Securing Our Connected World

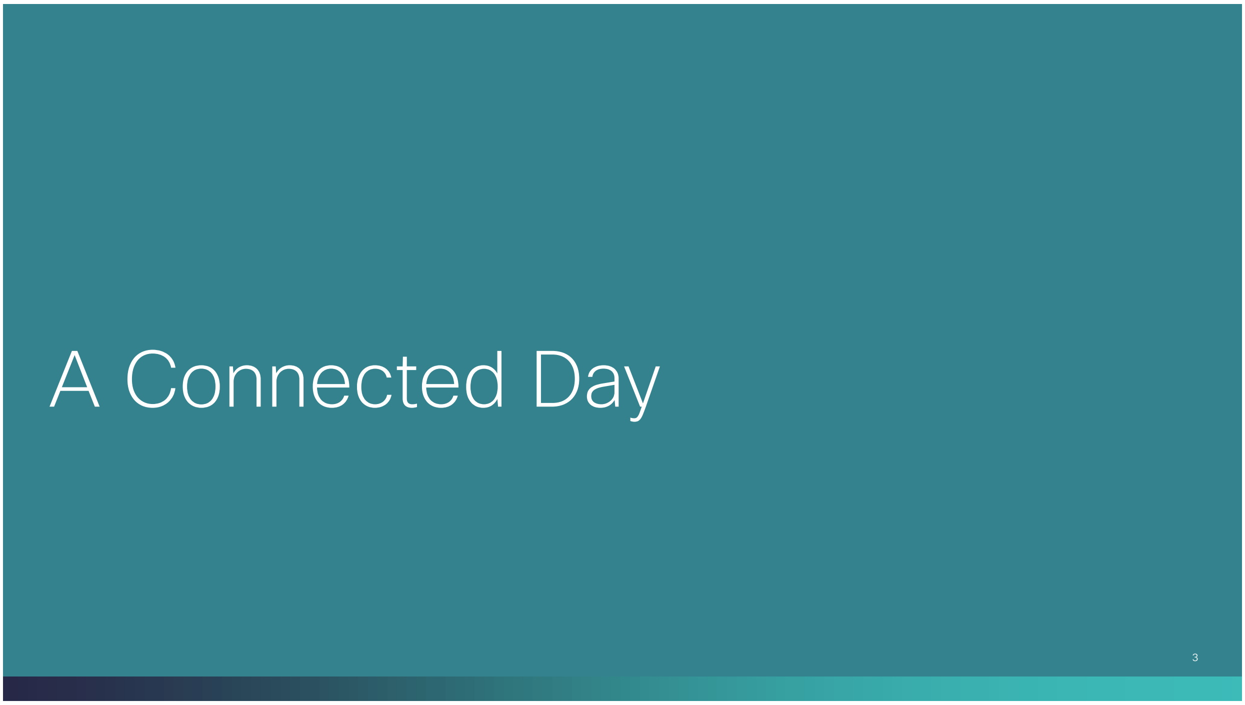
“Are You Ready”

Michele D. Guel
Distinguished Engineer, Cisco

July 2015

A Thought Provoking Journey

- A Connected Day
- Implications and opportunities
- Our Part



A Connected Day

A Connect World of Many “Smart Things”

Coffee Makers

Thermostats

Light Bulbs

Wall Sockets

Buildings

Sprinkler Systems

Cars

Cities

Baby Diapers

Factories

Fitness Trackers

Cows

Data Lakes

Motion Sensors

Phones

Animal Collars

Calendars

Surveillance Systems

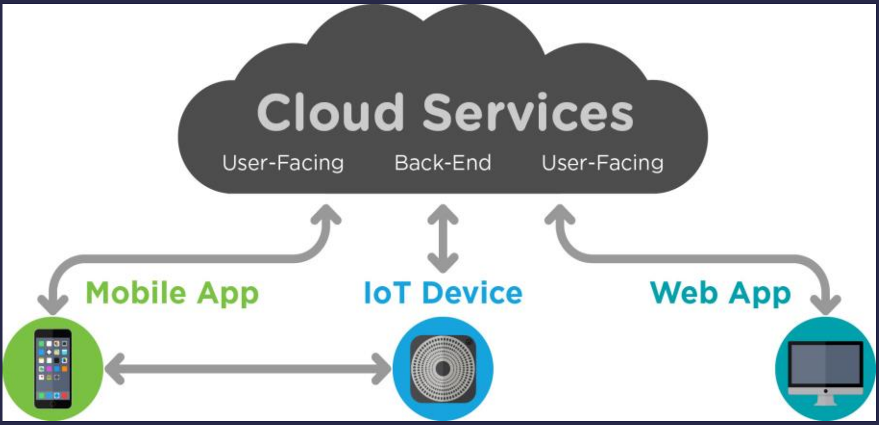
Door Locks

Medical Devices

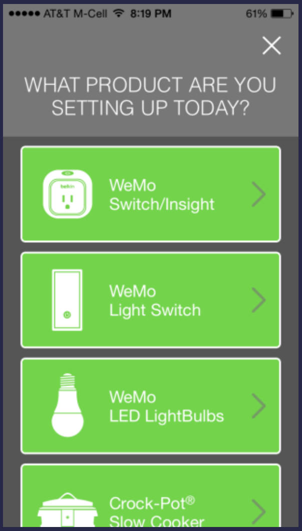
Wine Vineyards

Window Shades

Typical Architecture for Connected Things

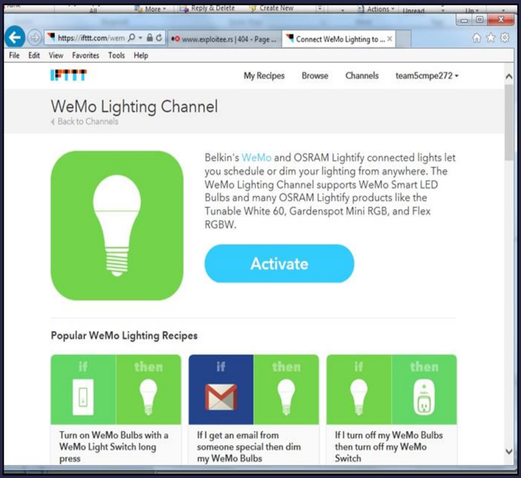


Fun with WeMO



WHAT PRODUCT ARE YOU SETTING UP TODAY?

- WeMo Switch/Insight
- WeMo Light Switch
- WeMo LED LightBulbs
- Crock-Pot® Slow Cooker



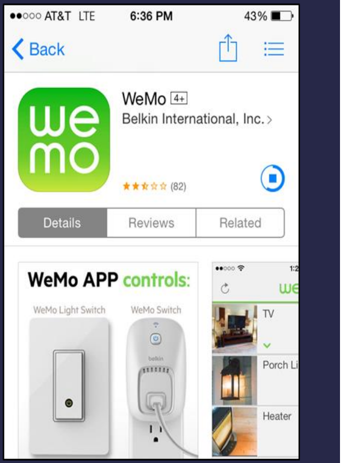
WeMo Lighting Channel

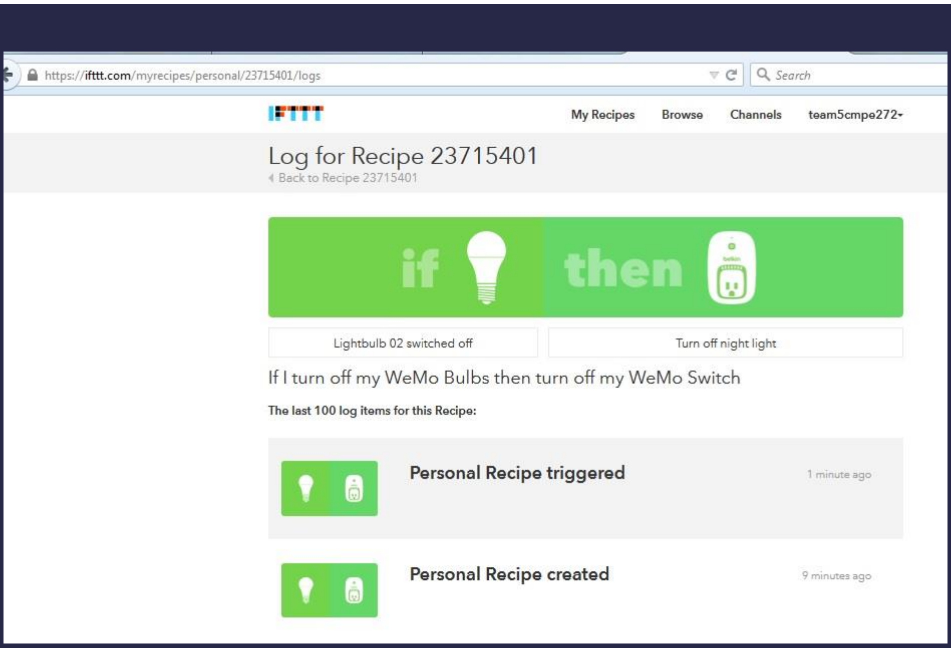
Back to Channels

Belkin's WeMo and OSRAM Lightify connected lights let you schedule or dim your lighting from anywhere. The WeMo Lighting Channel supports WeMo Smart LED Bulbs and many OSRAM Lightify products like the Tunable White 60, Gardenspot Mini RGB, and Flex RGBW.

Popular WeMo Lighting Recipes

- Turn on WeMo Bulbs with a WeMo Light Switch long press
- If I get an email from someone special then dim my WeMo Bulbs
- If I turn off my WeMo Bulbs then turn off my WeMo Switch





https://ifttt.com/myrecipes/personal/23715401/logs

Log for Recipe 23715401

◂ Back to Recipe 23715401

Lightbulb 02 switched off	Turn off night light

If I turn off my WeMo Bulbs then turn off my WeMo Switch

The last 100 log items for this Recipe:

Personal Recipe triggered — 1 minute ago

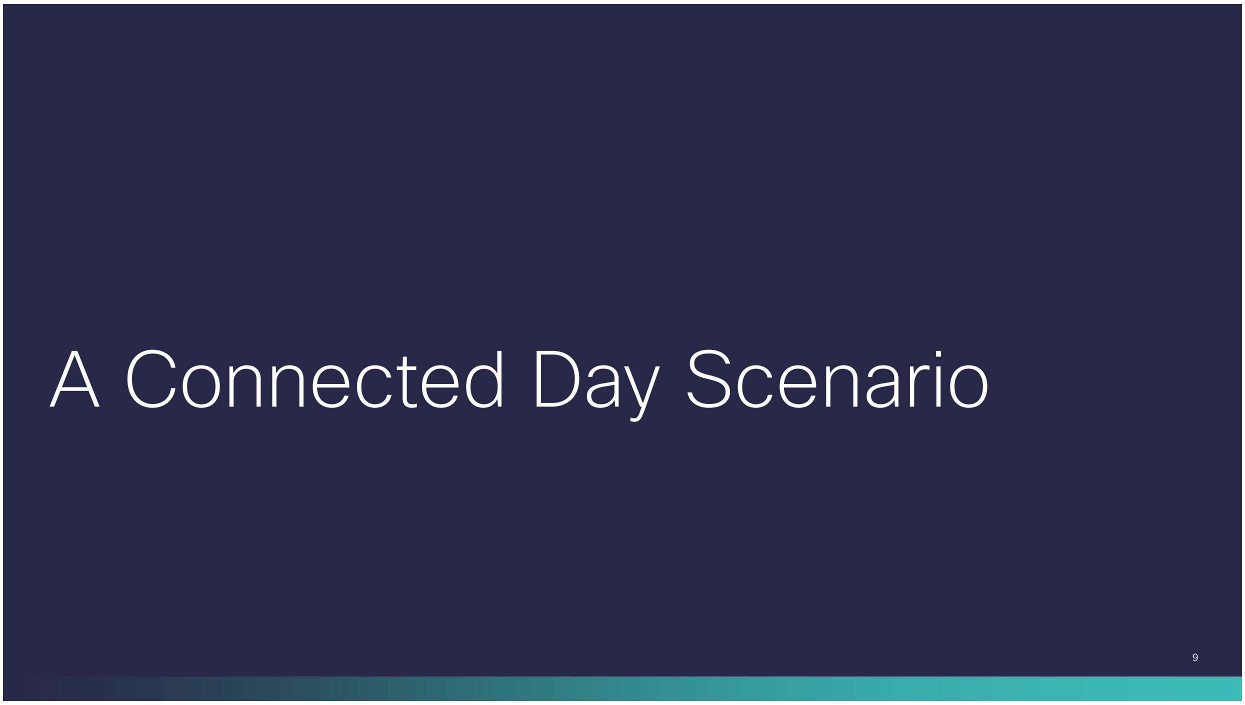
Personal Recipe created — 9 minutes ago

7

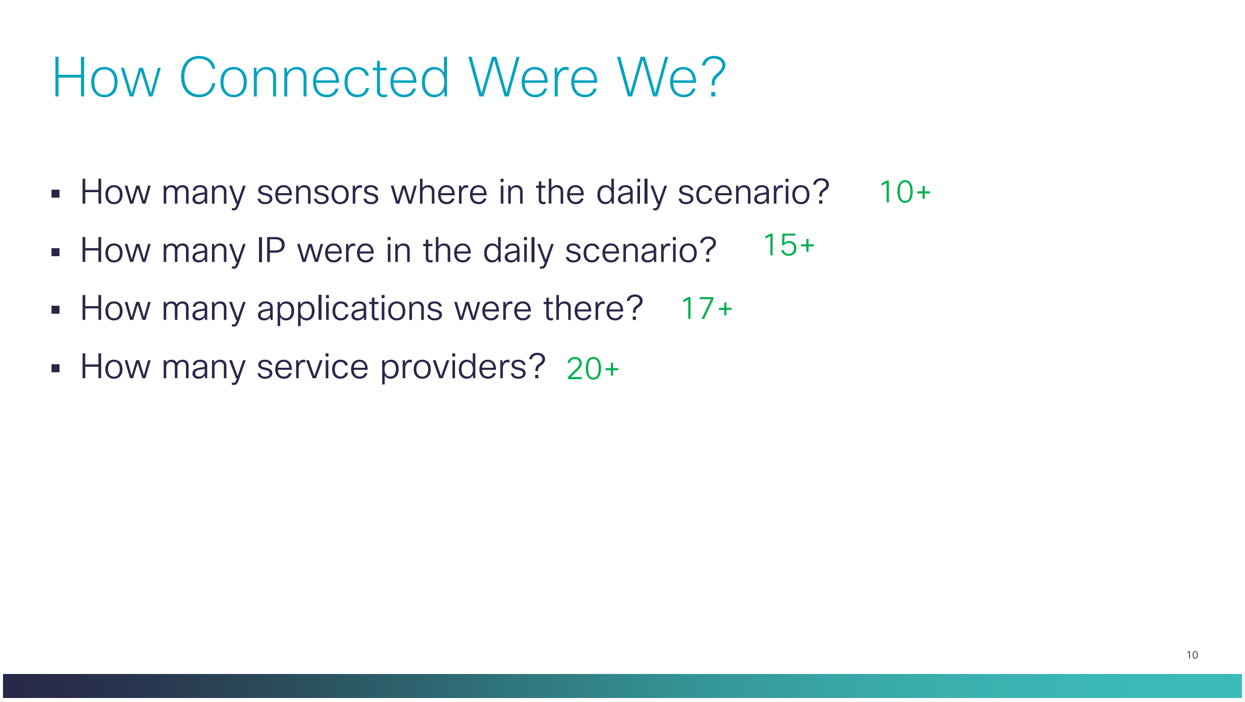
What Does Your Connected Day Look Like?

- How many applications and connected devices to you use before you leave the house for work?
- How many applications, service providers and cloud do you use in the course of your workday?
- How many social media “connections” do you send, receive or view on a daily basis?

8

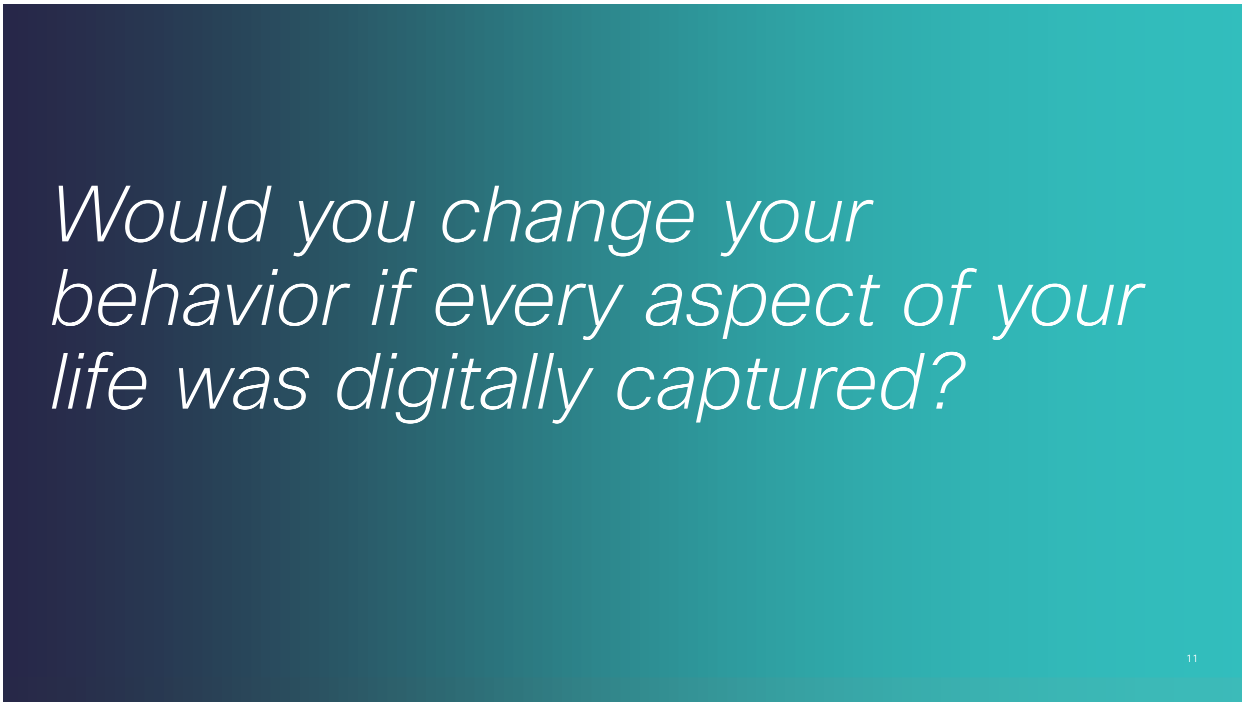


A Connected Day Scenario



How Connected Were We?

- How many sensors where in the daily scenario? 10+
- How many IP were in the daily scenario? 15+
- How many applications were there? 17+
- How many service providers? 20+



Would you change your behavior if every aspect of your life was digitally captured?

11

Challenges & Opportunities

12

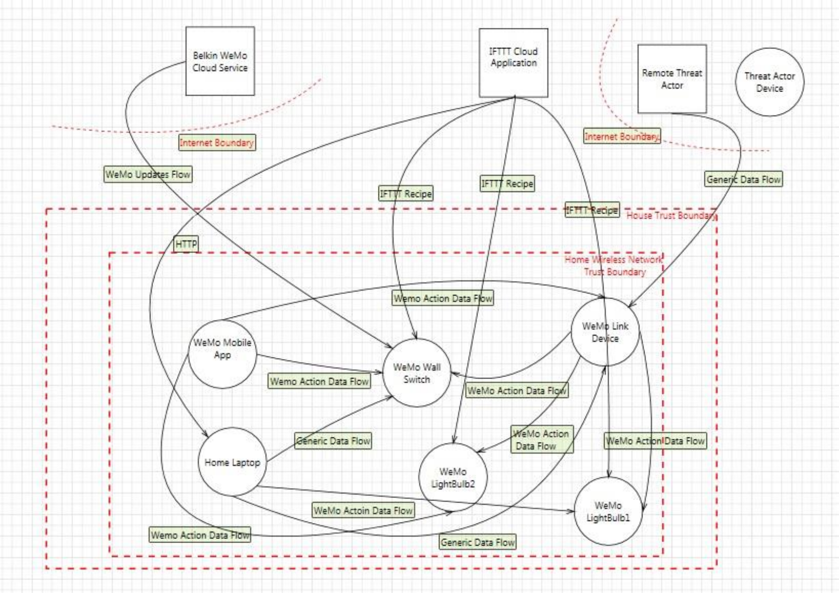
What are the Pluses in the Daily Scenario?

- Most efficient use of resources, time, money, and experience.
- Improved health and mental well-being.
- Reduced risk of missing important appointments, meetings, and experiences.
- More data to make informed decisions.
- Less worry about kids – you can track them, you can see them – they can see you.
- Increased automation (especially decisions) improves overall productivity in life.

What are the Major Negatives?

- Loss of privacy and worse, not guarantee of privacy.
- Increased availability and access to personal data may lead to increase of identity theft.
- Proliferation of daily activity data could lead to a much higher incidence of targeted attacks.
- Challenges in tracking, updating, and managing all of your connectedness.
- Loss of “humanness”?

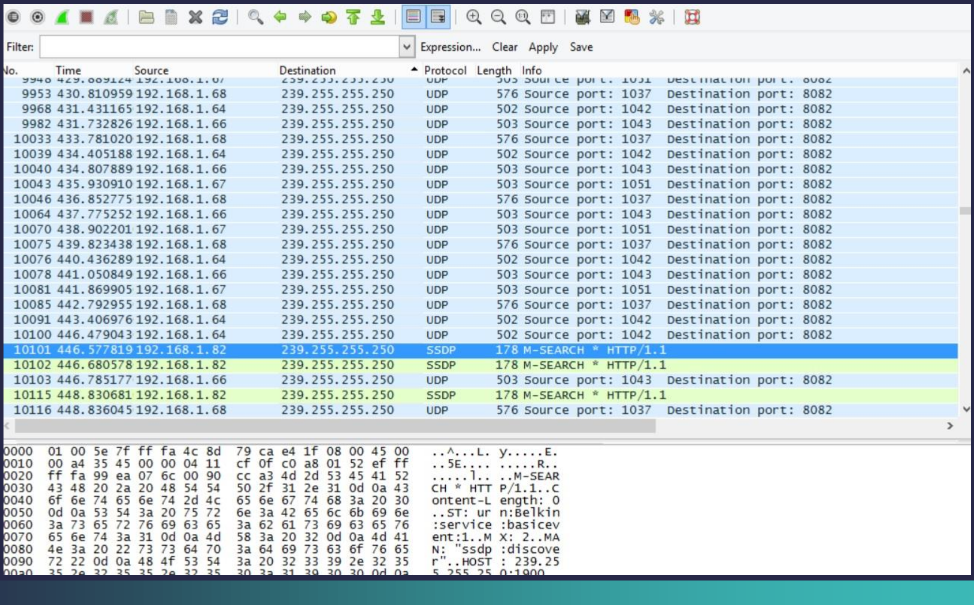
A Sample Threat Model DFD



Common Attack Patterns

- Endpoints (Sensors, devices, hubs)
  - Web based attacks (command/SQL injection, CSRF)
  - Altered firmware
  - Physical tampering to force report
  - Old /vulnerable firmware
- Communication channels (Zigbee, Bluetooth, WiFI)
- Cloud infrastructure (identity, policies, firmware updates, etc)
- User facing UI controls (AAA)

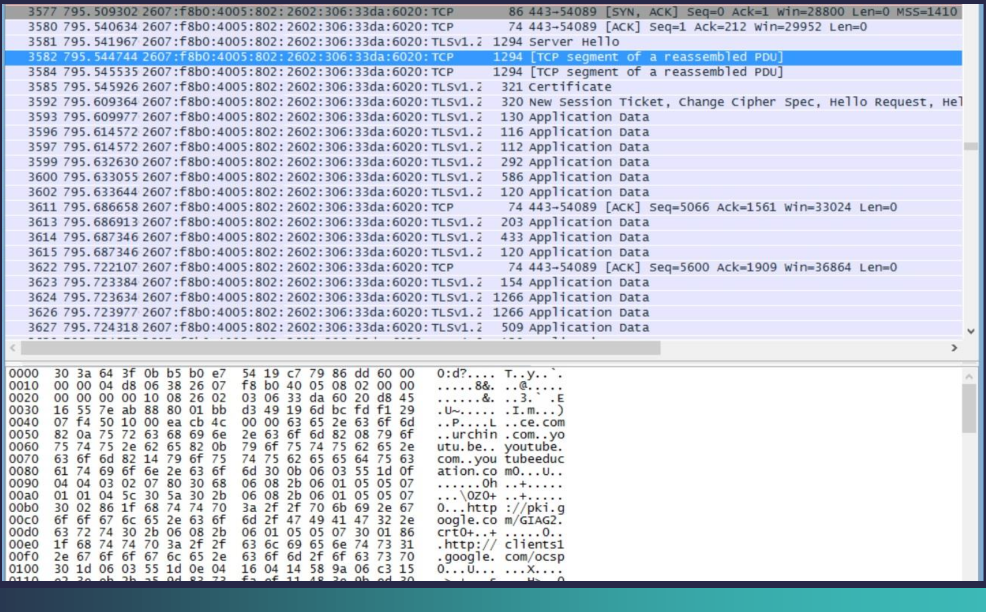
Discovery



```
No.   Time       Source         Destination      Protocol Length Info
 9948 429.889124 192.168.1.67   239.255.255.250  UDP      503 Source port: 1051  Destination port: 8082
 9953 430.810959 192.168.1.68   239.255.255.250  UDP      576 Source port: 1037  Destination port: 8082
 9968 431.431165 192.168.1.64   239.255.255.250  UDP      502 Source port: 1042  Destination port: 8082
 9982 431.732826 192.168.1.66   239.255.255.250  UDP      503 Source port: 1043  Destination port: 8082
10033 433.781020 192.168.1.68   239.255.255.250  UDP      576 Source port: 1037  Destination port: 8082
10039 434.405188 192.168.1.64   239.255.255.250  UDP      502 Source port: 1042  Destination port: 8082
10040 434.807889 192.168.1.66   239.255.255.250  UDP      503 Source port: 1043  Destination port: 8082
10043 435.930910 192.168.1.67   239.255.255.250  UDP      503 Source port: 1051  Destination port: 8082
10046 436.852775 192.168.1.68   239.255.255.250  UDP      576 Source port: 1037  Destination port: 8082
10064 437.775252 192.168.1.66   239.255.255.250  UDP      503 Source port: 1043  Destination port: 8082
10070 438.902201 192.168.1.67   239.255.255.250  UDP      503 Source port: 1051  Destination port: 8082
10075 439.823438 192.168.1.68   239.255.255.250  UDP      576 Source port: 1037  Destination port: 8082
10076 440.436289 192.168.1.64   239.255.255.250  UDP      502 Source port: 1042  Destination port: 8082
10078 441.050849 192.168.1.66   239.255.255.250  UDP      503 Source port: 1043  Destination port: 8082
10081 441.869905 192.168.1.67   239.255.255.250  UDP      503 Source port: 1051  Destination port: 8082
10085 442.792955 192.168.1.68   239.255.255.250  UDP      576 Source port: 1037  Destination port: 8082
10091 443.406976 192.168.1.64   239.255.255.250  UDP      502 Source port: 1042  Destination port: 8082
10100 446.479043 192.168.1.64   239.255.255.250  UDP      502 Source port: 1042  Destination port: 8082
10101 446.577819 192.168.1.82   239.255.255.250  SSDP     178 M-SEARCH * HTTP/1.1
10102 446.680578 192.168.1.82   239.255.255.250  SSDP     178 M-SEARCH * HTTP/1.1
10103 446.785177 192.168.1.66   239.255.255.250  UDP      503 Source port: 1043  Destination port: 8082
10115 448.830681 192.168.1.82   239.255.255.250  SSDP     178 M-SEARCH * HTTP/1.1
10116 448.836045 192.168.1.68   239.255.255.250  UDP      576 Source port: 1037  Destination port: 8082
```

```
0000  01 00 5e 7f ff fa 4c 8d  79 ca e4 1f 08 00 45 00   ..^...L. y.....E.
0010  00 a4 35 45 00 00 04 11  cf 0f c0 a8 01 52 ef ff   ..5E.... .....R..
0020  ff fa 99 ea 07 6c 00 90  cc a3 4d 2d 53 45 41 52   .....l.. ..M-SEAR
0030  43 48 20 2a 20 48 54 54  50 2f 31 2e 31 0d 0a 43   CH * HTT P/1.1..C
0040  6f 6e 74 65 6e 74 2d 4c  65 6e 67 74 68 3a 20 30   ontent-L ength: 0
0050  0d 0a 53 54 3a 20 75 72  6e 3a 42 65 6c 6b 69 6e   ..ST: ur n:Belkin
0060  3a 73 65 72 76 69 63 65  3a 62 61 73 69 63 65 76   :service :basicev
0070  65 6e 74 3a 31 0d 0a 4d  58 3a 20 32 0d 0a 4d 41   ent:1..M X: 2..MA
0080  4e 3a 20 22 73 73 64 70  3a 64 69 73 63 6f 76 65   N: "ssdp :discove
0090  72 22 0d 0a 48 4f 53 54  3a 20 32 33 39 2e 32 35   r"..HOST : 239.25
00a0  35 2e 32 35 35 2e 32 35  30 3a 31 39 30 30 0d 0a   5.255.25 0:1900
```

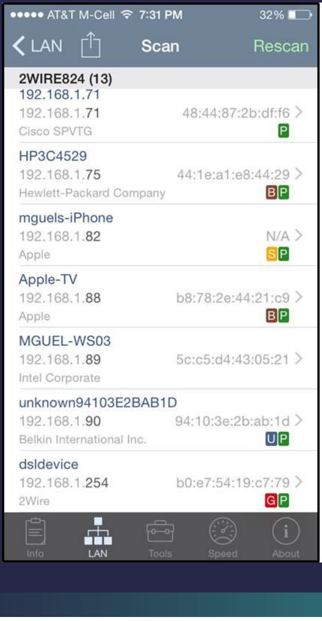
Firmware Update



```
3577 795.509302 2607:f8b0:4005:802:2602:306:33da:6020:TCP      86 443→54089 [SYN, ACK] Seq=0 Ack=1 Win=28800 Len=0 MSS=1410
3580 795.540634 2607:f8b0:4005:802:2602:306:33da:6020:TCP      74 443→54089 [ACK] Seq=1 Ack=212 Win=29952 Len=0
3581 795.541967 2607:f8b0:4005:802:2602:306:33da:6020:TLSv1.2 1294 Server Hello
3582 795.544744 2607:f8b0:4005:802:2602:306:33da:6020:TCP    1294 [TCP segment of a reassembled PDU]
3584 795.545535 2607:f8b0:4005:802:2602:306:33da:6020:TCP    1294 [TCP segment of a reassembled PDU]
3585 795.545926 2607:f8b0:4005:802:2602:306:33da:6020:TLSv1.2  321 Certificate
3592 795.609364 2607:f8b0:4005:802:2602:306:33da:6020:TLSv1.2  320 New Session Ticket, Change Cipher Spec, Hello Request, Hel
3593 795.609977 2607:f8b0:4005:802:2602:306:33da:6020:TLSv1.2  130 Application Data
3596 795.614572 2607:f8b0:4005:802:2602:306:33da:6020:TLSv1.2  116 Application Data
3597 795.614572 2607:f8b0:4005:802:2602:306:33da:6020:TLSv1.2  112 Application Data
3599 795.632630 2607:f8b0:4005:802:2602:306:33da:6020:TLSv1.2  292 Application Data
3600 795.633055 2607:f8b0:4005:802:2602:306:33da:6020:TLSv1.2  586 Application Data
3602 795.633644 2607:f8b0:4005:802:2602:306:33da:6020:TLSv1.2  120 Application Data
3611 795.686658 2607:f8b0:4005:802:2602:306:33da:6020:TCP      74 443→54089 [ACK] Seq=5066 Ack=1561 Win=33024 Len=0
3613 795.686913 2607:f8b0:4005:802:2602:306:33da:6020:TLSv1.2  203 Application Data
3614 795.687346 2607:f8b0:4005:802:2602:306:33da:6020:TLSv1.2  433 Application Data
3615 795.687346 2607:f8b0:4005:802:2602:306:33da:6020:TLSv1.2  120 Application Data
3622 795.722107 2607:f8b0:4005:802:2602:306:33da:6020:TCP      74 443→54089 [ACK] Seq=5600 Ack=1909 Win=36864 Len=0
3623 795.723384 2607:f8b0:4005:802:2602:306:33da:6020:TLSv1.2  154 Application Data
3624 795.723634 2607:f8b0:4005:802:2602:306:33da:6020:TLSv1.2 1266 Application Data
3626 795.723977 2607:f8b0:4005:802:2602:306:33da:6020:TLSv1.2 1266 Application Data
3627 795.724318 2607:f8b0:4005:802:2602:306:33da:6020:TLSv1.2  509 Application Data
```

```
0000  30 3a 64 3f 0b b5 b0 e7  54 19 c7 79 86 dd 60 00   0:d?.... T..y..`.
0010  00 00 04 d8 06 38 26 07  f8 b0 40 05 08 02 00 00   .....8&. ..@.....
0020  00 00 00 00 10 08 26 02  03 06 33 da 60 20 d8 45   ......&. ..3.` .E
0030  16 55 7e ab 88 80 01 bb  d3 49 19 6d bc fd f1 29   .U~..... .I.m...)
0040  07 f4 50 10 00 ea cb 4c  00 00 63 65 2e 63 6f 6d   ..P....L ..ce.com
0050  82 0a 75 72 63 68 69 6e  2e 63 6f 6d 82 08 79 6f   ..urchin .com..yo
0060  75 74 75 2e 62 65 82 0b  79 6f 75 74 75 62 65 2e   utu.be.. youtube.
0070  63 6f 6d 82 14 79 6f 75  74 75 62 65 65 64 75 63   com..you tubeeduc
0080  61 74 69 6f 6e 2e 63 6f  6d 30 0b 06 03 55 1d 0f   ation.co m0...U..
0090  04 04 03 02 07 80 30 68  06 08 2b 06 01 05 05 07   ......0h ..+.....
00a0  01 01 04 5c 30 5a 30 2b  06 08 2b 06 01 05 05 07   ...\0Z0+ ..+.....
00b0  30 02 86 1f 68 74 74 70  3a 2f 2f 70 6b 69 2e 67   0...http ://pki.g
00c0  6f 6f 67 6c 65 2e 63 6f  6d 2f 47 49 41 47 32 2e   oogle.co m/GIAG2.
00d0  63 72 74 30 2b 06 08 2b  06 01 05 05 07 30 01 86   crt0+..+ .....0..
00e0  1f 68 74 74 70 3a 2f 2f  63 6c 69 65 6e 74 73 31   .http:// clients1
00f0  2e 67 6f 6f 67 6c 65 2e  63 6f 6d 2f 6f 63 73 70   .google. com/ocsp
0100  30 1d 06 03 55 1d 0e 04  16 04 14 58 9a 06 c3 15   0...U... ...X....
```

Let’s Scan….



●●●●● AT&T M-Cell 7:31 PM 32%

< LAN Scan Rescan

2WIRE824 (13)

192.168.1.71
192.168.1.71 48:44:87:2b:df:f6 >
Cisco SPVTG P

HP3C4529
192.168.1.75 44:1e:a1:e8:44:29 >
Hewlett-Packard Company BP

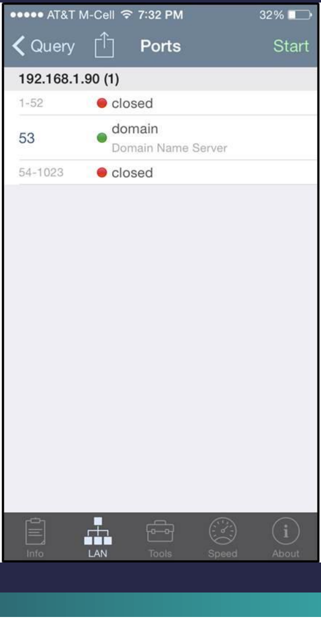
mguels-iPhone
192.168.1.82 N/A >
Apple SP

Apple-TV
192.168.1.88 b8:78:2e:44:21:c9 >
Apple BP

MGUEL-WS03
192.168.1.89 5c:c5:d4:43:05:21 >
Intel Corporate

unknown94103E2BAB1D
192.168.1.90 94:10:3e:2b:ab:1d >
Belkin International Inc. UP

dsldevice
192.168.1.254 b0:e7:54:19:c7:79 >
2Wire GP



●●●●● AT&T M-Cell 7:32 PM 32%

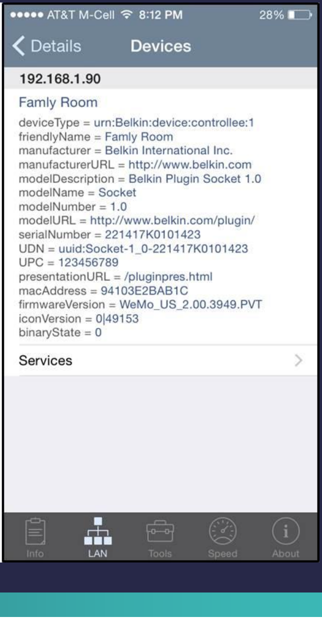
< Query Ports Start

192.168.1.90 (1)

1-52 ● closed

53 ● domain
Domain Name Server

54-1023 ● closed



●●●●● AT&T M-Cell 8:12 PM 28%

< Details Devices

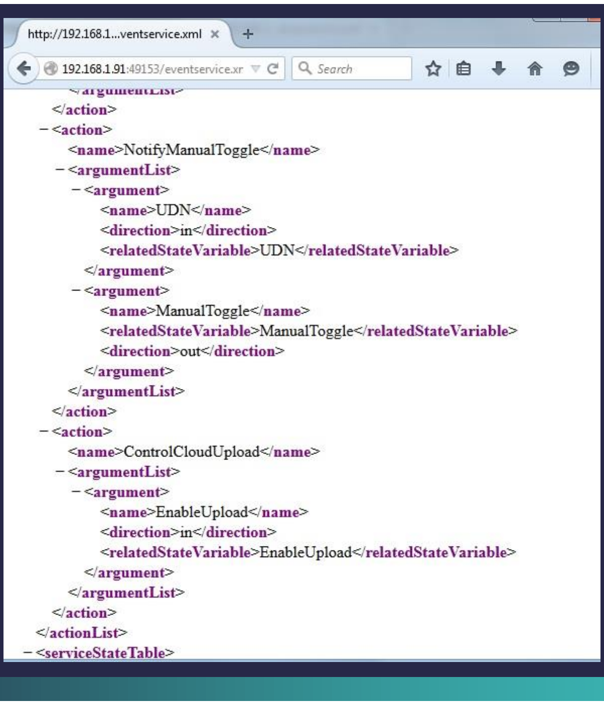
192.168.1.90

Famly Room

deviceType = urn:Belkin:device:controllee:1
friendlyName = Famly Room
manufacturer = Belkin International Inc.
manufacturerURL = http://www.belkin.com
modelDescription = Belkin Plugin Socket 1.0
modelName = Socket
modelNumber = 1.0
modelURL = http://www.belkin.com/plugin/
serialNumber = 221417K0101423
UDN = uuid:Socket-1_0-221417K0101423
UPC = 123456789
presentationURL = /pluginpres.html
macAddress = 94103E2BAB1C
firmwareVersion = WeMo_US_2.00.3949.PVT
iconVersion = 0|49153
binaryState = 0

Services >

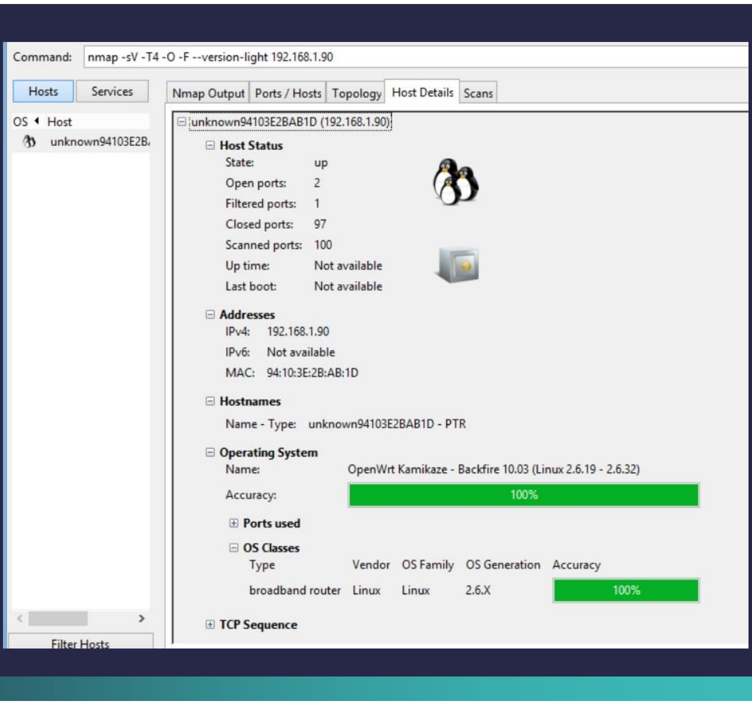
Some XML



http://192.168.1...ventservice.xml ×
+
192.168.1.91:49153/eventservice.xr
Search

```
      </argumentList>
    </action>
  – <action>
      <name>NotifyManualToggle</name>
    – <argumentList>
      – <argument>
          <name>UDN</name>
          <direction>in</direction>
          <relatedStateVariable>UDN</relatedStateVariable>
        </argument>
      – <argument>
          <name>ManualToggle</name>
          <relatedStateVariable>ManualToggle</relatedStateVariable>
          <direction>out</direction>
        </argument>
      </argumentList>
    </action>
  – <action>
      <name>ControlCloudUpload</name>
    – <argumentList>
      – <argument>
          <name>EnableUpload</name>
          <direction>in</direction>
          <relatedStateVariable>EnableUpload</relatedStateVariable>
        </argument>
      </argumentList>
    </action>
  </actionList>
– <serviceStateTable>
```

How About NMAP



Command: nmap -sV -T4 -O -F --version-light 192.168.1.90

unknown94103E2BAB1D (192.168.1.90)

Host Status

State: up
Open ports: 2
Filtered ports: 1
Closed ports: 97
Scanned ports: 100
Up time: Not available
Last boot: Not available

Addresses

IPv4: 192.168.1.90
IPv6: Not available
MAC: 94:10:3E:2B:AB:1D

Hostnames

Name - Type: unknown94103E2BAB1D - PTR

Operating System

Name: OpenWrt Kamikaze - Backfire 10.03 (Linux 2.6.19 - 2.6.32)
Accuracy: 100%

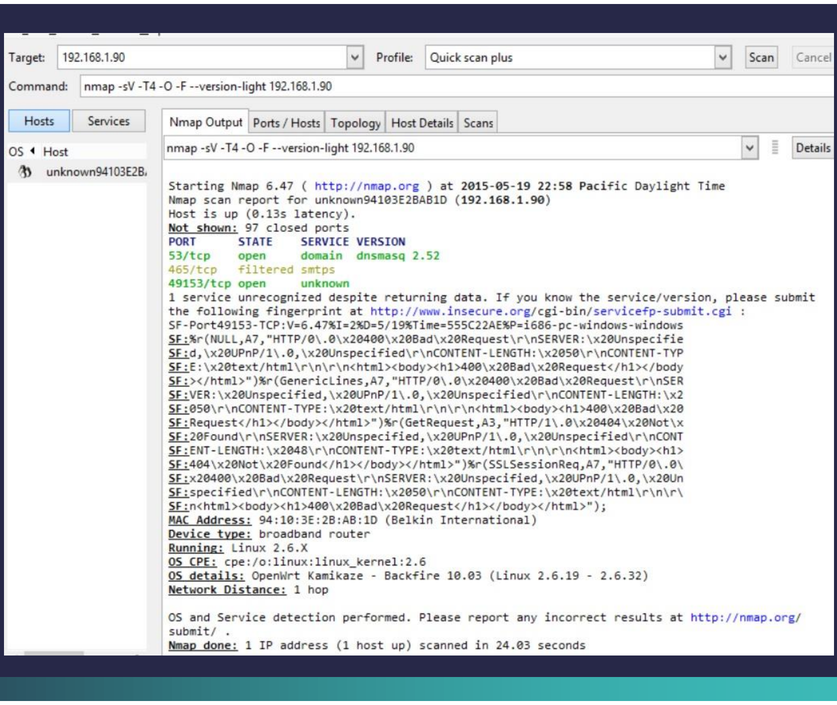
Ports used

OS Classes

Type	Vendor	OS Family	OS Generation	Accuracy
broadband router	Linux	Linux	2.6.X	100%

TCP Sequence

More NMAP



Target: 192.168.1.90
Profile: Quick scan plus
Command: nmap -sV -T4 -O -F --version-light 192.168.1.90

nmap -sV -T4 -O -F --version-light 192.168.1.90

```
Starting Nmap 6.47 ( http://nmap.org ) at 2015-05-19 22:58 Pacific Daylight Time
Nmap scan report for unknown94103E2BAB1D (192.168.1.90)
Host is up (0.13s latency).
Not shown: 97 closed ports
PORT      STATE    SERVICE VERSION
53/tcp    open     domain  dnsmasq 2.52
465/tcp   filtered smtps
49153/tcp open     unknown
1 service unrecognized despite returning data. If you know the service/version, please submit
the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port49153-TCP:V=6.47%I=2%D=5/19%Time=555C22AE%P=i686-pc-windows-windows
SF:%r(NULL,A7,"HTTP/0\.0\x20400\x20Bad\x20Request\r\nSERVER:\x20Unspecifie
SF:d,\x20UPnP/1\.0,\x20Unspecified\r\nCONTENT-LENGTH:\x2050\r\nCONTENT-TYP
SF:E:\x20text/html\r\n\r\n<html><body><h1>400\x20Bad\x20Request</h1></body
SF:></html>")%r(GenericLines,A7,"HTTP/0\.0\x20400\x20Bad\x20Request\r\nSER
SF:VER:\x20Unspecified,\x20UPnP/1\.0,\x20Unspecified\r\nCONTENT-LENGTH:\x2
SF:050\r\nCONTENT-TYPE:\x20text/html\r\n\r\n<html><body><h1>400\x20Bad\x20
SF:Request</h1></body></html>")%r(GetRequest,A3,"HTTP/1\.0\x20404\x20Not\x
SF:20Found\r\nSERVER:\x20Unspecified,\x20UPnP/1\.0,\x20Unspecified\r\nCONT
SF:ENT-LENGTH:\x2048\r\nCONTENT-TYPE:\x20text/html\r\n\r\n<html><body><h1>
SF:404\x20Not\x20Found</h1></body></html>")%r(SSLSessionReq,A7,"HTTP/0\.0\
SF:x20400\x20Bad\x20Request\r\nSERVER:\x20Unspecified,\x20UPnP/1\.0,\x20Un
SF:specified\r\nCONTENT-LENGTH:\x2050\r\nCONTENT-TYPE:\x20text/html\r\n\r\
SF:n<html><body><h1>400\x20Bad\x20Request</h1></body></html>");
MAC Address: 94:10:3E:2B:AB:1D (Belkin International)
Device type: broadband router
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: OpenWrt Kamikaze - Backfire 10.03 (Linux 2.6.19 - 2.6.32)
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at http://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.03 seconds
```

Our Part

As Individuals We Can…

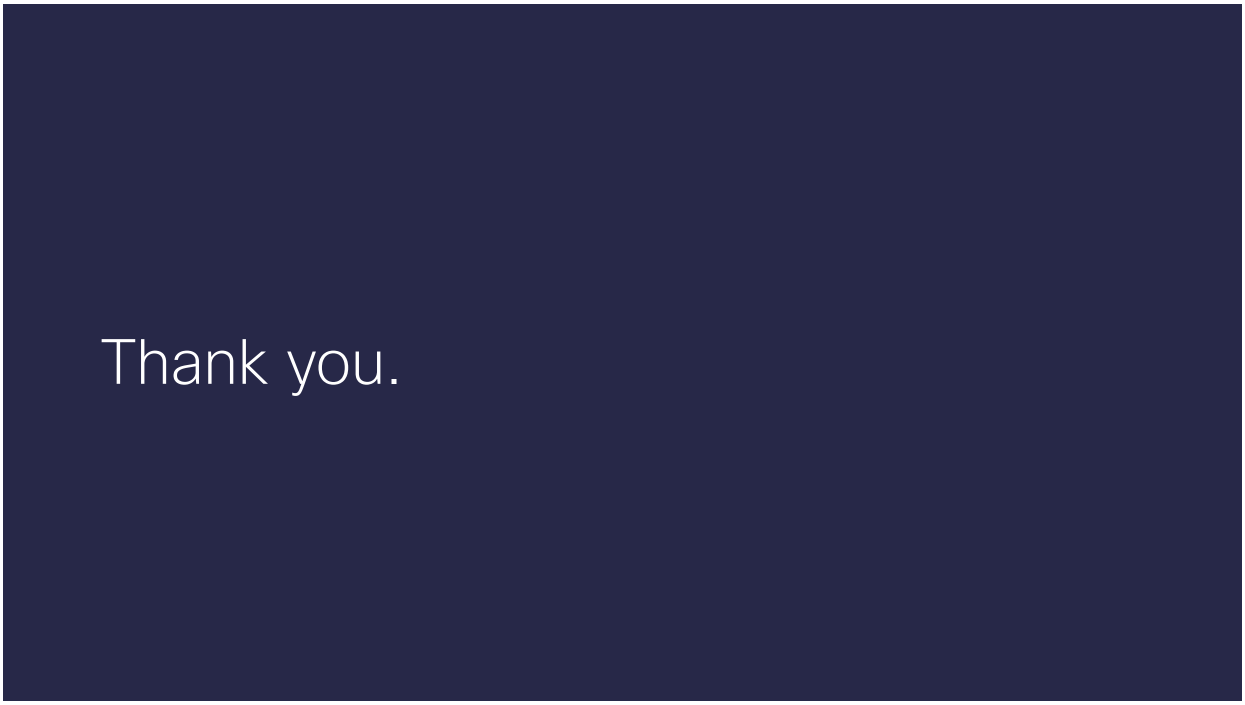
- Hold vendors accountable for secure products and applications.
- Don’t or refuse to use applications that have not default security features.
- Understand privacy laws for your region and that of your close family members. Understand who is capturing your personal data and how is it being used? Is there an opt-in or opt-out model?
- Get educated on current/emerging technologies – data science, cloud, Sensors.
- Encourage your kids to pursue STEM careers or at least understand key technologies and implications.

As Employees We Can…

- Hold vendors accountable for quality & assurance – know who you are partnering with and their quality.
- Develop and adopt standards for application integrity and trustworthiness.
  - Is there a concept of trust anchor or app signature we can apply?
- Develop and adopt standards for IP enabled devices/sensors. Need integrity and trustworthiness as well.
  - They should be secure by default
- Develop and adopt seamless and scalable identity for people, process and things.

Call to Action

- Plug in somewhere, either as an individual consumer or as an employee.
- Secure your connected world as best as you can.
- Understand what your children and grandchildren need to learn and be a part of that.
- Educate yourself and then be an advocate for the change that needs to happen.



Thank you.