Turning your IoT against you

Jill Peterson & Richard Frovarp

Disclaimers

Insert standard security presentation disclaimer here...

We’re not speaking on behalf of NDSU.

Our opinions do not represent NDSU.

Stuff like that.
“If they're getting valuable enough stuff from you, at least the organized crime folks have an incentive to issue regular updates to keep the appliance working after the manufacturer discontinues support.”

xkcd.com/1966
Use This


US $3.23

Compromise credentials

https://www.youtube.com/watch?v=GDv9Nvcw4O4

Remote Access, Local Fix

- 2015 Jeep Cherokee
- Remotely control wipers, AC, music, abruptly engage brakes, disable brakes, kill engine, disengage transmission, control steering wheel (while in reverse)

- After 9 months, Chrysler Announced a fix: deployed via USB stick

Default Passwords - Mirai

- Default passwords in IoT devices, largely cameras
- Launched a 620 Gbps attack against krebsonsecurity.com Sept 20, 2016
- Can install malware, harvest credentials, monitor location
- Will cover UPnP later in this talk
- Attack upstaged by memcached amplification attack against GitHub at 1.3 Tbps, have seen 1.7 Tbps
  - Out of scope of presentation, but unauthenticated UPD and on the public Internet
802.11i-2004 WPA2 PSK

- Devices browse channels and see if SSID is available
  - Hidden networks can’t hide the traffic or SSID from the traffic
- Four way handshake doesn’t transmit password, it uses PMK
- Generate the PMK
  - PMK = PBKDF2(HMAC-SHA1, PSK, SSID, 4096, 256)
  - SSID = Netgear, PSK = Password
  - PMK = 3521f5222de277eb5e98a5116087ed3ba613d399cd7f454bf7ed649ab1323
- Use a rainbow table: www.renderlab.net
  - 33Gb : 1 million passwords against 1000 SSID’s, download or order for $50 + shipping

Some SSIDs

airportthru
130
workgroup
mobile
HomeOffice
test
fa1779zypo
Harvard University
72653
HOMENETWORK
USR9106
linksys1
NETWORK
My Wireless Network A
5ECURy3p5TOR3
conexant
SMARTSIGHT
Guest
0CP2REDsoX
public
Truckstop.net
D-LINK
UBC
G604T_WIRELESS
WiFi - Analogy Time

- It's like you're walking around with your keys out
- Asking everyone if they are your roommate
- Sooner or later you'll find someone who is either up to no good or bored who will say yes

Pineapple
**UPnP (Universal Plug and Play)**

- Allows for discovery and interoperability between devices on a network
- Standards for interoperability of devices
  - Media servers are a great example
- Can also manipulate networking gear
  - Internet Gateway Device Protocol
  - Learn public IP address
  - Request a new public IP address
  - Enumerate existing port mappings
  - Add and remove port mappings
  - Assign lease times to mappings

---

**Simple Service Discovery Protocol (SSDP)**

```
M-SEARCH * HTTP/1.1
HOST:239.255.255.250:1900
ST:ssdp:all
MX:2
MAN:"ssdp:discover"

IP: 239.255.255.250
Port: 1900
```
Hue

('192.168.2.47', 1900) HTTP/1.1 200 OK
HOST: 239.255.255.250:1900
EXT:
CACHE-CONTROL: max-age=100
LOCATION: http://192.168.2.47:80/description.xml
SERVER: FreeRTOS/7.4.2 UPnP/1.0 IpBridge/1.16.0
hue-bridgeid: 001788FFFE180F63
ST: upnp:rootdevice
USN:
uuid:2f402f80-da50-11e1-9b23-001788180f63::upnp:rootdevice

Belkin Wemo

Unauthenticated HTTP

xmlns:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
<s:Body><u:SetBinaryState xmlns:u="urn:Belkin:service:basicevent:1"><BinaryState>1</BinaryState></u:SetBinaryState>
</s:Body></s:Envelope'
http://$IP:$PORT/upnp/control/basicevent1
Detour

- Fauxmo
  - Appears as a Belkin WeMo on the network
  - Allows you to execute arbitrary code for on and off actions
  - Thus is discoverable and directly callable from Amazon Echo’s
- [https://github.com/makermusings/fauxmo](https://github.com/makermusings/fauxmo)
- [node-red-contrib-wemo-emulator](https://github.com/makermusings/fauxmo)

Mesh Networks

- Communicates via open spectrum or powerlines
  - 2.4 GHz (Zigbee), 915 MHz (Insteon & Z-Wave)
- Devices can communicate with each other without a central controller
- Each device will repeat messages
- So adding a new device typically strengthens the network, as more paths from point A to point B exist
- Communication takes place outside of TCP/IP, WiFi, or anything else monitoring your network
Zigbee

- Mesh network operating on 2.4 GHz
- Controlled by the Zigbee Alliance
- Range of 70m indoors and 400m outdoors
- AES 128 encryption

Zigbee Light Link

- Interoperability specification for Zigbee
- Creates a Personal Area Network (PAN)
- Used by Philips Hue
- Latest version has a proximity test to prevent resets from long distances
- Factory reset includes Inter-PAN transaction identifier, specifies a non-zero random number
  - Obvious question becomes, what happens when you use zero?
Take Over a Light

- Eyal Ronen
- Factory reset message with ID = 0
- Light restarts, and comes back up in a compatibility mode for an older version of the protocol that doesn’t include the proximity test.

Light Worm

- Continuing to look at Hues
- Firmware updates are signed with a symmetric key
- Use multiple attacks to extract key
- Generate own firmware
- Sign it
- Distribute it
- Lights will push it out to each other
  - 15,000 randomly distributed lights in Paris to control city
- Profit
- IoT Goes Nuclear: Creating a Zigbee Chain Reaction
INSTEON

- Simulcast dual-mesh network (915 MHz US RF, 131.65 KHz powerline)
- RF range 150 feet unobstructed
- Each device assigned unique 24-bit ID number during manufacture
- Supports messages with encryption such as AES-256; HOWEVER
  - INSTEON Hub does not use encryption
  - Nodes not robust enough to use encryption

Replay

- Insteon Garage Door Control Kit configured via an Insteon Hub
- Using software-defined radio (SDR), the 915MHz radio signal used to open and close the door via the Garage Door Control device was captured
- The signal was filtered to remove background noise
- The signal was replayed to successfully actuate the Insteon Garage Door Control device

Insecure credential storage in app
Z-Wave

- Routed mesh network operating on 908 MHz (US)
- Open internationally recognized ITU standard, represented by the Z-Wave Alliance
- Network range up to about 400 feet
- One chip manufacturer (Sigma Designs)

S2 framework (required for smart devices, controllers, gateways, and hubs beginning 2 April 2017):

- Elliptic Curve Diffie–Hellman (ECDH) key exchange
- Tunneling over IP (Z/IP) through TLS 1.1 tunnel for cloud communication
- Uses a QR or pin code on the device for unique device authentication

At 2013 Black Hat, security experts demonstrated the theoretical hacking (on non-production devices with key-exchange problems) of Z-Wave smart locks and motion sensors to break into a home.

The Z-Wave Alliance invited these researchers to help design Security 2 (S2) framework.

Then they made the spec public.
Bluetooth

- Point-to-point ad-hoc wireless network in 2.4 GHz band
- Range of about 10 meters

Pairing

- Two sided
  - Enter a code on both sides
- One sided
  - Enter code displayed on device into phone
  - Although it might just be 0000 or 1234, which really isn’t any more secure than Just Works
- Out of Band
  - NFC is popular
- Just Works
  - No PIN or any other controls

Fender Mustang

MUSTANG™ GT 100
shop.fender.com $399.99
What could go wrong?

Bluetooth on everything

- Can be used to track locations of devices using app, kind of like Tile
- Can be used to modify torque settings
- Security problems were discovered by Mark Loveless from Duo Security.
  - Milwaukee ignored requests
  - Researcher escalated to US CERT
  - Minimal response back to US CERT

milwaukeeetool.com/
Speaking of Tracking Tags

- Can be identified with a simple Bluetooth scanner
- Allows unauthenticated connections - pretty much by design
- Some allow unauthenticated posting of location data
- Even worse some allow unauthenticated requests of location data
- Some allow changing attributes via simple scanner. No idea what those attributes do.

Bluetooth Scanner
Properties

NFC - Near Field Communications

- NFC card emulation
  - Think payments
- NFC reader / writer
  - Can write information to simple tags or read that information
- NFC peer to peer
  - Used to exchange information in adhoc manner
  - Is used to exchange Bluetooth pairing information
Prox

- Fairly uncommon in residential deployments
  - Might show up for gym access or underground parking garage fobs
- No encryption and no security

IFTTT

ADT Pulse proposed a channel on IFTTT with “recipes” like

- Armed away triggers energy-saving thermostat change
- If doorbell rings, send a real-time video clip of the front door
- If wearable changes from sleep to awake, **disarm security system**
- If a user texts “dog door,” then **unlock the back door**

*channel not yet created, so users observed to use workarounds via email/subject triggers*
Subaru

- Very simple incrementing code on keyfob
- Raspberry Pi + RLT-SDR RTL2832U DBV-T tuner = success
- Intercept keypress
- Increment code value
- Resend
- Will prevent fob from working for N presses
- Could overflow max number
- Tom Wimmenhove – GitHub

Privacy implications

- Consumer doesn’t know who is doing the ‘smart’ part of the device
- Vendors might share knowledge--home layout from smart vacuum
- Sometimes, metadata is the message
  - After two months of data collection, I was able to pick up a bunch of insights into the Hill household—what time they wake up, when they turn their lights on and off, when their child wakes up and falls asleep—but the weirdest one for me personally was knowing when Kashmir brushes her teeth. Her Philips Sonicare Connected toothbrush notifies the app when it’s being used, sending a distinctive digital fingerprint to the router. While not necessarily the most sensitive information, it made me imagine the next iteration of insurance incentives: Use a smart toothbrush and get dental insurance at a discount!

The House that Spied on Me
Privacy - VTech

- Toy manufacturer, with toys sending data back to their systems
- Shown to be vulnerable in 2015 due to SQL Injection, SQL statements returned in XML response body
- Dumped images, chat messages, audio recordings, passwords (single round MD5) for 3 million children
- To cover, updated terms of service: https://www.troyhunt.com/no-vtech-cannot-simply-absolve-itself/

“YOU ACKNOWLEDGE AND AGREE THAT ANY INFORMATION YOU SEND OR RECEIVE DURING YOUR USE OF THE SITE MAY NOT BE SECURE AND MAY BE INTERCEPTED OR LATER ACQUIRED BY UNAUTHORIZED PARTIES.”

- FTC - ~22 cents per child judgement in January 2018

Troy Hunt: www.troyhunt.com
WE MAY STARVE YOUR DOG OR CAT

PETNET SMARTFEEDER
Automatic pet feeder for dogs and cats.
Make sure your pets are always fed when you're away.
BUY NOW $119.94
Watch video

WARNING
You acknowledge and agree that the survival of Fido / Fluffy is directly dependent on the reliability of your home internet connection and the availability of our online services.

Troy Hunt: www.troyhunt.com

Contact us

Jill Peterson
jill.e.peterson@ndsu.edu

Richard Frovarp
richard.frovarp@ndsu.edu