AirBnB Beware:
short-term rentals, long-term pwnage

Presented by Jeremy Galloway 🌪️
Jeremy Galloway

I solve security problems -- occasionally there are computers involved. Current community affiliations include:

(ISC)$^2$ • ISSA • OWASP • OffSec
InfraGaurd • AHA! • HoneyNet
Tor Project • Citizen Lab • BSides
Internet Storm Center • SANS
SecurityTube • ShadowServer
Friends of the EFF • IEEE • OISF
Black Hat • BSDCWF • ISSW
Index of Cyber Security
The Satanic Temple

-REDITACTED-
The mission of The Satanic Temple is to encourage benevolence and empathy among all people. In addition, we embrace practical common sense and justice.
High-level takeaways
High-level takeaways

Short-term rentals have become so popular that their attack surface can no longer be ignored

Exposure to unsecured networks increases risk

Home networking hardware is worth targeting

The biggest threats are simple, not sophisticated

Most risk is mitigated when physical access to network hardware is restricted & VPNs are used
High-level takeaways

Short-term rentals have become so popular that their attack surface can no longer be ignored.

Exposure to unsecured networks increases risk.

Home networking hardware is worth targeting.

The biggest threats are simple, not sophisticated.

Most risk is mitigated when physical access to network hardware is restricted & VPNs are used.
High-level takeaways

Short-term rentals have become so popular that their attack surface can no longer be ignored

Exposure to unsecured networks increases risk

Home networking hardware is worth targeting

The biggest threats are simple, not sophisticated

Most risk is mitigated when physical access to network hardware is restricted & VPNs are used
High-level takeaways

Short-term rentals have become so popular that their attack surface can no longer be ignored.

Exposure to unsecured networks increases risk.

Home networking hardware is worth targeting.

The biggest threats are simple, not sophisticated.

Most risk is mitigated when physical access to network hardware is restricted & VPNs are used.
High-level takeaways

Short-term rentals have become so popular that their attack surface can no longer be ignored.

Exposure to unsecured networks increases risk.

Home networking hardware is worth targeting.

The biggest threats are simple, not sophisticated.

Most risk is mitigated when physical access to network hardware is restricted & VPNs are used.
High-level takeaways

Short-term rentals have become so popular that their attack surface can no longer be ignored.

Exposure to unsecured networks increases risk.

Home networking hardware is worth targeting.

The biggest threats are simple, not sophisticated.

Most risk is mitigated when physical access to network hardware is restricted & VPNs are used.
When things go Bump in the Network

[Origins of this talk]
Short-term rental market
Story time
Brave New World
The Sharing Economy
Brave New World
The Sharing Economy

I NEED...

YOU HAVE...

EFFICIENCY

TRUST
The emerging peer-to-peer, collaborative “sharing economy” will be a significant segment of the country’s future economic activity, stimulating new consumption, raising productivity and catalyzing individual innovation and entrepreneurship.

Brave New World
The Sharing Economy
PwC nailed it
AirBnB: Up, Up, and Away!
Short-term rentals are becoming more important in the US tourism industry.

One estimate puts the size of the domestic vacation rental market at $100 billion.

The number of people that have used a short-term rental has doubled in less than four years.
Short-term rentals are becoming more important in the US tourism industry.

One estimate puts the size of the domestic vacation rental market at $100 billion.
Short-term rentals are becoming more important in the US tourism industry.

One estimate puts the size of the domestic vacation rental market at $100 billion.

The number of people that have used a short-term rental has doubled in less than four years.
Short-term rentals are becoming more important in the US tourism industry.

One estimate puts the size of the domestic vacation rental market at $100 billion.

The number of people that have used a short-term rental has doubled in less than four years.
Let’s check those numbers again
Market Size in Billions (2015)

Short-term rentals shown in green
Airbnb Inc. lined up investors for a new funding round and an employee stock sale that will value the room-rental website at up to $30 billion and help defer an initial public offering, said people familiar with the matter.
NUMBER OF GUESTS STAYING WITH AIRBNB HOSTS DURING THE SUMMER

17M

2010 2011 2012 2013 2014 2015

0 5M 10M 15M

dataviz.com
More guests traveled on Airbnb this summer than the entire population of Greece, Sweden, or Switzerland.
Listings Targets everywhere

- Total Guests: 60,000,000+
- Cities: 34,000+
- Castles: 1,400+
- Countries: 191+
Listings Targets everywhere
Global Comparison:

350,000 Gas stations
187,000 Hotels
35,000 McDonalds
34,000 Subways
23,000 Starbucks
15,000 Burger Kings
11,500 Wal-Marts
Listings Targets everywhere

Listings Worldwide

2,000,000+
Airbnb Raises Over $100 Million as It Touts Strong Growth

Home-rental service posted $340 million of third-quarter revenue
Airbnb Raises Over $100 Million as It Touts Strong Growth

Home-rental service posted $340 million of third-quarter revenue

Exclusive: Airbnb to double bookings to 80 million this year - investors

SAN FRANCISCO | BY HEATHER SOMERVILLE
Airbnb Raises Over $100 Million as It Touts Strong Growth

Home-rental service posted $340 million of third-quarter revenue

Exclusive: Airbnb to double bookings to 80 million this year - investors

SAN FRANCISCO | BY HEATHER SOMERVILLE

Airbnb Raises $1.5 Billion in One of Largest Private Placements

Home-rental service valued at $25.5 billion
Airbnb overtakes hotel industry with red-hot growth

May 24, 2016, 2:06pm PDT   Updated May 25, 2016, 10:17am PDT

INDUSTRIES & TAGS   Travel & Tourism, Hospitality
Airbnb overtakes hotel industry with red-hot growth

May 24, 2016, 2:06pm PDT  Updated May 25, 2016, 10:17am PDT

INDUSTRIES & TAGS  Travel & Tourism, Hospitality

Airbnb's revenue soars 89 percent

Sep 1, 2016, 1:43pm PDT
Airbnb overtakes hotel industry with red-hot growth

May 24, 2016, 2:06pm PDT  Updated May 25, 2016, 10:17am PDT

INDUSTRIES & TAGS  Travel & Tourism, Hospitality

Airbnb's revenue soars 89 percent

Sep 1, 2016, 1:43pm PDT

Los Angeles landlords using Airbnb can make a year's income in 60 days, fuelling fears of housing crisis, says report

A new report from Inside Airbnb and the Los Angeles Alliance for a New Economy fuells fears that lucrative short-term lets are depriving the city of longer term lease, fuelling a housing crisis
Airbnb is growing in Ontario. There are more than 15,000 Airbnb hosts in the province, with 8,600 in Toronto. Over 7,600 bookings were made in Toronto in the first half of 2016.

Airbnb bookings data shows that hosts earn modest, but significant, amounts of supplemental income from hosting. The typical host earns $3,900 annually from their listing.

Airbnb’s host community in Ontario is composed of everyday people trying to pay the bills. More than half of our hosts in Ontario are women. 45 percent of our hosts are over the age of 40.
Revenue of AirBnB in New York City from 2010 to 2018 (millions)
Financial forecasting with Drizzy

tl;dr
Not every headline inspires confidence

Man allegedly burglarizes home after cancelling AirBnB reservation

It appears this is a new crime trend occurring in the Bay Area involving people renting out their homes via services such as AirBnb. Criminals are using these short-term rentals to steal valuables from the homeowners, cause damage to the residence, and obtain personal identifying information about the homeowners. Here are some tips that can help minimize the risk of becoming a victim:
Not every headline inspires confidence

These Startups Want To Be Airbnb Without Racial Profiling

October 4, 2016 // 07:00 AM EST
Airbnb hosts could be targeted by identity thieves: report

Though there isn't a direct link, 40% of survey respondents admitted to snooping while staying in homes they visit

June 29, 2016 08:30AM
WHAT TIME IS IT?

BUSINESS
Travel for work, feel at home

Be your best self when you’re on the road.

Link your work email to your account

Add Email
Corporate Ready

Travel Approved!
The perks of using Airbnb for Business

**It's easy to expense or charge work trips**

If your company is signed up for Airbnb for Business, you can charge trips directly to them.

**Stay at Business Travel Ready listings**

Stay with hosts who upgraded their services and amenities to welcome business travelers.

**Get $50 for any Airbnb stay**

On your first Airbnb business trip, we'll send you a $50 coupon for any Airbnb stay.
Biz-dashbord-pane-of-glass-2.0
Earn $50 in travel credit

Get a $50 travel credit, good for any Airbnb, when you check in for your first Airbnb business trip.

Link your work email to your account

Add Email
Corporate Ready

Concur & Airbnb: Bringing the Sharing Economy to Business Travelers
Whether traveling for business or pleasure, Tad Milbourn, chief executive of the San Francisco technology start-up Payable, stays at an Airbnb property whenever possible.

“It’s absolutely the coolest, being in someone’s house as opposed to a hotel,” he said. “And it’s superior, from the price, experience and novelty standpoint.”
Short-term rental biz be like
When was the last time you personally updated your router’s security?
Getting into the attacker mindset

SSID: AirBnBeware
Wireless Security: Open
Admin Pass: blank
Getting into the attacker mindset

Have
fun
Play
nice
😊
Google: dlink emulator

DIR-655 Emulator Selector - D-Link Support
support.dlink.com/emulators/dir655/
Please select an image below to access the desired emulator: DIR-655 Device UI · DIR-655 Device UI.
DIR-655 SecureSpot UI · DIR-655 SecureSpot UI.

EMULATOR | HOME - D-Link Support
support.dlink.com/emulators/dir615_revc/310na/tools_admin.htm
ADMINISTRATOR SETTINGS. The ‘admin’ and ‘user’ accounts can access the management interface. The admin has read/write access and can change ...

DAP-1522 Emulator Selector - D-Link Support
support.dlink.com/emulators/dap1522/
Please select an image below to access the desired emulator: DAP-1522 AP Mode · DIR-655 Device UI. DAP-1522 Bridge Mode · DIR-655 SecureSpot UI.
Scale of Trust

0 - Untrusted (yolo)

Somewhat trusted

100 - Mostly trusted
Scale of Trust

Your personal home network

Untrusted (yolo)       Somewhat trusted       Mostly trusted
Scale of Trust

A university network

0

Untrusted (yolo)  Somewhat trusted  Mostly trusted

100
Scale of Trust

Untrusted (yolo)      Somewhat trusted       Mostly trusted

Rando hotel kiosk

Untrusted (yolo)      Somewhat trusted       Mostly trusted
Scale of Trust

AirBnB rental network

Beware             Somewhat trusted       Mostly trusted
Local clients: laptops, desktops, phones

Home network

The internet

ISP
Countermeasures

Anti-virus
EMET (anti-exploitation)
End-point agent (telemetry)
Local security policies
Code signing

Local clients: laptops, desktops, phones
Countermeasures

Certificates
Firewalls
Bug bounties
HSTS / HPKP
Input filtering + validation
Local clients: laptops, desktops, phones

Home network

The internet

ISP
Countermeasures

Password protected admin panel
Lack of physical access
Countermeasures

- Password protected admin panel
- Lack of physical access
Unlike hosts that receive significant administrative security attention and for which security tools such as anti-malware exist, network devices are often working in the background with little oversight—until network connectivity is broken or diminished.

Malicious cyber actors take advantage of this fact and often target network devices. Once on the device, they can remain there undetected for long periods.
malicious hackers can gain full control of the network infrastructure enabling further compromise of other types of devices and data and allowing traffic to be redirected, changed, or denied. Possibilities of manipulation include denial-of-service, data theft, or unauthorized changes to the data.

Even if other compromised devices are detected, tracking back to a compromised infrastructure device is often difficult.

Malicious actors with persistent access to network devices can reattack and move laterally after they have been ejected from previously exploited hosts.
Exposure to unsecured networks
Sexual Exposure Calculator
How Many Partners Have You Been Indirectly Exposed to?

Type or select your location

Country: United States of America
State: TX
City: Austin

How many partners have you had? 7
On average, how many partners have each of your partners had before you? 4

Calculate Exposure
SEXUAL EXPOSURE: You have been indirectly exposed to 9,555 partners.

EQUIVALENT EXPOSURE: Your sexual exposure equates to 1.05% of the population of Austin, TX.

This equates to 96.70% of the population of Essex Junction, VT.
**SEXUAL EXPOSURE:** You have been indirectly exposed to **9,555** partners.

**EQUIVALENT EXPOSURE:**
Your sexual exposure equates to **1.05%** of the population of **Austin, TX**.

**Essex Junction, VT**
Exposure was derived using established formulas for a finite geometric series

\[ sexual\ exposure = n \left( \frac{1-n_p^6}{1-n_p} \right) \]

\( n = \text{number of partners you have had} \)

\( n_p = \text{number of partners your partners have had before you} \)
Think twice before having an unprotected ‘one network stand’
Scale of Trust

AirBnB rental network

Beware

Somewhat trusted

Mostly trusted
SoHo routers: A worthy target
Carna Botnet ~420K Clients 2012
“The vast majority of all unprotected devices are consumer routers or set-top boxes…”
INTEGO SECURITY ALERT - October 31, 2007
OSX.RSPlug.A Trojan Horse Changes Local DNS Settings to Redirect to Malicious DNS Servers
Operation Ghost Click
DNSChanger ~4M clients
2007-2011 ~$14M profit
CERT Polska 2013
DNS changing malware
MitM Polish online banking users
Real-World CSRF attack hijacks DNS Server configuration of TP-Link routers

document.writeln('<style type="text/css">@import url(http://admin:admin@192.168.1.1/userRpm/LanDhcpServerRpm.htm?dhcpserver=1&ip1=192.168.1.100&ip2=192.168.1.199&Lease=120&gateway=0.0.0.0&domain=&dnsserver=106.187.36.85&dnsserver2=8.8.8.8&Save=%B1%A3+%B4%E6);</style>')
More of the same in 2014 and 2015

“Web-based attack targeting home routers, the Brazilian way”

**PHISH PHARM: CYBERCRIMINALS USE PHISHING TO EXPLOIT ROUTER VULNERABILITIES AND CARRY OUT MAN-IN-THE-MIDDLE ATTACKS**
2014 continued

Attack campaign compromises 300,000 home routers, alters DNS settings

A Team Cymru EIS Report: Growing Exploitation of Small Office Routers Creating Serious Risks

 Powered by Team Cymru’s Threat Intelligence Group
Bizarre attack infects Linksys routers with self-replicating malware

Some 1,000 devices have been hit by the worm, which seeks out others to infect.

“The router situation is as touchy as a gasoline spill in an enclosed shopping mall.”

-Dan Geer
"Linux-based devices are again under the radar. This time, cyber criminals are infecting them with Mirai to carry out large-scale DDoS attacks."
Who’s getting pwned?

Top 10 #Linux devices involved to recent #telnet scanning activity by #ELF #botnet #DDoS #malware
pic from nic.cz
Abuse of Customer Premise Equipment

BHUSA 2014

Threats that abuse CPE (I)

The home router is a network proxy for most things on your home network

So own that and you control even well-defended devices on the home network

DNS changer botnet

- Attempted to reconfigure home router DNS server to only use adversary’s DNS server
- See FBI’s “Operation Ghost Click”
Average Paperclip Threat, The new APT
Ease of Attack:
I am APT and so can you!

APT: Average Paperclip Threat
Protected by lulz
Protected by lulz
R.I.P Your network security
R.I.P Your network security
What’s old is new again
What’s old is new again
Why target the network?
Why target the network?

"The network is the computer"

--John Gage of Sun Microsystems

circa early 1990s
Thought Experiment

Who is your favorite badass hacker?
Thought Experiment

How would you feel if they used your network at home, without supervision, for 24 hours, without restriction? 😈

And then you have to use the network after them? 😞
Home routers: Security not included
# Home routers: Security not included

[routerpwn.com](http://routerpwn.com)

<table>
<thead>
<tr>
<th>Home</th>
<th>Generators</th>
<th>Software</th>
<th>Hardware</th>
<th>Follow</th>
<th>Contact</th>
<th>About</th>
</tr>
</thead>
<tbody>
<tr>
<td>2Wire</td>
<td>Belkin</td>
<td>EE</td>
<td>Observa</td>
<td>Sitel</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3Com</td>
<td>Binatone</td>
<td>Fibrehome</td>
<td>Pirelli</td>
<td>SMC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alcatel-Lucent</td>
<td>Cisco</td>
<td>Freebox</td>
<td>Rom-O</td>
<td>Starbridge</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alpha-Networks</td>
<td>Cobham</td>
<td>Huawei</td>
<td>RugedddCom</td>
<td>Technicolor</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Arris</td>
<td>Comtrend</td>
<td>Linksys</td>
<td>Sagem</td>
<td>Thomson</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asmax</td>
<td>D-Link</td>
<td>MiFi</td>
<td>Seagate</td>
<td>TP-LINK</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asus</td>
<td>DD-WRT</td>
<td>Motorola</td>
<td>Siemens</td>
<td>TRENDnet</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Astoria</td>
<td>EasyBox</td>
<td>Netgear</td>
<td>Sitecom</td>
<td>Ubee / Ambit</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Show 50 entries

Search:

Show / hide columns
Tod Beardsley @todb · 30 Sep 2015

How to buy a new cable modem:

1) Look up ISP provider compat list.
2) Search model names on @metasploit .
3) Cancel cable.
<table>
<thead>
<tr>
<th>Date</th>
<th>D</th>
<th>A</th>
<th>V</th>
<th>Title</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016-09-13</td>
<td></td>
<td></td>
<td></td>
<td>ASUS DSL-X11 ADSL Router - Unauthenticated DNS Change</td>
<td>CGI</td>
</tr>
<tr>
<td>2016-09-13</td>
<td></td>
<td></td>
<td></td>
<td>COMTREND ADSL Router CT-5367 C01_R12, CT-5624 C01_R03 - Unauthenticated DNS Change</td>
<td>CGI</td>
</tr>
<tr>
<td>2016-09-13</td>
<td></td>
<td></td>
<td></td>
<td>PLANET VDR-300NU ADSL Router - Unauthenticated DNS Change</td>
<td>CGI</td>
</tr>
<tr>
<td>2016-09-13</td>
<td></td>
<td></td>
<td></td>
<td>Inteno EG101R1 VoIP Router - Unauthenticated DNS Change</td>
<td>CGI</td>
</tr>
<tr>
<td>2016-08-29</td>
<td></td>
<td></td>
<td></td>
<td>PLC Wireless Router GPN2.4P21-C-CN - Arbitrary File Disclosure</td>
<td>Rahul Raz</td>
</tr>
<tr>
<td>2016-07-25</td>
<td></td>
<td></td>
<td></td>
<td>Ubee EW3226 Modem/Router 1.0.20 - Multiple Vulnerabilities</td>
<td>Gergely Eberha.</td>
</tr>
<tr>
<td>2016-07-25</td>
<td></td>
<td></td>
<td></td>
<td>Technicolor TC7200 Modem/Router STD6.02.11 - Multiple Vulnerabilities</td>
<td>Gergely Eberha.</td>
</tr>
<tr>
<td>2016-07-11</td>
<td></td>
<td></td>
<td></td>
<td>Belkin Router AC1200 Firmware 1.00.27 - Authentication Bypass</td>
<td>Gregory Smiley</td>
</tr>
<tr>
<td>2016-06-27</td>
<td></td>
<td></td>
<td></td>
<td>Magnet Networks Tesley CPVA 642 Router - Weak WPA-PSK Passphrase Algorithm</td>
<td>Matt O'Connor</td>
</tr>
<tr>
<td>2016-06-15</td>
<td></td>
<td></td>
<td></td>
<td>Hyperoptic (Tilgin) Router HG23xx - Multiple Vulnerabilities</td>
<td>LiquidWorm</td>
</tr>
<tr>
<td>2016-04-27</td>
<td></td>
<td></td>
<td></td>
<td>Multiple Vendors (RomPager 4.34) - Misfortune Cookie Router Authentication Bypass</td>
<td>Milad Doorbash</td>
</tr>
<tr>
<td>2016-02-03</td>
<td></td>
<td></td>
<td></td>
<td>Viprinet Multichannel VPN Router 300 - Persistent Cross-Site Scripting</td>
<td>Portcullis</td>
</tr>
</tbody>
</table>
Backdoor Modules for Netgear, Linksys, and Other Routers

A week or so ago, I read the news of a new backdoor on several devices, including those made by Belkin, Cisco, NetGear, Linksys, and several others. A list of what seems to be affected devices can be found here. Eloi Vanderbeken, who posted his findings on GitHub made the original discovery. He also wrote a useful python proof-of-concept exploit, which allowed command injection, but I wanted Metasploit integration.
Home routers: Security not included

Compromising Embedded Linux Routers with Metasploit

Blog Post created by juan.vazquez on Apr 4, 2013
Home routers: Security not included

b1ack0wl @b1ack0wl - Oct 7
I'm staying at an Airbnb and I just saw this thing. I'm debating on pulling the firmware from it for uh, science! :D
Has your router been hijacked? How to check its settings

Check your router often to make sure it is safe to use

Posted on 2016/08/17 by Roland Waddilove in How-To, Internet, Security, Windows 10, Windows 7, Windows 8 // 0 Comments

Your computer and your router can be attacked by hackers and malware and they can cause havoc with your internet connection. You need to check your router asap to see if you have been compromised.
Router Checker is a free web-based tool you can use to check your device's connection to its DNS resolver, to make sure it is connecting to an authorized DNS server. A mismatch between the two may indicate DNS hijacking is underway.

To find out more about DNS hijacking and use the Router Checker tool, go to:
Router hacking: Child’s play, really

“I’m certain that there are other smart 15-year-old kids rounding up botnets of CCTV cameras that they can compromise and control” Matthew Prince, founder and CEO of Cloudflare

“They [PoodleCorp] love causing as much as chaos as they can” Cripthepoodle told Motherboard

crip @cripthedoodle · Oct 6
As most of you saw I was arrested by the FBI a couple hours ago and they seized all my stuff.... this is goodbye
If a bored teenager can hack your network, you’re in trouble

Anarchaos, aged 18, DEFCON 2004
If a bored teenager can hack your network, you’re in trouble

c0mrade, aged 15, NASA hacks, 1999
If a bored teenager can hack your network, you’re in trouble

Jake (not shown), aged 14, Call of Duty 2, 2011
Scale of Trust

AirBnB rental network

Beware Somewhat trusted Mostly trusted

0 100
Attacks
Attacks:
Potential impacts of a compromised network

“...exposure of sensitive information, modification of trusted data, and injection of data.”
Attacks
Remote Administration

ADMINISTRATION

Enable Graphical Authentication: ✓
Enable HTTPS Server: ✓
Enable Remote Management: ✓
Remote Admin Port: 37961
Use HTTPS: ✓
Remote Admin Inbound Filter: remote_hack_adm
Details: Allow 54.0.0.0-54.255.255.255
Attacks
Remote Administration

<table>
<thead>
<tr>
<th>Name</th>
<th>Action</th>
<th>Remote IP Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>remote_hack_adm</td>
<td>Allow</td>
<td>54.0.0.0-54.255.255.255</td>
</tr>
</tbody>
</table>

OPSEC++
Attacks
Just listen and wait

SYSLOG

The SysLog options allow you to send log information to a SysLog Server.

Save Settings  Don't Save Settings

SYSLOG SETTINGS

Enable Logging To Syslog  ✔
Server :

Syslog Server IP Address : 54.108.43.111  <<  Computer Name
Attacks
Just listen and wait
Attacks
Download router config to extract credentials

SYSTEM -- BACKUP SETTINGS

Back up DSL Router configurations. You may save your router configurations to a file on your PC. Note: Please always save configuration file first before viewing it.

Backup Settings
Attacks
Download router config to extract credentials

ISP
ADSL
L2TP
PPTP
PPPOE
DDNS
WEP/WPA
Login
**Attacks**

**Malice Level: Troll**

**Website blocking**

---

### 40 -- WEBSITE FILTERING RULES

Configure Website Filter below:

DENY computers access to ONLY these sites

---

Clear the list below...

---

<table>
<thead>
<tr>
<th>Website URL/Domain</th>
<th>Website URL/Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facebook.com</td>
<td>Google.com</td>
</tr>
<tr>
<td>Youtube.com</td>
<td>Amazon.com</td>
</tr>
<tr>
<td>Wikipedia.org</td>
<td>Twitter.com</td>
</tr>
</tbody>
</table>
Attacks
Malice Level: Troll
Parental Controls

PARENTAL CONTROL
Options to improve the speed and reliability of your Internet connection, to apply content filtering and to protect you from phishing sites. Choose from pre-configured bundles or register your router with OpenDNS® to choose from 50 content categories for custom blocking.

Save Settings | Don't Save Settings
Attacks
Malice Level: Troll
Reducing speed

WAN TRAFFIC SHAPING

Enable Traffic Shaping: 

Automatic Uplink Speed:

Measured Uplink Speed: Not Estimated

Manual Uplink Speed: 128 kbps

Connection Type: Cable Or Other Broadband Network

Detected xDSL or Other Frame Relay Network: No
Attacks
Expose hosts on the DMZ
(outside of the router/firewall)

The DMZ (Demilitarized Zone) option lets you set a single computer on your network outside of the router. If you have a computer that cannot run Internet applications successfully from behind the router, then you can place the computer into the DMZ for unrestricted Internet access.

**Note:** Putting a computer in the DMZ may expose that computer to a variety of security risks. Use of this option is only recommended as a last resort.

**Enable DMZ:**

**DMZ IP Address:** 192.168.0.100

Computer Name
Attacks
Reducing security

WI-FI PROTECTED SETUP

Enable: 

Lock Wireless Security Settings:

Reset to Unconfigured

PIN SETTINGS

Current PIN: 42599500

Generate New PIN | Reset PIN to Default
Attacks
Control network time

AUTOMATIC TIME CONFIGURATION

Enable NTP Server: ✔️
NTP Server Used: time.trustme.com

<< Select NTP Server
Attacks
Firmware modification
Skill Level: Advanced

FIRMWARE UPGRADE

Note: Some firmware upgrades reset the configuration options to the factory defaults. Before performing an upgrade, be sure to save the current configuration from the Tools → System screen.

To upgrade the firmware, your PC must have a wired connection to the router. Enter the name of the firmware upgrade file, and click on the Upload button.
Attacks
Remote Administration (advanced)

TR-069 CLIENT -- CONFIGURATION

Inform

Inform Interval: 300
ACS URL: beware.trustme.com
ACS User Name: admin
ACS Password: ************

Connection Request Authentication

Connection Request User Name: admin-beware
Connection Request Password: ************
Attacks
Remote Administration (advanced) via TR-069
Attacks
MitM via route hop

ROUTING
This Routing page allows you to specify custom routes that determine how data is moved around your network.

Save Settings  Don't Save Settings

32--ROUTE LIST

<table>
<thead>
<tr>
<th>Name</th>
<th>Destination IP</th>
<th>Metric</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>MITM</td>
<td>0.0.0.0</td>
<td>1</td>
<td>WAN</td>
</tr>
<tr>
<td>Netmask</td>
<td>0.0.0.0</td>
<td>Gateway</td>
<td>54.109.87.19</td>
</tr>
</tbody>
</table>
### Attacks

#### MitM via route hop

<table>
<thead>
<tr>
<th>ROUTING -- STATIC ROUTE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allows you to manually configure special routes that your network might need.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Static Route</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>ROUTING -- DEFAULT GATEWAY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allows you to configure Default Gateway used by WAN Interface.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default Gateway</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>ROUTING -- RIP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allows you to configure RIP (Routing Information Protocol).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>RIP</th>
</tr>
</thead>
</table>
Attacks
MitM via route hop

root@kal:~/pcaps# tcpdump -i eth0 -vv
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
19:11:56.428040 IP (tos 0x0, ttl 64, id 29936, offset 0, flags [DF], proto UDP (17), length 55)
   kal.42545 > gateway.domain: [bad udp cksum 0x36dd -> 0xe0a!] 21475+ A? ipinfo.io. (27)
19:11:56.428151 IP (tos 0x0, ttl 64, id 29937, offset 0, flags [DF], proto UDP (17), length 55)
   kal.42545 > gateway.domain: [bad udp cksum 0x36dd -> 0x1129!] 13764+ AAAA? ipinfo.io. (27)
19:11:56.428575 IP (tos 0x0, ttl 64, id 29938, offset 0, flags [DF], proto UDP (17), length 71)
   kal.51365 > gateway.domain: [bad udp cksum 0x36ed -> 0xc0c7!] 8489+ PTR? 2.111.16.172.in-addr.arpa. (43)
19:11:56.453036 IP (tos 0x0, ttl 128, id 10500, offset 0, flags [none], proto UDP (17), length 103)
Attacks
Owning DNS

**DNS SERVER CONFIGURATION**

- Obtain DNS server address automatically
- Use the following DNS server addresses
  - Preferred DNS server: 54.16.108.32
  - Alternate DNS server: 8.8.8.8
When the attacker gains control of DNS
Owning DNS: Attacks

HTTP/S downgrade
Sniff plain-text creds (passive)
Pharming (FakeDNS)
WPAD abuse
Hash capture (http_ntlm)
BEEF hooks
Browser Autopwn2
Evilgrade (malicious updates)
BDFProxy (MitM binary patching)
Owning DNS: Attacks

# Modifying systems' DNS settings allows cybercriminals to perform malicious activities like:

# Steering unknowing users to bad sites:
# These sites can be phishing pages that spoof well-known sites in order to trick users into handing out sensitive information.

# Replacing ads on legitimate sites:
# Visiting certain sites can serve users with infected systems a different set of ads from those whose systems are not infected.

# Controlling and redirecting network traffic:
# Users of infected systems may not be granted access to download important OS and software updates from vendors like Microsoft and from their respective security vendors.

# Pushing additional malware:
# Infected systems are more prone to other malware infections (e.g., FAKEAV infection).
Owning DNS: Attacks

“If an attacker registers a domain to answer leaked WPAD queries and configures a valid proxy, there is potential to conduct man-in-the-middle (MitM) attacks across the internet.”
Owning DNS: Attacks

So many great options! How to choose?
Owing DNS: Attacks

No 0day ✓
Almost zero exploit code (!autopwn2) ✓
Pre-built tools ✓
Little infrastructure needed (AWS free) ✓
Attacks are cross-platform ✓
Attacks are easy to perpetrate ✓
Attacks can be passive + automated ✓
Attacks can be difficult to detect ✓
Logs of attacks can be easily wiped ✓
Owning DNS: Attacks
A very simple demonstration

DYNAMIC IP (DHCP) INTERNET CONNECTION TYPE:

Use this Internet connection type if your Internet Service Provider (ISP) didn’t provide you with IP Address information and/or a username and password.

Host Name: 
Use Unicasting: (compatibility for some DHCP Servers)
Primary DNS Server: 52.94.12.133
Secondary DNS Server: 8.8.8.8
MTU: 1500 (bytes) MTU default = 1500
MAC Address: a0:99:9b:0b:e1:f1

Clone Your PC's MAC Address
Owing DNS: Attacks
Captive portal NTLM hash capture
Owning DNS: Attacks
Captive portal NTLM hash capture
Wide range of attack styles, can vary from:

- Nuanced to Direct
- Subtle to Aggressive
- Opportunistic to Persistent
- Generic to Personalized
- Simple to Sophisticated
- Passive to Invasive
- Annoying to Devastating
Attacker types

- Bored teen
- Tech savvy miscreant
- Trolls
- Grey hat
- Full blown black hat
- Hacktivist
- Evil property owner
- Motivated criminal
- Opportunistic criminal
Semi-targeted attacks

Conferences
Tradeshows
Sporting events
Specific locales (DC Beltway, Silicon Valley)
Holiday destinations
High end rentals for high end targets
Near military bases
Near corporate offices
How would you target?
Attacks
Owning DNS
How ICANN secures your DNS

Locked cages, seismic sensors, smartcards, cameras, EMF blocking, safes, iris scanning
How you secure your DNS

Kittens, wishful thinking, lulz
How you secure your DNS Security?

‘Compu’er says no’
Understanding risk
Understanding risk
Not so much...
Understanding risk
Much, much, more likely
Software exploits overrated - it's the humans you need to be watching

Dumb passwords and phishing the main threats

22 Aug 2016 at 17:54, John Leyden
Exploits and 0dayz are cool, but Credential Theft is the trend

The data set includes 100 separate internal penetration test engagements spanning 75 unique organizations.

The top four attack vectors are based on utilizing stolen credentials. This is a serious problem because credential theft will always work as long as the credentials are valid.Credential theft is highly reliable, repeatable, and has a low likelihood of negative impact for an attacker.

PRAETORIAN GROUP
Roaming Workers Exposed When They Don’t Turn on the VPN
Brought to you by OpenDNS

In a recent study, IDG reveals that roaming workers are consciously and unconsciously sidestepping corporate VPNs in the name of convenience. The risk is great as workers mobilize, using laptops to access sensitive data and cloud-based applications. In this informative webcast, we dive into the specifics of the research—what security measures are working and what aren’t. You’ll walk away with learned advice and a proven path to mitigating the risks of an ever-roaming workforce.
Traditional approaches to security—firewalls, proxy servers and anti-virus solutions—are simply not enough to avoid off-network security issues.

74% experienced security issues as a result of off-network usage

More Remote Users = More Security Issues
(75% of laptop users or more)  (35% of all IT security issues)
Protecting yourself
Mitigations for renters (technical)
Hardcode DNS in all devices
Mitigations for renters (technical)
Hardcode DNS in all devices
Mitigations for renters (technical)
Ensure ‘Automatic proxy setup’ is disabled
Mitigations for renters (technical)
Ensure no unknown proxy is in use
Mitigations for renters (technical)
Trusted Free VPN
Mitigations for renters (technical)
Trusted Free VPN (w/limits)

Desktop
- Mac
  - Mac 64-bit OS X 10.6.8 and later
  - What's New
- Windows
  - Windows Vista and later
  - What's New

Mobile
- iOS
  - iPads and iPhones with iOS 7 and later
- Android
  - Android 4.0.1 and later

Browser Extensions
Lightweight extensions that only tunnel data inside your browser.

- Chrome
  - For Chrome Browser 22+ on Windows, OS X, Linux and Chrome OS
- Opera
  - For Opera Browser on Windows and OS X
Mitigations for renters (technical)

Trusted Free Mobile VPN

**Opera Free VPN – Unlimited Free VPN with Adblock**

*By Opera Software ASA*

**Description**

Opera VPN blocks ads and lets you change your virtual location. Unblock more content and stop trackers from following you around the web — completely free.

[View More by This Developer](https://store.example.com)

**What’s New in Version 1.1.1**

Fixed a critical bug affecting iPad.
Mitigations for renters (technical)
Corporate VPN***

Ensure WPAD/Proxy settings are correct

Corp VPNs typically use split-tunneling, which may leave large amounts of traffic unprotected
Mitigations for renters (technical)
Corporate VPN***
Mitigations for renters (technical)
Use mobile apps off WiFi
Mitigations for renters (technical)
Tether to 4G/LTE
Mitigations for renters (technical)
Never use plain-text auth

HTTP
FTP
Telnet
POP3
SMTP
LDAP
VNC
Mitigations for renters (technical)
2FA/MFA everything you care about
https://twofactorauth.org

Two Factor Auth (2FA)
List of websites and whether or not they support 2FA.
Add your own favorite site by submitting a pull request on the GitHub repo.
Mitigations for renters (behavioral)

Watch Mr. Robot
Mitigations for renters (behavioral)
Be skeptical and aware when travelling
Mitigations for renters (behavioral)
Demand HSTS + HPKP from providers
Mitigations for renters (behavioral)

Ask yourself:

When is it okay to *not* use a VPN?
When is it okay to *not* use a VPN?

Public WiFi risks are well-known, but few use VPN to increase security

Chris Talbot @northerntalbot
Published: August 19th, 2016

The risks associated with using public WiFi hotspots appear to be well understood, but that doesn’t stop the average person from using such access points without appropriate security measures in place.
Mitigations for owners
Remove physical access to hardware

Lock in a closet or secure room
Mitigations for owners

Remove physical access to hardware

Alert (TA16-250A)
The Increasing Threat to Network Infrastructure Devices and Recommended Mitigations

Original release date: September 06, 2016 | Last revised: September 28, 2016

- Implement robust password policies and use the strongest password encryption available.
- Protect router/switch by controlling access lists for remote administration.
- Restrict physical access to routers/switches.
- Backup configurations and store offline. Use the latest version of the network device operating system and update with all patches.
Mitigations for owners

Remove physical access to hardware
Lock in a closet or secure room (like R. Kelly)
Mitigations for owners
Remove physical access to hardware
Lock in an electronics enclosure
Mitigations for owners
Remove physical access to hardware
Lock in an electronics enclosure
Mitigations for owners
Remove physical access to hardware
Don’t offer internet access (gasp!)
Mitigations for owners

Never share your personal WiFi connection
Mitigations for owners
Backup and restore router settings routinely

<table>
<thead>
<tr>
<th>SYSTEM -- BACKUP SETTINGS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Back up DSL Router configurations. You may save your router configurations to a file on your PC.</td>
</tr>
<tr>
<td><strong>Note:</strong> Please always save configuration file first before viewing it.</td>
</tr>
<tr>
<td>Backup Settings</td>
</tr>
</tbody>
</table>
Mitigations for owners

Add an ‘Online Safety’ section to your Guest Welcome Guide
This is not going away any time soon
This is not going away any time soon

RFP discloses SQL injection in 1998
‘Year of the Breach’ 2011 - ?

---[ Phrack Magazine  Volume 8, Issue 54 Dec 25th, 1998, article 08 of 12

------------------------[ NT Web Technology Vulnerabilities

--------[ rain.forest.puppy / [WT] <rfpuppy@iname.com>

*Note: most of the vulnerabilities in this document have NOT been made public; they were discovered by rain.forest.puppy, or other members of WT. Lots of new toys out there on the Internet lately. Seems like the web is the way to go, and every software spigot is demanding they be 'web-enabled'. A lot are reinventing the wheel, bundling sub-standard web servers to serve up their HTML and Java interface.
This is not going away any time soon
There is no patch, update, or easy fix
So what’s the ‘REAL Solution™ ’?
So what’s the ‘REAL Solution™ ’?

Better software on our networking hardware by holding vendors accountable
So what’s the ‘REAL Solution™ ’?

This cannot be the accepted norm:

ABBA-solutely crapulous! Swedish router-maker won't patch gaping hole

Inteno says SOHOpeless security problem should be fixed by carriers
So what’s the ‘REAL Solution™ ’?
This cannot be the accepted norm:

This Chinese Router Is Depressingly Insecure and Downright Evil

Is this the most insecure router in the world? Probably yes.

Aug 22, 2016 04:30 GMT · By Catalin Cimpanu · Share: ·

A Wi-Fi router manufactured and sold only in China by BHU contains so many security holes that you're looking for trouble every time you plug it in and exposing it to the Internet.
Conclusion & Takeaways

Be skeptical and stay aware when traveling, whether or not you stay at a rental

If the network is untrusted, use a VPN or 4G/LTE mobile network

Be cautious of ‘one network stands’

‘Average Paperclip Threats’ (APTs) are simple, but potentially devastating

Remove physical access to hardware if you ♡ security
Homework

Ask security pros and hackers at SecTor if they would use an AirBnB network without a VPN.

Ask how they secure their own devices when using random, unknown, or untrusted networks.
Thank you for your time!
FIN
Free Edward Snowden
Free Julian Assange
Free Chelsea Manning
Free Jeremy Hammond
Free All Political Prisoners
Cheers

JeremyNGalloway at gmail
EcstaticSec.tumblr.com