

RSA® Conference 2018

San Francisco | April 16–20 | Moscone Center

SESSION ID: HTA-F02



EXFILTRATING DATA THROUGH IOT

Mike Raggo

CSO & Threat Research
802 Secure, Inc.
@DataHiding @MikeRaggo

Chet Hosmer

Founder
Python Forensics, Inc. *A Non Profit Research Institute*
@PythonForensics

Speaker Introduction



Mike Rago

Mike Rago is Chief Security Officer at 802 Secure and has over 20 years of security research experience.

His current focus is wireless IoT threats impacting the enterprise. Michael is the author of “Mobile Data Loss: Threats & Countermeasures” and “Data Hiding” for Syngress Books, and contributing author for “Information Security the Complete Reference 2nd Edition”.

A former security trainer, Michael has briefed international defense agencies including the FBI and Pentagon, and is a frequent presenter at security conferences, including Black Hat, DEF CON, Gartner, DoD Cyber Crime, OWASP, HackCon, and SANS.



Chet Hosmer

Is an international author, educator & researcher, and founder of Python Forensics, Inc., a non-profit research institute focused on the collaborative development of open source investigative technologies using the Python programming language.

- A Visiting Professor at Utica College in the Cybersecurity Graduate Program, where his research and teaching is focused on data hiding, active cyber defense and security of industrial control systems.

- Adjunct Professor at Champlain College in the Digital Forensics Graduate Program, where his research and teaching is focused on solving hard digital investigation problems using the Python programming language.

“Apply” Slide



- Our role is to provide insights based on our research/analysis of data exfiltration vulnerabilities found in IoT protocols (i.e. SSDP, P25, Zigbee, Z-Wave, WiFi, uPnP). With an eye toward mitigating weaknesses in current protocols and to impact future protocol designs to eliminate them.
- From a student perspective we hope to first make you aware of these vulnerabilities and weaknesses. Then more specifically delve into the details and demonstrate data exfiltration using IoT protocols.
- The application of this knowledge will allow you to assess and mitigate these risks as you integrate IoT technologies into your production systems, as well as making informed decisions regarding IoT device and protocol selection.

RSA® Conference 2018

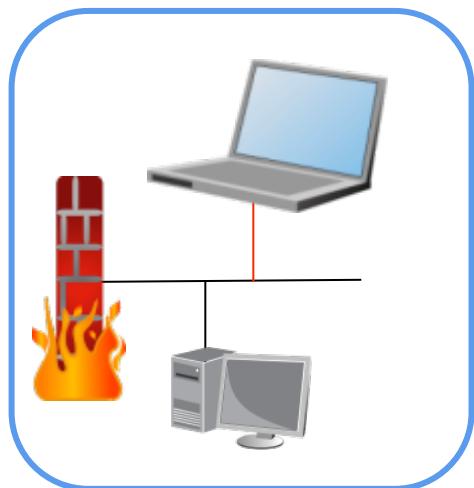


What's really different about IoT?

IoT is more than smart devices



Detecting Exfiltration on the Wire - Old School



Detecting Exfiltration in an IoT World

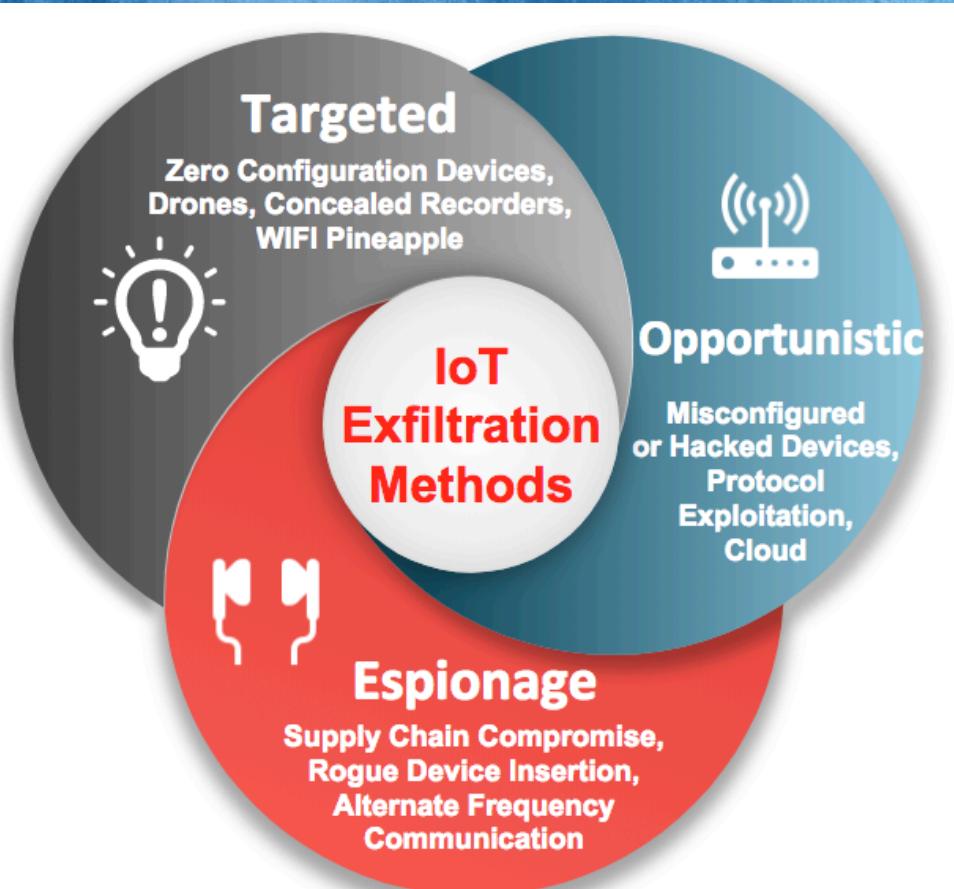


IoT exfiltration is easy - No one is monitoring!

Exfiltration Methods

Zero Configuration Devices

Are obscured from normal network operations - can operate autonomously outside the scope of the enterprise network.



Protocol Limitations

Many IoT protocols lack even basic authentication, integrity and privacy considerations.

Supply Chain Integrity

Data is back channeled to remote country or close proximity listening stations. Communication is obfuscated by the cloud or the use of alternate protocols and frequencies.

Smart Watch Exfiltration



Tested 4 Smartwatches

Apple Watch, Samsung Gear 2 Neo. Moto 360, U8



Samsung
Tizen



Apple
watchOS



U8 Nucleus



Android Wear
(Moto 360)

Smart Watch Exfiltration



- U8 Nucleus Smart Watch found to be sending data through the app on the mobile device to a random IP in China, over an encrypted channel



- Samsung Gear 2 Neo found with no password and allowed remote privilege escalation (disclosed to Samsung and now patched)
- HackCon Norway, BSidesSF, DEF CON Demo Lab demonstrated SWATtack - python tool for exploiting smartwatches

IoT Hubs and Exfiltration



- Many IoT devices and IoT Hubs now have USB ports for data backup
- New USB backup flash drives support Wireless (WiFi, BT, etc.)



Z-Wave Hub with
Ethernet and USB Ports



EXFIL - Steal and exfiltrate surveillance files, data, videos, etc. Nothing seen on the corporate WiFi or Wired Network

Windows Virtual WiFi (7, 8, & 10)



- This is native to Windows operating system. In all versions of Windows 7, 8, & 10
- Setup at the DOS Prompt
- Share either a Wired or Wireless connection
The user can share their own desktop (*like SoftAP, not ad-hoc network*)
- And the user can share their network connection with others - USING THE SAME WiFi CARD!
- Corporate wireless network may use authentication and encryption
 - BUT the user can share that connection with others, allowing those users to connect to the corporate network with weaker authentication & encryption, or OPEN!!!

```
C:\Administrator:C:\Windows\System32\cmd.exe
C:\Windows\system32>ipconfig /all

Windows IP Configuration

Host Name . . . . . : phantom
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : launchmodem.com

Wireless LAN adapter Wireless Network Connection 2:

Connection-specific DNS Suffix . . . . . : Microsoft Virtual WiFi Miniport Adapter
Description . . . . . : Microsoft Virtual WiFi Miniport Adapter
Physical Address . . . . . : 00-23-[REDACTED]
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::b46b:[REDACTED] (Preferred)
IPv4 Address . . . . . : 192.168.1.37.1<Preferred>
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
DHCPv6 IAID . . . . . : 419439438
DHCPv6 Client DUID . . . . . : 00-01-00-01-[REDACTED]

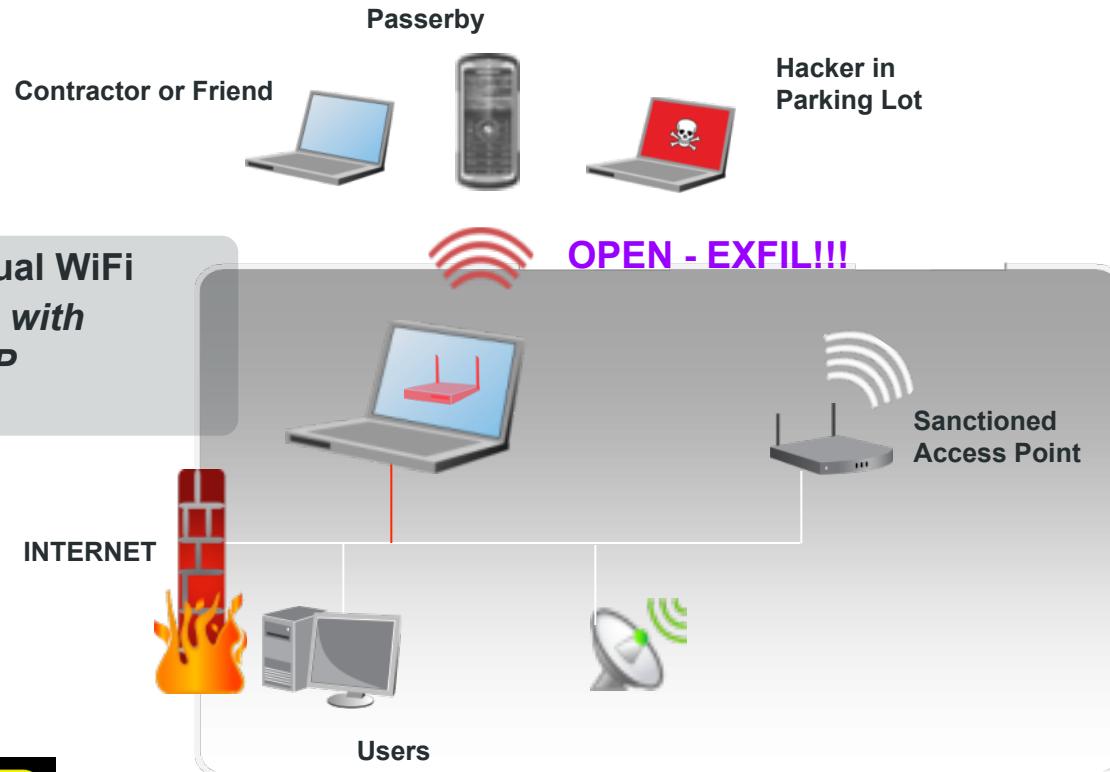
DNS Servers . . . . . : fec0:0:0:ffff::1x2
fec0:0:0:ffff::2x2
fec0:0:0:ffff::3x2
NetBIOS over Tcpip. . . . . : Enabled

Wireless LAN adapter Wireless Network Connection:

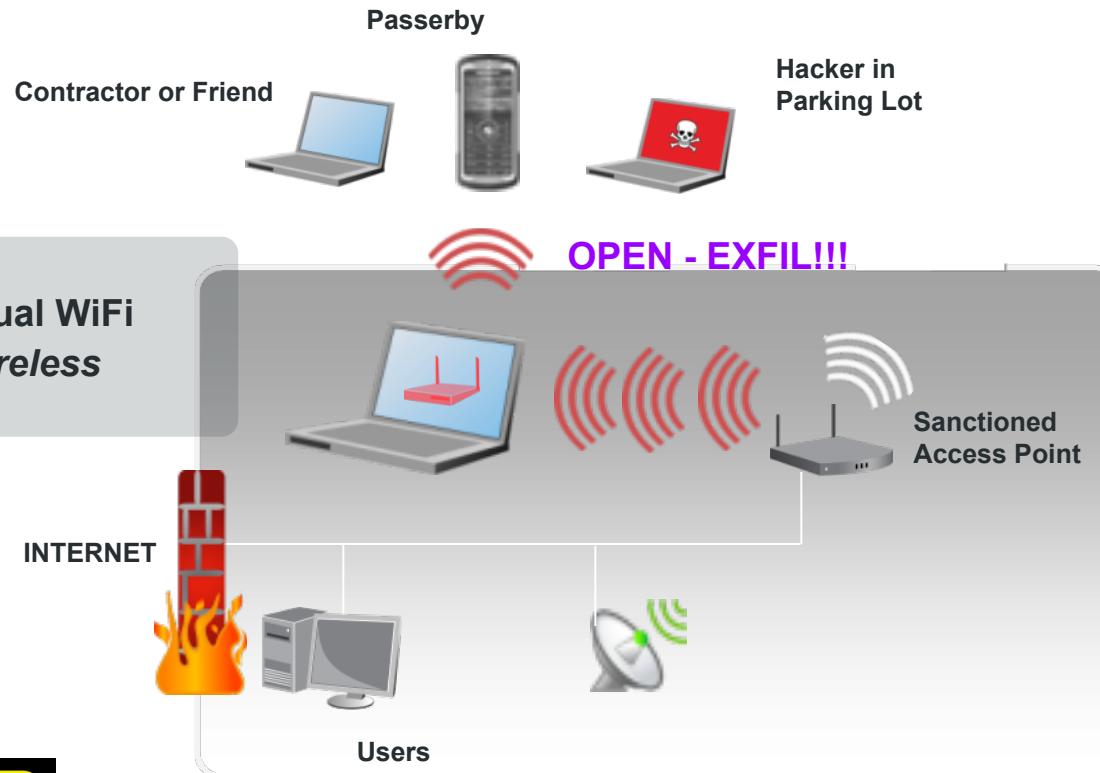
Connection-specific DNS Suffix . . . . . : launchmodem.com
Description . . . . . : Dell Wireless 1490 Dual Band WLAN Mini-Ca
rd
Physical Address . . . . . : 00-23-[REDACTED]
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::3183:[REDACTED]
IPv4 Address . . . . . : 192.168.1.87<Preferred>
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Friday, February 12, 2010 12:05:53 PM
Lease Expires . . . . . : Saturday, February 13, 2010 12:05:53 PM
Default Gateway . . . . . : 192.168.1.254
DHCP Server . . . . . : 192.168.1.254
DHCPv6 IAID . . . . . : 218112846
DHCPv6 Client DUID . . . . . : 00-01-00-01-[REDACTED]

DNS Servers . . . . . : 192.168.1.254
192.168.1.254
NetBIOS over Tcpip. . . . . : Enabled
```

Wireless Rogues on Network - Virtual WiFi



Wireless Rogues on Network - Virtual WiFi



Nearby IoT Threats - Drones

- Video and Audio Surveillance, Wireless surveillance
- Drop cellphones, pathogens, battery operated spy cameras
- Consumer drones pair via WiFi (Virtual AP) with smartphones and tablets
- Most organizations blind to threat (1-2 per day, 3-7 per week)



Drones



Drones



- Forensics/Detection - who, what, when, where, how

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
10:A4:BE: [REDACTED]	-38	177	1058	10	1	54e.	OPN		FLD-3a7 [REDACTED]

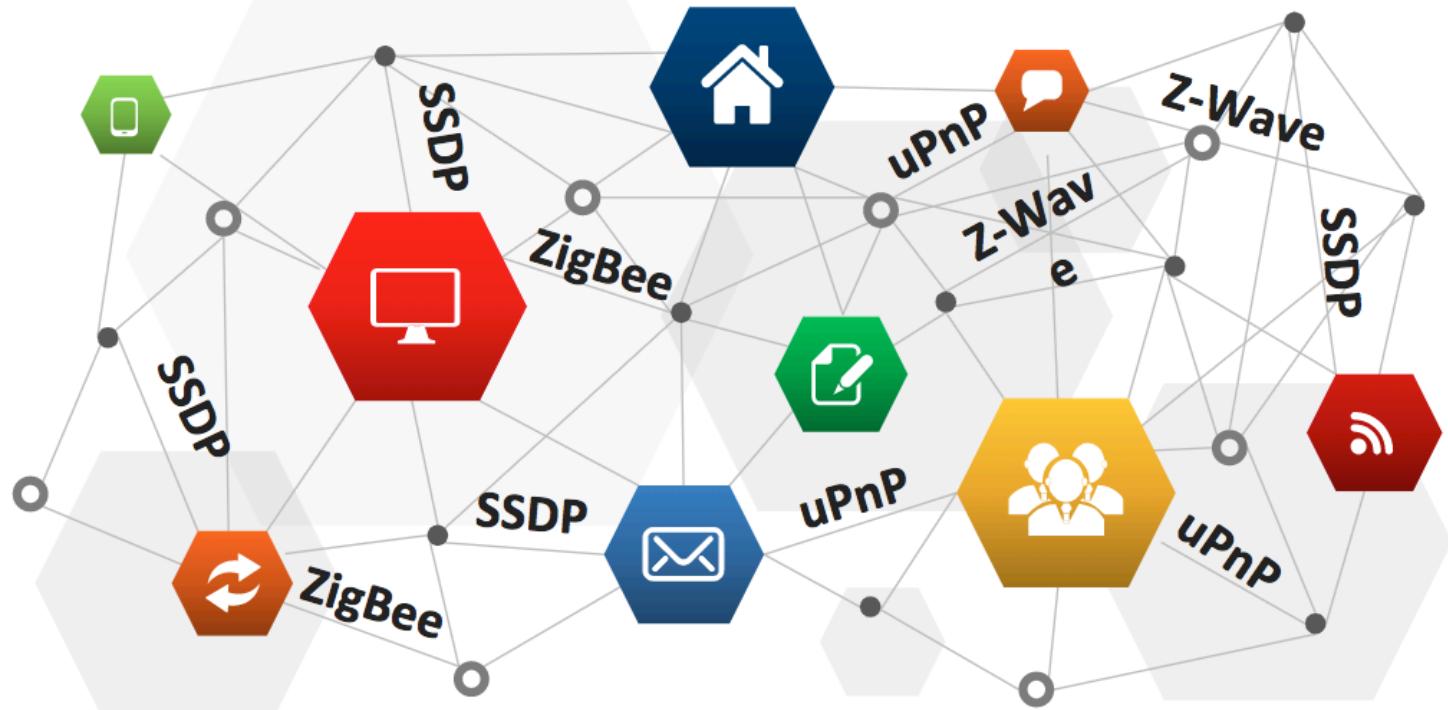
BSSID	STATION	PWR	Rate	Lost	Frames	Probe
10:A4:BE: [REDACTED]	98:F1: [REDACTED]	-34	54e-54e	472	1075	

```
root@kali:/home#
```

This is the MAC address of my Android device. Notice that the WiFi is Open with no security.

Notice that the SSID begins with “FLD-“. This then followed by the last 3 octets of the Drone’s MAC address (BSSID)

IoT Protocol Exfiltration



Exploiting Lack of Integrity in IoT Protocols



- What - Many devices support UPnP to allow an app or other devices to discover other devices (M2M)
- Sends multicast packets broadcasted to local network
- SSDP UPNP - Simple Service Discovery Protocol (Part of Universal Plug and Play)
 - M-SEARCH - Discover packet sent by app or another device
 - NOTIFY - Device announces itself on the network, routinely, and also when it leaves

Exploitation of SSDP - ULA OPT Field



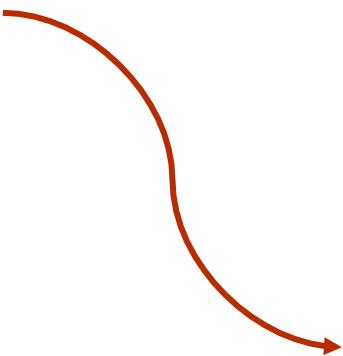
- ULA OPT FIELD
 - Unique Local Addresses - Site-Routable
 - Used in NOTIFY and M-SEARCH messages
 - For use in IPv4 and IPv6 (for backward compatibility)

Reference: <http://upnp.org/specs/arch/UPnP-arch-DeviceArchitecture-v1.1-AnnexA.pdf>

UDP - Exploitation of SSDP



Our Target



ssdp_wemo_test.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
23168	1228.265	[REDACTED]	c03:...	QUIC	85	Payload (Encrypted),
23169	1228.276	[REDACTED]	800:...	QUIC	85	Payload (Encrypted),
23170	1228.335	[REDACTED]	30:e...	QUIC	92	Payload (Encrypted),
23171	1228.435	89 43.861106196 192.168.1.68	239.255.255.250	SSDP	143	M-SEARCH * HTTP/1.1
		437 213.976658511 192.168.1.68	239.255.255.250	SSDP	143	M-SEARCH * HTTP/1.1

Simple Service Discovery Protocol

NOTIFY * HTTP/1.1\r\n

Request Method: NOTIFY

Request URI: *

Request Version: HTTP/1.1

HOST: 239.255.255.250:1900\r\n

CACHE-CONTROL: max-age=1800\r\n

LOCATION: http://192.168.1.75:49152/description.xml\r\n

OPT: "http://schemas.upnp.org/upnp/1/0/"; ns=01\r\n

01-NLS: ad [REDACTED]

NT: upnp:rootdevice\r\n

NTS: ssdp:alive\r\n

....1.. NOTIFY

* HTTP/ 1.1.HOS

T: 239.2 55.255.2

50:1900. .CACHE-C

ONTROL: max-age=

1800. .LO CATION:

http://1 92.168.1

Simple Service Discovery Protocol (ssdp), 408 bytes

Packets: 151109 - Displayed: 151109 (100.0%) Profile: Default

SSDP OPT FIELD
FOR URL

UDP - Exploitation of SSDP



#RSAC

```
▼ Simple Service Discovery Protocol
  ▼ NOTIFY * HTTP/1.1\r\n
    ▶ [Expert Info (Chat/Sequence): NOTIFY * HTTP/1.1\r\n]
      Request Method: NOTIFY
      Request URI: *
      Request Version: HTTP/1.1
      HOST: 239.255.255.250:1900\r\n
      CACHE-CONTROL: max-age=1800\r\n
      LOCATION: http://192.168.1.75:49152/description.xml\r\n
      OPT: "https://linktomyhiddenmessageonweb"; ns=01\r\n
```

- Modify SSDP OPT Field with Hidden Message, URL, etc.
- Covert communications, dead drop, malware callback to CnC for updates, etc.

Covert UDP - SSDP



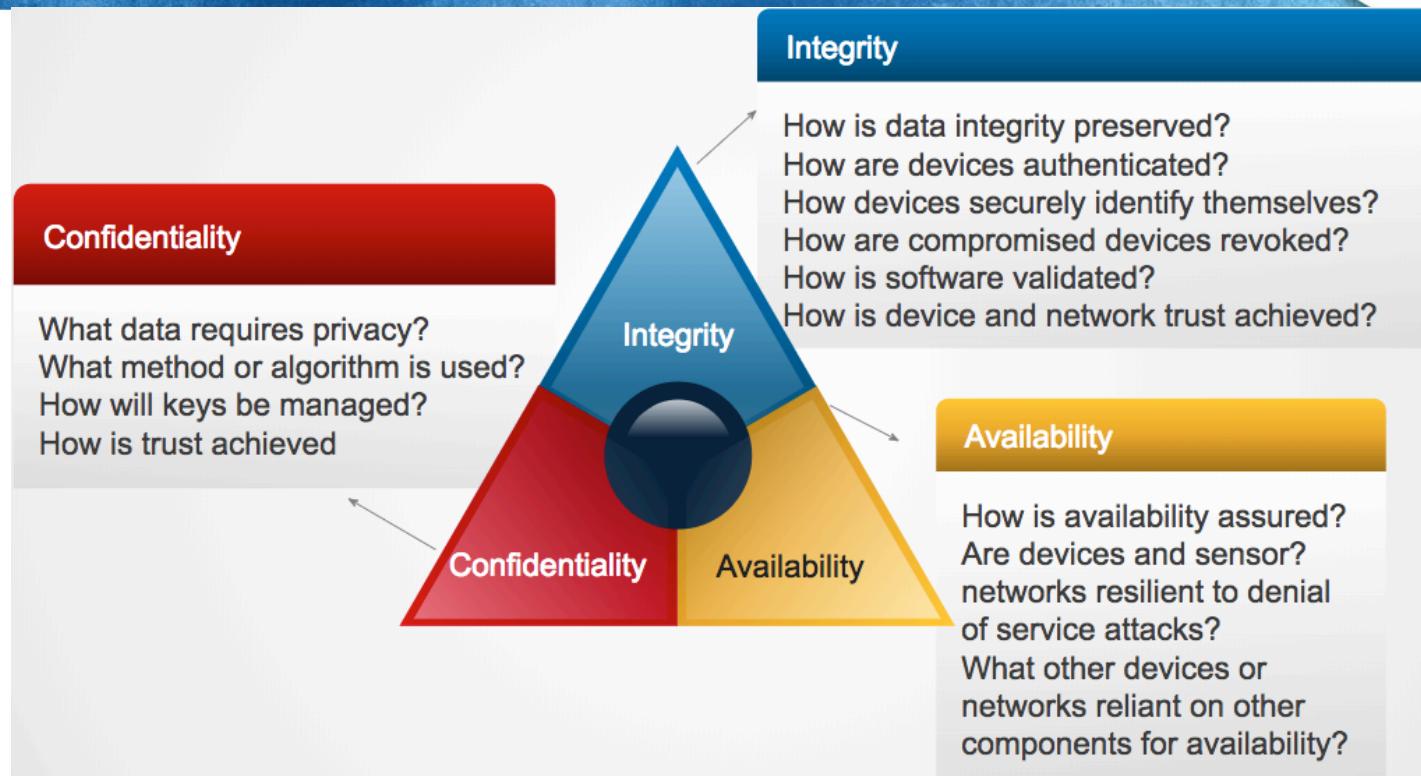
1. Smart Plug sends M-Search
2. M-Search packet embeds hidden message/content or CnC URL in OPT field
3. Received by other IoT devices on network

Two-way conversations using SSDP to hide content (M2M)



4. Smart TV receives M-Search packet and responds
5. NOTIFY packets send a packet back with embedded response

IoT Device Critical Considerations



RSA® Conference 2018



Exfiltration Demo

Exfiltration Case Study and Demo



- Exfiltration Example
- Typical Broadcast Message

```
broadCastMsg = \  
'M-SEARCH * HTTP/1.1\r\n' \  
'HOST:192.168.86.115:1900\r\n' \  
'ST:upnp:rootdevice\r\n' \  
'MX:2\r\n' \  
'MAN:"ssdp:discover"\r\n' \  
\r\n'
```

Exfiltration Case Study and Demo



- Exfiltration Example
- Typical Broadcast Message
- Broadcast Message Data Appending Example - Simple

```
broadCastMsg = \  
'M-SEARCH * HTTP/1.1\r\n' \  
'HOST:192.168.86.115:1900\r\n' \  
'ST:upnp:rootdevice\r\n' \  
'MX:2\r\n' \  
'MAN:"ssdp:discover"\r\n' \  
'Hello World\r\n'
```

Plain-Text
Insertion



Exfiltration Case Study and Demo



- Exfiltration Example
- Typical Broadcast Message
- Broadcast Message Data Appending Example - Obfuscated

```
broadCastMsg = \  
'M-SEARCH * HTTP/1.1\r\n' \  
'HOST:192.168.86.115:1900\r\n' \  
'ST:upnp:rootdevice\r\n' \  
'MX:2\r\n' \  
'MAN:"ssdp:discover"\r\n' \  
'894629\r\n'
```



Index to
pre-exchanged
lookup table

Python Script to Exfiltrate Data using SSDP



```
1 import socket
2
3 broadCastMsg = \
4     'M-SEARCH * HTTP/1.1\r\n' \
5     'HOST:239.255.255.250:1900\r\n' \
6     'ST:upnp:rootdevice\r\n' \
7     'MX:2\r\n' \
8     'MAN:"ssdp:discover"\r\n' \
9     'Hello World\r\n'
10
11 # Set up socket to receive IoT responses
12 udpSocket = socket.socket(socket.AF_INET, socket.SOCK_DGRAM, socket.IPPROTO_UDP)
13 udpSocket.settimeout(30)
14 udpSocket.sendto(broadCastMsg, ('239.255.255.250', 1900))
15
16 try:
17     while True:
18         data, address = udpSocket.recvfrom(65535)
19         print "Data: ", data
20         print "Address: ", address
21 except socket.timeout:
22     pass
23
```

```
=====
Data: HTTP/1.1 200 OK
ST: upnp:rootdevice
EXT:
USN: uuid:786fad77-04b4-4845-97f4-602b8885aeea::upnp:rootdevice
SERVER: Reciva UPnP/1.0 Radio/1.0 DLNA/DOC/1.50
CACHE-CONTROL: max-age=1800
LOCATION: http://192.168.86.41:8050/786fad77-04b4-4845-97f4-602b8885aeea/description.xml

Address: ('192.168.86.41', 1900)
=====
```



Response from
Bose Wave Radio

Prescription for better non-Exfil Hygiene



- Monitor for **anomalous network behaviors - wired AND wireless!!!**
 - Strange outbound destinations, and from what IoT source internally
 - Detection of odd (non-WiFi) frequencies and protocols (BT, Zigbee, etc.)
 - Out-of-band & off network WiFi connectivity
- Monitor for **neighboring IoT threats**
 - Drones, spy cameras, wireless attacks
- Monitor wired “and” wireless security postures across **Enterprise Network** and **IoT/IoT autonomous network deployments**
 - Misconfigurations
 - State change of devices
 - Cloud connections and Outbound Data Storage from IoT devices

Thank You!



Michael Rago
@MikeRago
www.802secure.com



Chet Hosmer
@PythonForensics
www.python-forensics.org