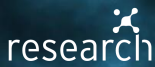




black hat[®]
EUROPE 2018
DECEMBER 3-6, 2018
EXCEL LONDON / UNITED KINGDOM

When Machines Can't Talk

Security & Privacy Issues of M2M Data Protocols



Federico Maggi
Senior Threat Researcher



POLITECNICO
MILANO 1863

Davide Quarta
Post-doc Researcher (now at EURECOM)

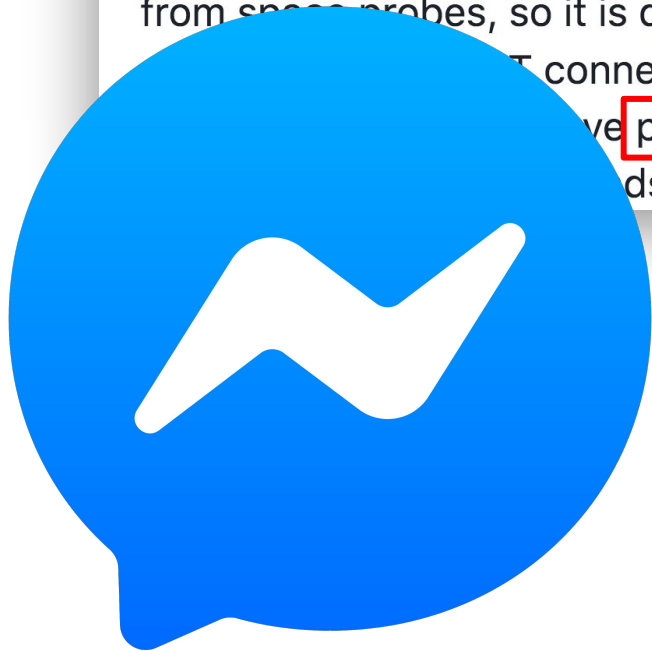
 #BHEU / @BLACKHATEVENTS



Collaborators

Stefano Zanero, POLIMI
Pouyan Sepehrdad, QUALCOMM PSI

One of the problems we experienced was long latency when sending a message. The method we were using to send was reliable but slow, and there were limitations on how much we could improve it. With just a few weeks until launch, we ended up building a new mechanism that maintains a persistent connection to our servers. To do this without killing battery life, we used a protocol called MQTT that we had experimented with in Beluga. MQTT is specifically designed for applications like sending telemetry data to and from space probes, so it is designed to use bandwidth and batteries sparingly. By maintaining a persistent connection and routing messages through our chat pipeline, we achieved phone-to-phone delivery in the hundreds of milliseconds.



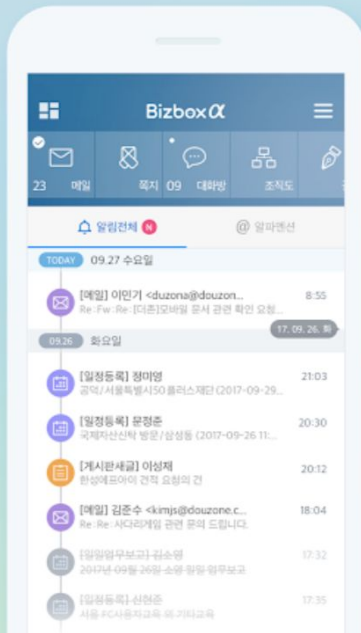
확인해야 하는 업무를 한눈에 파악이 가능한 메인화면

사용자의 편의를 고려한 인터랙션 디자인을 통해
직관적인 업무 기능 제공



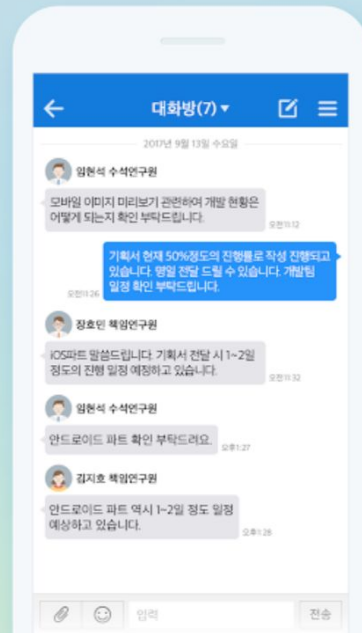
한 페이지 안에서 모든 알림을 확인 가능한 통합알림

하나의 알림 페이지에서 사내에서 공유되는
업무의 히스토리를 한눈에 빠르게 확인 가능



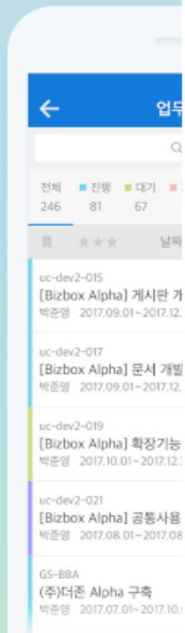
소통과 협업을 위한 실시간 대화가 가능한 대화방

일반 대화방 및 조직 기준의 프로젝트 대화방,
자주 참여하는 대화방을 즐겨찾기하는 기능 제공



프로젝트의 체계적으로 업무

프로젝트, 업무
표준화된 업무절차와



확인해야 하는 업무를
한눈에 파악이 가능한

한 페이지 안에서
모든 알림을 확인 가능한

소통과 협업을 위한
실시간 대화가 가능한

프로젝트으
체계적으로

```
{ "type": "001", "eventType": "MAIL", "eventSubType": "MA001", "viewType": "A", "setting": { "systemPushYn": "Y", "alertYn": "Y", "portalYn": "Y" }, "title": { "kr": "[ ] Most Urgent - 17E393: Enquiry for Flanges / Forgings for [ ] Industries.net" }, "content": { "kr": "Dear Sir, Sub : Enquiry for Flanges & Forgings R ef. : Design & Supply of High Pressure vessels for [ ] Phase2 FEED Project, [ ] is in process of bid", "title": "Most Urgent - Enquiry for Flanges / Forgings [ ] Phase-2FEED Project, [ ]", "fileList": [ { "fileSize": "252280", "fileName": "Forgings [ ] .rar", "originalFileName": "[ ]", "fileExtn": "rar", "fileSn": "6", "fileUrl": "[ ] co.kr: [ ]&encoding=base64&{0}&{1}" }, { "boxSeq": 66, "empName": "[ ]", "paramStr": "muidlemail", "email": "[ ] .com", "empSeq": "8", "muid": 1475371 } ], "sendName": "[ ]", "timeStamp": 1520325791292, "subSeq": "1271722", "seq": "[ ]_192.168.122.1.eml", "mailSeq": 1271722, "sendEmail": "[ ] industries.net" }, "mobileViewYn": "Y", "receiver": { "8": { "reserveMessage": 0, "message": 2, "markTalk": 0, "total": 8, "mail": 2, "projectTalk": 0, "mailDomain": { "9": 2 }, "mention": 0, "ea": { "9": { "eapproval": 0, "eapprovalRef": 0 } }, "pushYn": "Y", "lang": "kr", "normalTalk": 4 } }, "url": "[ ]" }
```



내일 안으로 발송되었습니다.
Re: Re: SK3342451 관련 문의 드립니다.

[일정업무보고] 김소영
2017년 09월 20일 소문 활동 업무보고

[일정동작] 신현준
서울 4차산업진흥국에 회신되었습니다.

안드로이드 버전에서 1:1로 영도 영도
예상하고 있습니다.

09:18

이력 전송

[Bizbox Alpha] 공통사용
박준영 2017.08.01 - 2017.08

GS-BBA
(주)더존 Alpha 구축
박준영 2017.07.01 - 2017.10

USERS

Large **consumer electronics** and mobile device manufacturer

Marine industry

Automotive parts manufacturer

Civil engineering, manufacturing and **constructions**

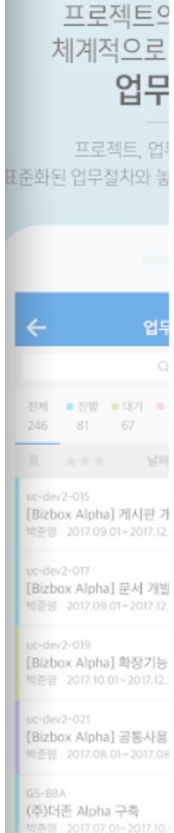
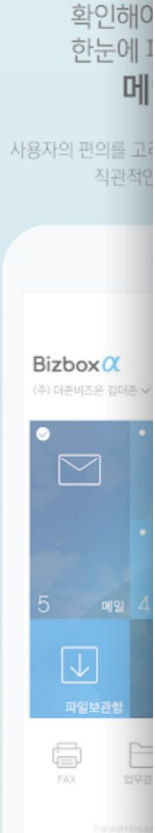
Medical & rehabilitation equipment

Logistics

Internet service providers

Industry-grade TFT display manufacturer

Fashion and clothing industry



How does
MQTT
work?

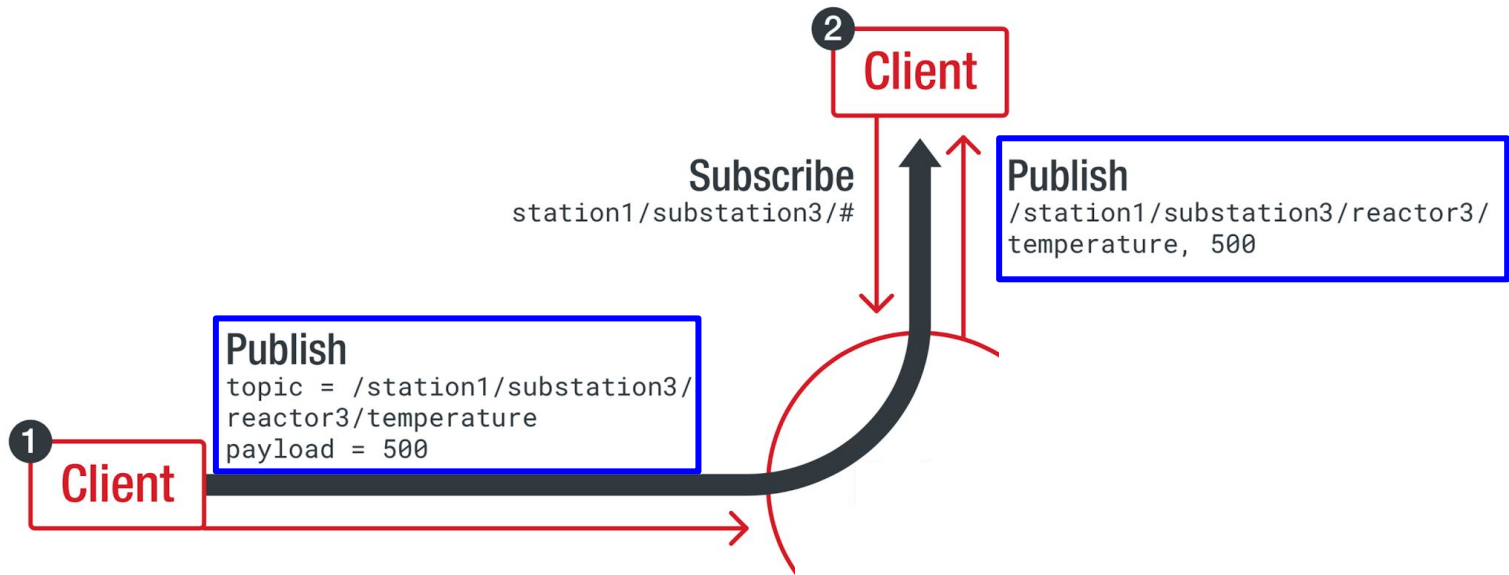
2

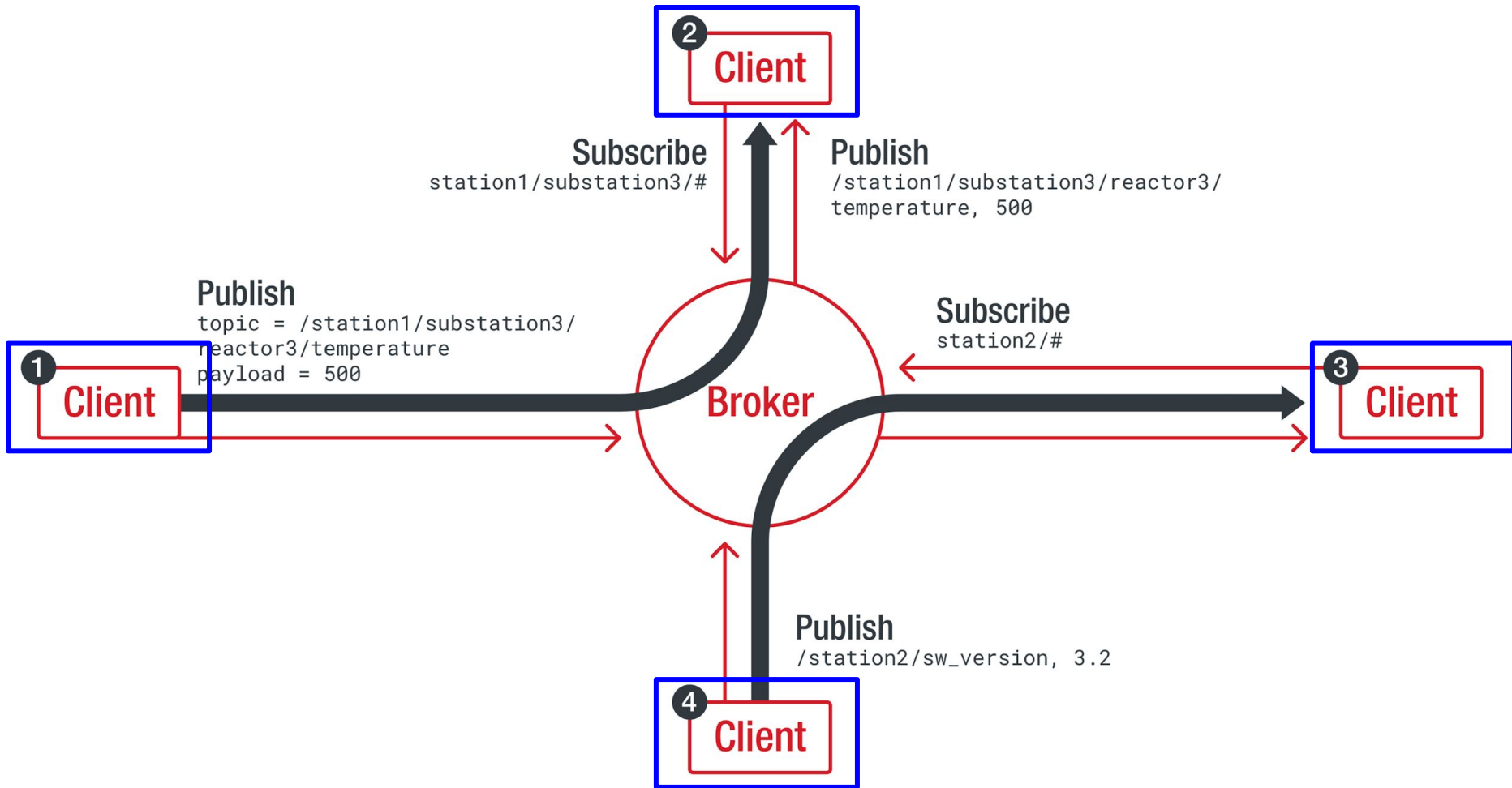
Client

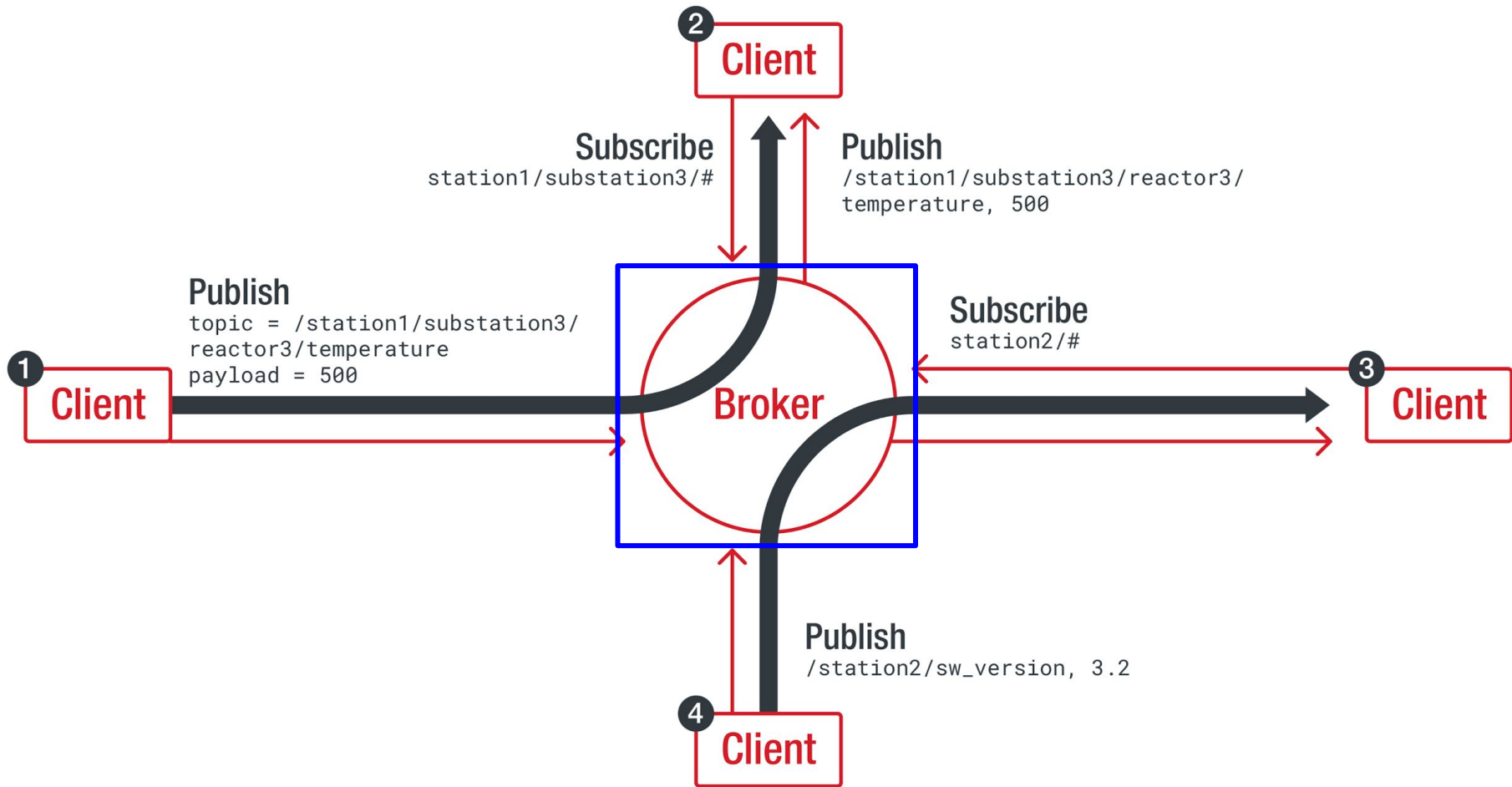
Subscribe

station1/substation3/#





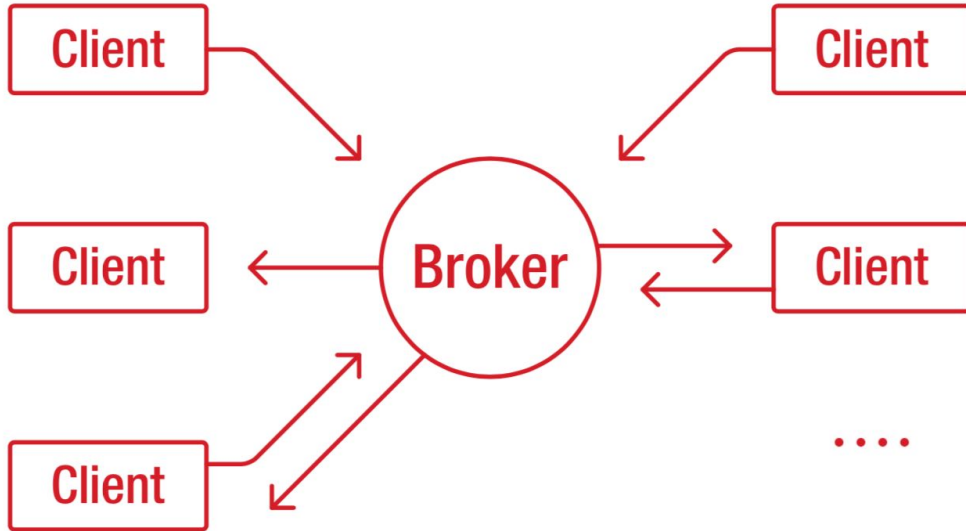




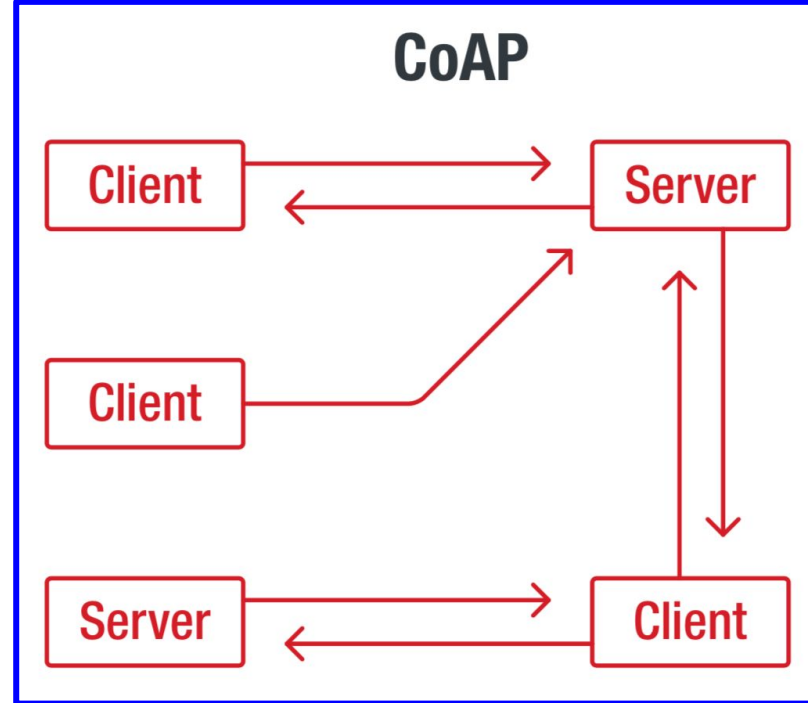
How about
CoAP?

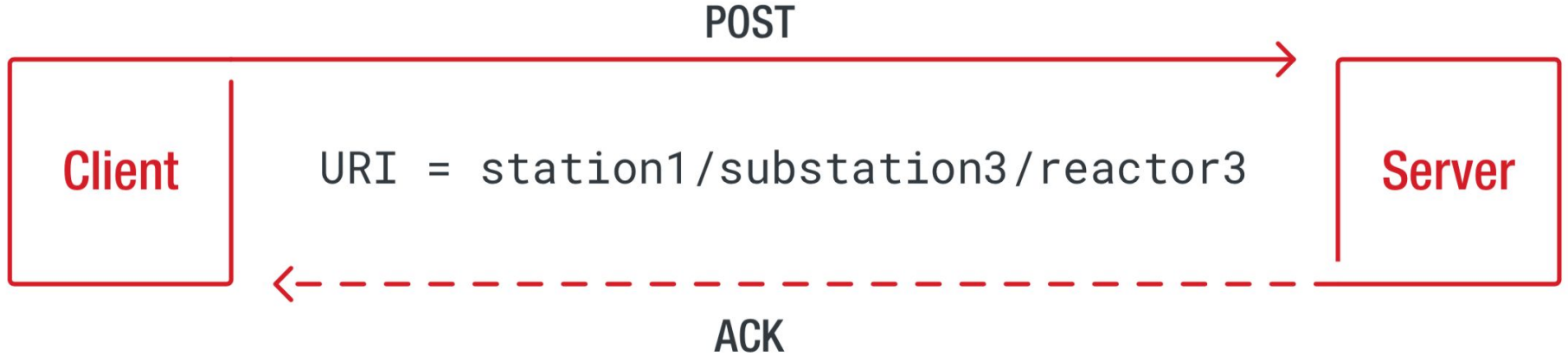


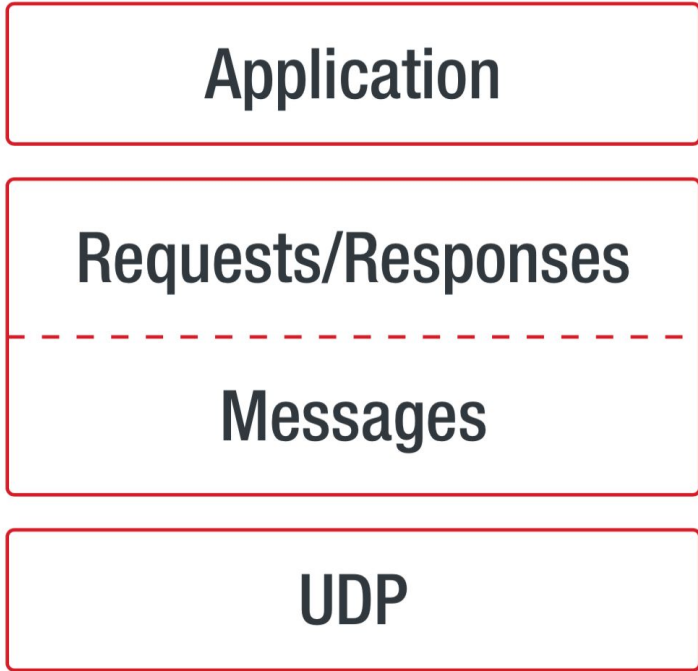
MQTT



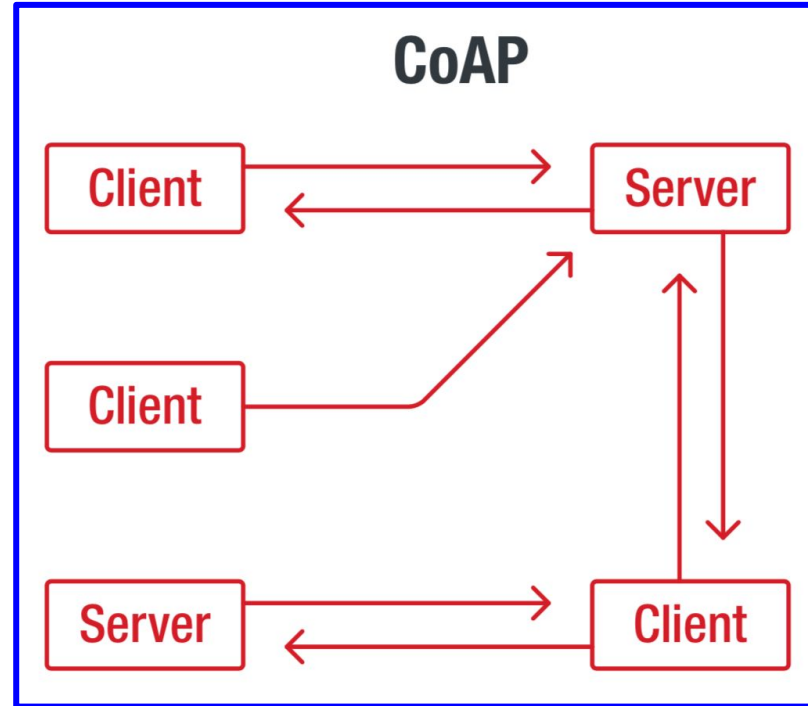
CoAP







CoAP



MQTT is popular
(and CoAP is gaining
a lot of traction, too)

Repositories	12K
Code	587K
Commits	91K
Issues	30K
Topics	102
Wikis	4K
Users	75

12,763 repository results

Sort: Most stars

Languages	
JavaScript	2,301
Python	1,717
Java	1,676
C++	1,058
C	791
Go	417
C#	247
HTML	219
Shell	209

home-assistant/home-assistant Python ★ 13.4k
 Open-source home automation platform running on Python 3

python home-automation mqtt raspberry-pi

Updated 6 hours ago

cesanta/mongoose C ★ 4.4k
 Mongoose Embedded Web Server Library - Mongoose is more than an embedded webserver. It is a multi-protocol embedded n...

Updated 5 days ago

hybridgroup/gobot Go ★ 4k
 Golang framework for robotics, drones, and the Internet of Things (IoT)

go sphero arduino mqtt raspberry-pi

Apache-2.0 license Updated 12 days ago

PokemonGoF/PokemonGo-Bot Python ★ 3.6k
 The Pokemon Go Bot, baking with community.

pokestops pokemongof pokemongo-bot

MIT license Updated 28 days ago 5 issues need help

mqttjs/MQTT.js JavaScript ★ 3.1k
 The MQTT client for Node.js and the browser

mqtt mqtt-broker iavascript nodejs-librav

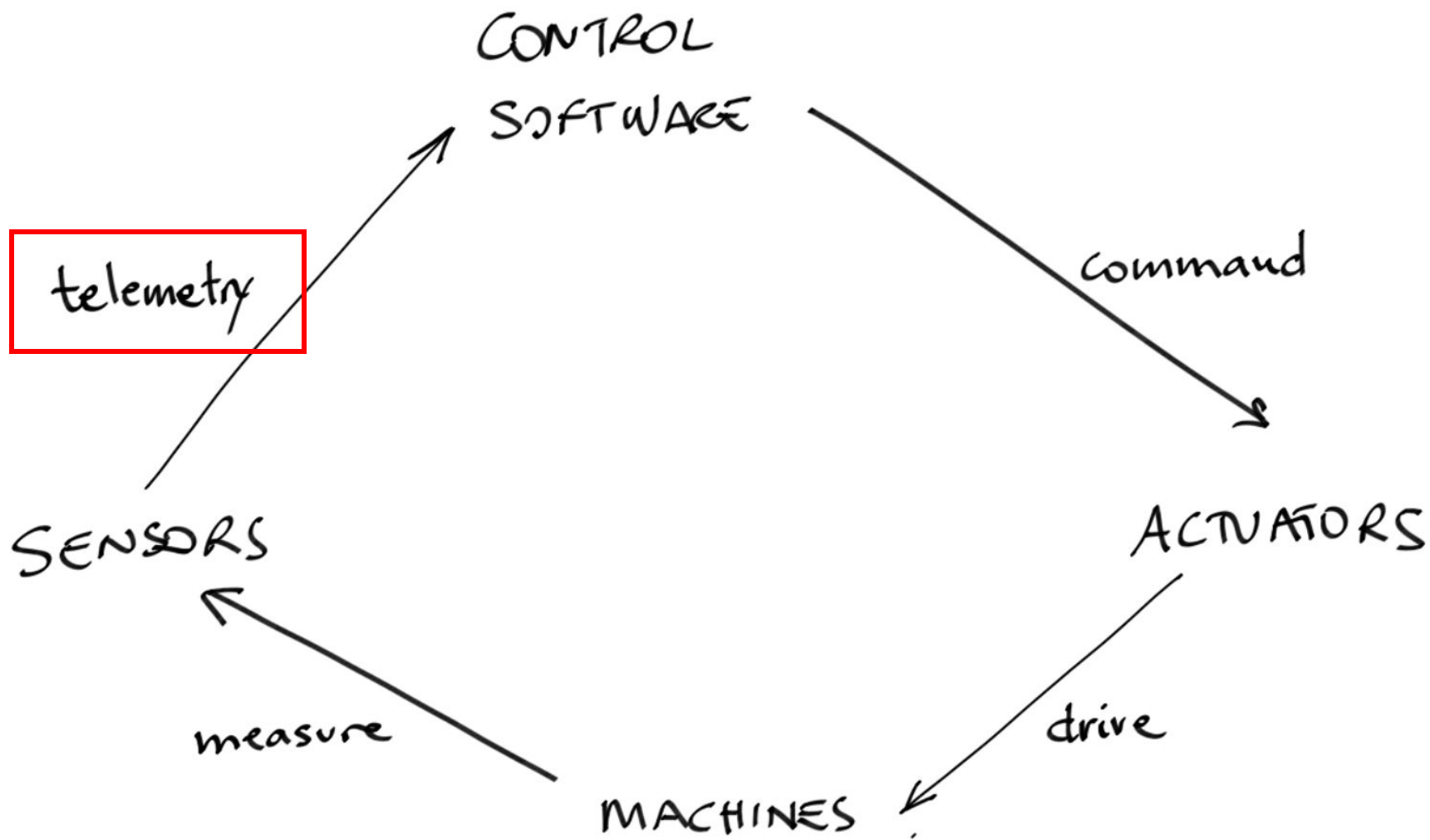
Advanced search Cheat sheet

Languages

JavaScript	2,301
Python	1,717
Java	1,676
C++	1,058
C	791
Go	417
C#	247
HTML	219
Shell	209

Applications

TELEMETRY

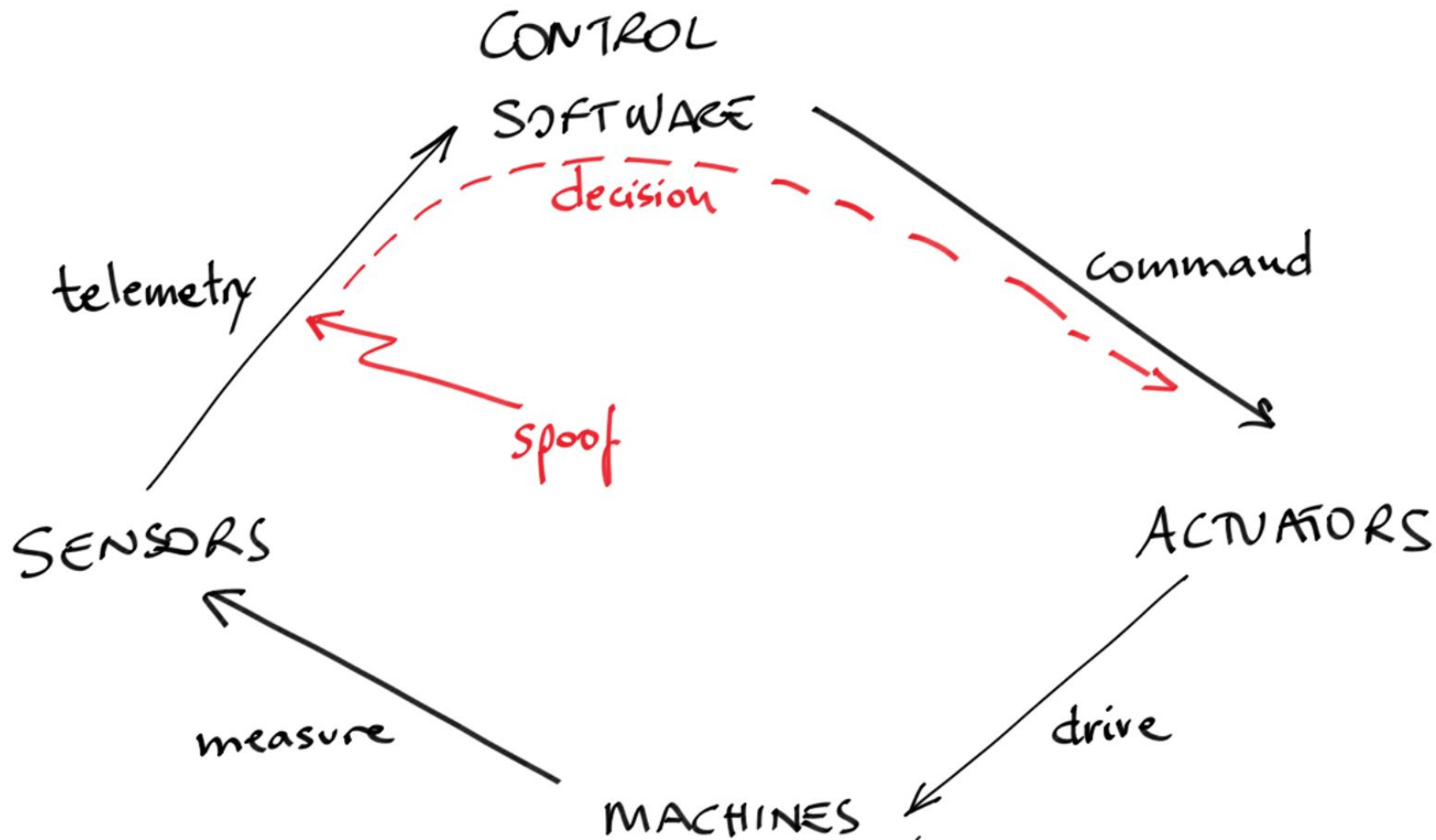


```
{
  "datetime": 1521823646233,
  "data": {
    "reactor": {
      "volume": 574.73,
      "temperature": { "jet": 27.6 },
      "slurry_depth": {
        "depth": 2.931, "pressure": 12.371
      },
    },
    "feeding": {
      "enabled": true, "status": false,
      "flow_rate": 0.346, "today": 0.02
    },
    "mixing": {
      "enabled": true, "status": false, "time": 600
    },
    "gas": {
      "height": 90.133,
      "analyser": {
        "CH4": [7.5, 10.1], "O2": [0, 0], "CO2": [0, 0], "H2S": [1425, 15]
      }
    }
  }
}
```



```
{
  "telemetryDataList": [{
    "date": "Mar 14, 2018 7:09:50 PM",
    "category": "main",
    "description": "InfoAxes Position Y",
    "deviceDescription": "CNC [red] [red]",
    "dataType": "NUMERIC",
    "devId": 7,
    "varId": 40,
    "value": 0.0,
    "quality": true
  }, {
    "date": "Mar 14, 2018 7:09:50 PM",
    "category": "main",
    "description": "InfoAxes Position Z",
    "deviceDescription": "CNC [red] [red]",
    "dataType": "NUMERIC",
    "devId": 7,
    "varId": 42,
    "value": 0.0,
    "quality": true
  }, {
    "date": "Mar 14, 2018 7:09:50 PM",
    "category": "main",
    "description": "InfoAxes Position X",
    "deviceDescription": "CNC [red] [red]",
    "dataType": "NUMERIC",
    "devId": 7,
    "varId": 38,
    "value": 0.0,
    "quality": true
  }, {
```

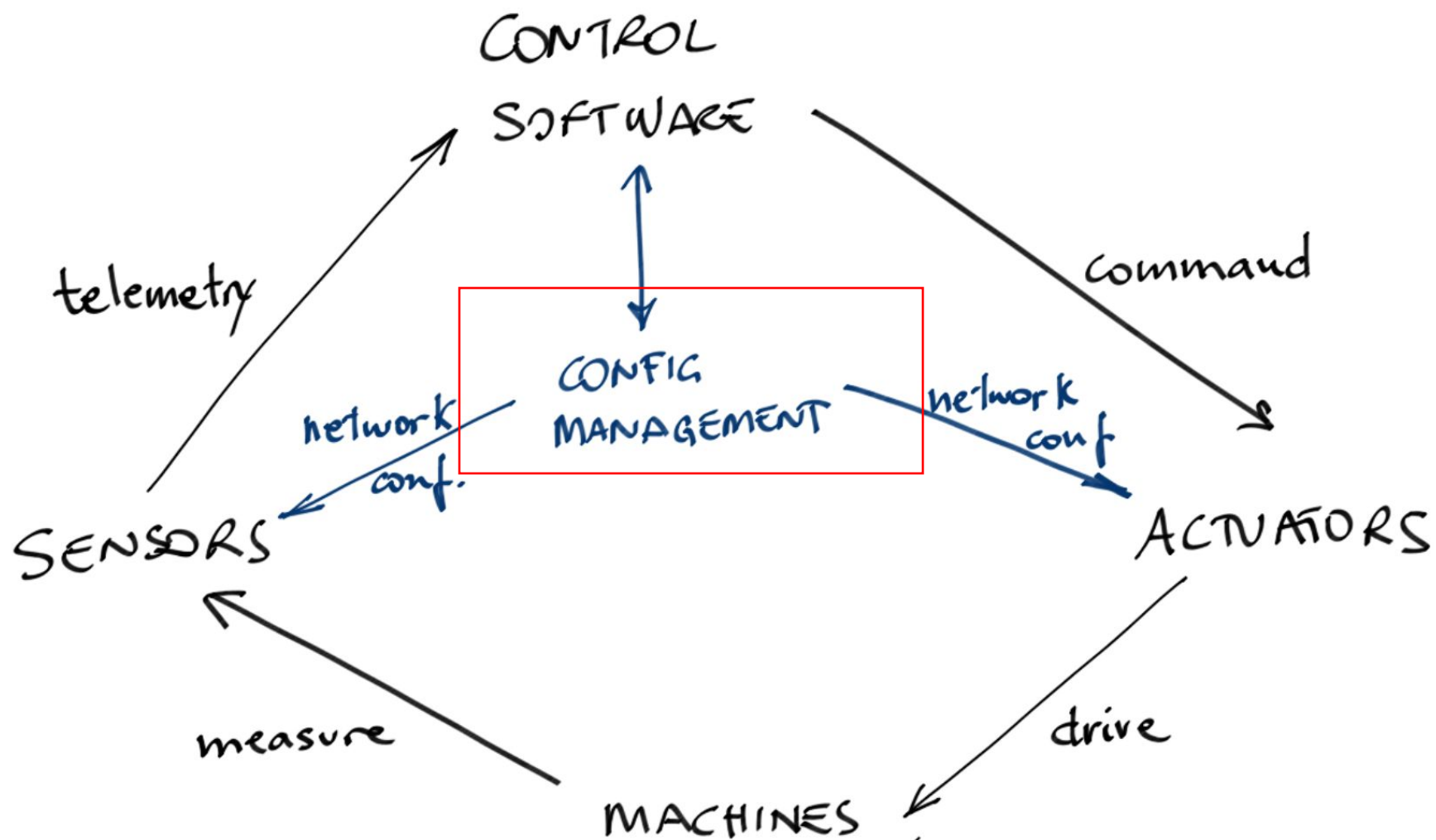
```
gazine":0,"t_name":2,"t_no":0,"t_place":2,"t_radius":0,"t_state":35,"t_type":5,"t_wear_length":0,"t_wear_radius":0},{"t_ST":0,"t_cutting_current":0,"t_cutting_time":0,"t_drilling_angle":0,"t_drilling_member":0,"t_length":-265,"t_magazine":0,"t_name":4,"t_no":6,"t_place":8,"t_radius":0,"t_state":83,"t_type":106,"t_wear_length":0,"t_wear_radius":0},{"t_ST":0,"t_cutting_current":10,"t_cutting_time":0,"t_drilling_angle":0,"t_drilling_member":0,"t_length":0,"t_magazine":0,"t_name":3,"t_no":2,"t_place":8,"t_radius":0,"t_state":80,"t_type":88,"t_wear_length":0,"t_wear_radius":0},{"t_ST":0,"t_cutting_current":2,"t_cutting_time":0,"t_drilling_angle":0,"t_drilling_member":0,"t_length":0,"t_magazine":0,"t_name":4,"t_no":4,"t_place":9,"t_radius":0,"t_state":74,"t_type":109,"t_wear_length":0,"t_wear_radius":0},{"t_ST":0,"t_cutting_current":33,"t_cutting_time":0,"t_drilling_angle":0,"t_drilling_member":0,"t_length":0,"t_magazine":0,"t_name":9,"t_no":4,"t_place":6,"t_radius":0,"t_state":103,"t_type":53,"t_wear_length":0,"t_wear_radius":0},{"t_ST":0,"t_cutting_current":4,"t_cutting_time":0,"t_drilling_angle":0,"t_drilling_member":0,"t_length":0,"t_magazine":0,"t_name":6,"t_no":0,"t_place":10,"t_radius":0,"t_state":62,"t_type":73,"t_wear_length":0,"t_wear_radius":0},{"t_ST":0,"t_cutting_current":18,"t_cutting_time":0,"t_drilling_angle":0,"t_drilling_member":0,"t_length":0,"t_magazine":0,"t_name":2,"t_no":7,"t_place":1,"t_radius":0,"t_state":35,"t_type":52,"t_wear_length":0,"t_wear_radius":0},{"t_ST":0,"t_cutting_current":174,"t_cutting_time":0,"t_drilling_angle":0,"t_drilling_member":0,"t_length":0,"t_magazine":0,"t_name":3,"t_no":6,"t_place":8,"t_radius":0,"t_state":73,"t_type":24,"t_wear_length":0,"t_wear_radius":0},{"t_ST":0,"t_cutting_current":11,"t_cutting_time":0,"t_drilling_angle":0,"t_drilling_member":0,"t_length":0,"t_magazine":0,"t_name":1,"t_no":13,"t_place":11,"t_radius":0,"t_state":63,"t_type":101,"t_wear_length":0,"t_wear_radius":0},{"t_ST":0,"t_cutting_current":190,"t_cutting_time":0,"t_drilling_angle":0,"t_drilling_member":0,"t_length":0,"t_magazine":0,"t_name":8,"t_no":12,"t_place":16,"t_radius":0,"t_state":2,"t_type":73,"t_wear_length":0,"t_wear_radius":0},{"t_ST":0,"t_cutting_current":7,"t_cutting_time":0,"t_drilling_angle":0,"t_drilling_member":0,"t_length":-201,"t_magazine":0,"t_name":2,"t_no":12,"t_place":1,"t_radius":0,"t_state":78,"t_type":74,"t_wear_length":0,"t_wear_radius":0},{"t_ST":0,"t_cutting_current":0,"t_cutting_time":0,"t_drilling_angle":0,"t_drilling_member":0,"t_length":0,"t_magazine":0,"t_name":3,"t_no":18,"t_place":16,"t_radius":0,"t_state":127,"t_type":39,"t_wear_length":0,"t_wear_radius":0},{"t_ST":0,"t_cutting_current":0,"t_cutting_time":0,"t_drilling_angle":0,"t_drilling_member":0,"t_length":0,"t_magazine":0,"t_name":1,"t_no":7,"t_place":3,"t_radius":0,"t_state":106,"t_type":56,"t_wear_length":0,"t_wear_radius":0},{"t_ST":0,"t_cutting_current":0,"t_cutting_time":0,"t_drilling_angle":0,"t_drilling_member":0,"t_length":-181,"t_magazine":0,"t_name":1,"t_no":14,"t_place":10,"t_radius":0,"t_state":40,"t_type":13,"t_wear_length":0,"t_wear_radius":0}]],"rt":["workssys.r.mt-mitsubishi"],"timestamp":"2017-08-17T15:03:16.255+08:00"}
```



Applications

DEVICE

MANAGEMENT



Resources in [coap://192.168.245.105/well-known/core](https://192.168.245.105/well-known/core)

href	title
------	-------

Request Resource	coap://192.168.245.105/well-known/core/request
WLAN Resource	coap://192.168.245.105/well-known/core/wlan
Success Resource	coap://192.168.245.105/well-known/core/success
ACK Resource	coap://192.168.245.105/well-known/core/ack
SHOW Resource	coap://192.168.245.105/well-known/core/show
Regist Resource	coap://192.168.245.105/well-known/core/regist
Resource	coap://192.168.245.105/well-known/core

[/well-known/core](#)

[coap://192.168.245.105/well-known/core/basic](#)

[coap://192.168.245.105/well-known/core/basic/regist](#)

should post example:{"deviceId"

[coap://192.168.245.105/well-known/core/basic/regist/ack](#)

[coap://192.168.245.105/well-known/core/basic/regist/ack](#)

[coap://192.168.245.105/well-known/core/basic/regist/ack](#)

```
userIp:null
SUCCESS_RESP:
userDevices:
toLinkDevices:
```

[coap://192.168.245.105/well-known/core/basic/regist](#)

should post example:{"device

[coap://192.168.245.105/well-known/core/basic/regist/ack](#)

[coap://192.168.245.105/well-known/core/basic/regist/ack](#)

[coap://192.168.245.105/well-known/core/basic/regist/ack](#)

```
userIp:null
SUCCESS_RESP:
userDevices:
toLinkDevices:
```

[coap://192.168.245.105/well-known/core/basic/regist/ack](#)

should post example:{"passwo

[coap://192.168.245.105/well-known/core/basic/regist/ack](#)

192.168.1.1

[coap://192.168.245.105/well-known/core/basic/regist/ack](#)

[coap://192.168.245.105/well-known/core/basic/regist/ack](#)

should post example:{"password": " ", "encrypt": "MIXED-WPAPSK2", "SSID": " "}

TOTAL RESULTS

515,459

TOP COUNTRIES



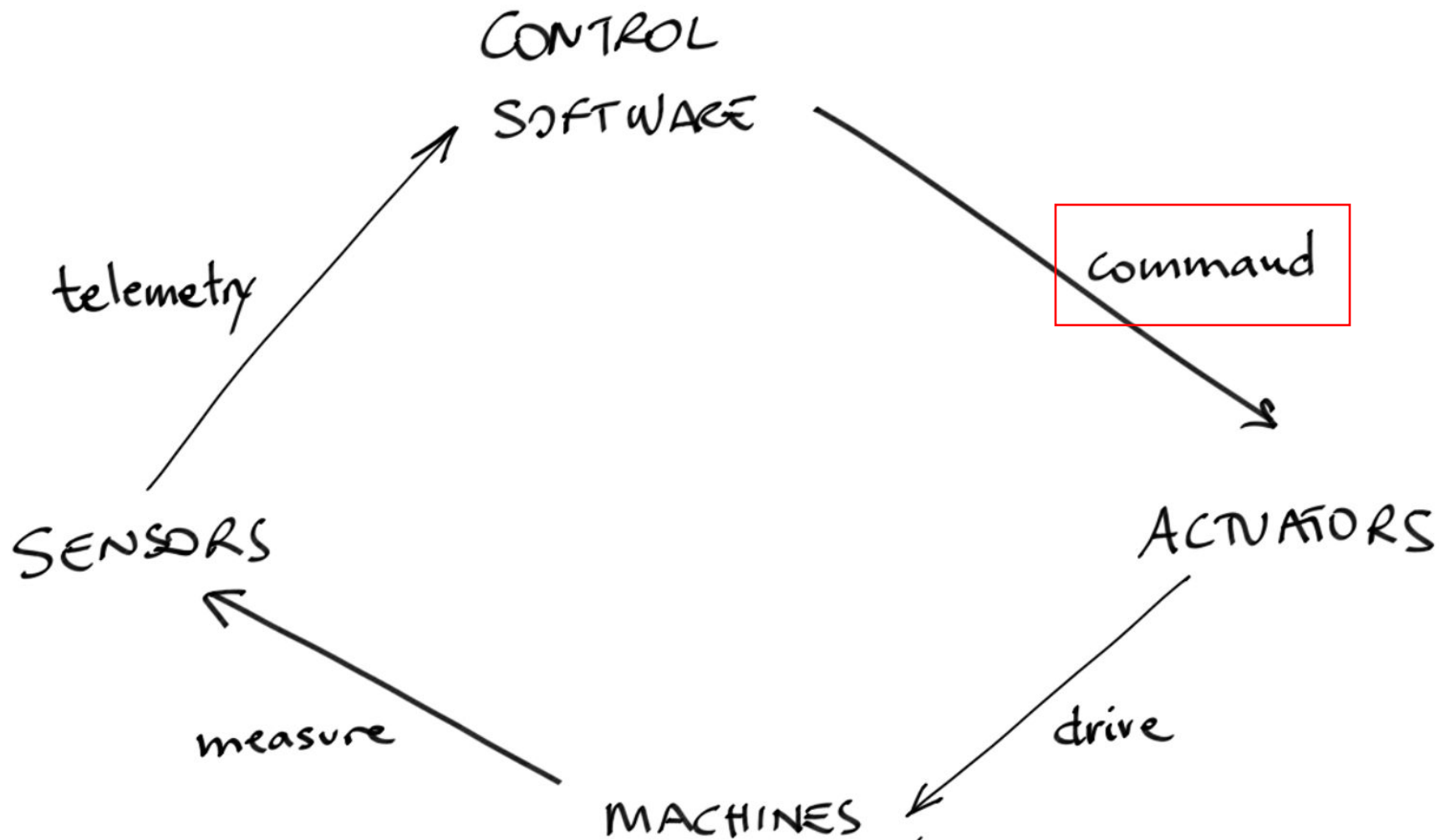
China

515,459

[token: 4]

Applications

COMMAND QUEUEING





福田口岸 071

```
{
  "_index": 979,
  "user": "shnett",
  "project": "express-box", "station": "shenzhen",
  "stationName": "深圳站点",
  "equipment": "[-redacted]-box-1", "equipmentName": "讯美柜组格口-1",
  "command": "open-door", "commandName": "开柜门",
  "trigger": "user", "phase": "executing",
  "operator": "shnett", "operatorName": "shnett", "_id": "[-redacted]60b2b9a77d1",
  "startTime": "2018-03-24T03:53:32.490Z",
  "parameters": [{
    "key": "value",
    "value": null, "_id": "[-redacted]60b2b9a77d6"
  }, {
    "key": "opentype",
    "value": "0", "_id": "[-redacted]60b2b9a77d5"
  }, {
    "key": "orderid", "_id": "[-redacted]60b2b9a77d4"
  }, {
    "key": "ordertype",
    "value": "[-redacted]", "_id": "[-redacted]60b2b9a77d3"
  }, {
    "key": "opener",
    "value": "ppz-1[-redacted]", "_id": "[-redacted]60b2b9a77d2"
  }],
  "priority": 0, "phase": "executing"
}
```

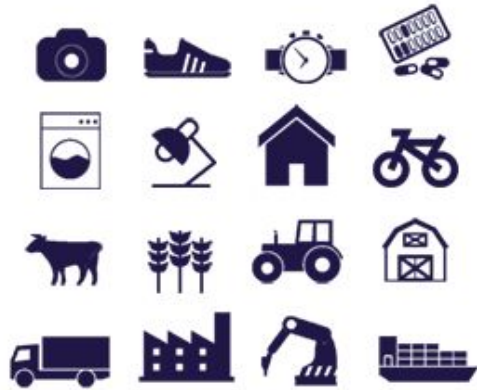
Dangerous Applications

Over The Air

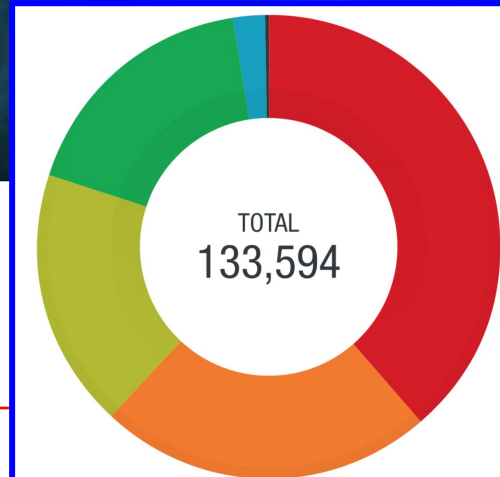
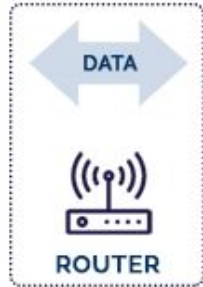
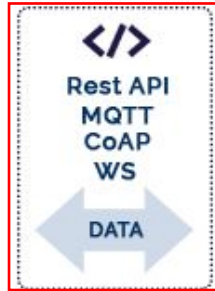
Firmware

Upgrades

Industrial IoT Products and Brands



**CONNECTED
DEVICES**



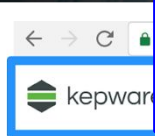
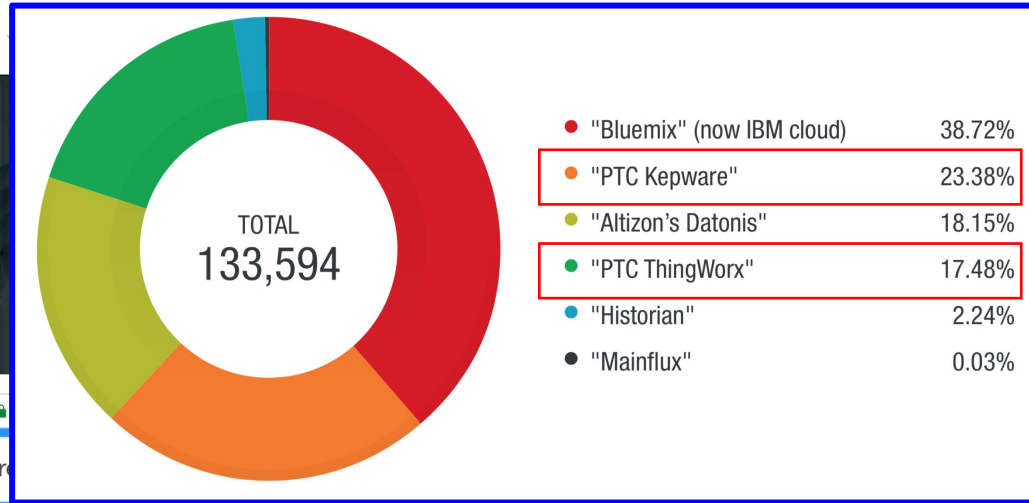
● "Bluemix" (now IBM cloud)	38.72%
● "PTC Kepware"	23.38%
● "Altizon's Datonis"	18.15%
● "PTC ThingWorx"	17.48%
● "Historian"	2.24%
● "Mainflux"	0.03%



Legacy Equipment, Meet IoT

Explore 3 ways to merge legacy equipment with modern assets.

[Learn More](#)



Features

KEPServerEX provides critical technical features that enable accessibility, aggregation, optimization, connectivity, security, and diagnostics. Expand the topics below to learn more about these features.

Explore the new features and enhancements that make **KEPServerEX Version 6** enterprise-ready and IoT-friendly.

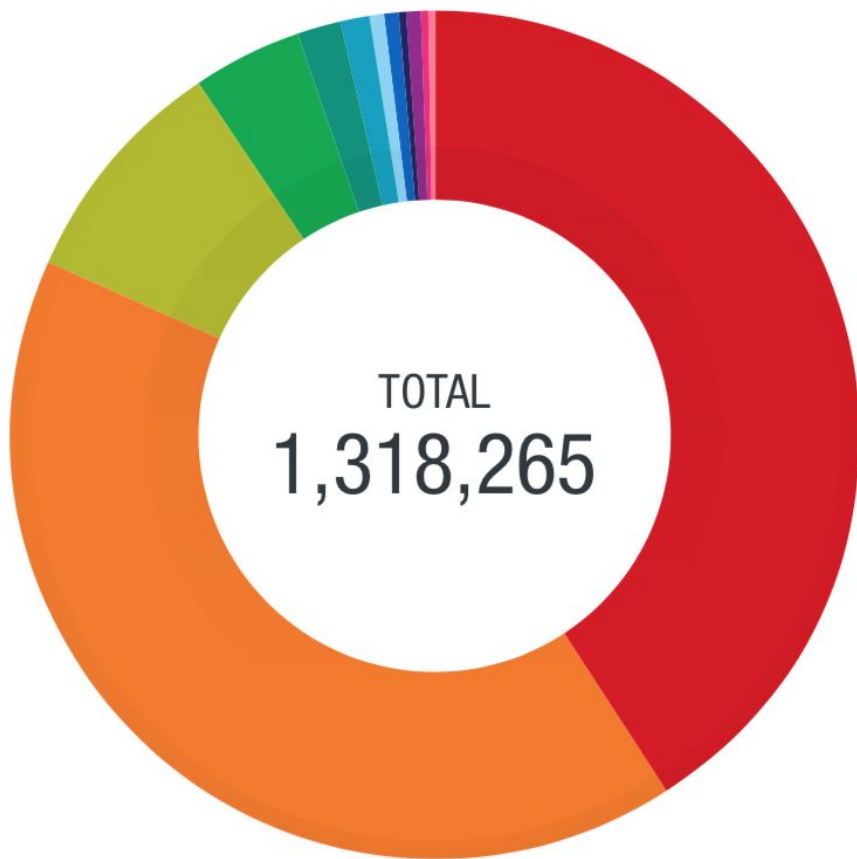
Accessibility

KEPServerEX provides data access for client applications (such as MES and SCADA) and IoT and Big Data analytics software via OPC, proprietary protocols (including GE NIO, SuiteLink/FastDDE, and Splunk), IT protocols (including MQTT, REST, ODBC, and SNMP), and flow measurement export to common Oil & Gas industry formats.

MQTT Industrial IoT Gateways

What's the most popular (field) protocol transported over MQTT?

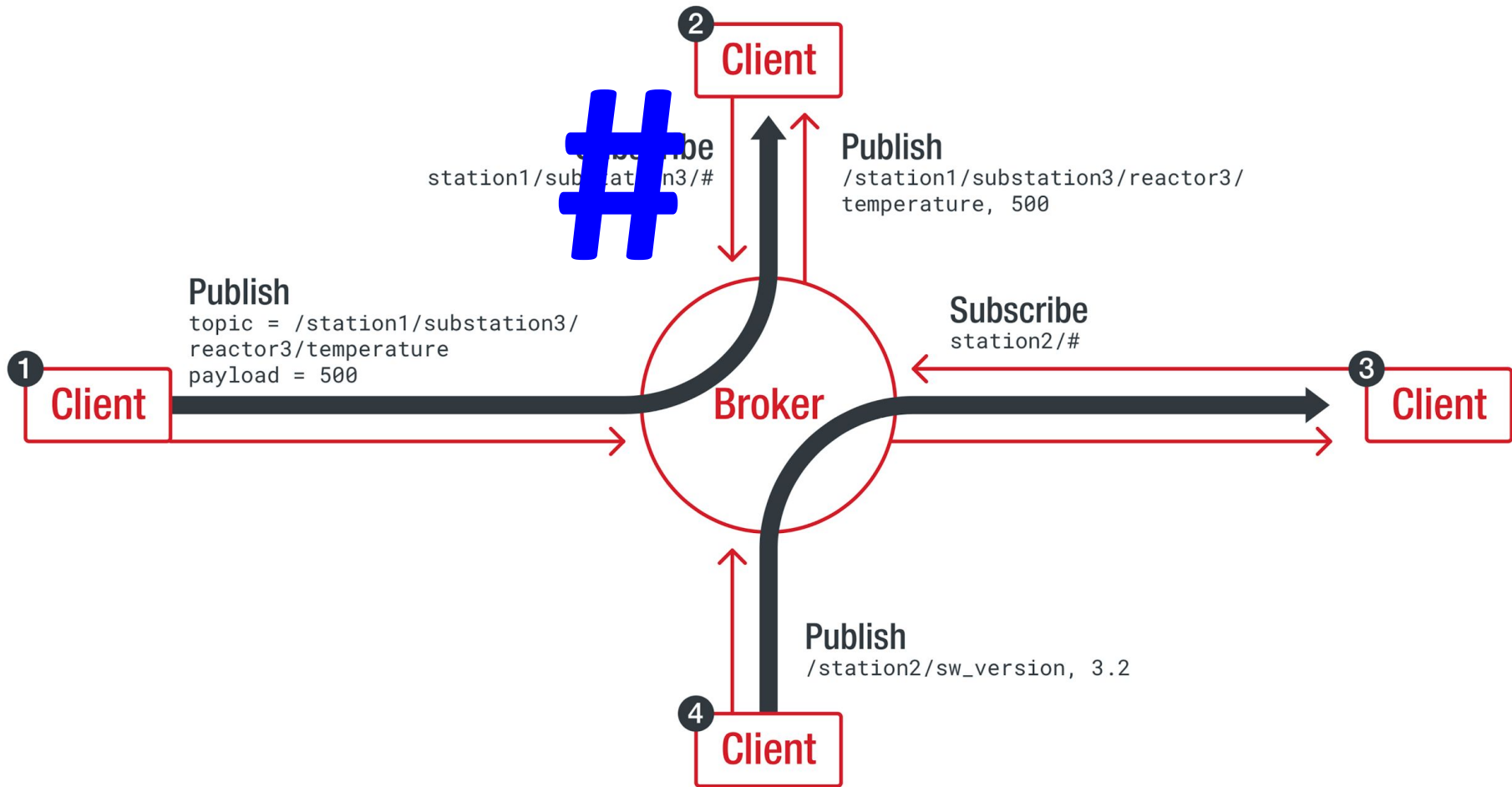




● "zwave"	40.96%
● "jsonrpc"	40.92%
● "knx"	8.81%
● "modbus"	4.15%
● "J1939"	1.57%
● "1wire"	1.17%
● "RS485"	0.6%
● "EtherCAT"	0.47%
● "insteon"	0.43%
● "enocean"	0.4%
● "RS232"	0.26%
● "profinet"	0.21%
● "bacnet"	0.05%

IoT & IIoT solutions
depend on
MQTT (and CoAP)

Problem 1





Scanning the entire internet. There is an increase..

Defcon24: Around 59.000

Blackhat 2017: Around 87.000

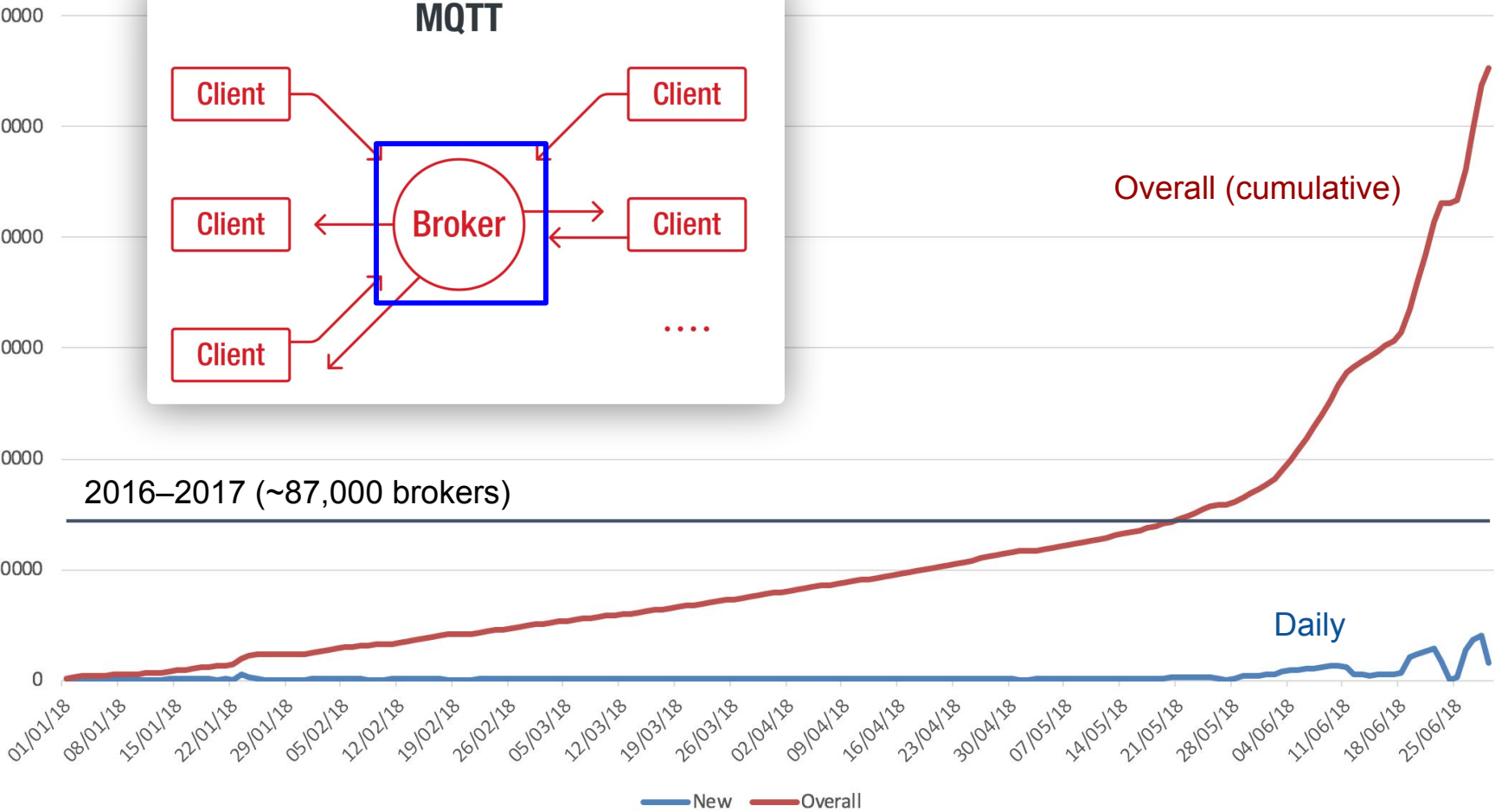
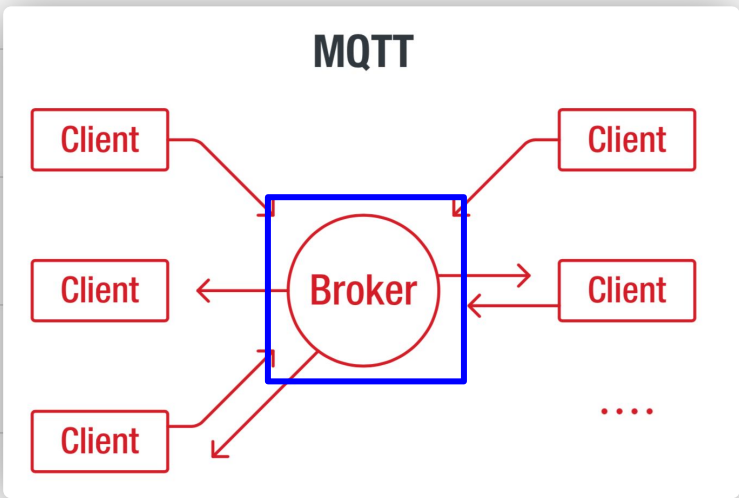
Then again; Robust increase, or more temporary devices available at that exact moment

2016–2017

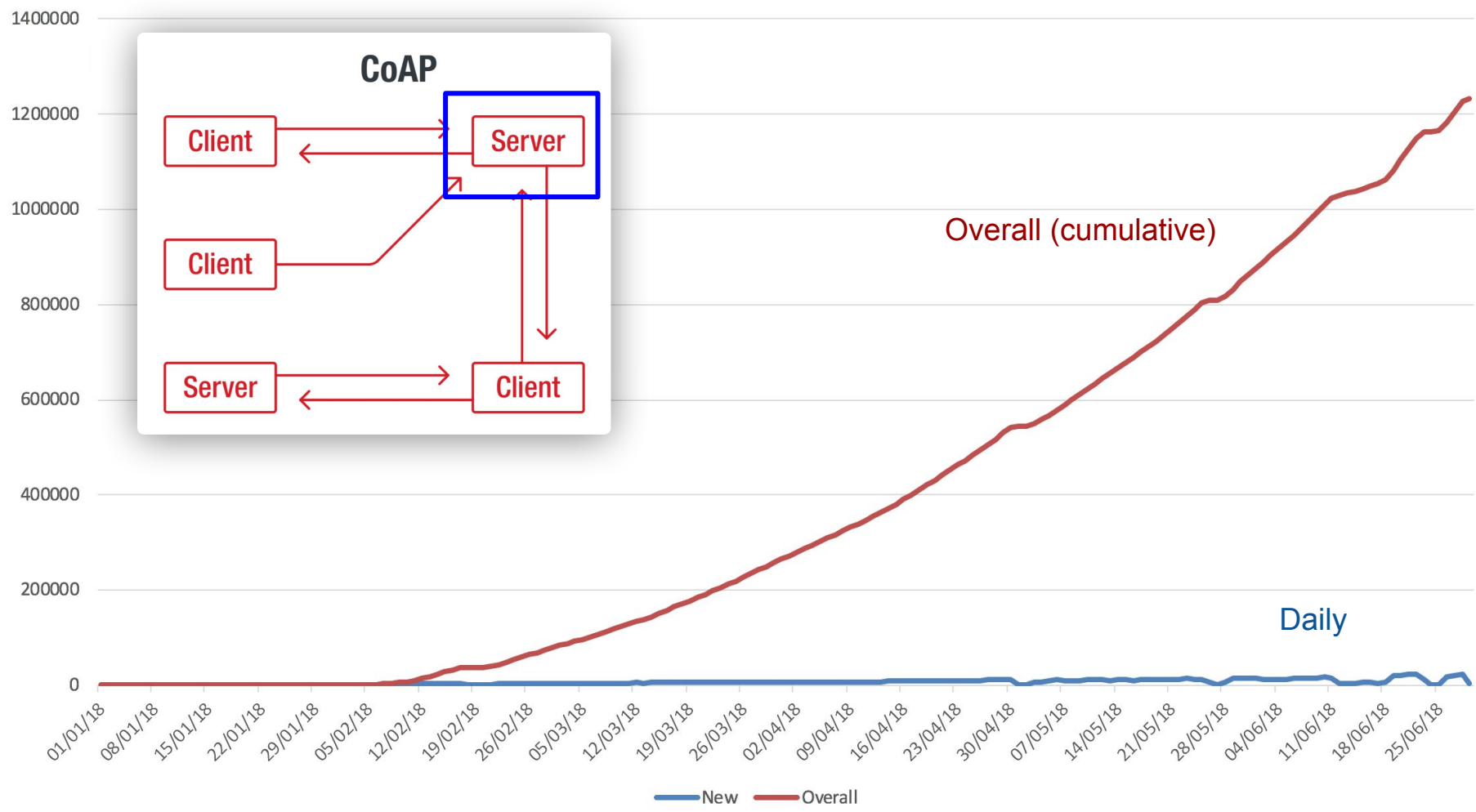
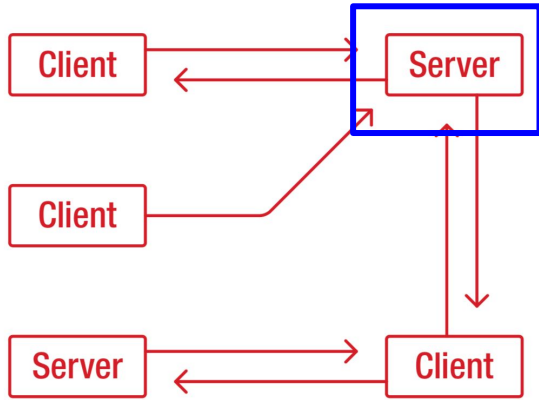


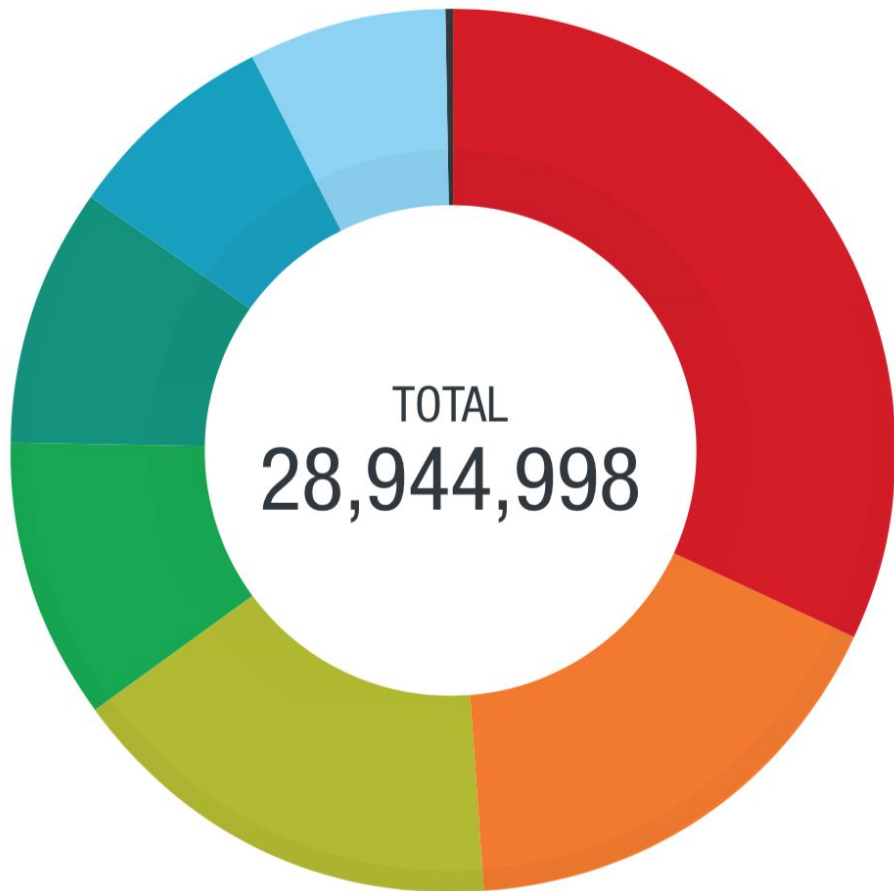
2018

MQTT public brokers



CoAP





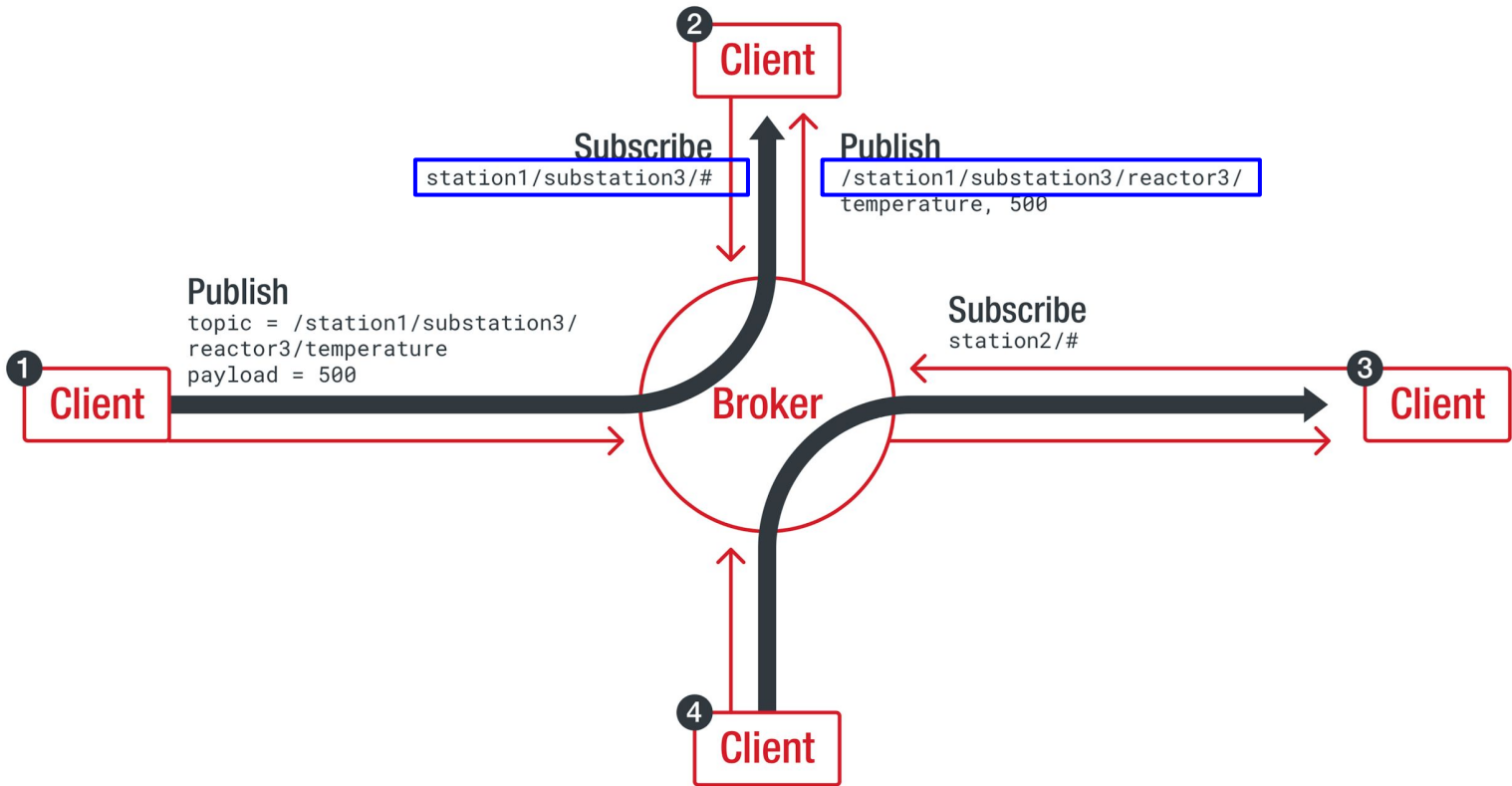
● Environment	9,290,248
● Positioning	4,906,998
● Energy	4,660,216
● Manufacturing	2,966,387
● Emergency	2,726,825
● Transportation	2,267,192
● Consumer	2,124,047
● Others	3,085
Industrial control systems	957
Ticketing	664
Communication System	648
Food	645
Agriculture	94
Healthcare	63
Healthcare	14

Is it just a
**deployment &
exposure**
problem?

Let's dig deeper
(Federico → Davide)

Problem 2

`/how/to/parse/topic/filters`



4.7 Topic Names and **Topic Filters**

4.7.1 Topic wildcards

The topic level separator is used to introduce structure into the Topic Name. If present, it divides t
A subscription's Topic Filter can contain special wildcard characters, which allow you to subscribe
The wildcard characters can be used in Topic Filters, but MUST NOT be used within a Topic Nam

4.7.1.1 Topic level separator

The forward slash ('/' U+002F) is used to separate each level within a topic tree and provide a hierarchical structure to the Topic Names. The Filters specified by subscribing Clients. Topic level separators can appear anywhere in a Topic Filter or Topic Name. Adjacent Topic level sep

4.7.1.2 Multi-level wildcard

The number sign ('#' U+0023) is a wildcard character that matches any number of levels within a topic. The multi-level wildcard represents th
following a topic level separator. In either case it MUST be the last character specified in the Topic Filter [MQTT-4.7.1-2].

Non normative comment

For example, if a Client subscribes to "sport/tennis/player1/#", it would receive messages published using these topic names:

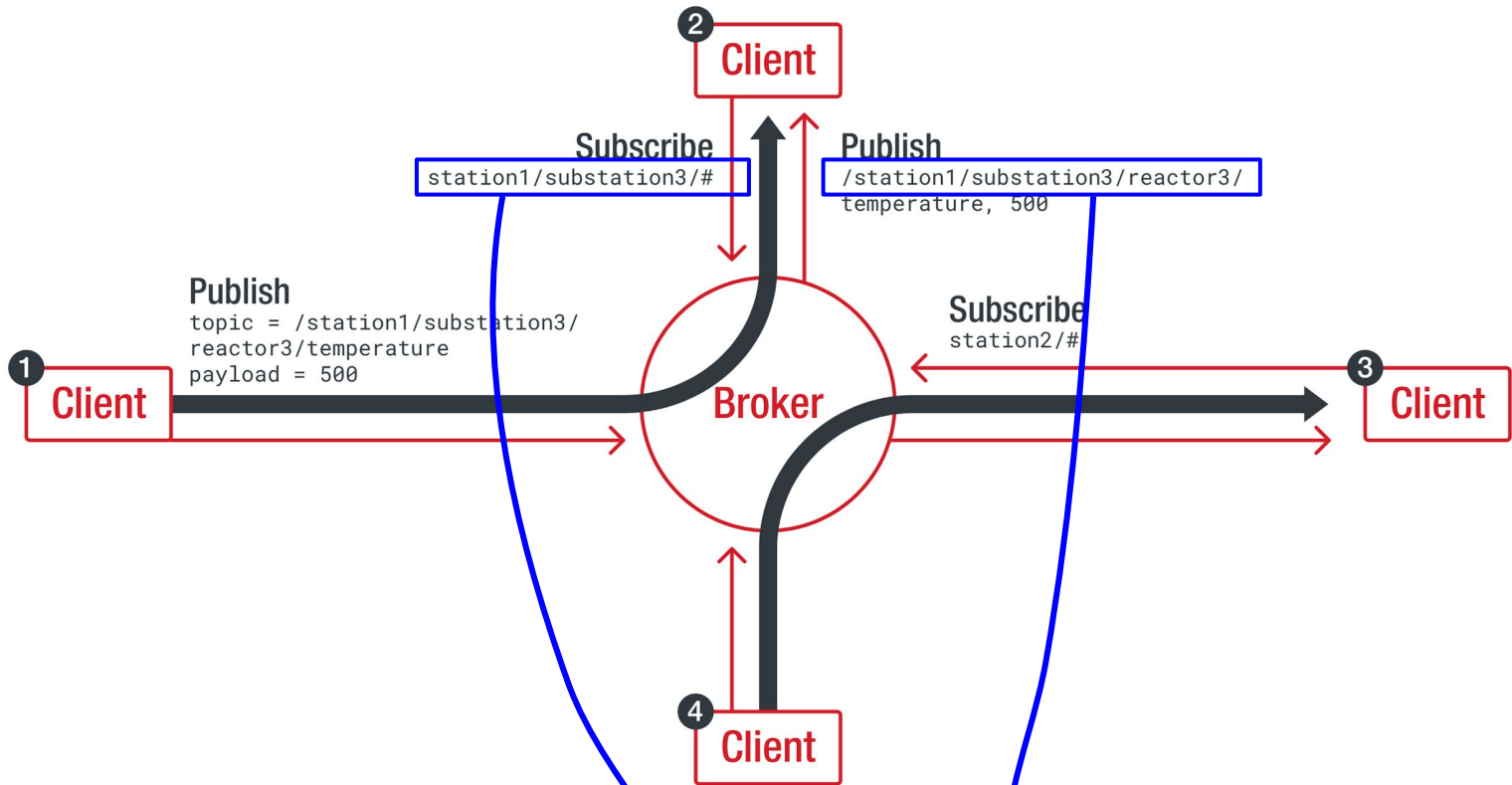
- "sport/tennis/player1"
- "sport/tennis/player1/ranking"
- "sport/tennis/player1/score/wimbledon"

Non normative comment

- "sport/#" also matches the singular "sport", since # includes the parent level.
- "# is valid and will receive every Application Message
- "sport/tennis/#" is valid
- "sport/tennis#" is not valid
- "sport/tennis/#/ranking" is not valid

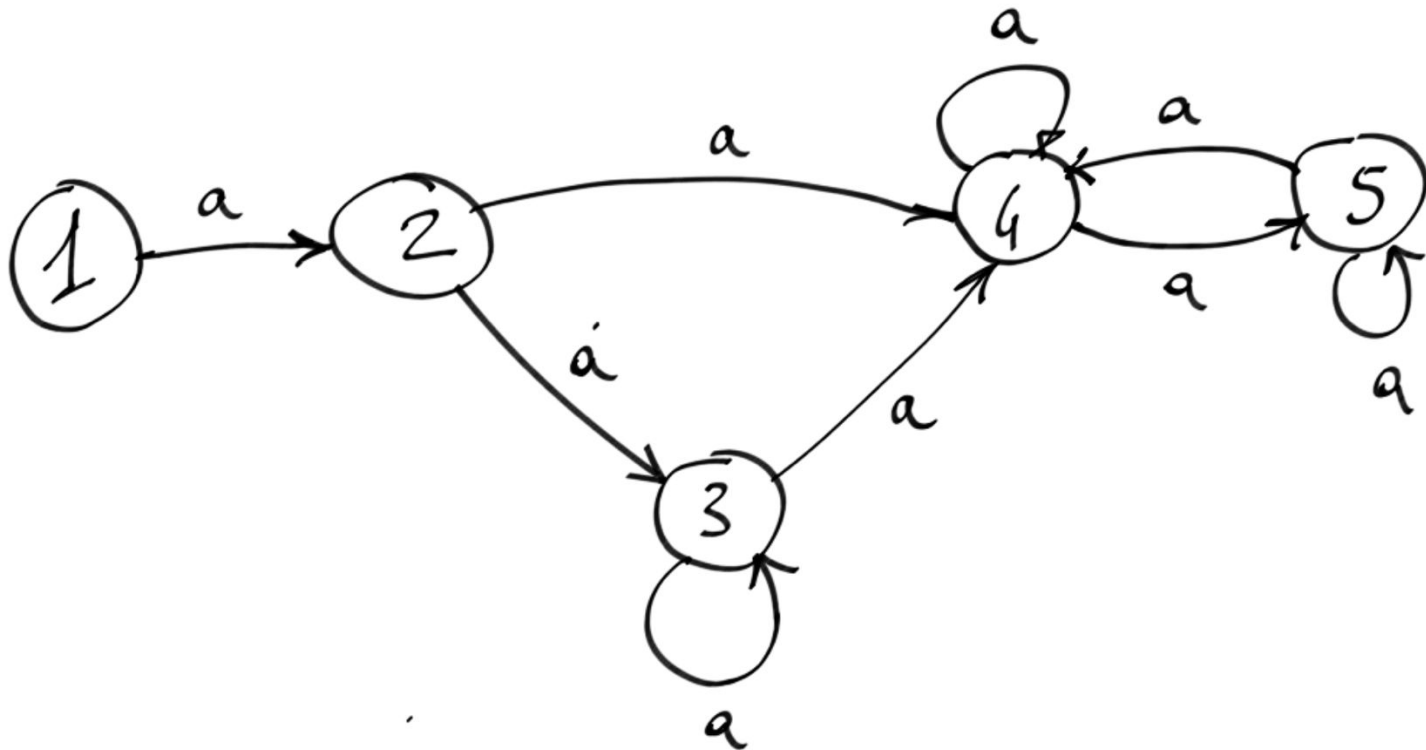
RegEx.match

/how/not/to/parse/topic/filters



RegEx.match

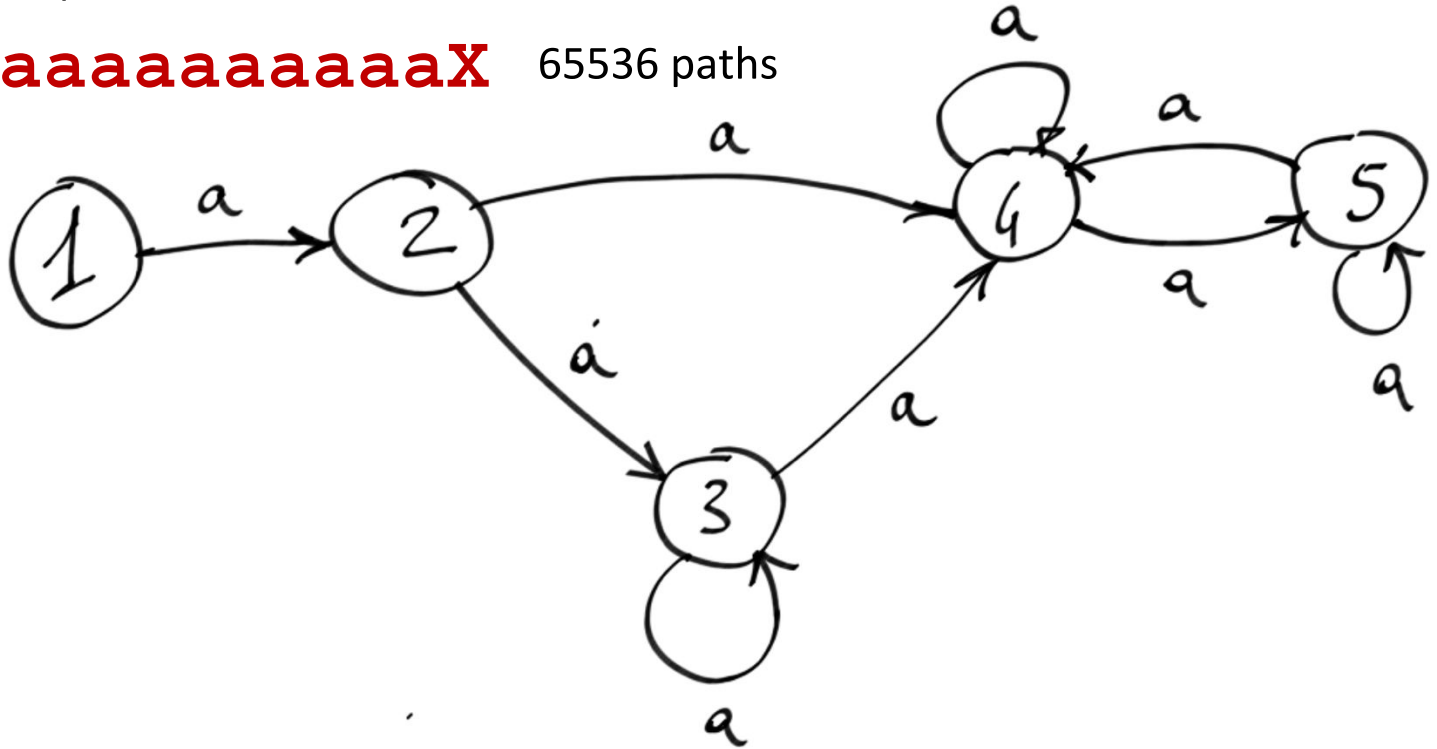
$^ (a+) + \$$



$^{\wedge}(a+) + \$$

aaaX 16 paths

aaaaaaaaaaaaaaaaaX 65536 paths



```
+` +, +: .+ .+ +; +; !+ !+ +` +`
+` +. +: ,+ `+ ++ +; !+ ;+ + +.
+` +. +: ,+ `+ + !+ + +.
+` +. +: ,+ `+ :+ !+ +++++.
+` +. +: ,+ `+ ++ !+ +++++.
+` +. +: ,+ `+ ++ !+ + +.
+` +. +: ,+ `+ ++: ++ !+ ;+ + +.
+` +. +: .+ .+ +; +; !+ !+ + +.
+` +. +: +++; ++ ++! ++ ++! + +.
+` +. +: +++ ++++ ++! ++! + +.
```

```
{"pid":1806,"hostname":"Eternia","name":"mosca","level":30,"time":1520280422157,"msg":"server started","mqtt":1883,"v":1}
subscriptionsoooooooooooooons
{"pid":1806,"hostname":"Eternia","name":"mosca","level":30,"time":1520280426231,"msg":"client connected","client":"hbmqt/G?8T7ysIvBNn_WxD","v":1}
{"pid":1806,"hostname":"Eternia","name":"mosca","level":30,"time":1520280426240,"msg":"subscribed to topic","topic":"^[
\u0000a-Z]*","qos":1,"client":"hbmqt/G?8T7ysIvBNn_WxD","v":1}
/home/ocean/projects/mqtt/servers/mosca/lib/persistence/mongo.js:271
  var regexp = new RegExp(pattern.replace(/(#!\+)/, ".+").replace('\ ', '\\\\'));
                ^
SyntaxError: Invalid regular expression: /^[
```

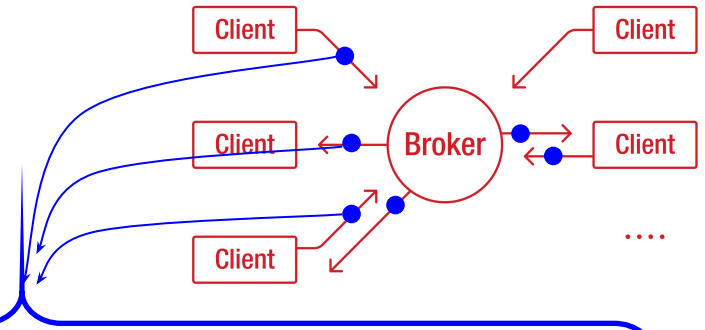
BONUS: Broker crash via malformed regex

[CVE-2018-11615](https://cve.circl.lu/entry/CVE-2018-11615)



PoC || GTFO

Problem 3



**Control
packet type
+ Flags**

**Remaining
length**

**Variable
length
header**

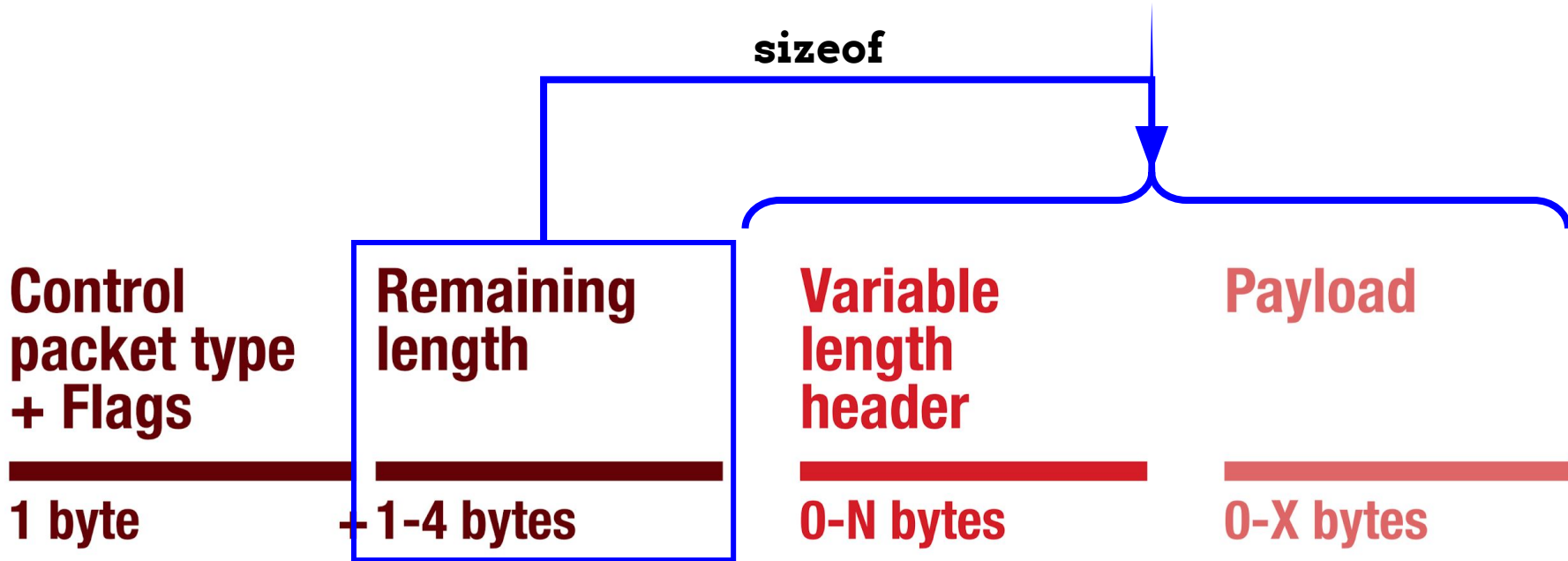
Payload

1 byte

+ 1-4 bytes

0-N bytes

0-X bytes



2.2.3 Remaining Length

Position: starts at byte 2.

The Remaining Length is the number of bytes remaining within the current packet, including data in the variable header and the payload. The Remaining Length does not include the bytes used to encode the Remaining Length.

The Remaining Length is encoded using a variable length encoding scheme which uses a single byte for values up to 127. Larger values are handled as follows. The least significant seven bits of each byte encode the data, and the most significant bit is used to indicate that there are following bytes in the representation. Thus each byte encodes 128 values and a "continuation bit". The maximum number of bytes in the Remaining Length field is four.

Non normative comment

For example, the number 64 decimal is encoded as a single byte, decimal value 64, hexadecimal 0x40. The number 321 decimal ($= 65 + 2 \cdot 128$) is encoded as two bytes, least significant first. The first byte is $65 + 128 = 193$. Note that the top bit is set to indicate at least one following byte. The second byte is 2.

Non normative comment

This allows applications to send Control Packets of size up to 268,435,455 (256 MB). The representation of this number on the wire is: 0xFF, 0xFF, 0xFF, 0x7F.

[Table 2.4](#) shows the Remaining Length values represented by increasing numbers of bytes.

```
multiplier = 1
value = 0
do
    digit = 'next digit from stream'
    value += (digit AND 127) * multiplier
    multiplier *= 128
while ((digit AND 128) != 0)
```

```
multiplier = 1
value = 0
do
    digit = 'next digit from stream'
    value += (digit AND 127) * multiplier
    multiplier *= 128
while ((digit AND 128) != 0)
```



```
multiplier = 1
value = 0
do
  digit = 'next digit from stream'
  value += (digit AND 127) * multiplier
  multiplier *= 128
while ((digit AND 128) != 0)
```



MQTT V3.1 Protocol Specification

Standard

```
multiplier = 1
value = 0
do
  digit = 'next digit from stream'
  value += (digit AND 127) * multiplier
  multiplier *= 128
while ((digit AND 128) != 0)
```

```
multiplier = 1
value = 0
do
  encodedByte = 'next byte from stream'
  value += (encodedByte AND 127) * multiplier
  multiplier *= 128
  if (multiplier > 128*128*128)
    throw Error(Malformed Remaining Length)
while ((encodedByte AND 128) != 0)
```

OASIS 

MQTT Version 3.1.1

Standard

```
multiplier = 1
```

```
multiplier = 1
```

```
value = 0
```

```
do
```

```
  encodedByte = 'next byte from stream'
```

```
  value += (encodedByte AND 127) * multiplier ) != 0)
```

```
  if (multiplier > 128*128*128)
```

```
    throw Error(Malformed Remaining Length)
```

```
  multiplier *= 128
```

```
while ((encodedByte AND 128) != 0)
```



MQTT Version 3.1.1 Errata 01

```
from stream'
```

```
127) * multiplier
```



MQTT V3.1 Protocol Specification

Standard

```
  encodedByte = 'next byte from stream'
```

```
  value += (encodedByte AND 127) * multiplier
```

```
  multiplier *= 128
```

```
  if (multiplier > 128*128*128)
```

```
    throw Error(Malformed Remaining Length)
```

```
while ((encodedByte AND 128) != 0)
```

From spec to code

```
242     do {
243         if(!readByte(&digit)) return 0;
244         buffer[len++] = digit;
245         length += (digit & 127) * multiplier;
246         multiplier *= 128;
247     } while ((digit & 128) != 0);
248     *lengthLength = len-1;
```



MQTT.ORG

Watch ▾

216

★ Star

1,726

Fork

773

THE IOT PLATFORM YOU CAN TRUST

"Adding GPS trackers to our expensive pro press systems allowed us to completely eliminate loss saving us close to \$20,000. We were also able to serve more customers in the process by keeping the pro presses in circulation."

[View Case Study >](#)

KEN MEYER
Vice President

C & D Mechanical, Inc.

"After testing many other products and not having much luck, I was very optimistic when I tried Losant. With no programming background I was still able to get our first job site connected and able to monitor the water main remotely. A big problem has been solved thanks to Losant."

[View Case Study >](#)

BOB GELETY
Lead Engineer



"We are thrilled by the results we have realized since beginning our work with Losant."

[View Case Study >](#)

KURT LARSON
Co-Founder & CTO



BOSCH



```
242     do {
243 +     if (len == 6) {
244 +         // Invalid remaining length encoding - kill the connection
245 +         _state = MQTT_DISCONNECTED;
246 +         _client->stop();
247 +         return 0;
248 +     }
249     if(!readByte(&digit)) return 0;
250     buffer[len++] = digit;
251     length += (digit & 127) * multiplier;
252     multiplier *= 128;
253 } while ((digit & 128) != 0);
254 *lengthLength = len-1;
```




ZERO DAY
INITIATIVE



 **MQTT**.ORG

 Watch ▾

216

 Star

1,726

Fork

773

Problem 4



MQTT Version 3.1.1

The character data in a UTF-8 encoded string MUST be well-formed UTF-8 as defined by the Unicode specification [Unicode] and restated in RFC 3629 [RFC3629]. In particular this data MUST NOT include encodings of code points between U+D800 and U+DFFF. If a Server or Client receives a Control Packet containing ill-formed UTF-8 it MUST close the Network Connection [MQTT-1.5.3-1].

A UTF-8 encoded string MUST NOT include an encoding of the null character U+0000. If a receiver (Server or Client) receives a Control Packet containing U+0000 it MUST close the Network Connection [MQTT-1.5.3-2].

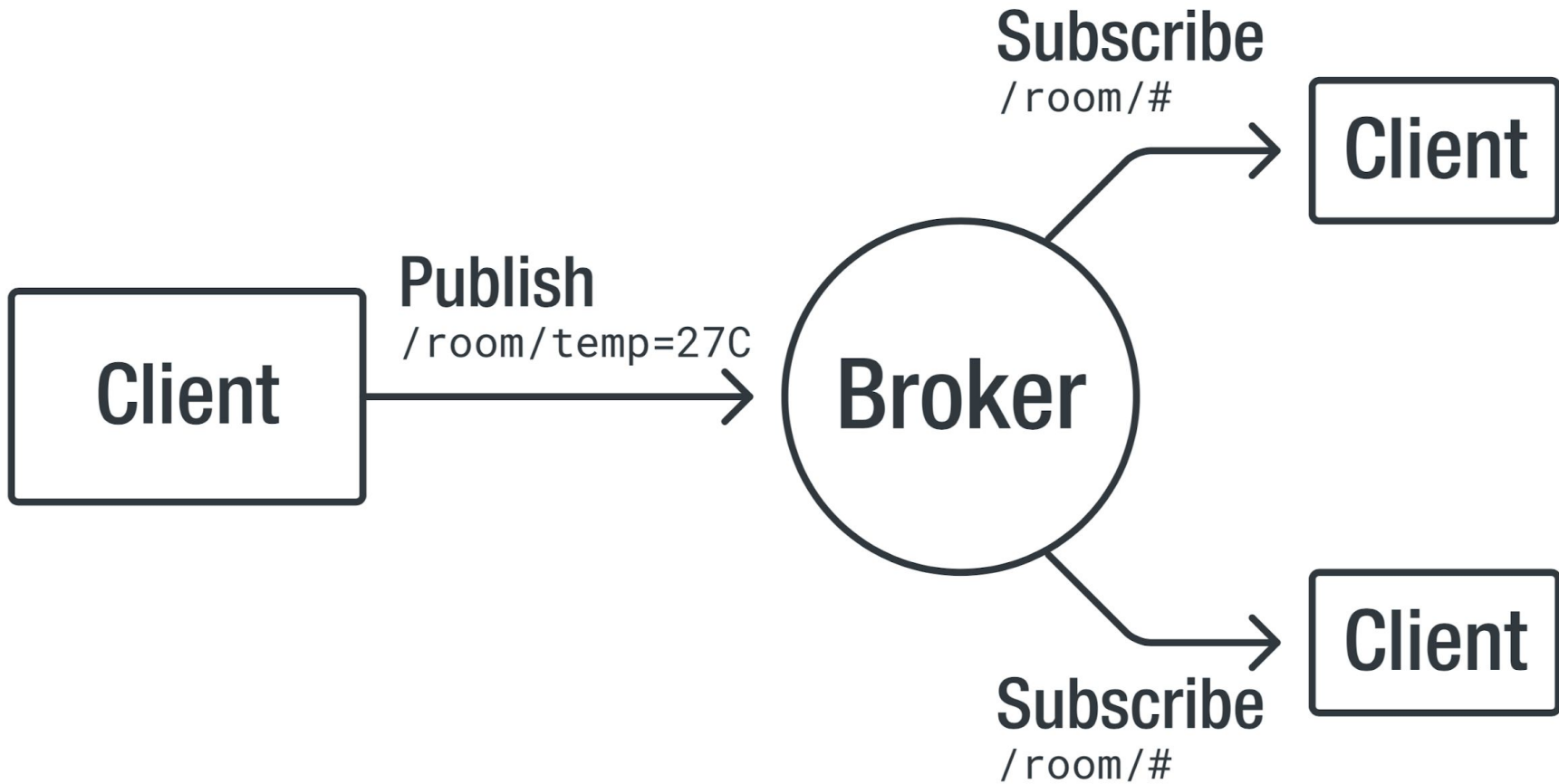
The data SHOULD NOT include encodings of the Unicode [Unicode] code points listed below. If a receiver (Server or Client) receives a Control Packet containing any of them it MAY close the Network Connection:

U+0001..U+001F control characters

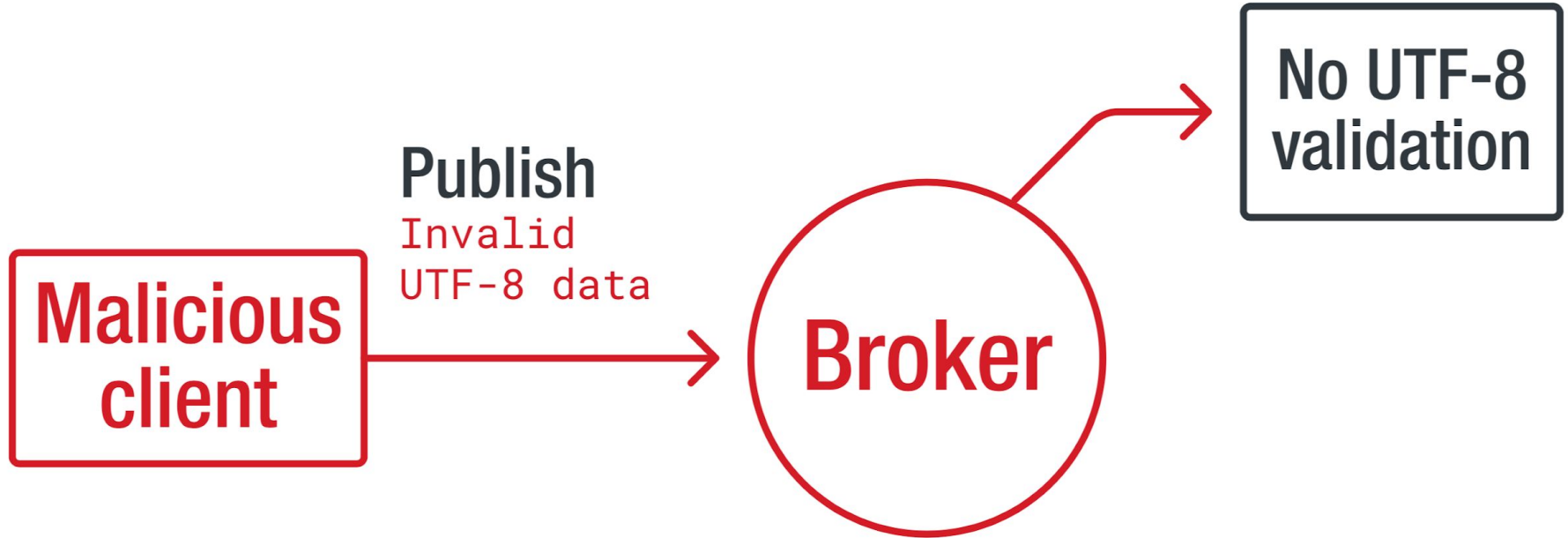
U+007F..U+009F control characters

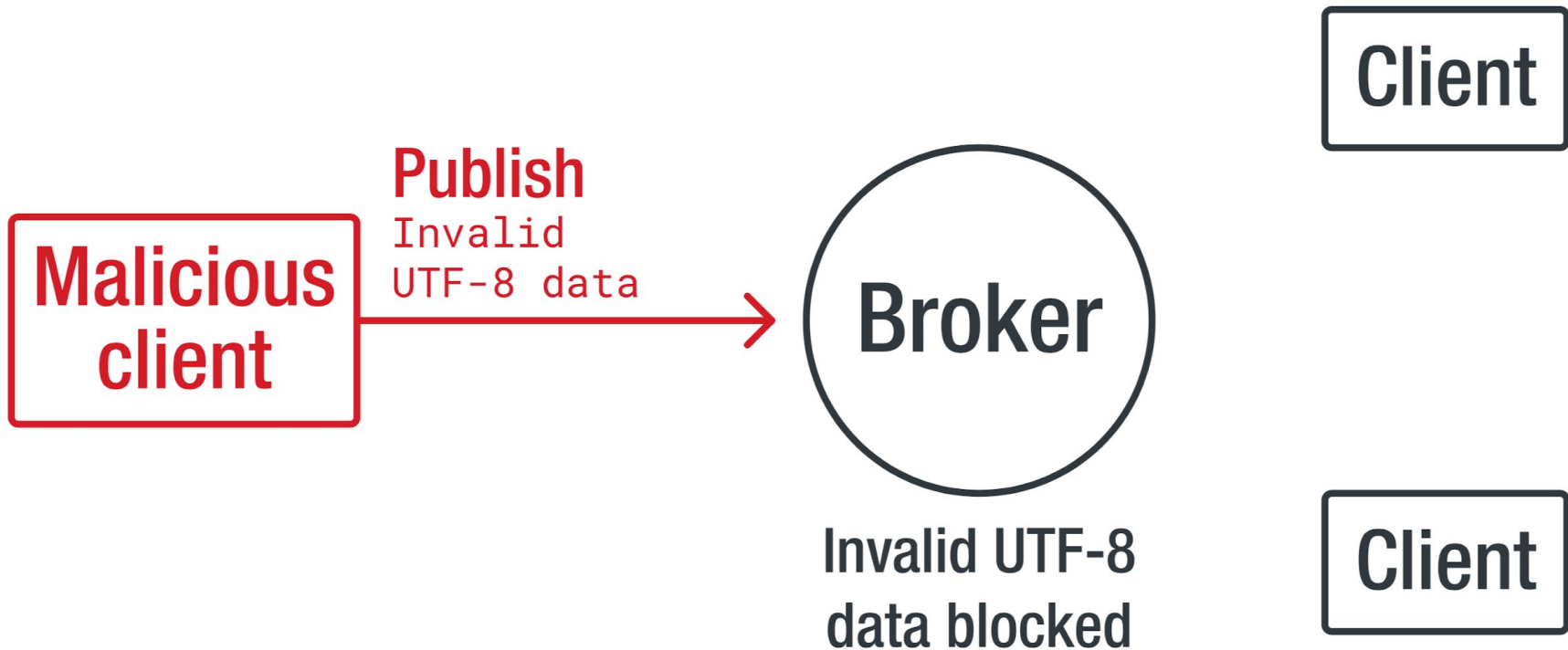
Code points defined in the Unicode specification [Unicode] to be non-characters (for example U+0FFFF)

A UTF-8 encoded sequence 0xEF 0xBB 0xBF is always to be interpreted to mean U+FEFF ("ZERO WIDTH NO-BREAK SPACE") wherever it appears in a string and MUST NOT be skipped over or stripped off by a packet receiver [MQTT-1.5.3-3].

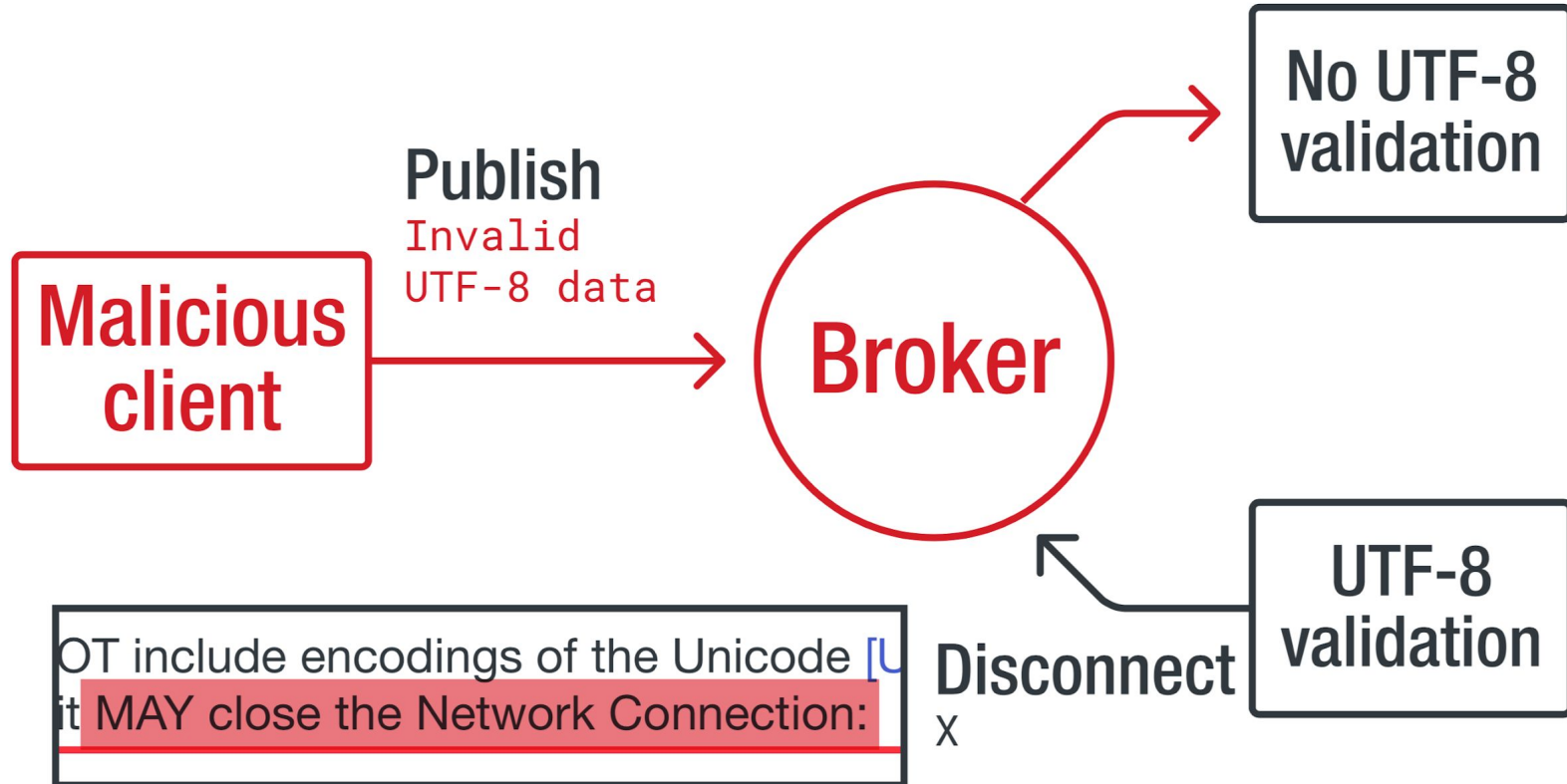


Both Broker and Client Don't Validate UTF-8

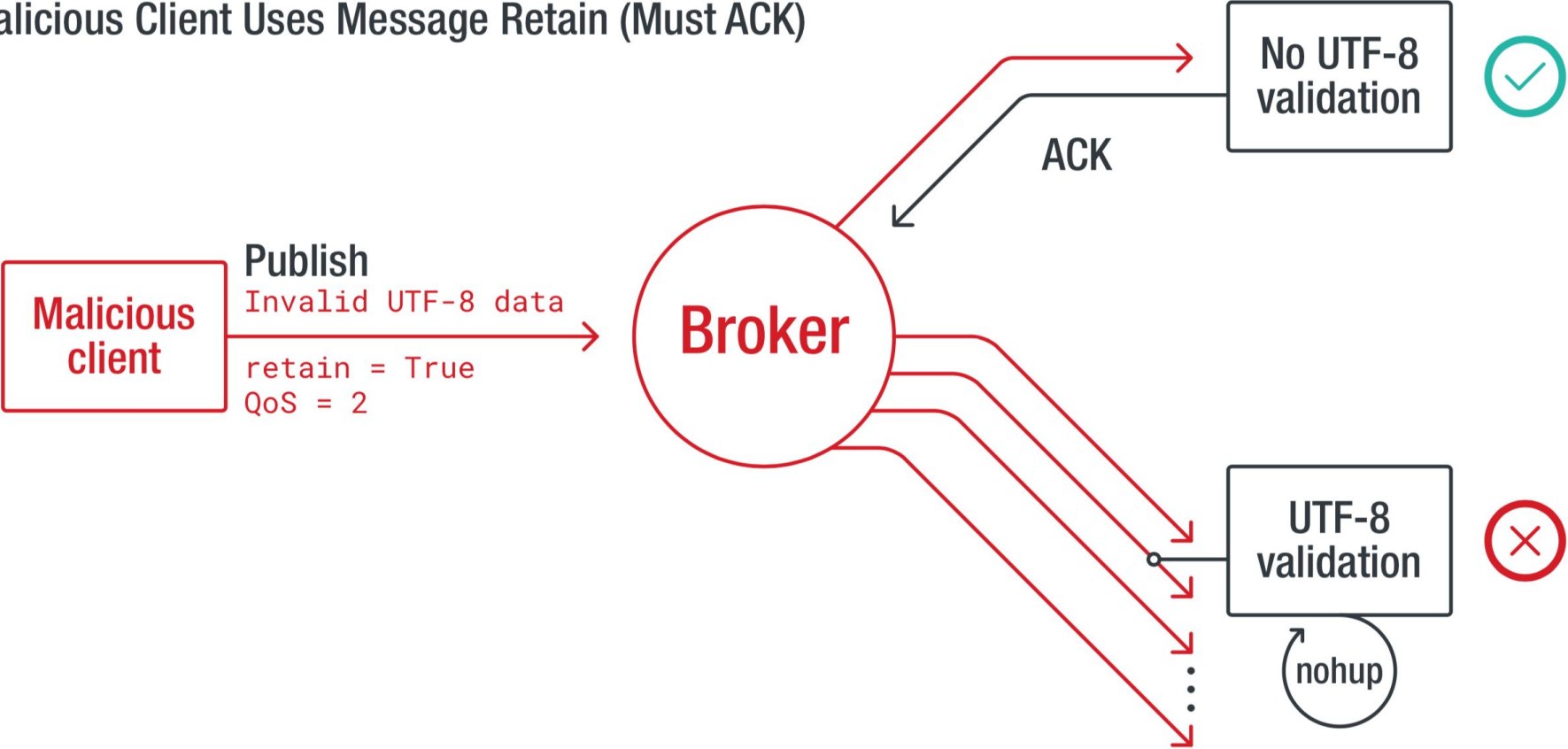




Broker Doesn't Validate vs. Client Does Validate



Malicious Client Uses Message Retain (Must ACK)



MQTT Handling of Disallowed Unicode code points Version 1.0

Working Draft 01

08 February 2018

Technical Committee:

OASIS Message Queuing Telemetry Transport (MQTT) TC

[CVE-2017-7653](#)

MQTT Handling of Disallowed Unicode code points Version 1.0

Abstract:

This Committee Note describes identified exposures in the handling of disallowed Unicode code points. Users of MQTT are alerted to the possibility that some combinations of MQTT Clients and Servers might allow properly authorized publishing Clients to cause the disconnection of properly authorized subscribing Clients. We describe how to identify if this risk is present and how to eliminate it.

full power machines to embedded and low power machines. Sensors and actuators, which are often the sources and destinations of MQTT messages, can be very small and lacking in power. This also applies to the embedded machines to which they are connected, which is where Mosquitto could be run.

Typically, the current implementation of Mosquitto has an executable in the order of 120kB that consumes around 3MB RAM with 1000 clients connected. There have been reports of successful tests with 100,000 connected clients at modest message rates.

As well as accepting connections from MQTT client applications, Mosquitto has a bridge which allows it to connect to other MQTT servers, including other Mosquitto instances. This allows networks of MQTT servers to be constructed, passing MQTT messages from any location in the network to any other, depending on the configuration of the bridges.

Licenses:


[Eclipse Distribution License 1.0 \(BSD\)](#)

[Eclipse Public License 1.0](#)

CVE-2017-7653

Latest Releases:

From December 21st, 2015 to May 2nd, 2018

Name	Date	Review
1.5	2018-05-02	
1.4.16	2018-04-18	
1.4.15	2018-02-28	
1.4.14	2017-07-10	
1.4.13	2017-06-27	
1.4.12	2017-05-29	
1.4.11	2017-02-20	
1.4.9	2016-06-03	
1.4.8	2016-02-14	
1.4.7	2015-12-21	



PROJECT LINKS

- [Website](#)
- [MQTT protocol discussion Google Group](#)
- [MQTT Community](#)
- [OASIS MQTT Technical Committee](#)
- [Wiki](#)

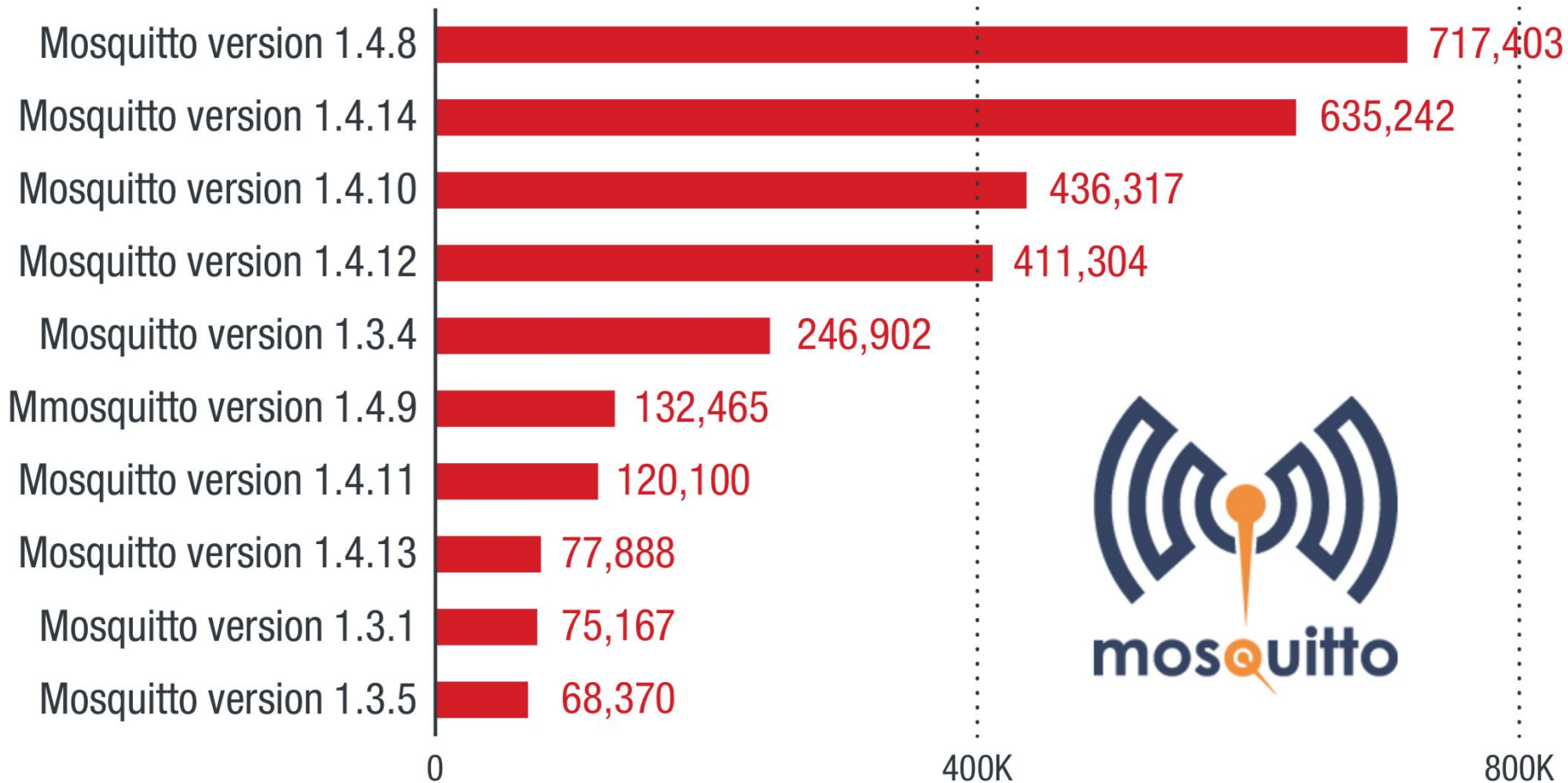
RELATED PROJECTS

Related Projects:

Eclipse IoT

» [Eclipse Paho](#)

Project Hierarchy:



PoC || GTFO

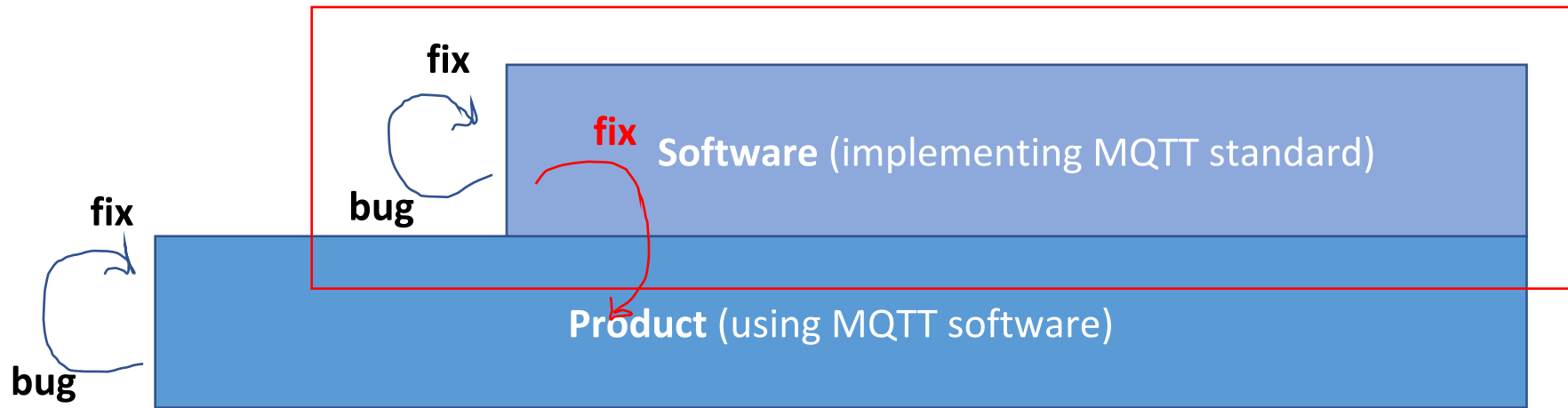
Lesson learned:
Security angle
on standards
(Davide → Federico)

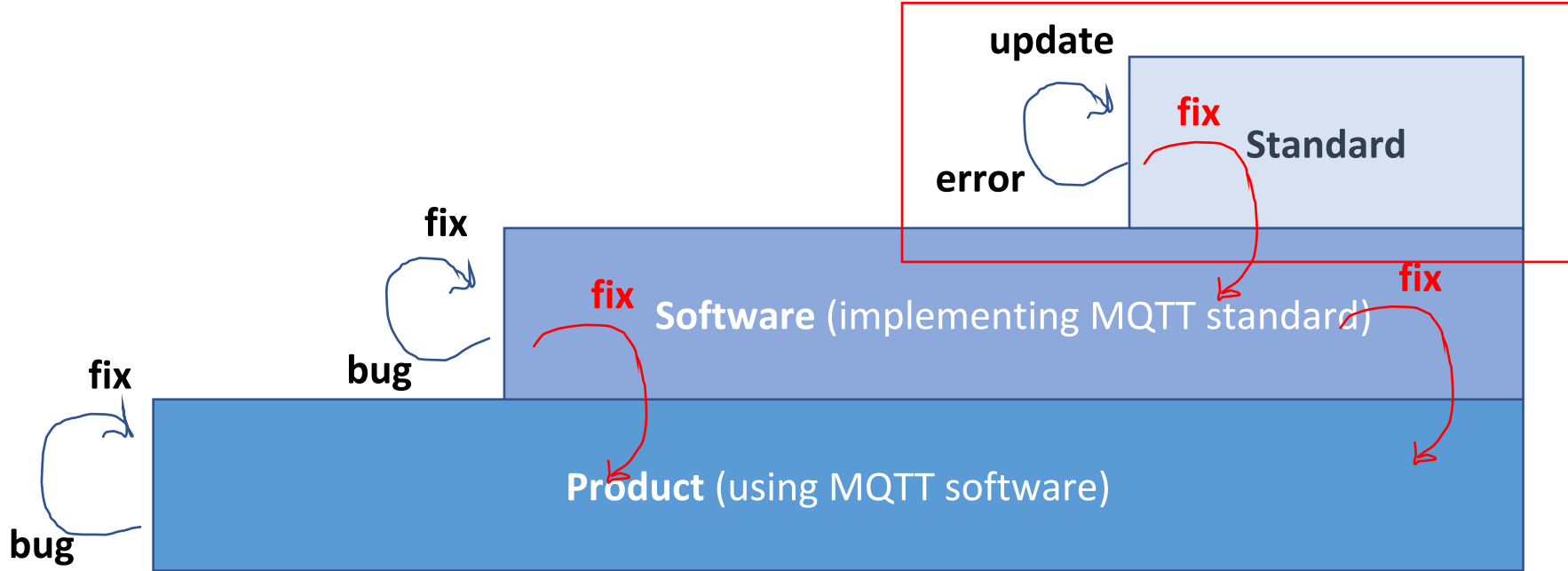


fix

bug

Product (using MQTT software)

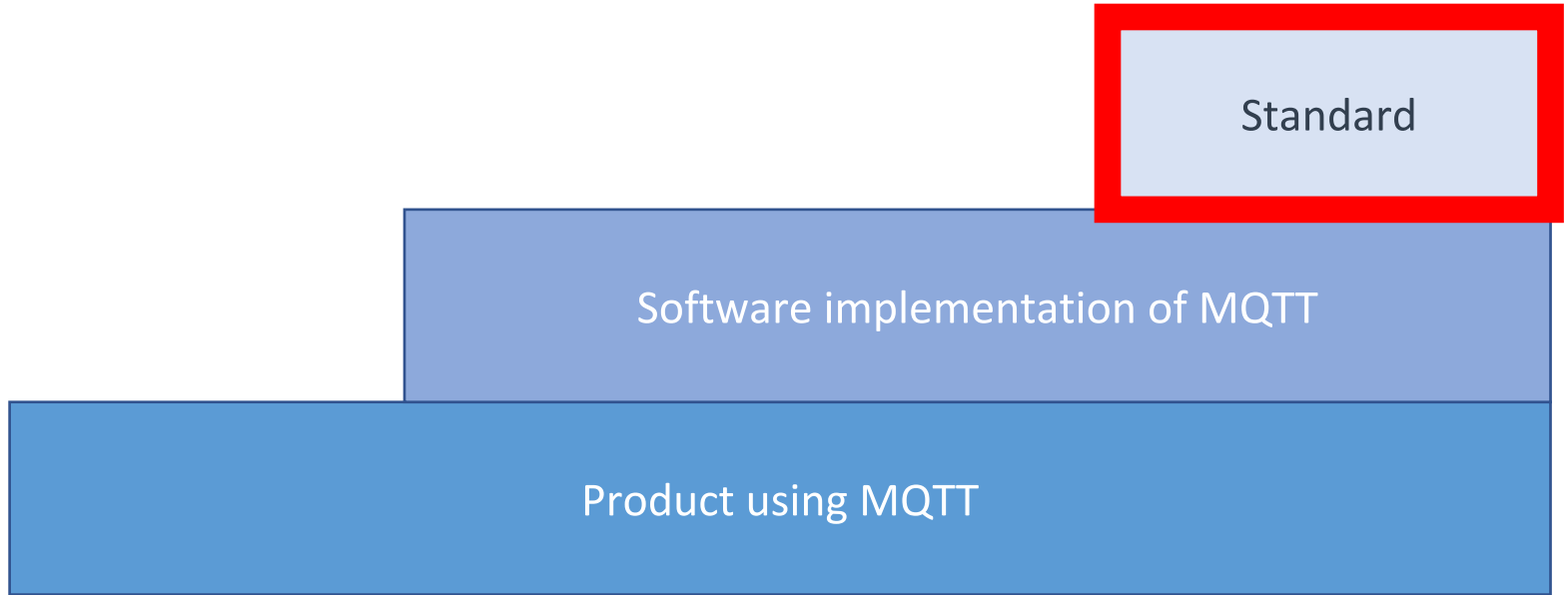




**August
2010**



**December
2015**



Standard

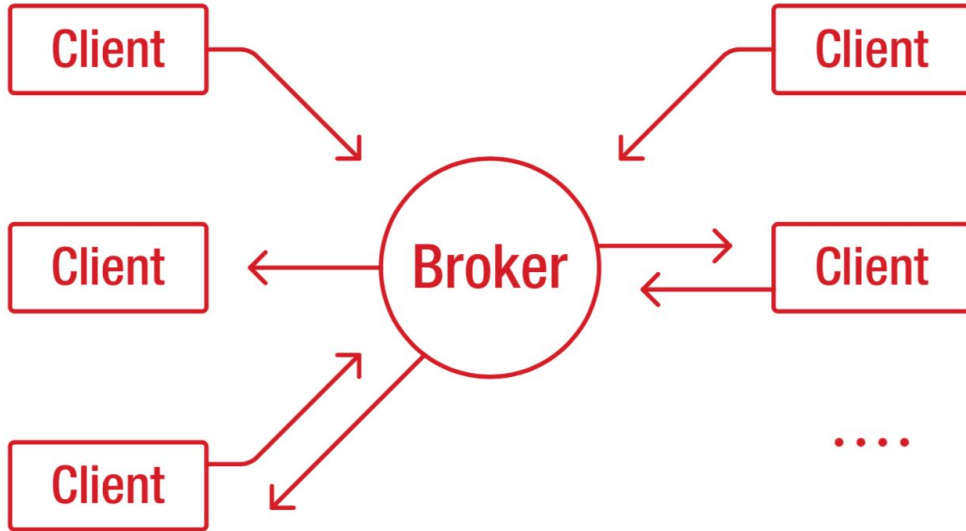
Software implementation of MQTT

Product using MQTT

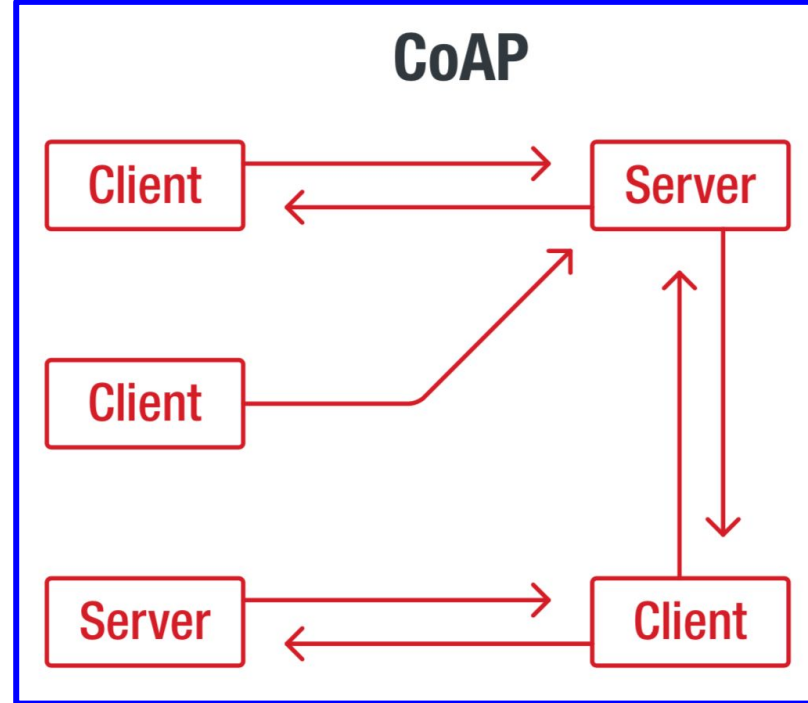
How about
CoAP?



MQTT

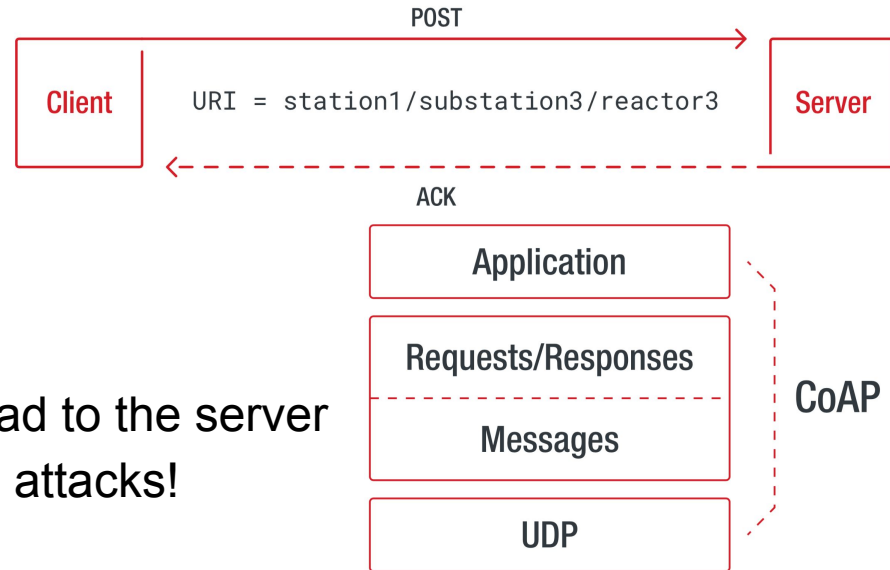


CoAP





- RFC **very clear** on potential security issues (**YAY! Built in and not bolt on!**)
- based on **UDP**: recall what this means!
 - open servers can be used
 - to bypass firewall ACLs
 - as reflectors
- CoAP allows to write (even large) payload to the server
 - perfect candidate for **amplification** attacks!



Time	Source	Destination	Protocol	Length	Info
2607	141.014541		CoAP	60	CON, MID:56326, GET, TKN:00 00 e7 27, End of Block #554, /.well-known/core
2608	141.035941		CoAP	113	ACK, MID:56326, 2.05 Content, TKN:00 00 e7 27, Block #554, /.well-known/core
2609	141.037175		CoAP	60	CON, MID:56327, GET, TKN:00 00 e7 28, End of Block #555, /.well-known/core
2610	141.056132		CoAP	113	ACK, MID:56327, 2.05 Content, TKN:00 00 e7 28, Block #555, /.well-known/core
2611	141.056975		CoAP	60	CON, MID:56328, GET, TKN:00 00 e7 29, End of Block #556, /.well-known/core
2612	141.070050		CoAP	113	ACK, MID:56328, 2.05 Content, TKN:00 00 e7 29, Block #556, /.well-known/core
2613	141.070750		CoAP	60	CON, MID:56329, GET, TKN:00 00 e7 2a, End of Block #557, /.well-known/core
2614	141.084059		CoAP	113	ACK, MID:56329, 2.05 Content, TKN:00 00 e7 2a, Block #557, /.well-known/core
2615	141.084928		CoAP	60	CON, MID:56330, GET, TKN:00 00 e7 2b, End of Block #558, /.well-known/core
2616	141.106669		CoAP	113	ACK, MID:56330, 2.05 Content, TKN:00 00 e7 2b, Block #558, /.well-known/core
2617	141.107940		CoAP	60	CON, MID:56331, GET, TKN:00 00 e7 2c, End of Block #559, /.well-known/core
2618	141.124426		CoAP	113	ACK, MID:56331, 2.05 Content, TKN:00 00 e7 2c, Block #559, /.well-known/core
2619	141.125229		CoAP	60	CON, MID:56332, GET, TKN:00 00 e7 2d, End of Block #560, /.well-known/core
2620	141.125546		CoAP	113	ACK, MID:56332, 2.05 Content, TKN:00 00 e7 2d, Block #560, /.well-known/core
2621	141.126092		CoAP	60	CON, MID:56333, GET, TKN:00 00 e7 2e, End of Block #561, /.well-known/core
2622	141.139059		CoAP	113	ACK, MID:56333, 2.05 Content, TKN:00 00 e7 2e, Block #561, /.well-known/core
2623	141.139698		CoAP	60	CON, MID:56334, GET, TKN:00 00 e7 2f, End of Block #562, /.well-known/core
2624	141.153055		CoAP	113	ACK, MID:56334, 2.05 Content, TKN:00 00 e7 2f, Block #562, /.well-known/core
2625	141.153785		CoAP	60	CON, MID:56335, GET, TKN:00 00 e7 30, End of Block #563, /.well-known/core
2626	141.177625		CoAP	113	ACK, MID:56335, 2.05 Content, TKN:00 00 e7 30, Block #563, /.well-known/core
2627	141.178477		CoAP	60	CON, MID:56336, GET, TKN:00 00 e7 31, End of Block #564, /.well-known/core
2628	141.193359		CoAP	58	ACK, MID:56336, 2.05 Content, TKN:00 00 e7 31, End of Block #564, /.well-known/core

▶ Frame 2607: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0

▶ Null/Loopback

▶ Internet Protocol Version 4, Src: [REDACTED], Dst: [REDACTED]

▼ User Datagram Protocol, Src Port: 62672, Dst Port: 5683

Source Port: 62672

Destination Port: 5683

Length: 36

Checksum: 0xfe37 [unverified]

[Checksum Status: Unverified]

[Stream index: 8]

▶ Constrained Application Protocol, Confirmable, GET, MID:56326

No.	Time	Source	Destination	Protocol	Length	Info
2607	141.014541			CoAP	60	CON, MID:56326, GET, TKN:00 00 e7 27, End of Block #554, /.well-known/core
2608	141.035941			CoAP	113	ACK, MID:56326, 2.05 Content, TKN:00 00 e7 27, Block #554, /.well-known/core
2609	141.037175			CoAP	60	CON, MID:56327, GET, TKN:00 00 e7 28, End of Block #555, /.well-known/core
2610	141.056132			CoAP	113	ACK, MID:56327, 2.05 Content, TKN:00 00 e7 28, Block #555, /.well-known/core
2611	141.056975			CoAP	60	CON, MID:56328, GET, TKN:00 00 e7 29, End of Block #556, /.well-known/core
2612	141.070050			CoAP	113	ACK, MID:56328, 2.05 Content, TKN:00 00 e7 29, Block #556, /.well-known/core
2613	141.070750			CoAP	60	CON, MID:56329, GET, TKN:00 00 e7 2a, End of Block #557, /.well-known/core
2614	141.084059			CoAP	113	ACK, MID:56329, 2.05 Content, TKN:00 00 e7 2a, Block #557, /.well-known/core
2615	141.084928			CoAP	60	CON, MID:56330, GET, TKN:00 00 e7 2b, End of Block #558, /.well-known/core
2616	141.106669			CoAP	113	ACK, MID:56330, 2.05 Content, TKN:00 00 e7 2b, Block #558, /.well-known/core
2617	141.107940			CoAP	60	CON, MID:56331, GET, TKN:00 00 e7 2c, End of Block #559, /.well-known/core
2618	141.124426			CoAP	113	ACK, MID:56331, 2.05 Content, TKN:00 00 e7 2c, Block #559, /.well-known/core
2619	141.125229			CoAP	60	CON, MID:56332, GET, TKN:00 00 e7 2d, End of Block #560, /.well-known/core
2620	141.125546			CoAP	113	ACK, MID:56332, 2.05 Content, TKN:00 00 e7 2d, Block #560, /.well-known/core
2621	141.126092			CoAP	60	CON, MID:56333, GET, TKN:00 00 e7 2e, End of Block #561, /.well-known/core
2622	141.139059			CoAP	113	ACK, MID:56333, 2.05 Content, TKN:00 00 e7 2e, Block #561, /.well-known/core
2623	141.139698			CoAP	60	CON, MID:56334, GET, TKN:00 00 e7 2f, End of Block #562, /.well-known/core
2624	141.153055			CoAP	113	ACK, MID:56334, 2.05 Content, TKN:00 00 e7 2f, Block #562, /.well-known/core
2625	141.153785			CoAP	60	CON, MID:56335, GET, TKN:00 00 e7 30, End of Block #563, /.well-known/core
2626	141.177625			CoAP	113	ACK, MID:56335, 2.05 Content, TKN:00 00 e7 30, Block #563, /.well-known/core
2627	141.178477			CoAP	60	CON, MID:56336, GET, TKN:00 00 e7 31, End of Block #564, /.well-known/core
2628	141.193359			CoAP	113	ACK, MID:56336, 2.05 Content, TKN:00 00 e7 31, Block #564, /.well-known/core

▶ Frame 2607: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
 ▶ Null/Loopback
 ▶ Internet Protocol Version 4, Src: [REDACTED], Dst Port: 62672
 ▶ User Datagram Protocol, Src Port: 62672, Dst Port: 5683
 Source Port: 62672
 Destination Port: 5683
 Length: 36
 Checksum: 0xfe37 [unverified]
 [Checksum Status: Unverified]
 [Stream index: 8]
 ▶ Constrained Application Protocol, Confirmable, GET, MID:56326

▶ Frame 2608: 113 bytes on wire (904 bits), 113 bytes captured (904 bits) on interface 0
 ▶ Null/Loopback
 ▶ Internet Protocol Version 4, Src: [REDACTED], Dst Port: 62672
 ▶ User Datagram Protocol, Src Port: 5683, Dst Port: 62672
 Source Port: 5683
 Destination Port: 62672
 Length: 89
 Checksum: 0xfe6c [unverified]
 [Checksum Status: Unverified]
 [Stream index: 8]
 ▶ Constrained Application Protocol, Acknowledgement, 2.05 Content, MID:56326

Time	Source	Destination	Protocol	Length	Info
2607	141.014541		CoAP	60	CON, MID:56326, GET, TKN:00 00 e7 27, End of Block #554, /.well-known/core
2608	141.035941		CoAP	113	ACK, MID:56326, 2.05 Content, TKN:00 00 e7 27, Block #554, /.well-known/core
2609	141.037175		CoAP	60	CON, MID:56327, GET, TKN:00 00 e7 28, End of Block #555, /.well-known/core
2610	141.056132		CoAP	113	ACK, MID:56327, 2.05 Content, TKN:00 00 e7 28, Block #555, /.well-known/core
2611	141.056975		CoAP	60	CON, MID:56328, GET, TKN:00 00 e7 29, End of Block #556, /.well-known/core
2612	141.070050		CoAP	113	ACK, MID:56328, 2.05 Content, TKN:00 00 e7 29, Block #556, /.well-known/core
2613	141.070750		CoAP	60	CON, MID:56329, GET, TKN:00 00 e7 2a, End of Block #557, /.well-known/core
2614	141.084059		CoAP	113	ACK, MID:56329, 2.05 Content, TKN:00 00 e7 2a, Block #557, /.well-known/core
2615	141.084928		CoAP	60	CON, MID:56330, GET, TKN:00 00 e7 2b, End of Block #558, /.well-known/core
2616	141.106669		CoAP	113	ACK, MID:56330, 2.05 Content, TKN:00 00 e7 2b, Block #558, /.well-known/core
2617	141.107940		CoAP	60	CON, MID:56331, GET, TKN:00 00 e7 2c, End of Block #559, /.well-known/core
2618	141.124426		CoAP	113	ACK, MID:56331, 2.05 Content, TKN:00 00 e7 2c, Block #559, /.well-known/core
2619	141.125229		CoAP	60	CON, MID:56332, GET, TKN:00 00 e7 2d, End of Block #560, /.well-known/core
2620	141.125546		CoAP	113	ACK, MID:56332, 2.05 Content, TKN:00 00 e7 2d, Block #560, /.well-known/core
2621	141.126092		CoAP	60	CON, MID:56333, GET, TKN:00 00 e7 2e, End of Block #561, /.well-known/core
2622	141.139059		CoAP	113	ACK, MID:56333, 2.05 Content, TKN:00 00 e7 2e, Block #561, /.well-known/core
2623	141.139698		CoAP	60	CON, MID:56334, GET, TKN:00 00 e7 2f, End of Block #562, /.well-known/core
2624	141.153055		CoAP	113	ACK, MID:56334, 2.05 Content, TKN:00 00 e7 2f, Block #562, /.well-known/core
2625	141.153785		CoAP	60	CON, MID:56335, GET, TKN:00 00 e7 30, End of Block #563, /.well-known/core
2626	141.177625		CoAP	113	ACK, MID:56335, 2.05 Content, TKN:00 00 e7 30, Block #563, /.well-known/core
2627	141.178477		CoAP	60	CON, MID:56336, GET, TKN:00 00 e7 31, End of Block #564, /.well-known/core
2628	141.193359		CoAP	113	ACK, MID:56336, 2.05 Content, TKN:00 00 e7 31, Block #564, /.well-known/core

Protocol	BAF
SNMP v2	6.3
NTP	556.9
DNS _{NS}	54.6
DNS _{OR}	28.7
NetBios	3.8
SSDP	30.8
CharGen	358.8
QOTD	140.3
BitTorrent	3.8
Kad	16.3
Quake 3	63.9
Steam	5.5
ZAv2	36.0
Salinity	37.3
Gameover	45.4

Frame 2607: 60 bytes on wire (480 bits) captured (480 bits) on interface 0
Null/Loopback
Internet Protocol Version 4, Src: 141.014541, Dst: 141.014541
User Datagram Protocol, Src Port: 5683, Dst Port: 62672
Source Port: 5683
Destination Port: 62672
Length: 89
Checksum: 0xfe6c [unverified] [Checksum Status: Unverified] [Stream index: 8]
Constrained Application Protocol, Acknowledgement, 2.05 Content, MID:56326

Frame 2607: 60 bytes on wire (480 bits) captured (480 bits) on interface 0
Null/Loopback
Internet Protocol Version 4, Src: 141.014541, Dst: 141.014541
User Datagram Protocol, Src Port: 5683, Dst Port: 62672
Source Port: 5683
Destination Port: 62672
Length: 36
Checksum: 0xfe37 [unverified] [Checksum Status: Unverified] [Stream index: 8]
Constrained Application Protocol, Confirmable, GET, MID:56326

CoAP 2.47x

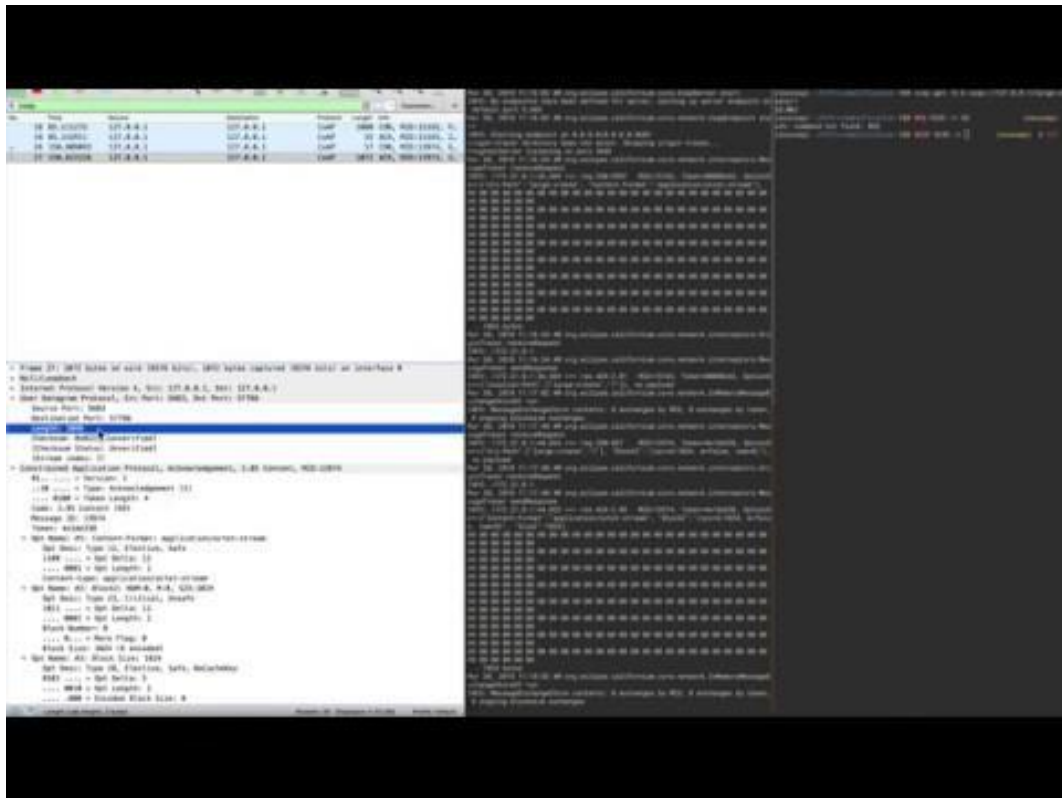
Bandwidth Amplification Factor (BAF)

Reference table from: <https://christian-rossow.de/publications/amplification-ndss2014.pdf>

In summary, this specification adds a pair of Block options to CoAP that can be used for **block-wise transfers**. Benefits of using these options include:

- o Transfers larger than what can be accommodated in constrained-network link-layer packets can be performed in smaller blocks.
- o No hard-to-manage conversation state is created at the adaptation layer or IP layer for fragmentation.
- o The transfer of each block is acknowledged, enabling individual retransmission if required.
- o **Both sides have a say in the block size that actually will be used.**
- o The resulting exchanges are easy to understand using packet analyzer tools and thus quite accessible to debugging.
- o If needed, the Block options can also be used (without changes) to provide random access to power-of-two sized blocks within a resource representation.

PoC || GTFO



BAF = 31.75X

Protocol	<i>all</i>
SNMP v2	6.3
NTP	556.9
DNS _{NS}	54.6
DNS _{OR}	28.7
NetBios	3.8
SSDP	30.8
CharGen	358.8
QOTD	140.3
BitTorrent	3.8
Kad	16.3
Quake 3	63.9
Steam	5.5
ZAv2	36.0
Salinity	37.3
Gameover	45.4

In summary, this specification adds a pair of options that can be used for block-wise transfers. The options include:

- o Transfers larger than what can be accommodated by network link-layer packets can be performed.
- o No handling of congestion state is required at the link layer or IP layer for fragmentation.
- o The transfer of each block is acknowledged and retransmission if required.
- o Both sides have a say in the block size used.
- o The resulting exchanges are easy to understand with analyzer tools and thus quite accessible.
- o If needed, the Block options can also be used to provide random access to power-of-two resource representation.

CoAP: 32x
1Mbps: 32Mbps

Protocol	<i>all</i>
SNMP v2	6.3
NTP	556.9
DNS _{NS}	54.6
DNS _{OR}	28.7
NetBios	3.8
SSDP	30.8
CharGen	358.8
QOTD	140.3
BitTorrent	3.8
Kad	16.3
Quake 3	63.9
Steam	5.5
ZAv2	36.0
Salicy	37.3
Gameover	45.4

The CoAP protocol is the next big thing for DDoS attacks

CoAP DDoS attacks have already been detected in the wild, some clocking at 320Gbps.



By Catalin Cimpanu for Zero Day | December 5, 2018 -- 04:13 GMT (04:13 GMT) | Topic: Security



RFC 7252, also known as the Constrained Application Protocol (CoAP), is about to become one of the most abused protocols in terms of DDoS attacks, security researchers have told ZDNet.

MORE FROM CATALIN CIMPANU



Security
Twelve US states join for the first to file multistate data breach law



Security
A botnet of over 20,000 WordPress sites is attacking other WordPress sites



Security
BeatStars discloses security breach in Twitter live stream



Security
Adobe releases out-of-band security update for newly discovered Flash zero-day

NEWSLETTERS

ZDNet Security

Your weekly update on security around globe, featuring research, threats, and m



TOTAL RESULTS

515,459

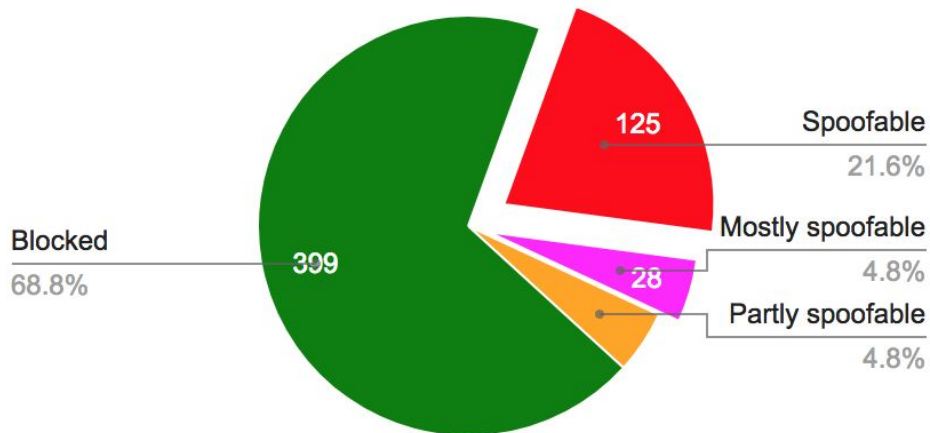
TOP COUNTRIES



China

515,459

IPv4 autonomous systems (excluding NAT)



Big Picture
&
Takeaways



Security impact

Privacy impact

Root cause: Changes in the design

Root cause: Implementation vulnerabilities

Root cause: Unsecured deployments and no default security

Security impact

Privacy impact

Root cause: Changes in the design

Root cause: Implementation vulnerabilities

- Data validation

- Protocol parsing

Root cause: Unsecured deployments and no default security

Feature abuse

- Amplification

- Listing

Security impact

Privacy impact

Reconnaissance

Lateral movement

Industrial espionage

Remote control or DoS of a machine

Targeted attacks

Root cause: Changes in the design

Root cause: Implementation vulnerabilities

- **Data validation**
Unicode issues
- **Protocol parsing**
Length fields
Topic filtering

Root cause: Unsecured deployments and no default security

Feature abuse

- **Amplification**
(CoAP only)
- **Listing**
- Secrets
- Automation systems
- Network details
- People and asset tracking
- OTA upgrades

Security impact

Privacy impact





TREND MICRO research

The Fragility of Industrial IoT's Data Backbone
Security and Privacy Issues in MQTT and CoAP Protocols

Federico Maggi and Rainer Vosseler
Trend Micro Research

Davide Quarta
EURCOM and Politecnico di Milano

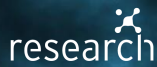




blackhat[®]
EUROPE 2018
DECEMBER 3-6, 2018
EXCEL LONDON / UNITED KINGDOM

When Machines Can't Talk

Security & Privacy Issues of M2M Data Protocols



Federico Maggi
Senior Threat Researcher



POLITECNICO
MILANO 1863

Davide Quarta
Post-doc Researcher (now at EURECOM)

 #BHEU / @BLACKHATEVENTS