



IOActive Inc Presents  
Licensed by Sunshine  
Cracked by:  
Mad Brad.



Taking over the world through MQTT - Aftermath

LAS VEGAS NEVADA  
MANDALA BAY 25TH OF JULY 2017

Last year at Defcon 24 Acidgen presented **Light Weight Protocol! Serious Equipment!**  
The findings where highly severe, however the initial response was weak.  
Acidgen Pushed on, And got the worlds attention on the MQTT protocol...

WHO AM I?



For those who didn't read the bio:

Work for IOActive

Been breaking things since age 16

Was part of Corelan (Hi PVE!)

Pentests, Fuzzing, Exploit Dev, Webapps and IoT

Twitter: [@acidgen](#)



WHO HEARD BOUT 'DIS BEFORE?



Who in here has heard bout MQTT before?  
Who in here uses MQTT?



I WILL SHOW YOU...



The easiest "Hack" on BlackHat this year  
How people can do severe damage  
What things I found  
And how to use this protocol securely

STORY TIME...



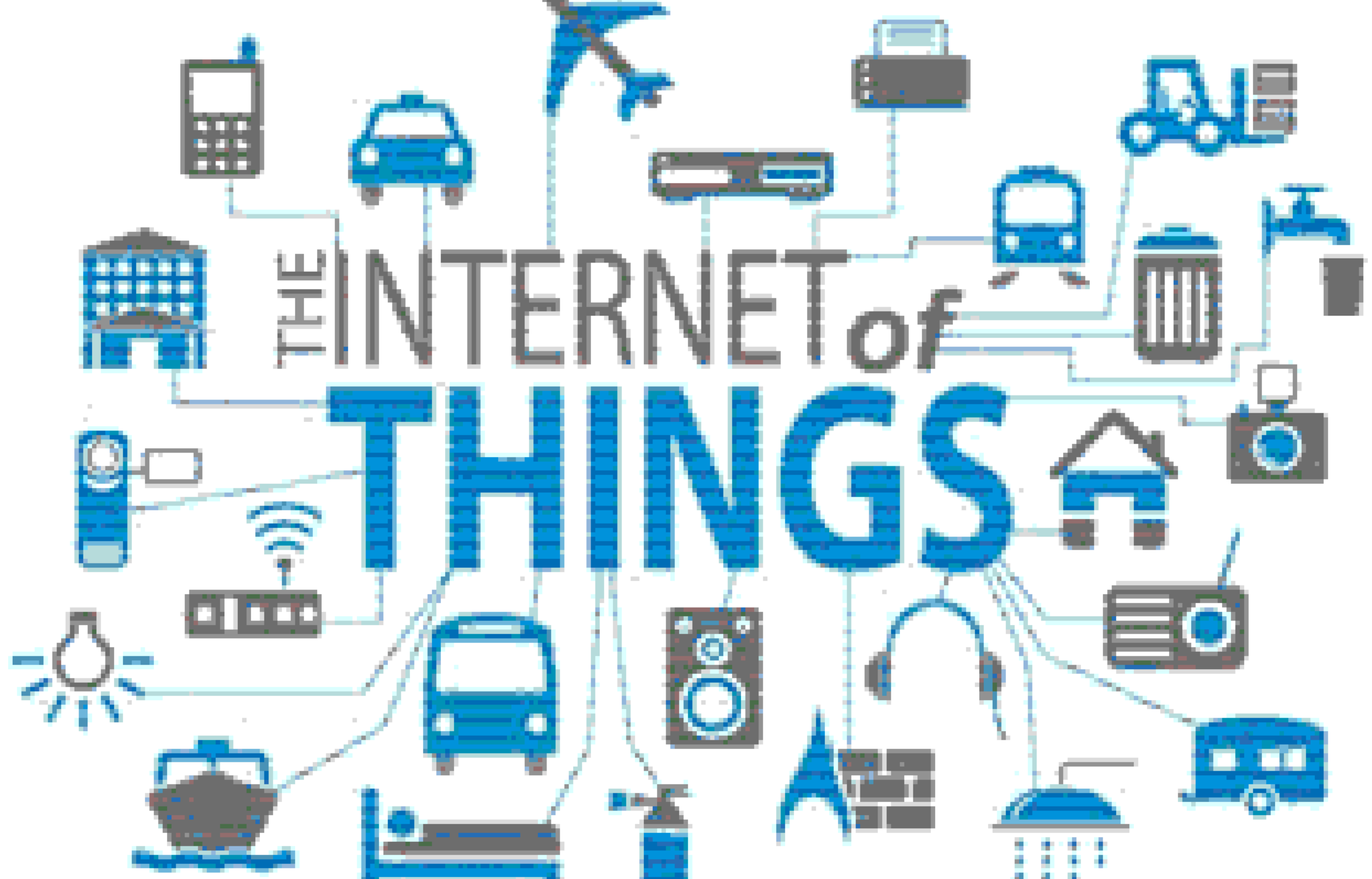
Meanwhile...



All your base are belong to us....

```
sensor/radiation/cpm: 33  
sensor/radiation/uSv: 0.18
```

<http://bit.ly/1NJ6CtA>



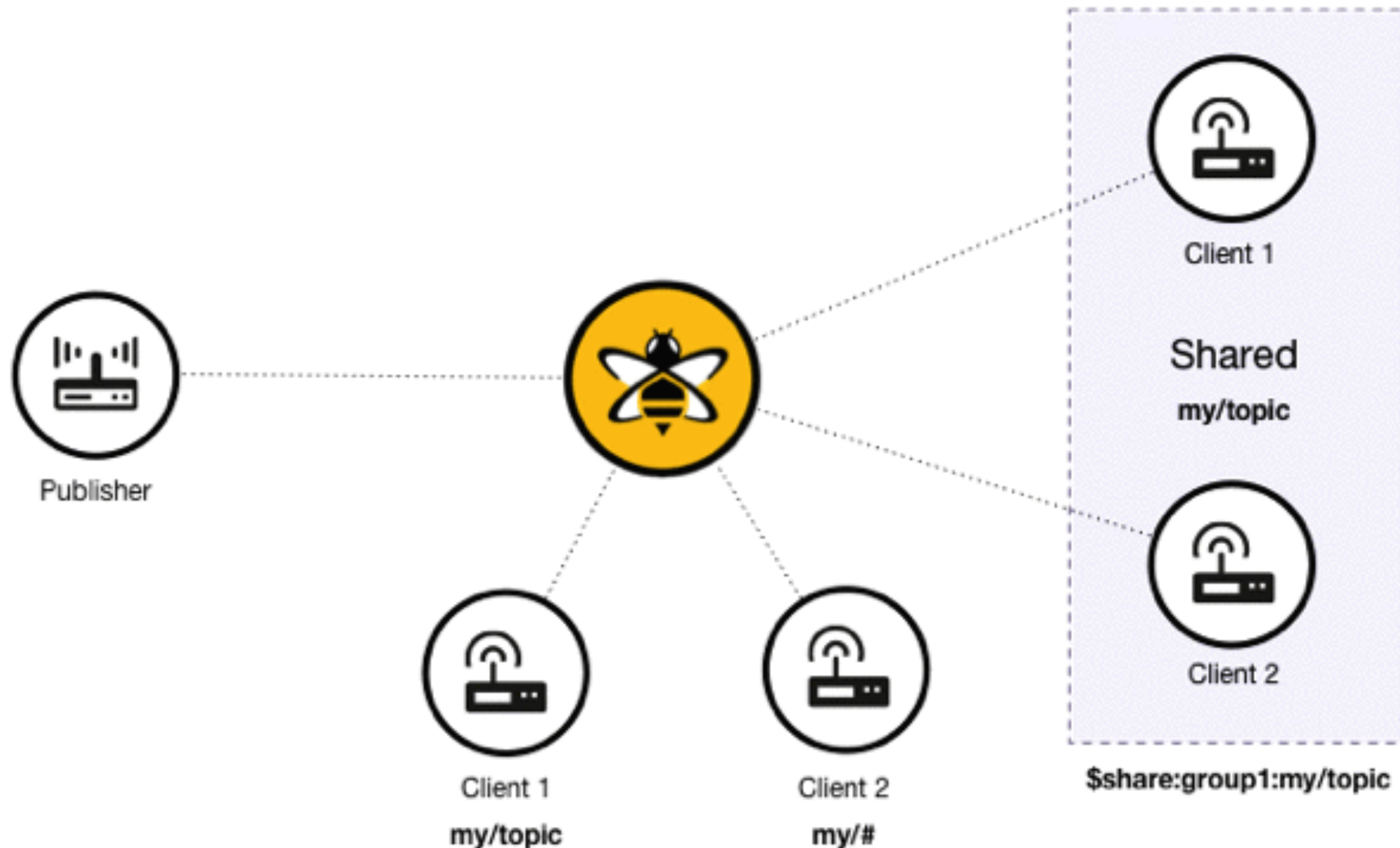




Invented 1999-2000  
Andy Stanford Clarke + Arlene Nipper = MQTT  
Was IBM, Given to OASIS 2013 - OPEN SOURCE  
Port 1883 and 8883 (Secure-MQTT)

Fast  
Bandwidth Efficient  
QoS  
Able to deliver messages for offline clients  
M2M Coms

# HOW DOES IT WORK?





TOPICS?

Topics are like small channels  
These channels can work as identifiers

Sensor in Attic might send to:

myhome/Attic/temp

You phone listens to:

myhome/Attic/temp

And gives you the last known temp reading

CAN YOU DEMO THE BASICS?



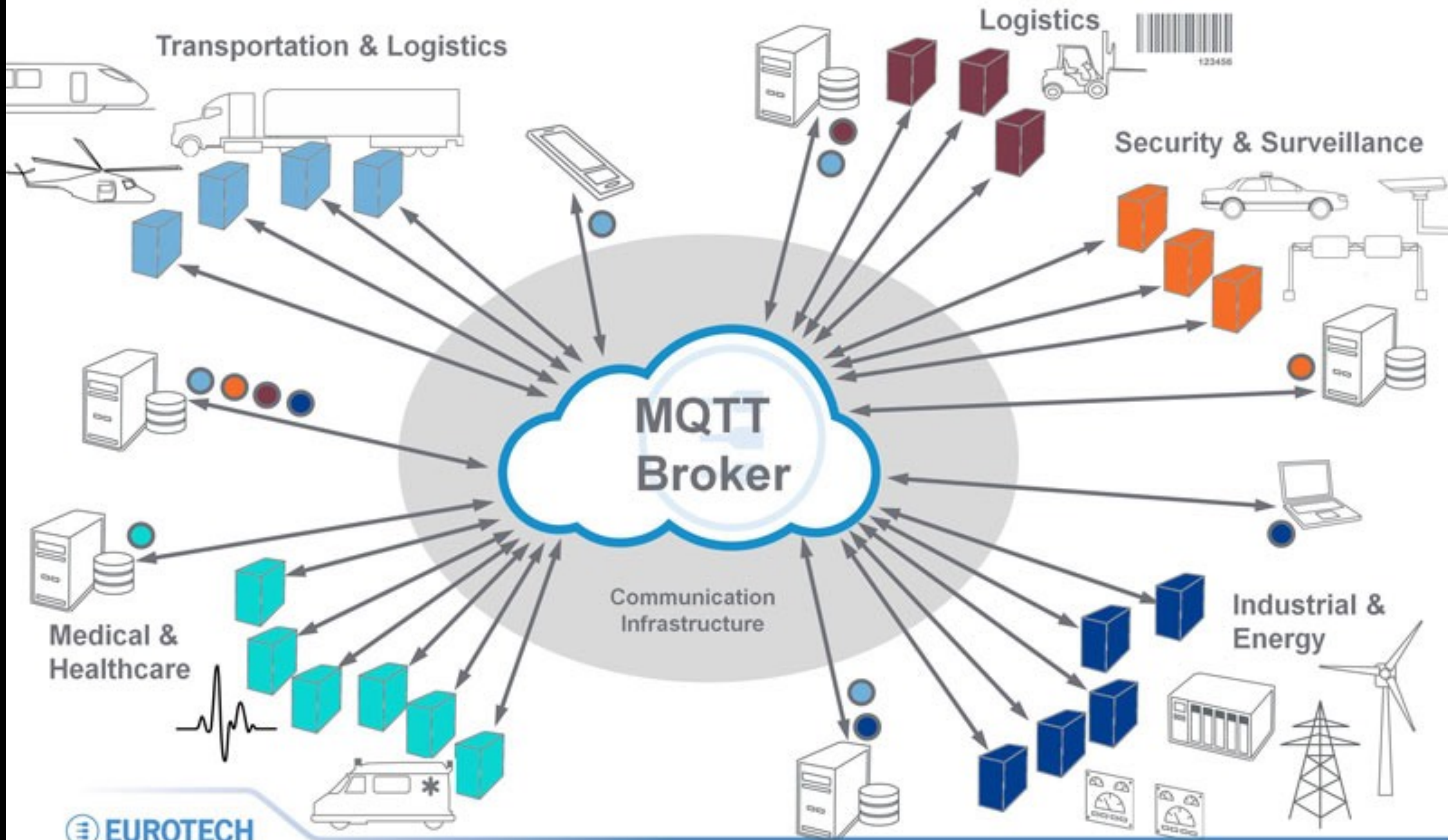
sheepfilms.co.uk

WHO USES IT?



# The Internet of Things

## Decoupling Producers & Consumers of M2M Device Data





From the manual:

- 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

MQTT solutions are often deployed in hostile communication environments



## Protection:

- Authentication of users and devices
- Authorization of access to Server resources
- Integrity of MQTT Control Packets and application data contained therein
- Privacy of MQTT Control Packets and application data contained therein



Protection is rarely used...  
What did Shodan say way back?  
Around 17.000 Brokers with data:

|      |
|------|
| 1883 |
| tcp  |
| mqtt |

MQTT Connection Code: 0

Topics:

ActiveMQ/Advisory/MasterBroker

ActiveMQ/Advisory/Consumer/Topic/#





Scanning the entire internet. There is an increase..

Defcon24: Around 59.000

Blackhat 2017: Around 87.000

Then again; Robust increase, or more temporary devices available at that exact moment



Using Masscan, subscribing to the #  
Listening for 10 seconds....

FINDINGS ARE REDACTED FROM ONLINE VIEW  
AROUND 6 - 8 SLIDES REMOVED



Due to the sensitive nature of the findings  
they have been redacted from online view

ATTACKING WEB APPLICATIONS...



What happens if you take data from MQTT,  
And just place that on a Webpage?

ATTACKING WEB APPLICATIONS...



THIS EXAMPLE HAS BEEN REDACTED FROM ONLINE  
VIEW, WILL ONLY BE SHOWN LIVE

MANIPULATING SQL STATEMENTS...



THIS EXAMPLE HAS BEEN REDACTED FROM ONLINE  
VIEW, WILL ONLY BE SHOWN LIVE

PARTI...PART..OH SH\*T...



PARTICLE ACCELERATOR LIVE DEMO

USERNAME AND PASSWORD?



Joffrey alex@0xdeadcode.se  
The MQTT Bruteforcer  
DEMO



MEDICAL DEVICES, TRAINS, YOU NAME IT...



REDACTED 4 SLIDES

A pixel art character with a green cap, blue jacket, and brown pants is shown in a walking pose. A white speech bubble with a black border points to the character, containing the text "REMEDY?".

REMEDY?

What can you possibly do?

- 1) Are you sure you want to expose this?
- 2) Are you sure you want to expose this?
- 3) Are you su.....
- 4) Encryption
- 5) Username / Password
- 6) Unique Device ID
- 7) Pinned Certificates

A pixel art character with a green cap, blue jacket, and brown pants is shown in a walking pose. A white speech bubble with a black border is positioned above the character's head, containing the text 'REMEDY?'.

REMEDY?

Reversing Hardware  
Stealing Certificate  
Stealing Username / Password  
Connecting to the Broker  
Subscribing to #



CLOUD?

There are people / Services forcing you to do it  
right.

Amazon, IBM Watson  
I want to FORCE U/P/E

Did a small test on a Device hooked to the Amazon  
Cloud. It threw me out head first.

IOT IN GENERAL, DONT...



This is for IoT in General  
Don't just set it up  
Don't just follow the N N N F  
Think about WHAT you are doing  
Or...

# Internet of Things Teddy Bear Leaked 2 Million Parent and Kids Message Recordings



**THANK YOU**

Twitter: @acidgen