Hacking Your Friends and Neighbors For Fun… (no profit, just fun)

Joshua Wright
jwright@willhackforsushi.com
SANS Security East
January 18, 2013

This is Not a Normal Talk

- This talk is not about defense
- This talk is not about forensics
- This talk is not about intrusion detection
- This talk is not about penetration testing*

This talk is about revenge.

* OK, it's a little bit about penetration testing.

I Am Not A Vengeful Person…

...But My Neighbors Are Stealing From Me

They Picked The Wrong Person To Steal From

They Are Stealing My Internet Access

- At least, it started out that way
- I had an open AP setup for testing attack tools, SSID: "victor-timko"
- Multiple unknown clients regularly join my network, accessing the Internet
  - Arpwatch FTW!

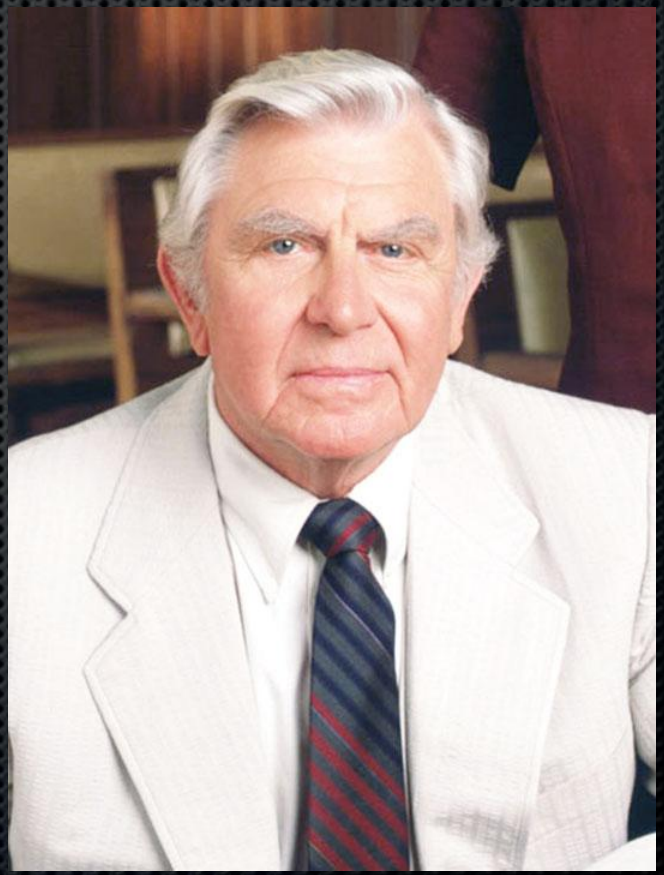
```
# arpwatch -m jwright@willhackforsushi.com -i eth0 -d

         ip address: 172.16.0.75
          interface: eth0
   ethernet address: 00:1d:ba:d5:c3:20
    ethernet vendor: Sony Corporation
          timestamp: Sunday, January 6, 2013 15:23:13 -0500
```

I Could Just Shut It Down…

- … But what's the fun in that?
- I decided to manipulate the stolen Internet access instead
- This became a source of much amusement for me over several months
  - I even invested in a high-gain antenna to make the signal better for the ne'er do wells

Is This Legal?

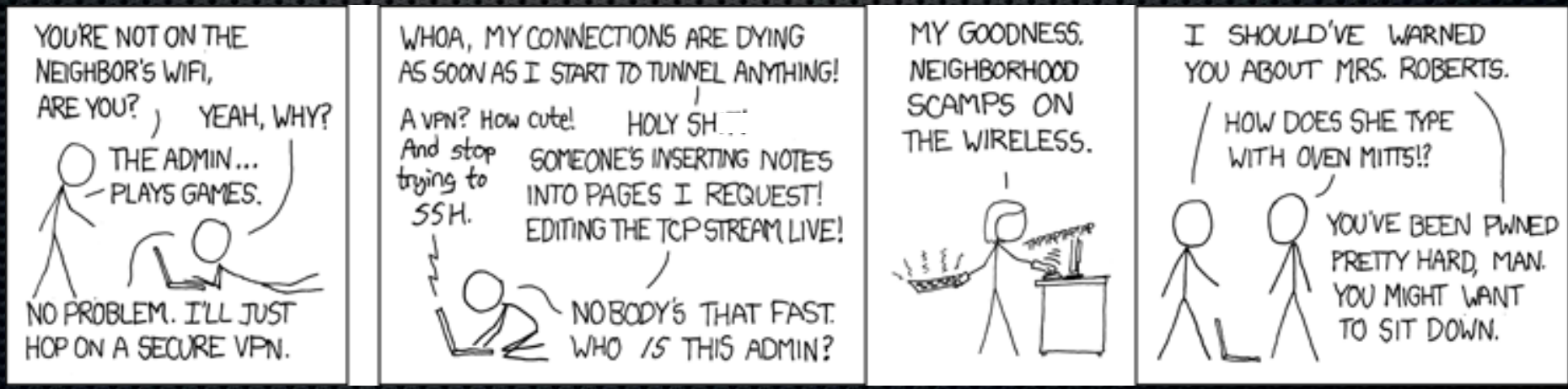
- I am not a lawyer, and I'm not attractive enough to play one on TV
- However, this is my network, and I can do what I want with it
- Consult your own attorney for advice*



* This is not really my attorney

This Has Been Done Before…

- Pete Stevens "Upside Down Ternet"
  - www.ex-parrot.com/pete
- XKCD classic "neighborhood scamps"
- g0tmi1k enhanced Pete's original work with LAN MitM attacks

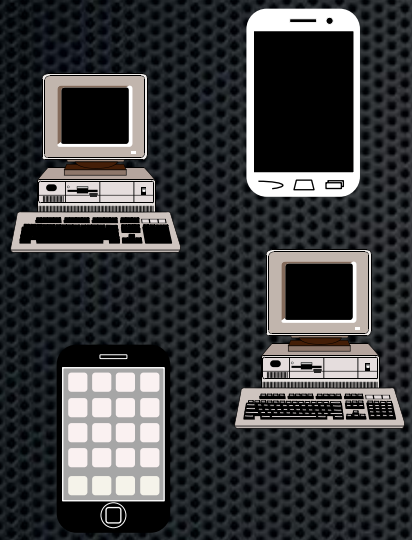


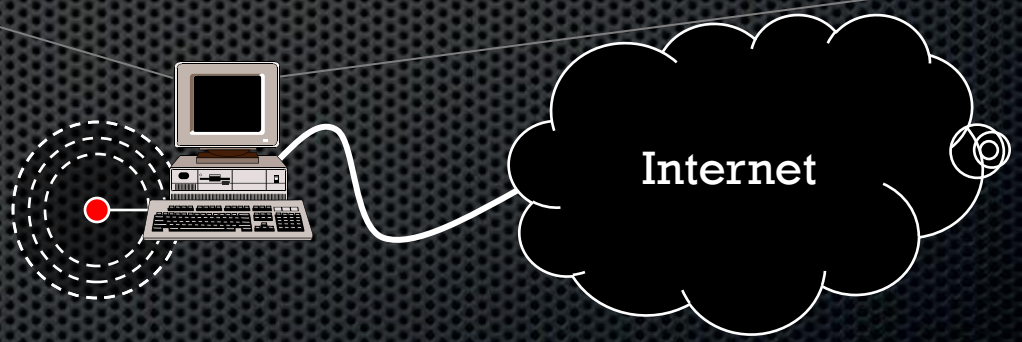
…I Am Doing It Better

- I'm making it easy for anyone else to implement this on their own
  - Connect to an upstream network for Internet access
  - Start the i-love-my-neighbors VM
  - Plug in a wireless card
  - Go!
- Plus, I'm much more devious than Pete

The Setup

1. Block all traffic except HTTP, DNS
2. Block all traffic destined for my internal IP address range
3. Redirect HTTP traffic to Squid proxy listener on TCP/3128
4. Squid inspects traffic content before returning to downstream client





Neighborhood Scamps

Ubuntu Linux guest and a USB wireless card

Squid Proxy

- Open source HTTP proxy with transparency support
  - Can proxy clients without explicit client configuration
- Option to "rewrite URL's" with a custom tool
  - url_rewrite_directive /path/to/tool

Incoming Data	URL client_ip "/" FQDN user method
Return Data	New (or original) URL

URL Rewriting

- The end-user sees the original URL they requested
- The Squid script returns any modified URL desired
- We can manipulate content:
  - Take URL request from user
  - Download content with wget to a local file
  - Modify content as desired
  - Return new URL on local server

HTML Content Manipulation

- Retrieve any HTML/CSS page
- Use standard text modification tools to manipulate content
  - sed, grep, awk, cut
  - Perl, Python
- Knowledge of regular expressions is helpful here

```
$url =~ s/(q=.+)&/$1+"+in+my+pants"&/;
```

Image Content Manipulation

- So much fun!
- Essential tool: ImageMagick mogrify
  - Allows us to modify images on the command line

"Use the mogrify program to resize an image, blur, crop, despeckle, dither, draw on, flip, join, re-sample, and much more. " mogrify man page


```
$ mogrify -annotate +32+80 "This is my TFH" -pointsize 36 in.jpg
```

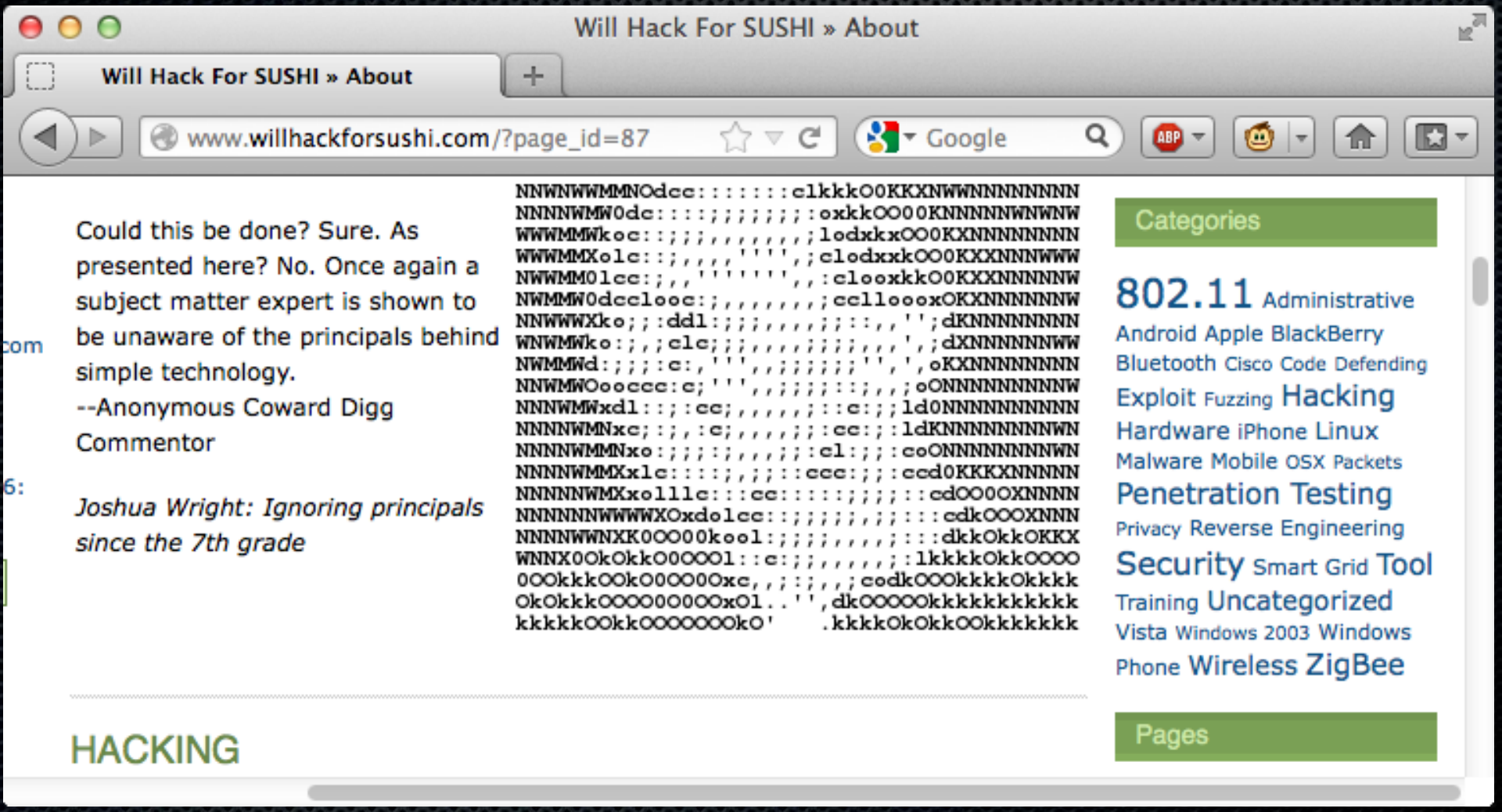
Picking an SSID

- "linksys": a solid choice
  - A little cliché, but well-known
  - It's the universal "Hey, here's a sucker" SSID
- "PANERA", "attwifi", "tmobile"
  - Lots of people looking for these networks already
  - Consult your attorney first
- Or, you could be more devious about it…
  - "youcanthackthis": Not Entrapment! (for me)

Getting Started

- Connect host to the Internet
  - Wired or wireless
- Boot the i-love-my-neighbors VM
  - Login as root, "sec617" as the password
- Plug in a USB wireless card
- Run "./neighbor" to list services
- Run "./neighbor wlan0 eth0 *service*" to start the desired service

DEMO


Will Hack For SUSHI » About
Will Hack For SUSHI » About
www.willhackforsushi.com/?page_id=87
Google
Could this be done? Sure. As presented here? No. Once again a subject matter expert is shown to be unaware of the principals behind simple technology.
--Anonymous Coward Digg Commentor
Joshua Wright: Ignoring principals since the 7th grade
Categories
802.11 Administrative Android Apple BlackBerry Bluetooth Cisco Code Defending Exploit Fuzzing Hacking Hardware iPhone Linux Malware Mobile OSX Packets Penetration Testing Privacy Reverse Engineering Security Smart Grid Tool Training Uncategorized Vista Windows 2003 Windows Phone Wireless ZigBee
Pages
HACKING

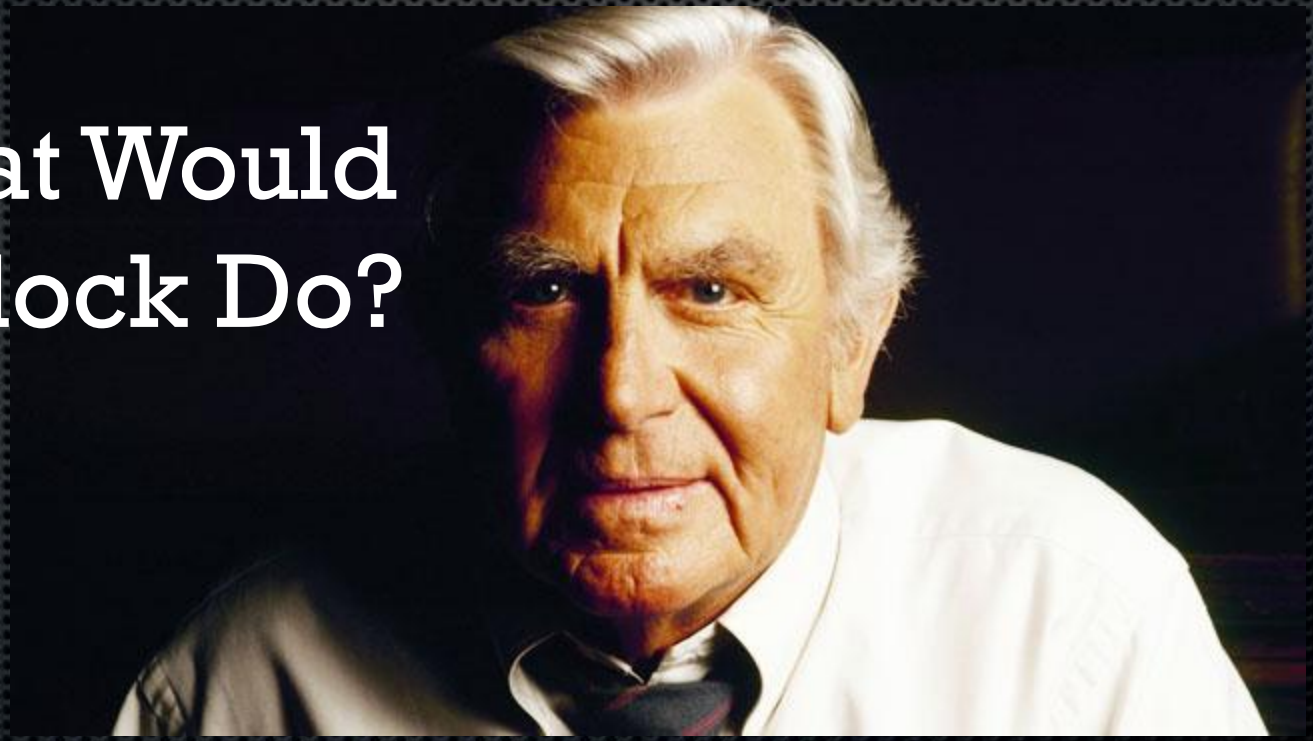
Script Summary

asciiImages	Convert all images to ASCII art
blurImages	Progressively blur images over time
fightClub	Add image animation to all images
flipImages	Flip all images vertically
flopImages	Flop all images horizontally
kittenWar	Randomly redirect people to www.kittenwar.com
nogoogleBing	Force people to use Bing when they access Google
replaceImages	Replace all images with cute cat on laptop picture
rickrollYoutube	Obligatory Rick Roll
timeMachine	Use old versions of websites
touretteImages	Add animated happy words to images
uselessWeb	Redirect randomly to theuselessweb.com sites

Where Else Could This Be Fun?

- The airport, coffee shops, restaurants*
- Hacker conferences, LAN parties*
- Definitely not at SANS conferences

What Would Matlock Do?



* Seriously, contact your attorney

Download

- This is the very first release of i-love-my-neighbors!
  - Translation: There are a lot of undiscovered bugs
- If you add new services (scripts) or run into bugs, please let me know!
- See me to grab a copy while at the conference

http://neighbor.willhackforsushi.com

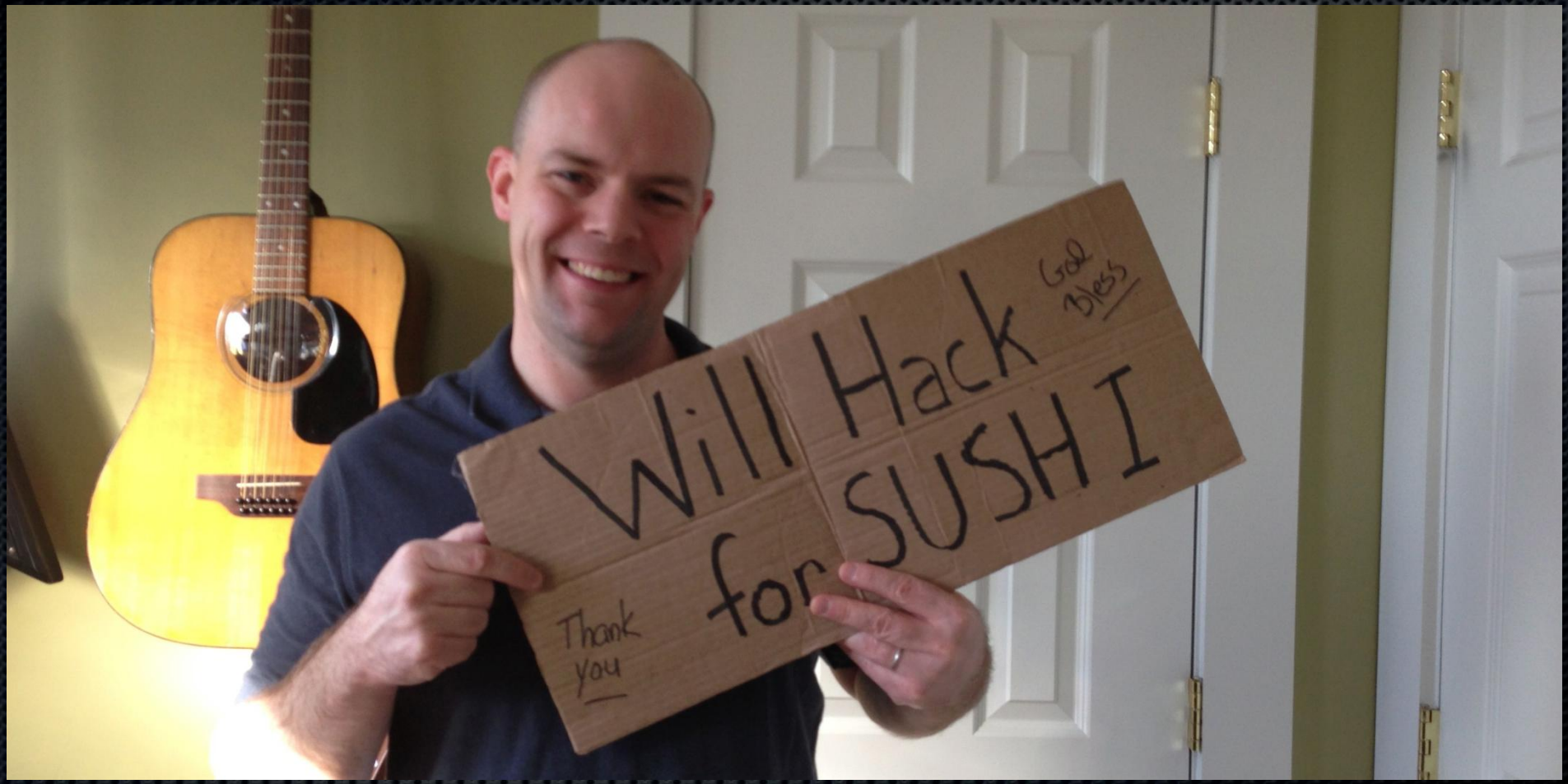
Wireless Card Support

- Linux-supported, mac80211 stack card with AP support
  - Check linuxwireless.org/en/users/Drivers (must say "Yes" in the AP column")
- Recommended: rt2800usb chipset
  - ALFA AWUS051NH (hard to find)
  - Linksys WUSB600N, WUSB100
  - TRENDnet TEW-644UB

A Cautionary Tale

- Wireless is not safe. Especially not open wireless.
  - I'm blurring web pages, but I could be delivering malicious Java JAR files instead
  - Or Adobe files, there have been 1 or 2 vulnerabilities there
- Consider taking SEC617, "Ethical Hacking Wireless, and Defenses" (sans.org/sec617)
  - Learn wireless protocol analysis, crypto, WiFi, ZigBee, DECT, Bluetooth and more
  - Get some cool toys (including a a/b/g/n USB wireless card compatible with i-love-my-neighbors)

Questions?
Thank you!



jwright@willhackforsushi.com - 401-524-2911 - @joswr1ght