



IOT: EXPLORING THE THREAT SURFACE

Jason Ortiz

Sr. Integration Engineer

CONTENTS

INTRO

THE BIG IDEA

SECURING THE EDGE

SECURING THE REST

SECURING THE DATA

01 |

INTRODUCTION

02 |

THE BIG IDEA

EVERYTHING I KNOW ABOUT IOT

EVERYTHING I KNOW ABOUT IOT SECURITY



QUESTIONS?
THANK YOU.

EVERYTHING I THINK SORT OF MAKES SENSE...

- » IoT Ecosystem
 - » The Edge
 - » The Fog/Mist
 - » The Cloud

WHAT IS THE BIG IDEA?

» Data

TECHNOLOGY

YESTERDAY / BY MICHAEL ACCARDI

General Motors Watches You Listen To The Radio

» Data

Alphabet's 'smart city' idea sparks concerns over data use,
sharing of profits

» Data

» Simple

Internet of Things (IoT) in Healthcare Market Set to Exhibit Momentous Revenue Share at US \$322.77 Billion by 2025

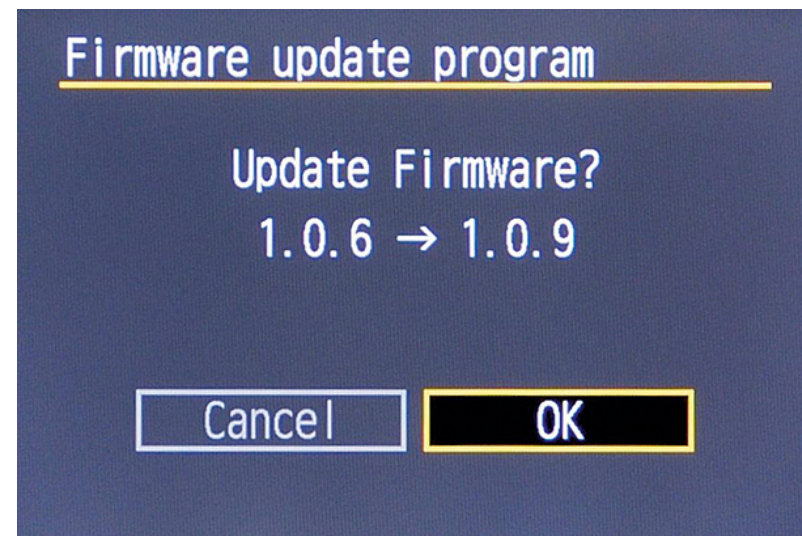
03 |

SECURING THE EDGE

FIRMWARE

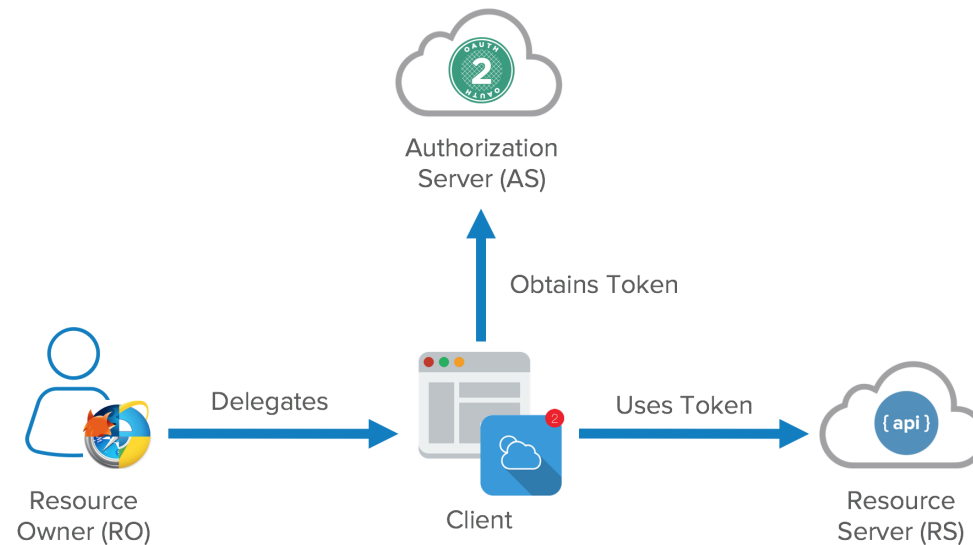
- » Vulnerabilities
 - » Conventional
 - » Stored keys?
 - » Memory dump keys?

- » Updates ... or NOT



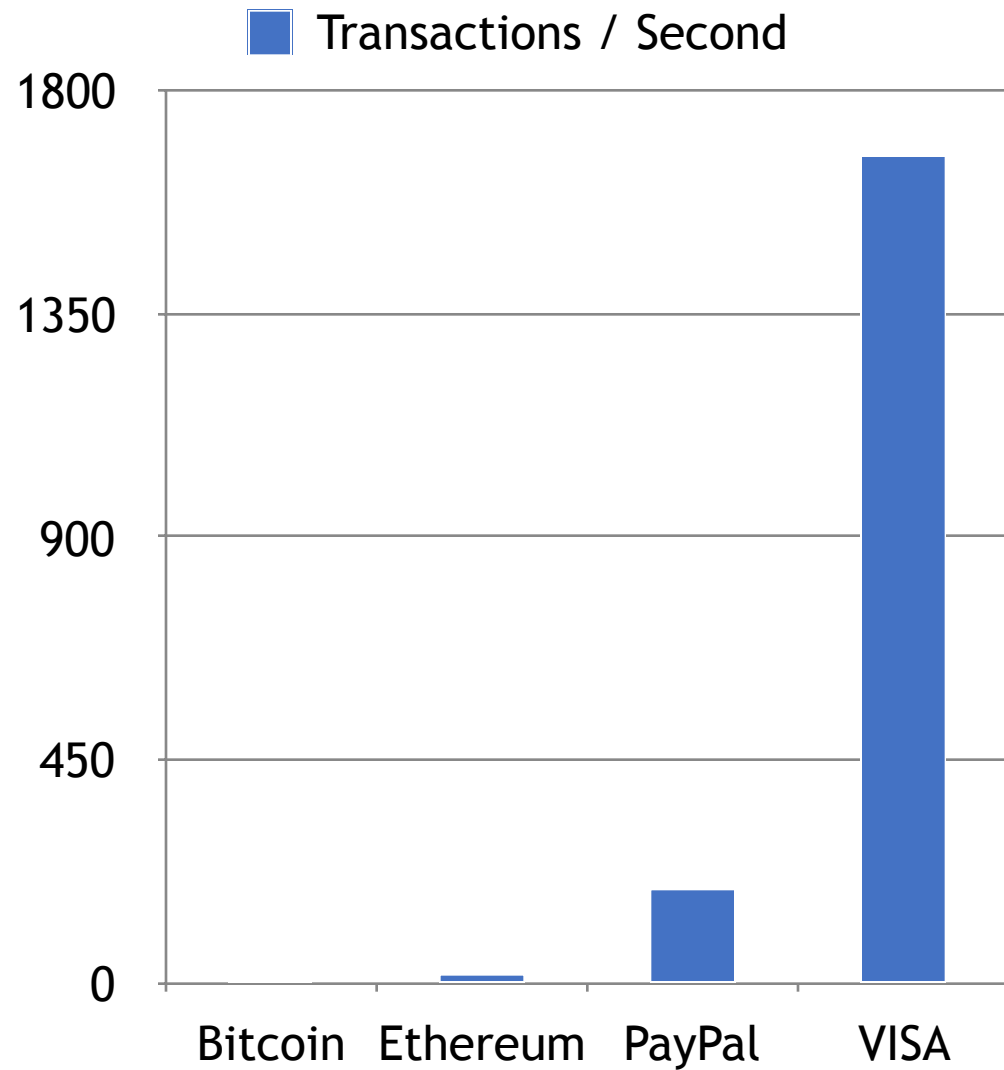
AUTHENTICATION

- » Sooooo many things!
- » Based mostly in HTTP



AUTHENTICATION

- » Elliptic Curve Crypto?
- » Blockchain?



PAYLOADS

#	downloaded malware	% of attacks
1	Backdoor.Linux.Mirai.c	15.97%
2	Trojan-Downloader.Linux.Hajime.a	5.89%
3	Trojan-Downloader.Linux.NyaDrop.b	3.34%
4	Backdoor.Linux.Mirai.b	2.72%
5	Backdoor.Linux.Mirai.ba	1.94%
6	Trojan-Downloader.Shell.Agent.p	0.38%
7	Trojan-Downloader.Shell.Agent.as	0.27%
8	Backdoor.Linux.Mirai.n	0.27%
9	Backdoor.Linux.Gafgyt.ba	0.24%
10	Backdoor.Linux.Gafgyt.af	0.20%

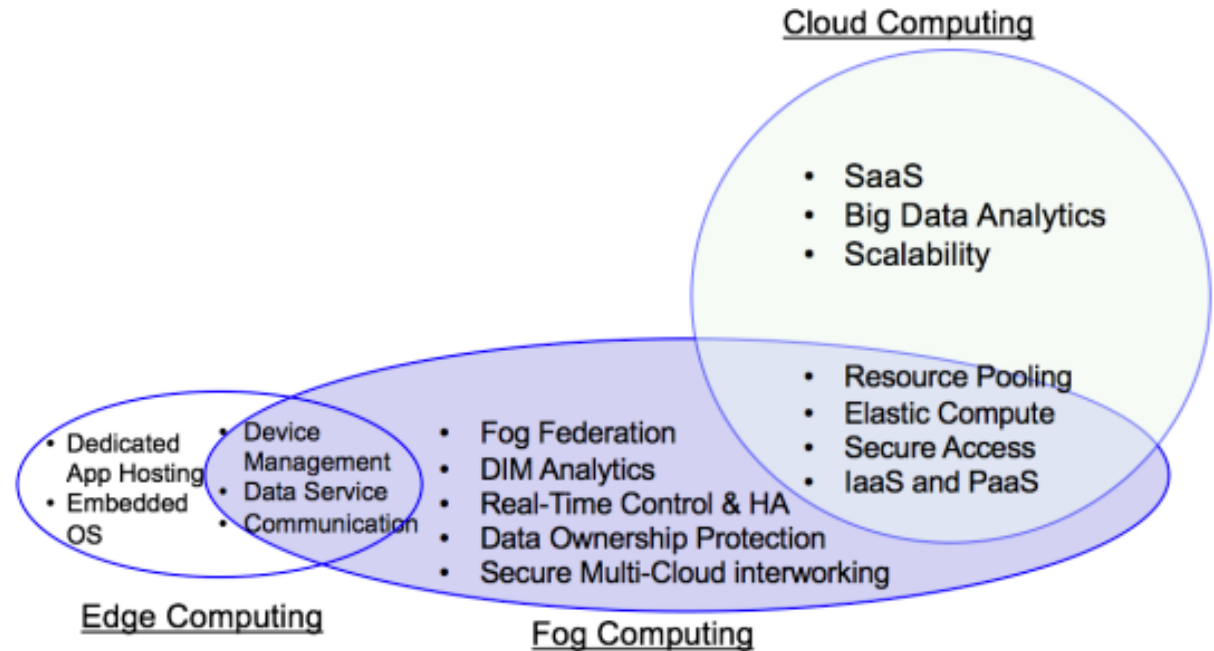
Top 10 malware downloaded onto infected IoT device following a successful Telnet password crack

04 |

SECURING THE MIST, OR FOG, OR WHATEVER

OK BUT REALLY

- » The Edge
- » The Fog
- » The Mist
- » The Cloud



COMPONENTS

- » Networking
- » Messaging
- » Data



NETWORKING

- » Which part?
 - » User -> Stand Alone Device?
 - » User -> Cloud Connected Device?
 - » User -> Hub?
 - » Device -> Hub?
 - » Hub -> Cloud?
 - » User -> Cloud?
 - » Device -> Device?
 - » Device -> Cloud?

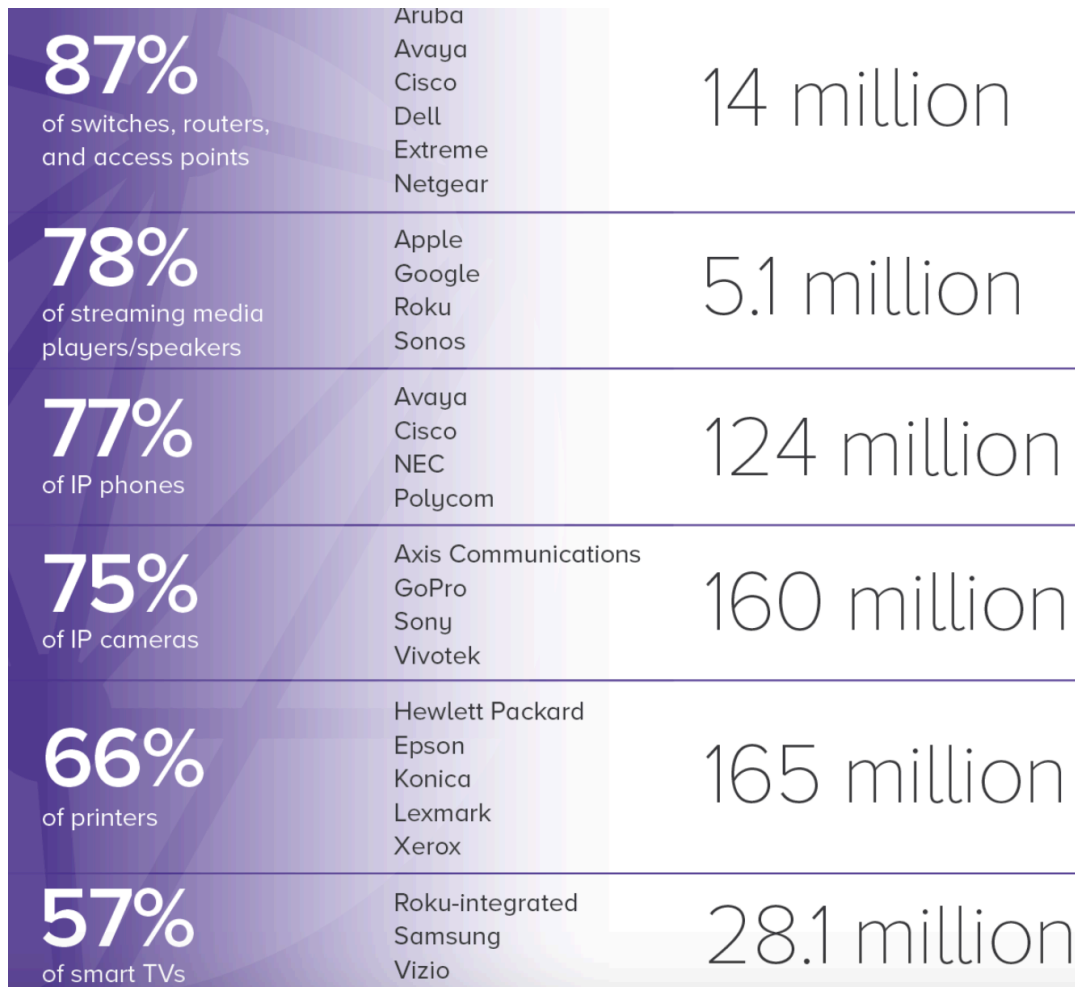
DNS REBINDING

- » Same Origin Policy
- » bad.js
- » [CVEs? You bet](#)



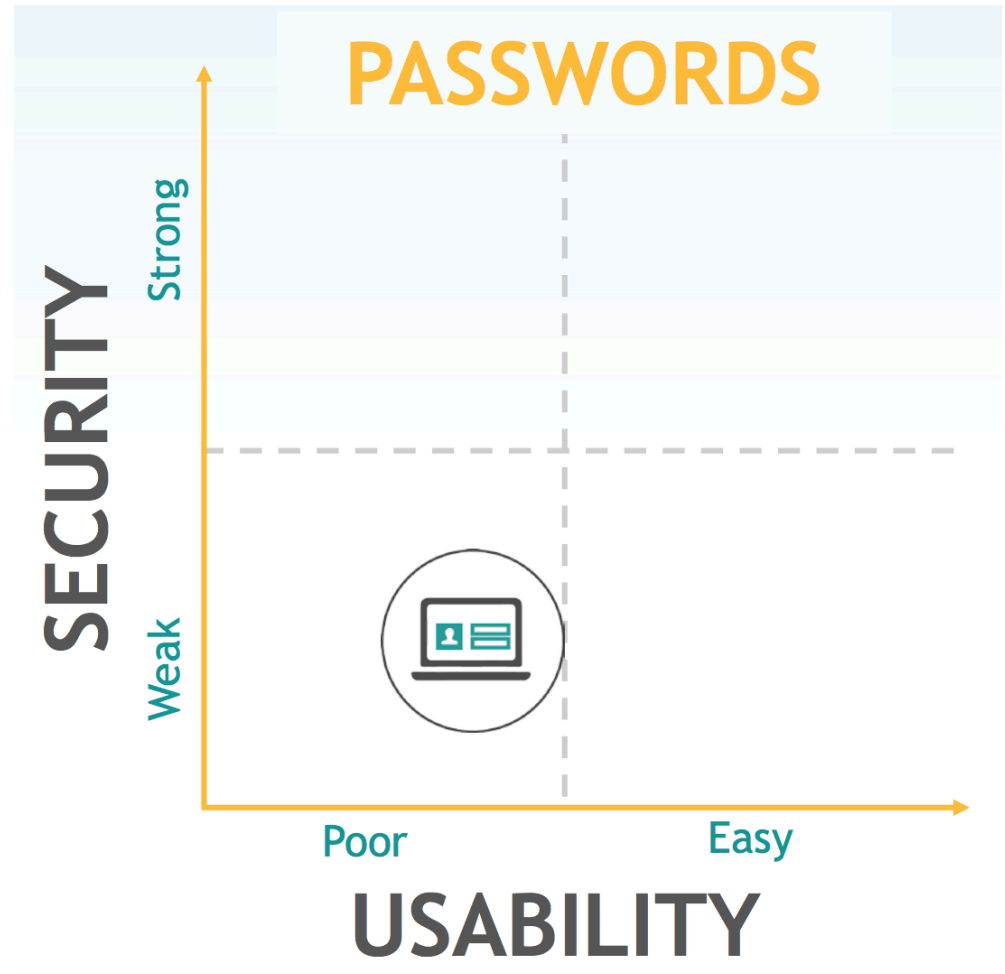
DNS REBINDING

» Vulns Everywhere!



SECURE NETWORKING?

- » Heavy Use of HTTPS
- » Authentication?
- » FIDO Alliance



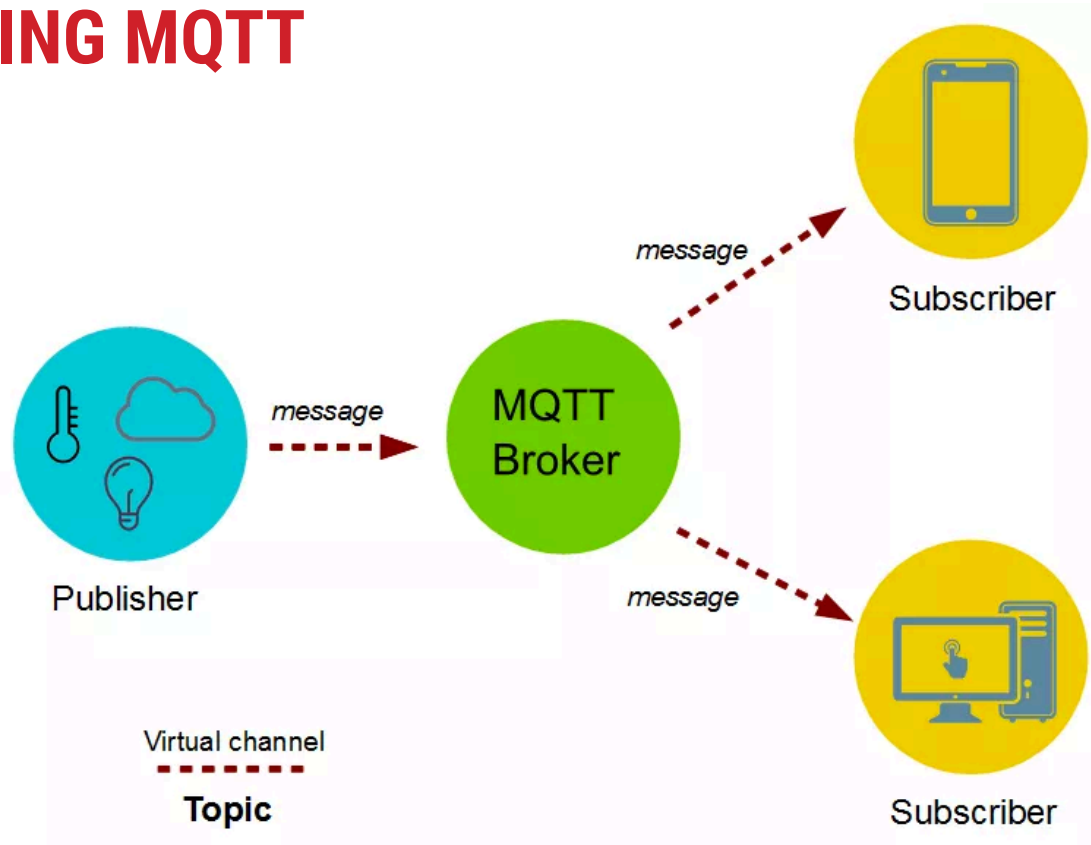
MESSAGING (QUEUES)

- » RabbitMQ
 - » [Complex setup](#)
 - » Basic security

- » [nats.io](#)
 - » Auth
 - » TLS

```
authorization {  
  users = [  
    {user: alice, password: foo}  
    {user: bob, password: bar}  
  ]  
}
```

MESSAGING MQTT

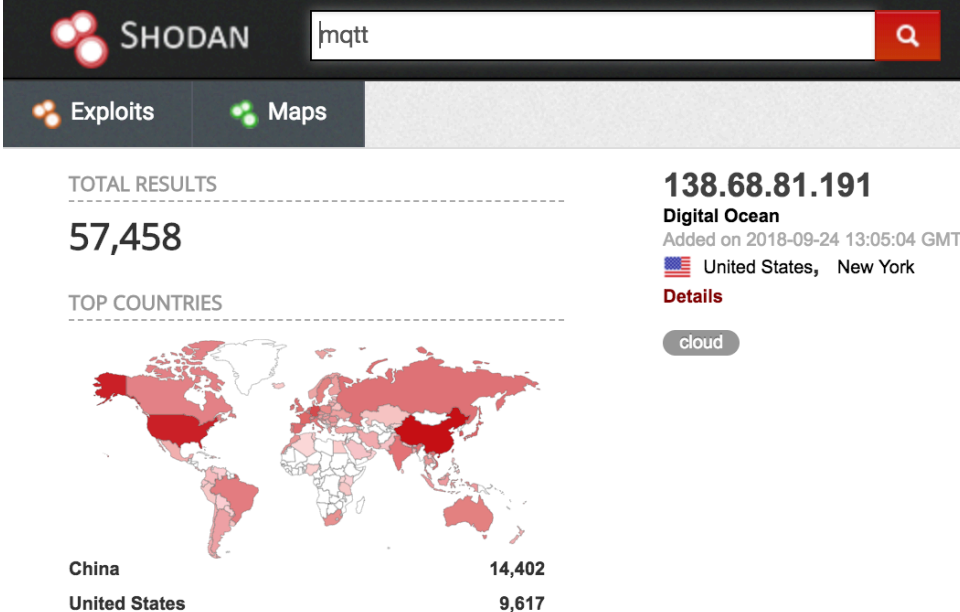


MESSAGING (MQTT)

» Anything interesting on a public broker?

» SHODAN

» C2 through MQTT



The screenshot shows the Shodan search interface. At the top, the Shodan logo is on the left, and a search bar contains the text 'mqtt'. Below the search bar are two tabs: 'Exploits' and 'Maps'. The main content area displays the search results for 'mqtt'. On the left, it shows 'TOTAL RESULTS' as '57,458'. Below this is a 'TOP COUNTRIES' section with a world map where countries are shaded in red. A table below the map lists the top countries: China with 14,402 results and the United States with 9,617 results. On the right side of the results, the IP address '138.68.81.191' is displayed in large text, followed by the organization 'Digital Ocean', the date 'Added on 2018-09-24 13:05:04 GMT', and the location 'United States, New York'. There is a 'Details' link and a 'cloud' button below the location information.

SHODAN mqtt

Exploits Maps

TOTAL RESULTS

57,458

TOP COUNTRIES

China 14,402

United States 9,617

138.68.81.191

Digital Ocean

Added on 2018-09-24 13:05:04 GMT

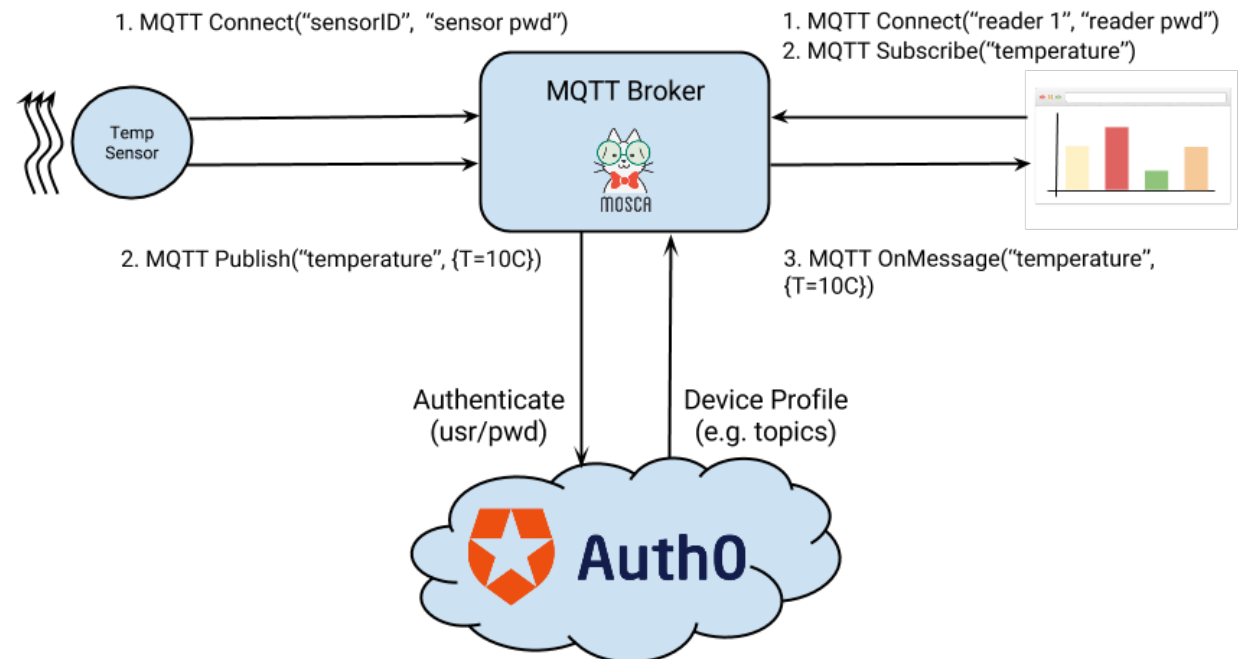
United States, New York

Details

cloud

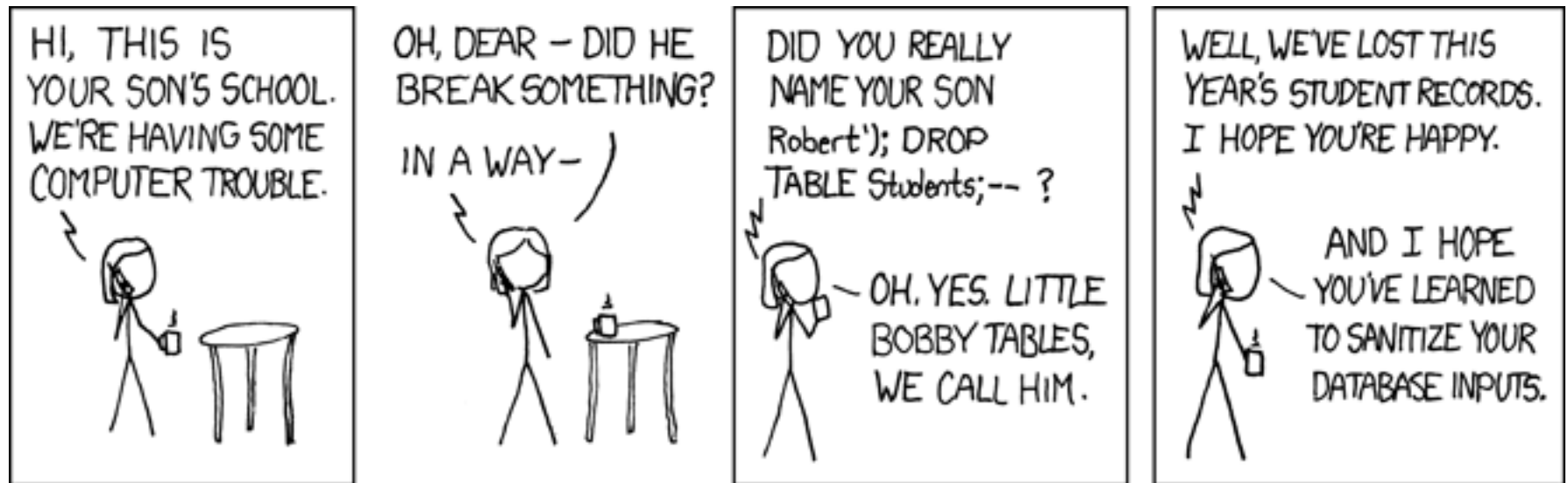
SECURING MQTT

- » Enterprise Solution (HiveMQ)
- » 3rd party broker



WEB INTERFACES

- » Basic Vulnerabilities
- » Custom HTTP servers ... but why?



Databases

» [Mongo](#)



» Postgres

```
# TYPE  DATABASE        USER            ADDRESS          METHOD
# "local" is for Unix domain socket connections only
local  all             all             trust
# IPv4 local connections:
host   all             all             127.0.0.1/32    trust
# IPv6 local connections:
host   all             all             ::1/128         trust
# Allow replication connections from localhost, by a user with the
# replication privilege.
local  replication     all             trust
host   replication     all             127.0.0.1/32    trust
host   replication     all             ::1/128         trust
host  all             all             trust
```

pg_hba.conf

05 |

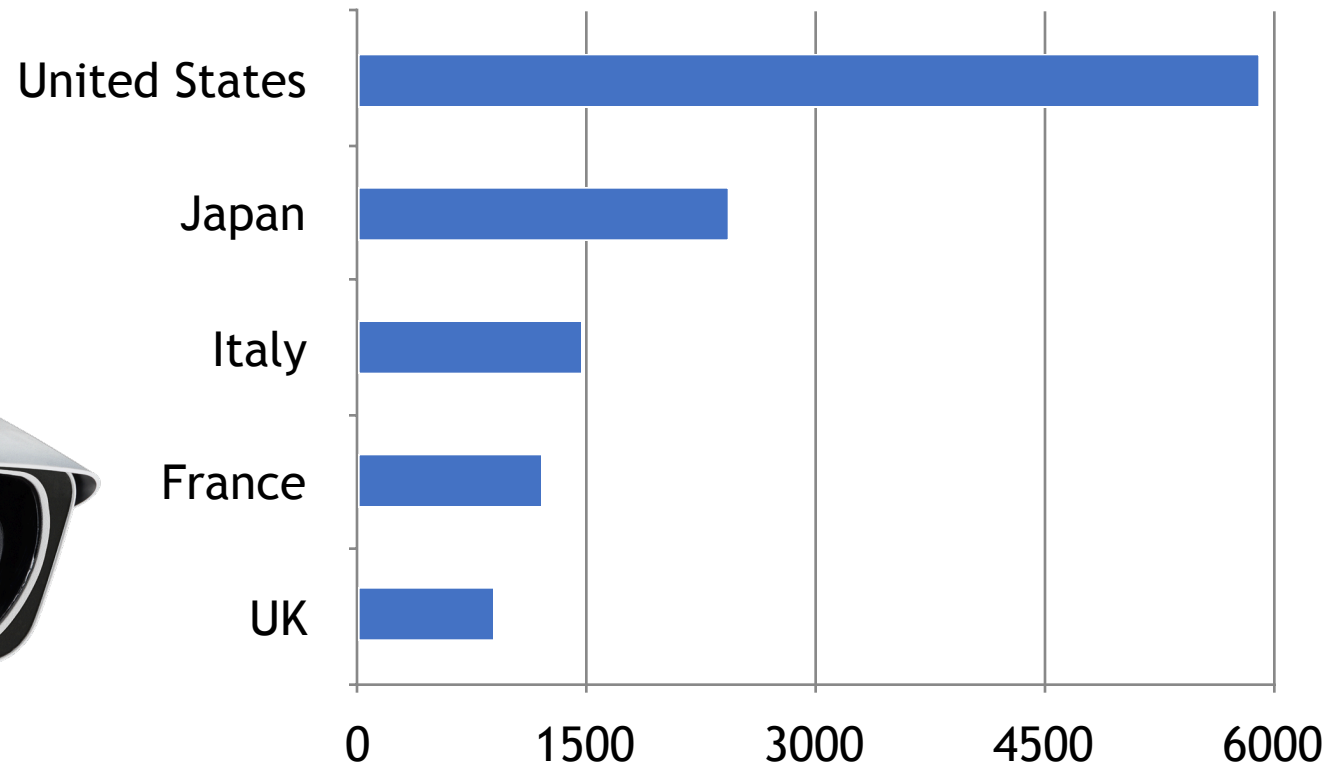
SECURING THE DATA

SECURING THE DATA

- » Make No Mistake ... I do mean PRIVACY
- » Is perimeter security dead?

SECURING THE DATA

» Cameras



SECURING THE DATA

» Cars and Cities?

TECHNOLOGY

YESTERDAY / BY MICHAEL ACCARDI

General Motors Watches You Listen To The Radio

Alphabet's 'smart city' idea sparks concerns over data use, sharing of profits

SECURING THE DATA

» Wearable Medical Devices



“Frankly, I don’t give a damn if someone wants to change their heart rate data.”

SECURING THE DATA

» Mobile/Automated Drs.



SECURING THE DATA

» Medical Data Everywhere

FDA Approves Blockchain/IoT Pilot to Track Specialty Prescription Drugs Across 3 States

PRESS RELEASE

Healthcare IoT market will witness massive growth due to Rising investments for implementation of IoT solutions in the U.S.

Published: Apr 25, 2019 2:02 p.m. ET

8 Amazing Software Medical Devices Reshaping the Healthcare Industry In 2019

Internet of Things (IoT) in Healthcare Market Set to Exhibit Momentous Revenue Share at US \$322.77 Billion by 2025

SECURING THE DATA





QUESTIONS?
THANK YOU.