **Hardware hacks - Overview**
  - Possible hacks, WRT autopsy



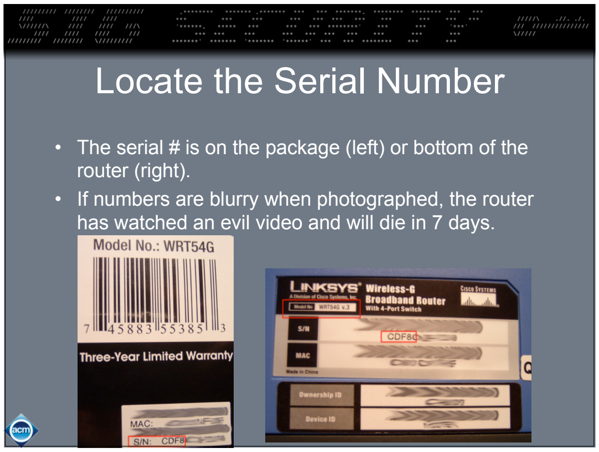
DISCLAIMER

Opening the cover of your WRT or flashing it with an unofficial firmware voids your warranty and can cause irreversible hardware damage. Neither ACM, ACM SIG Security, nor myself will be responsible for any damage done to your WRT should you perform any of these modifications. Amazingly, even President Bush and members of his administration cannot be held at fault for any damages to your WRT. **ANY MODIFICATIONS PERFORMED ON YOUR WRT WILL BE AT YOUR OWN RISK.** Additionally, there is no guarantee the information contained herein is accurate, though all attempts to keep it as error-free as possible have been made.



Before You Begin

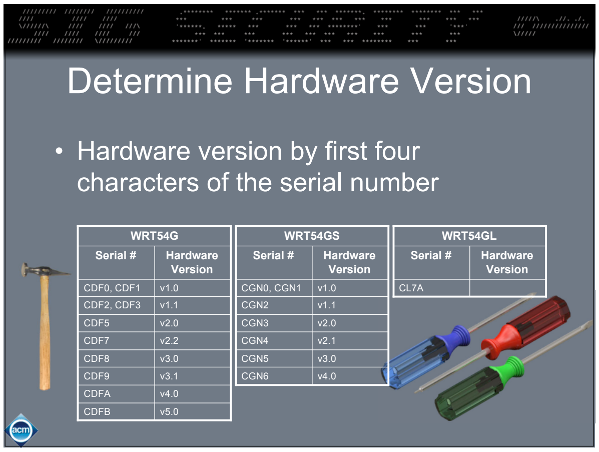
Minor items that can prevent accidents from happening…



Locate the Serial Number

- The serial # is on the package (left) or bottom of the router (right).
- If numbers are blurry when photographed, the router has watched an evil video and will die in 7 days.

Model No.: WRT54G
7 45883 55385 3
Three-Year Limited Warranty
MAC:
S/N: CDF8
LINKSYS Wireless-G Broadband Router With 4-Port Switch
S/N
CDF8
MAC
Ownership ID
Device ID



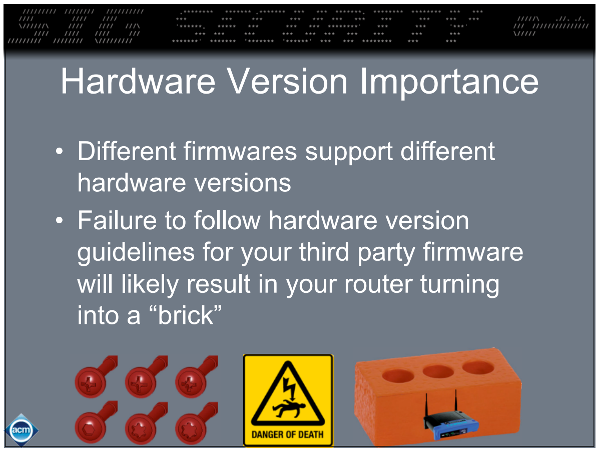
Determine Hardware Version

- Hardware version by first four characters of the serial number

WRT54G	
Serial #	Hardware Version
CDF0, CDF1	v1.0
CDF2, CDF3	v1.1
CDF5	v2.0
CDF7	v2.2
CDF8	v3.0
CDF9	v3.1
CDFA	v4.0
CDFB	v5.0

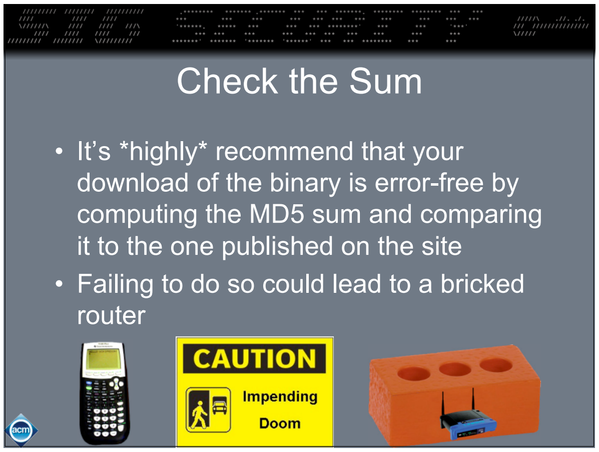
WRT54GS	
Serial #	Hardware Version
CGN0, CGN1	v1.0
CGN2	v1.1
CGN3	v2.0
CGN4	v2.1
CGN5	v3.0
CGN6	v4.0

WRT54GL	
Serial #	Hardware Version
CL7A	



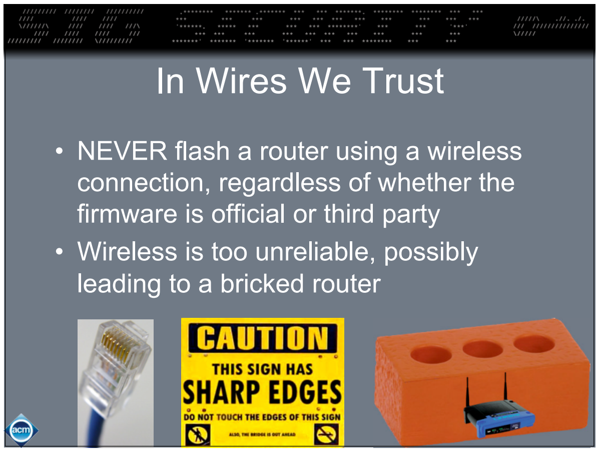
Hardware Version Importance

- Different firmwares support different hardware versions
- Failure to follow hardware version guidelines for your third party firmware will likely result in your router turning into a “brick”



Check the Sum

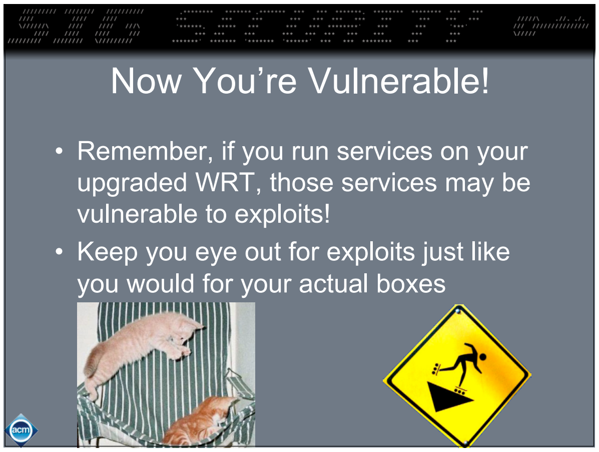
- It’s *highly* recommend that your download of the binary is error-free by computing the MD5 sum and comparing it to the one published on the site
- Failing to do so could lead to a bricked router



In Wires We Trust

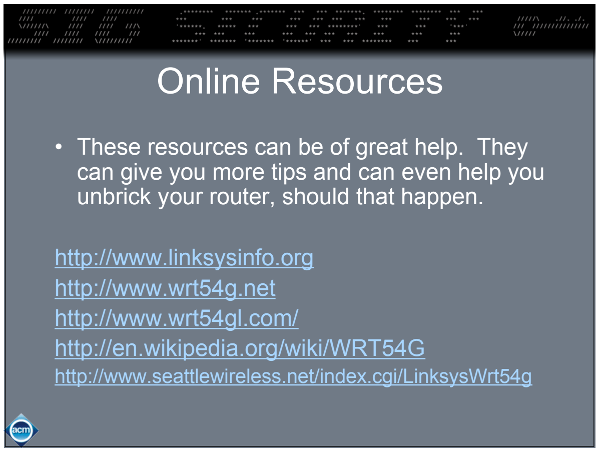
- NEVER flash a router using a wireless connection, regardless of whether the firmware is official or third party
- Wireless is too unreliable, possibly leading to a bricked router

CAUTION
THIS SIGN HAS
SHARP EDGES
DO NOT TOUCH THE EDGES OF THIS SIGN
ALSO, THE BRIDGE IS OUT AHEAD



Now You're Vulnerable!

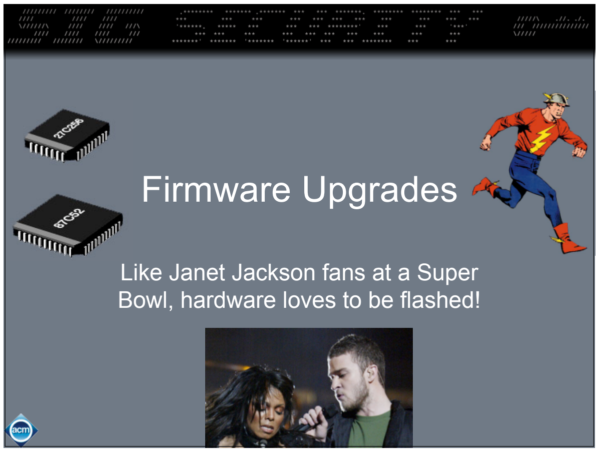
- Remember, if you run services on your upgraded WRT, those services may be vulnerable to exploits!
- Keep you eye out for exploits just like you would for your actual boxes



Online Resources

- These resources can be of great help. They can give you more tips and can even help you unbrick your router, should that happen.

http://www.linksysinfo.org
http://www.wrt54g.net
http://www.wrt54gl.com/
http://en.wikipedia.org/wiki/WRT54G
http://www.seattlewireless.net/index.cgi/LinksysWrt54g



Firmware Upgrades

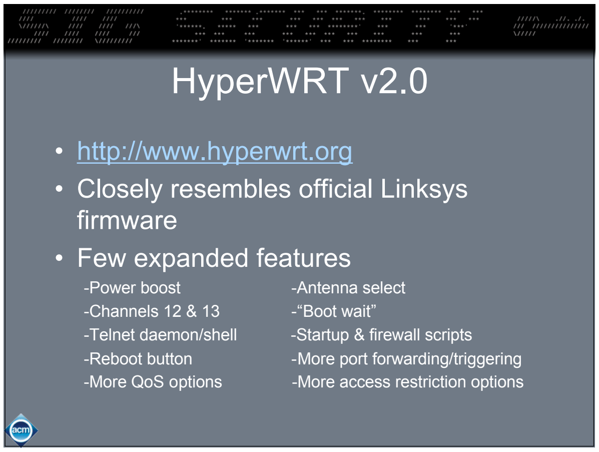
Like Janet Jackson fans at a Super Bowl, hardware loves to be flashed!

27C256
87C52

Candidate 1: HyperWRT

For those that want to add a little Mountain Dew to what they already have…

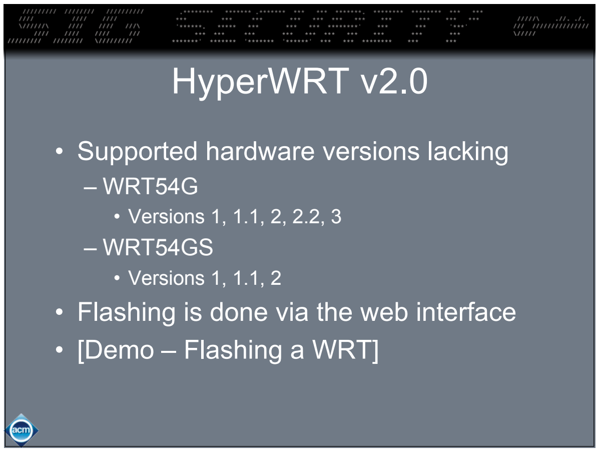
Mountain Dew



HyperWRT v2.0

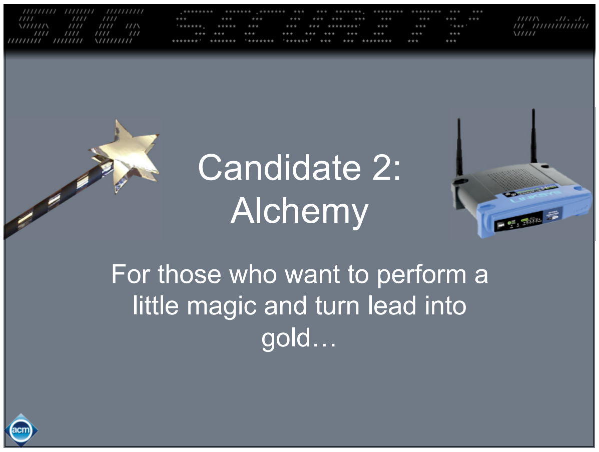
- http://www.hyperwrt.org
- Closely resembles official Linksys firmware
- Few expanded features

  -Power boost
  -Channels 12 & 13
  -Telnet daemon/shell
  -Reboot button
  -More QoS options
  -Antenna select
  -“Boot wait”
  -Startup & firewall scripts
  -More port forwarding/triggering
  -More access restriction options



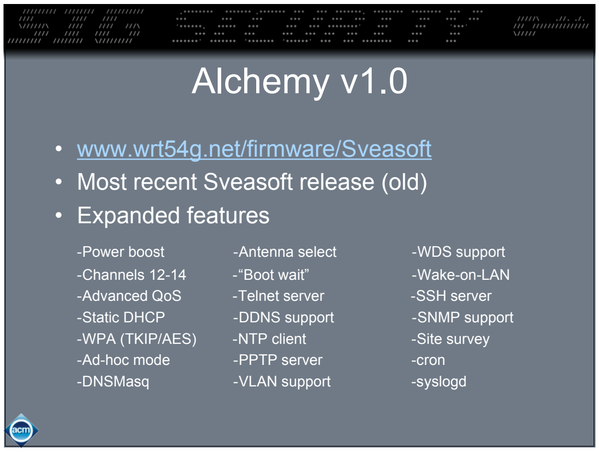
HyperWRT v2.0

- Supported hardware versions lacking
  - WRT54G
    - Versions 1, 1.1, 2, 2.2, 3
  - WRT54GS
    - Versions 1, 1.1, 2
- Flashing is done via the web interface
- [Demo – Flashing a WRT]



Candidate 2: Alchemy

For those who want to perform a little magic and turn lead into gold…



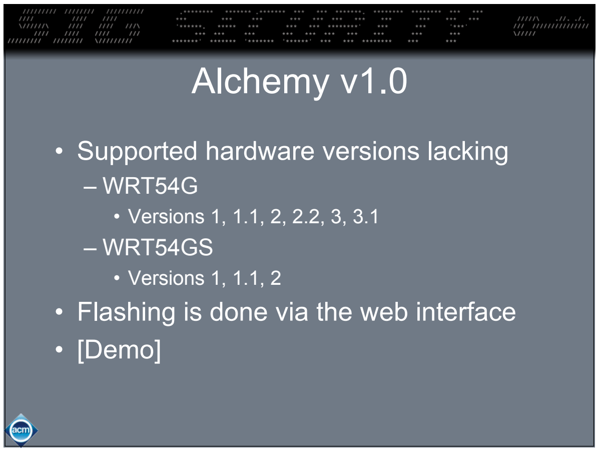
Alchemy v1.0

- www.wrt54g.net/firmware/Sveasoft
- Most recent Sveasoft release (old)
- Expanded features

-Power boost
-Channels 12-14
-Advanced QoS
-Static DHCP
-WPA (TKIP/AES)
-Ad-hoc mode
-DNSMasq

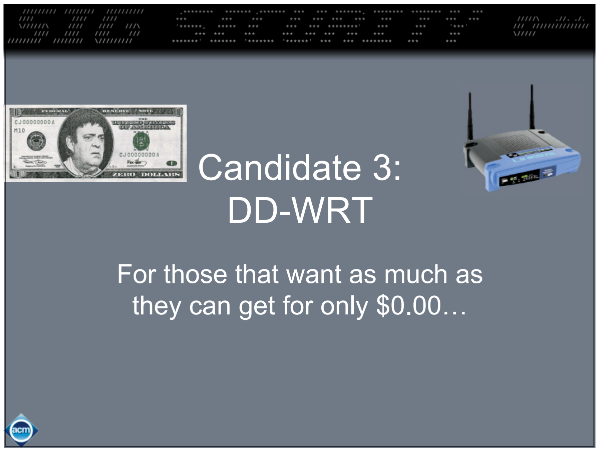
-Antenna select
-“Boot wait”
-Telnet server
-DDNS support
-NTP client
-PPTP server
-VLAN support

-WDS support
-Wake-on-LAN
-SSH server
-SNMP support
-Site survey
-cron
-syslogd



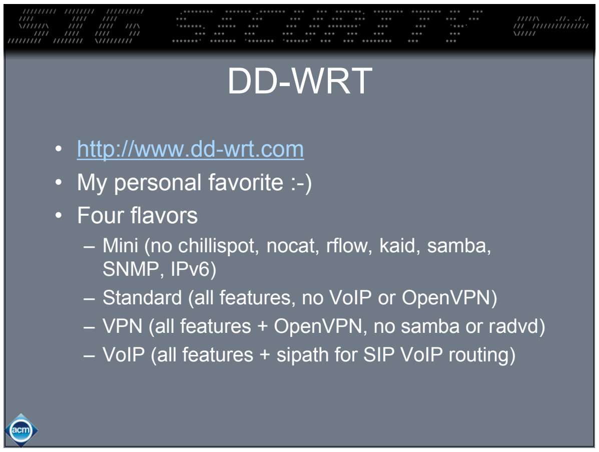
Alchemy v1.0

- Supported hardware versions lacking
  - WRT54G
    - Versions 1, 1.1, 2, 2.2, 3, 3.1
  - WRT54GS
    - Versions 1, 1.1, 2
- Flashing is done via the web interface
- [Demo]



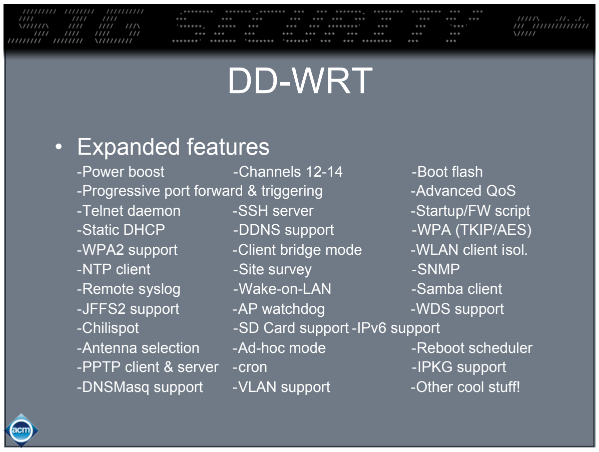
Candidate 3: DD-WRT

For those that want as much as they can get for only $0.00…



DD-WRT

- http://www.dd-wrt.com
- My personal favorite :-)
- Four flavors
  - Mini (no chillispot, nocat, rflow, kaid, samba, SNMP, IPv6)
  - Standard (all features, no VoIP or OpenVPN)
  - VPN (all features + OpenVPN, no samba or radvd)
  - VoIP (all features + sipath for SIP VoIP routing)



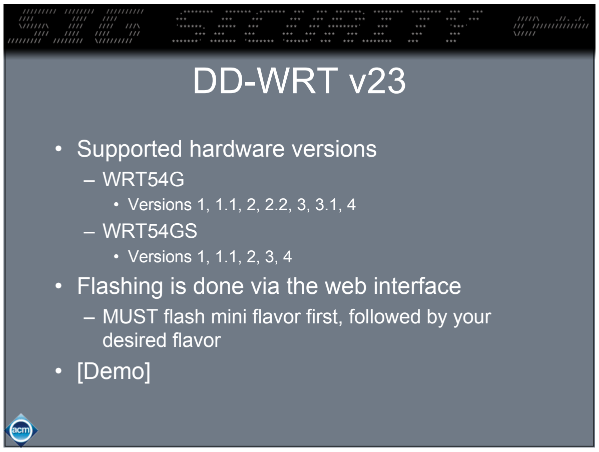
DD-WRT

- Expanded features

-Power boost
-Progressive port forward & triggering
-Telnet daemon
-Static DHCP
-WPA2 support
-NTP client
-Remote syslog
-JFFS2 support
-Chilispot
-Antenna selection
-PPTP client & server
-DNSMasq support

-Channels 12-14
-SSH server
-DDNS support
-Client bridge mode
-Site survey
-Wake-on-LAN
-AP watchdog
-SD Card support -IPv6 support
-Ad-hoc mode
-cron
-VLAN support

-Boot flash
-Advanced QoS
-Startup/FW script
-WPA (TKIP/AES)
-WLAN client isol.
-SNMP
-Samba client
-WDS support
-Reboot scheduler
-IPKG support
-Other cool stuff!



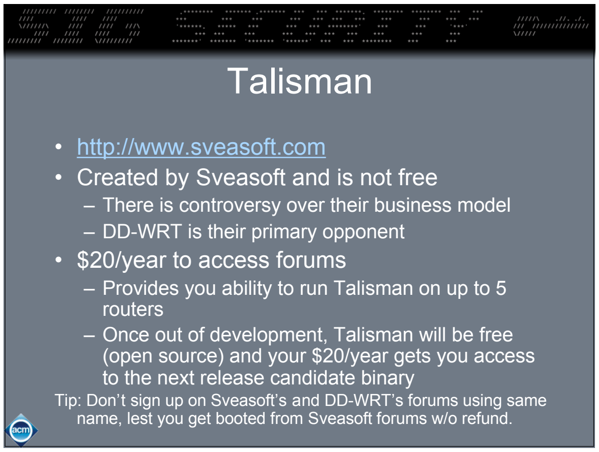
DD-WRT v23

- Supported hardware versions
  - WRT54G
    - Versions 1, 1.1, 2, 2.2, 3, 3.1, 4
  - WRT54GS
    - Versions 1, 1.1, 2, 3, 4
- Flashing is done via the web interface
  - MUST flash mini flavor first, followed by your desired flavor
- [Demo]

Candidate 4: Talisman

For those that must have everything, can shell out $20.00, are cool with NSA spying, and believeth in stretching the GPL…

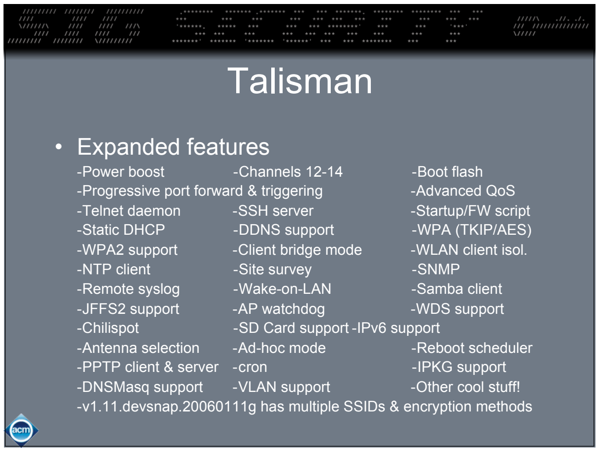
GPL



Talisman

- http://www.sveasoft.com
- Created by Sveasoft and is not free
  - There is controversy over their business model
  - DD-WRT is their primary opponent
- $20/year to access forums
  - Provides you ability to run Talisman on up to 5 routers
  - Once out of development, Talisman will be free (open source) and your $20/year gets you access to the next release candidate binary

Tip: Don't sign up on Sveasoft's and DD-WRT's forums using same name, lest you get booted from Sveasoft forums w/o refund.



Talisman

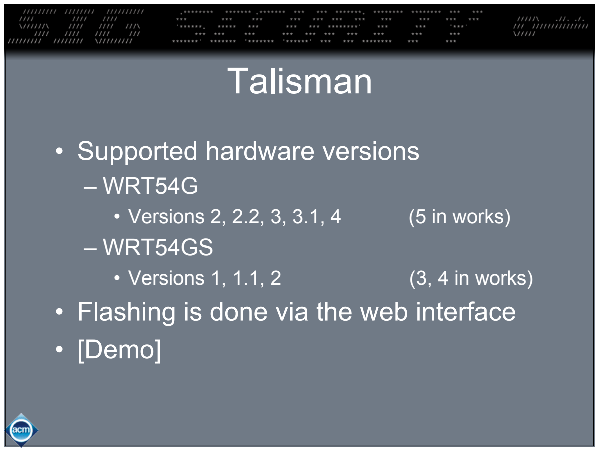
- Expanded features

  -Power boost
  -Progressive port forward & triggering
  -Telnet daemon
  -Static DHCP
  -WPA2 support
  -NTP client
  -Remote syslog
  -JFFS2 support
  -Chilispot
  -Antenna selection
  -PPTP client & server
  -DNSMasq support

  -Channels 12-14
  -SSH server
  -DDNS support
  -Client bridge mode
  -Site survey
  -Wake-on-LAN
  -AP watchdog
  -SD Card support -IPv6 support
  -Ad-hoc mode
  -cron
  -VLAN support

  -Boot flash
  -Advanced QoS
  -Startup/FW script
  -WPA (TKIP/AES)
  -WLAN client isol.
  -SNMP
  -Samba client
  -WDS support
  -Reboot scheduler
  -IPKG support
  -Other cool stuff!

  -v1.11.devsnap.20060111g has multiple SSIDs & encryption methods

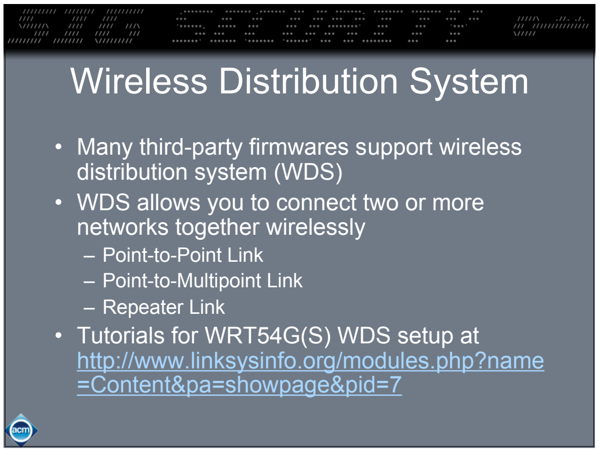


Talisman

- Supported hardware versions
  - WRT54G
    - Versions 2, 2.2, 3, 3.1, 4 (5 in works)
  - WRT54GS
    - Versions 1, 1.1, 2 (3, 4 in works)
- Flashing is done via the web interface
- [Demo]

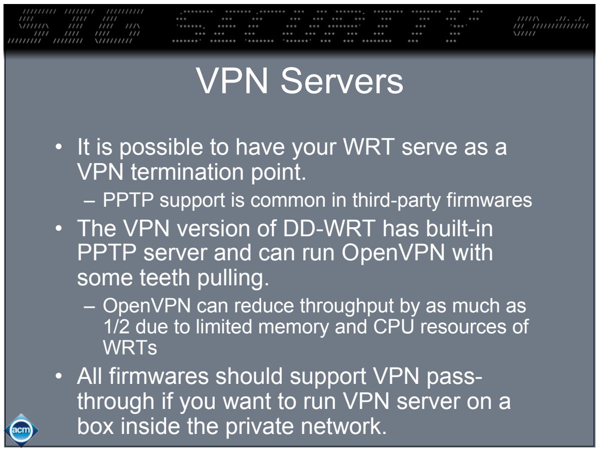
Advanced Functionality

Why install something cool and not fully utilize it?



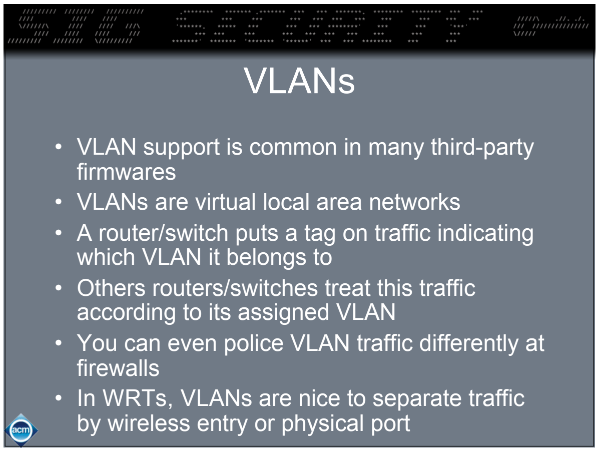
Wireless Distribution System

- Many third-party firmwares support wireless distribution system (WDS)
- WDS allows you to connect two or more networks together wirelessly
  - Point-to-Point Link
  - Point-to-Multipoint Link
  - Repeater Link
- Tutorials for WRT54G(S) WDS setup at http://www.linksysinfo.org/modules.php?name=Content&pa=showpage&pid=7



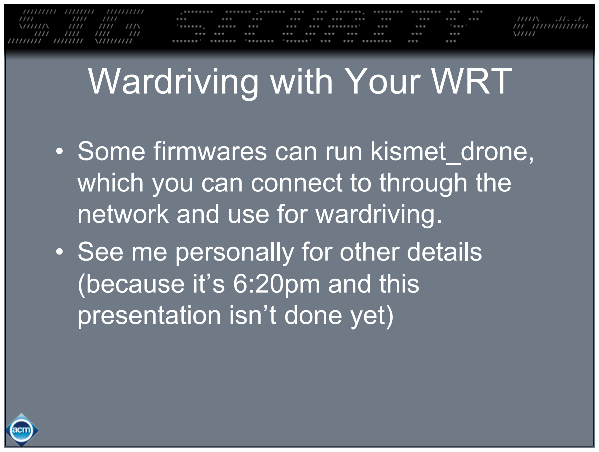
VPN Servers

- It is possible to have your WRT serve as a VPN termination point.
  - PPTP support is common in third-party firmwares
- The VPN version of DD-WRT has built-in PPTP server and can run OpenVPN with some teeth pulling.
  - OpenVPN can reduce throughput by as much as 1/2 due to limited memory and CPU resources of WRTs
- All firmwares should support VPN pass-through if you want to run VPN server on a box inside the private network.



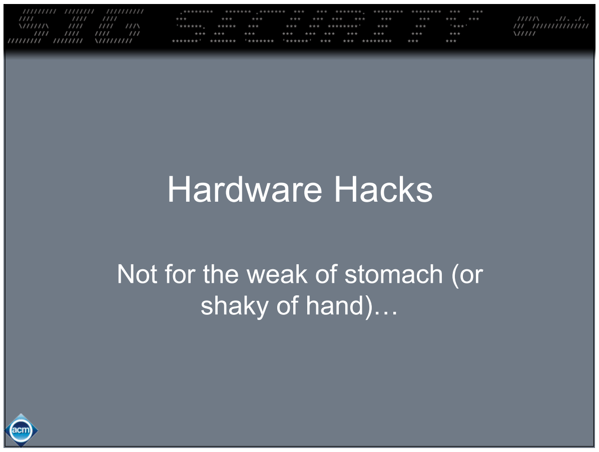
VLANs

- VLAN support is common in many third-party firmwares
- VLANs are virtual local area networks
- A router/switch puts a tag on traffic indicating which VLAN it belongs to
- Others routers/switches treat this traffic according to its assigned VLAN
- You can even police VLAN traffic differently at firewalls
- In WRTs, VLANs are nice to separate traffic by wireless entry or physical port



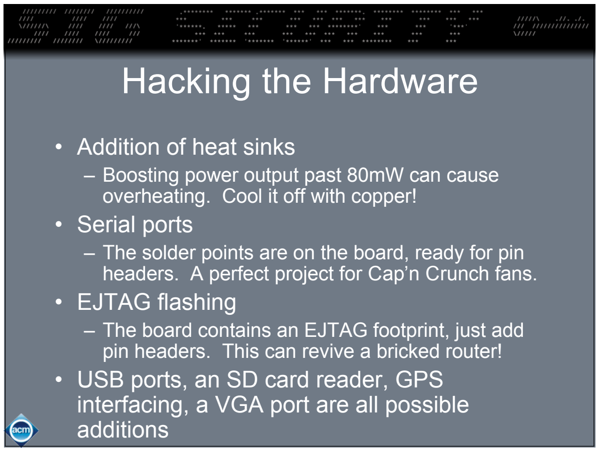
Wardriving with Your WRT

- Some firmwares can run kismet_drone, which you can connect to through the network and use for wardriving.
- See me personally for other details (because it’s 6:20pm and this presentation isn’t done yet)



Hardware Hacks

Not for the weak of stomach (or shaky of hand)…

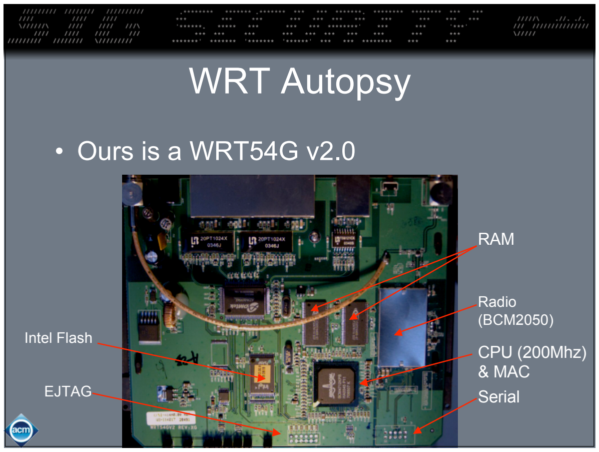


Hacking the Hardware

- Addition of heat sinks
  - Boosting power output past 80mW can cause overheating. Cool it off with copper!
- Serial ports
  - The solder points are on the board, ready for pin headers. A perfect project for Cap'n Crunch fans.
- EJTAG flashing
  - The board contains an EJTAG footprint, just add pin headers. This can revive a bricked router!
- USB ports, an SD card reader, GPS interfacing, a VGA port are all possible additions

WRT Autopsy

- We are gathered here today to celebrate the life of a bricked WRT. May it rest in peace in the future…but right now, let's cut it open and locate its vital organs!



WRT Autopsy

- Ours is a WRT54G v2.0

Special Thanks

- UMR IT sacrificed three WRTs for demonstration purposes
- Jason Trent provided the bricked WRT that underwent the autopsy
- And you attended the talk

Thank You!
Your Message Here!
WineEtc.com

Questions?

¿Preguntas? ¿ Perguntas? Vragen? Fragen? Ερωτήσεις Domande? Вопросы