Fix your F***ing Router
Already

Aaron Grothe
NEbraskaCERT
Disclaimer

Replacing your firmware on your router is a process that for a lot of routers will invalidate your warranty and in a worst case scenario give you a very poor night light.
Disclaimer (Cont’d)

After not having bricked a router in 6+ years I managed to brick one Sunday night getting ready for this talk. I was stupid and did something stupid the router is still broken though :-(
Quick Survey

How many of you are running the firmware that came with your router?
How many of you have patched your router since you plugged it in?
How many of you keep looking for the update that never comes?
Why upgrade/new Firmware?

Four quick examples from a quick DuckDuckGo Search
D-Link to issue router firmware updates for backdoor vulnerability

October 15, 2013 by Nancy Owano
Router Vulnerability Puts 12 Million Home and Business Routers at Risk

Friday, December 19, 2014  Swati Khandelwal
Asus router vulnerabilities go unfixed despite reports

You may not think of your Wi-Fi router as a wide-open barn door between your computer and the Internet, but for many Asus router owners, it is.

by Seth Rosenblatt / February 18, 2014 4:50 PM PST
Vulnerabilities in some Netgear routers open door to remote attacks

Lucian Constantin
IDG News Service

Vulnerabilities in the management interfaces of some wireless router and network-attached storage products from Netgear expose the devices to remote attacks that could result in their complete compromise, researchers warn.

The latest hardware revision of Netgear’s N600 Wireless Dual-Band Gigabit Router, known as WNDR3700v4 and shown above, has several vulnerabilities that allow
Its Even Worse

That is just the vendors who are willing to issue security fixes and acknowledge issues. If you get some of the off brand routers or your router is older you might not ever get a notice or an update.
Not Just For Security

You get a lot of new features/capabilities with new firmware as well

We’ll go into them later in the talk
What are some of my Options?

There are a couple of options we’re going to discuss:

DD-WRT - http://www.dd-wrt.com
OpenWRT - http://openwrt.org
Tomato - http://www.polarcloud.com/tomato
What are some more of my Options?

These are a couple of other ones to consider

LibreCMC - [http://www.librecmc.org](http://www.librecmc.org)
OpenWireless - [http://www.openwireless.org](http://www.openwireless.org)
DD-WRT - My Personal Choice

DD-WRT supports a lot of hardware for a look at the router database hit

https://www.dd-wrt.com/site/support/router-database

It has more features than OpenWRT - NAS, etc
OpenWRT

OpenWRT is a smaller release, therefore possibly more secure.
Builds all the versions of the software pretty much automatically using their buildroot system
DD-WRT is a fork of the OpenWRT project
Tomato

Tomato is lean & mean
Tomato mostly supports WRT & Buffalo routers
Forked from HyperWRT
LibreCMC

LibreCMC is a FSF-approved “free” distribution for wifi routers
It doesn’t use any binary blobs or software that doesn’t provide source
Because of this it supports a lot less hardware :-(

OpenWireless.org

Project trying to create free/open Wireless environment for everyone
Only supports one router brand currently
Has a bit of a political agenda but is very cool in concept
Demo of Upgrade

For this demo we’re going to take a TP-Link 841n and upgrade it from its stock firmware to DD-WRT.

For this we’re going to use the gui that comes with the TPLink and flash to DD-WRT.
TP-LINK TL-WR841N Wireless N300 Home Router, 300Mbps, IP QoS, WPS Button
by TP-LINK

6,591 customer reviews
1000+ answered questions

#1 Best Seller in Computer Routers

List Price: $38.29
Price: $19.68 Prime
You Save: $18.61 (49%)

In Stock.
Ships from and sold by Amazon.com. Gift-wrap available.

Want it Wednesday, July 15? Order within 1 hr 5 mins and choose Two-Day Shipping at checkout. Details

- Wireless N speed up to 300Mbps ideal applications for video streaming, online gaming VoIP, web browsing and multi-tasking
- Two 5dBi antennas greatly increase the wireless
Whining about how Easy it is now

About 8 years ago when I first went to DD-WRT on a netgear n600 you had to hook up a serial cable and interrupt it when booting and then execute a bunch of nvram commands, and hope for the best. You kids today and your Rock’n’Roll music and your Ipods
How to Upgrade

Identify Version and Model Number of Router
Download replacement firmware and save to PC
Login to the Router via web interface
Select upload new firmware
Reboot
Let's Do IT!!!
Some Cool Features

Adjust power of Radios hardware - Careful!!!
VPN Support
Virtual Interfaces
Adblocking / ActiveX filtering, etc
EOIP
Xlink KAI
Some More Cool Features

QOS
DMZs, remote access, etc
Bridge/Repeater/Etc
IPTables support!!!
Hardware that Works well with it

TP-Link - very cheap routers - $20.00 / amazon
Buffalo - Come with DD-WRT out of the Box
Most Linksys/Cisco stuff works pretty well
LinkSys - WRT routers - origin of name
How did I brick my Router?

Was trying to restore to stock firmware for demo

Wasn’t able to upload the original firmware and have it take over

Decided to go command line and use telnet/scp and mtd (memory technology device) to show the router who was boss

Write failed, ignored, rebooted anyway, brick
Can I unbrick my Router?

99% sure yes. Just haven’t had the time yet.

Could setup tftp server and firmware will be retrieved automatically
Could buy new hardware open router and let it know who it’s daddy
KEDSUM® CP2102 Module STC Download Cable USB 2.0 to TTL 6PIN Serial Converter For STC

by KEDSUM

72 customer reviews

Price: $7.99 Prime

Note: Available at a lower price from other sellers, potentially without free Prime shipping.

Only 16 left in stock.
Sold by KEDSUM and Fulfilled by Amazon. Gift-wrap available.

Want it Thursday, July 16? Order within 19 hrs and choose One-Day Shipping at checkout. Details

2 new from $2.48
Router Update

Did the tftpd trick to get the router working again.

Have loaded LibreCMC on it, so let's take a bit of a look at it
How I’m using it right now

At my house my primary router is an Archer C7 running the latest version of DD-WRT
Have an 841n setup with port forwarding for most of my experiments (mostly chatty android apps, etc)
How I’m using it right now

At my parent’s house they are running a TPLINK 841n and an old LinkSys Router. Both are DD-WRT - the linksys allows their LG tv to use the wired connection instead of wireless which keeps losing its PSK.
Tips

Make sure you’ve got the right version of your hardware identified. E.g. TP-Link 841n v7 and v9 need different hardware

Read the wiki for the hardware you are going to try it out on

Performance for various firmwares can be up and down
Tips (More)

You can do things like run torrents directly off your router if you want. There are software packages like Optware for DD-WRT and OpenWRT

30-30-30 (How to Reset your Router)
Lifehacker

Article on how to choose the best firmware for your wi-fi router

So is it worth it?

For me the answer is yes. I’m able to have one interface across all my different routers and I have a lot of control over what the routers do and don’t do. The ability to do things like port forwarding and iptables are very useful to me in my experiments.
Can I switch between Firmwares?

Depends on the router

For a lot of them the suggested course is to restore to factory firmware then upgrade again. That is also how I bricked my router
Switch Firmwares (cont’d)

There are differences

/\linux (dd-wrt) vs /\firmware (openwrt) for firmware locations

You can find some guides talking about how to do it
Richard Lloyd on Youtube

Has some very nice info on tplink recovery

https://www.youtube.com/user/richardlloydusa/videos
Q & A

Questions?? and Hopefully some Answers :-)

References for Examples

http://thehackernews.com/2014/12/router-vulnerability-puts-12-million.html
References for Examples (Cont)