Embedded Systems Hacking and My Plot To Take Over The World

Version 1.5

Paul Asadoorian
Founder & CEO, PaulDotCom Enterprises
http://pauldotcom.com
paul@pauldotcom.com

Who am I?

- I had this really boring slide about who I am
- Then I realized that's not really who I am
- What follows is the "Powerpoint" version of "a little about me"...

PaulDotCom Security Weekly
http://www.pauldotcom.com

Podcast

- 2005 - Present
- ~ 200 episodes
- Awards, blah
- Thursdays 7PM EST

Hack Naked

HACK NAKED http://pauldotcom.com

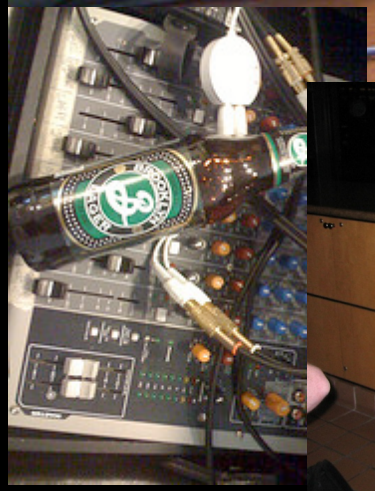
Why Hack Naked?

Beer


SANS
www.sans.org


SkullSplitter
www
tcom


HACK
NAKED




HACK
NAKED
VACATION LAND

Computer Destruction

PaulDotCom

John "Father John" Strand

Paul "Salad Shooter" Asadoorian

Larry "Dirty Uncle" Pesce

Mick "Jr. Salad Shooter" Douglas

"Byte_Bucket"

Carlos "Dark0perator" Perez

Mike "The Original Intern" Perez

Mark Baggett

Darren "Girly Mustache" Wigley

"Hail Nessus!"

- My day job: I work for Tenable Network Security as a "Product Evangelist"
- I use Tenable products and write blogs, publish podcasts, teach courses, and produce videos
- http://blog.tenablesecurity.com

Taking Over The World

- Many have tried
- No one truly successful
- What are the three things you need to take over the world?
  - Yes, I've spent time thinking about this
- All geeks ~~like~~ deal with "specifications" and "Requirements"

Requirements For World Domination

1. **Money** - You need to buy stuff, like armies, countries, pay people off, etc...

2. **Power** - You need the ability to use those resources to influence & control people

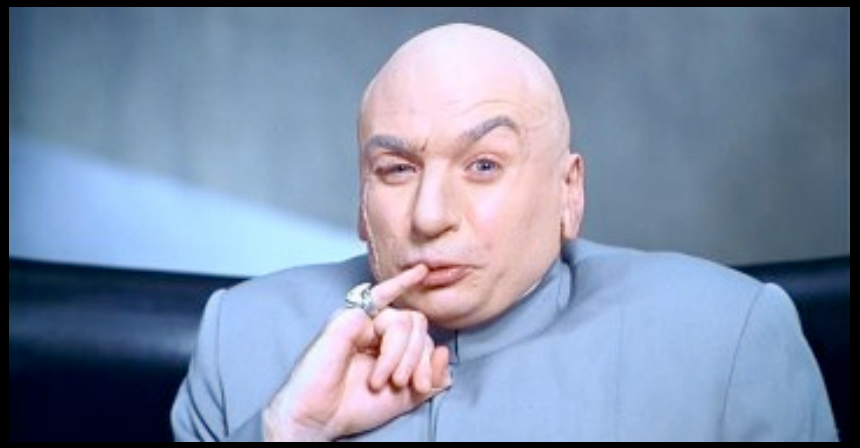
3. **Stealth** - If everyone knows about your plan, it is doomed from the beginning

Using Embedded Systems To Make Money

- **Video games** - Most are involved in commerce and network connected
- **Entertainment** - Apple TV, Roku, all link back to your credit card somehow
- **Wireless routers** - Route your traffic when doing online banking, Paypal, Ebay, etc...
- **Printers/Fax** - How many times have you printed sensitive information?

Using Embedded Systems To Gain Power

- Network traffic (e.g. information) flows through them
- Information = Power
  - The ability to manipulate information is powerful
- Multiple computers can be controlled at once



Using Embedded Systems To Gain Power

- Embedded systems are an integral to controlling water, electricity, and sewage treatment

- See research from Josh Wright (http://www.willhackforsushi.com) and Travis Goodspeed (http://travisgoodspeed.blogspot.com/)

Benefits To Targeting Embedded Systems - Stealth

- No one pays attention to them until they are broken
- Security is left out to save resources, make it easy, and money (as is logging)
  - Vendors are focused on profit, which also never equals security
  - Competition has driven vendors to cut costs to make products cheaper
- Potentially no interactive user (mouse/ keyboard)

Benefits Of Targeting Embedded Systems - Stealth

- Embedded systems contain vulnerabilities that go unnoticed because everyone looking for them does not have every device that was ever made
- "Can you send me a free router in exchange for some security testing?"

They Are Everywhere

SSID Stats (top 1000)

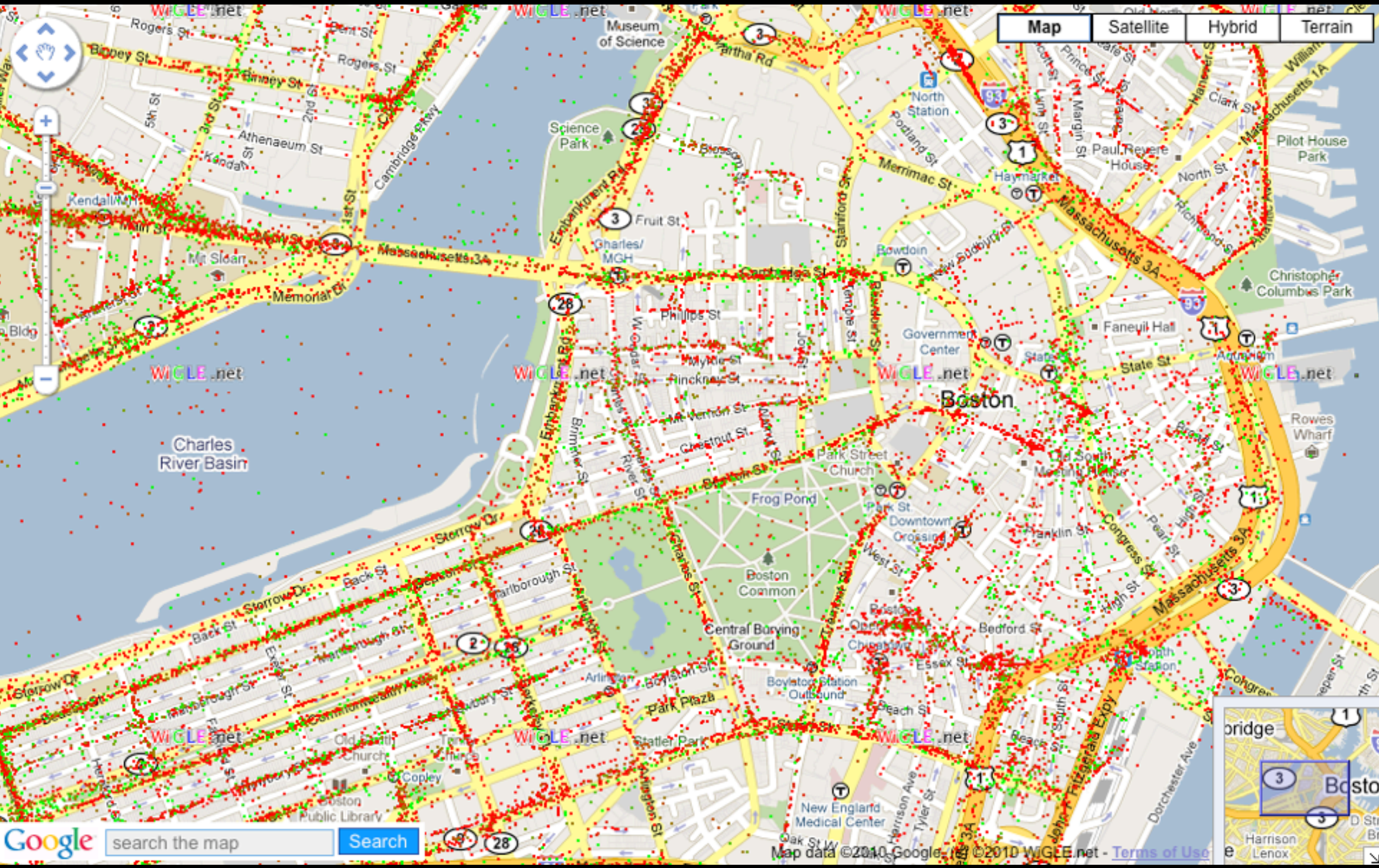
SSID	Total	Percent
<no ssid>	1957492	9.660%
linksys	1751543	8.644%
default	541572	2.672%
NETGEAR	491861	2.427%
Belkin54g	227715	1.123%
no_ssid	206541	1.019%
Wireless	200543	0.989%
hpsetup	151730	0.748%
WLAN	99043	0.488%
ACTIONTEC	82407	0.406%

Manufacturer Stats

Manufacturer	Total	Percent
Linksys	2695479	13.302%
D-Link	1310898	6.469%
Cisco	1153941	5.694%
Dell	889249	4.388%
Netgear	798122	3.938%
2wire	448893	2.215%
Belkin	442110	2.181%
Symbol	300751	1.484%
Apple Computer	223718	1.104%
Lucent	199088	0.982%

http://wigle.net/gps/gps/main/ssidstats

In Places Like Boston



And They Are Vulnerable...

Researchers scanning the internet for vulnerable embedded devices have found nearly 21,000 routers, webcams and VoIP products open to remote attack. Their administrative interfaces are viewable from anywhere on the internet and their owners have failed to change the manufacturer's default password.

http://www.wired.com/threatlevel/2009/10/vulnerable-devices/#ixzz0foWysVrp

"The researchers have provided ISPs with their findings in the hope that they will do something to protect vulnerable customers."


NOT!

And No One Wants To Be Responsible For Them

Chen said he contacted Time Warner's security department four weeks ago and was told that the company was aware of the security vulnerability but ***"cannot do anything about it."***

Time Warner's Dudley says the SMC8014 modem/routers are just a small portion of the ***14 million devices*** *its customers are using.*

http://www.wired.com/threatlevel/2009/10/time-warner-cable/

What if "Bob" Scanned the Internet?

- Use Google, find most popular ISPs that provide cable modem routers to users (or other interesting devices)
- Use ARIN todiscover the IP address ranges assigned to those ISPs
- Use Nmap to discover all devices that have port 80 open and identify the service/banner
- Manually poke through results and see what you find
  - Or automate something to find vulnerabilities

Example Vulnerabilities We Could Look For

- Wireless Routers - TONS of FAIL on the Internet
  - Default, weak, or missing passwords are COMMON
  - Linksys HNAP - Information leakage and lame denial of service with no mitigation
- Printers - JetDirect authentication weaknesses
- Roku Player - Entertainment device

Shodan is Handy For Exploring The Inernet

SHODAN
Computer Search Engine

port:80,23 huawei

A known vulnerability or poor implementation in "Huawei" routers helps take over countries

» Top countries matching your search	
Colombia	1,307
Venezuela, Bolivarian Republic of	86
China	30
United States	13

201.244.139.14
Linux recent 2.4
Added on 16.02.2010

```
HTTP/1.0 401 Unauthorized
Server: micro_httpd
Cache-Control: no-cache
Date: Sat, 01 Jan 2000 13:24:39 GMT
WWW-Authenticate: Basic realm="Huawei SmartAX MT880"
Content-Type: text/html
Connection: close
```

A whois lookup returns comprehensive results

Scanning the Internet is Time Consuming

- Scanning the Internet is fun (so Bob tells me)
- It takes a long time, even when limiting to one port

```
# nmap --version-light --open --min-hostgroup 1024 -T4 -n
  -PN -oG results.gnmap -sV -p 80 -iL isp.targetips
```

524288 IP addresses (32620 hosts up) scanned in 9769.46 seconds (2.7 hours)

2272512 IP addresses (2272512 hosts up) scanned in 135156.66 seconds (37.5 Hours)

Finding Devices Without Scanning The Internet

- NTP could be used to identify devices
  - Example: http://carnal0wnage.blogspot.com/2010/04/network-time-protocol-ntp-fun.html
- DNS zone transfers from certain places reveal interesting results
- Brute-forcing DNS sub-domains can reveal hosts too
  - Example: http://www.gnucitizen.org/blog/hacking-linksys-ip-cameras-pt-6/

NTP: All your ntp are point to us

- Netgear shipped thousands of routers in 2003 and pointed them to ntp1.cs.wisc.edu
  - http://pages.cs.wisc.edu/~plonka/netgear-sntp/
- Issued firmware fix, but who does that?
- Routers still point to it, and thanks to HD Moore we can query it easily with metasploit
- Gives us a list of Netgear routers that Bob would attack

Metasploit NTP Module

```
msf > use auxiliary/scanner/ntp/ntp_monlist
msf auxiliary(ntp_monlist) > set RHOSTS ntp1.cs.wisc.edu
RHOSTS => ntp1.cs.wisc.edu
msf auxiliary(ntp_monlist) > run

[*] Sending probes to 128.105.39.11->128.105.39.11 (1 hosts)
[*] 128.105.39.11:123 205.237.147.11:23457 (128.105.39.11)
[*] 128.105.39.11:123 86.29.31.176:23457 (128.105.39.11)
[*] 128.105.39.11:123 209.192.117.17:23457 (128.105.39.11)
[*] 128.105.39.11:123 70.54.203.193:60128 (128.105.39.11)
[*] 128.105.39.11:123 222.254.78.74:10001 (128.105.39.11)
```

Lots of DSL/Cable Providers on the list

What are chances these users have not updated firmware?

```
71.161.67.98 domain name pointer adsl-67-161-71.shv.bellsouth.net.
76.72.108.68 domain name pointer ip68-108-72-76.lv.lv.cox.net.
117.131.29.65 domain name pointer CPE-65-29-131-117.wi.res.rr.com
45.21.110.76 domain name pointer c-76-110-21-45.hsd1.fl.comcast.net
61.195.100.98 domain name pointer rrcs-98-100-195-61.central.biz.rr.com.
164.133.254.76 domain name pointer adsl-76-254-133-164.dsl.skt2ca.sbcglobal.net.
```

DNS Zone Transfer - MUCH faster!

```
# time host -la ourlinksys.com 66.161.11.121 >
ourlinksys.com.out

real  0m2.564s
user  0m0.456s
sys   0m0.068s

# wc -l ourlinksys.com.out 120815 ourlinksys.com.out
```

This no longer works with the above domain since I accidentally published the information without sanitizing.

Check out Metasploit's "gather/dns_enum" module written by Carlos Perez

Target specific devices

D-Link

DIR-655

SETUP | ADVANCED | TOOLS | STATUS

- ADMIN
- TIME
- SYSLOG
- EMAIL SETTINGS
- SYSTEM
- FIRMWARE
- DYNAMIC DNS
- SYSTEM CHECK
- SCHEDULES

DYNAMIC DNS

The DDNS feature allows you to host a server (Web, FTP, Game Server, etc...) using a domain name that you have purchased (www.whateveryournameis.com) with your dynamically assigne IP address. Most broadband Internet Service Providers assign dynamic (changing) IP addresses. Using a DDNS service provider, your friends can enter your host name to connect to your game server no matter what your IP address is.

Sign up for D-Link's Free DDNS service at www.DLinkDDNS.com.

Save Settings | Don't Save Settings

DYNAMIC DNS

Enable Dynamic DNS: ☑

Server Address: <<

✓ Select Dynamic DNS Server
www.DLinkDDNS.com
www.DynDNS.com (Custom)
www.DynDNS.com (Free)

(e.g.: me.mydomain.net)

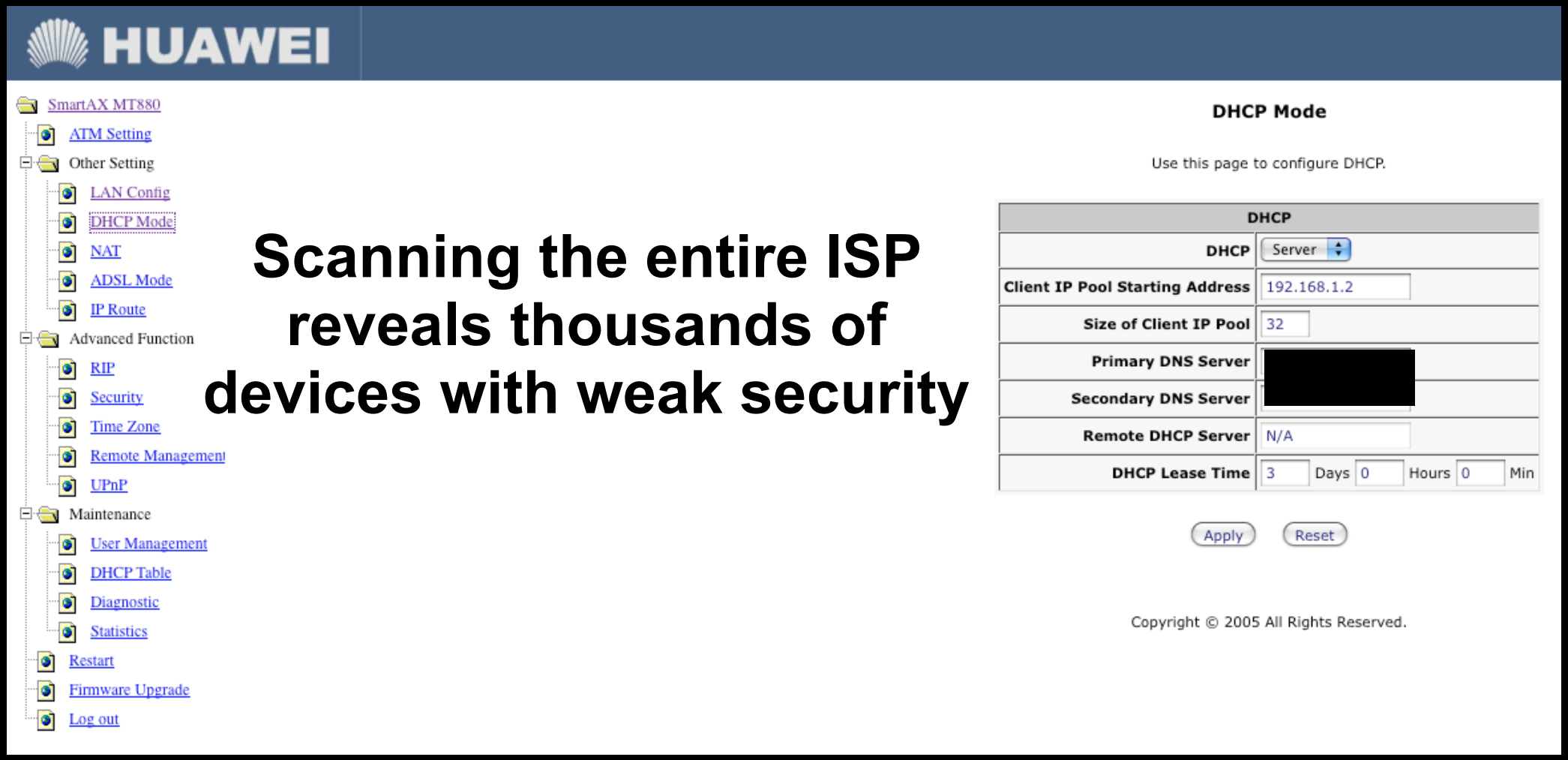
Password or Key:

Verify Password or Key:

Timeout: 576 (hours)

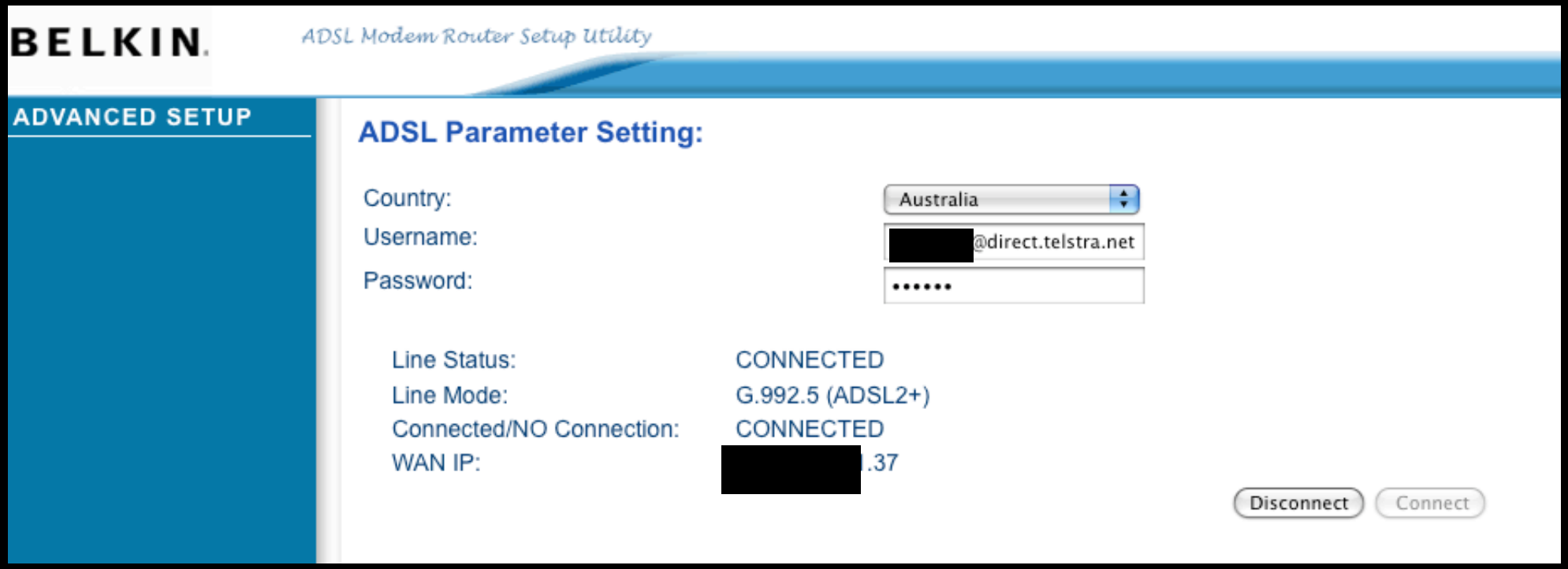
Status: Disconnect

DNS Is The Internet



Scanning the entire ISP reveals thousands of devices with weak security

Global Reach



This Required NO PASSWORD

Airties RT-111

http://[redacted]/cgi-bin/webcm

AirTies wireless networks

AirTies RT-111 ADSL2+ 4 Portlu Modem

- ANASAYFA
- ADSL
- YEREL AĞ
- FIREWALL
- NAT
- ROUTING
- YÖNETİM
- DDNS
- ARAÇLAR
- RAPOR

Hoş Geldiniz

Bir AirTies ürününü tercih ettiğiniz için AirTies ailesi olarak teşekkür ederiz.

Modemin bütün özelliklerini öğrenmek ve en verimli şekilde kullanabilmek için kullanma kılavuzunu dikkatle okumanızı öneririz.
Herhangi bir sorunla karşılaştığınızda AirTies Çağrı Merkezi Hattına 0212-4440239 numaralı telefondan ulaşabilirsiniz.
Modeminizin çalışma durumu ile ilgili bilgiler aşağıda sunulmuştur.

Internet Bağlantısı:	Bağlantı var
ADSL Bağlantısı:	Bağlantı var
ADSL Hızı:	512 / 1024 kbps
Internet IP Adresi:	[redacted]
ADSL MAC Adresi	00:1C:A8:40:70:C9
Ethernet:	Bağlantı var
DHCP Sunucu:	Etkin
Firmware Sürümü:	1.0.13
Seri No:	AT0030801007290
Sistemin Açık Kalma Süresi:	188 Saat 1 Dakika
Sistem Saati:	17 Şubat 2010 05:58:28

So easy "hacker" Nichole Richie can do it!

"Airhead socialite Nicole Richie broke into the Twitter account of her chums last week as part of a prank that proves just about anyone can become a password hacker."

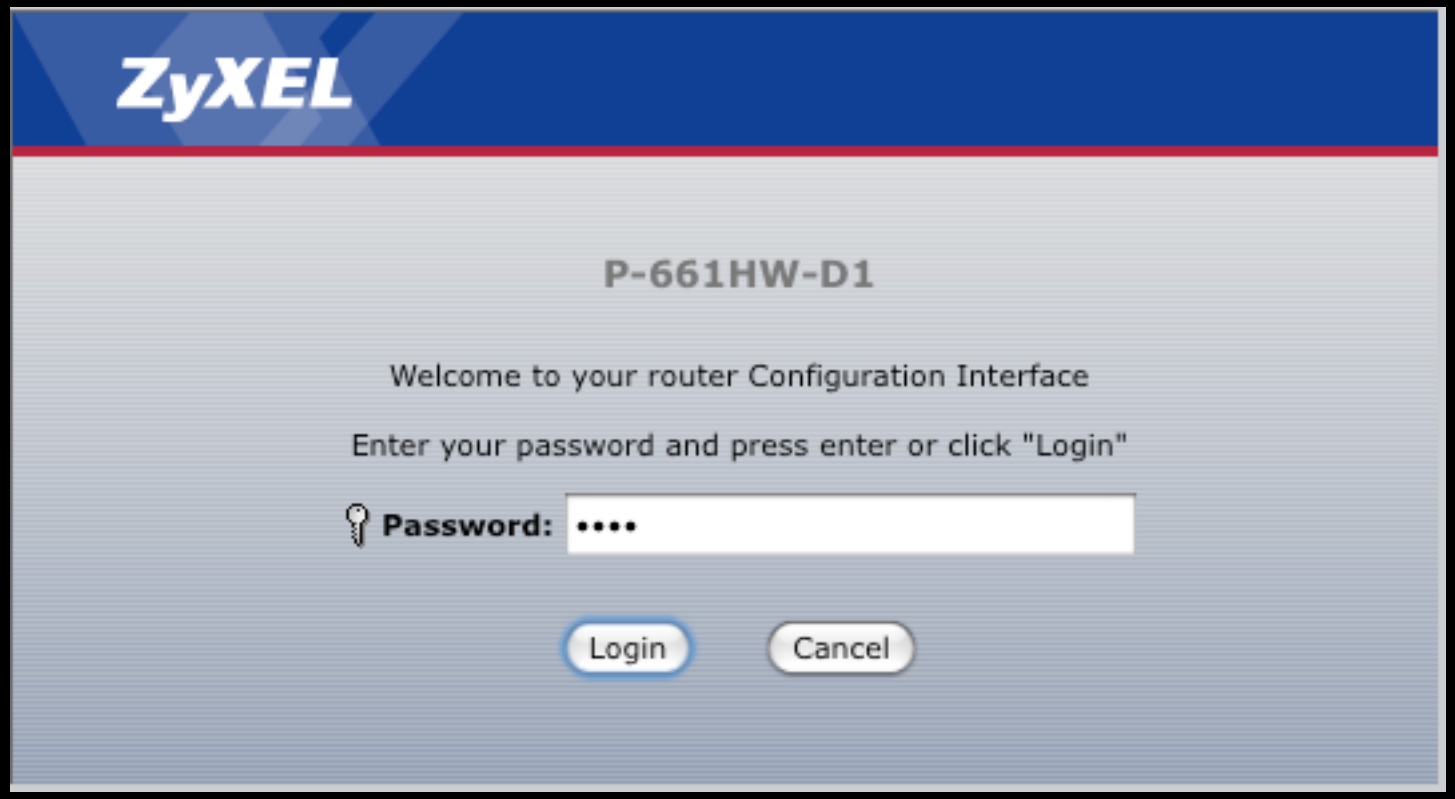
http://www.theregister.co.uk/2010/04/06/richie_twitter_hacking_prank/

She socially engineered in order to get the passwords!

Most devices do not even require this level of sophistication!

Rumour: Nicole will attend Defcon 2010 and give a presentation on hacking Twitter

The Password Is Already There!

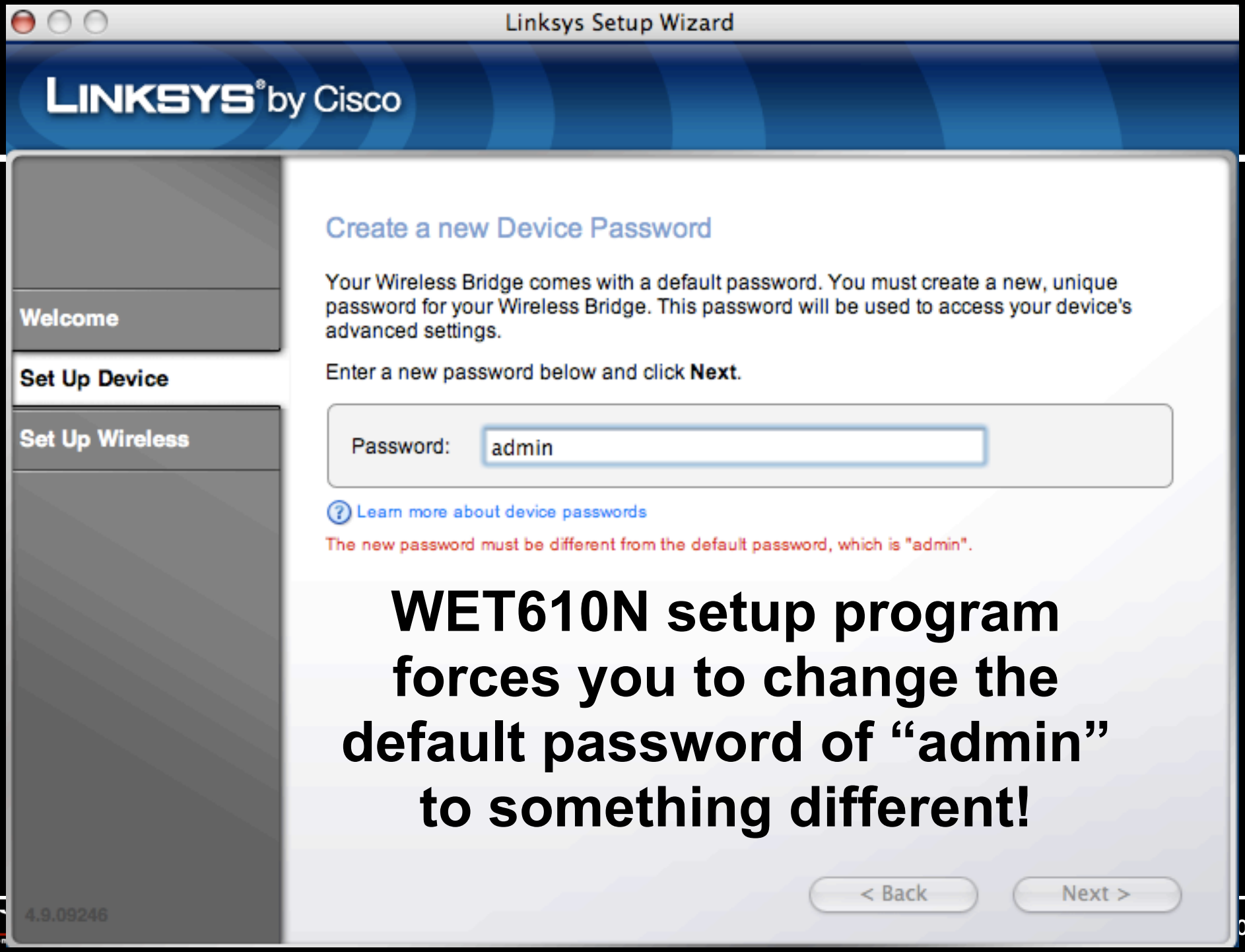


Social engineering not required!

This Gets Scary

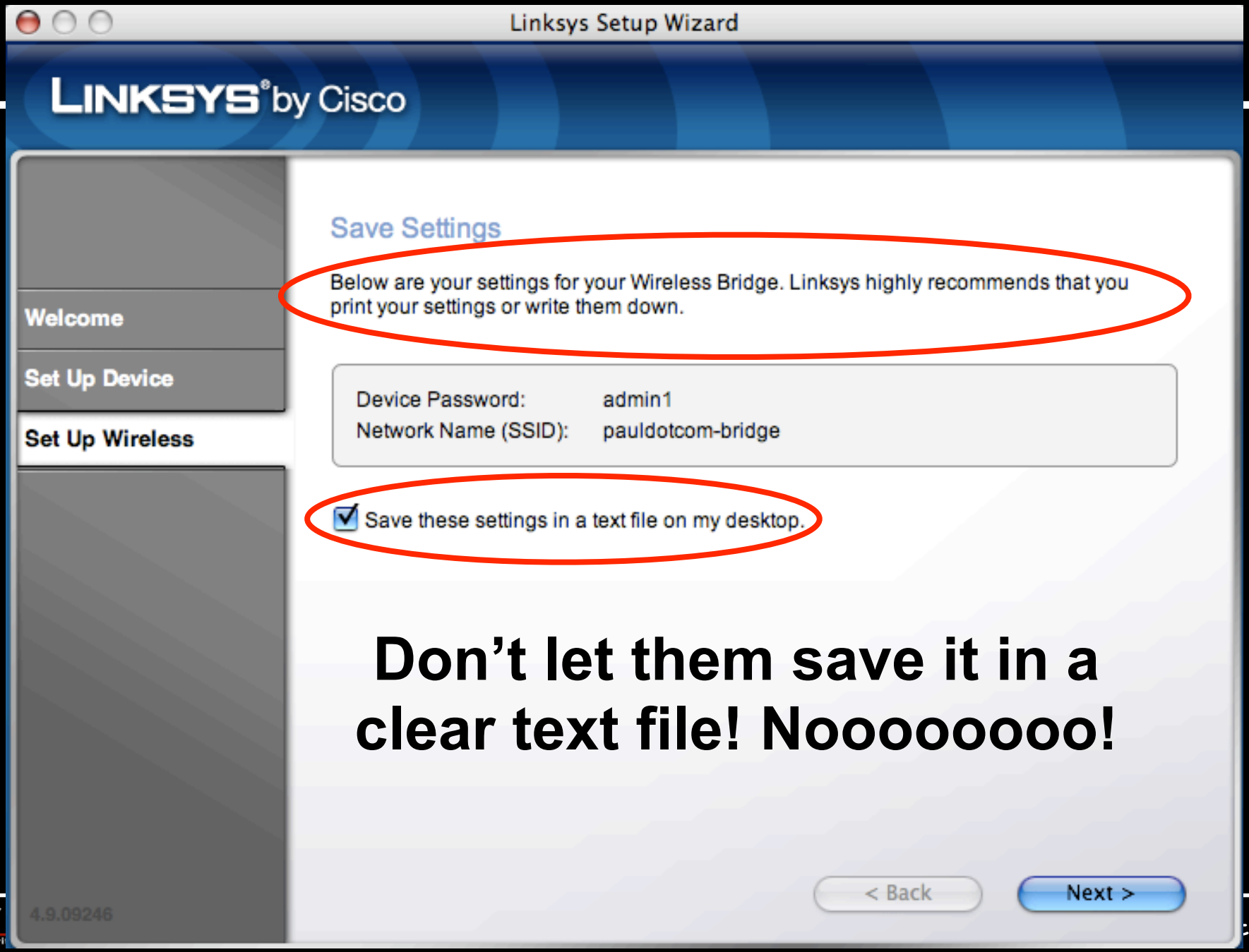
- A certain ISP based in Turkey left default or blank passwords on seemingly every router
- This helps in our plot for world domination:
  - Target geographic regions, exploit vulnerabilities exposed by that particular ISP+Cable Modem combo
  - Change DNS servers and control user's "Internets"
  - Change passwords and lock out user and ISP (not too stealthy)
  - Upload new firmware to provide new functionality (like password logging, SSL MiTM, etc...)

EPIC WIN!



WET610N setup program forces you to change the default password of “admin” to something different!

EPIC ~~WIN~~ FAIL!

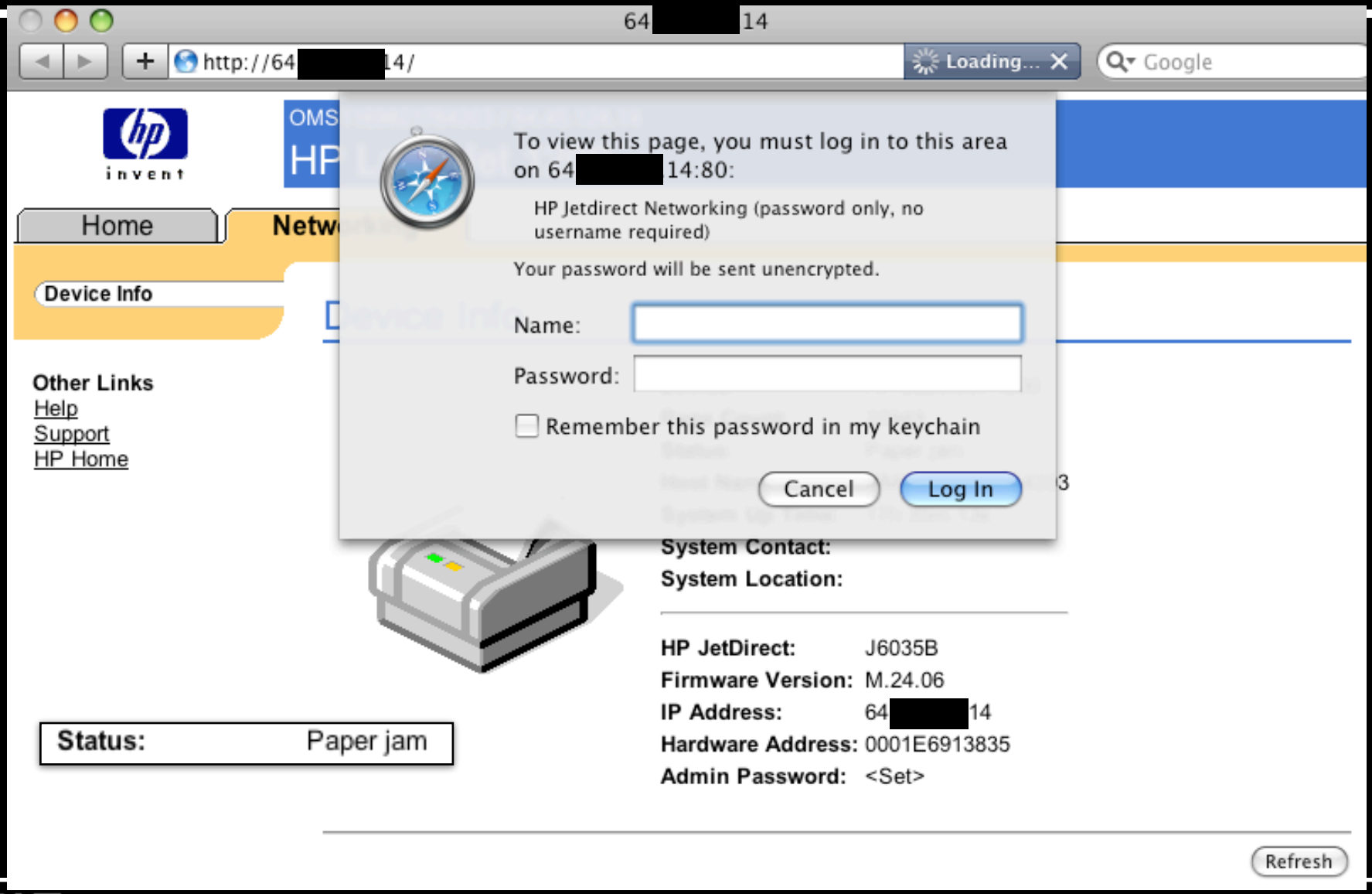


Don't let them save it in a clear text file! Noooooooo!

Steps to Control Routers

- **Step 1** - Buy router
- **Step 2** - Find vulnerability
- **Step 3** - See what DDNS providers it supports by default
- **Step 4** - Try zone transfer, if fails, go to step 5
- **Step 5** - Brute force subdomains of DDNS provider
- **Step 6** - Check NTP settings, see if it points to an NTP server by default (unlikely)
- **Step 7** - Scan the Internet at random (or target and ISP and look for that router (Slow)
- **Step 8** - Exploit vulnerabilities and control routers

Can we at least get a USERNAME with a password!



Roku

press up
press down
press left
press right
press select
press home
press fwd
press back
press pause

```
# nc 192.168.1.240 8080
D0C9DP009064
ETHMAC 00:0d:4b:4c:29:5e
WIFIMAC 00:0d:4b:4c:29:5f
>
```

http://forums.roku.com/viewtopic.php?t=20106&sid=f0702e3bbba722ac7f1a59307209782c

World Domination Propaganda

http://www.i-hacked.com/content/view/274/48/

Even More Attacks

- HD Moore found several flaws in VxWorks, scanned 3.1 billion IP addresses and found 250,000 systems exposed to the Internet
  - http://blog.metasploit.com/2010/08/vxworks-vulnerabilities.html
- Craig Heffner discovered a DNS rebinding attack on several routers allowing attackers to gain control of administrative interfaces
  - http://code.google.com/p/rebind/

Even More Attacks (2)

- Ki-Chan Ahn and Dong-Joo Ha created malware for Nintendo Wii and DS systems
  - http://games.venturebeat.com/2010/07/31/live-demos-of-hacking-the-nintendo-ds-and-the-wii-to-spread-malware/
- Barnaby Jack remotely attacked two different ATMs and "made the money come out" (without a card+pin #)
  - http://www.youtube.com/watch?v=qwMuMSPW3bU

Potential Linksys Vulnerability

- Reported to Cisco PSIRT Feb 17, 2010
- HNAP request can crash admin web server on certain models with certain firmware versions
- Low impact vulnerability discovered by accident while trying to send a valid request
- The HNAP request format was taken directly from Cisco's own documentation

Curl Rules

```
curl http://192.168.1.70:80/HNAP1/ -v --basic \

--user  admin:admin -H \

'SOAPAction: "http://purenetworks.com/HNAP1/
GetWLanRadioSecurity"' \

--data @xml/GetWLanRadioSecurity.xml
```

```
<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope>
<soap:Body>
<GetWLanRadioSecurity xmlns="http://purenetworks.com/HNAP1/" />
</soap:Body>
</soap:Envelope>
```

Lame?

- Turns out to not be reproducible (my router was a DD-WRT upgrade)
- Certainly lame. However shows just how fragile these devices and protocols are
- What would happen if you were to actually fuzz HNAP?
- Release notes of firmware running on device say "Fixed HNAP issue"
- **However, there is no way to disable HNAP**

But Seriously, What Do We Do About It?

- I can show you embedded systems security fail until you are tired of hearing about it (which was probably 15 minutes ago or longer)
- I could go out and find more vulnerabilities and talk about them
- Some problems are implementation-based, nevermind a 0day (e.g. no HNAP disable)
- So how do we fix it?

I hope we can agree on one thing

Embedded systems security sucks!

Not even a giant pink binky will stop me from talking about it

www.securityfail.com

www.securityfail.com

- Used to redirect to ww.grc.com (Gigidy)
- It is now a public Wiki where people can write mini-articles on security failures
- First major section will be dedicated to embedded systems
- Write-in about how embedded security has failed you
  - 0Days are okay too, but not sure that will help
- Raise awareness and work to change the industry to implement better security on devices

www.securityfail.com

Some GOALS to get us started:

- We want vendors of embedded systems to:
  - FORCE the user to select the password
  - Allow users to disable protocols
  - Only enable secure management protocols by default (HTTPS, SSH)
- We want ISPs to:
  - Block inbound port 80 on user subnets
  - Manage customer devices properly and implement security

Sign up for an account

- Email me if you want an account in the mean time
- Or just send me your stories anonymously
- **This is a non-profit project**
  - Its sole purpose is to raise awareness and hopefully work with the industry to change

So what about World Domination?

TAKING OVER THE WORLD

There's an app for that.

PunditKitchen.com

Things I wanted to cover but ran out of space

- The "Chuck Norris" worm, which could a version of the psyb0t?
- Static analysis of device firmware, mounting the filesystems, finding vulnerabilities
- Analyzing video game systems, Tivo, and Blue-Ray players as they are network connected
- Wireless type worms and default Wifi settings
- Segmentation is just a band-aid

Don't Forget: http://www.securityfail.com

- **Presentations:** http://pauldotcom.com/presentations.html
- **Radio:** http://pauldotcom.com/radio
- **Live Stream:** http://pauldotcom.com/live
- **Forum:** http://forum.pauldotcom.com/
- **Mailing List:** http://mail.pauldotcom.com
- **Webcasts:** http://pauldotcom.com/webcasts
- **Insider:** http://pauldotcom.com/insider
- **Email:** psw@pauldotcom.com