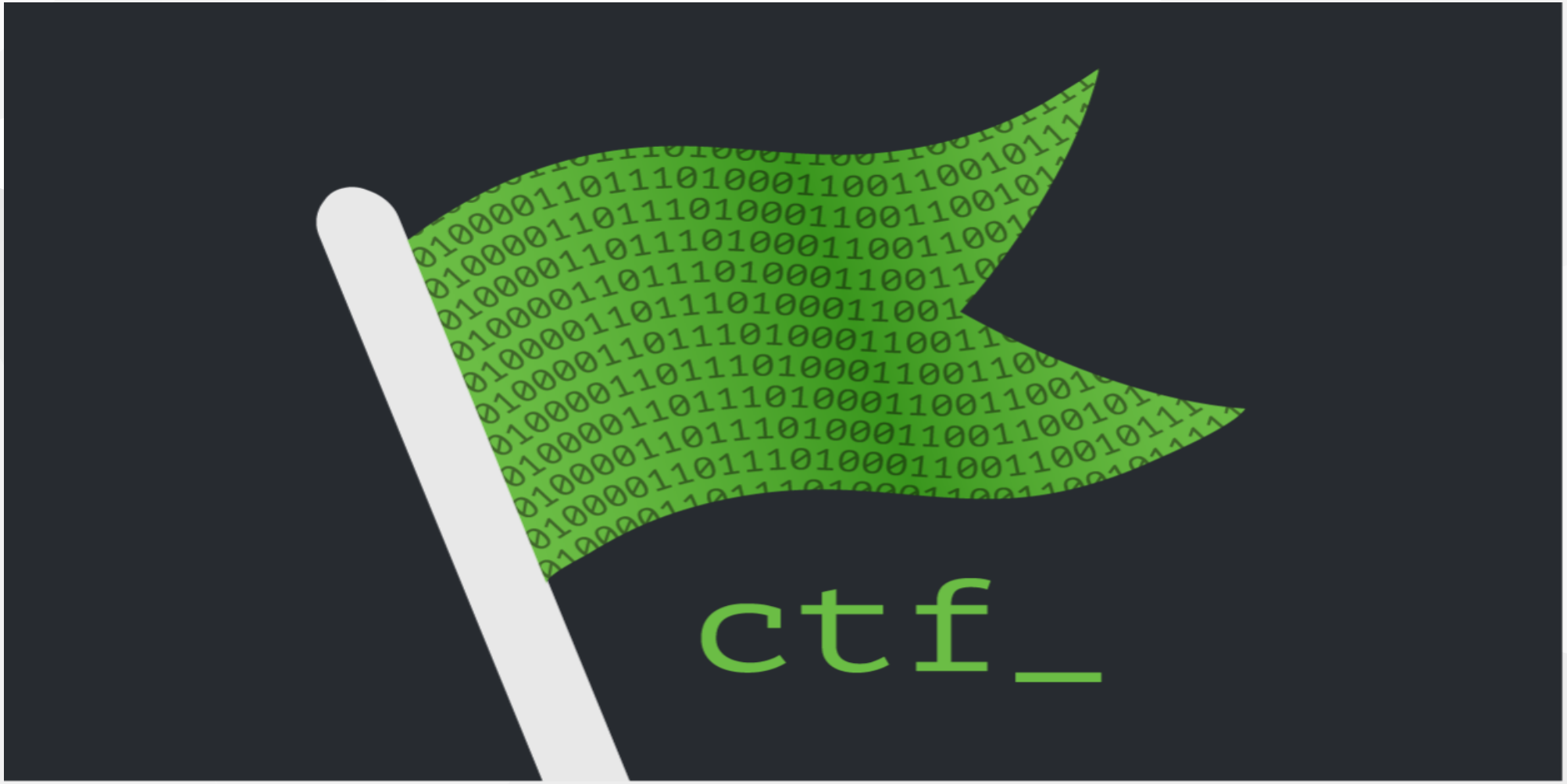
DESCON CTF

CTF

- Capture the flag
- Game designed to let you learn to hack in a safe, rewarding environment
- Where: ctf.descon.me
- Style: jeopardy
- Flag format: DCTF{flag}
- Categories:
  - Web, Misc, Crypto, RE, Stegano, IoT

Don't forget to have fun!



Lightning talk:

IOT SECURITY VULNERABILITIES


Sale
Connected Appliances
klossner
"CAN I INTEREST YOU IN A FIREWALL FOR YOUR TOASTER?"

OWASP IOT Top 10 (1-5)

1. Weak, Guessable or Hardcoded passwords
2. Insecure network services
3. Insecure ecosystem interfaces
4. Lack of secure update mehanism
5. Use of insecure components

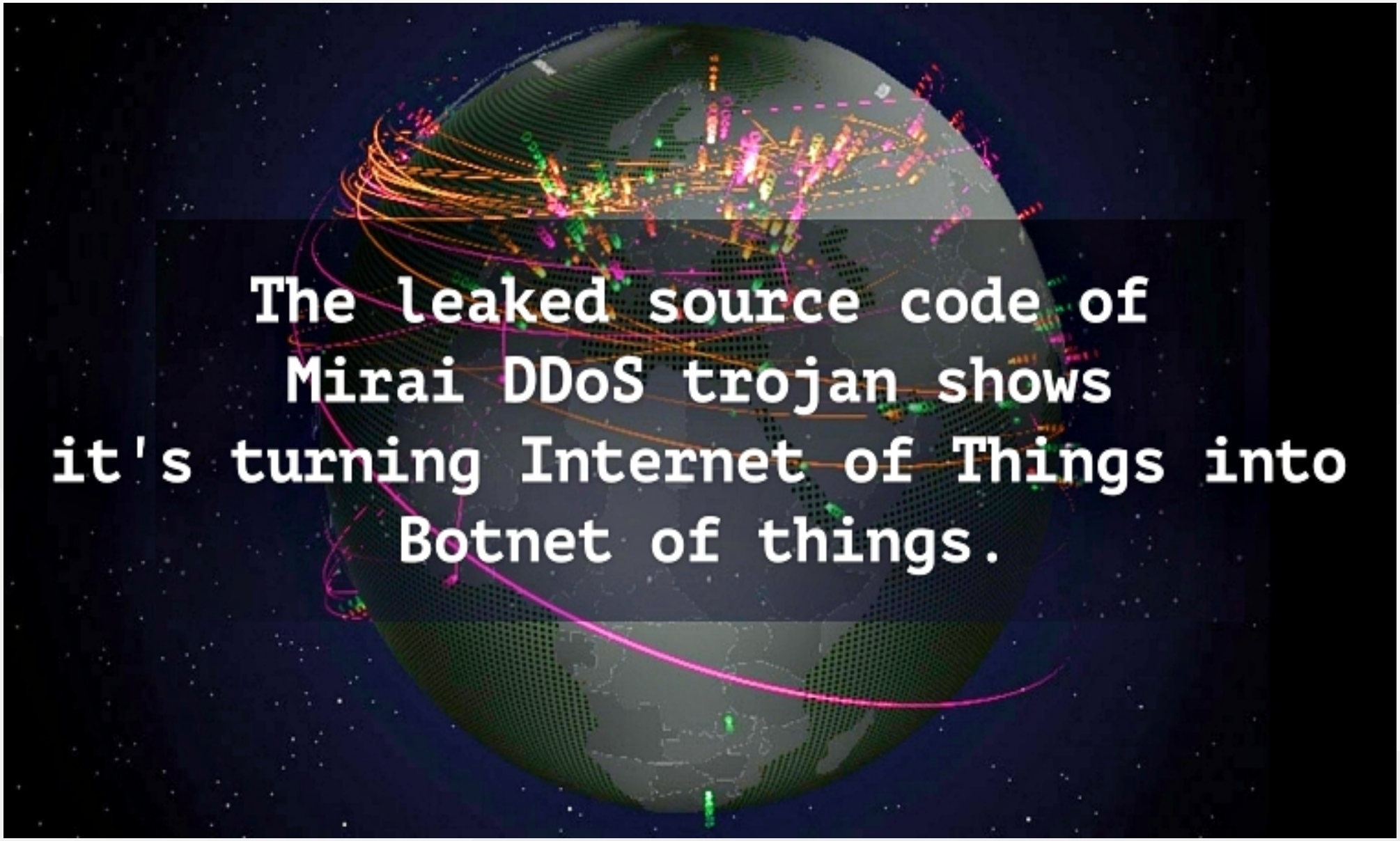
OWASP IOT Top 10 (6-10)

6. Insufficient privacy protection
7. Insecure data transfer and storage
8. Lack of device management
9. Insecure default settings
10. Lack of physical hardening

Bad passwords

- Types of bad passwords:
  - Weak
  - Guessable
  - Hardcoded
  - Default
- Used in couple CTF challenges

"LET THE HACKERS GUESS."


The leaked source code of
Mirai DDoS trojan shows
it's turning Internet of Things into
Botnet of things.

- Vatican has the highest botnet density in Europe
  - One bot for every 5 internet users

Username Enumeration

- Ability to collect a set of valid usernames by interacting with the authentication mechanism

Account Lockout

- Ability to continue sending authentication attempts after 3 - 5 failed login attempts

Insecure Network Services

- Unneeded or insecure network services running on the device itself that compromise the confidentiality, integrity, or availability of information or allow unauthorized remote control
  - Vulnerable Services
  - Buffer Overflow
  - Open Ports via UPnP
  - Exploitable UDP Services
  - Denial-of-Service
  - DoS via Network Device Fuzzing

Example

- Ports open to the internet possibly without the user's knowledge via UPnP.

```
Port 80 and 443 exposed to the internet via a home router.
```

- In the cases above, the attacker is able to disable the device completely with an HTTP GET or access the device via the internet over port 80 and/or port 443.

Shodan.io

175[redacted]

n175[redacted]ic.optusnet.com.au

City	Langwarrin
Country	Australia
Organization	Optus
ISP	Optus
Last Update	2018-02-23T17:46:01.888838
Hostnames	[redacted]ic.optusnet.com.au
ASN	AS4804

Ports

8443

Services

8443
tcp
https

Avtech AVN801 network camera Version: 1.0

```
HTTP/1.1 200 OK
Date: Fri, 23 Feb 2018 17:46:00 GMT
Server: Linux/2.x UPnP/1.0 Avtech/1.0
Connection: close
Last-Modified: Tue, 13 Dec 2016 05:48:10 GMT
Content-Type: text/html
ETag: 470-17649-1481608090
Content-Length: 17649
```

Insecure Web Interface

- Account Enumeration
- Weak Default Credentials
- Credentials Exposed in Network Traffic
- Cross-site Scripting (XSS)
- SQL-Injection
- Session Management
- Weak Account Lockout Settings

Lack of Transport Encryption

- Username and password are transmitted in the clear over the network

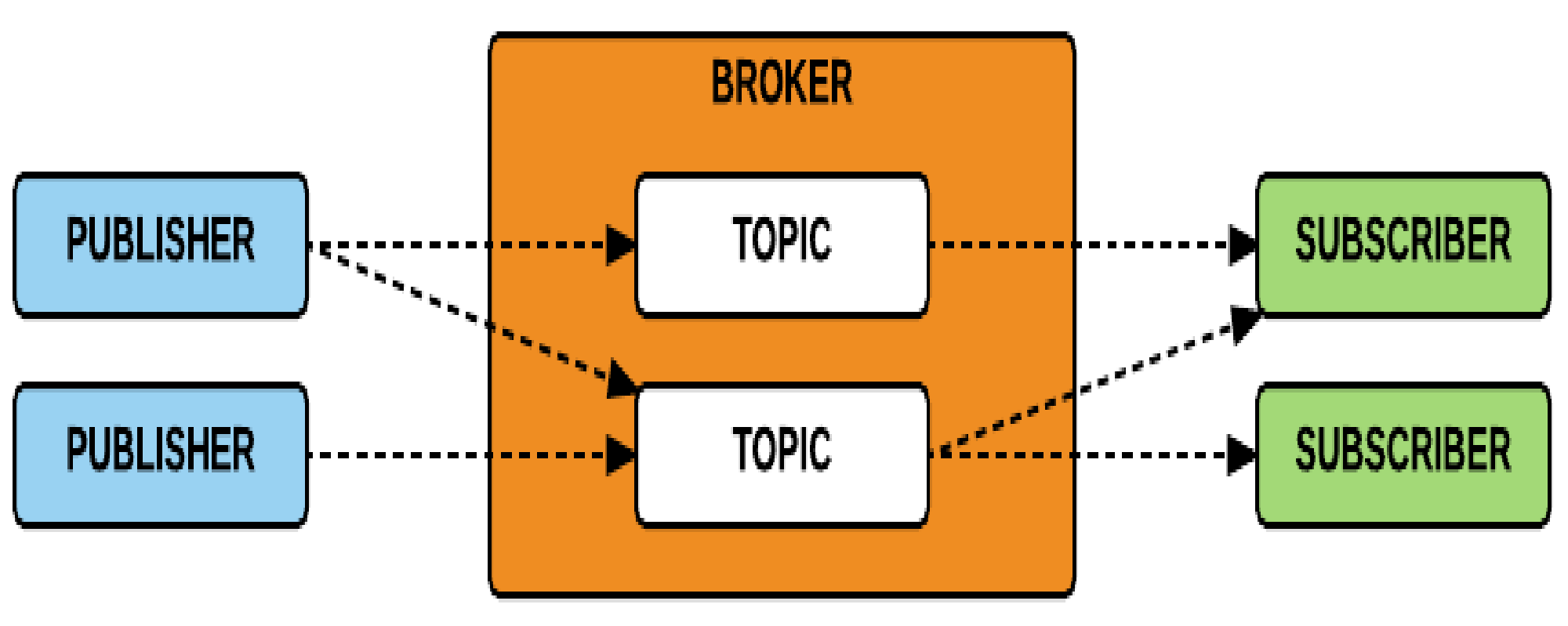
```
http://www.xyzcloud.com/login.php?userid=3&password=1234
```

- In the cases above, the attacker has the ability to view sensitive data in the clear due to lack of transport encryption
- Used in one ctf challenge

MQTT

- publish subscribe based message passing protocol
- the HTTP of IOT
  - shares all of the vulnerabilities that HTTP and other old insecure protocols have
- By default:
  - without authentication
  - password sent in cleartext

MQTT Architecture



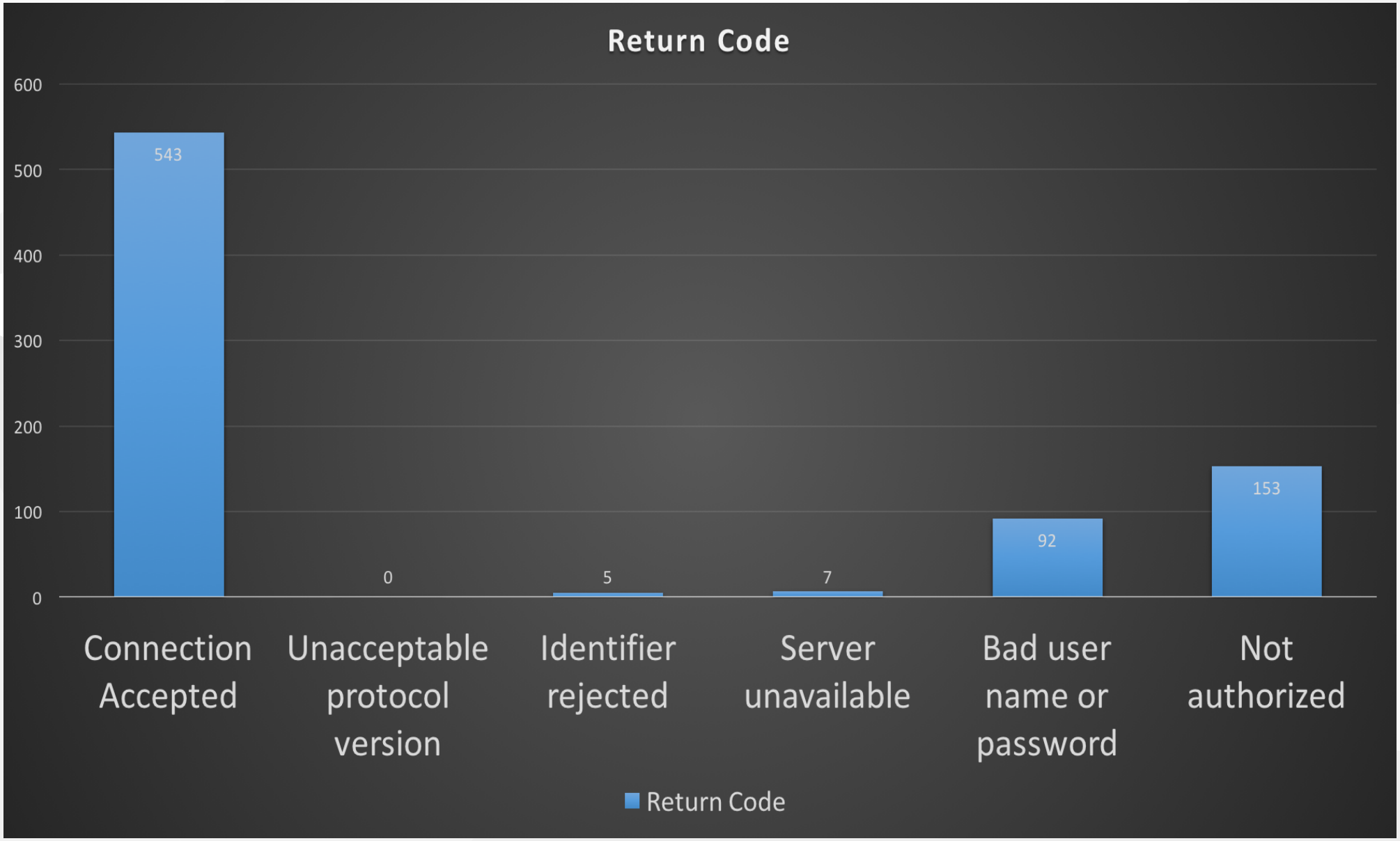
Message example

```
[*] Topic: owntracks
[*] Message:
{
    "_cp": true,
    "_type": "location",
    "acc": 20,
    "batt": 60,
    "conn": "w",
    "lat": [redacted]
    "lon": [redacted]
    "t": "u",
    "tid": "b3",
    "tst": [redacted]
}
```

NEWS

32,000 smart homes can be easily hacked due to misconfigured MQTT servers

Thanks to MQTT servers which are either misconfigured or not protected with a password, it is easy peasy to hack a smart home.


Return Code
600
500
400
300
200
100
0
543
0
5
7
92
153
Connection Accepted
Unacceptable protocol version
Identifier rejected
Server unavailable
Bad user name or password
Not authorized
Return Code

Lack of ability to securely update the device

- Update sent without encryption
- Updates not signed
- Update location writable
- Update verification
- Malicious update
- Missing update mechanism
- No manual update mechanism

Poor Physical Security

- Access to Software via USB Ports
- Obtaining console access via serial interfaces (SPI / UART)
- Removal of Storage Media
- NFC
- Even QR codes can be used as input vector
- Used in couple ctf challenges

Backing Up the Internet of Things

Final idea

- Tomorrow, after workshops, let's check together the security aspects of Klimamerko
- What we can do:
  - Review the administrative interface of the device
  - Identify all data types that are being collected
  - Check how the passwords are stored
  - Check web and cloud interface
  - Code audit
  - Check physical security: USB port, Serial port, SD card...

Useful links:

- https://www.researchgate.net/publication/324149744_A_Comprehensive_IoT_Attacks_Survey_based_on_a_Building-blocked_Reference_Mode
- https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project
- https://www.corero.com/resources/ddos-attack-types/mirai-botnet-ddos-attack
- https://www.sba-research.org/wp-content/uploads/publications/QR_Code_Security.pdf