black hat® EUROPE 2019

DECEMBER 2-5, 2019
EXCEL LONDON, UK

Sneak into Your Room: Security Holes in the Integration and Management of Messaging Protocols on Commercial IoT Clouds

Sneak into Your Room: Security Holes in the Integration and Management of Messaging Protocols on Commercial IoT Clouds

Yan Jia, Luyi Xing, Yuhang Mao, Dongfang Zhao,
XiaoFeng Wang, Shangru Zhao, and Yuqing Zhang

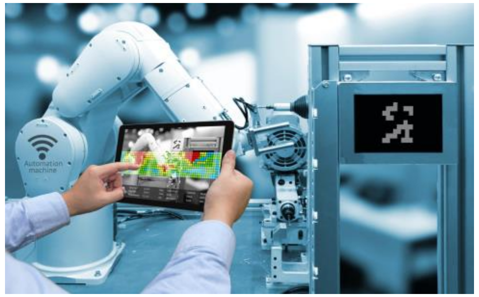
School of Cyber Engineering, Xidian University, China
National Computer Network Intrusion Protection Center, University of Chinese Academy of Sciences ,China
Indiana University Bloomington, USA

西安电子科技大学 XIDIAN UNIVERSITY
中国科学院大学 University of Chinese Academy of Sciences
INDIANA UNIVERSITY BLOOMINGTON

amazon

19 °C
AUTO
ECO
3°C

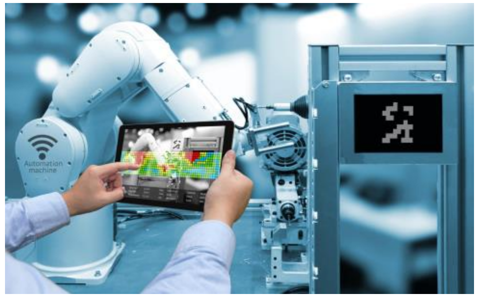
Victoria 73

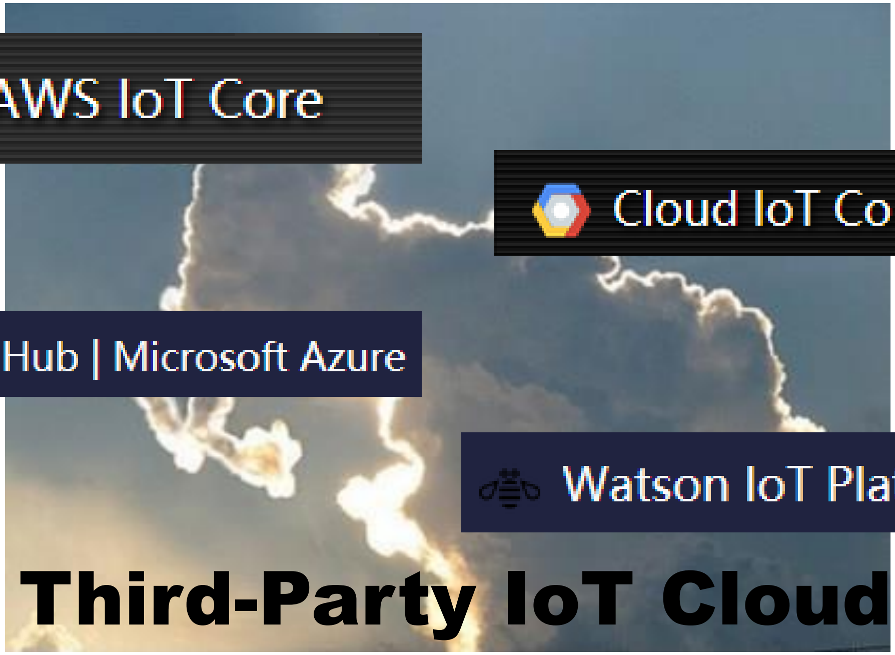

Automation machine

CLEAN
iRobot
Roomba

PHILIPS

IoT Cloud





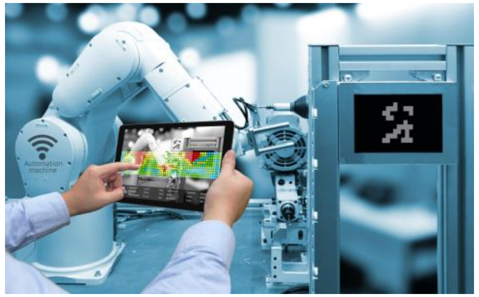
AWS IoT Core

Cloud IoT Core | Google

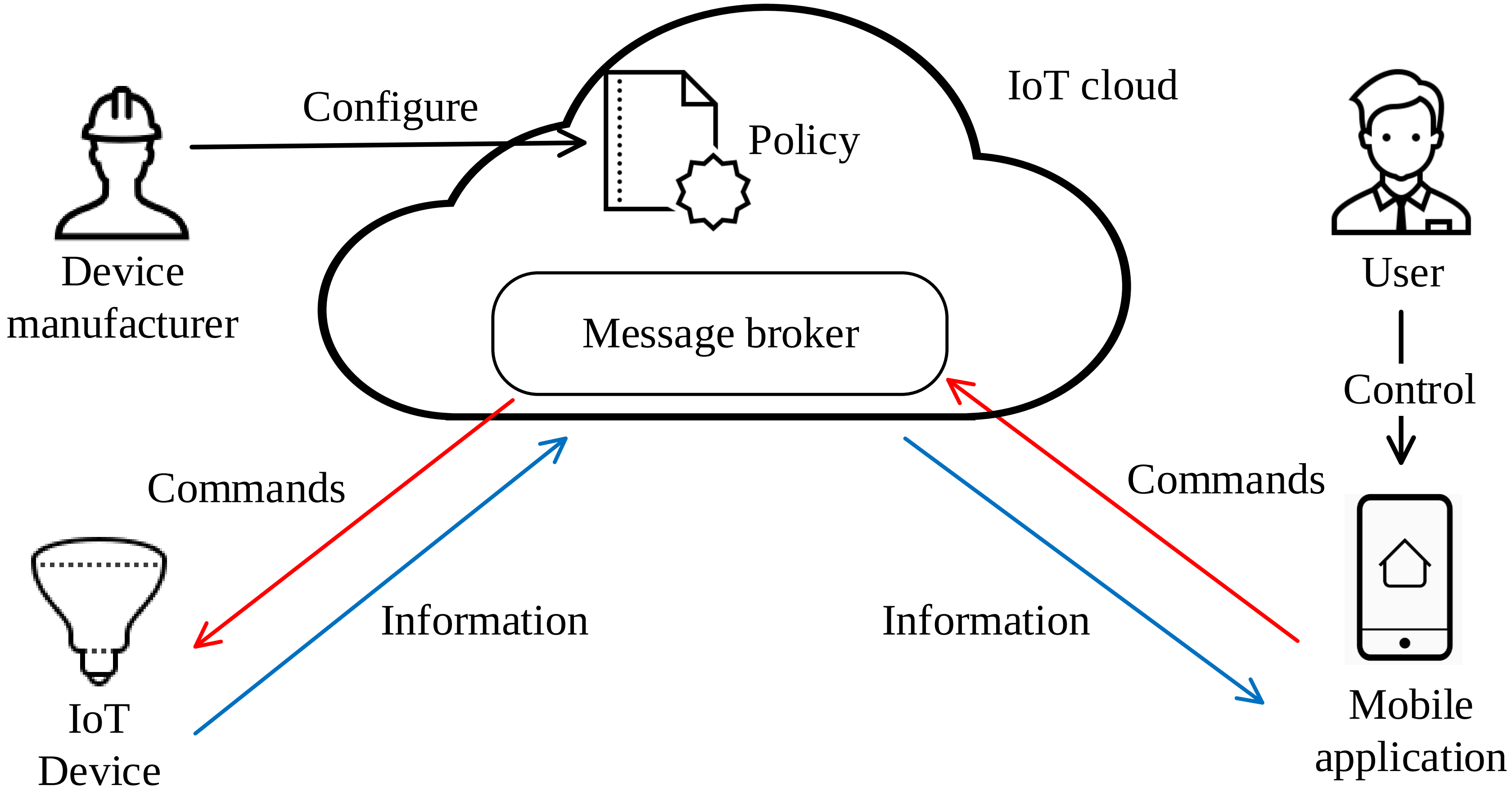
IoT Hub | Microsoft Azure

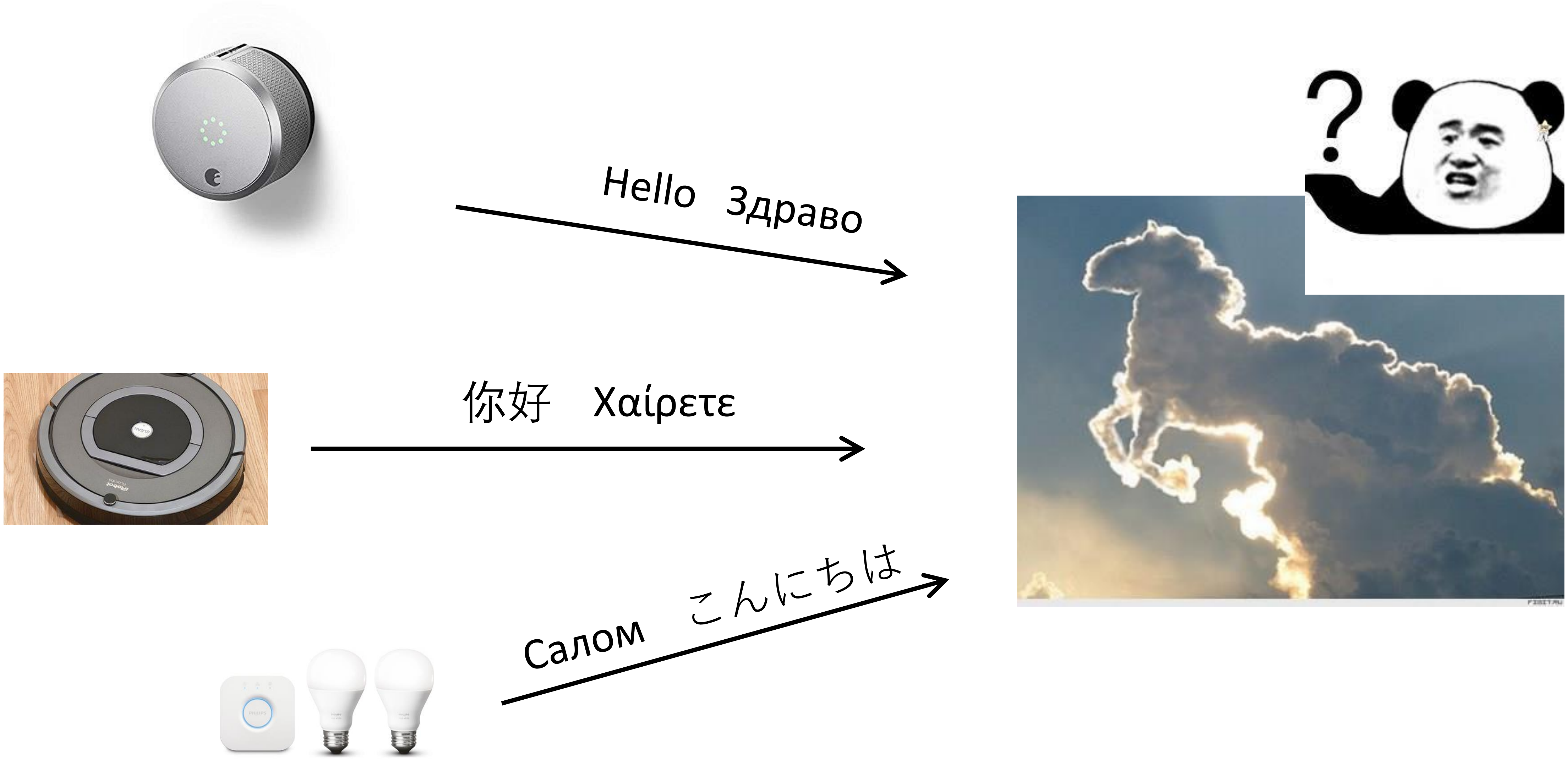
Watson IoT Platform | IBM

Third-Party IoT Cloud



Architecture of Cloud-based IoT Communication

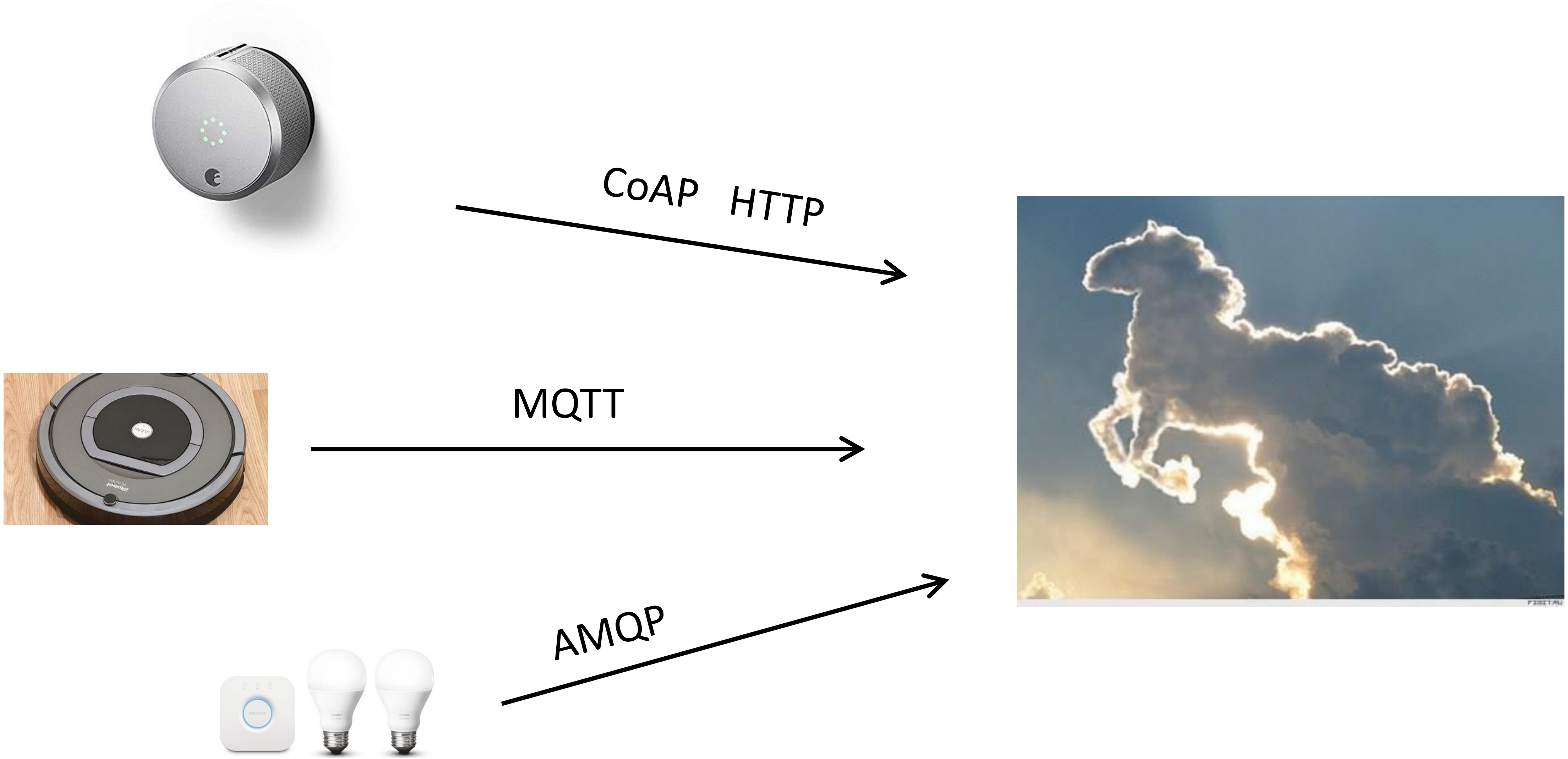




Hello Здраво

你好 Χαίρετε

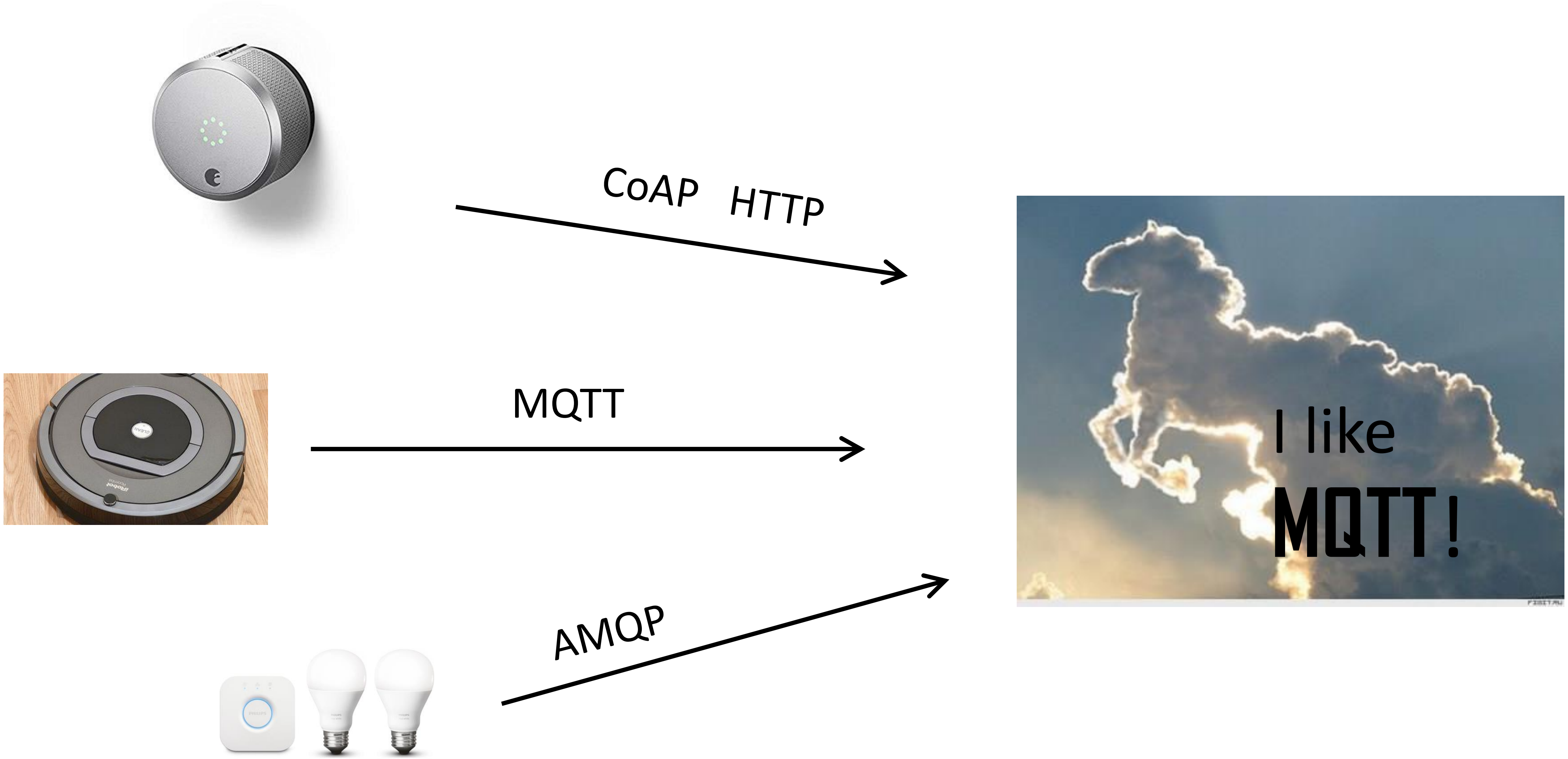
Салом こんにちは



CoAP HTTP

MQTT

AMQP



CoAP HTTP

MQTT

AMQP

I like MQTT!

- MQTT is deployed by

Alibaba Cloud
Worldwide Cloud Services Partner

tuya.com

IoT Hub | Microsoft Azure

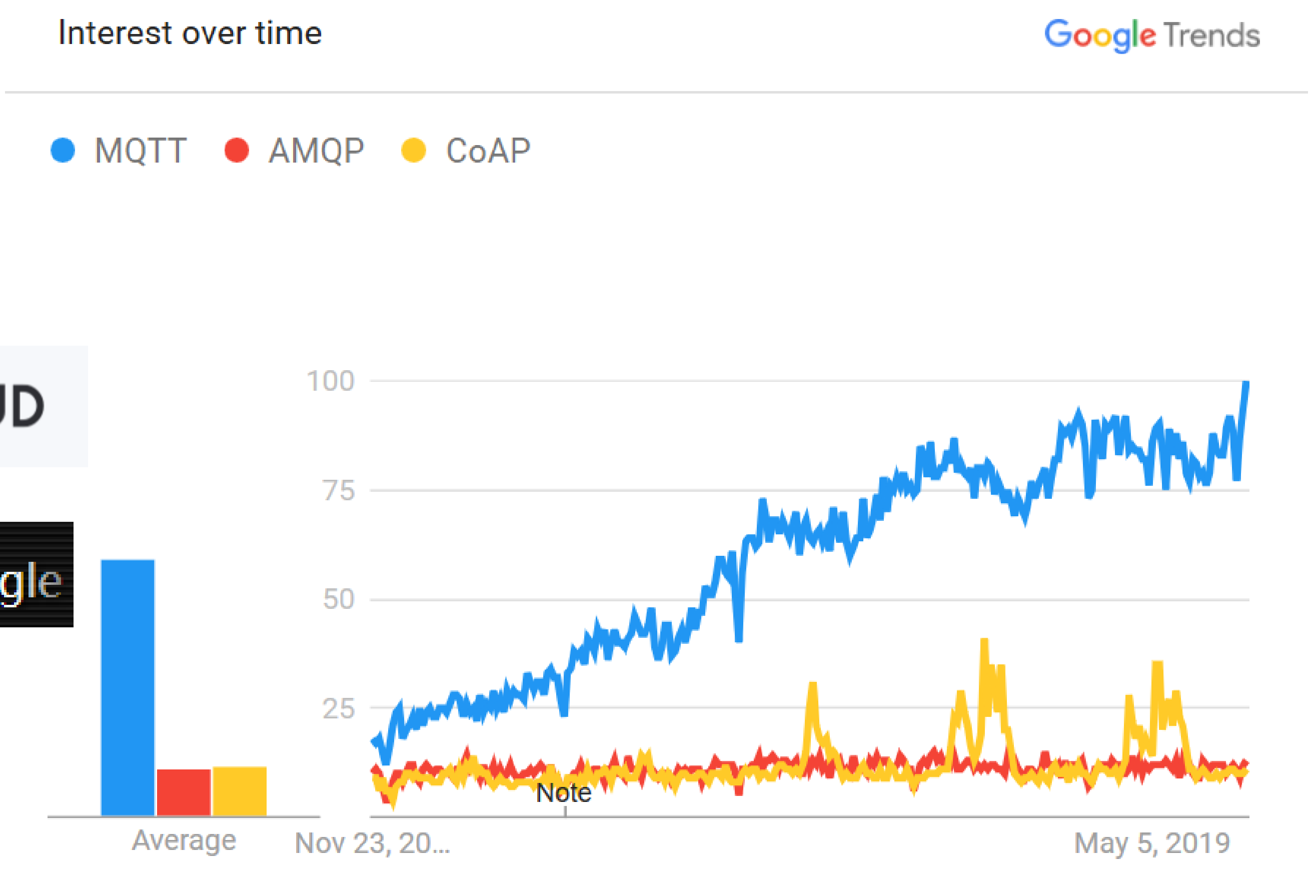
BAIDU AI CLOUD

AWS IoT Core

Cloud IoT Core | Google

SUNING 苏宁易购

Watson IoT Platform | IBM



Worldwide. Past 5 years. Web Search.

What is MQTT

- Message Queuing Telemetry Transport (MQTT)
- M2M/IoT connectivity protocol
- Publish/subscribe messaging transport
- OASIS/IOS Standard
- TCP/IP port 1883, port 8883 (over SSL)

WIKIPEDIA

It was created in 1999 and used to monitor an oil pipeline through the desert.

OASIS

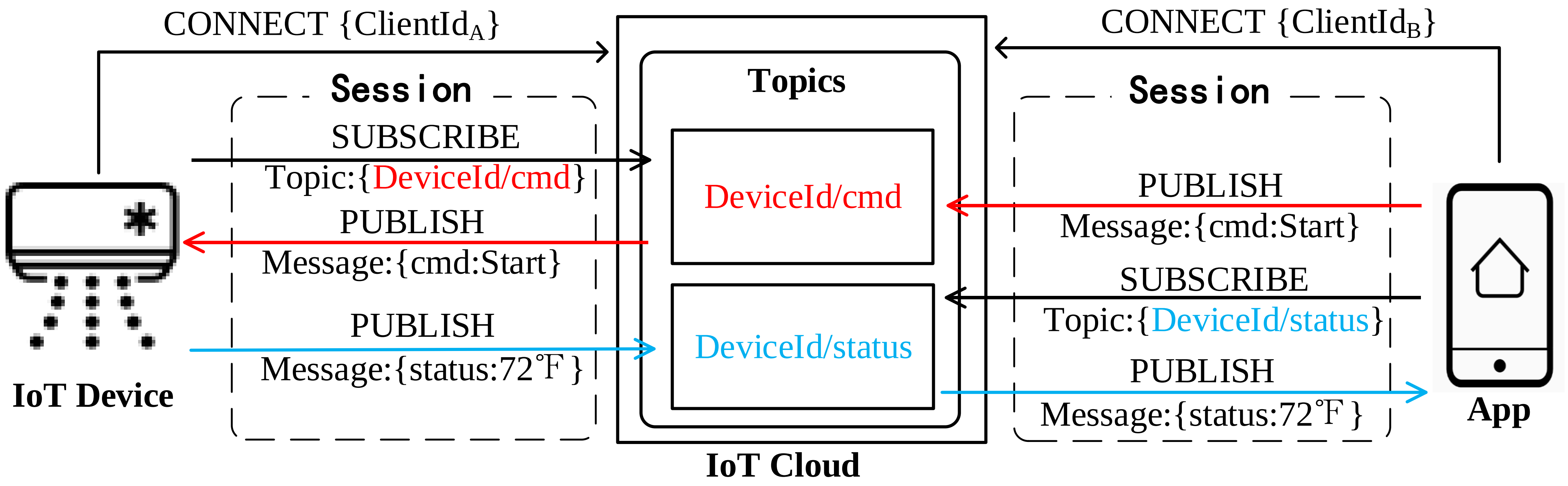
MQTT Version 5.0

OASIS Standard

07 March 2019

How MQTT works

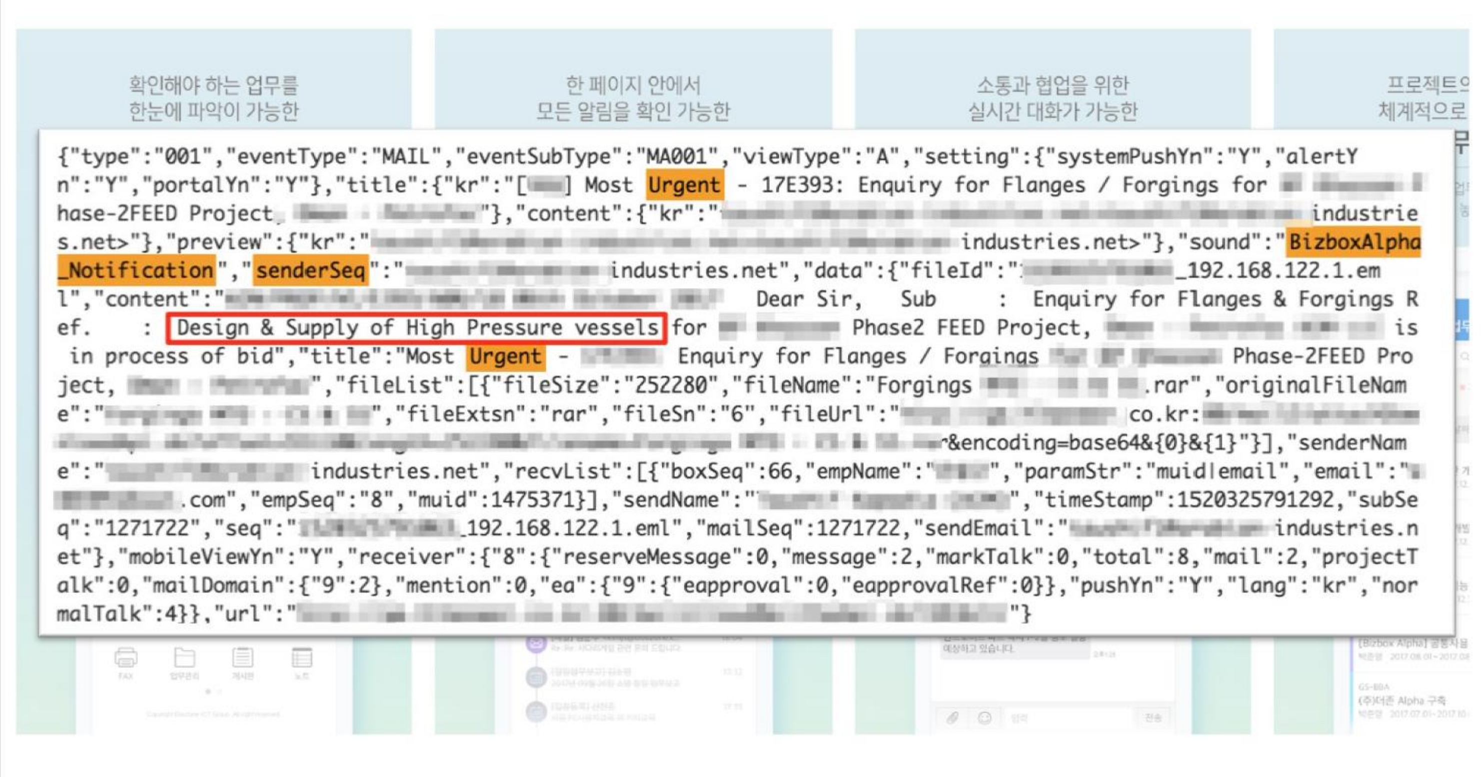
Type of Messages: Connect, Topic, Subscribe, Publish



Is MQTT secured?

No.

#



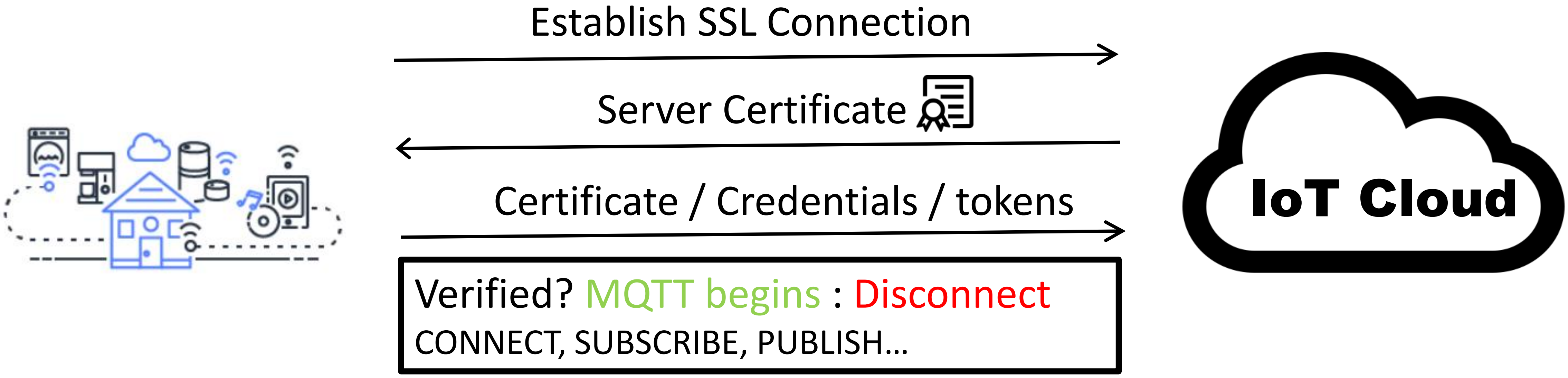
```
{"type":"001","eventType":"MAIL","eventSubType":"MA001","viewType":"A","setting":{"systemPushYn":"Y","alertY
n":"Y","portalYn":"Y"},"title":{"kr":"[[redacted]] Most Urgent - 17E393: Enquiry for Flanges / Forgings for [redacted]
hase-2FEED Project, [redacted]"},"content":{"kr":"[redacted] industrie
s.net>"},"preview":{"kr":"[redacted] industries.net>"},"sound":"BizboxAlpha
_Notification","senderSeq":"[redacted] industries.net","data":{"fileId":"[redacted]_192.168.122.1.em
l","content":"[redacted] Dear Sir,    Sub     :  Enquiry for Flanges & Forgings R
ef.    : Design & Supply of High Pressure vessels for [redacted] Phase2 FEED Project, [redacted] is
 in process of bid","title":"Most Urgent - [redacted] Enquiry for Flanges / Forgings [redacted] Phase-2FEED Pro
ject, [redacted]","fileList":[{"fileSize":"252280","fileName":"Forgings [redacted].rar","originalFileNam
e":"[redacted]","fileExtsn":"rar","fileSn":"6","fileUrl":"[redacted] co.kr:[redacted]
[redacted]&encoding=base64&{0}&{1}"}],"senderNam
e":"[redacted] industries.net","recvList":[{"boxSeq":66,"empName":"[redacted]","paramStr":"muid|email","email":"[redacted]
[redacted].com","empSeq":"8","muid":1475371}],"sendName":"[redacted]","timeStamp":1520325791292,"subSe
q":"1271722","seq":"[redacted]_192.168.122.1.eml","mailSeq":1271722,"sendEmail":"[redacted] industries.n
et"},"mobileViewYn":"Y","receiver":{"8":{"reserveMessage":0,"message":2,"markTalk":0,"total":8,"mail":2,"projectT
alk":0,"mailDomain":{"9":2},"mention":0,"ea":{"9":{"eapproval":0,"eapprovalRef":0}},"pushYn":"Y","lang":"kr","nor
malTalk":4}},"url":"[redacted]"}
```

[1] Lucas Lundgren. Blackhat USA 2017

[2] Federico Maggi, Davide Quarta. Blackhat Europe 2018.

Protection of MQTT on IoT Clouds

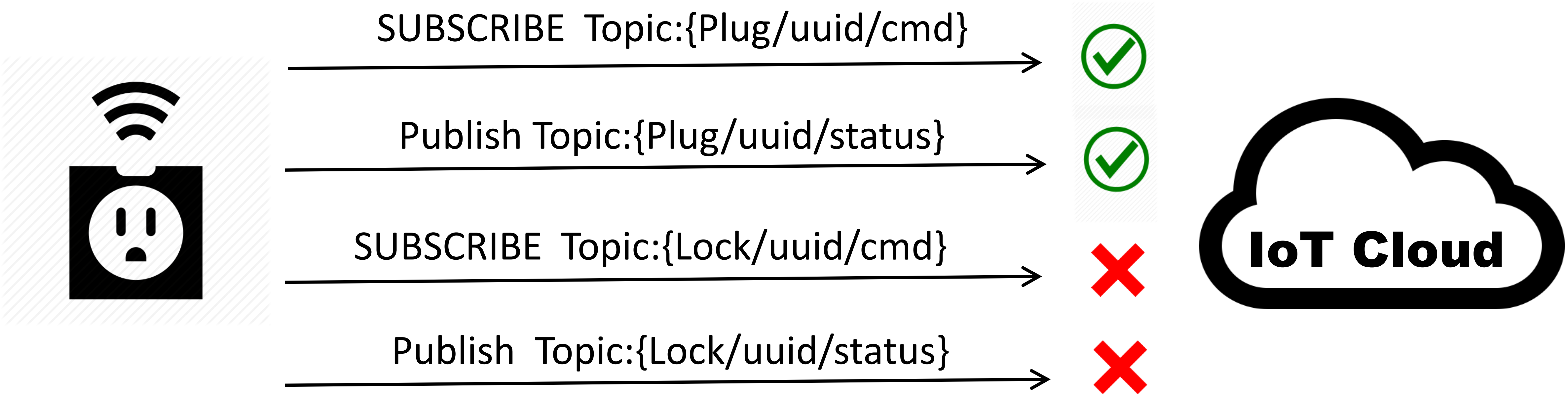
- Authentication
  - X.509 Client Certificates
  - Username/Password in MQTT Connect
  - Other Identities (e.g., Amazon Cognito)



Verified? MQTT begins : Disconnect
CONNECT, SUBSCRIBE, PUBLISH…

Protection of MQTT on IoT Clouds

- Authorization
  - Flexible policy
  - Access control template


SUBSCRIBE Topic:{Plug/uuid/cmd}
✓
Publish Topic:{Plug/uuid/status}
✓
SUBSCRIBE Topic:{Lock/uuid/cmd}
✗
Publish Topic:{Lock/uuid/status}
✗
IoT Cloud

Is MQTT really secured ?

Alibaba Cloud | Worldwide Cloud Services Partner

tuya.com

IoT Hub | Microsoft Azure

BAIDU AI CLOUD

AWS IoT Core

Cloud IoT Core | Google

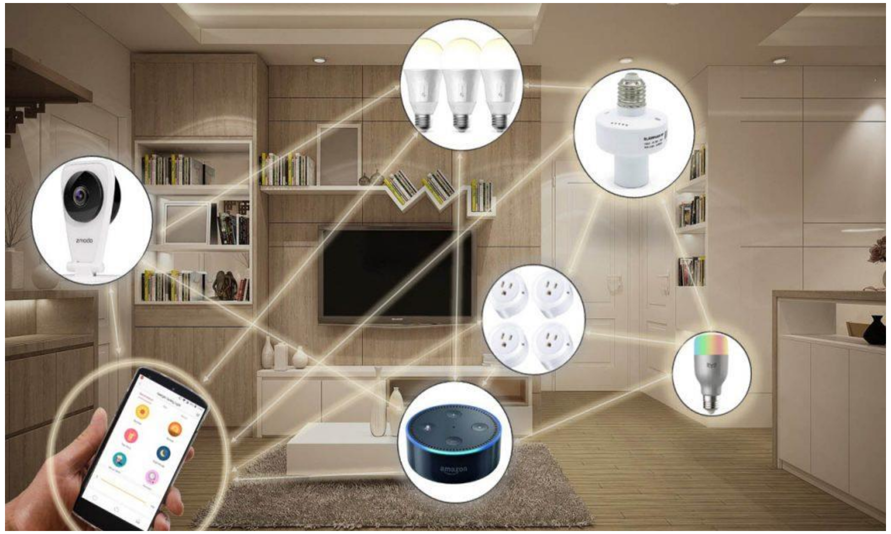
SUNING 苏宁易购

Watson IoT Platform | IBM

mosquitto

Usage scenarios of MQTT becomes more complex.

industrial proprietary devices → various IoT devices that can be shared and transferred

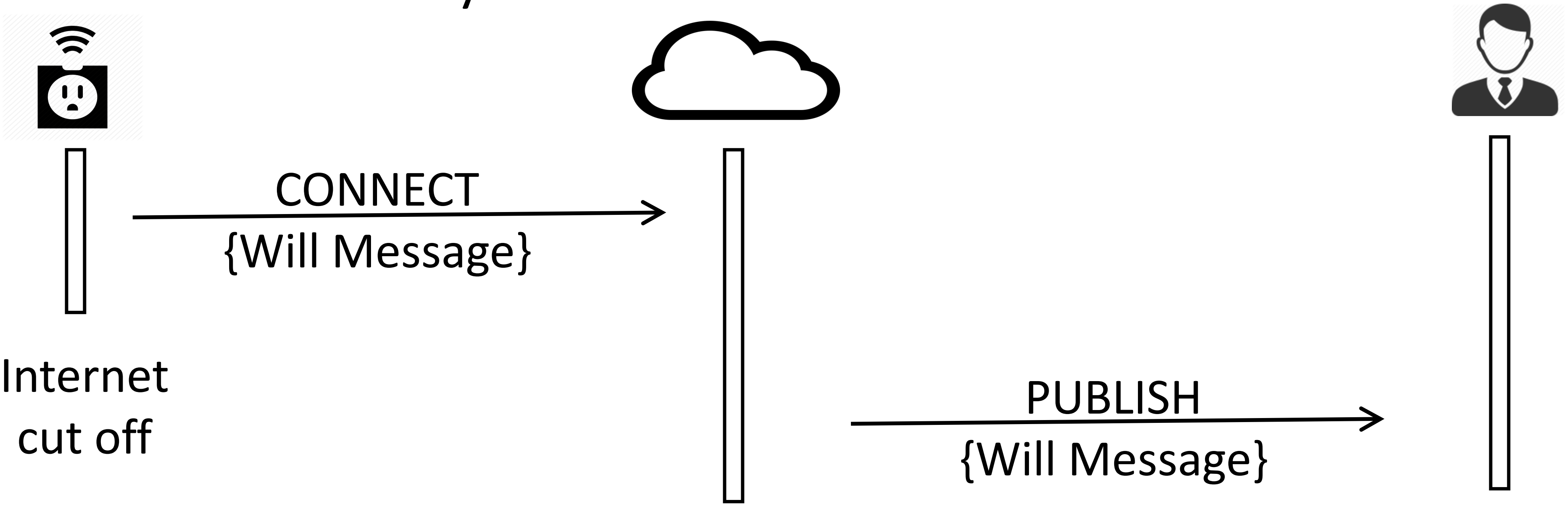


Attack #1

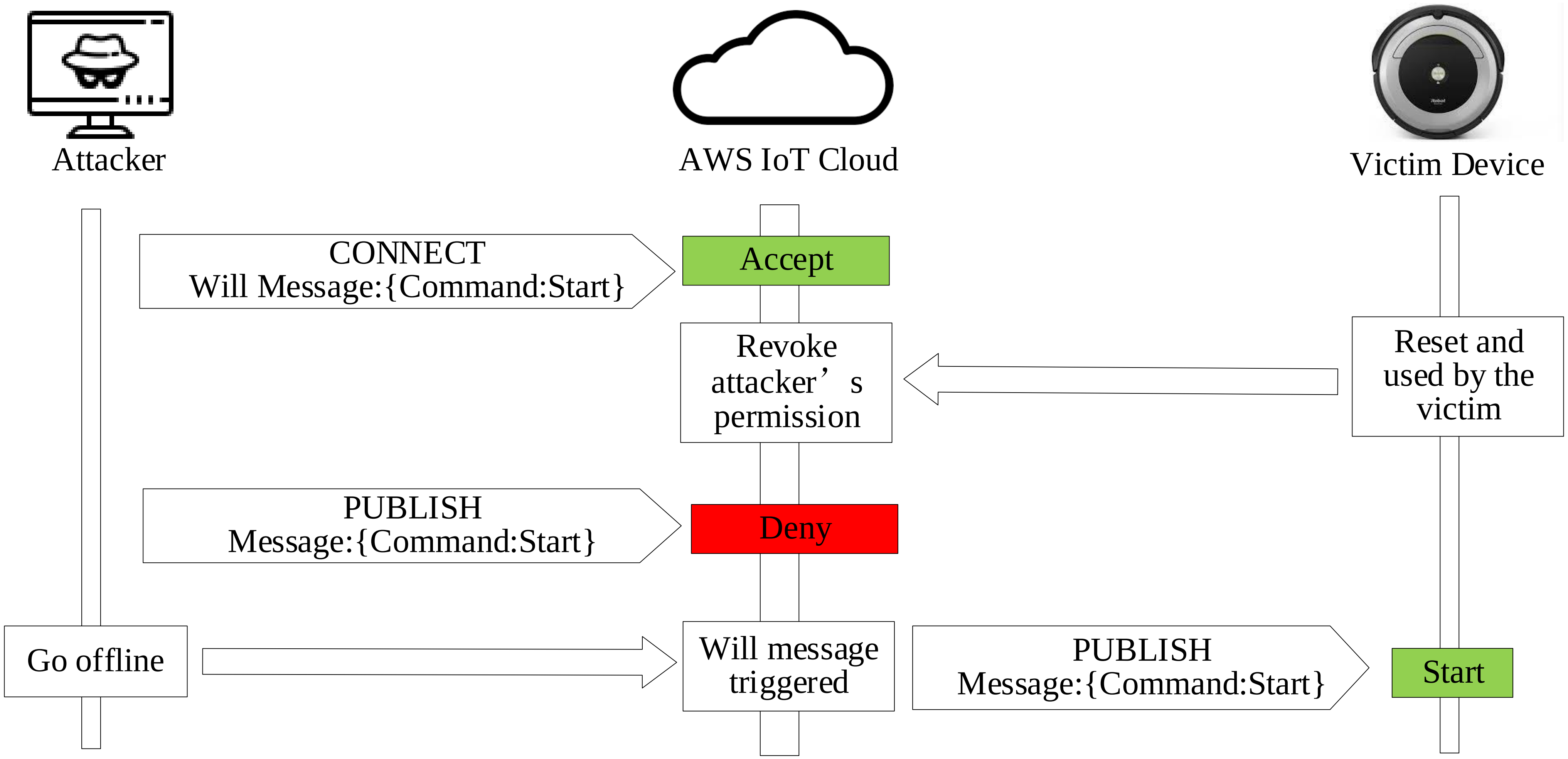
Unauthorized MQTT Messages

Will Message

- An optional payload in CONNECT
- Carries topics and messages
- Published by the server when client disconnects accidentally



Will Message Attack



Attacker

AWS IoT Cloud

Victim Device

CONNECT
Will Message:{Command:Start}

Accept

Revoke attacker’ s permission

Reset and used by the victim

PUBLISH
Message:{Command:Start}

Deny

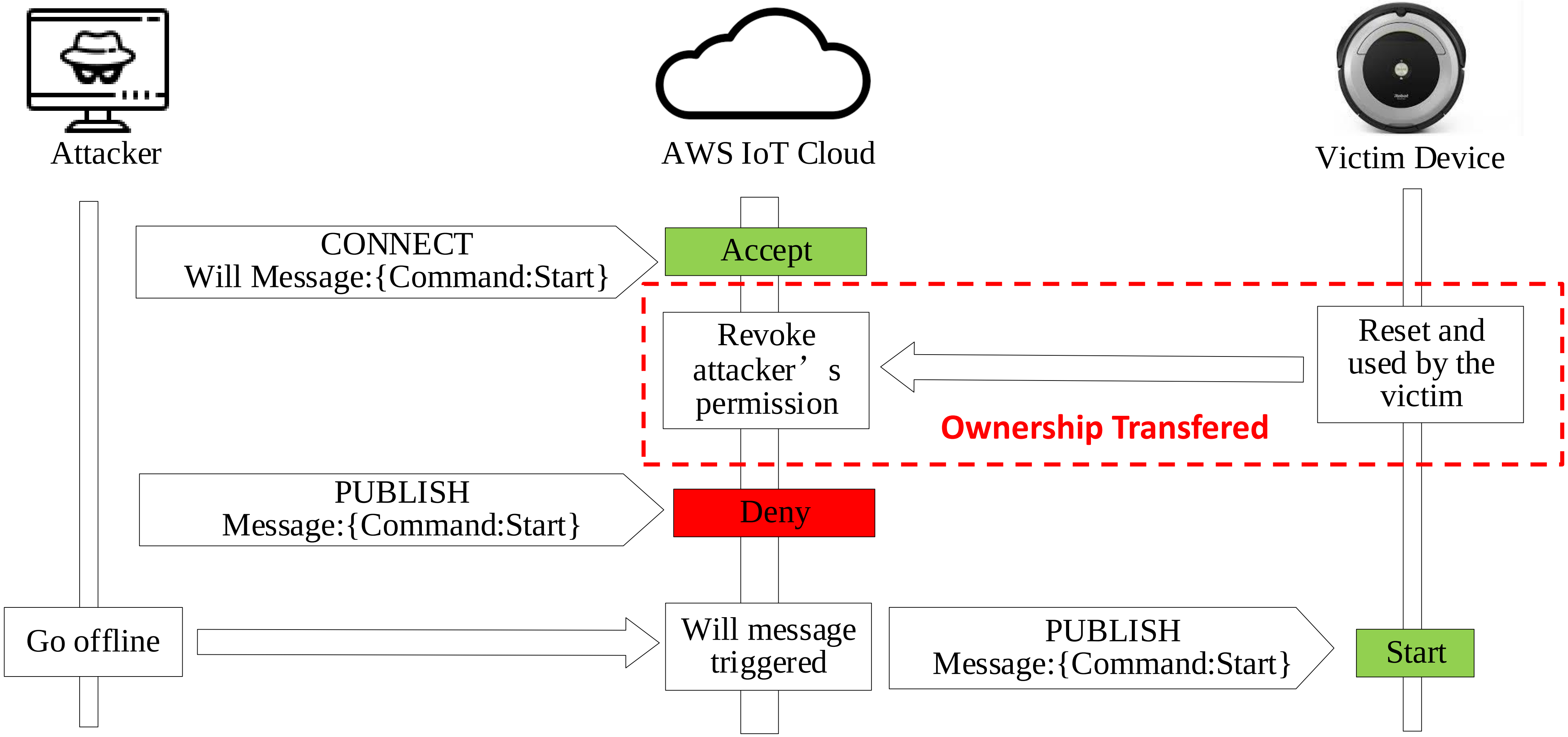
Go offline

Will message triggered

PUBLISH
Message:{Command:Start}

Start

Will Message Attack



Attacker

AWS IoT Cloud

Victim Device

CONNECT
Will Message:{Command:Start}

Accept

Revoke attacker’ s permission

Reset and used by the victim

Ownership Transfered

PUBLISH
Message:{Command:Start}

Deny

Go offline

Will message triggered

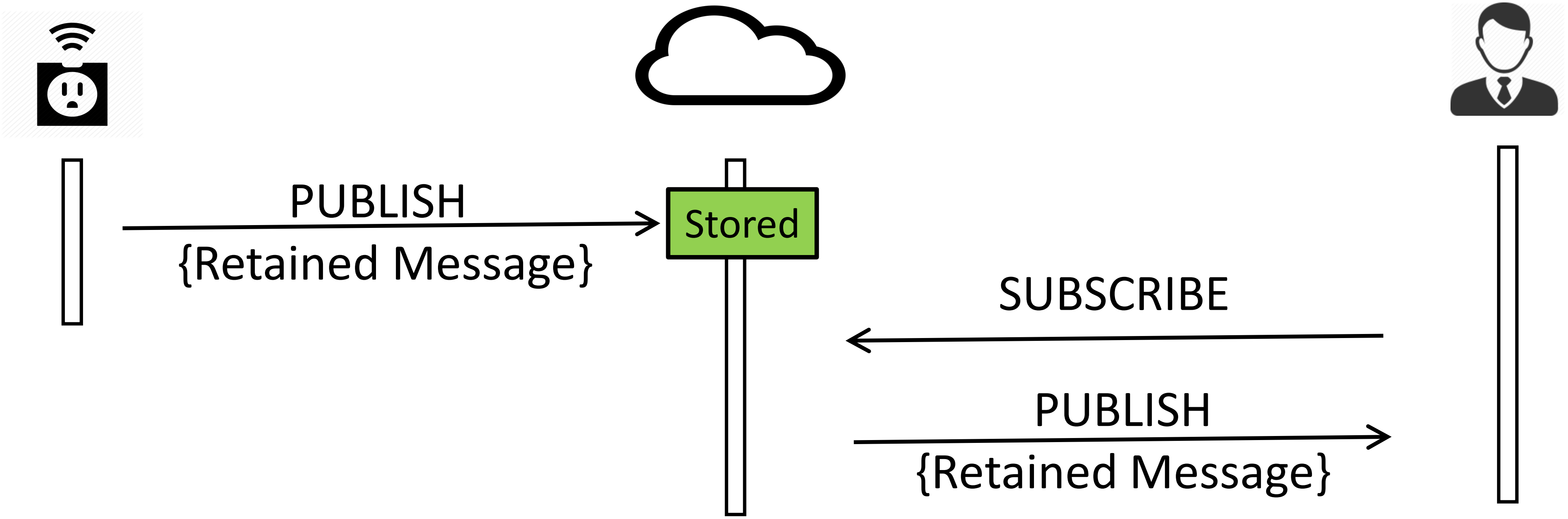
PUBLISH
Message:{Command:Start}

Start

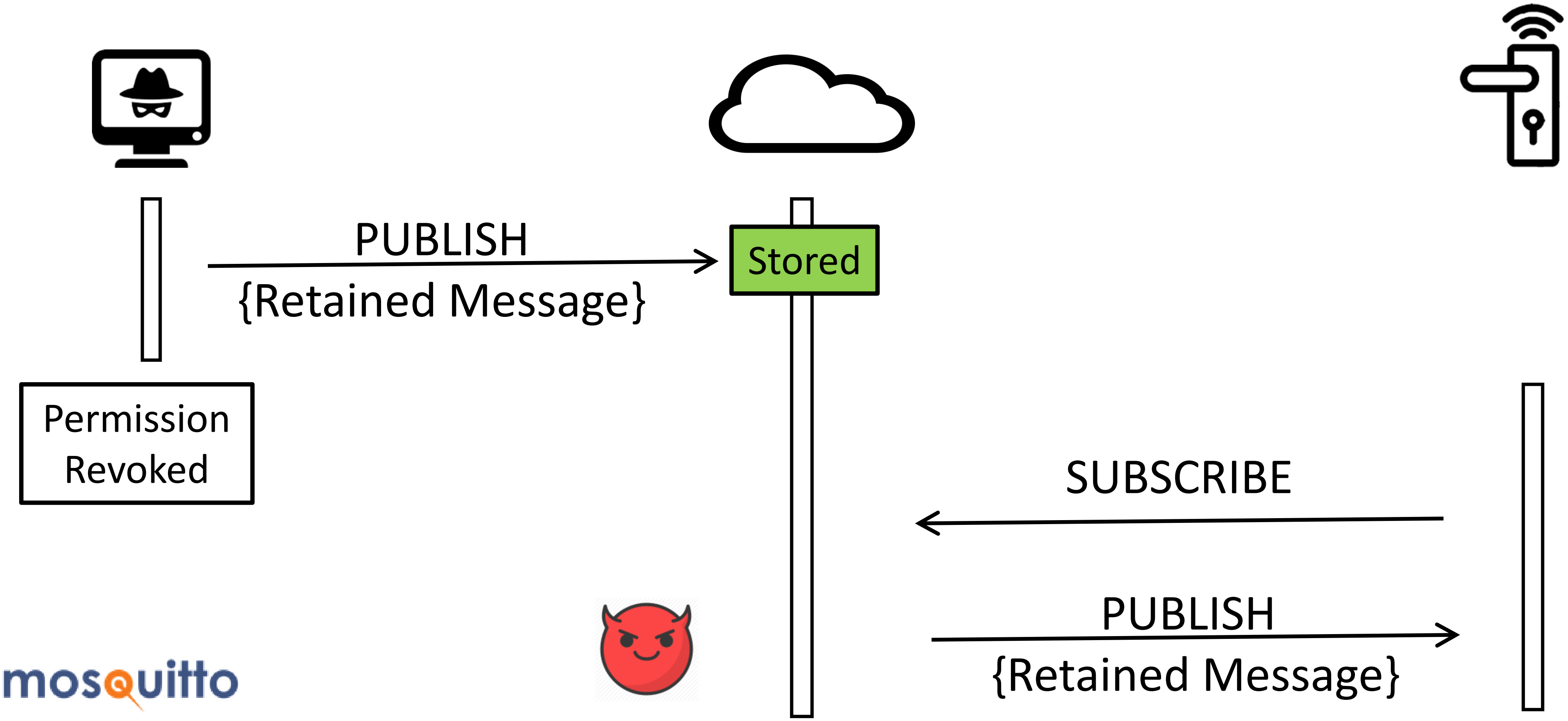
Video Demo

Retained Message

- A normal MQTT message with the retained flag set to be true
- Stored by the server for that topic
- Client that subscribes to the topic will receive the message



Retained Message Attack



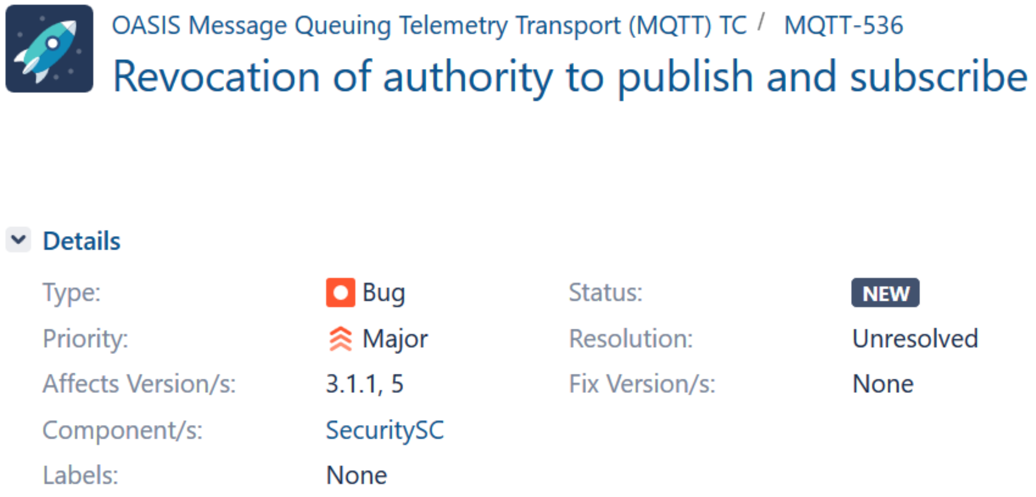
mosquitto

CVE-2018-12546

Why?

- It seems a feature as designed **Comments from MQTT TC**
  - “The Will message is accepted at the time it is set. That act of acceptance grants the permission for it to be delivered at a later time. The client is out of the picture. “

- Open discussion
  - [OASIS Open Issues MQTT-536]
  - mqtt-comment@lists.oasis-open.org



OASIS Message Queuing Telemetry Transport (MQTT) TC / MQTT-536

Revocation of authority to publish and subscribe

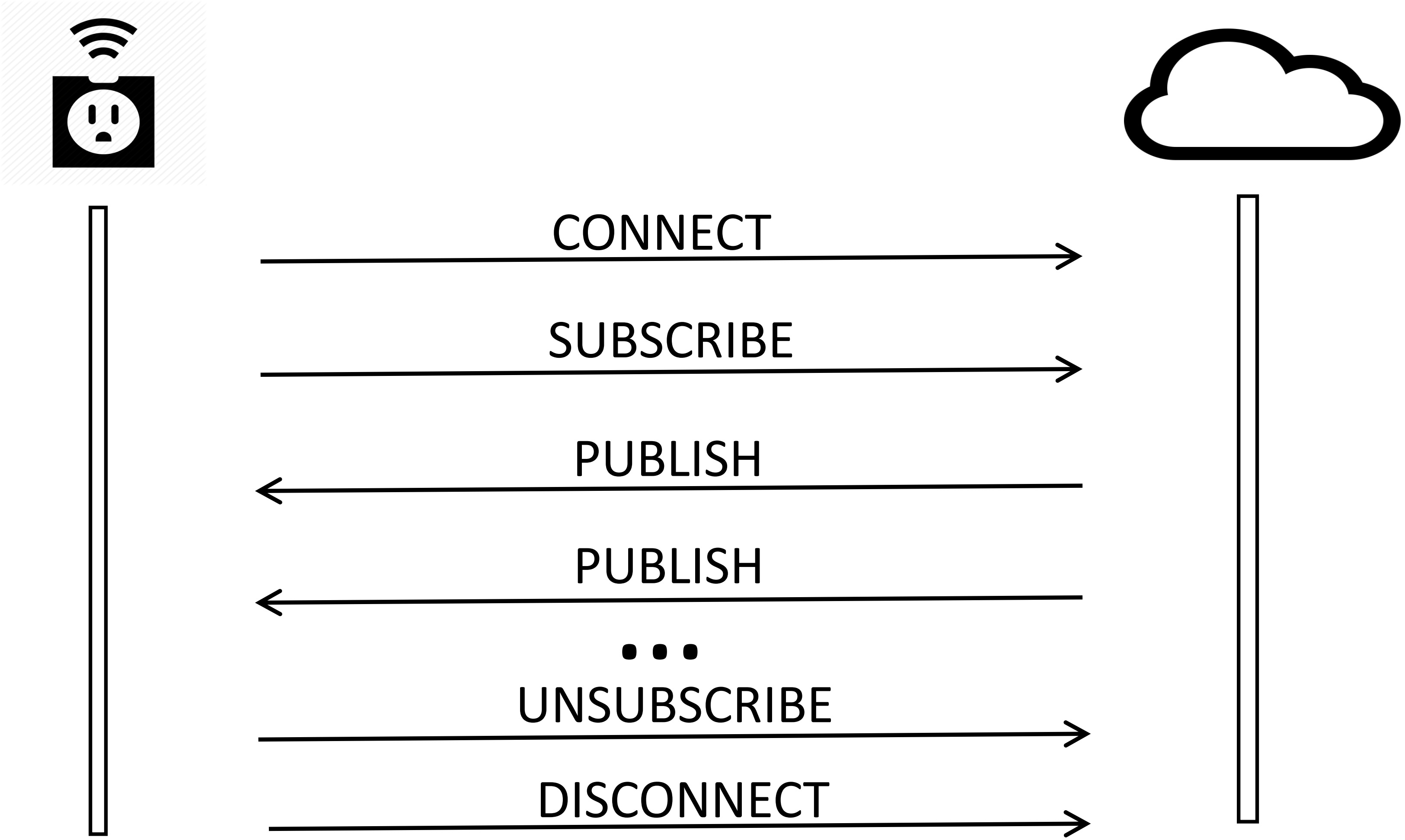
Details

Type:	Bug	Status:	NEW
Priority:	Major	Resolution:	Unresolved
Affects Version/s:	3.1.1, 5	Fix Version/s:	None
Component/s:	SecuritySC		
Labels:	None		

Attack #2

Faults in Managing MQTT Sessions

MQTT Session



CONNECT

SUBSCRIBE

PUBLISH

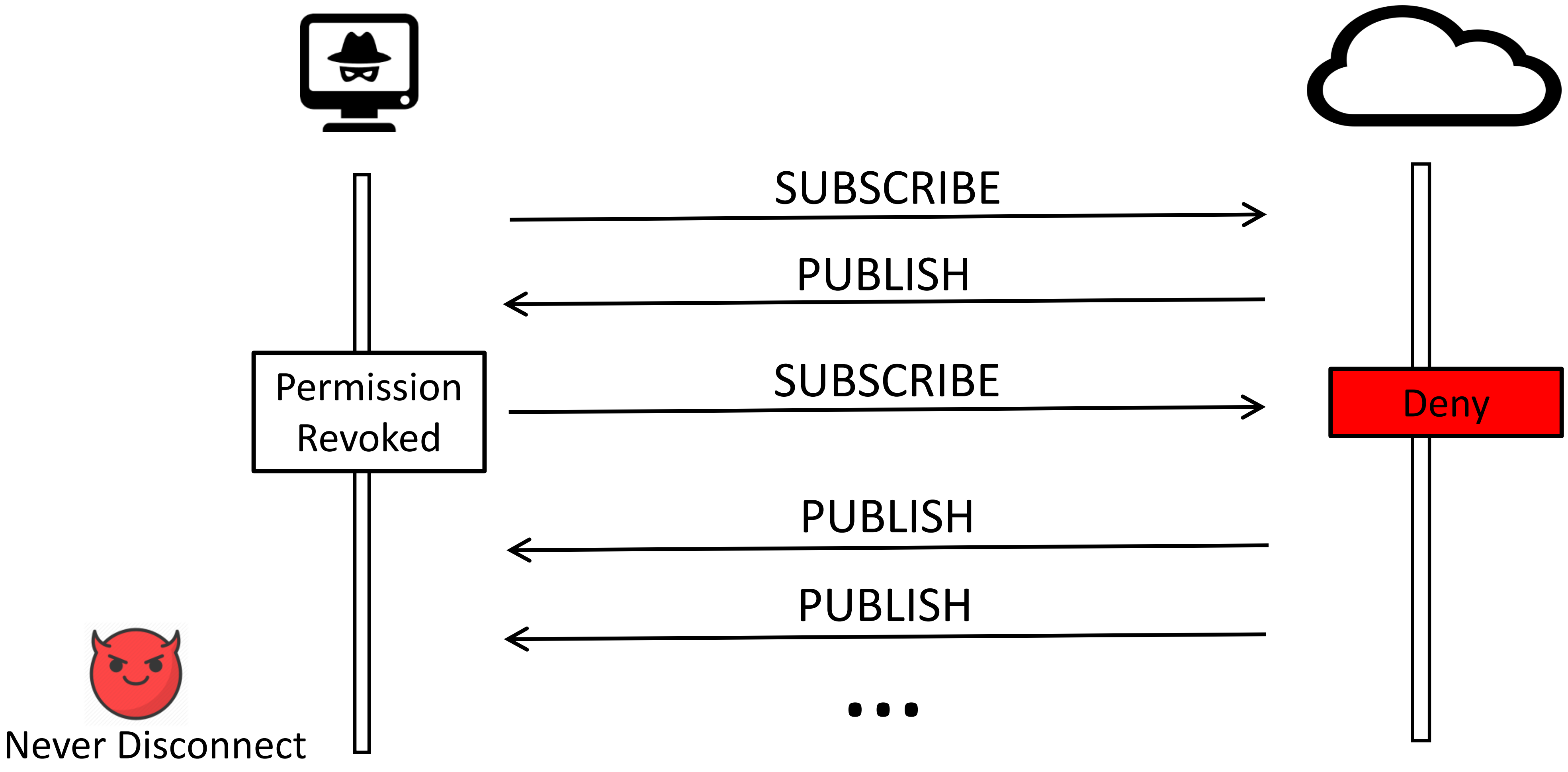
PUBLISH

...

UNSUBSCRIBE

DISCONNECT

Problem in MQTT Session Management



Security Adopted

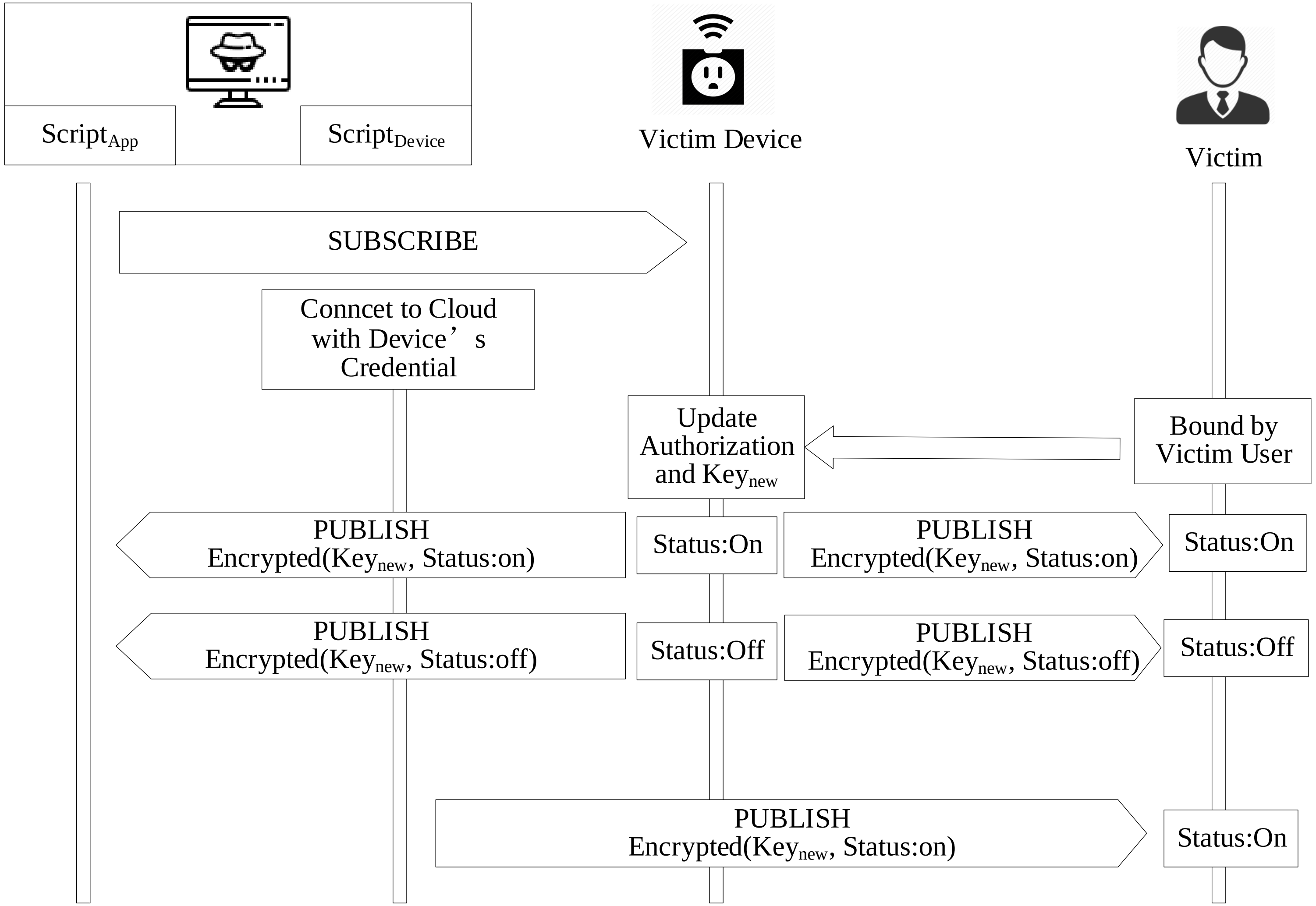
- Application-layer encryption

- Update the encryption key along with the user
  - Cannot be read by others
  - But can be replayed

- Update the credentials of device after reset
  - Preventing device forgery
  - But can be forged by keeping MQTT session

tuya.com

Impersonation Attack on Tuya Smart



Script$_{App}$
Script$_{Device}$
Victim Device
Victim
SUBSCRIBE
Conncet to Cloud with Device’s Credential
Update Authorization and Key$_{new}$
Bound by Victim User
PUBLISH Encrypted(Key$_{new}$, Status:on)
Status:On
PUBLISH Encrypted(Key$_{new}$, Status:on)
Status:On
PUBLISH Encrypted(Key$_{new}$, Status:off)
Status:Off
PUBLISH Encrypted(Key$_{new}$, Status:off)
Status:Off
PUBLISH Encrypted(Key$_{new}$, Status:on)
Status:On

Video Demo

Why?

- "The Server MAY use a security component to authorize particular actions on the topic resource for a given Client." -- MQTT 5.0 specification
  - CONNECT
  - SUBSCRIBE
  - PUBLISH

Session is not in picture

- Clients manage the session
  - SUBSCRIBE
  - UNSUBSCRIBE
  - DISCONNECT

NEVER TRUST CLIENT

Why?

- “The Server MAY use a security component to authorize particular actions on the topic resource for a given Client.” -- MQTT 5.0 specification
    - CONNECT
    - SUBSCRIBE
    - PUBLISH

Session is not in picture

- Clients manage the session
    - SUBSCRIBE
    - UNSUBSCRIBE
    - DISCONNECT

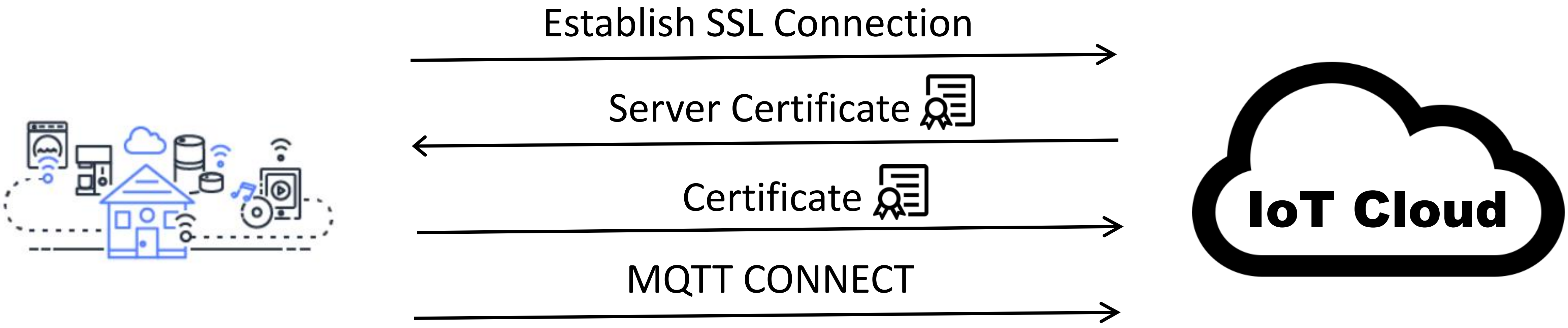
NEVER TRUST CLIENT

Good news:
MQTT5 allows DISCONNECT
to be sent by server.

Attack #3

Unauthenticated MQTT Identity

Identity Management in MQTT



Establish SSL Connection

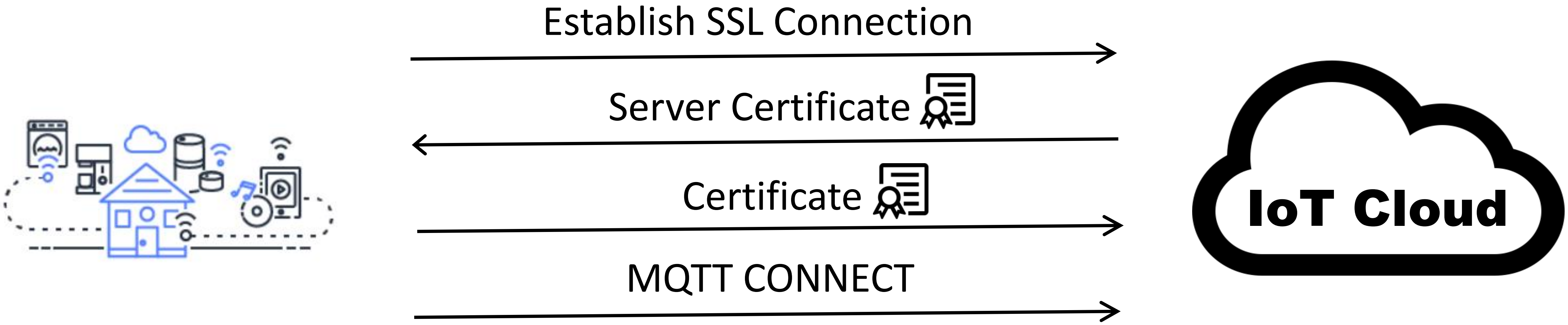
Server Certificate

Certificate

MQTT CONNECT

IoT Cloud

Identity Management in MQTT



Establish SSL Connection

Server Certificate

Certificate

MQTT CONNECT

IoT Cloud

CONNECT

ClientId
Will Flag
Clean Session Flag
Password Flag
…

Client Identifier (ClientId)

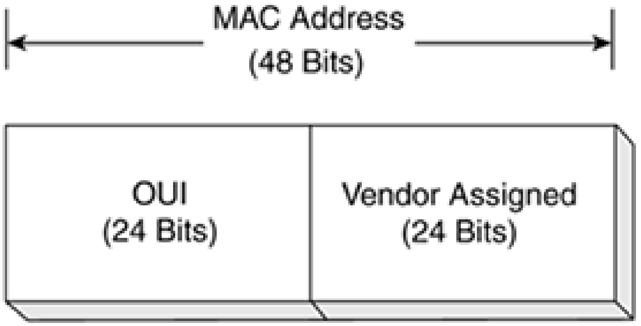
- “The Client Identifier (ClientId) identifies the Client to the Server. Each Client connecting to the Server has a unique ClientId.” -- MQTT Specification
  - If two clients claim the same ClientId, the later one will kick the connected one off.

- “The Server MUST allow ClientIds which are between 1 and 23 UTF-8 encoded bytes in length.” -- MQTT Specification
  - As short as 1-byte

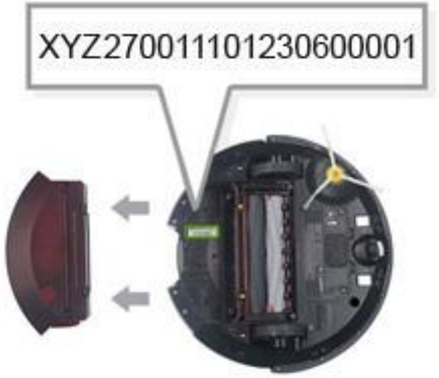
OASIS Standard

ClientId in Vendors View

- “Do you manufacture the device with a client identifier - such as using its MAC address? “ – IBM Knowledge Center
  - Unique
  - Easy to guess



- Serial number of device
  - Unique
  - Easy to guess



- Constant string
  - Identify the device
  - Device sharing

Attack

- iRobot Roomba 690
  - Looks like a 16-digit serial number (e.g, 3147C60043211234)
  - Queried 200,000 numbers through a Web API
  - Found 10,000 ClientIds in wild after hours
  - The ClientId of mobile app can be changed

Attack

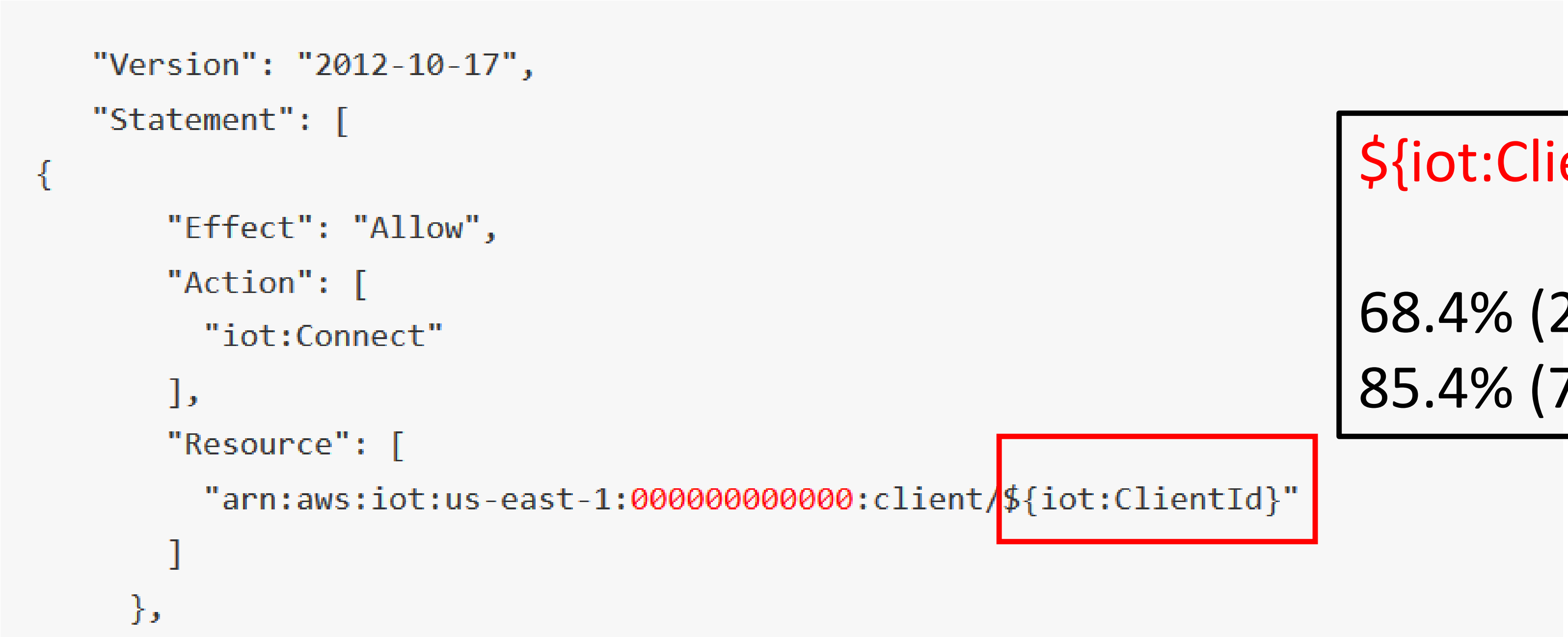
- iRobot Roomba 690
  - Looks like a 16-digit serial number (e.g, 3147C60043211234)
  - Queried 200,000 numbers through a Web API
  - Found 10,000 ClientIds in wild after hours
  - The ClientId of mobile app can be changed
  - Kick the 10,000 robots offline!

PoC Attack

- iRobot Roomba 690
  - Looks like a 16-digit serial number (e.g, 3147C60043211234)
  - Queried 200,000 numbers through a Web API
  - Found 10,000 ClientIds in wild after hours
  - The ClientId of mobile app can be changed
  - ~~Kick the 10,000 robots offline!~~
  - Only kick our own robot offline
  - One client identity, 2,000 concurrent connections (on our own AWS IoT endpoint)
- Session hijacking
  - Clean session flag

Why?

- ClientId is not a secret
- No feature provided by (some) IoT clouds to restrict the ClientId
- Misleading development guide



```
    "Version": "2012-10-17",
    "Statement": [
  {
        "Effect": "Allow",
        "Action": [
          "iot:Connect"
        ],
        "Resource": [
          "arn:aws:iot:us-east-1:000000000000:client/${iot:ClientId}"
        ]
      },
```

${iot:ClientId} or *

68.4% (26/38) recommended by AWS
85.4% (76/89) on Github

AWS Blog

Attack #4

Authorization Mystery of MQTT Topics

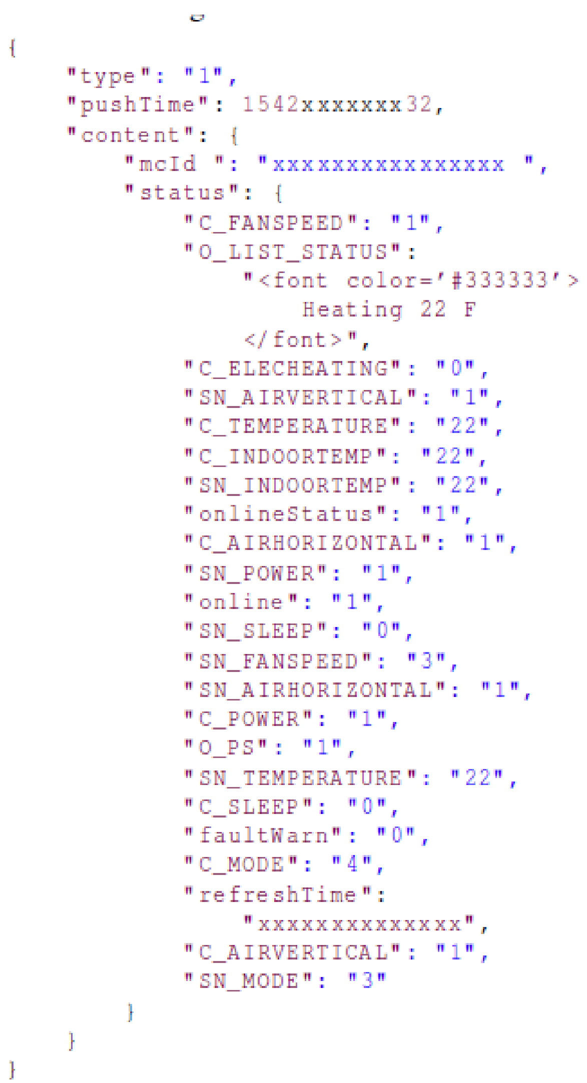
Authorization Mystery of MQTT Topics

- sport/#
  - sport/tennis/player1
  - sport/tennis/player1/ranking
  - sport/football/
- When it comes to policy of AWS IoT…
  - *-irbthbu/things/${robotid}/cmd
  - botnet/-irbthbu/things/${robotid}/cmd

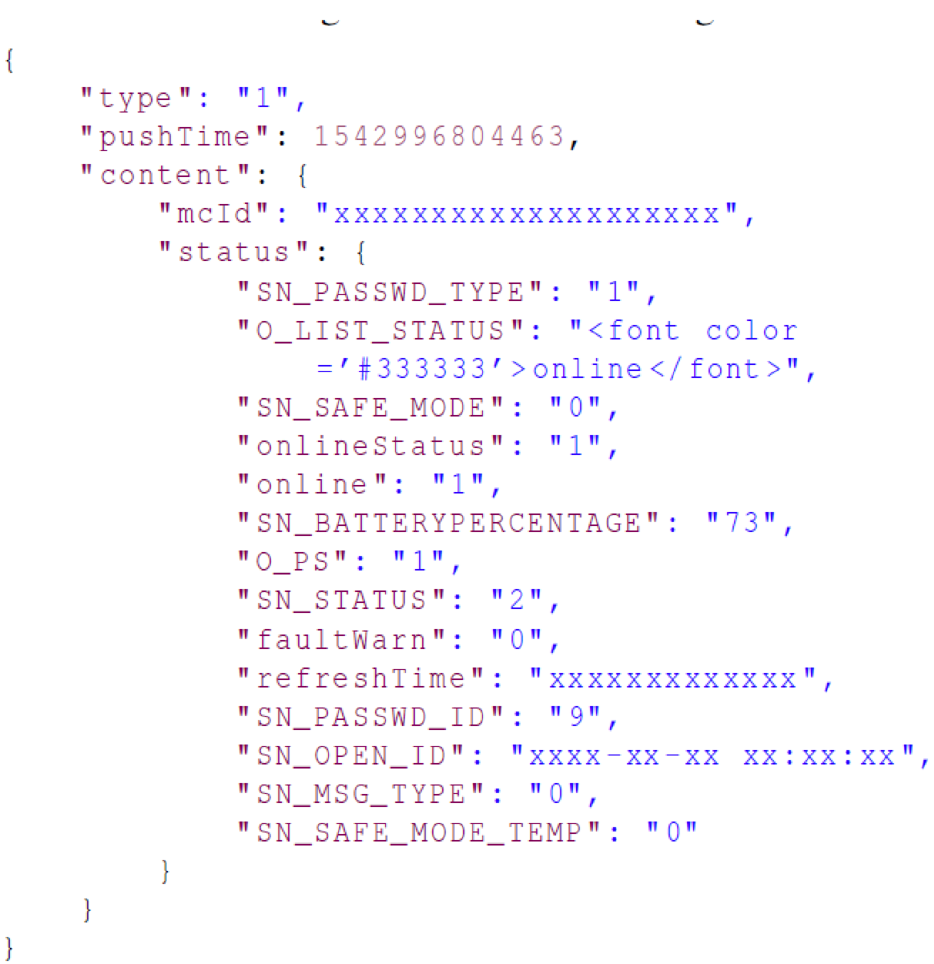
Buy One

Get One aws FREE!

#



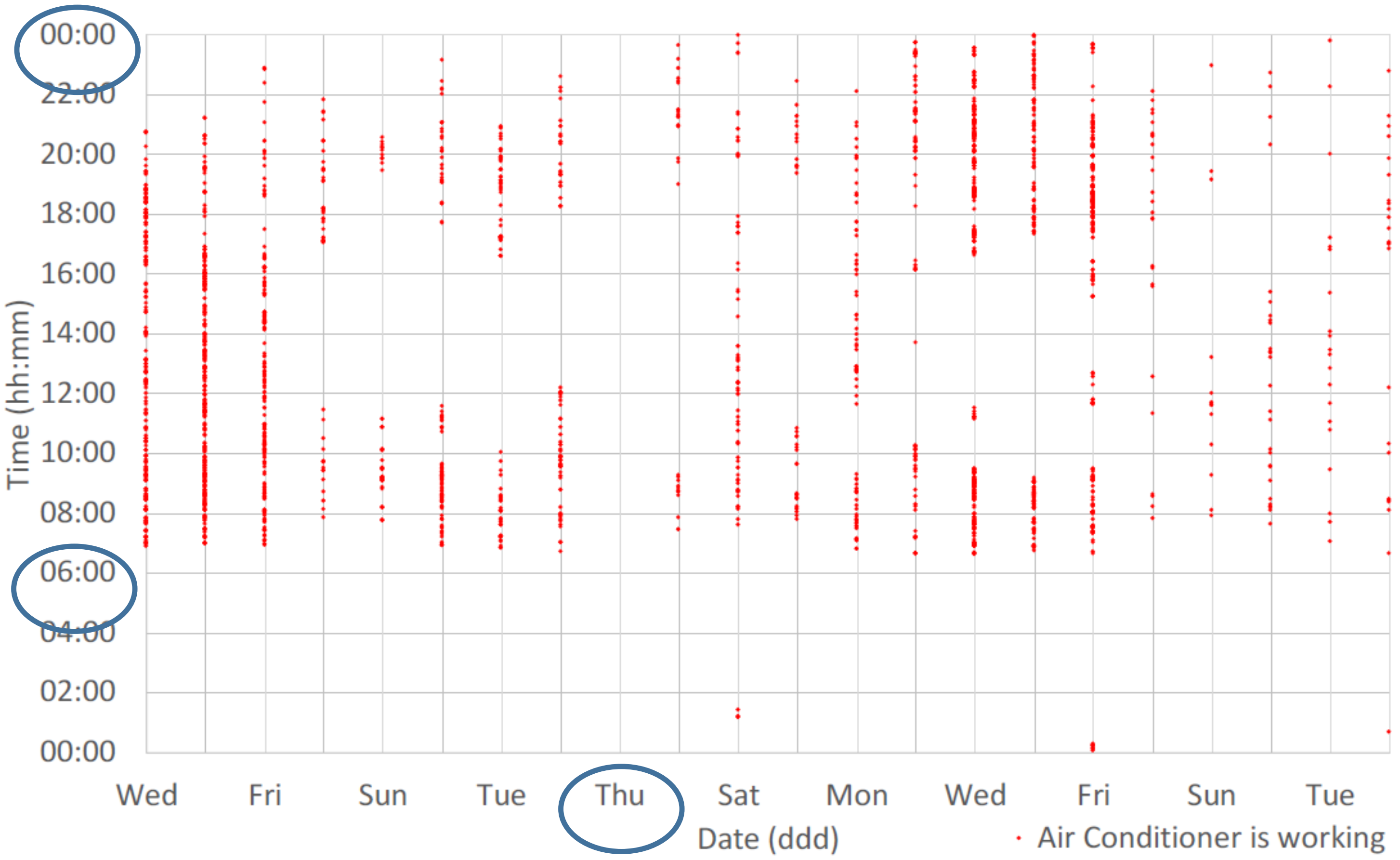
```
{
    "type": "1",
    "pushTime": 1542xxxxxxx32,
    "content": {
        "mcId ": "xxxxxxxxxxxxxxxx ",
        "status": {
            "C_FANSPEED": "1",
            "O_LIST_STATUS":
                "<font color='#333333'>
                    Heating 22 F
                </font>",
            "C_ELECHEATING": "0",
            "SN_AIRVERTICAL": "1",
            "C_TEMPERATURE": "22",
            "C_INDOORTEMP": "22",
            "SN_INDOORTEMP": "22",
            "onlineStatus": "1",
            "C_AIRHORIZONTAL": "1",
            "SN_POWER": "1",
            "online": "1",
            "SN_SLEEP": "0",
            "SN_FANSPEED": "3",
            "SN_AIRHORIZONTAL": "1",
            "C_POWER": "1",
            "O_PS": "1",
            "SN_TEMPERATURE": "22",
            "C_SLEEP": "0",
            "faultWarn": "0",
            "C_MODE": "4",
            "refreshTime":
                "xxxxxxxxxxxxx",
            "C_AIRVERTICAL": "1",
            "SN_MODE": "3"
        }
    }
}
```



```
{
    "type": "1",
    "pushTime": 1542996804463,
    "content": {
        "mcId": "xxxxxxxxxxxxxxxxxxxx",
        "status": {
            "SN_PASSWD_TYPE": "1",
            "O_LIST_STATUS": "<font color
                ='#333333'>online</font>",
            "SN_SAFE_MODE": "0",
            "onlineStatus": "1",
            "online": "1",
            "SN_BATTERYPERCENTAGE": "73",
            "O_PS": "1",
            "SN_STATUS": "2",
            "faultWarn": "0",
            "refreshTime": "xxxxxxxxxxxxx",
            "SN_PASSWD_ID": "9",
            "SN_OPEN_ID": "xxxx-xx-xx xx:xx:xx",
            "SN_MSG_TYPE": "0",
            "SN_SAFE_MODE_TEMP": "0"
        }
    }
}
```

- 800 million real-world MQTT messages from a popular smart home Cloud
- IRB approval
- Observation
  - E-mail / Phone number
  - device IDs and types (e.g., door lock, air conditioner, camera, etc.)
  - device status (“open”, “on”, “off”, “heating”, etc.)
  - device location (“home”, “office”, “living room”, etc.)
  - information captured by the device (temperature, air quality, etc.)
  - cohabitants relation ("[Person Name set by user] opened the door”)
  - Timestamp
  - …

Air conditioning status of a device



Lessons Learnt

Lessons Learnt

- Carefully applying a common-purpose protocol to your application
- Guard the ClientId
  - Building the tie of platform-layer identity and ClientId
- Guard various messages
  - Clients should never accept messages from previous users
- Guard sessions, not only actions
  - Consider sessions in authorization model (even extend state of the protocol)
- Guard resources
  - Consider specific syntax features of protocols

Thank You

西安電子科技大學
XIDIAN UNIVERSITY

中国科学院大学
University of Chinese Academy of Sciences

INDIANA UNIVERSITY
BLOOMINGTON