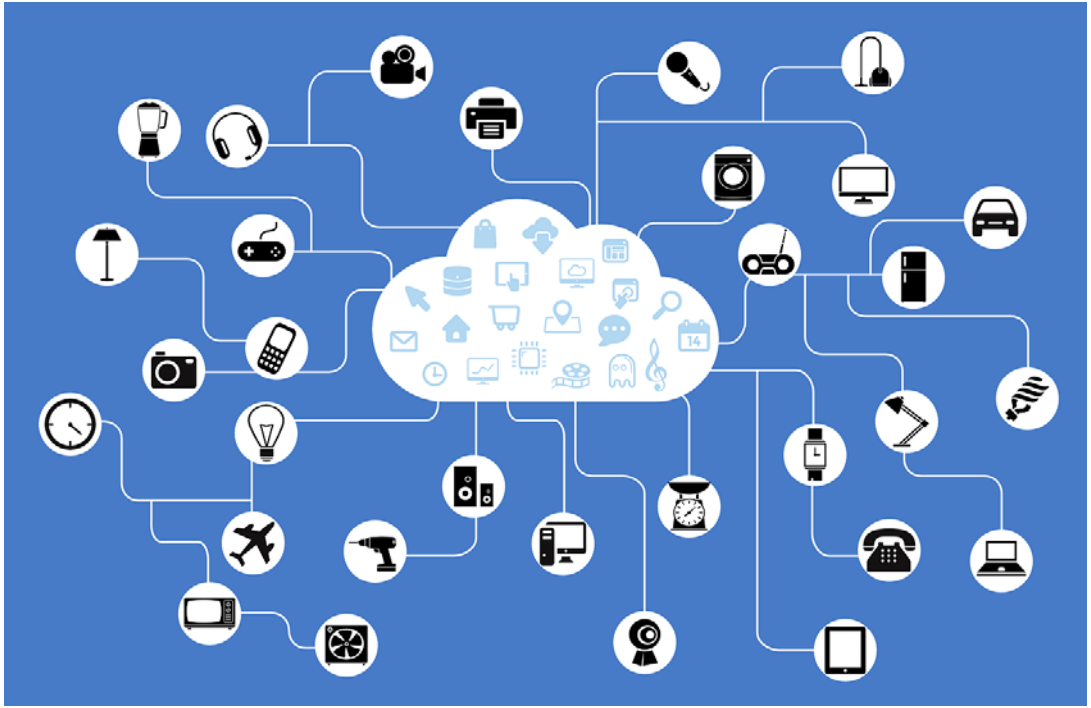
RSAConference2017
San Francisco | February 13 – 17 | Moscone Center

SESSION ID: HTA-R03

Lightweight Protocol! Serious Equipment! Critical Implications!

Lucas Lundgren
Senior Security Consultant
NCC Group
Twitter: @acidgen

Internet of Things



Internet of Things

Internet of Things

The end game
33. Rb7 Nf4 34. Bc4 – Black Resigns

RSAConference2017

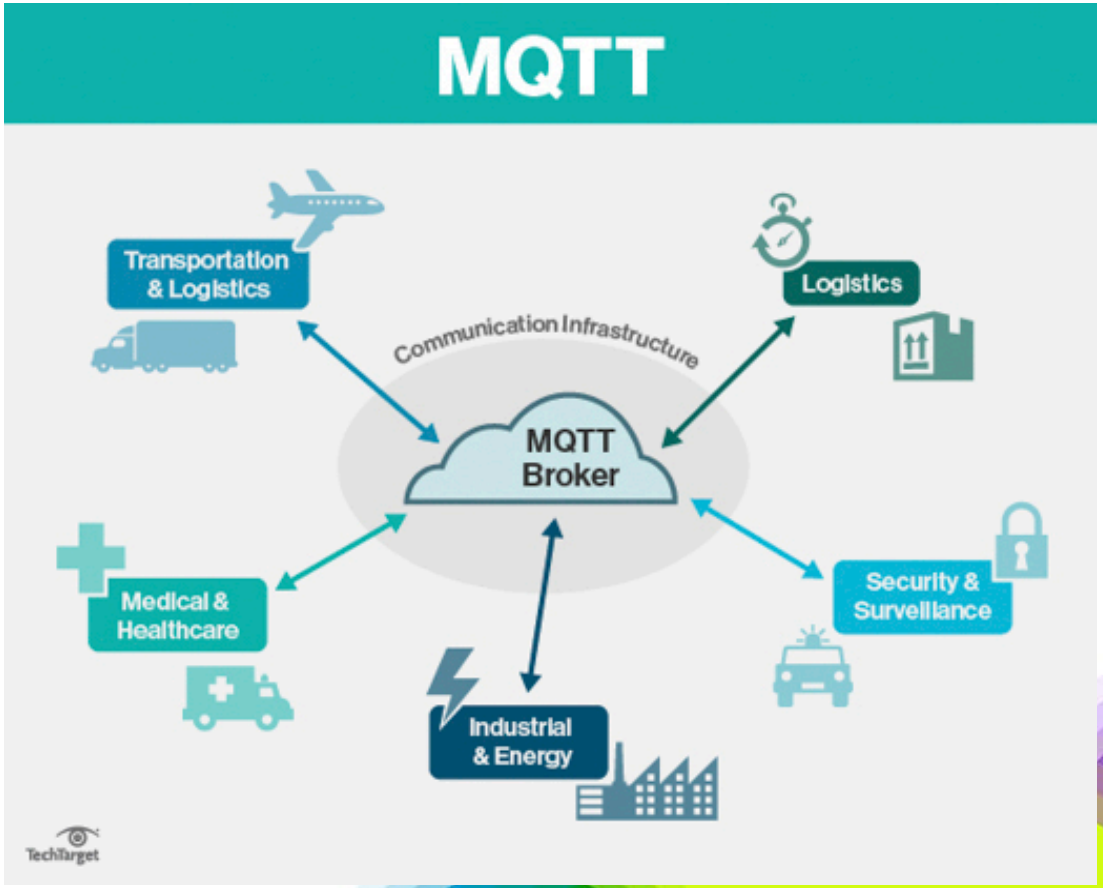
MQ Telemetry Transport

MQTT

MQ Telemetry Transport

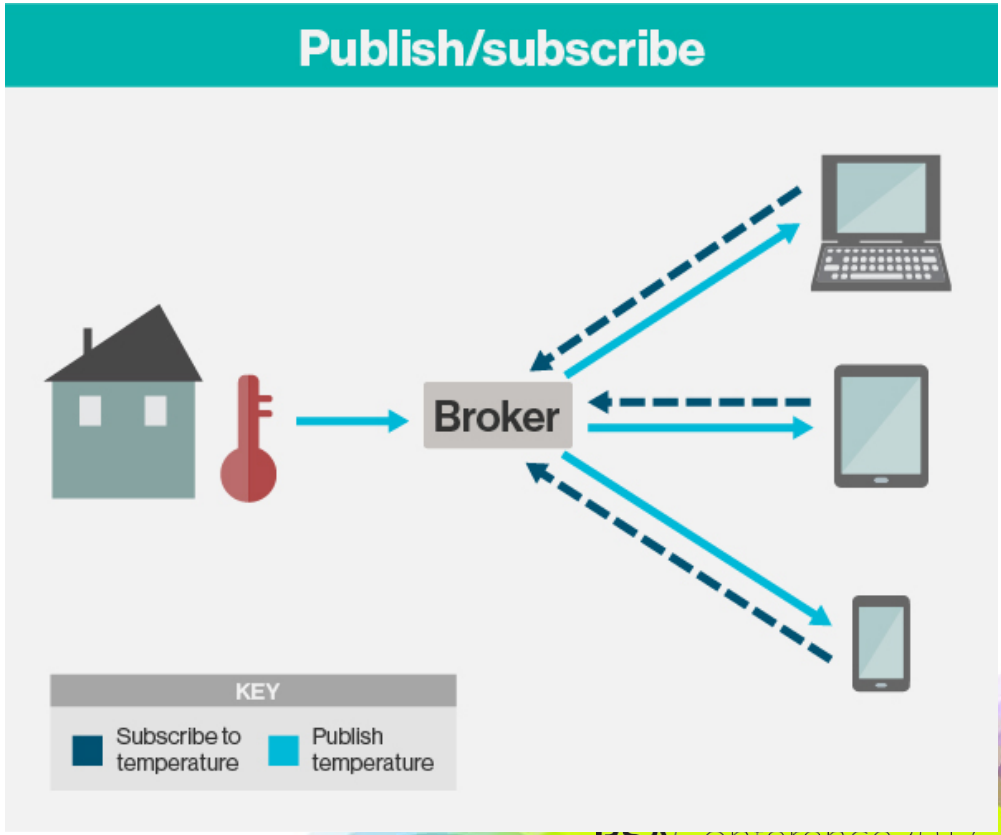
- Developed by Arlene Nipper (Arcom) and Andy Stanford Clarke (IBM)
- Combating Unreliable internet connection
- Quality of Service (QoS)
- Simplicity / Light Weight / Power Consumption Friendly
- Became Royalty Free as of 2010
- Picked up by the OASIS standard (SAML,AMQP)
- The Facto Message Standard for ISO as of June 2016

MQ Telemetry Transport



MQ Telemetry Transport

- How does this work?
- Example Topic:
- Myhouse/attic/temp1
- Myhouse/#



I never heard of it MQTT, have you?

- Found port 1883 during a test for a client
- Dug deeper and was introduced by the same things you are right now

MQ Telemetry Transport

- So what? Just give me the problem already!

RSAConference2017

MQ Telemetry Transport

Security

MQTT Manual and Security

- Taken From the official manual on MQTT
  - Devices could be compromised
  - Data at rest in Clients and Servers might be accessible
  - Protocol behaviors could have side effects (e.g. “timing attacks”)
  - Denial of Service (DoS) attacks
  - Communications could be intercepted, altered, re-routed or disclosed
  - Injection of spoofed Control Packets
  - Exists in hostile environments and should have U/P/E

MQTT – Public test servers

- Demo (Live)

RSAConference2017

MQ Telemetry Transport

Research

Scouring Internet for port 1883

- So what if we scanned the entire internet?
- I want DATA not just that the port is open
- What known sign can you use to LISTEN to everything on a broker?
- That's right # (Hashtag)
- Modified the scanner (Masscan) to Send data in Subscribe to #

Here thy be stats

- Around 59.000 Brokers (Servers)
- Unknown amount of devices (100.000+ can be connected per broker)
- Uncountable amount of Server types (Open Source, Closed Source)

Data Collected

- Emergency Response System

Data Collected

- Pipeline Presssure Control

```
Pipeline Pressure(Control server)
XXXX/XXXXX/XXX: cc=CGUA&site=XXXXX&utype=TM804&loc=XXXX
22&stavgs=true&bursts=/mnt/cf/bursts/&useFTP=true&
FTPsvr=XXXXXXXXXXXXXX&FTPusr=cXXX&FTPpw=fmXXXXXXXXXXX
XX&FTPavgs=true&useMQTT=true&MQTTpfx=XXXXXXXXX&MQTTsvr=
XXXXXXXXXXXXXXXX&MQTTprt=1883&useFlwM=false&flowSlp=
1.XXXXXXXX&flowIcp=12.XXXXXX&presSen=IMPRESS&presSlp
=3.46455E-7&presIcp=2.505623&XXXXXXX=XXX
```

Data Collected

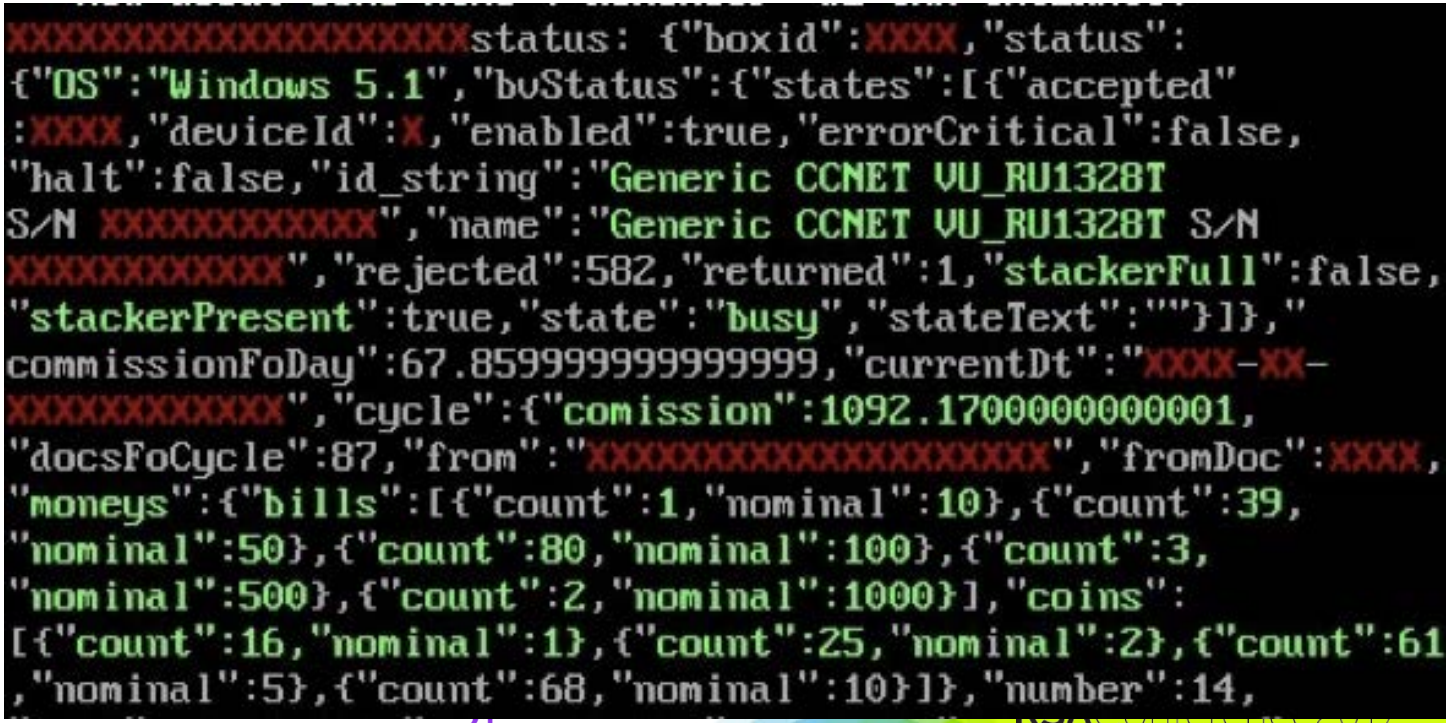
- Cars

Cars (I think it is, since its on a road moving Lat+Long)


```
[{"t":"XXXXXXXXXXXXXXXXX","d":[{"id":
"GPS_LatLng","v":"XXXXXXXXXXXXXXX
XXXXX"},{"id":"F_SPEED","v":"81"},
{"id":"F_LON_G","v":"0.2 "},{"id":"F_ACL_POS",
"v":"81"},{"id":"F_SW_BRAKE","v":"0"},
{"id":"F_TURNR","v":"0"},{"id":"F_TURNL","
v":"0"},{"id":"F_SENSOR","v":"1"}]}]
```

ATM

- This is bad? Counted 15.000 Unique ATMS



Can it get any worse?

- Can it get worse?
- YES!

We can change it

- We can write, that means we can manipulate

MQTT Protection

How can we fix this?

What can we do to protect this? MQTT IS AWESOME

- Where's the actual problem?
  - Misconfiguration (NNNF – No Username/Password Encryption)
  - Exposure – Should the broker be exposed like this?
  - IP Whitelisting? – Might be an option
  - Even IoT Gateway (Firewall type etc)

What can we do to protect this?

- How about the battery driven? Low Voltage?
  - Encryption would decrease the battery / Life time
  - Username and password is simply not enough anymore
  - Segmented 3g/4g network is an option!
  - Wireless IoT type gateway, that handles encryption?

Apply

- Ports and traffic to look out for
  - Port 1883 TCP
  - Port 8883 TCP (MQTT Encrypted)

Example with Nmap:
nmap –sS –sV –v –p 1883,8883 –oA mqtt-scan IPRANGE
If you like more data:
nmap –sS –sV –v –p 1883,8883 –oA mqtt-scan-data –script=mqtt-subscribe IPRANGE

Apply

- Ask your IT Staff, since this can be different!
  - PASSWORD / ENCRYPTION if this is open and exposed, take action NOW!
  - Why does this need to be exposed?
  - Can we lock it down?
  - What happens when this goes down?
  - How do we monitor and protect it ?
  - Is there any internal documentation?
  - Small Battery driven Sensors?
  - Talk to your THIRD party Supplier, (Alarms/sensors)

The end game
33. Rb7 Nf4 34. Bc4 – Black Resigns

Questions?

About, MQTT, IoT, Security? Need more examples?

Appendix A

- Buy an account at Shodan
  - Search for : org:”Your Org” port:1883,8889
- Nmap Scan (IP range e.g 192.168.1.0/24)
  - nmap –sS –sV –v –p 1883,8883 –oA file IPRANGE
  - nmap –sS –sV –v –p 1883,8883 –oA file –script=mqtt-subscribe IPRANGE

Appendix B

- Hodor.rb – Small insignificant script to read data from open brokers
  - http://bit.ly/2k5qQpa
- MQTT.FX Application used in the presentation:
  - http://mqttfx.jfx4ee.org

Appendix C

- Sources for Further reading:
- Security:
  - http://www.hivemq.com/blog/introducing-the-mqtt-security-fundamentals
- MQTT Manual and Setup:
  - http://mqtt.org/documentation