GT CONSULT

[ProdCon]

Bradley Geldenhuys – Hacking IoT Devices

What is an IoT device

The **Internet of things** (**IoT**) is a system of interrelated computing devices, mechanical and digital machines provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.

Therefore an IoT device is a sensor on that network that transmits data to another device

How do they communicate

WiFi/Ethernet

Bluetooth Low Energy

Radio Frequency

Zigbee / Z-Wave

NFC / RFID

WiFi/Ethernet

2.4GHZ and 5GHZ

TCP/UDP

IP Address

Router

Bluetooth BLE

- Bluetooth (Classic) VS BLE
- BLE = Bluetooth Low Energy
- Completely different protocols not interchangeable
- sleeps between connections (10x less power)
- connects super fast
- smaller packets
- 2.4Ghz
- Peripheral device and Central Device
- MESH Network capability
- Smart Watches and sensors
- Bluetooth 4.0 Nano USB Adapter

Radio Frequency - RF

- 433 MHz and 315 MHz
- Peripheral device and Central Device
- Sensors, Remotes, Gates, Doors
- HackRF One – Great Scott Gadgets
- Sonoff RF Bridge
- Broadlink IR + RF
- SDR – Software Defined Radio

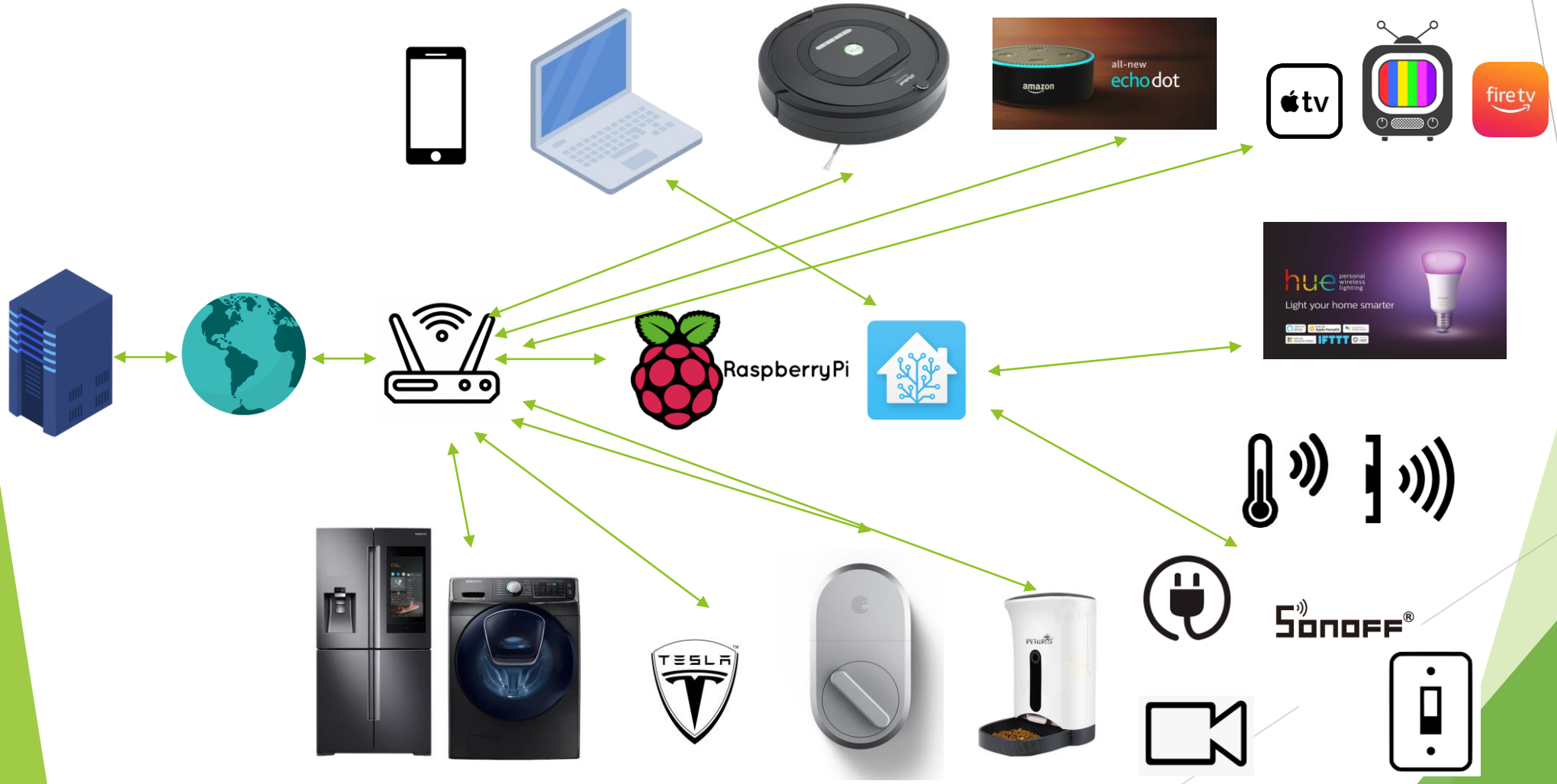
What about Zigbee and Z-Wave

- Z-Wave 908.42 MHz ZigBee 2.4Ghz
- ZigBee Is an Open Standard; Z-Wave Is Not (Owned by Silicon labs)
- ZigBee requires less power
- Z-Wave has a further distance advantage 10m-20m vs 90m-100m (Indoors)
- Zigbee 250 kbit/s vs 100 kbit/s
- Zigbee uses 128-bit keys Z-Wave uses Security 2 secure key exchange using Elliptic Curve Diffie-Hellman (ECDH)
- Zigbee 65000 vs Z-Wave network can consist of up to 232 devices
- Sonoff Zigbee Bridge / Hubitat Elevation Home Automation Hub

Taking a closer look at MQTT

- **(MQ Telemetry Transport or Message Queuing Telemetry Transport)** is an open OASIS and ISO standard (ISO/IEC 20922) lightweight, publish-subscribe network protocol that transports messages between devices. The protocol usually runs over TCP/IP; however, any network protocol that provides ordered, lossless, bi-directional connections can support MQTT. It is designed for connections with remote locations where a "small code footprint" is required or the network bandwidth is limited.
- Broker Client Relationship
- Messages are sent in Topics
- Topics are subscribed to
- Connect, Disconnect, Publish
- No encryption on auth
- A lot of anonymous servers
- Wireshark / Mosquito Broker /MQTTLens

How does a smart home / office work



Identifying the Attack Surface

- Remote Access to Local Devices
  - Shodan
  - Google
  - Metasploit
  - Camerarader (RTSP)
- Local Access via RF / Zigbee / BLE / NFC / RFID
  - Remember those apps and devices I mentioned earlier ☺
- Local Access via WiFi / Ethernet
  - Aircrack-ng
- Shared Subnet
  - Wireshark
  - NMAP

TOTAL RESULTS

440,816

TOP COUNTRIES

United States	
China	
Korea, Republic of	
Germany	
Australia	

TOP ORGANIZATI

Google Cloud
Google
SK Broadband
Amazon.com
Hangzhou Alibaba A

TOP OPERATING S

Linux 3.x
Windows Server 20
FreeBSD 9.x

TOP PRODUCTS

MQTT
Mosquitto
OpenSSH
VNC
Microsoft ftpd

TOTAL RESULTS

5,033,544

TOP COUNTRIES

United States
China
Korea, Republic of
Brazil
Viet Nam

TOP SERVICES

554
8554
10554
1024
9090

TOP ORGANIZATIONS

Korea Telecom
China Telecom
HiNet
China Unicom Liaoning
VNPT

TOP OPERATING SYSTEMS

Linux 3.x
Linux 2.6.x
Linux 2.4.x
Windows 7 or 8
Windows Server 2008

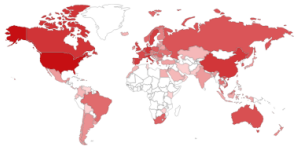
TOP PRODUCTS

Squid http proxy
Apple AirTunes roapd
Apple QuickTime Streaming Server
ACTi E32 webcam rtspd
Apache httpd

TOTAL RESULTS

47,532

TOP COUNTRIES



United States	6,211
Italy	3,440
Canada	2,863
Germany	2,856
China	2,727
More...	

TOP PORTS

8123	21,183
443	17,184
80	2,856
8443	381
8080	159
More...	

TOP ORGANIZATIONS

Cogent Communications	1,772
China Telecom	1,685
Comcast Cable	1,638
Telecom Italia	1,137
Ziggo	856
More...	

TOP PRODUCTS

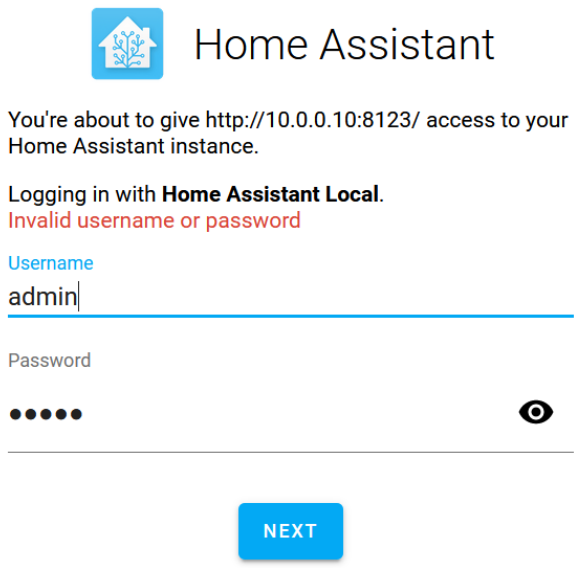
nginx	4,743
Apache httpd	94
Indy httpd	11
Postfix smtpd	9
Mosquitto	8
More...	

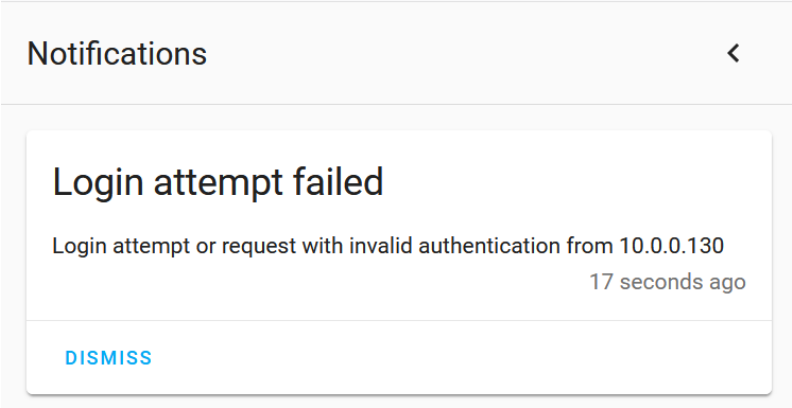
TOP OPERATING SYSTEMS

Windows 6.1	4
Linux 3.x	1

Brute Force

Home Assistant Login





Brute Force

RTSP with docker run -t ullaakut/cameradar

```
docker run --net=host -t ullaakut/cameradar -t localhost -p 8554 -T 3s -s 3 -d
Loading credentials...ok
  > Loading credentials dictionary from path "/app/dictionaries/credentials.json"
  > Loaded 14 usernames and 25 passwords
Loading routes...ok
  > Loading routes dictionary from path "/app/dictionaries/routes"
  > Loaded 165 routes
Scanning the network...ok
  > Found 1 RTSP streams
Attacking routes of 1 streams...ok
Attempting to detect authentication methods of 1 streams...ok
  > Stream rtsp://:@127.0.0.1:8554/live.sdp uses basic authentication method
Attacking credentials of 1 streams...ok
Validating that streams are accessible...ok
▶       Device RTSP URL:        rtsp://admin:admin@127.0.0.1:8554/live.sdp
        Available:              ✔
        IP address:             127.0.0.1
        RTSP port:              8554
        Auth type:              basic
        Username:               admin
        Password:               admin
        RTSP route:             /live.sdp


✔ Successful attack: 1 device was accessed
```

Sniffing

```
▷ Transmission Control Protocol, Src Port: 64008 (64008), Dst Port: 1883 (1883), Seq: 1, Ack: 1, Len: 39
◢ MQ Telemetry Transport Protocol
  ◢ Connect Command
    ◢ 0001 0000 = Header Flags: 0x10 (Connect Command)
        0001 .... = Message Type: Connect Command (1)
        .... 0... = DUP Flag: Not set
        .... .00. = QOS Level: Fire and Forget (0)
        .... ...0 = Retain: Not set
      Msg Len: 37
      Protocol Name: MQIsdp
      Version: 3
    ◢ 1100 0010 = Connect Flags: 0xc2
        1... .... = User Name Flag: Set
        .1.. .... = Password Flag: Set
        ..0. .... = Will Retain: Not set
        ...0 0... = QOS Level: Fire and Forget (0)
        .... .0.. = Will Flag: Not set
        .... ..1. = Clean Session Flag: Set
        .... ...0 = (Reserved): Not set
      Keep Alive: 30
      Client ID: mqtt
      User Name: mqtt-spy
      Password: mqtt123
```

No.

20
22
24
25
26
28
29

essage from publishing client

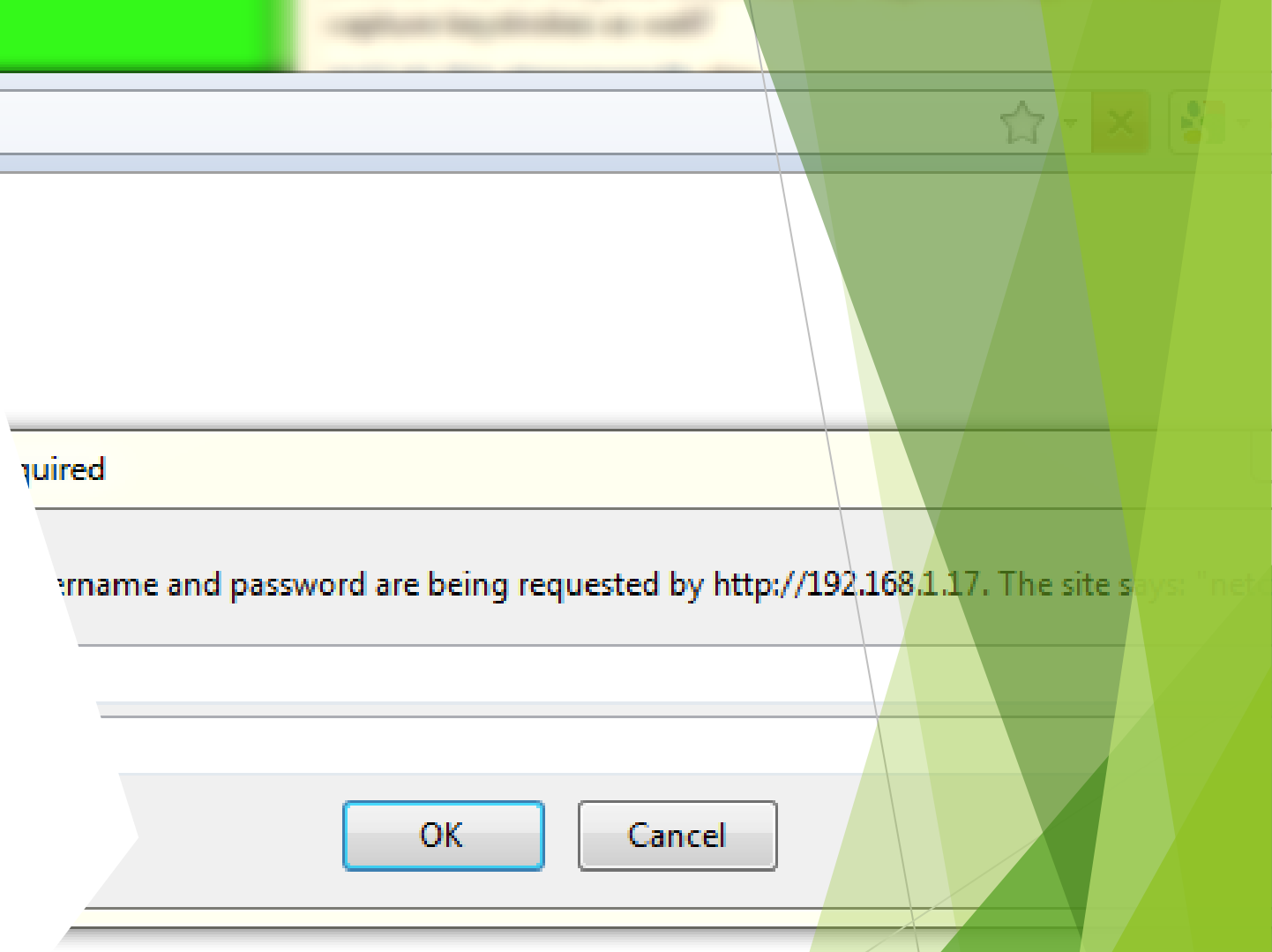
essage from broker to
g client

Exploits

Taplock BLE Exploit

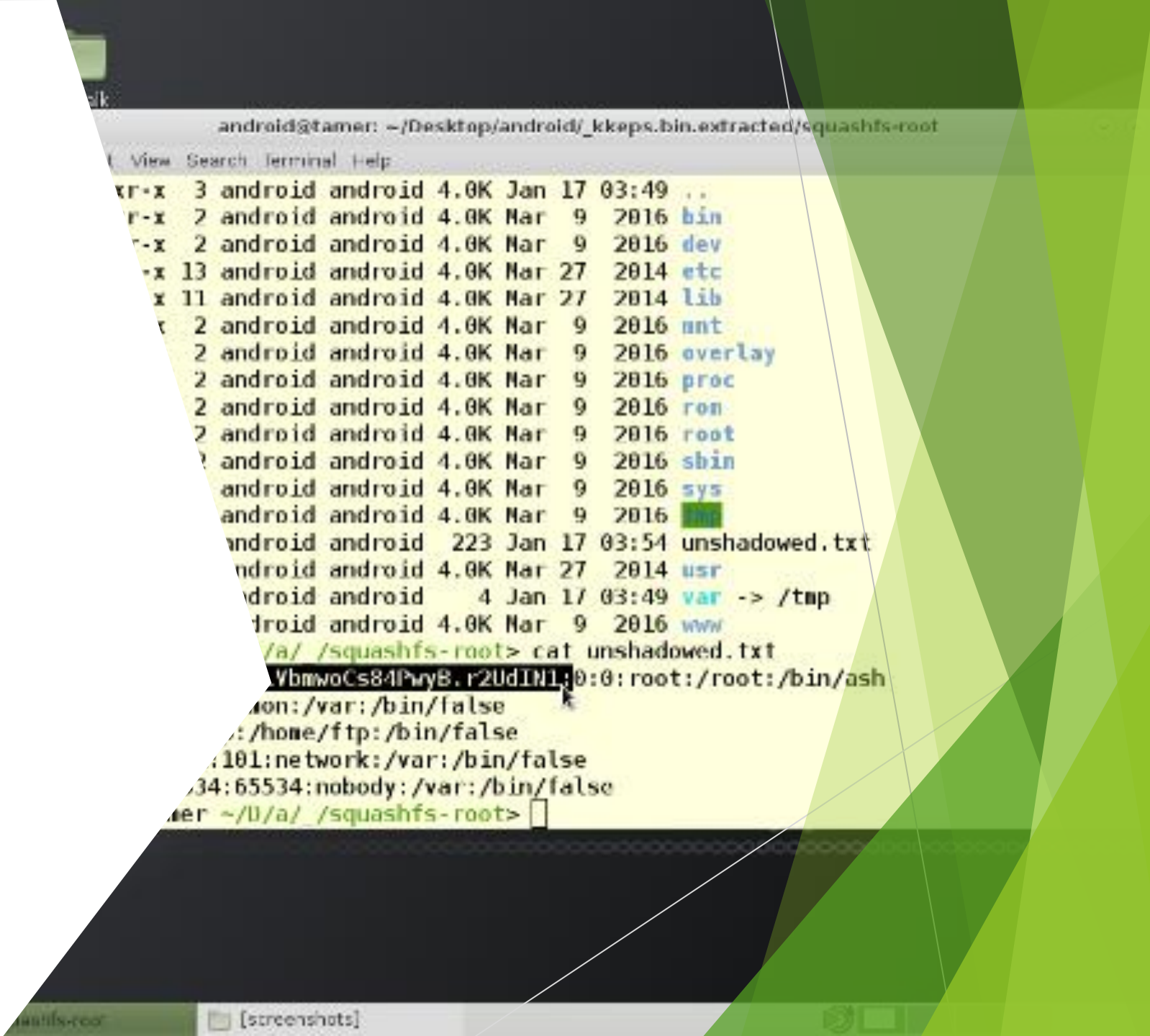
Authentication Bypass

/cgi-bin/anony/mjpg.cgi



Reverse Engineer

- Firmware
- .bin
- Binwalk



Takeaways

- Tasmota all the IoT things
- Secure Home Assistant and use the Multi Factor Authentication
- Force Authentication on the MQTT Broker
- HTTPS all the things / DuckDNS and Lets Encrypt (Don’t use personal naming)
- Virtual Tunnelling over Firewall Rules
- Don’t use the same username and password for all items
- Update firmware and software regularly
- VLAN IoT devices / Zero Trust Network Design
- Create a separate SSID for IoT Devices

References

- Hacking Bluetooth low energy (BLE) smart devices
  - https://medium.com/datadriveninvestor/hacking-bluetooth-low-energy-ble-smart-devices-bd58bf56268b
  - https://www.youtube.com/watch?v=3e4DBk5BKLg&feature=youtu.be
  - https://twitter.com/alissaknight
- HackRF One - https://greatscottgadgets.com/hackrf/one/
- Sonoff RF Bridge - https://sonoff.tech/product/accessories/433-rf-bridge
- Broadlink - http://www.ibroadlink.com/products/ir+rf
- RTLSDR - https://www.rtl-sdr.com/big-list-rtl-sdr-supported-software/
- Zigbee - https://en.wikipedia.org/wiki/Zigbee
- Zigbee Certificate Fall Back vuln - https://www.heise.de/security/meldung/Deepsec-ZigBee-macht-Smart-Home-zum-offenen-Haus-3010287.html
- Z-Wave - https://en.wikipedia.org/wiki/Z-Wave
- Zigbee vs Z-Wave - https://goodhomeautomation.com/z-wave-vs-zigbee-smart-home-protocols/
- MQTT - https://en.wikipedia.org/wiki/MQTT
- Tasmota - https://tasmota.github.io/docs/
- Camerader - https://github.com/Ullaakut/cameradar
- Iot Security Testing and Exploitation Framework - https://2018.pass-the-salt.org/files/talks/25-expliot.pdf
- Dissecting MQTT using Wireshark - http://blog.catchpoint.com/2017/07/06/dissecting-mqtt-using-wireshark/
- MQTT PwN - https://buildmedia.readthedocs.org/media/pdf/mqtt-pwn/latest/mqtt-pwn.pdf

References

- Taplock Exploit - https://www.pentestpartners.com/security-blog/totally-pwning-the-tapplock-smart-lock - https://www.youtube.com/watch?v=BLfI2_xOmK8&feature=emb_logo
- Binwalk - https://iotmyway.wordpress.com/2018/07/01/exploiting-the-vulnerable-kankun-smart-plug/
- Auth Bypass - http://console-cowboys.blogspot.com/2012/01/trendnet-cameras-i-always-feel-like.html
- Awesome IoT Hacks - https://github.com/nebgnahz/awesome-iot-hacks
- Awesome Embedded and IoT Security - https://github.com/fkie-cad/awesome-embedded-and-iot-security
- IOTsploit - https://github.com/iotsploit
- IoT Goat - https://github.com/OWASP/IoTGoat

Thank You

- Bradley Geldenhuys
- Brad@gtconsult.com
- Twitter @bradgcoza