Device Connection: Security design in the Age of IoT

Presented by:
Alex Fagundes
PowerObjects, An HCL Company
Who am I?

Director of Architecture – PowerObjects, an HCL company
10 years at PowerObjects
Focus on CRM & Cloud architecture and design
CISSP/CISSA 10 years ago
No affiliation with any of examples or findings Nissan/Netgear/Etc

Who is PowerObjects, an HCL Company
Over 400 employees
Design / Implement / Consult
Dynamics 365/CRM
Implementations now involving IoT
Part of HCL – 100K employees India based services company
Why am I here?

- Nothing to sell
- Interest in Security & IoT
- 3 goals
  1. 5 simple design principals for IoT
  2. Increase awareness of mass quantities of insecure IoT
  3. See something insecure, say something
     - These devices are all over the place – even Timbuktu

Tweet along: #Sec360

www.Secure360.org
Agenda

• IoT Trends
  • Why now?
  • Are we creating a dormant monster?
• 5 must have design principals
• Side stories
  • The day the internet stopped
  • Nissan Leaf Connected App
  • Few stories?
    • Dlink
    • Asus

Tweet along: #Sec360
www.Secure360.org
IoT Trends

- 2015 – 6 billion connected devices
- 2020 – 20 billion connected devices
  - IoT devices – more than half consumer IoT devices

Consumer devices
- Thermostats, TVs, Dvds, cars, security systems...
- Refrigerators – control temp, ice maker, etc from app
- Printers – notify via email when low
- Deck Led lightning, lights, etc
- Cars
  - etc

Business / Industrial
- Building controls systems
- All types of sensors
- Red light sensors
  - etc

Tweet along: #Sec360  
www.Secure360.org
Why the increase in IoT

- Inexpensive to add functionality
  - Raspberry Pi – 1 GB ram, Wifi, etc - $39.95
  - Amazon IoT Platform - https://aws.amazon.com/iot
  - Microsoft Dynamics CRM – built-in functionality
  - etc

- Consumers see a value add or demand it
  - Baby monitors, cameras, smart thermostats, etc
  - Coffee make with smartphone app
  - Deck LED lights
  - Wifi cameras – almost all have app/remote connectivity

Tweet along: #Sec360 www.Secure360.org
Why the increase in IoT

Industry as a whole

• More efficient
  • Vending machine notifies when inventory is low
  • Detect a leaking roof before you see water
  • …

• Decrease down time
  • Air pump phones home with issues
  • Change machine uploads remaining coins
  • Proactive send data
  • Tesla – proactively notify owner of xyz maintenance needs
  • …
With the increase of IoT

- Businesses - Can ship before software is ready
  - Ship with beta software / non working functionality
  - Easy to update later
  - Example - Tesla, My Samsung TV, etc

- Businesses - Proactively engage and ‘know more’ about your consumers
  - Printers & cartridge re-fil
  - What features being used / not used
  - Gain lots of insight/knowledge
    - Example – Amazon Alexa
    - Smart TVs – Are they monitoring what you watch?
      https://www.theverge.com/2017/2/7/14527360/vizio-smart-tv-tracking-settlement-disable-settings

**Samsung:** Samsung has an opt-in tracking service, called SyncPlus, that may have been turned on when your TV was set up. Option to disable it is located in the settings menu, hidden inside the “Terms & Policy” section.
What’s the problem?

• Consumers are happier
• Business do better
• Less work for everyone
• Things are more proactive
• The world is more connected
• Everyone is happy

"SO, WHAT'S THE"

PROBLEM??

www.Secure360.org
What’s the problem?

- Tons of vulnerable devices
  - With poor security
  - Devices pieced together from different vendors
  - No one patching
  - All over the place

- 170MM Exposed IoT in 10 Major US cities
  - Many lack basic security
Disclaimer

• Everything in this presentation is for informational purposes
• Don’t do bad stuff
• Hacking is illegal

Tweet along: #Sec360
www.Secure360.org
What’s the problem?

• That many? No way
• Lets check live
• https://Shodan.io and https://censys.io
  • Searchable Inventory of all Internet Connected Devices
  • March 16 2017 – IpCamera ‘Go Ahead Vulnerability’
    • Go Head server code is ok, but vendor implementing introduced vulnerability
  • 2 out of 10 have default credentials
  • 180K vulnerable cameras March 16 2017
  • Now?

https://www.shodan.io/search?query=GoAhead+5ccc069c403ebaf9f0171e9517f40e41
What’s the problem?

- Shodan Search engine – what else we seeing?
  - Billy Rios – found 1819 building management
  - Red-light cameras
  - All kinds of sensors

- My findings
  - Lots of vulnerable switches/routers
  - Lots of open/vulnerable ip cameras
  - Tons of devices that should NOT be internet facing

Short Demo: https://www.shodan.io/search?query=GoAhead+5ccc069c403ebaf9f0171e9517f40e41

Forbes Shodan Article
https://www.forbes.com/sites/kashmirhill/2013/09/05/the-crazy-things-a-savvy-shodan-searcher-can-find-exposed-on-the-internet/#112f4b5e3c7e
What’s the problem?

- Censys – [https://censys.io/about](https://censys.io/about)
  - Good or bad idea
  - Is your IP listed? Search: ip:xxxxxx
    - Or network, or more complex queries
  - Search your neighbors/block
  - Easy to query – Query by vulnerability
  - ‘Hacker Friendly’ ?
  - More info
- [https://krebsonsecurity.com/tag/censys-project/](https://krebsonsecurity.com/tag/censys-project/)
- [https://blog.kaspersky.com/shodan-censys/11430/](https://blog.kaspersky.com/shodan-censys/11430/) - Censys Vs Shodan

Tweet along: #Sec360

www.Secure360.org
5 IoT Design Principals
for both (consumer & business)
IoT Design – Two common design patterns:

- Two common pattern in the IoT world

a. Serverless / no middle tier
   Dvd players, Tvs, Balcony lights, Printers, IP Cameras, building control systems, windmills, etc

b. Server based / Middle tier
   Thermostats, Cars, Alarm System, Cameras – home and industry devices
IoT Design Principal 1 - Authenticate

- Authenticate! Period.
  - If sending non-public information must authenticate
  - If connecting to a device must authenticate
    - User Name/Password
    - Private/Public Key
    - Random Gen before shipping

Tweet along: #Sec360
www.Secure360.org
IoT Design Principal 1 - Authenticate

• Consumer devices
  • No authentication leaves vulnerable to exploits
  • Vulnerable to loss data or damage
  • Most homes have vulnerable devices or have devices with default credentials
  • Later example – the day the Internet Crashed

Nissan Leave – Troy’s blog
https://www.troyhunt.com/controlling-vehicle-features-of-nissan/
IoT Design Principal 1 - Authenticate

• Nissan Leave
  • Best Selling EV in the world
  • 250K Leaves in the world as of Dec 2016
  • App – driving history (2 years driving, charging, climate, …)

Nissan Leave – Troy’s blog
https://www.troyhunt.com/controlling-vehicle-features-of-nissan
IoT Design Principal 1 - Authenticate

• How did a Nissan Leaf Mobile App authenticate?
  ★ A. No authentication
  ★ B. Every car had a sequential number
  ★ C. VIN number
  D. Public/Private key

The API:
https://canada.nissanconnect.com/owners/leaf/setHvac?vin=1N4A.....5520&fan=on

Nissan Leave – Troy’s blog
https://www.troyhunt.com/controlling-vehicle-features-of-nissan/
IoT Design Principal 1 - Authenticate

• Nissan app – back online – down for 2 months
• What could have happened?
  • Iterate thru VINs – heat up ALL cars to 90 degrees?
  • Iterate thru VINs - Download driving history – past 2 year
  • Nothing super bad - No physical damage
• Any others?

Chrysler Jeep
https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
“Uconnect’s cellular connection also lets anyone who knows the car’s IP address gain access from anywhere in the country.”

The fix – All vehicles affected need to be patched via USB stick
IoT Design Principal 2 – No Defaults

• Serverless architecture
  • Still needs good security architecture
  • No default logins
  • No default back doors

• In this day and age – default credentials?
  Example: FTC vs Dlink – Jan 2017


• Baby monitors, home grade wifi/routers, my cheap zone free dvd player from ebay shipped directly from Quanzhou
IoT Design Principal 2 – No Defaults

- Have you scanned your home network?
- Download Nessus – free for home usage

<table>
<thead>
<tr>
<th>Host</th>
<th>Vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.11.22</td>
<td>38</td>
</tr>
<tr>
<td>192.168.11.1</td>
<td>23</td>
</tr>
<tr>
<td>192.168.11.4</td>
<td>7</td>
</tr>
<tr>
<td>192.168.11.2</td>
<td>1</td>
</tr>
<tr>
<td>192.168.11.6</td>
<td>1</td>
</tr>
</tbody>
</table>
IoT Design Principal 2 – No Defaults

• This must be industry standard:
  Force pwd change during setup
  Never allow a default to remain

RESET YOUR PASSWORD

Enter new password

Re-enter new password

RESET
IoT Design Principal 2 – No Defaults

- Are things that bad?
- Yes – In addition to cameras/dvd players/etc/certain home grade wifi routers
- My favorite Dlink – Example DWR-932B – 20 vulnerabilities
  - Slick little router – fancy package – lots of features
  - Default – admin / 1234 – unchangeable
  - Send UDP HELODBG – root access via telnet
  - HTTP deamon vulnerable
  - Hardcoded wifi setup pin
  - etc

Tweet along: #Sec360
www.Secure360.org

Throw away your Dlink router – Sep 2016
https://threatpost.com/backdoored-d-link-router-should-be-trashed-researcher-says/120979/
IoT Design Principal 3 - Encryption

• Encryption is a must
  • Encryption during transit
  • Encrypting at rest

• If data not public – must encrypt
  • No HTTP – only HTTPS
  • SSL is cheap
  • Must be default and not optional
IoT Design Principal 3 - Encryption

• Home devices
  • Vast majority use HTTP for configuration
  • Some allow both HTTP and HTTPS, but default to HTTP
  • Redirect HTTP to HTTPS is OK

• Anything Internet facing HTTPS ONLY
  • Cameras
  • Routers
  • Etc

• Phone Apps
  • Store credentials encrypted
IoT Design Principal 3 - Encryption

• Even alarm systems.
• Not necessarily an IoT, but should have encryption
• My ‘wireless’ systems also forgot to use encryption
  • SimpliSafe - $200 hardware need to harvest pins from 200 yard away
  • Most other also have same issue: ADT, Vivint, etc
• But probably still ok for home usage
• Could all have been avoided with simple encryption

SimpliSafe Alarm – vulnerability unfixable
https://www.forbes.com/sites/thomasbrewster/2016/02/17/simplisafe-alarm-attacks/#22ec23743b00
Most Home Alarm systems vulnerable
https://www.wired.com/2014/07/hacking-home-alarms/
Hacking Simpli Safe
https://www.youtube.com/watch?v=EebXrSPk01Y
IoT Design Principal 4 – Self-Update

• ‘Normal Consumers’
  • Do NOT keep checking for new firmware
  • Do NOT scan their home network on regular basis
  • Do NOT have segmentation – Guest/Main/IoT networks

• Consumers
  • Use the set and forget concept
  • 40% have never patched their devices
  • 40% leave all defaults
  • Path of least resistance.

a. Self-update by default is a must
User could optionally turn off

Tweet along: #Sec360
www.Secure360.org

Slashdot – Ubuntu survey
IoT Design Principal 4 – Self-Update

- What happened on Oct 21 2016?
  - The internet crashed 😊
- Oct 20th – Chris Baker publishes blog
  - Iot Attack – Impact on Managed DNS Operator
    “What is the risk rating of misconfigured NTP servers vs. compromised IP cameras and DVRs”
  - Dyn – large DNS provider
  - DoS attacks nothing new
- Oct 21st – Massive Internet Outtage in US
- What caused it?
  - Hacked Cameras & DVRs used for DDOS attack on Dyn
    “The password is hardcoded into the firmware”
  - Oct 6 – 512K devices vulnerable hardware

Chris Baker’s Blog
IoT Design Principal 4 – Self-Update

• Oct 21st 2016
  • Massive Denial of service attack targeting Dyn
  • Mirai
    • Source published in Sep 2016
    • Used to search the internet for Vulnerable IoT devices

“It’s remarkable that virtually an entire company’s product line has just been turned into a botnet that is now attacking the United States,”
  • Infected devices searched for other infected devices

KrebsOnSecurity -
Vulnerable Devices targeted by Mirai

<table>
<thead>
<tr>
<th>Username/Password</th>
<th>Manufacturer</th>
<th>Link to supporting evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin/123456</td>
<td>ACTI IP Camera</td>
<td><a href="https://www.ycombinator.com/item?id=11114012">https://www.ycombinator.com/item?id=11114012</a></td>
</tr>
<tr>
<td>root7uKm0v0zv0</td>
<td>Dahua IP Camera</td>
<td><a href="http://www.cam4.org/index.php?topic=9526.0">http://www.cam4.org/index.php?topic=9526.0</a></td>
</tr>
<tr>
<td>root7uKm0v0zv0</td>
<td>Dahua IP Camera</td>
<td><a href="http://www.cam4.org/index.php?topic=9526.0">http://www.cam4.org/index.php?topic=9526.0</a></td>
</tr>
<tr>
<td>root7uKm0v0zv0</td>
<td>Dahua IP Camera</td>
<td><a href="http://www.cam4.org/index.php?topic=9526.0">http://www.cam4.org/index.php?topic=9526.0</a></td>
</tr>
<tr>
<td>root7uKm0v0zv0</td>
<td>Dahua IP Camera</td>
<td><a href="http://www.cam4.org/index.php?topic=9526.0">http://www.cam4.org/index.php?topic=9526.0</a></td>
</tr>
<tr>
<td>root/admin</td>
<td>DreamBox TV receiver</td>
<td><a href="http://www.satellites.co.uk/forums/thread/root-root-password-plugin.1011149/">http://www.satellites.co.uk/forums/thread/root-root-password-plugin.1011149/</a></td>
</tr>
<tr>
<td>root/txv</td>
<td>EV ZLX Two-way Speaker</td>
<td>?</td>
</tr>
<tr>
<td>root4junttech</td>
<td>Guangzhou Huan Optical</td>
<td><a href="https://news.ycombinator.com/item?id=11114012">https://news.ycombinator.com/item?id=11114012</a></td>
</tr>
<tr>
<td>root/h3511</td>
<td>H.264 - Chinese DVR</td>
<td><a href="http://www.aliexpress.com/item.js?&amp;k=058&amp;tt=24030&amp;st=craze16">http://www.aliexpress.com/item.js?&amp;k=058&amp;tt=24030&amp;st=craze16</a></td>
</tr>
<tr>
<td>root/h3518</td>
<td>Hikvision IP Camera</td>
<td><a href="https://lacasias.wordpress.com/2014/09/10/4-region-h3518-in-a-camera-module/">https://lacasias.wordpress.com/2014/09/10/4-region-h3518-in-a-camera-module/</a></td>
</tr>
<tr>
<td>root/k123</td>
<td>Hikvision IP Camera</td>
<td><a href="https://github.com/berjancolangelo/74cd06a6f47325074356180c78127d">https://github.com/berjancolangelo/74cd06a6f47325074356180c78127d</a></td>
</tr>
<tr>
<td>root/k124</td>
<td>Hikvision IP Camera</td>
<td><a href="https://github.com/berjancolangelo/74cd06a6f47325074356180c78127d">https://github.com/berjancolangelo/74cd06a6f47325074356180c78127d</a></td>
</tr>
<tr>
<td>root/ls07d</td>
<td>Hikvision IP Camera</td>
<td><a href="https://github.com/berjancolangelo/74cd06a6f47325074356180c78127d">https://github.com/berjancolangelo/74cd06a6f47325074356180c78127d</a></td>
</tr>
<tr>
<td>admin/mcspm</td>
<td>Mobotix Network Camera</td>
<td><a href="http://www.mobotix.com/thumbnail-password-defaults/76/">http://www.mobotix.com/thumbnail-password-defaults/76/</a></td>
</tr>
<tr>
<td>root/mdhpc</td>
<td>Shenzhen Anian Security Camera</td>
<td><a href="http://www.amazon.com/MegaPac-Vistas-Network-Surveillance-Camera/product-reviews/B00ESFBD7I">http://www.amazon.com/MegaPac-Vistas-Network-Surveillance-Camera/product-reviews/B00ESFBD7I</a></td>
</tr>
<tr>
<td>admin/smcdmin</td>
<td>SIM Routers</td>
<td><a href="http://www.leans.com/houtet-default/SIMROUTER">http://www.leans.com/houtet-default/SIMROUTER</a></td>
</tr>
</tbody>
</table>


IoT Design Principal 5 – Digital Signature

- Firmware updates
  - Manual or automatic
  - SHOULD be automatic
  - Need to check digital signature
  - Sign with private key
  - Public key can verify authenticity

- Old school in the Operating system world
  - Windows patches, Linux patches, etc
  - Powershell scripts
  - Apps in Apple Store

Telsa – Via Wifi connection activated brakes. Tesla adding digital signatures validation to firmware.
IoT Design Principal 5 – Digital Signature

• Consumer devices – cameras/routers/etc
• Most not verifying digital signatures
• What’s the danger:
  1. Compromised server attacker could infect compromise thousands
  2. Easy for government entity to slip a patch in your self-updating device
IoT Design Principal 6 – Ip White List

- Ip White List
  - Effective method to cut down attack surface
  - Always specify allowed source ips/networks
- Depending on design may take re-engineer
- Applicable to both industrial IoT and Home IoT
IoT – 5 Security Design Principals

1. Authenticate
2. No defaults
3. Encryption
4. Self-update
5. Digital signature
6. Ip White List

Also includes Secure SDLC
Secure Software Development Life Cycle

Tweet along: #Sec360
www.Secure360.org
What’s next for IoT

- Will keep growing at fast pace
  - Home devices
  - Business/machines
  - Cars
- Need regulation
  - Minimum requirements
  - Credit Card Industry – PCI
  - Medical Industry – Hipaa Hitech Act
  - IoT industry needs something similar
    - Self audit
    - Fines if vulnerable and not following guidelines

Tweet along: #Sec360
What’s next for IoT

- FTC enforcing a little bit
  - Only router manufacturers with lack of security
  - Example: Asus
    - 1200 router compromised
    - Admin/admin
    - Bypass login page
  - Settled:
    - Just $16,000 fine
    - Now must establish security program and independent audit for 20 years

Asus – Settled with FTC
What’s next for IoT

• What about hackable Cameras?
• What about hackable DvRs?

• FTC – IoT Home Inspector Challenge
    • $25K price and 3K for honorable mention
    • Deadline May 22\(^{nd}\) 2017
What can you do?

• Home Devices
  • Change all defaults
  • Run vulnerability scan (nessus)
  • Separate wifi network?
  • Ip White List for Anything Internet Facing

• Business Devices
  • Ask questions
  • 5 security design principals
  • Be aware of Internet Facing devices
Questions?

Fill out a survey!!!!!

My Info
Alex.Fagundes@HCL-PowerObjects.com
www.PowerObjects.com