When A Password Is Not Enough

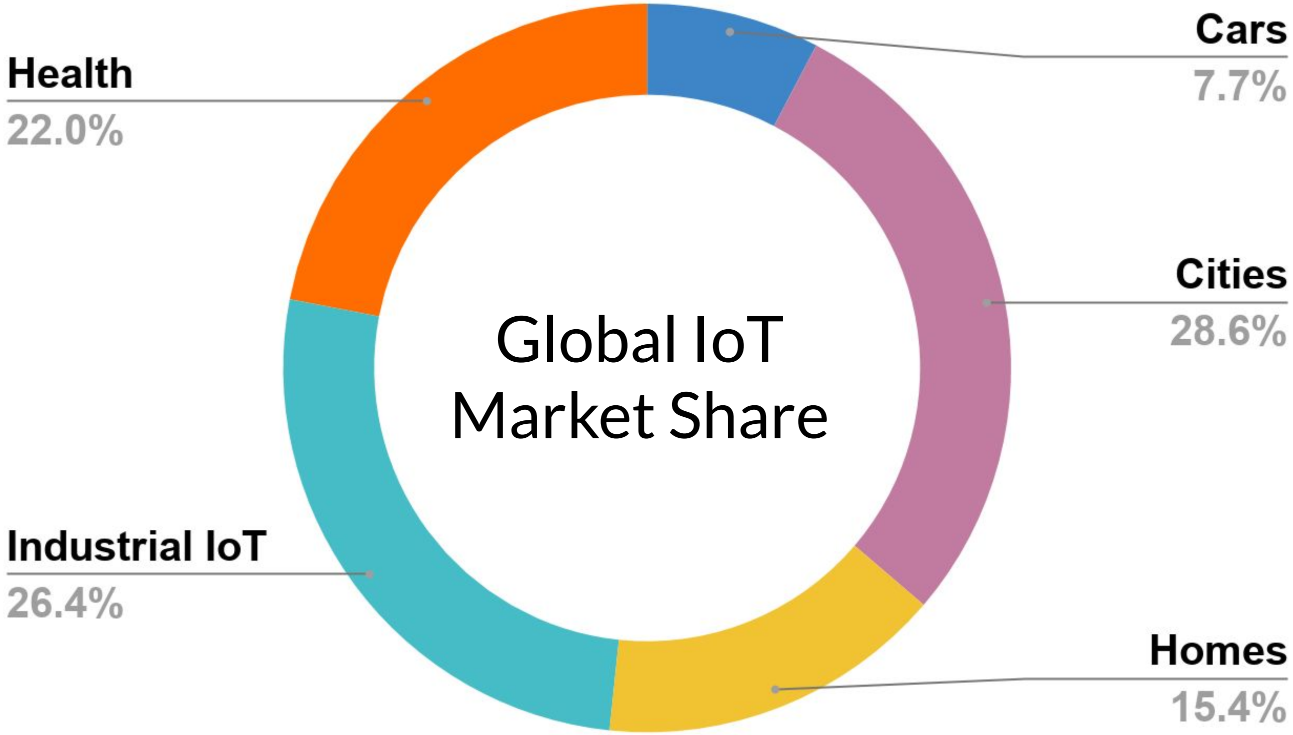
Developing A New Way Of Protecting Smart Homes

Simona Musilova | @siimi_m_

APOSEMAT

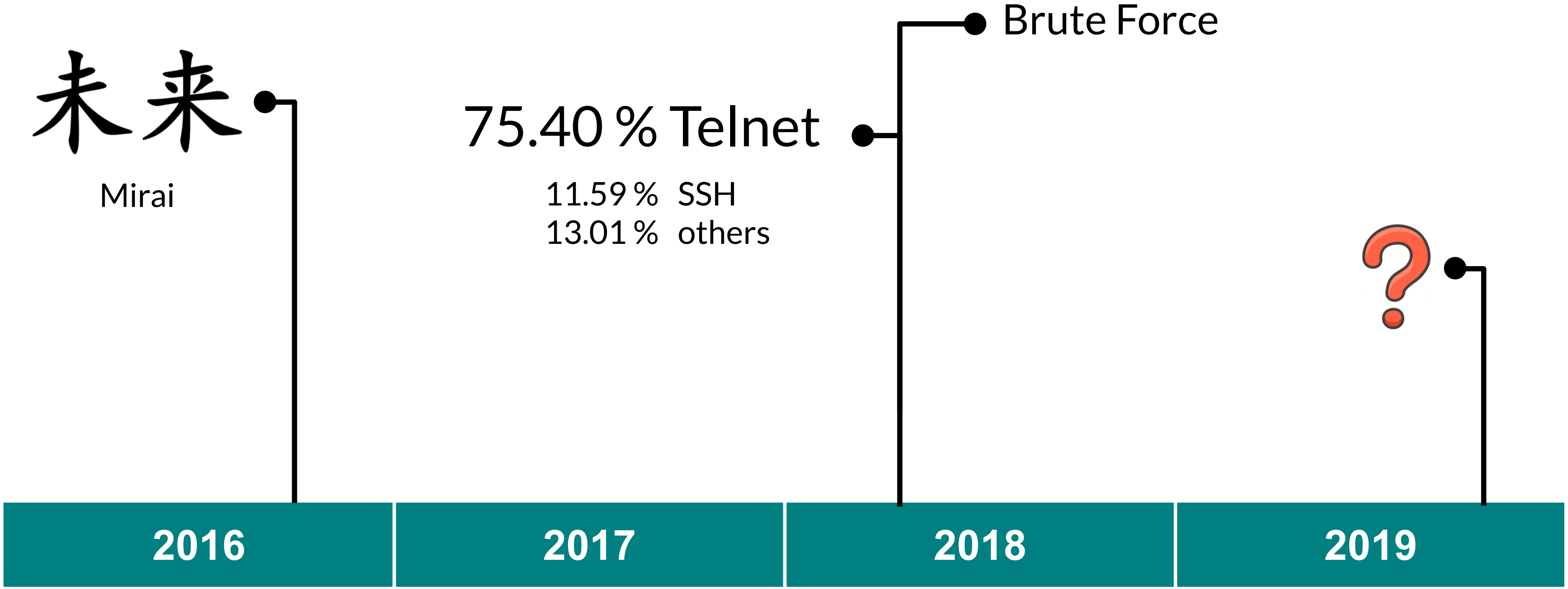
CTU
CZECH TECHNICAL
UNIVERSITY
IN PRAGUE

Internet of Things



*saveatlast.co

Attacks against IoT



未来

Mirai

75.40 % Telnet

11.59 % SSH
13.01 % others

Brute Force

❓

2016

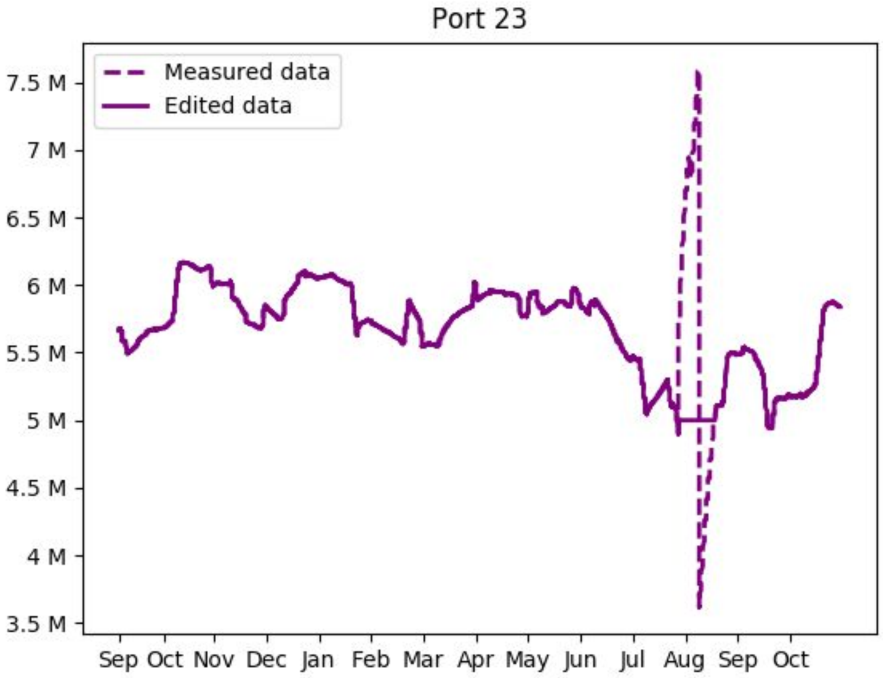
2017

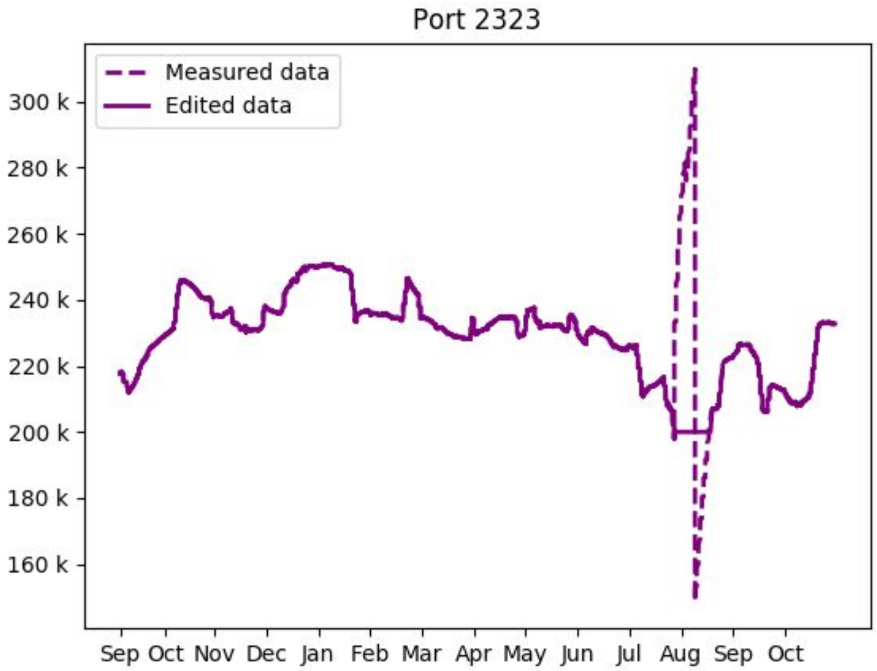
2018

2019

*KasperskyLab

The Number Of Telnet Devices


Port 23

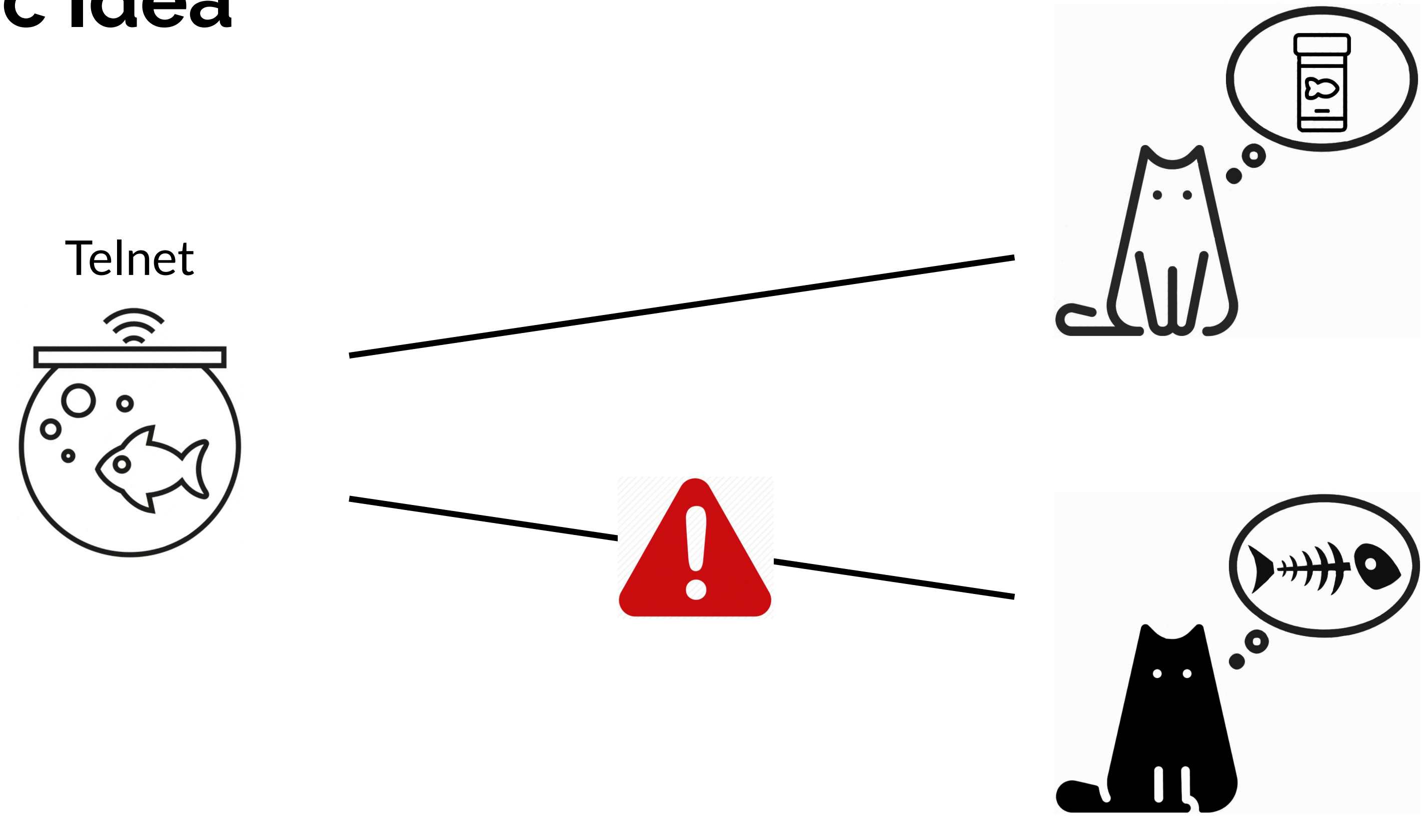

Port 2323

*Shodan

Any Telnet IDS?

Let’s create our own Telnet analyser!

Basic Idea



Telnet

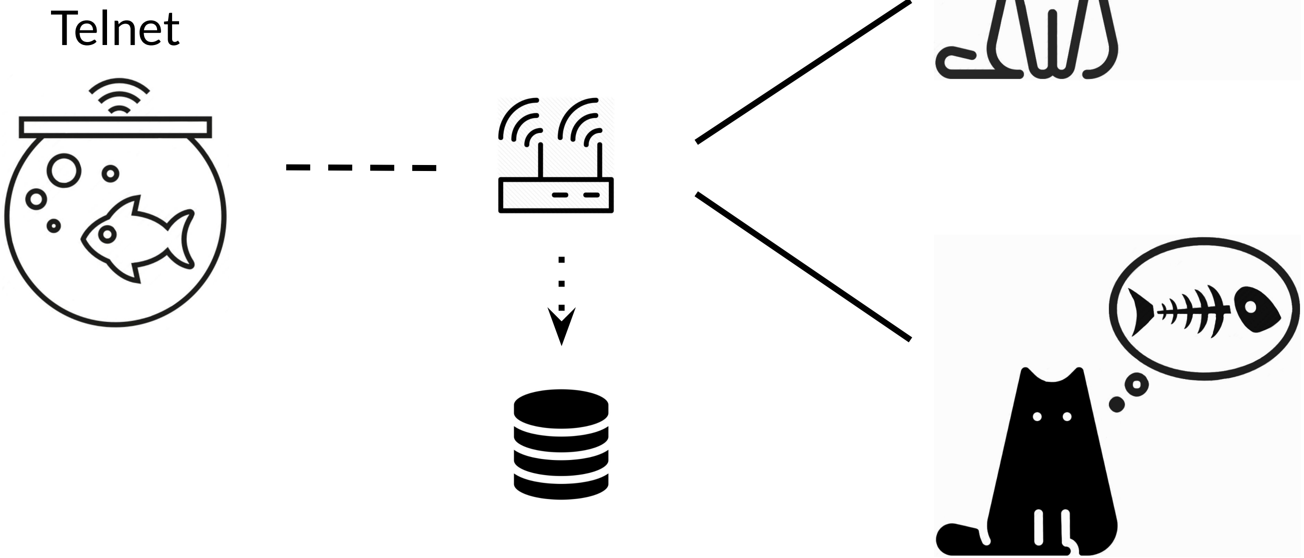
Capture Teln tra

Parse Telnet payload

Extract typing characteristics

Compare with the admin profile

Port mirroring



Capture Telne ✓
tra

Parse Telnet payload

Extract typing characteristics

Compare with the admin profile

Packet analysis

Layer	Protocol
Application	Telnet
Transport	TCP
Internet	IP
Network Access	Ethernet

Capture Telnet traffic ✓

Parse Telnet payload

Extract typing characteristics

Compare with the admin profile

TCP protocol

Packet analysis → Byte stream analysis

```
ff fb 25 ff fd 03 ff fb 18 ff fb 1f ff fb 20 ff fb 21
ff fb 22 ff fb 27 ff fd 05 ff fc 23 ff fa 1f 00 c5 00
34 ff f0 ff fa 20 00 33 38 34 30 30 2c 33 38 34 30 30
ff f0 ff fa 27 00 00 55 53 45 52 01 73 69 6d 69 ff f0
ff fa 18 00 58 54 45 52 4d 2d 32 35 36 43 4f 4c 4f 52
ff f0 ff fc 01 ff fd 01 0d 00 70 69 72 61 74 65 0d 00
68 79 70 72 69 6f 74 0d 00 0d 00 6c 73 0d 00 0d 00 ...
```

Capture Telnet traffic ✓

Parse Telnet payload

Extract typing characteristics

Compare with the admin profile

Telnet protocol

```
ff fb 25 ff fd 03 ff fb 18 ff fb 1f ff fb 20 ff fb
21 ff fb 22 ff fb 27 ff fd 05 ff fc 23 ff fa 1f 00
c5 00 34 ff f0 ff fa 20 00 33 38 34 30 30 2c 33 38
34 30 30 ff f0 ff fa 27 00 00 55 53 45 52 01 73 69
6d 69 ff f0 ff fa 18 00 58 54 45 52 4d 2d 32 35 36
43 4f 4c 4f 52 ff f0 ff fc 01 ff fd 01 70 69 72 61
74 65 0d 00 68 79 70 72 69 6f 74 0d 00 0d 00 6c 73
0d 00 0d 00 6d 6b 64 69 72 20 74 65 6c 6e 65 74 74
0d 00 63 64 20 74 65 6c 09 74 0d 00 6c 6c 0d 00 6c
73 0d 00 76 69 20 6c 6f 67 2d 66 69 6c 65 2e 6c 6f
67 0d 00 74 65 73 74 69 74 65 73 74 20 ...
```

Capture Telnet traffic ✓

Parse Telnet payload

Extract typing characteristics

Compare with the admin profile

Telnet protocol

```
ff fb 25 ff fd 03 ff fb 18 ff fb 1f ff fb 20 ff fb
21 ff fb 22 ff fb 27 ff fd 05 ff fc 23 ff fa 1f 00
c5 00 34 ff f0 ff fa 20 00 33 38 34 30 30 2c 33 38
34 30 30 ff f0 ff fa 27 00 00 55 53 45 52 01 73 69
6d 69 ff f0 ff fa 18 00 58 54 45 52 4d 2d 32 35 36
43 4f 4c 4f 52 ff f0 ff fc 01 ff fd 01 70 69 72 61
74 65 0d 00 68 79 70 72 69 6f 74 0d 00 0d 00 6c 73
0d 00 0d 00 6d 6b 64 69 72 20 74 65 6c 6e 65 74 74
0d 00 63 64 20 74 65 6c 09 74 0d 00 6c 6c 0d 00 6c
73 0d 00 76 69 20 6c 6f 67 2d 66 69 6c 65 2e 6c 6f
67 0d 00 74 65 73 74 69 74 65 73 74 20 ...
```

Capture Telnet traffic ✓

Parse Telnet payload

Extract typing characteristics

Compare with the admin profile

Telnet protocol

```
ff fb 25 ff fd 03 ff fb 18 ff fb 1f ff fb 20 ff fb
21 ff fb 22 ff fb 27 ff fd 05 ff fc 23 ff fa 1f 00
c5 00 34 ff f0 ff fa 20 00 33 38 34 30 30 2c 33 38
34 30 30 ff f0 ff fa 27 00 00 55 53 45 52 01 73 69
6d 69 ff f0 ff fa 18 00 58 54 45 52 4d 2d 32 35 36
43 4f 4c 4f 52 ff f0 ff fc 01 ff fd 01 70 69 72 61
74 65 0d 00 68 79 70 72 69 6f 74 0d 00 0d 00 6c 73
0d 00 0d 00 6d 6b 64 69 72 20 74 65 6c 6e 65 74 74
0d 00 63 64 20 74 65 6c 09 74 0d 00 6c 6c 0d 00 6c
73 0d 00 76 69 20 6c 6f 67 2d 66 69 6c 65 2e 6c 6f
67 0d 00 74 65 73 74 69 74 65 73 74 20 ...
```

Capture Telnet traffic ✓

Parse Telnet payload

Extract typing characteristics

Compare with the admin profile

Telnet protocol

```
70 69 72 61 74 65 0d 00 68 79 70 72 69 6f 74 0d 00
0d 00 6c 73 0d 00 0d 00 6d 6b 64 69 72 20 74 65 6c
6e 65 74 74 0d 00 63 64 20 74 65 6c 09 74 0d 00 6c
6c 0d 00 6c 73 0d 00 76 69 20 6c 6f 67 2d 66 69 6c
65 2e 6c 6f 67 0d 00 74 65 73 74 69 74 65 73 74 20
74 69 74 1b 1b 1b 5a 5a 1b 5b 41 0d 00 69 74 65 73
74 20 73 74 61 72 74 3a 20 1b 21 21 64 61 74 65 0d
00 69 74 65 73 74 20 73 74 61 72 74 3a 20 1b 4f 42
7f 1b 5a 5a 0d 00 0d 00 68 6f 73 74 6e 61 6d 65 20
6d 79 64 65 76 69 63 65 0d 00 73 75 64 6f 20 68 6f
73 74 6e 61 6d 65 20 6d 79 64 65 76 69 63 65 0d 00
0d 00 6e 65 74 73 74 61 74 0d 00 76 69 ...
```

Capture Telnet traffic ✓

Parse Telnet payload

Extract typing characteristics

Compare with the admin profile

Telnet protocol

```
70 69 72 61 74 65 0d 00 68 79 70 72 69 6f 74 0d 00
0d 00 6c 73 0d 00 0d 00 6d 6b 64 69 72 20 74 65 6c
6e 65 74 74 0d 00 63 64 20 74 65 6c 09 74 0d 00 6c
6c 0d 00 6c 73 0d 00 76 69 20 6c 6f 67 2d 66 69 6c
65 2e 6c 6f 67 0d 00 74 65 73 74 69 74 65 73 74 20
74 69 74 1b 1b 1b 5a 5a 1b 5b 41 0d 00 69 74 65 73
74 20 73 74 61 72 74 3a 20 1b 21 21 64 61 74 65 0d
00 69 74 65 73 74 20 73 74 61 72 74 3a 20 1b 4f 42
7f 1b 5a 5a 0d 00 0d 00 68 6f 73 74 6e 61 6d 65 20
6d 79 64 65 76 69 63 65 0d 00 73 75 64 6f 20 68 6f
73 74 6e 61 6d 65 20 6d 79 64 65 76 69 63 65 0d 00
0d 00 6e 65 74 73 74 61 74 0d 00 76 69 ...
```

Capture Telnet traffic ✓

Parse Telnet payload

Extract typing characteristics

Compare with the admin profile

Telnet protocol

```
70 69 72 61 74 65
68 79 70 72 69 6f 74
6c 73
6d 6b 64 69 72 20 74 65 6c 6e 65 74 74
63 64 20 74 65 6c 09 74
6c 6c 7f 73
76 69 20 6c 6f 67 2d 66 69 6c 65 2e 6c 6f 67
1b 5a 5a 5b 41
...
```

Capture Telnet traffic ✓

Parse Telnet payload

Extract typing characteristics

Compare with the admin profile

Telnet protocol

```
70 69 72 61 74 65
68 79 70 72 69 6f 74
6c 73
6d 6b 64 69 72 20 74 65 6c 6e 65 74 74
63 64 20 74 65 6c 09 74
6c 6c 7f 73
76 69 20 6c 6f 67 2d 66 69 6c 65 2e 6c 6f 67
1b 5a 5a 5b 41
...
```

Capture Telnet traffic ✓

Parse Telnet payload

Extract typing characteristics

Compare with the admin profile

Telnet protocol

```
70 69 72 61 74 65
68 79 70 72 69 6f 74
6c 73
6d 6b 64 69 72 20 74 65 6c 6e 65 74 74
63 64 20 74 65 6c 09 74
6c 73
76 69 20 6c 6f 67 2d 66 69 6c 65 2e 6c 6f 67
1b 5a 5a 5b 41
...
```

Capture Telnet traffic ✓

Parse Telnet payload

Extract typing characteristics

Compare with the admin profile

Telnet protocol

```
70 69 72 61 74 65
68 79 70 72 69 6f 74
6c 73
6d 6b 64 69 72 20 74 65 6c 6e 65 74 74
63 64 20 74 65 6c 09 74
6c 73
76 69 20 6c 6f 67 2d 66 69 6c 65 2e 6c 6f 67
1b 5a 5a 5b 41
...
```

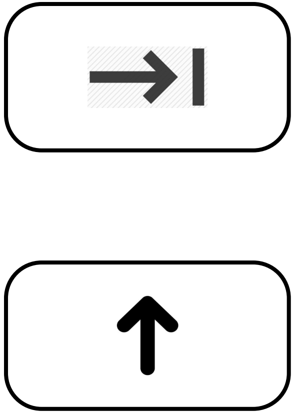
Capture Telnet traffic

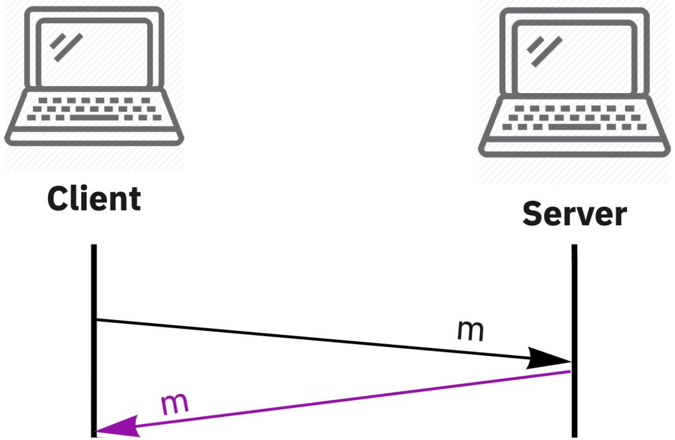
Parse Telnet payload

Extract typing characteristics

Compare with the admin profile

Telnet protocol





Capture Telnet traffic ✓

Parse Telnet payload

Extract typing characteristics

Compare with the admin profile

Telnet protocol

```
70 69 72 61 74 65
68 79 70 72 69 6f 74
6c 73
6d 6b 64 69 72 20 74 65 6c 6e 65 74 74
63 64 20 74 65 6c 09 74
6c 73
76 69 20 6c 6f 67 2d 66 69 6c 65 2e 6c 6f 67
1b 5a 5a 5b 41
...
```

Capture Telnet traffic

Parse Telnet payload

Extract typing characteristics

Compare with the admin profile

Telnet protocol

```
70 69 72 61 74 65

68 79 70 72 69 6f 74

6c 73

6d 6b 64 69 72 20 74 65 6c 6e 65 74 74

63 64 20 74 65 6c 6e 65 74 74

6c 73

76 69 20 6c 6f 67 2d 66 69 6c 65 2e 6c 6f 67

1b 5a 5a

76 69 20 6c 6f 67 2d 66 69 6c 65 2e 6c 6f 67
```

Capture Teln tra c ✓

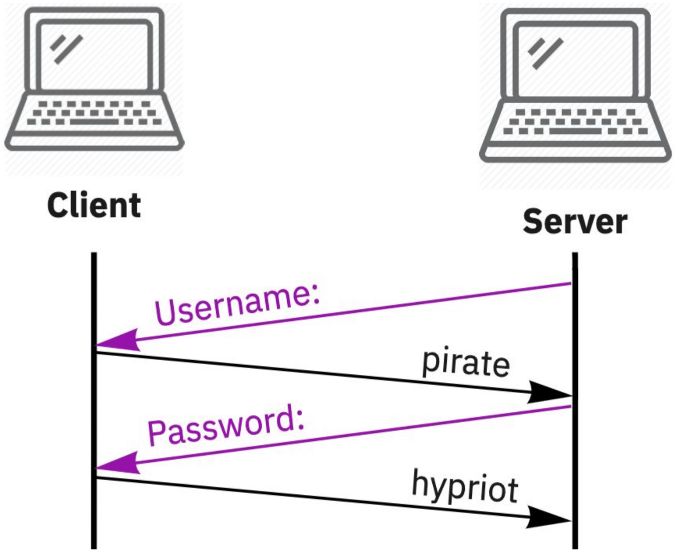
Parse Telnet pay d ✓

Extract typing characteristics

Compare with the admin profile

Telnet protocol

```
pirate
hypriot
---------------------
ls
mkdir telnett
cd telnett
ls
vi log-file.log
[ESC] ZZ
vi log-file.log
```



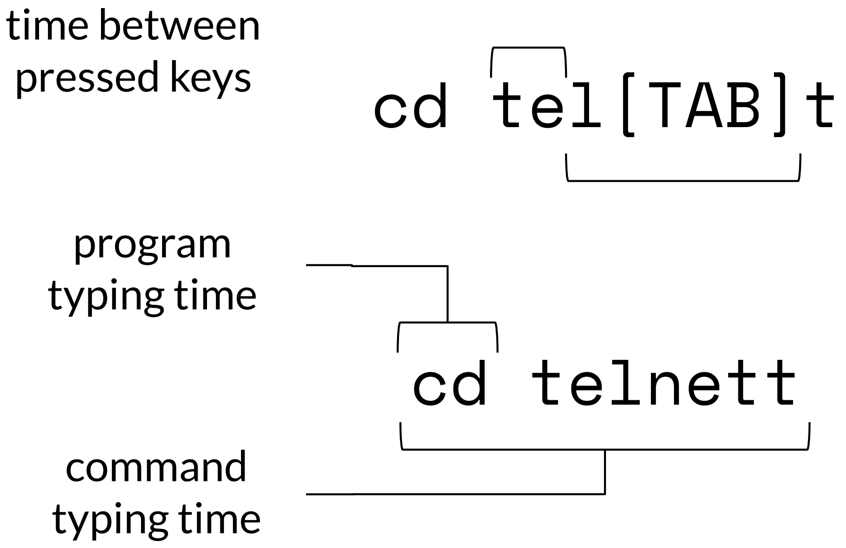
Capture Telnet traffic ✓

Parse Telnet payload ✓

Extract typing characteristics

Compare with the admin profile

Typing times



time between pressed keys

cd tel[TAB]t

program typing time

cd telnett

command typing time

Capture Telne ✓
tra

Parse Telnet ✓
pay

Extract typing characteristics

Compare with the admin profile

Special bytes

typos:	`BACKSPACE / DELETE`
new lines:	`ENTER`
autofilling:	`ARROWS / TAB`
other:	`ESC`

Capture Telnet traffic ✓

Parse Telnet payload ✓

Extract typing characteristics

Compare with the admin profile

Credentials

username

****

username

****

- → the order
- → the histogram
- → how the user typed
- → what the user sent

Capture Telnet traffic ✓

Parse Telnet payload ✓

Extract typing characteristics

Compare with the admin profile

Commands

`commands`

`programs`

→ the order

→ how the user typed

→ what the user sent

→ VI detection

Capture Telnet traffic ✓

Parse Telnet payload ✓

Extract typing characteristics ✓

Compare with the admin profile

Session data

When?

- ➔ the day of week
- ➔ the time in the day

Where from?

- ➔ the IP address
- ➔ geo location

Duration

- ➔ time
- ➔ sent bytes

State

- ➔ login attempts

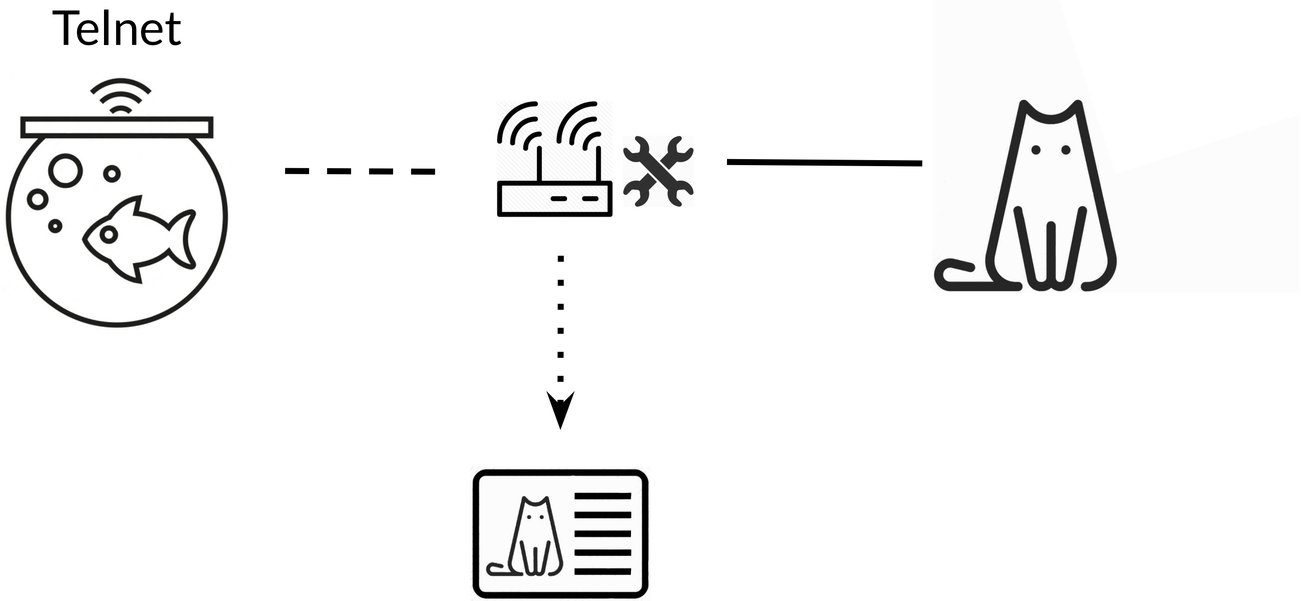
Capture Telnet traffic ✓

Parse Telnet payload ✓

Extract typing characteristics ✓

Compare with the admin profile

Profile of the admin



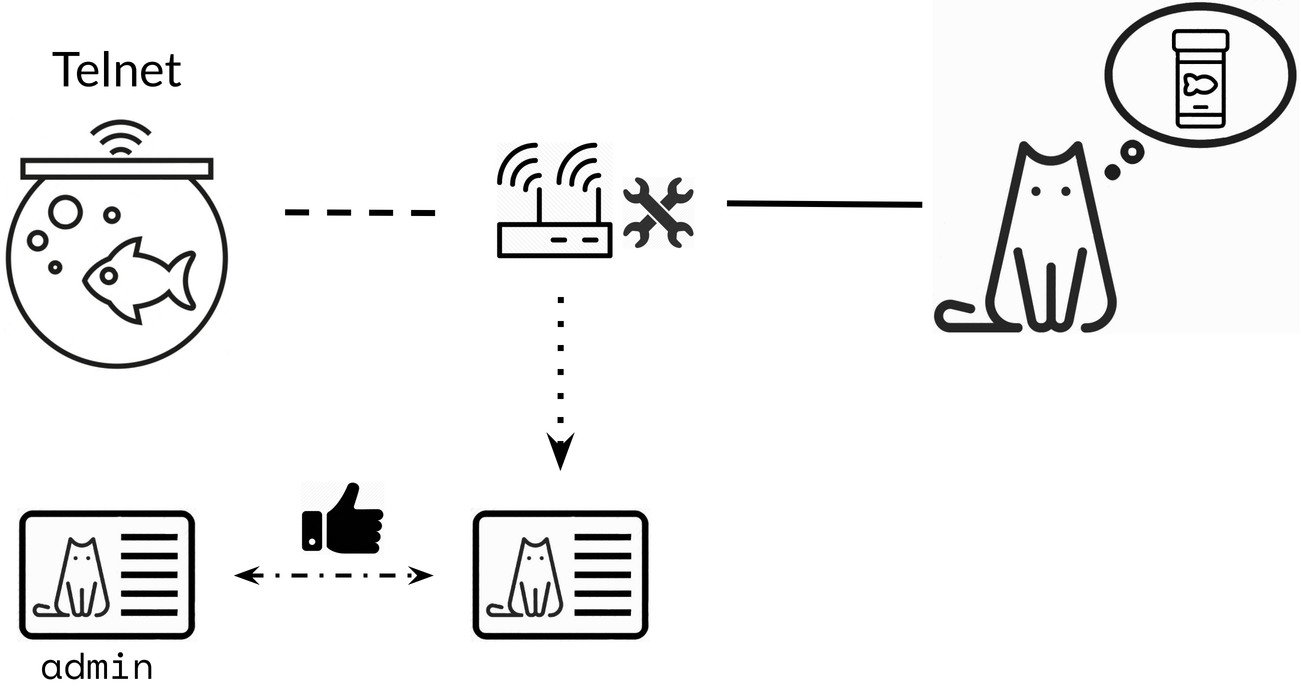
Capture Telnet traffic ✓

Parse Telnet payload ✓

Extract typing characteristics ✓

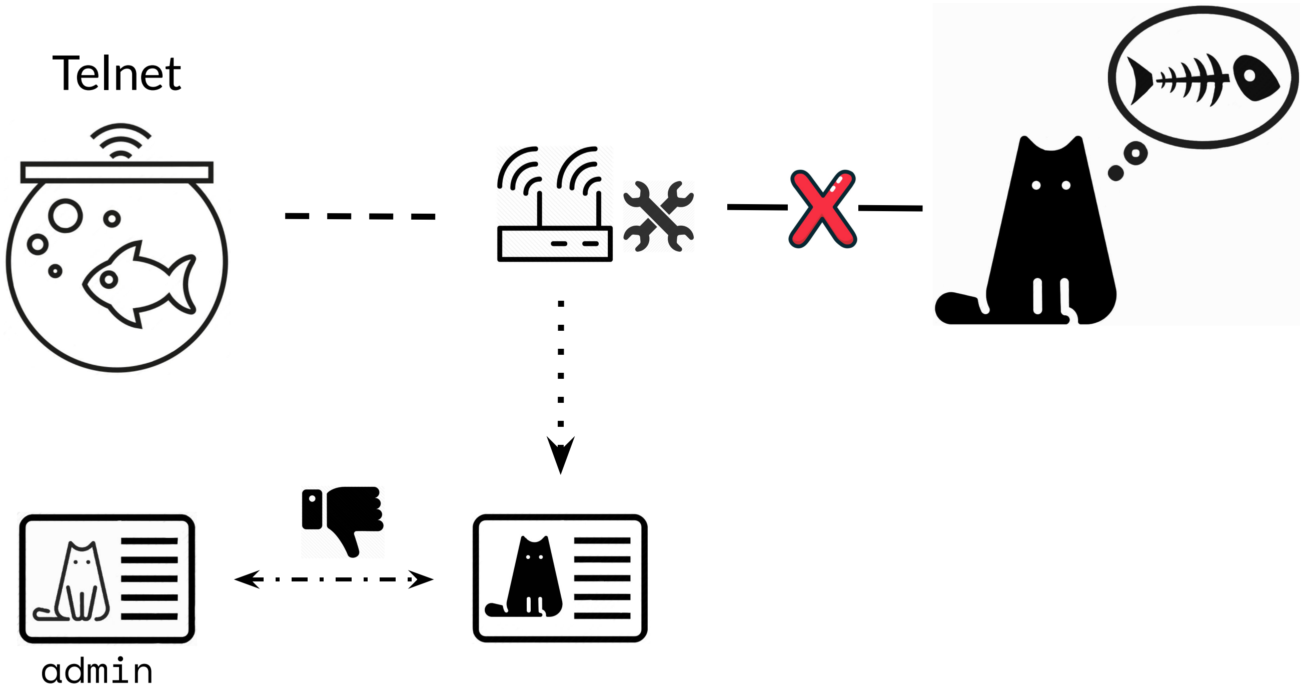
Compare with the admin profile

New incoming session



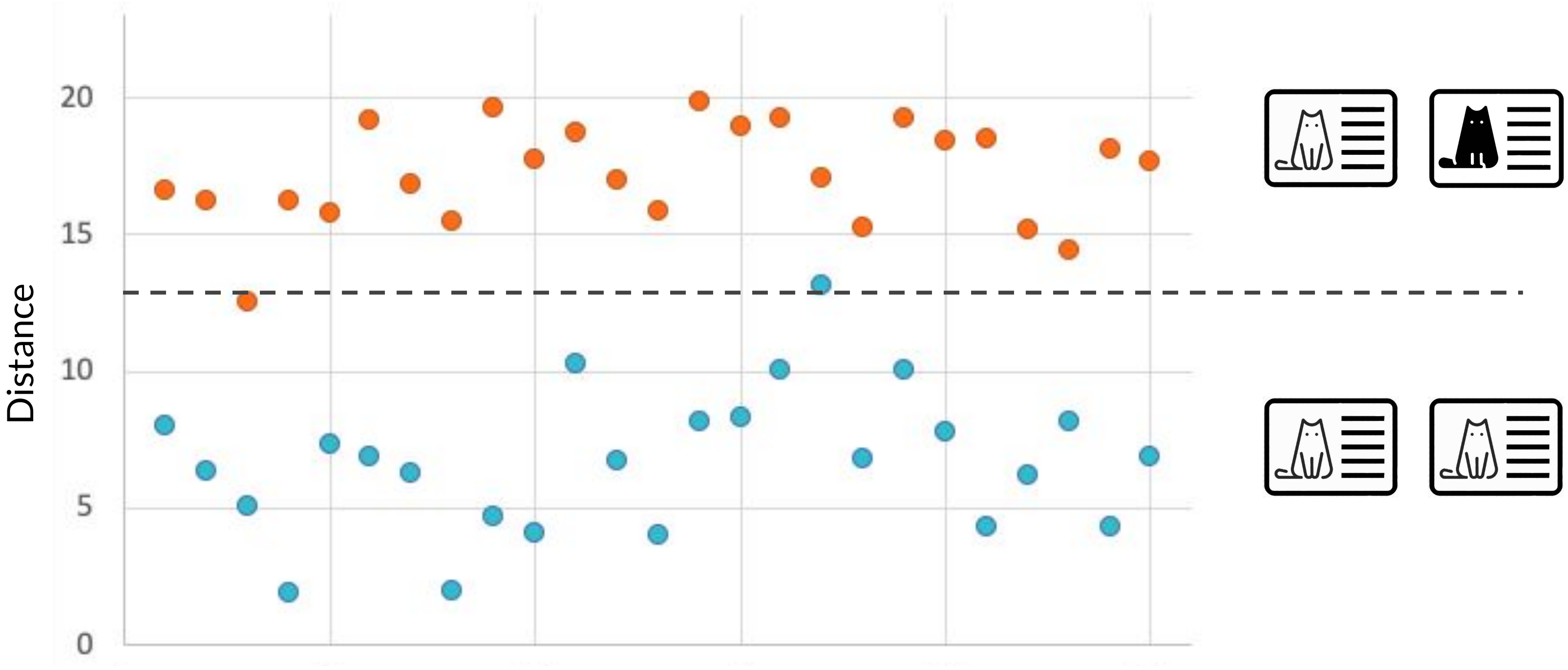
- Capture Telnet traffic ✓
- Parse Telnet payload ✓
- Extract typing characteristics ✓
- Compare with the admin profile ✓

New incoming session

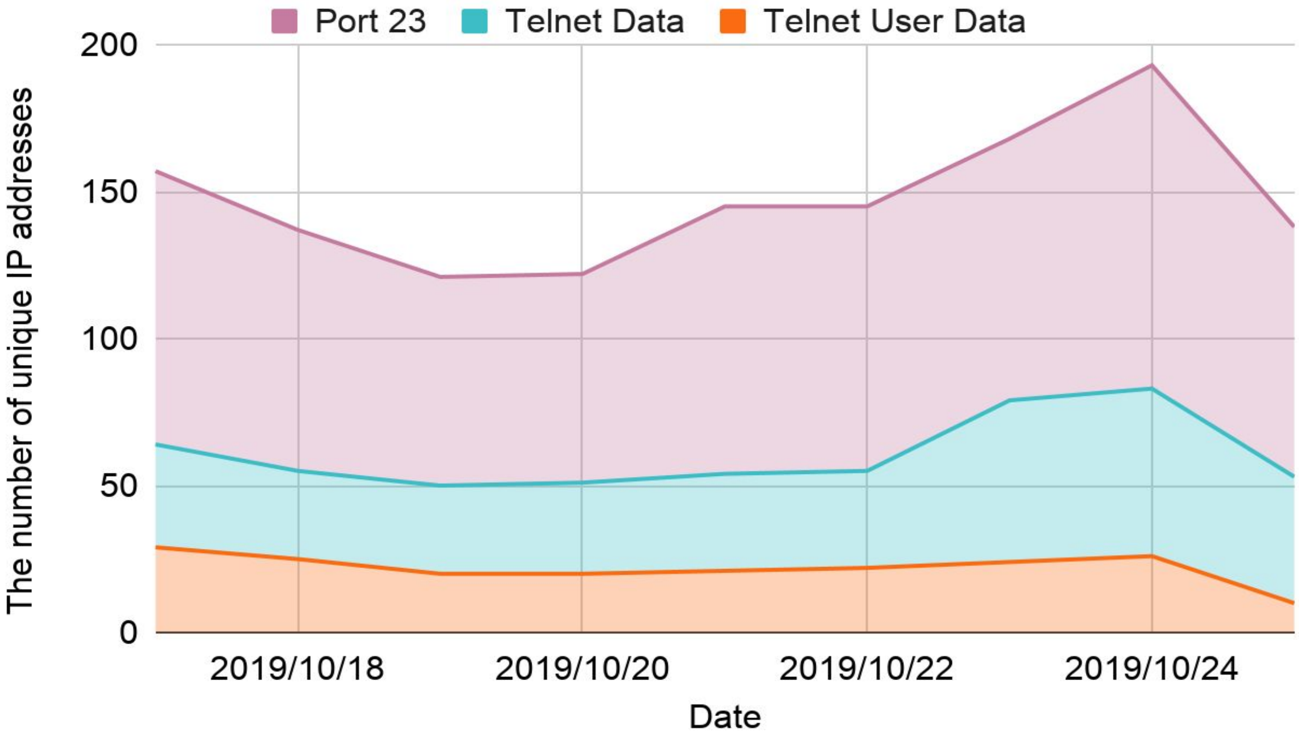


Results

Compare User Profiles



Connections to Telnet server



Conclusions

➔ Behavioral detection is possible

➔ Protection of IoT devices can be done better

> “Cybersecurity is a shared responsibility. The more systems we secure, the more secure we all are.”
>
> Jeh Johnson

Q&A

When A Password Is Not Enough

Developing A New Way Of Protecting Smart Homes

Simona Musilova | @siimi_m_