PONDURANCE

IOT: EXPLORING THE THREAT SURFACE

Jason Ortiz

Sr. Integration Engineer

CONTENTS

01 | INTRODUCTION

02 | THE BIG IDEA

EVERYTHING I KNOW ABOUT IOT

EVERYTHING I KNOW ABOUT IOT SECURITY

PONDURANCE

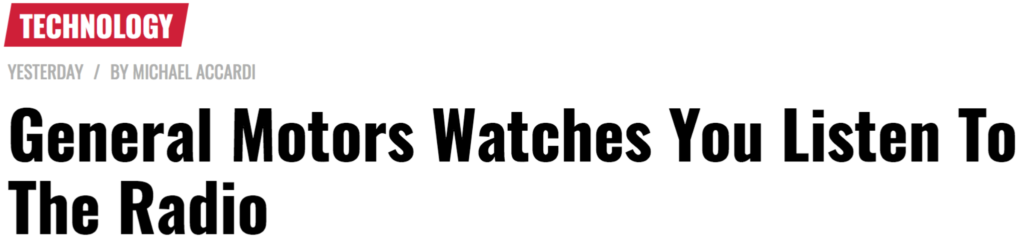
QUESTIONS?
THANK YOU.

EVERYTHING I THINK SORT OF MAKES SENSE…

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

WHAT IS THE BIG IDEA?

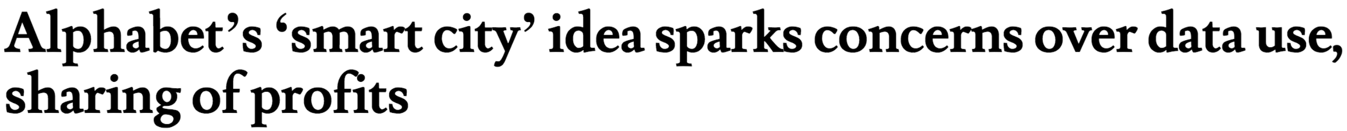
- Data
- Data
- Data
- Simple



TECHNOLOGY

YESTERDAY / BY MICHAEL ACCARDI

General Motors Watches You Listen To The Radio

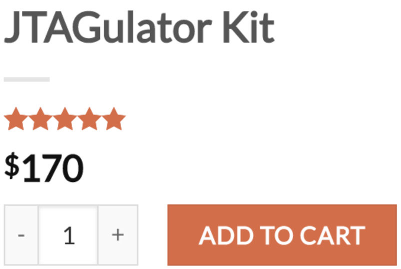


Alphabet's 'smart city' idea sparks concerns over data use, sharing of profits

03 | SECURING THE EDGE

HARDWARE

- Physical Ports
  - uArt
  - JTAG



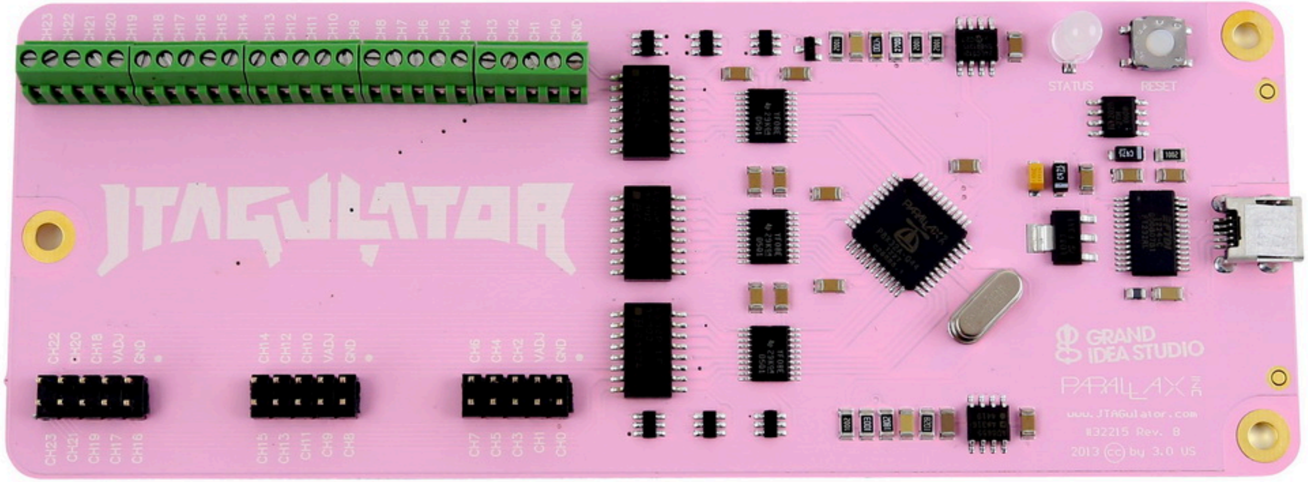
JTAGulator Kit

★★★★★

$170

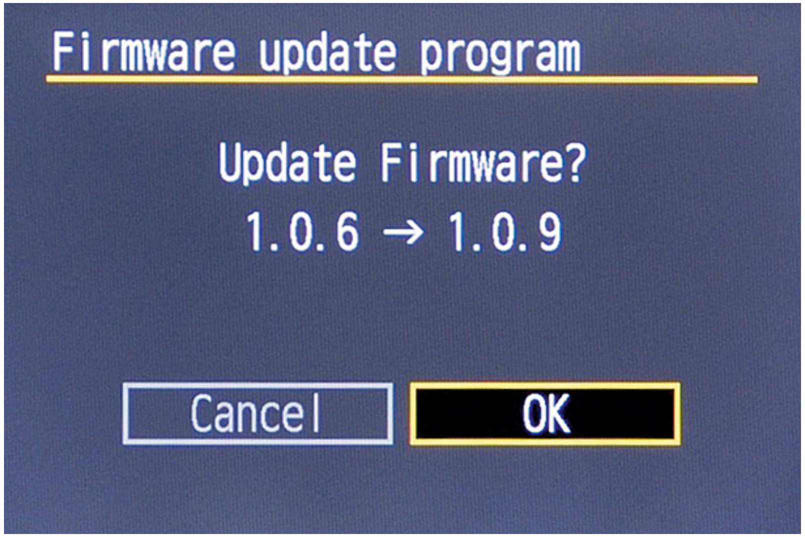
- 1 +

ADD TO CART



FIRMWARE

- Vulnerabilities
  - Conventional
  - Stored keys?
  - Memory dump keys?
- Updates … or NOT



Firmware update program

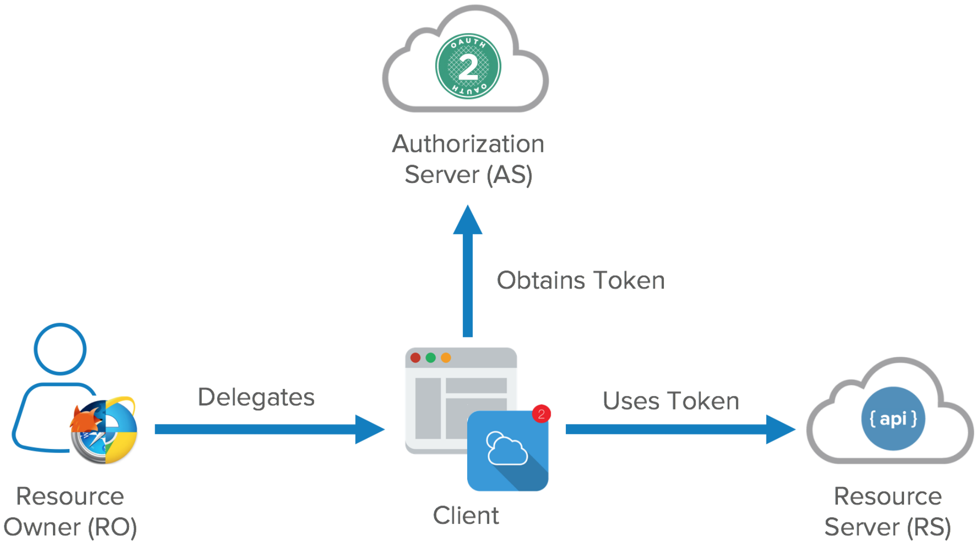
Update Firmware?

1.0.6 → 1.0.9

AUTHENTICATION

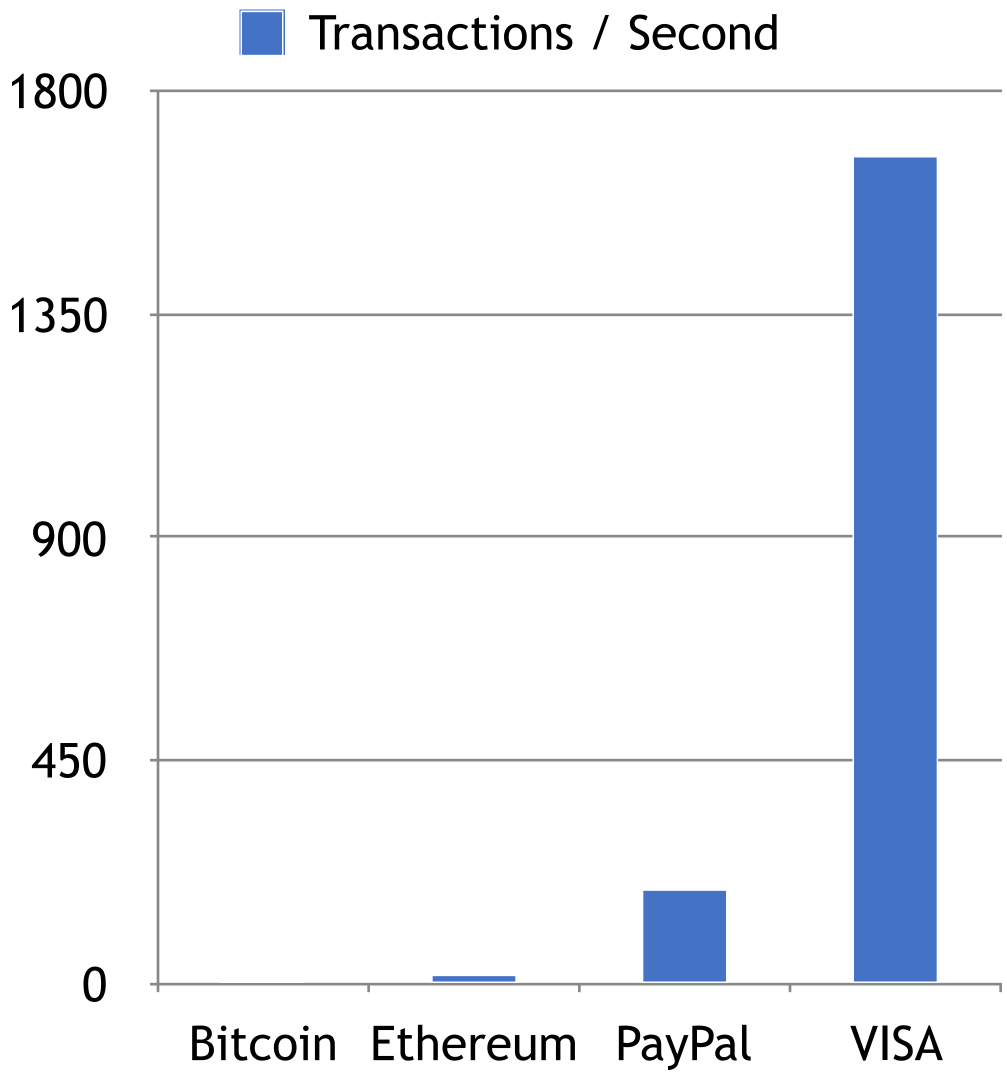
- » Sooooo many things!

- » Based mostly in HTTP

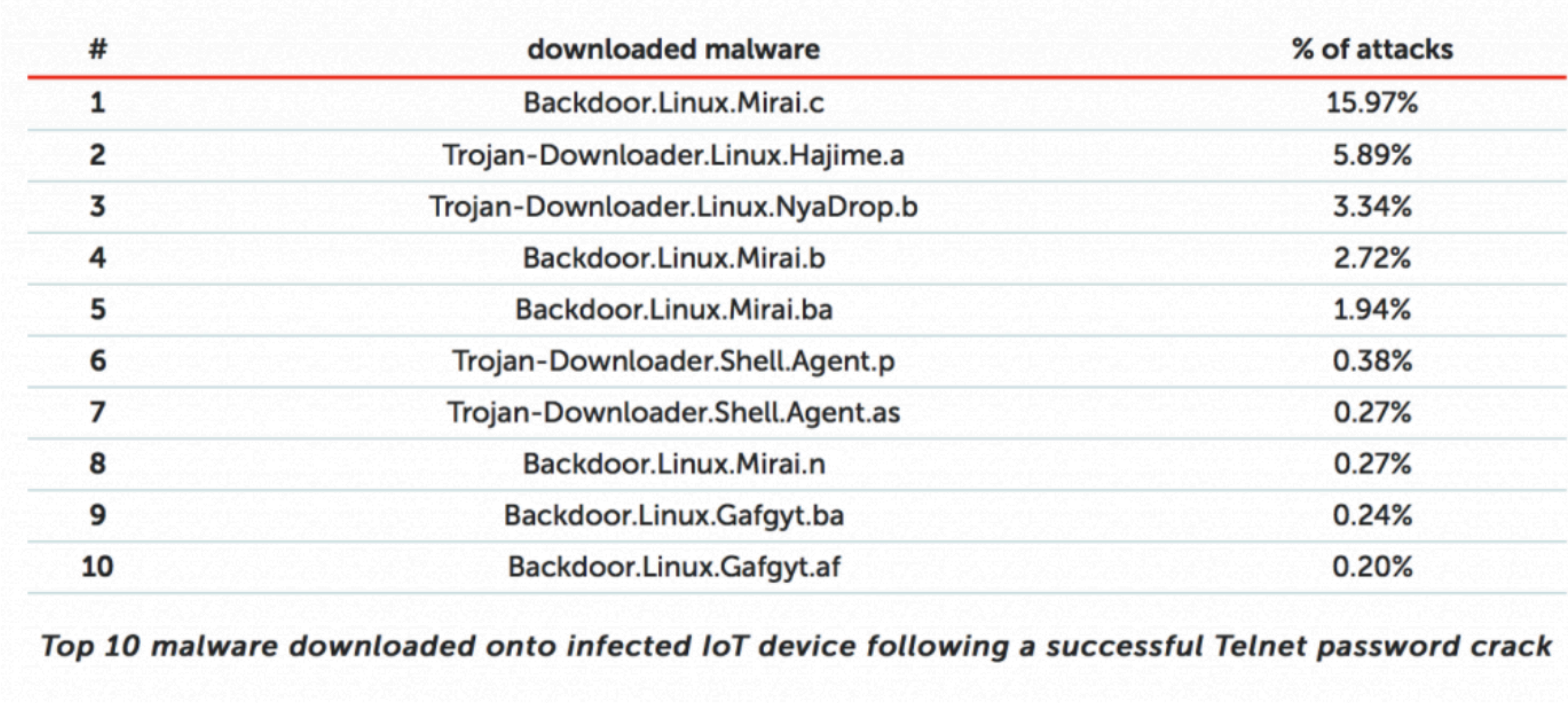


AUTHENTICATION

- » Elliptic Curve Crypto?
- » Blockchain?



PAYLOADS



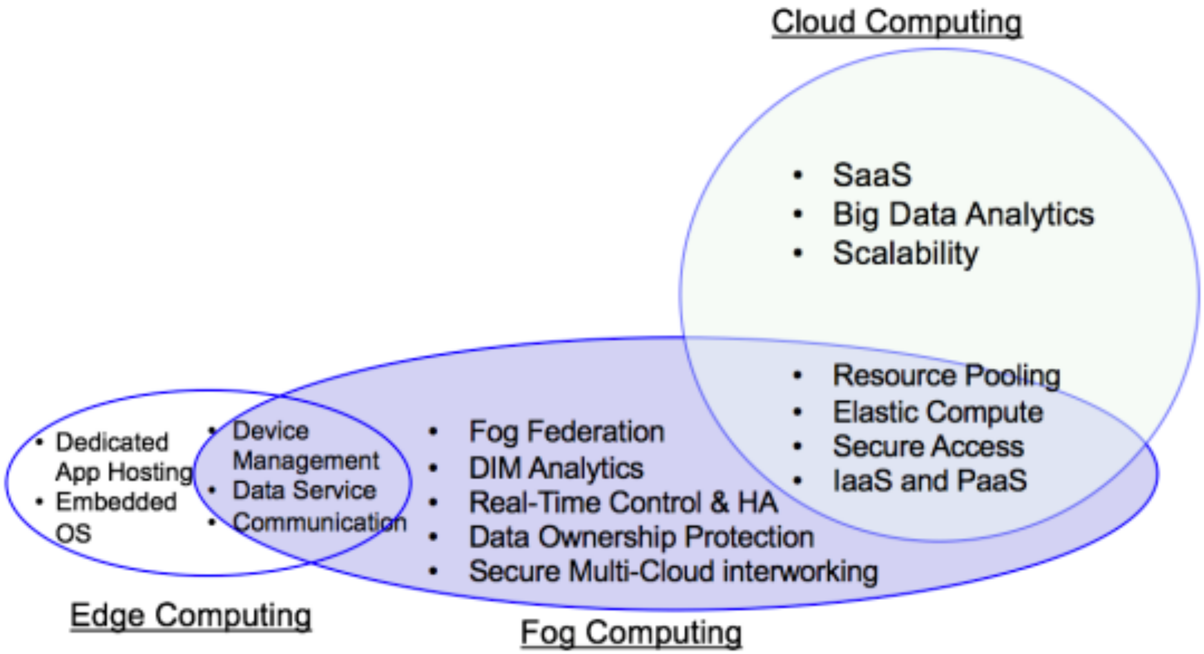
#	downloaded malware	% of attacks
1	Backdoor.Linux.Mirai.c	15.97%
2	Trojan-Downloader.Linux.Hajime.a	5.89%
3	Trojan-Downloader.Linux.NyaDrop.b	3.34%
4	Backdoor.Linux.Mirai.b	2.72%
5	Backdoor.Linux.Mirai.ba	1.94%
6	Trojan-Downloader.Shell.Agent.p	0.38%
7	Trojan-Downloader.Shell.Agent.as	0.27%
8	Backdoor.Linux.Mirai.n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

NETWORKING

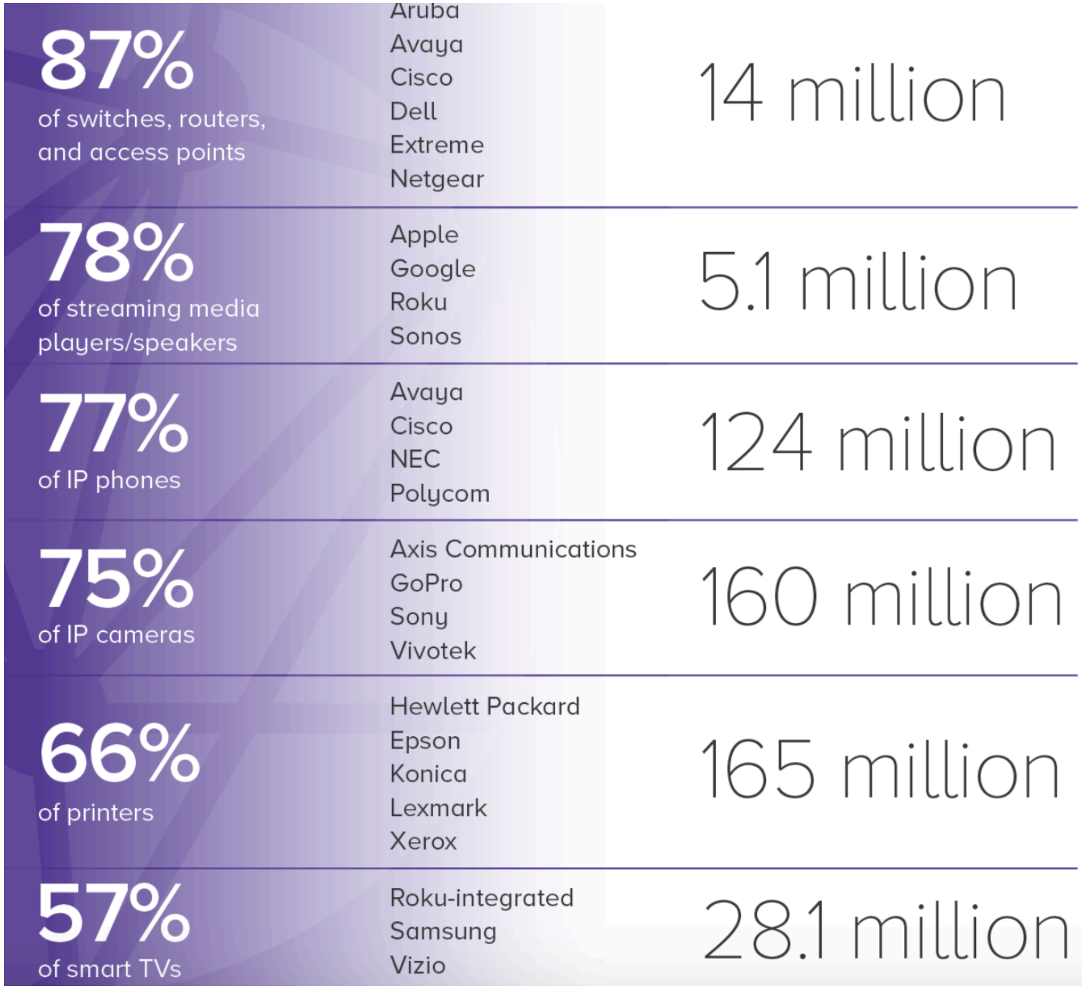
- Which part?
  - User -> Stand Alone Device?
  - User -> Cloud Connected Device?
  - User -> Hub?
  - Device -> Hub?
  - Hub -> Cloud?
  - User -> Cloud?
  - Device -> Device?
  - Device -> Cloud?

DNS REBINDING

- Same Origin Policy
- bad.js
- CVEs? You bet

DNS REBINDING

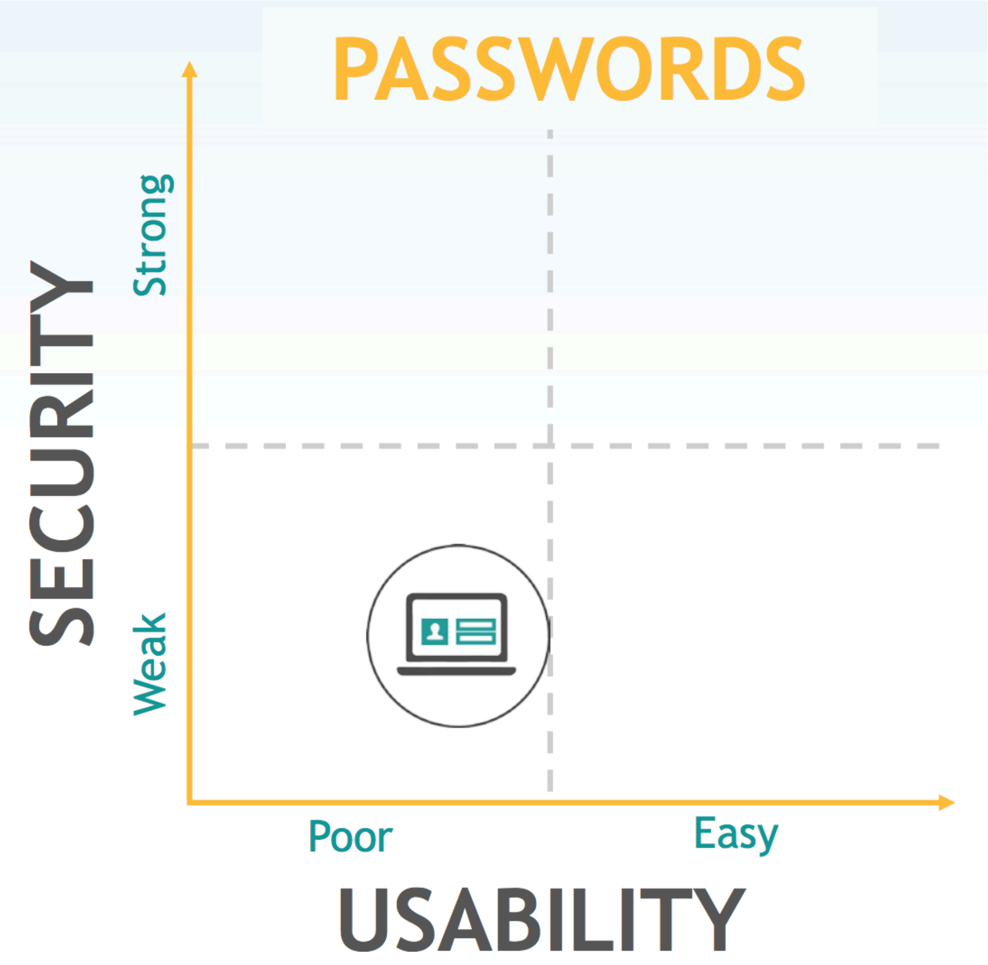
- Vulns Everywhere!



87% of switches, routers, and access points	Aruba Avaya Cisco Dell Extreme Netgear	14 million
78% of streaming media players/speakers	Apple Google Roku Sonos	5.1 million
77% of IP phones	Avaya Cisco NEC Polycom	124 million
75% of IP cameras	Axis Communications GoPro Sony Vivotek	160 million
66% of printers	Hewlett Packard Epson Konica Lexmark Xerox	165 million
57% of smart TVs	Roku-integrated Samsung Vizio	28.1 million

SECURE NETWORKING?

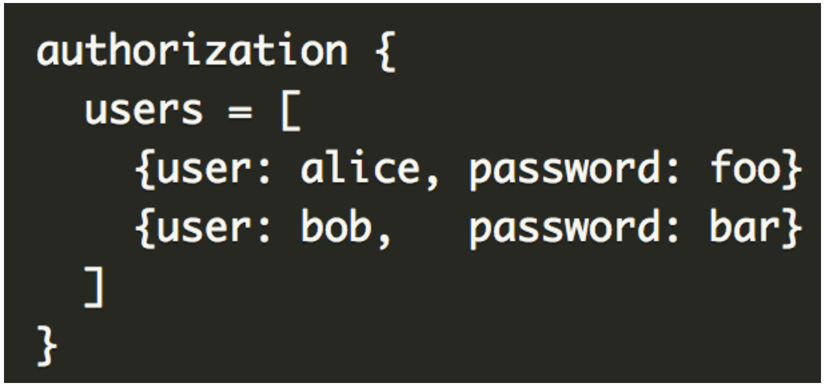
- Heavy Use of HTTPS
- Authentication?
- FIDO Alliance



QUEUES

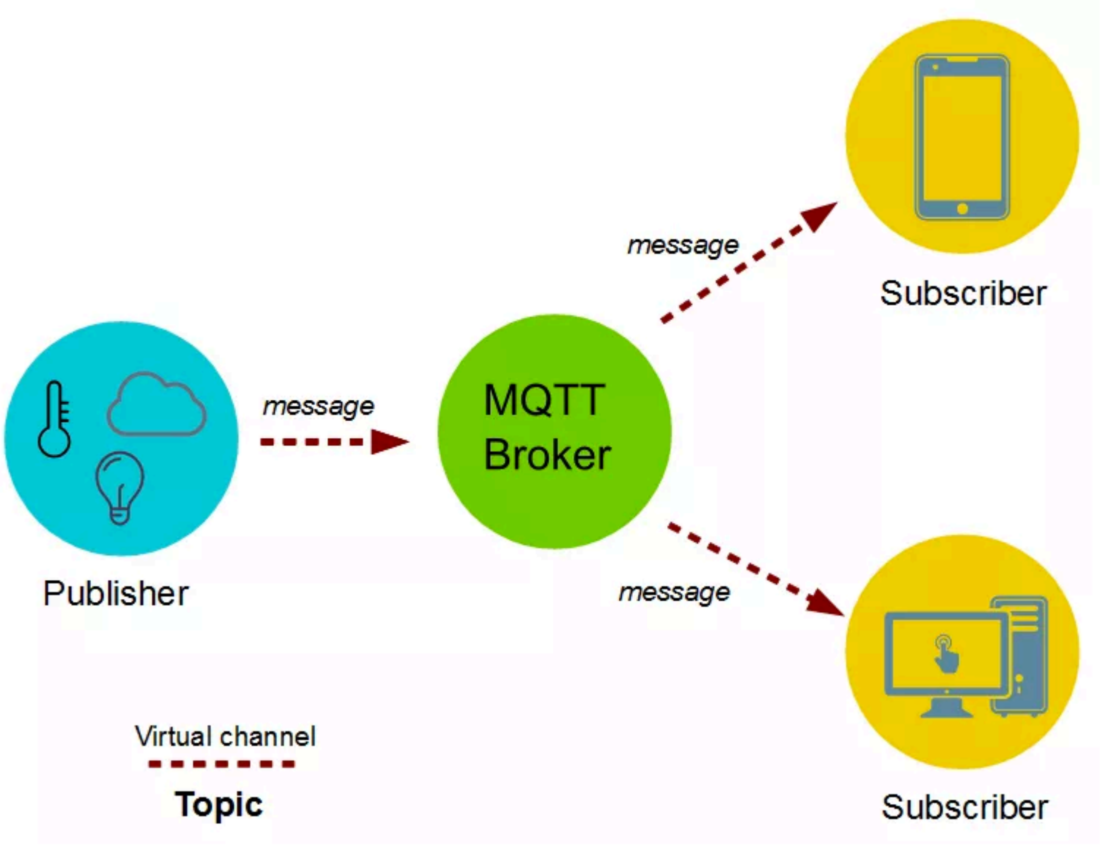
- RabbitMQ
  - Complex setup
  - Basic security

- nats.io
  - Auth
  - TLS



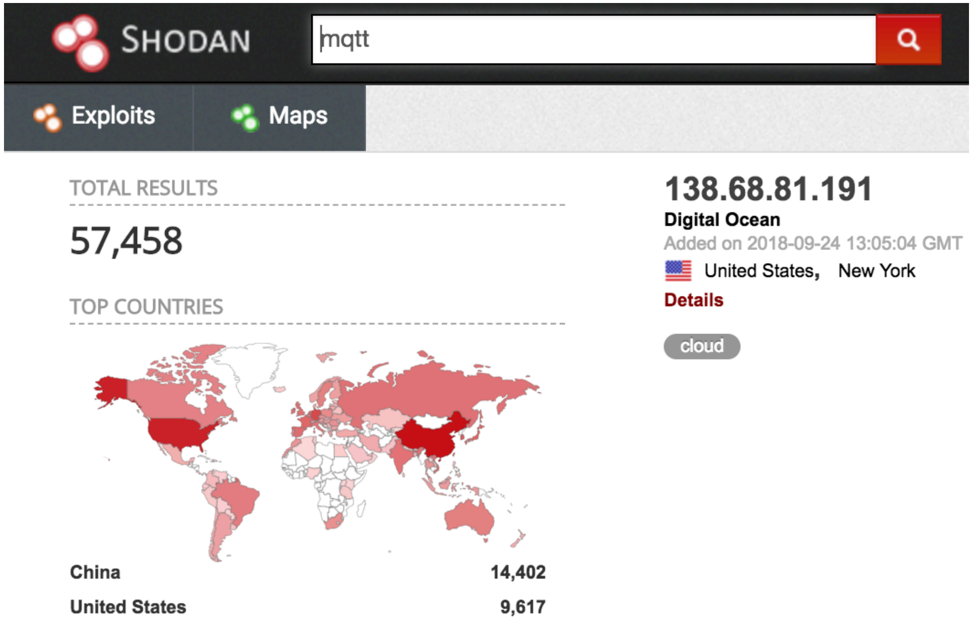
```
authorization {
  users = [
    {user: alice, password: foo}
    {user: bob,   password: bar}
  ]
}
```

MQTT


message
Subscriber
message
MQTT
Broker
Publisher
message
Virtual channel
Topic
Subscriber

MQTT

- Anything interesting on a public broker?
- SHODAN
- C2 through MQTT



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

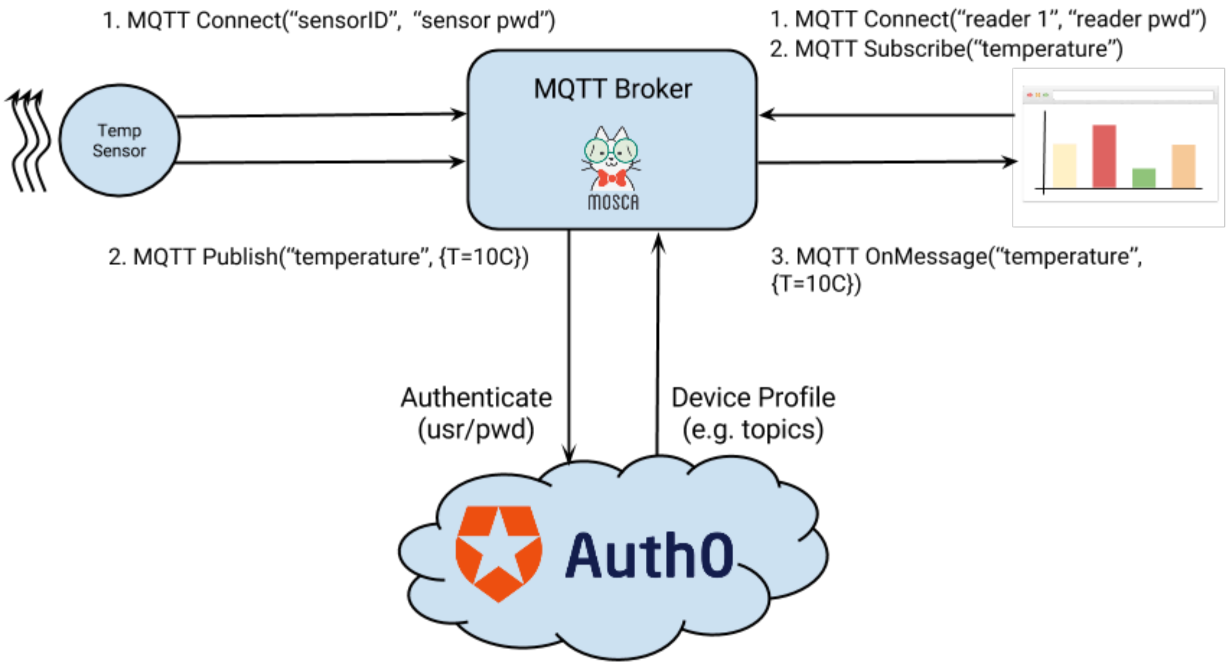
United States, New York

Details

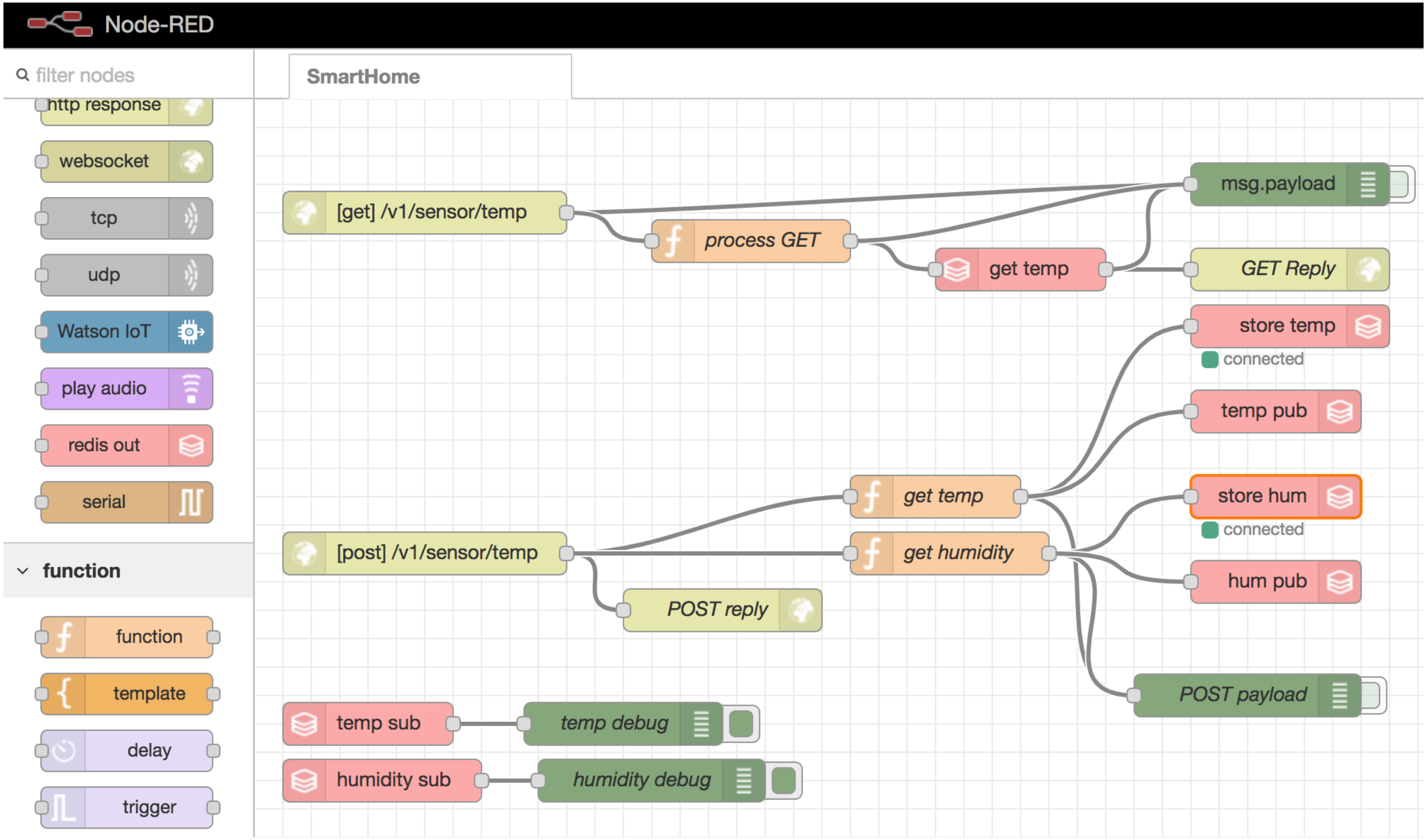
cloud

SECURING MQTT

- Enterprise Solution (HiveMQ)
- 3rd party broker


1. MQTT Connect("sensorID", "sensor pwd")
1. MQTT Connect("reader 1", "reader pwd")
2. MQTT Subscribe("temperature")
Temp Sensor
MQTT Broker
MOSCA
2. MQTT Publish("temperature", {T=10C})
3. MQTT OnMessage("temperature", {T=10C})
Authenticate (usr/pwd)
Device Profile (e.g. topics)
Auth0

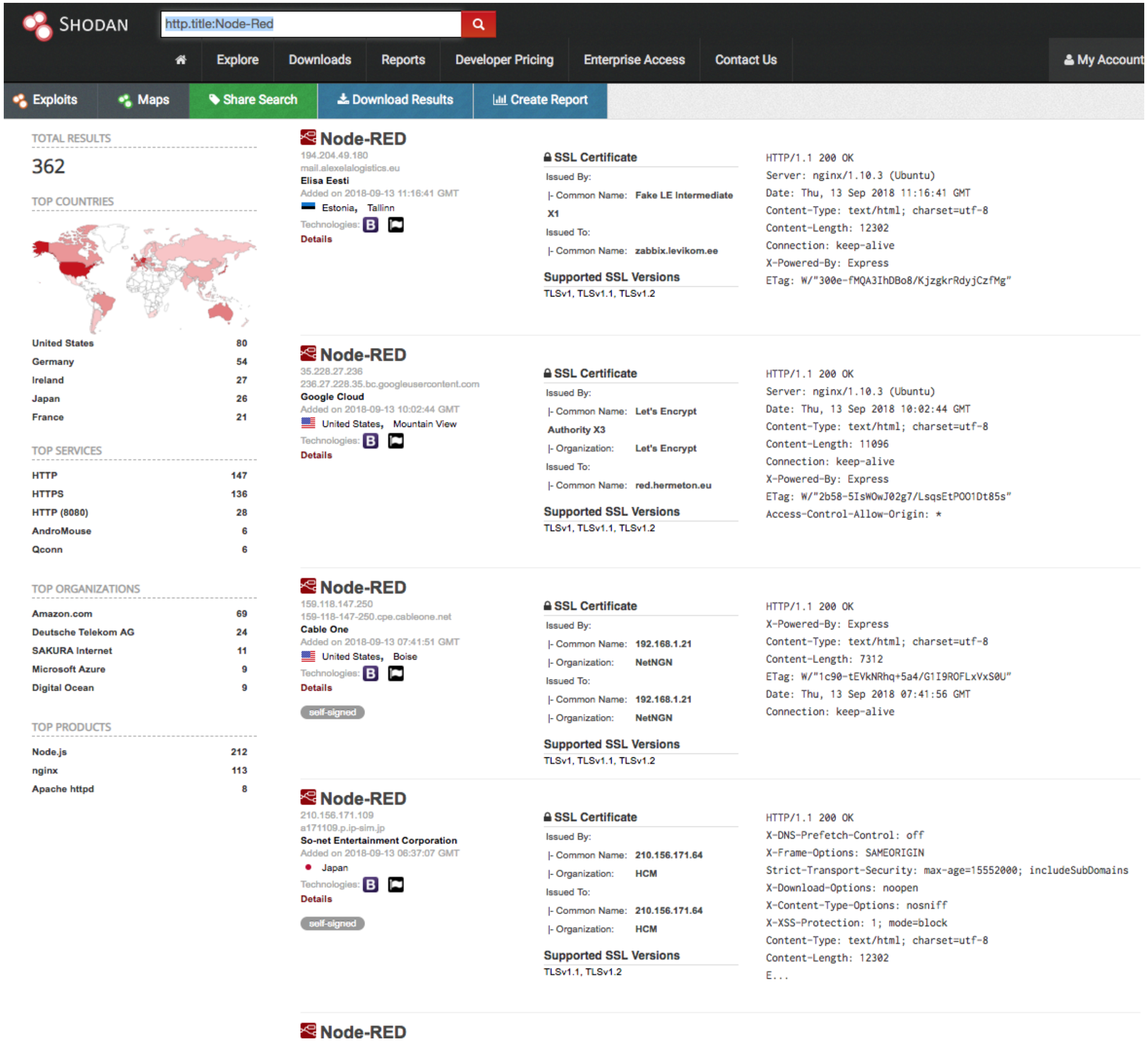
NODERED


Node-RED
filter nodes
SmartHome
http response
websocket
tcp
udp
Watson IoT
play audio
redis out
serial
function
function
template
delay
trigger
[get] /v1/sensor/temp
process GET
get temp
msg.payload
GET Reply
store temp
connected
temp pub
get temp
store hum
connected
[post] /v1/sensor/temp
get humidity
hum pub
POST reply
POST payload
temp sub
temp debug
humidity sub
humidity debug

THE … WHATEVER

NODERED

- Security?
- Anything live?
- API!



SHODAN http.title:Node-Red

Explore | Downloads | Reports | Developer Pricing | Enterprise Access | Contact Us | My Account

Exploits | Maps | Share Search | Download Results | Create Report

TOTAL RESULTS

362

TOP COUNTRIES

United States	80
Germany	54
Ireland	27
Japan	26
France	21

TOP SERVICES

HTTP	147
HTTPS	136
HTTP (8080)	28
AndroMouse	6
Qconn	6

TOP ORGANIZATIONS

Amazon.com	69
Deutsche Telekom AG	24
SAKURA Internet	11
Microsoft Azure	9
Digital Ocean	9

TOP PRODUCTS

Node.js	212
nginx	113
Apache httpd	8

Node-RED

194.204.49.180
mail.alexelalogistics.eu
Elisa Eesti
Added on 2018-09-13 11:16:41 GMT
Estonia, Tallinn
Technologies:
Details

SSL Certificate
Issued By:
|- Common Name: Fake LE Intermediate X1
Issued To:
|- Common Name: zabbix.levikom.ee
Supported SSL Versions
TLSv1, TLSv1.1, TLSv1.2

```
HTTP/1.1 200 OK
Server: nginx/1.10.3 (Ubuntu)
Date: Thu, 13 Sep 2018 11:16:41 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 12302
Connection: keep-alive
X-Powered-By: Express
ETag: W/"300e-fMQA3IhDBo8/KjzgkrRdyjCzfMg"
```

Node-RED

35.228.27.236
236.27.228.35.bc.googleusercontent.com
Google Cloud
Added on 2018-09-13 10:02:44 GMT
United States, Mountain View
Technologies:
Details

SSL Certificate
Issued By:
|- Common Name: Let's Encrypt Authority X3
|- Organization: Let's Encrypt
Issued To:
|- Common Name: red.hermeton.eu
Supported SSL Versions
TLSv1, TLSv1.1, TLSv1.2

```
HTTP/1.1 200 OK
Server: nginx/1.10.3 (Ubuntu)
Date: Thu, 13 Sep 2018 10:02:44 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 11096
Connection: keep-alive
X-Powered-By: Express
ETag: W/"2b58-5IsWOwJ02g7/LsqsEtPOO1Dt85s"
Access-Control-Allow-Origin: *
```

Node-RED

159.118.147.250
159-118-147-250.cpe.cableone.net
Cable One
Added on 2018-09-13 07:41:51 GMT
United States, Boise
Technologies:
Details
self-signed

SSL Certificate
Issued By:
|- Common Name: 192.168.1.21
|- Organization: NetNGN
Issued To:
|- Common Name: 192.168.1.21
|- Organization: NetNGN
Supported SSL Versions
TLSv1, TLSv1.1, TLSv1.2

```
HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: text/html; charset=utf-8
Content-Length: 7312
ETag: W/"1c90-tEVkNRhq+5a4/G1I9ROFLxVxS0U"
Date: Thu, 13 Sep 2018 07:41:56 GMT
Connection: keep-alive
```

Node-RED

210.156.171.109
a171109.p.ip-sim.jp
So-net Entertainment Corporation
Added on 2018-09-13 06:37:07 GMT
Japan
Technologies:
Details
self-signed

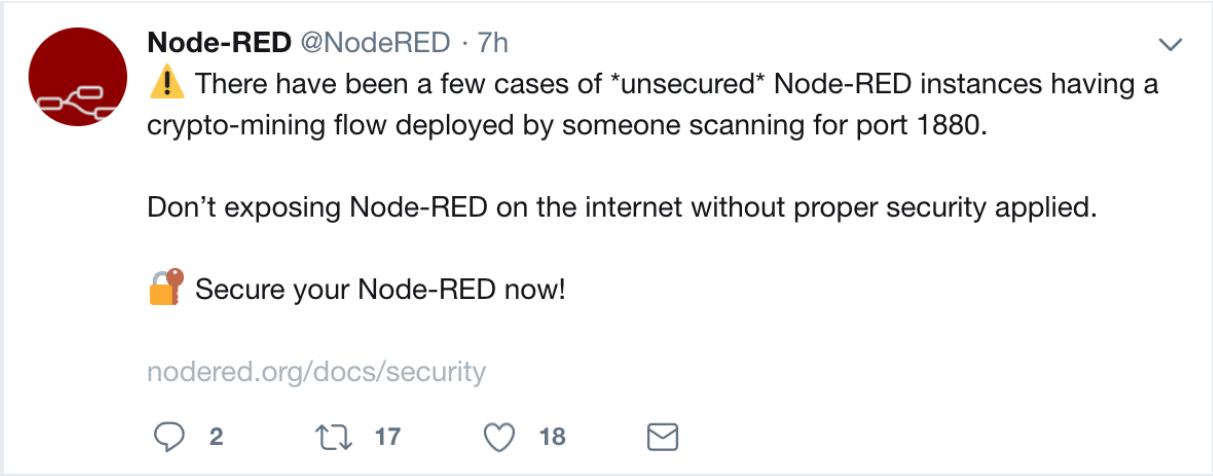
SSL Certificate
Issued By:
|- Common Name: 210.156.171.64
|- Organization: HCM
Issued To:
|- Common Name: 210.156.171.64
|- Organization: HCM
Supported SSL Versions
TLSv1.1, TLSv1.2

```
HTTP/1.1 200 OK
X-DNS-Prefetch-Control: off
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=15552000; includeSubDomains
X-Download-Options: noopen
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Content-Type: text/html; charset=utf-8
Content-Length: 12302
E...
```

Node-RED

SECURING NODERED

- Authentication
- Secure Comms



Node-RED @NodeRED · 7h

⚠️ There have been a few cases of *unsecured* Node-RED instances having a crypto-mining flow deployed by someone scanning for port 1880.

Don’t exposing Node-RED on the internet without proper security applied.

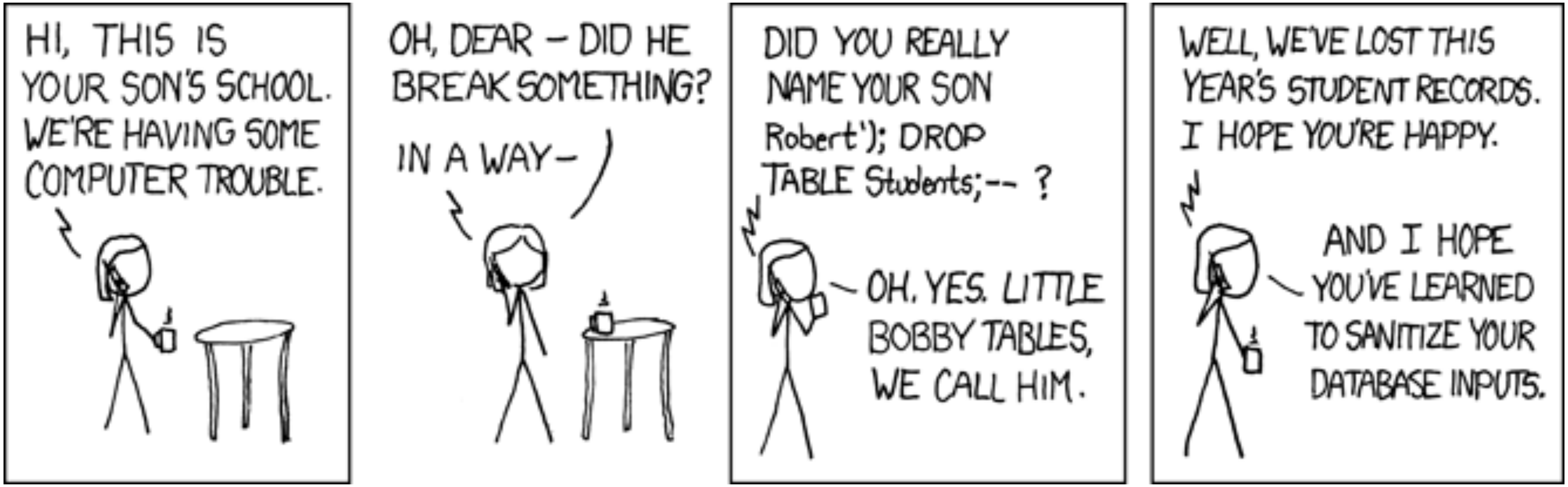
🔐 Secure your Node-RED now!

nodered.org/docs/security

WEB INTERFACES

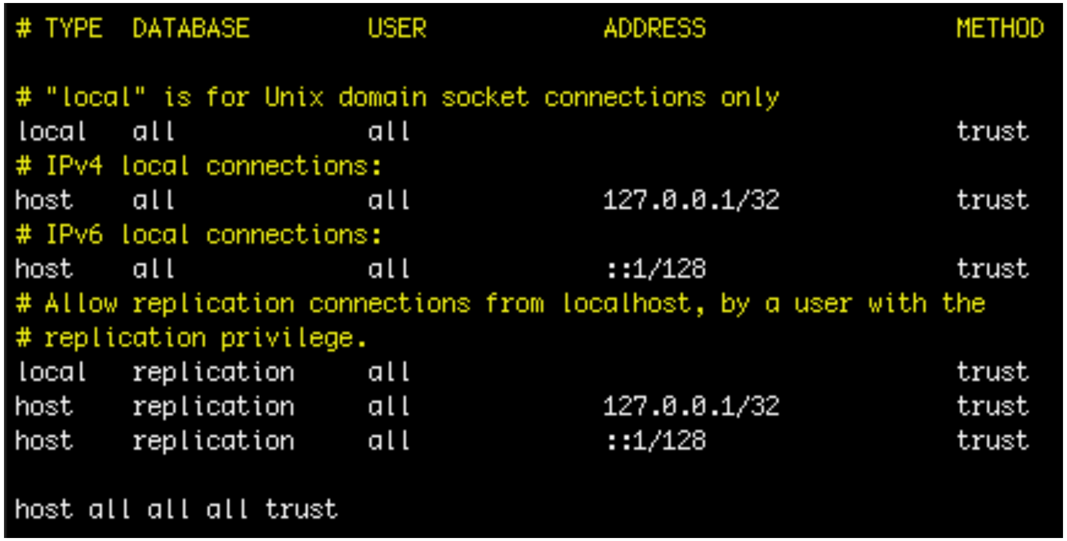
» Basic Vulnerabilities

» Custom HTTP servers … but why?


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

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 all trust
```

pg_hba.conf

INDICES

- ElasticSearch ✓

05 | SECURING THE DATA

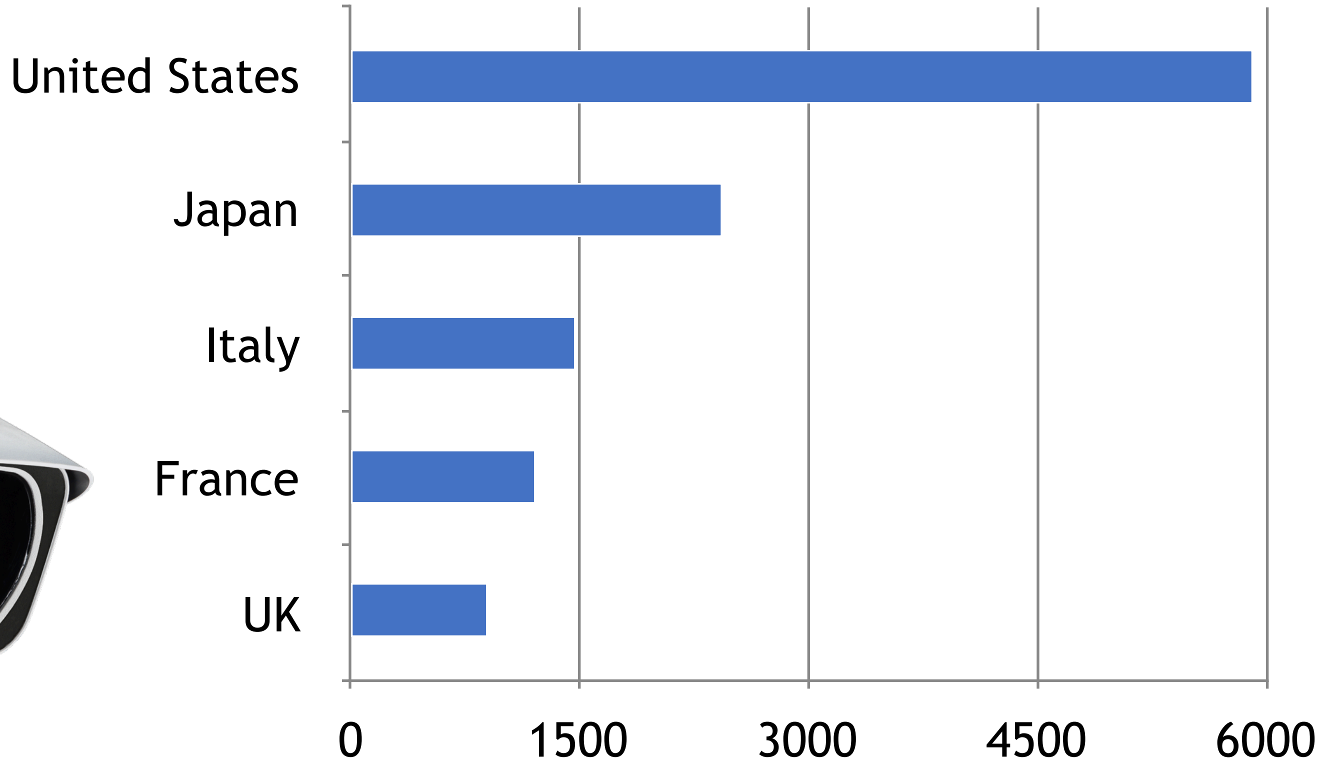
SECURING THE DATA

- Make No Mistake … I mean PRIVACY

- Is perimeter security dead?

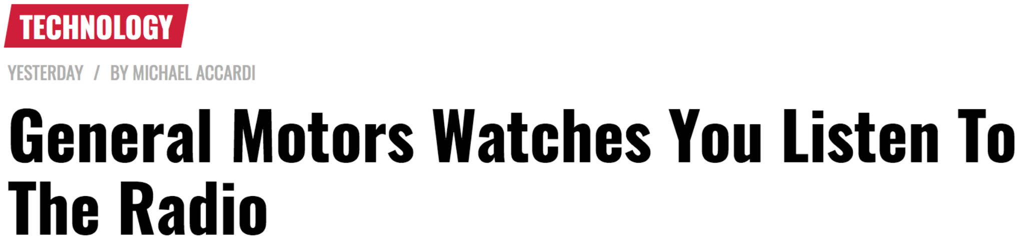
SECURING THE DATA

- Cameras



SECURING THE DATA

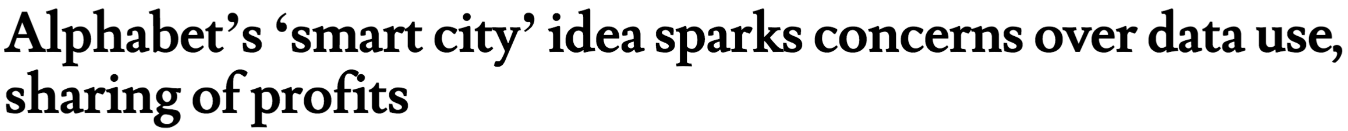
- Cars and Cities?



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

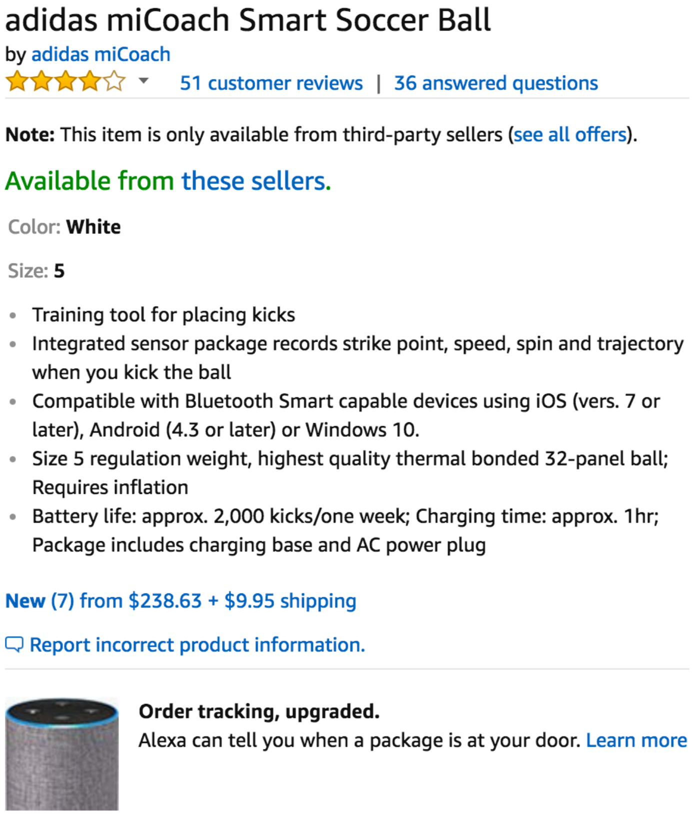
- Wearable Medical Devices

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

We're still working on getting you more information about the Smart Ball on adidas.com so come back soon. In the meantime, here's the product article number G83963 for your reference, it's categorized as: Training and Soccer Balls

SECURING THE DATA

» ?



adidas miCoach Smart Soccer Ball

by adidas miCoach

★★★★☆ 51 customer reviews | 36 answered questions

Note: This item is only available from third-party sellers (see all offers).

Available from these sellers.

Color: **White**

Size: **5**

- Training tool for placing kicks
- Integrated sensor package records strike point, speed, spin and trajectory when you kick the ball
- Compatible with Bluetooth Smart capable devices using iOS (vers. 7 or later), Android (4.3 or later) or Windows 10.
- Size 5 regulation weight, highest quality thermal bonded 32-panel ball; Requires inflation
- Battery life: approx. 2,000 kicks/one week; Charging time: approx. 1hr; Package includes charging base and AC power plug

New (7) from $238.63 + $9.95 shipping

Report incorrect product information.

Order tracking, upgraded.
Alexa can tell you when a package is at your door. Learn more

QUESTIONS?

THANK YOU.