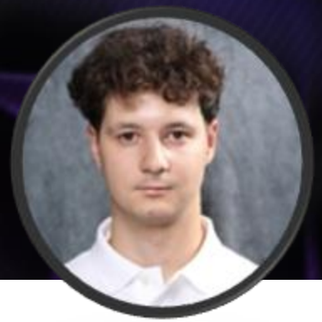
black hat BRIEFINGS
DECEMBER 10-11, 2025
EXCEL LONDON / UNITED KINGDOM

Ghosts in the Stream: Exposing Lives and Devices Behind Encrypted Doors

Speakers: Kristopher Schlett, Béla Genge

Contributors: Ioan Pădurean, Savio Sciancalepore



Kristopher SCHLETT

Masters' Student

Vulnerability research

TU/e EINDHOVEN UNIVERSITY OF TECHNOLOGY

Béla GENGE

Senior Security Researcher

IoT security, vulnerability research

Bitdefender

Ioan PĂDUREAN

Junior Security Researcher

Applied ML techniques, IoT security

Bitdefender

Savio SCIANCALEPORE*

Senior Assistant Professor

TU/e EINDHOVEN UNIVERSITY OF TECHNOLOGY

Most of this research was conducted as part of Mr. Schlett MSc thesis under joint supervision between Bitdefender and Eindhoven University of Technology (TU Eindhoven). The research topic was provided by Bitdefender as part of an industry-academia collaboration. The section concerning machine learning was developed exclusively by Bitdefender.

*Author of the photo: Mrs. Angeline Swinkels

Agenda

1. Introduction & the why?

2. Fundamental concepts

3. Our setup: from baby steps to full office setup

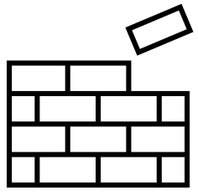
4. The fun part: exposing semantics behind encryption: **loss of privacy**

5. Possible fixes, conclusions & key takeaways

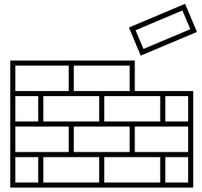
Introduction & motivation

The rising star of IoT technology

matter



Interoperability



Mandatory security

Everybody is (in) Matter

matter

- Global collaboration (**600+**):
  - 32 promoters
  - 279 participants
  - 284 adopters

- Device certification programs aligned with several directives

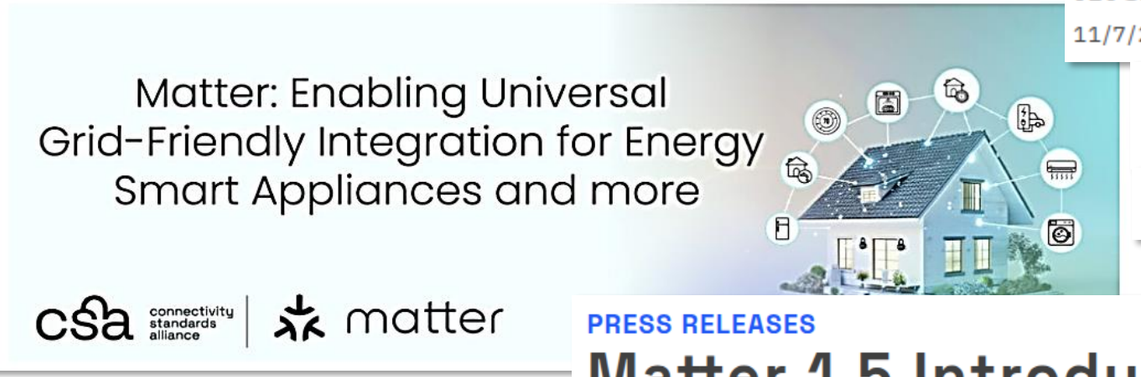
Matter is becoming
the (single?)
established standard for IoT

Matter progress

BLOGS

Matter: Enabling Universal Grid-Friendly Integration for Energy Smart Appliances and more

10/1/2024



PRESS RELEASES

Matter 1.4 Enables More Capable Smart Homes

11/7/2024

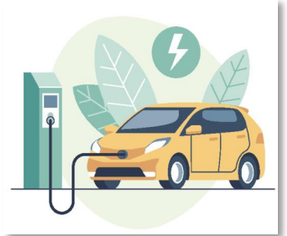
Enhanced Network Infrastructure with Home Routers and Access Points (HRAP)

New Energy Device Types and Capabilities

PRESS RELEASES

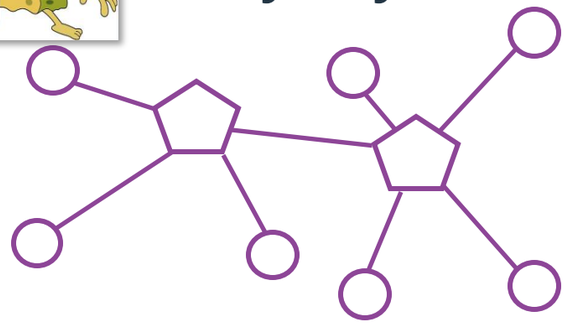
Matter 1.5 Introduces Cameras, Closures, and Enhanced Energy Management Capabilities

11/20/2025



The perspective: IoT progress

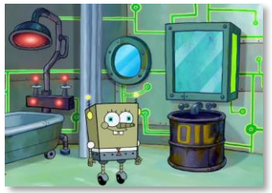
Early days



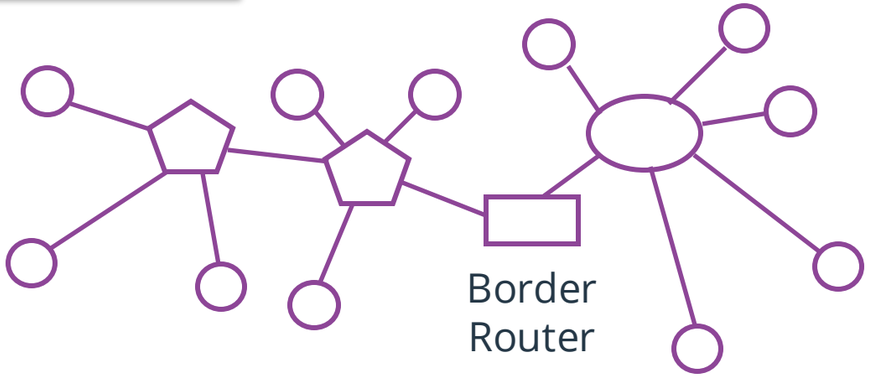
Optional security

One network-wide symmetric key

VS



Today



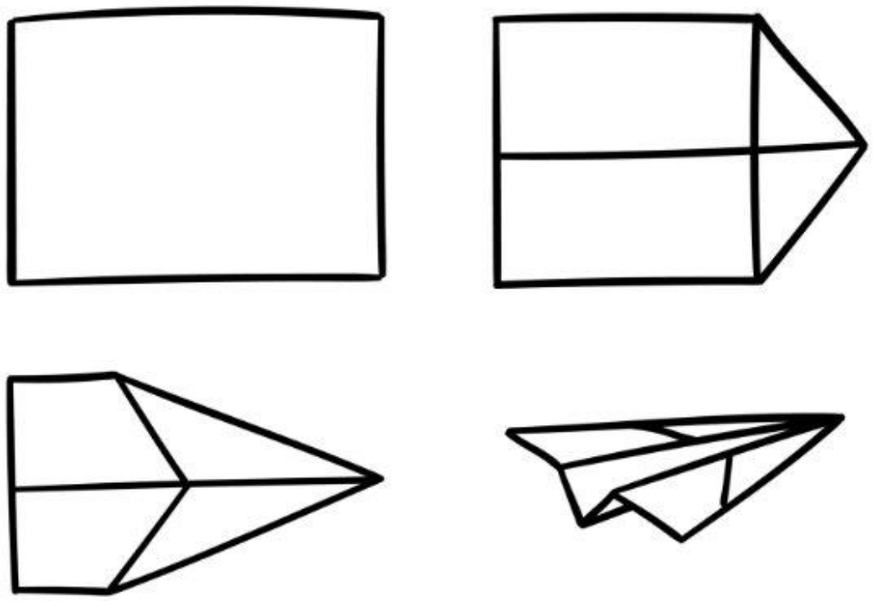
Mandatory security

Symmetric session keys

Fabric-specific certificates

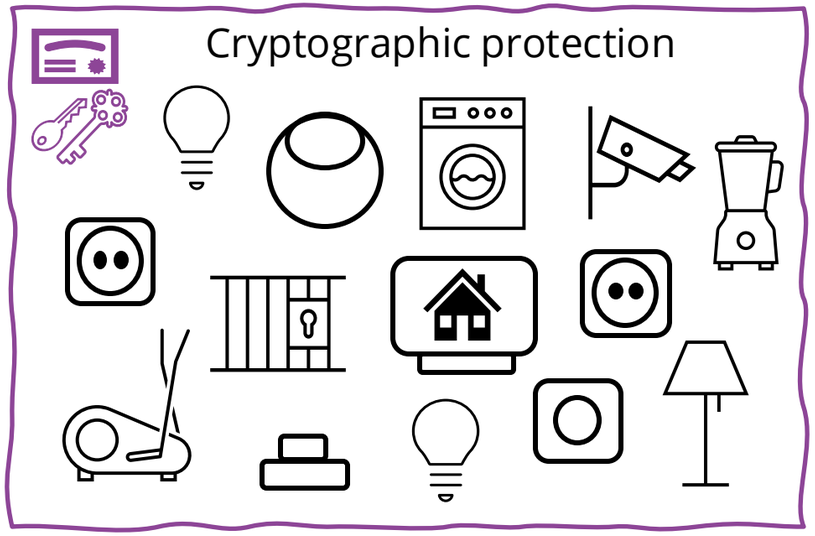
Key exchange algorithms

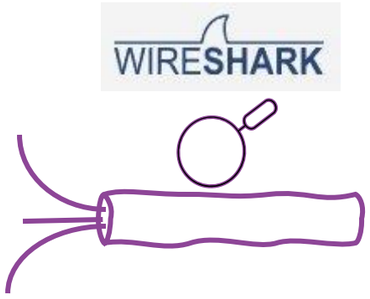
Ephemeral asymmetric keys



On paper, everything looks good!

Our job: looking at the traffic





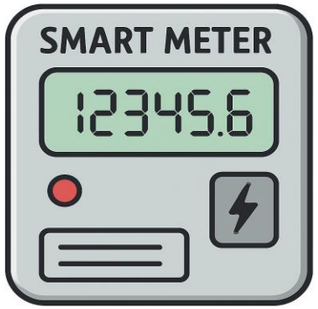

```
Matter                96 5540 → 59065 Len=34
Matter               135 5540 → 59065 Len=73
Matter               104 59065 → 5540 Len=42
Matter                96 5540 → 59065 Len=34
Matter               121 59065 → 5540 Len=59
Matter               129 5540 → 59065 Len=67
Matter                96 59065 → 5540 Len=34
Matter               135 5540 → 59065 Len=73
Matter               104 59065 → 5540 Len=42
Matter                96 5540 → 59065 Len=34
Matter               121 59065 → 5540 Len=59
Matter               129 5540 → 59065 Len=67
Matter                96 59065 → 5540 Len=34
Matter               291 5540 → 59065 Len=229
Matter               104 59065 → 5540 Len=42
Matter                96 5540 → 59065 Len=34
Matter               262 5540 → 59065 Len=200
Matter               104 59065 → 5540 Len=42
Matter                96 5540 → 59065 Len=34
Matter               135 5540 → 59065 Len=73
Matter               104 59065 → 5540 Len=42
Matter                96 5540 → 59065 Len=34
Matter               135 5540 → 59065 Len=73
Matter               104 59065 → 5540 Len=42
```

... started seeing "Ghosts"




34, 73, 42, 34, 59, 67, 34, 73, 42, 34, 59, 67, 34, 229, 42, 34, 200,
42, 34, 73, 42, 34, 73, 42


Déjà vu



Compromised through Compression

Privacy Implications of Smart Meter Traffic Analysis

Pol Van Aubel and Erik Poll

Digital Security group, Institute for Computing & Information Sciences
Radboud University, the Netherlands
pol.vanaubel@cs.ru.nl erikpoll@cs.ru.nl

How to Find out What's Going on in Encrypted Smart Meter Networks - without Decrypting Anything

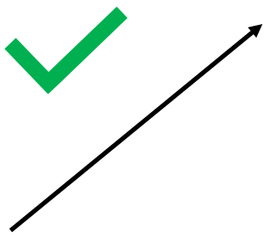
Oliver Eigner, Department of Computer Science and Security, St. Pölten University of Applied Sciences, Austria, oliver.eigner@fhstp.ac.at
Hubert Schölnast, Department of Computer Science and Security, St. Pölten University of Applied Sciences, Austria, hubert.schoelnast@fhstp.ac.at
Paul Tavolato, Faculty of Computer Science, University of Vienna, Austria, paul.tavolato@univie.ac.at

DOI: https://doi.org/10.1145/3664476.3670925
ARES 2024: The 19th International Conference on Availability, Reliability and Security, Vienna, Austria, July 2024

... and many other

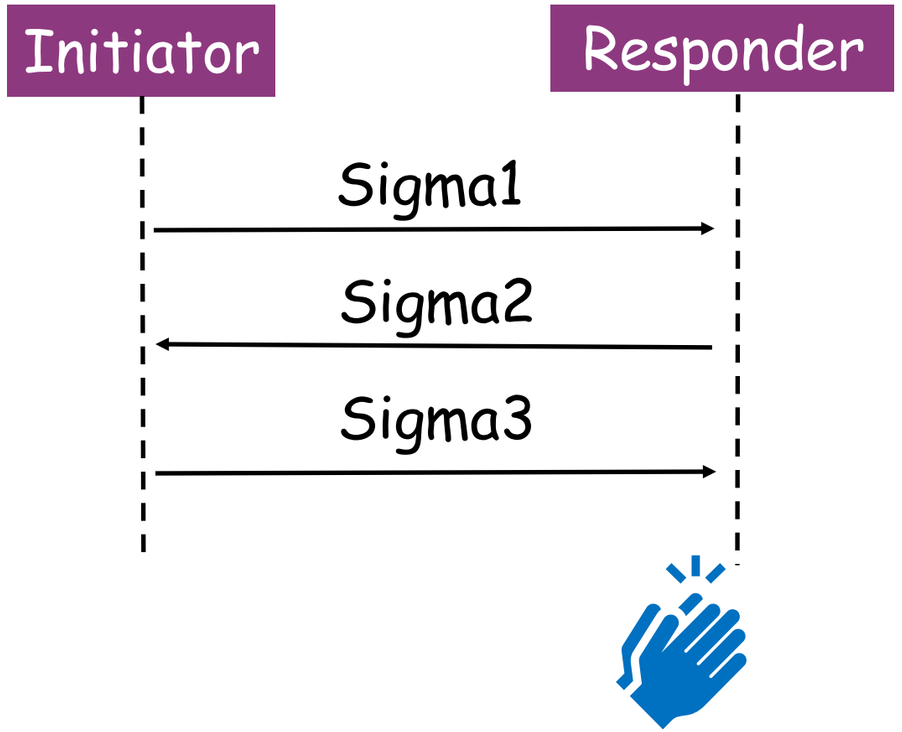
How is this possible?

Confidentiality, Integrity, Authenticity, etc.



Cryptography

Privacy



Work in Progress

Loading...

- Random resumption ID
- Ephemeral Keys
- Shared Secret
- Sign, Verify (Certs, PubKeys)
- Random numbers
- Encrypt, Decrypt (Certs, Sign)

. . .

It was supposed to solve all problems, but it didn't

(Privacy) Questions popped up

Privacy is taken seriously across **Europe** – **GDPR, CRA,** etc.

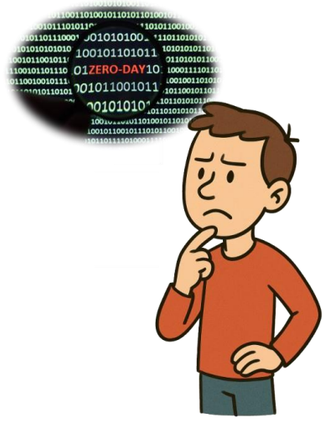
Are patterns consistent across …

… different device types?

… different device vendors?

meross Aqara SONOFF

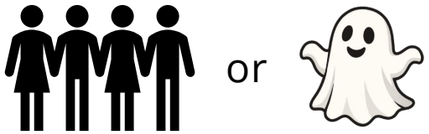
… different Matter controllers?



Can we infer …

… device type?

… user presence / absence?



… automations / dependencies?

Fundamental concepts

Strong cryptographic protection

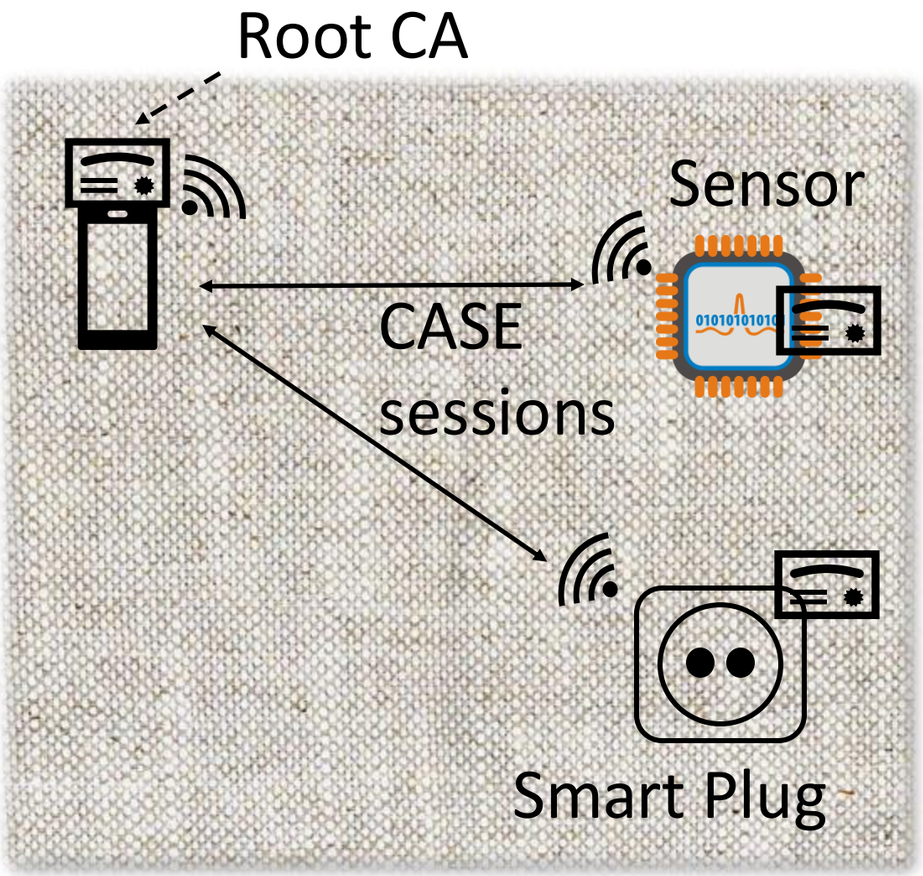
- More detailed background in a previous **Black Hat** Europe talk:

Breaking Matter: Vulnerabilities in the Matter Protocol

Bela Genge | Senior Security Researcher, Bitdefender
Ioan Padurean | Junior Software Developer, Bitdefender

https://blackhat.com/eu-24/briefings/schedule/#breaking-matter-vulnerabilities-in-the-matter-protocol-42374

- Devices are added (commissioned) into a security enclave: **Fabric**
- **Fabric:** collection of devices sharing a trusted root certificate



Matter **fabric**

What about privacy?

1. Publishing device details as part of device discovery (mDNS-SD) is optional

```
TXT: VP=4933+40962
TXT Length: 12
TXT: MIP4=0.0.0.0
TXT Length: 44
TXT: MIP6=fe80:0000:0000:0000:4ae1:e9ff:fec3:d74e
```

```
TXT Length: 8
TXT: SII=3300
TXT Length: 8
TXT: SAI=1100
TXT Length: 3
TXT: T=0
```

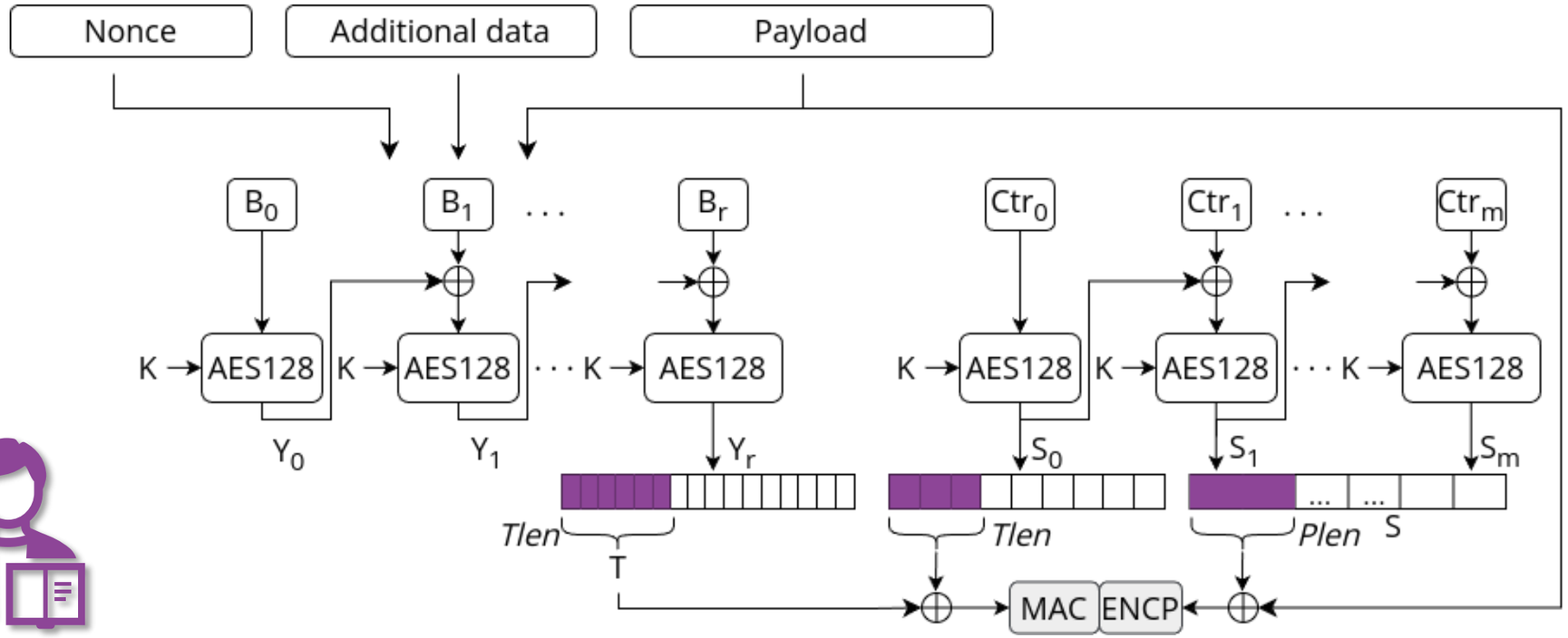
?

2. Matter CASE protocol started versioning only from standard version 1.3

3. Traffic is encrypted

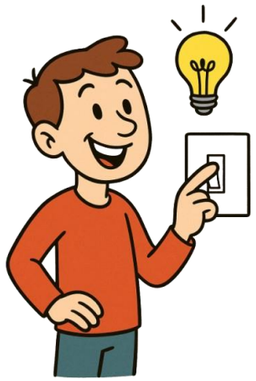
How are packets encrypted?

- Matter specification version 1.4.0
- Each packet is encrypted using an AES-CCM scheme, as defined by NIST 800-38C
- At the moment, only AES 128-bit is supported

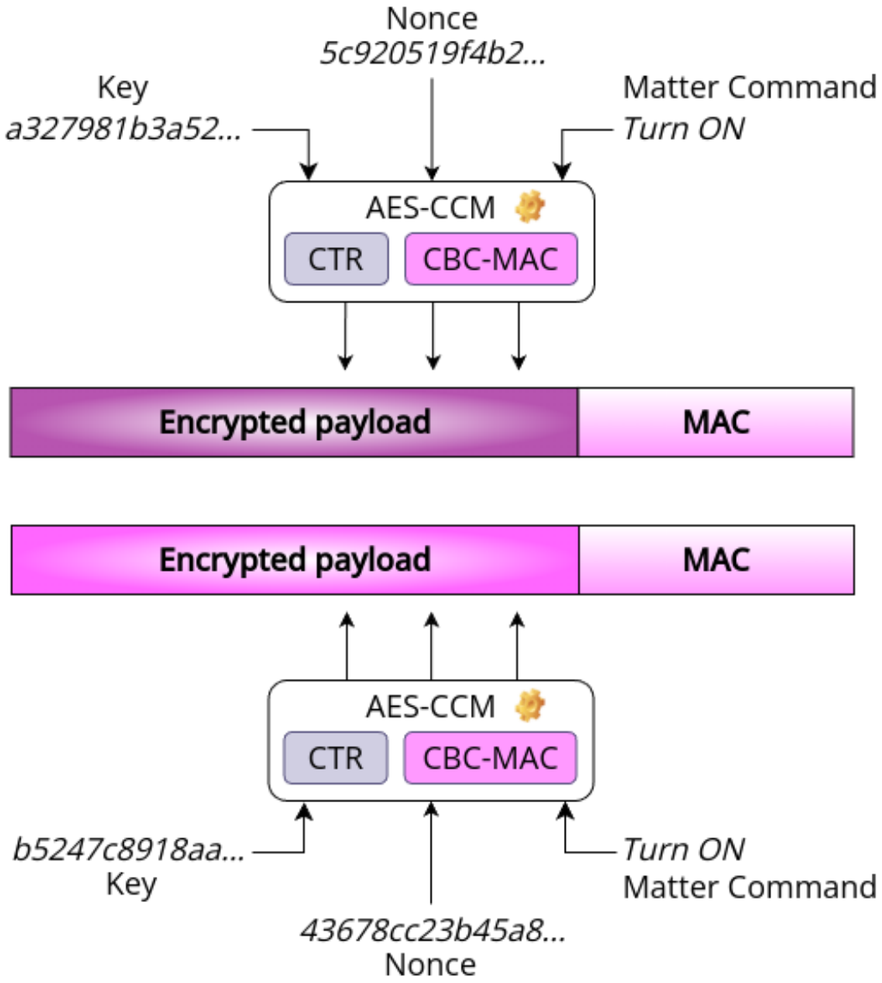


In other words …

- The same action (e.g., Matter command) will generate the same request – response sizes, and ultimately packet sizes



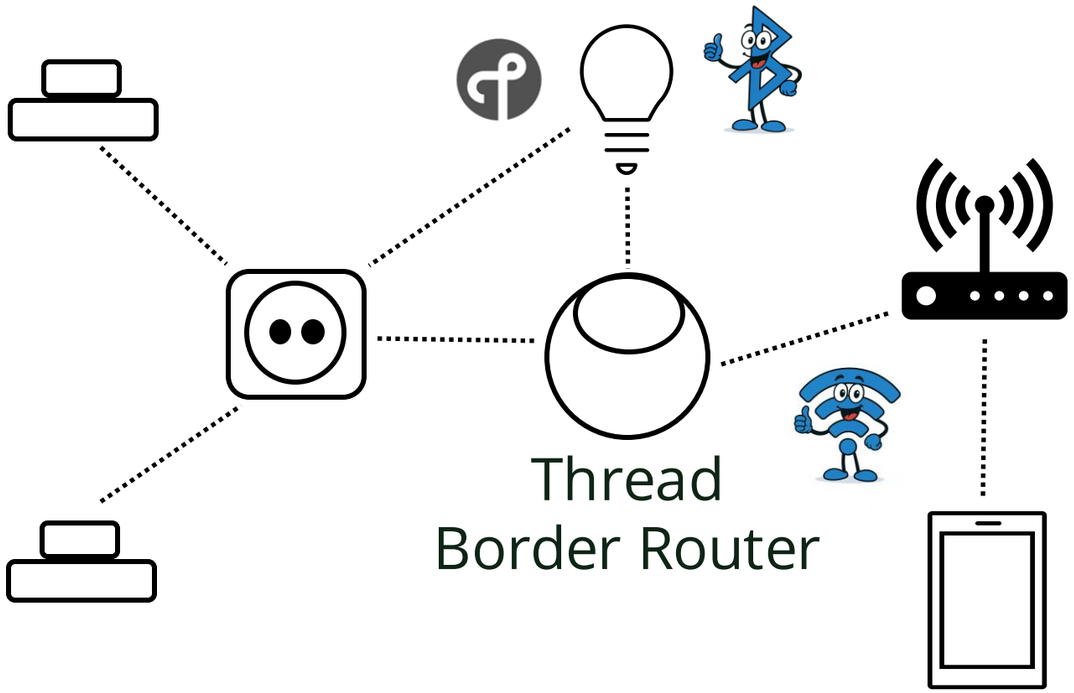
Packet size: ***Sz***

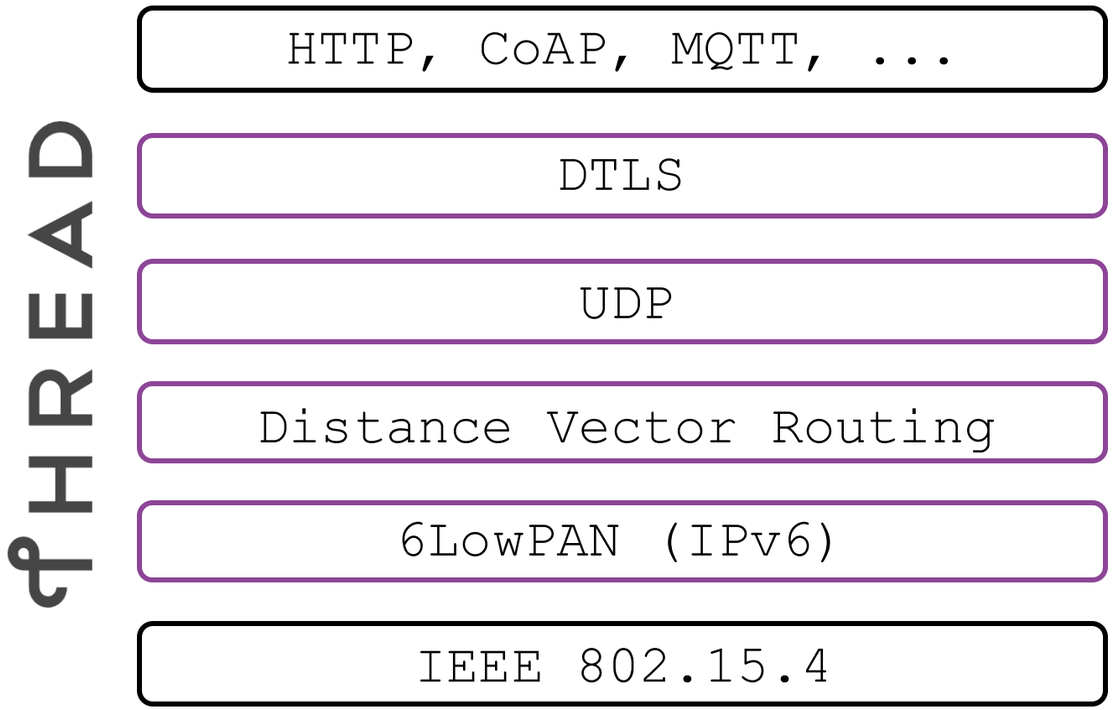


Packet size: ***Sz***

Bluetooth, Thread and Wi-Fi

- Bluetooth – initial commissioning
- Thread:
  - IPv6-based protocol for low-power, mesh networks
  - It uses 6LoWPAN/IEEE 802.15.4
- Wi-Fi – supported by many devices





Devices & technical context

Real devices

Door / window

Weather sensors

Door locks

Motion sensors

Smart plugs

Border routers / Matter controllers

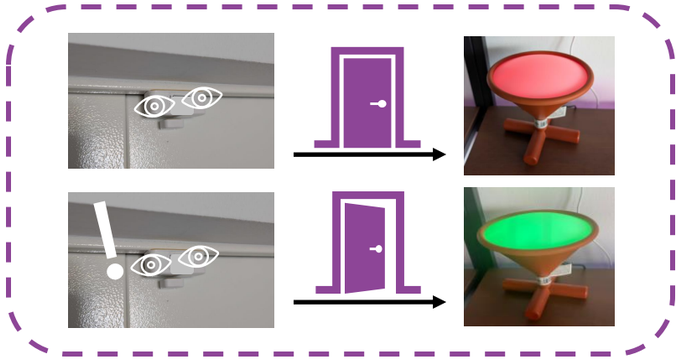
Thermostats

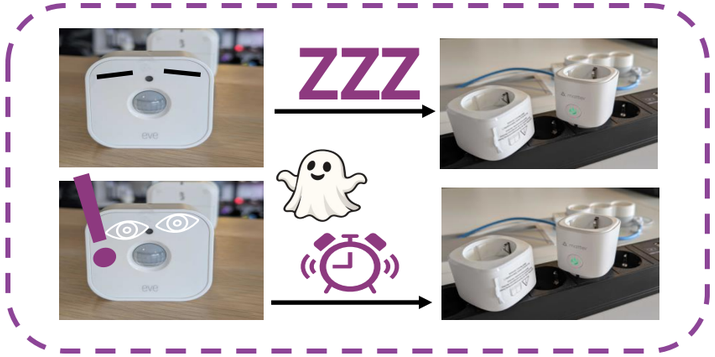
Smart light

… in a realistic setup

We have automations in a real setting!

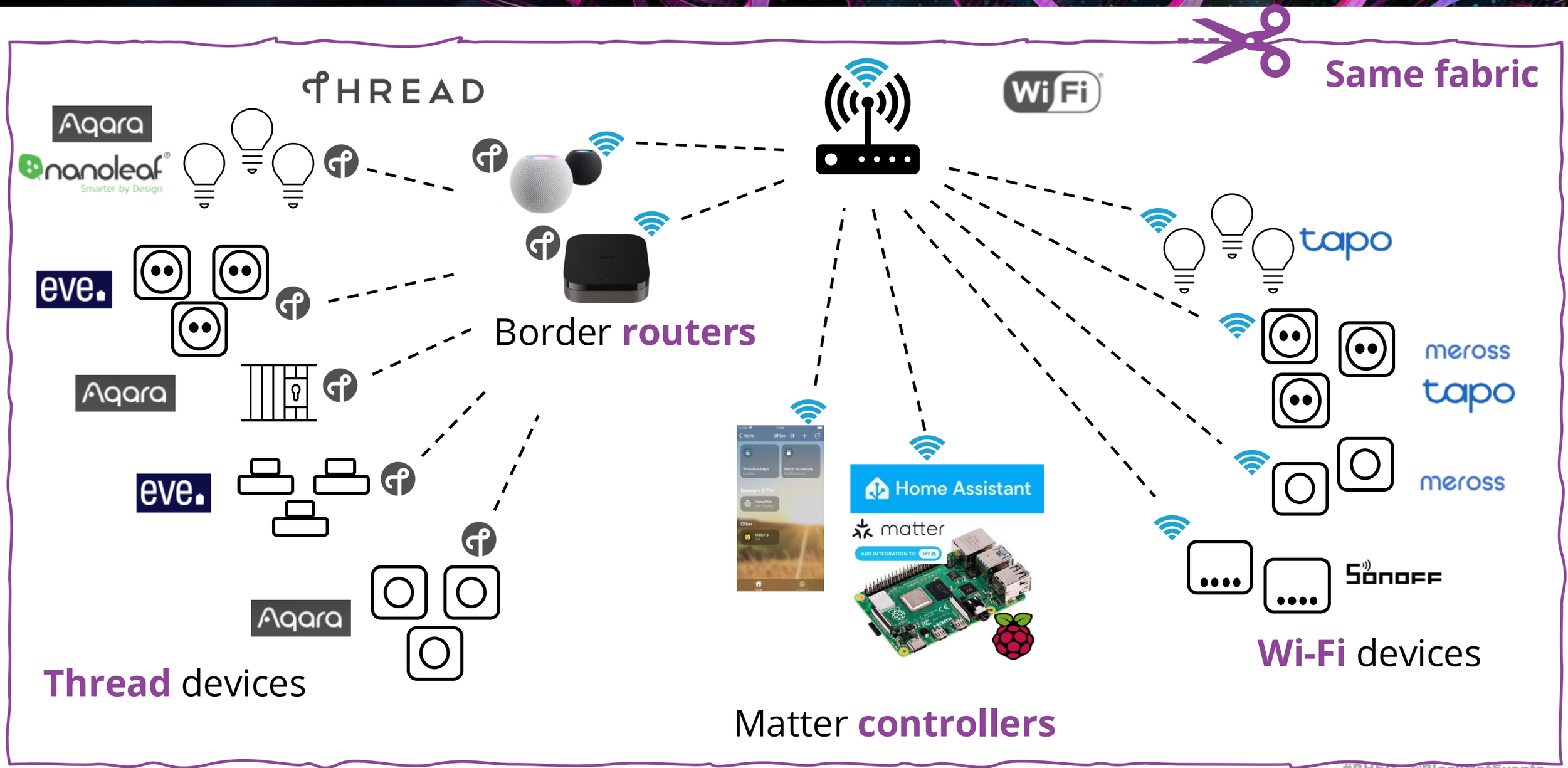
Devices and automations were configured @Bitdefender's office in Târgu Mureș, Romania!



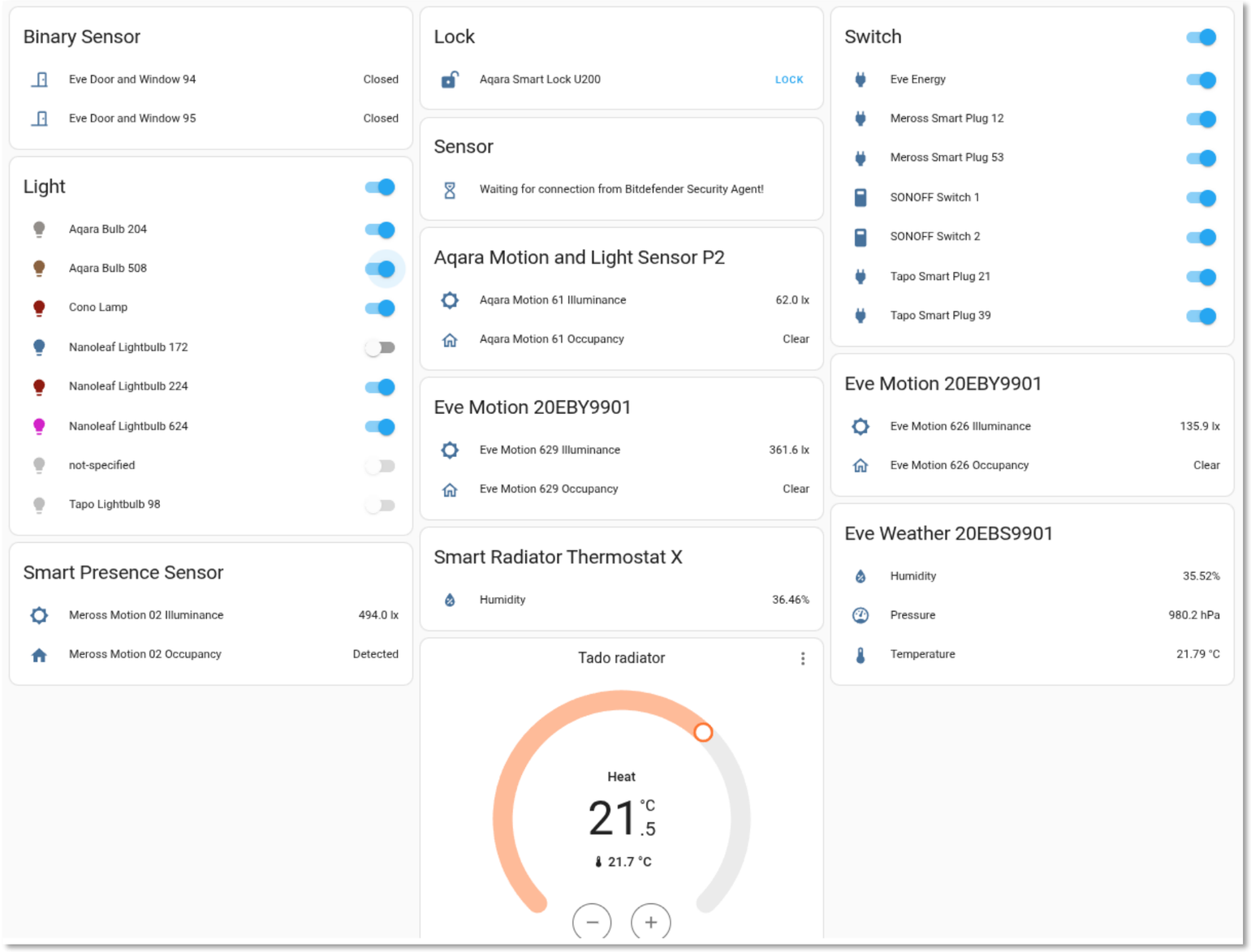


Automation: Events generated by a sensor trigger actions to be generated by other devices

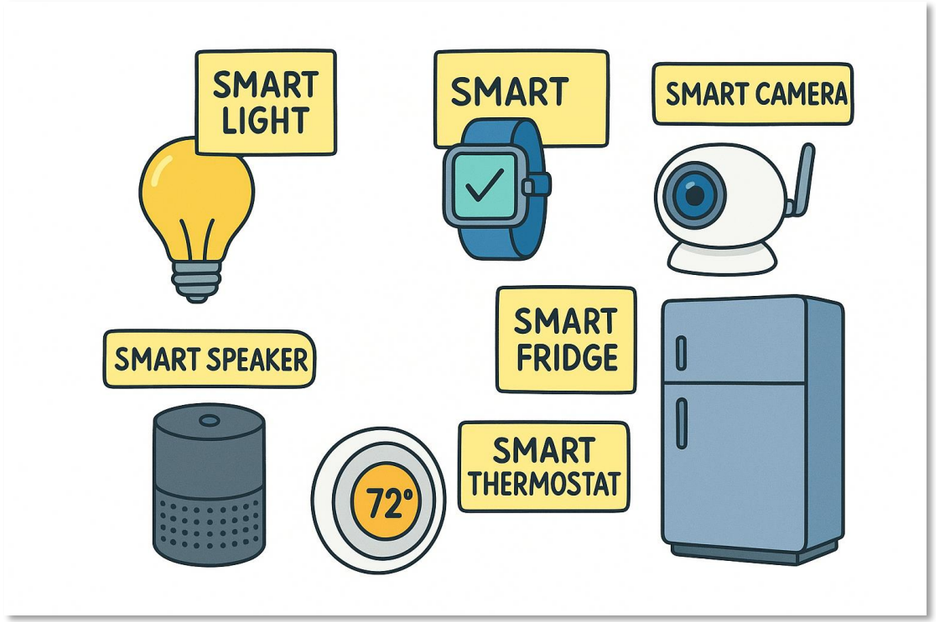
Network setup



View from Home Assistant

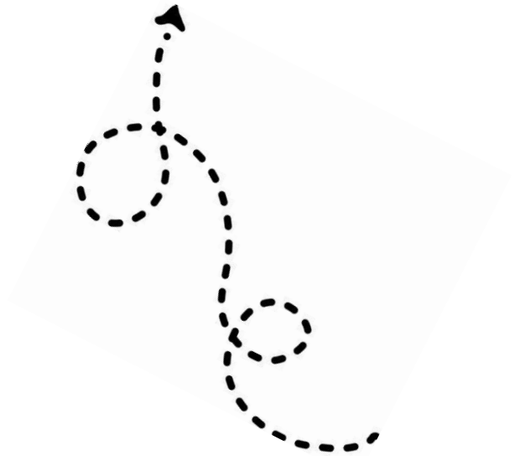


Encrypted traffic labeling



Navigating the obstacles

Joint MSc thesis between Eindhoven University of Technology & Bitdefender

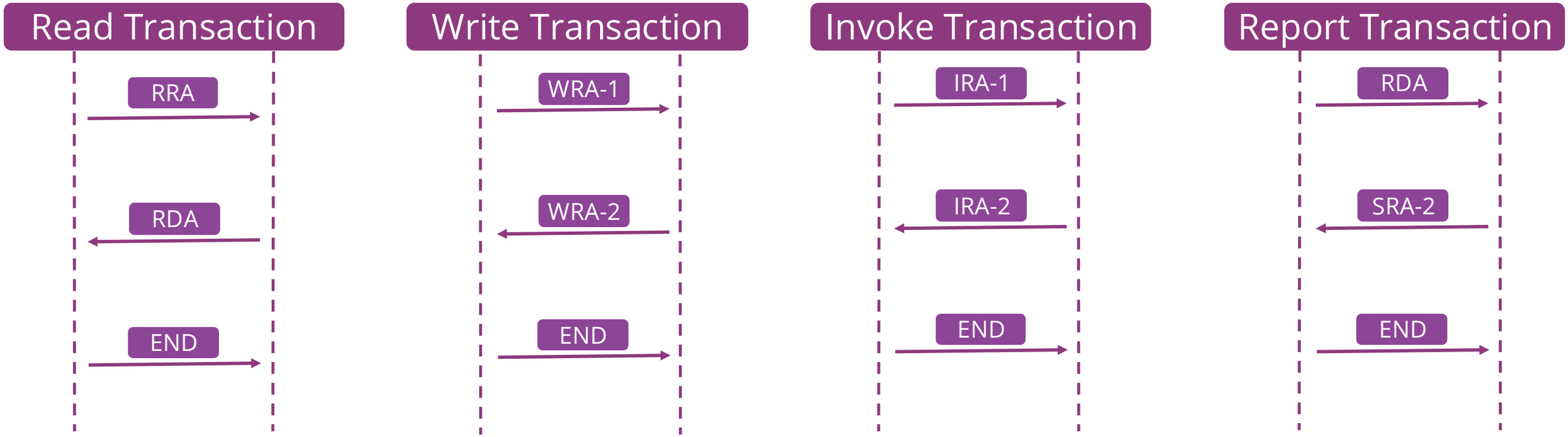


2500 km…

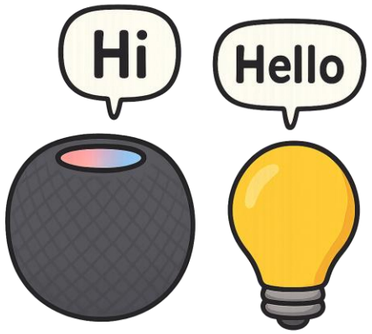
https://gisgeography.com/europe-map/

Little knowledge and seemingly endless documentation

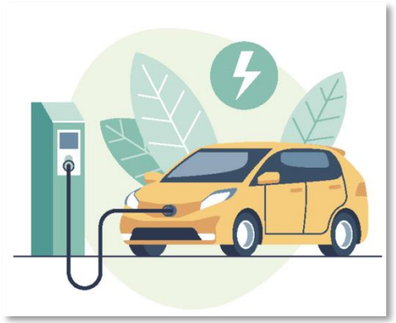
What can devices do?



RRA – Read Request Action
RDA – Report Data Action
END – End-of-sequence / Ack
WRA-1 – Write Request Action
WRA-2 – Write Response Action
IRA-1 – Invoke Request Action
IRA-2 – Invoke Response Action
SRA-2 – Status Response Action



From cute light bulb to door locks, to …



https://www.pinterest.com/pin/if-you-can-make-it-here-you-can-make-it-anywhere--503488433312230976/

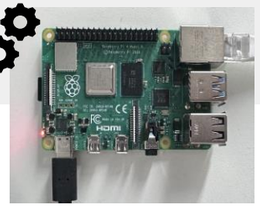
First steps were humble

Tapo
Smart Plug

Tapo
Smart Bulb

matter

Home Assistant



project-chip / connectedhomeip

Simulated
Smart Blub

project-chip / connectedhomeip

Simulated
Smart Lock

Issued request

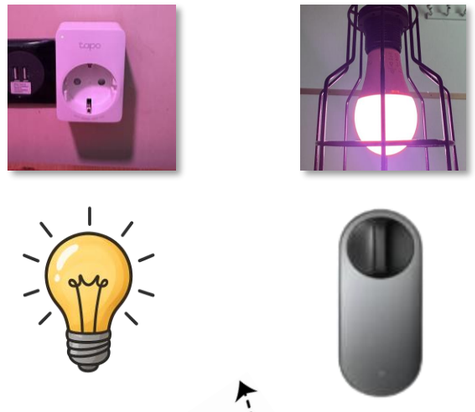
```
Matter      137 35879 → 5540  Len=75
Matter      130 5540 → 35879  Len=68
```

Received response

```
InvokeResponseMessage =
...
CommandPathIB = {
    EndpointId = 0x1,
    ClusterId = 0x6,
    CommandId = 0x1,
},
StatusIB = {
    status = 0x00 (SUCCESS),
},
...
InteractionModelRevision = 1
```

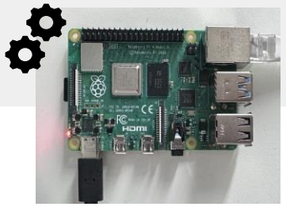
Glimpses of the Ghost

All **Devices**



matter

Home Assistant



In All cases!

WIRESHARK

```
Matter    1325540 → 35879  Len=70
Matter    10435879 → 5540  Len=42
Matter     965540 → 35879  Len=34
```

WIRESHARK

```
Matter    2095540 → 35879  Len=147
Matter    10435879 → 5540  Len=42
Matter     965540 → 35879  Len=34
```

Home Assistant **Logs**

END

```
--- Type 0000:10 (SecureChannel:StandaloneAck) (B:34)
```

SRA-2

```
--- Type 0001:01 (IM:StatusResponse) (B:42)
```

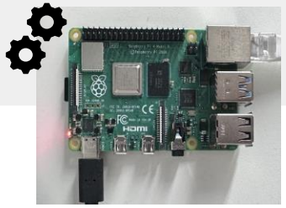
Glimpses of the Ghost

Simulated
Smart Bulb

project-chip / connectedhomeip

matter

Home Assistant



```
Matter     124 58379 → 5540 Len=62
Matter     170 5540 → 58379 Len=108
Matter      96 58379 → 5540 Len=34
```

RRA

```
-- Type 0001:02 (IM:ReadRequest)
(B:62)
AttributePathIB = {
     Endpoint = 0x0,
     Cluster = 0x28,
     Attribute = 0x0000_0001,
}
AttributePathIB = {
     Endpoint = 0x0,
     Cluster = 0x28,
     Attribute = 0x0000_0002,
}
...
```

RDA

```
--- Type 0001:05
(IM:ReportData) (B:108)
...
AttributePathIB = {
     Endpoint = 0x0,
     Cluster = 0x28,
     Attribute = 0x0000_0002,
}
Data = 65521 (unsigned),
...
AttributePathIB = {
     Endpoint = 0x0,
     Cluster = 0x28,
     Attribute = 0x0000_0001,
}
Data = "TEST_VENDOR" (11 chars),
...
```

$$\frac{\text{Length of RDA}}{\text{Length of RRA}} \geqslant 1.2$$

Dissection of the Ghosts

```
Matter          96 5540 → 59065 Len=34
Matter         135 5540 → 59065 Len=73
Matter         104 59065 → 5540 Len=42
Matter          96 5540 → 59065 Len=34
Matter         121 59065 → 5540 Len=59
Matter         129 5540 → 59065 Len=67
Matter          96 59065 → 5540 Len=34
Matter         135 5540 → 59065 Len=73
Matter         104 59065 → 5540 Len=42
Matter          96 5540 → 59065 Len=34
Matter         121 59065 → 5540 Len=59
Matter         129 5540 → 59065 Len=67
Matter          96 59065 → 5540 Len=34
Matter         291 5540 → 59065 Len=229
Matter         104 59065 → 5540 Len=42
Matter          96 5540 → 59065 Len=34
Matter         262 5540 → 59065 Len=200
Matter         104 59065 → 5540 Len=42
Matter          96 5540 → 59065 Len=34
Matter         135 5540 → 59065 Len=73
Matter         104 59065 → 5540 Len=42
Matter          96 5540 → 59065 Len=34
Matter         135 5540 → 59065 Len=73
Matter         104 59065 → 5540 Len=42
```

Packet **Patterns**

```
Matter  END      96 5540 → 59065 Len=34
Matter  RDA     135 5540 → 59065 Len=73
Matter  SRA-2   104 59065 → 5540 Len=42
Matter  END      96 5540 → 59065 Len=34
Matter  IRA-1   121 59065 → 5540 Len=59
Matter  IRA-2   129 5540 → 59065 Len=67
Matter  END      96 59065 → 5540 Len=34
Matter  RDA     135 5540 → 59065 Len=73
Matter  SRA-2   104 59065 → 5540 Len=42
Matter  END      96 5540 → 59065 Len=34
Matter  IRA-1   121 59065 → 5540 Len=59
Matter  IRA-2   129 5540 → 59065 Len=67
Matter  END      96 59065 → 5540 Len=34
Matter  RDA     291 5540 → 59065 Len=229
Matter  SRA-2   104 59065 → 5540 Len=42
Matter  END      96 5540 → 59065 Len=34
Matter  RDA     262 5540 → 59065 Len=200
Matter  SRA-2   104 59065 → 5540 Len=42
Matter  END      96 5540 → 59065 Len=34
Matter  RDA     135 5540 → 59065 Len=73
Matter  SRA-2   104 59065 → 5540 Len=42
Matter  END      96 5540 → 59065 Len=34
Matter  RDA     135 5540 → 59065 Len=73
Matter  SRA-2   104 59065 → 5540 Len=42
```

It gets worse …

Same Device Types

↓

Same Clusters

↓

Same Commands

↓

Fingerprints!

Aaahhh .. **interoperability,** it's good but…

```
Matter          137 35879 → 5540 Len=75
Matter          130 5540 → 35879 Len=68
Matter           96 35879 → 5540 Len=34
```

```
Matter          137 35879 → 5540 Len=75
Matter          130 5540 → 35879 Len=68
Matter           96 35879 → 5540 Len=34
```

```
Matter          137 35879 → 5540 Len=75
Matter          130 5540 → 35879 Len=68
Matter           96 35879 → 5540 Len=34
```

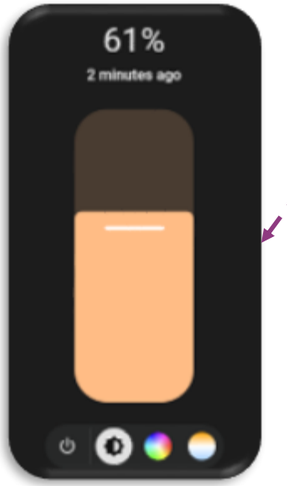
Fingerprints: example

Smart **Bulbs**

Turn **On/Off**

```
35879 → 5540 Len=59
```

Available **Commands**



Change **Intensity**

```
5540 → 35879 Len=71
35879 → 5540 Len=70
```

Home Assistant

Apple

Change **Color (RGB)**

```
35879 → 5540 Len=75
```

Change **Color (Kelvin)**

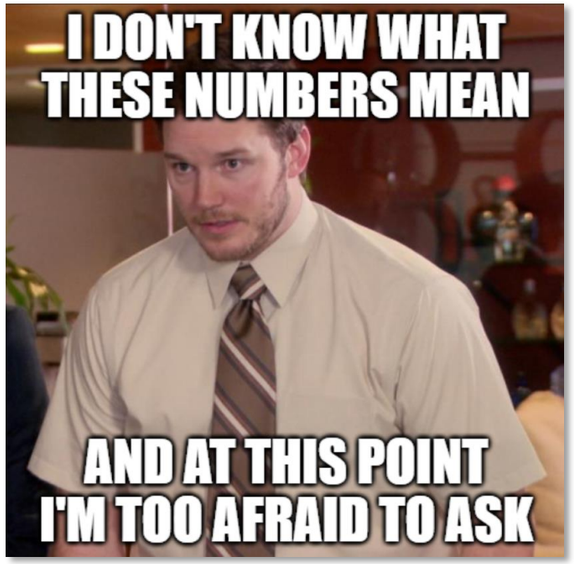
```
35879 → 5540 Len=73
35879 → 5540 Len=72
```

Warm Kelvin

Cool Kelvin

Fingerprints: total

Device type	Observed IRA-1 packet length	Observed packet length sequences
Smart Bulb	{59, 70/71, 72, 73, 75}	{(75 → 59), (73 → 59), (72 → 59)}
Smart Lock	{64}	{(38 → 64), (39 → 64)}
Smart Plug	{59}	∅
Sensor	∅	∅



The full picture

```
Matter  IRA-1    133 35879 → 5540  Len=71
Matter  IRA-2    129 5540 → 35879  Len=67
Matter  END       96 35879 → 5540  Len=34
Matter  RDA      132 5540 → 35879  Len=70
Matter  SRA-2    104 35879 → 5540  Len=42
Matter  END       96 5540 → 35879  Len=34
Matter  RDA      209 5540 → 35879  Len=147
Matter  SRA-2    104 35879 → 5540  Len=42
Matter  END       96 5540 → 35879  Len=34
Matter  IRA-1    137 35879 → 5540  Len=75
Matter  IRA-2    130 5540 → 35879  Len=68
Matter  END       96 35879 → 5540  Len=34
Matter  IRA-1    121 35879 → 5540  Len=59
Matter  RDA      188 5540 → 35879  Len=126
Matter  IRA-2    129 5540 → 35879  Len=67
Matter  SRA-2    104 35879 → 5540  Len=42
Matter  END       96 35879 → 5540  Len=34
Matter  END       96 5540 → 35879  Len=34
```

Change **Intensity**

Change **Color (RGB)**

Turn **On/Off**

Inferred information

- ✓ **Device Type**
- ✓ **Command Names**
- — **Controller Type**

Empirical results

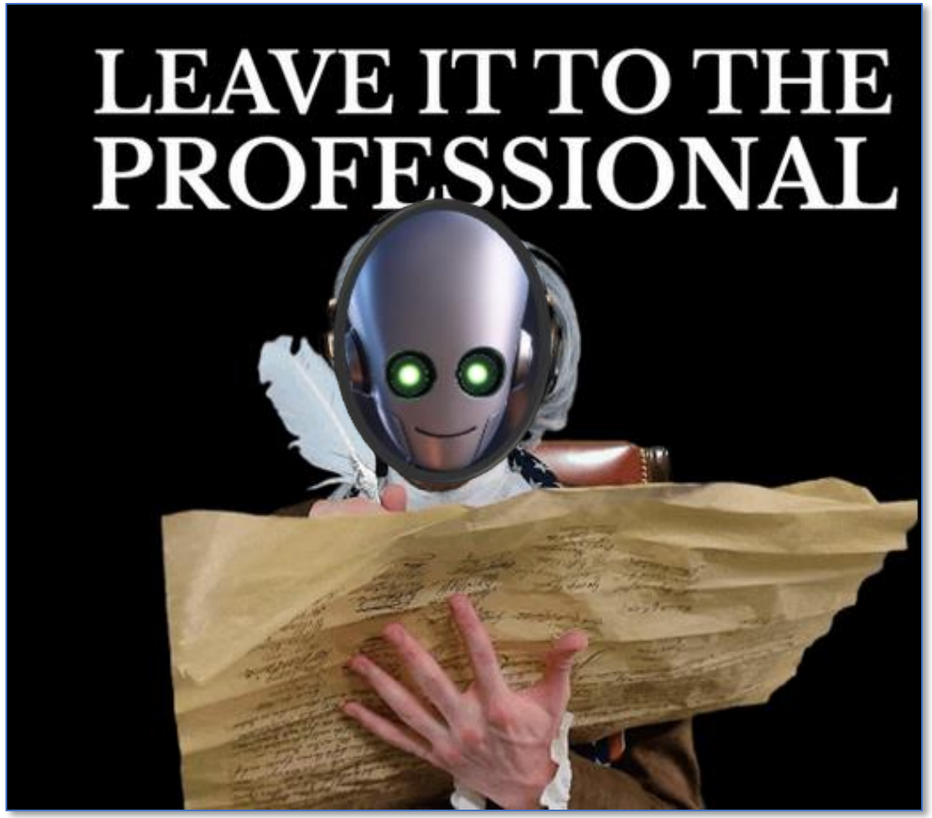
+5% pkt loss +0.5s delay

Packet Labeling	Dataset I	Dataset II	Dataset III
All packet Types	99.87%	98.43%	97.41%
Invoke, Read, Write Requests	99.60%	95.17%	91.88%

Device type	Dataset I	Dataset II	Dataset III	Dataset IV
Smart Bulb	**100%**	57.14%	97.60%	88.00%
Smart Lock	**100%**	**100%**	-	-
Smart Plug	**100%**	**100%**	-	-
Sensor	**100%**	**100%**	-	-

Dataset = A capture of **a fragment of users' behaviors** as exposed through user – device interactions

Time for some ML



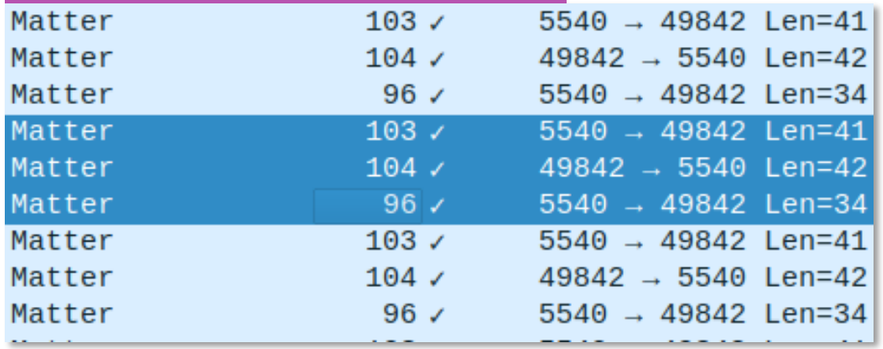
Baby steps with Random Forests (RF)

- ? Door / window
- ? Smart light
- ? Smart thermostat
- ? Motion sensor
- ? Smart switch
- ? Smart lock
- ? Weather sensor

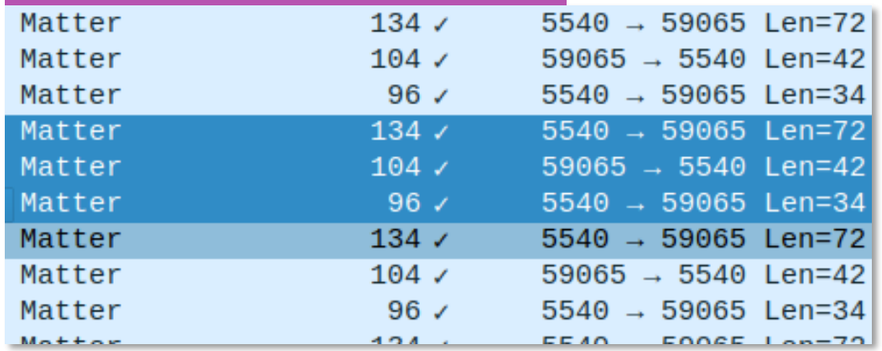
You can't just start learning!

We need some knowledge

'Empty' report sequence: 41, 42, 34



'Non-empty' report sequence: 72, 42, 34



For some devices these are not just sequences, they represent more than **90% of the traffic**!

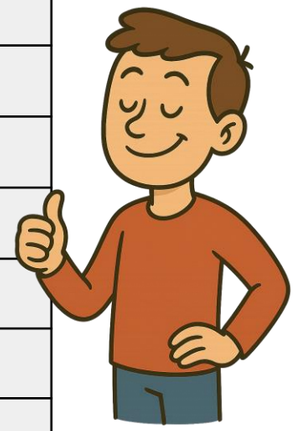
Device	Total nb. of packets	41-42-34 %	72-42-34 %	Remaining %
Aqara Smartlock	6557	**91.96%**	0	8.04%
Nanoleaf bulb	35446	**85.52%**	0	14.48%
Sonoff Switch	36380	69.29%	0	30.71%
Tapo Switch	182551	0	0	100%
Eve Weather	3944	0.07%	19.39%	80.54%
Tado Radiator	277479	0	99.37%	0.63%
Meross motion	35882	76.67%	20.09%	3.24%
Eve motion	8878	21.79%	39.97%	38.24%

And the results are here!

Device	Device type	Dataset I	Dataset II	Dataset III	Dataset IV
Meross motion 2	Motion sensor	**100%**	**100%**	67.27%	-
Eve motion 1	Motion sensor	**100%**	97.69%	**100%**	96.38%
Eve motion 2	Motion sensor	**100%**	97.76%	**100%**	98.18%
Aqara motion	Motion sensor	**100%**	95.26%	90.20%	-
Eve Door & Window 1	Door sensor	**100%**	99.66%	**100%**	99.82%
Eve Door &Window 2	Door sensor	**100%**	99.81%	**100%**	99.88%
Aqara smart lock	Smart lock	**100%**	84.08%	**100%**	**100%**
Eve weather	Weather sensor	**100%**	97.36%	**100%**	98.59%
Tado radiator	Smart thermostat	**100%**	96.02%	-	-

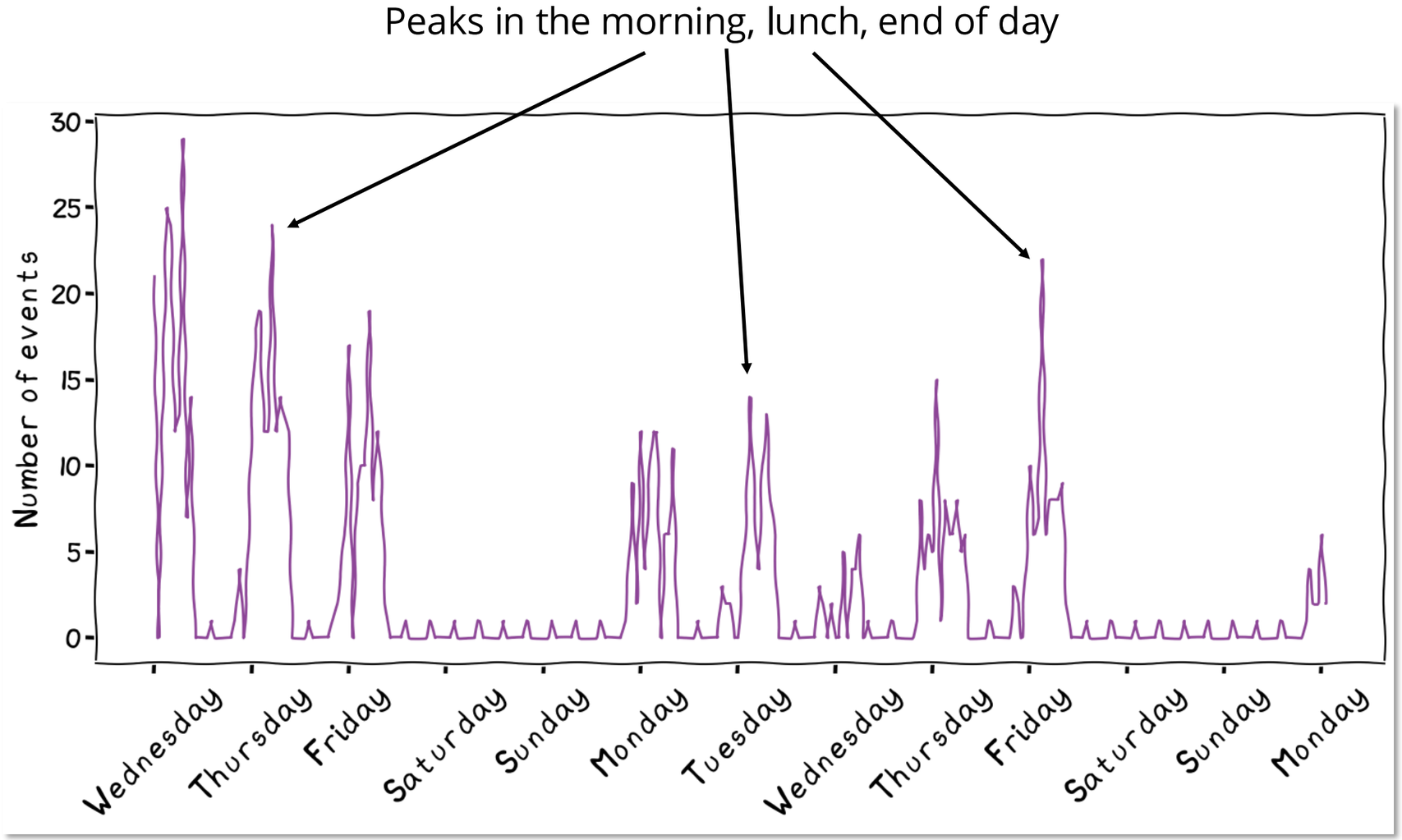
We got similar results for all devices

Device	Device type	Dataset I	Dataset II	Dataset III	Dataset IV
Nanoleaf light bulb 1	Smart light	**100%**	**100%**	**100%**	**100%**
Nanoleaf light bulb 2	Smart light	**100%**	**100%**	-	98.41%
Nanoleaf light bulb 3	Smart light	81.52%	77.36%	82.63%	-
Aqara light bulb 1	Smart light	**100%**	**100%**	-	-
Aqara light bulb 1	Smart light	**100%**	**100%**	-	-
Cono lamp	Smart light	**100%**	**100%**	**100%**	-
Tapo light bulb	Smart light	-	-	99.75%	-
Eve energy	Smart switch	**100%**	99.76%	**100%**	99.68%
Tapo smart plug 1	Smart switch	**100%**	99.89%	**100%**	99.84%
Tapo smart plug 2	Smart switch	**100%**	99.90%	**100%**	99.82%
Meross smart plug 1	Smart switch	98.34%	85.70%	-	95.60%
Meross smart plug 2	Smart switch	98.67%	94.66%	85.97%	95.86%
Sonoff switch 1	Smart switch	96.55%	93.89%	85.36%	75.86%
Sonoff switch 2	Smart switch	94.11%	88.43%	84.22%	68.85%



Any (user) privacy issues?

Do people come to office?

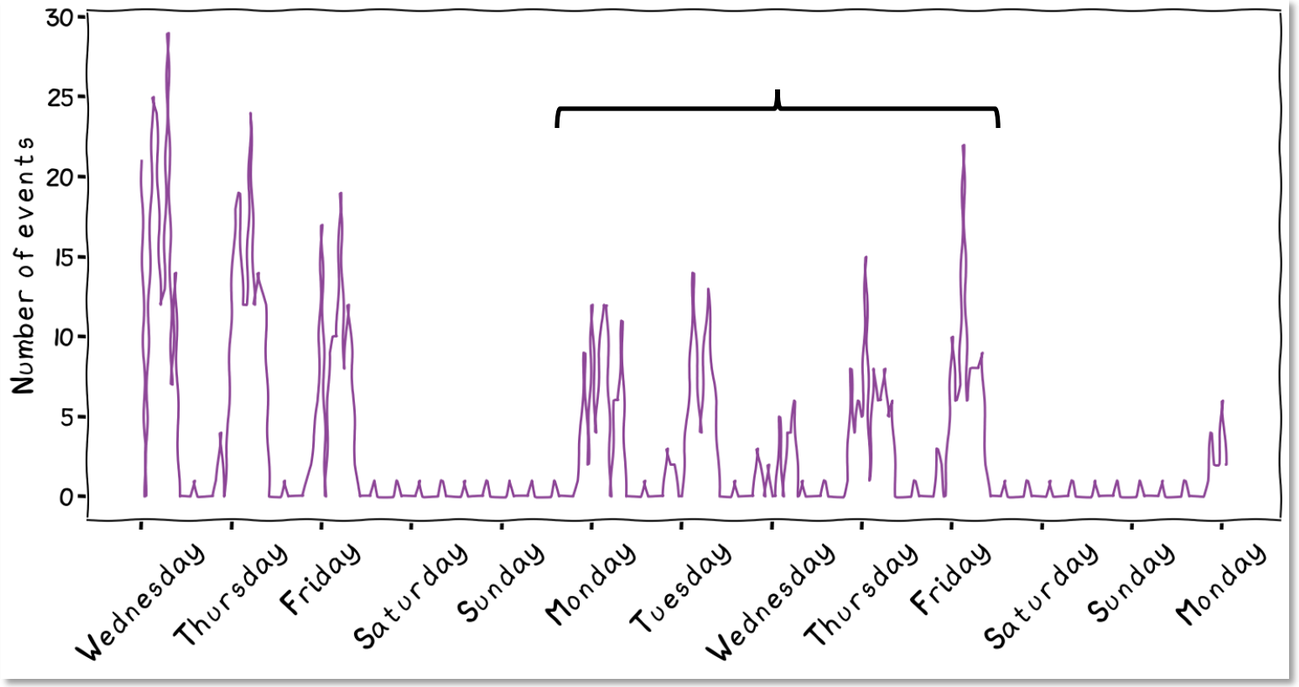


Contact sensor

Can you guess how many?

What happened on this week?

+

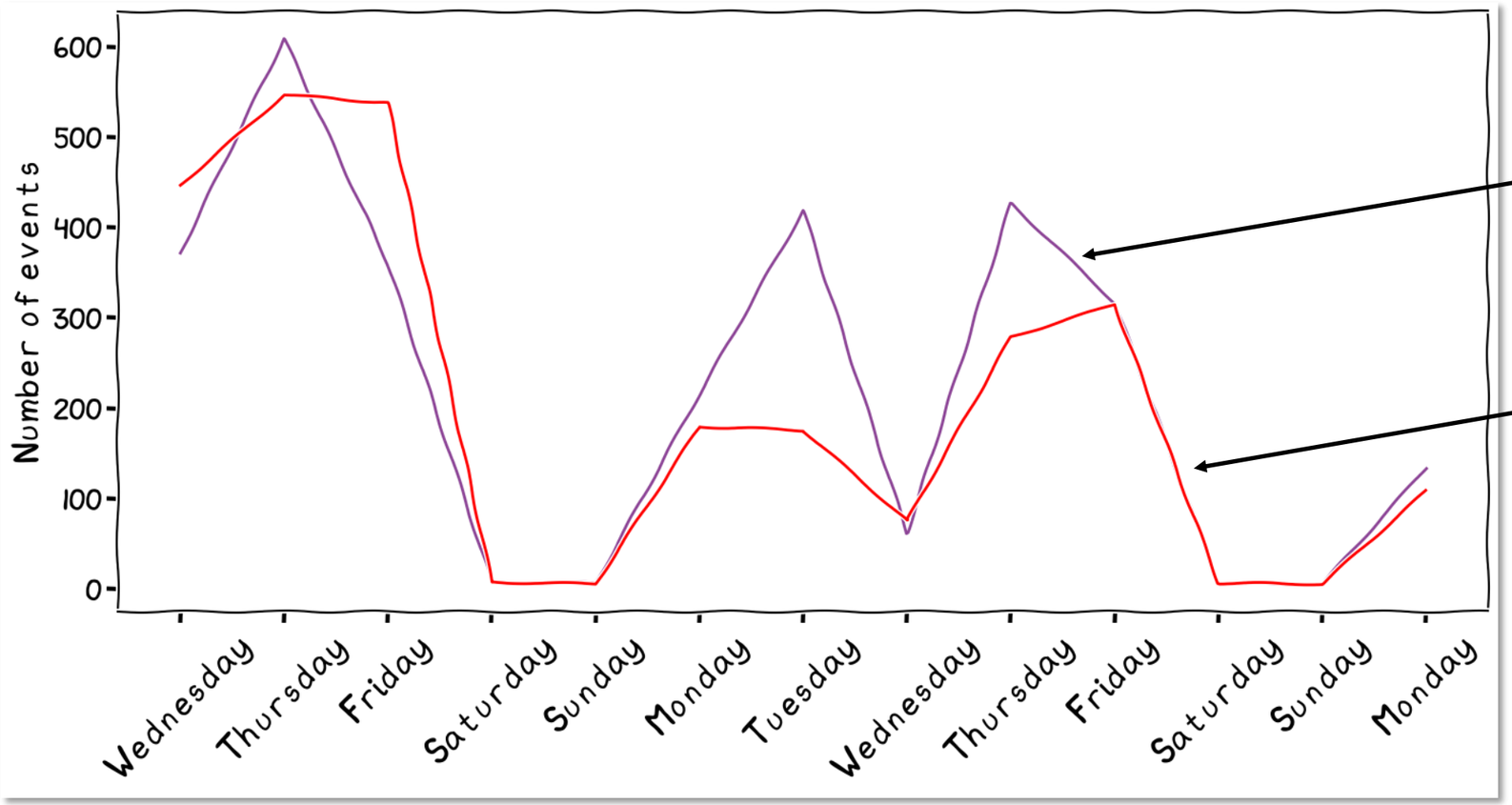


Can you make a similar prediction for the future?

=

Staff from Tg. Mures office traveled to the summit?

How is activity split?

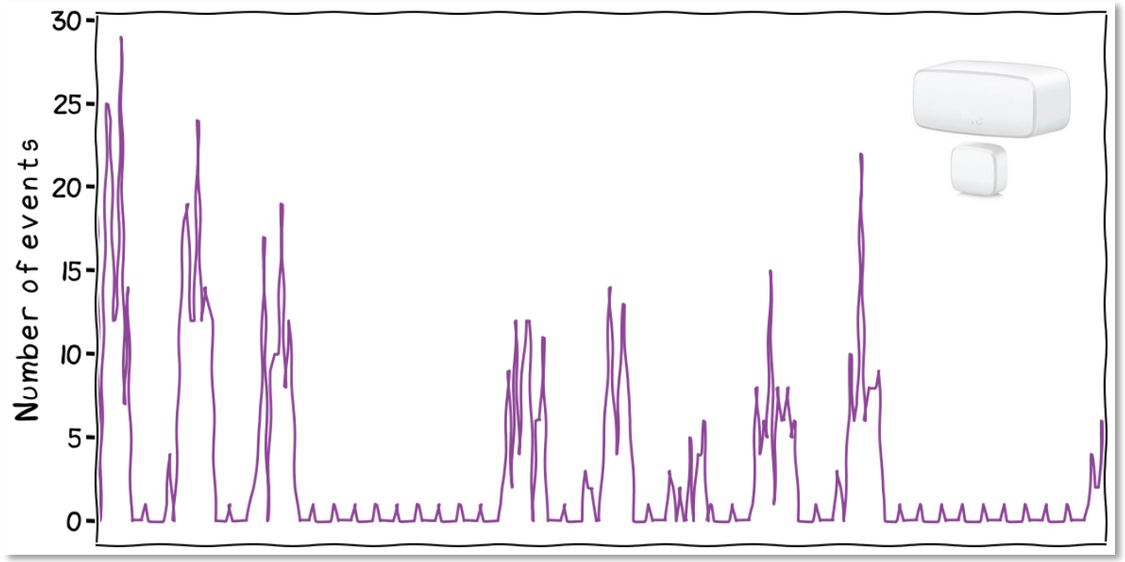


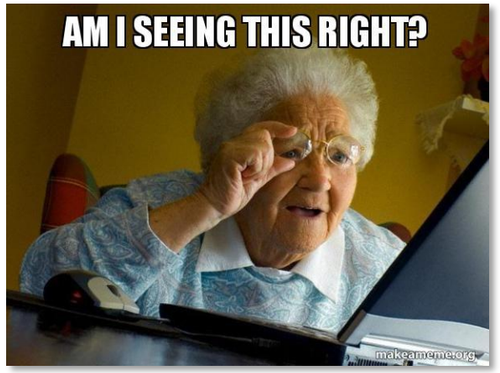
Motion sensors

Lots of harmful exploitations...

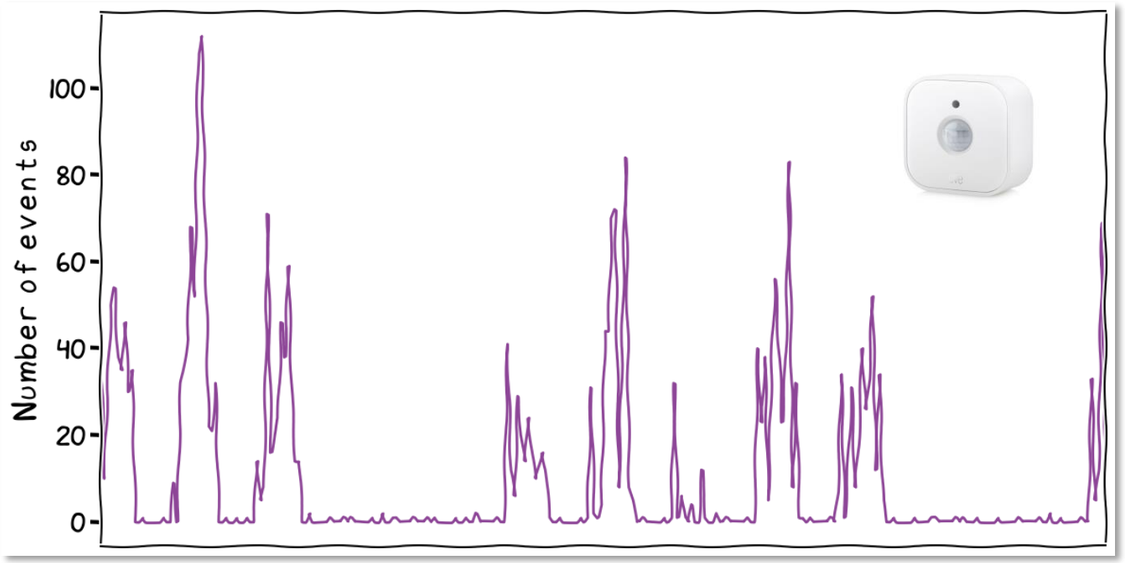
So certain office regions are more "visited"?

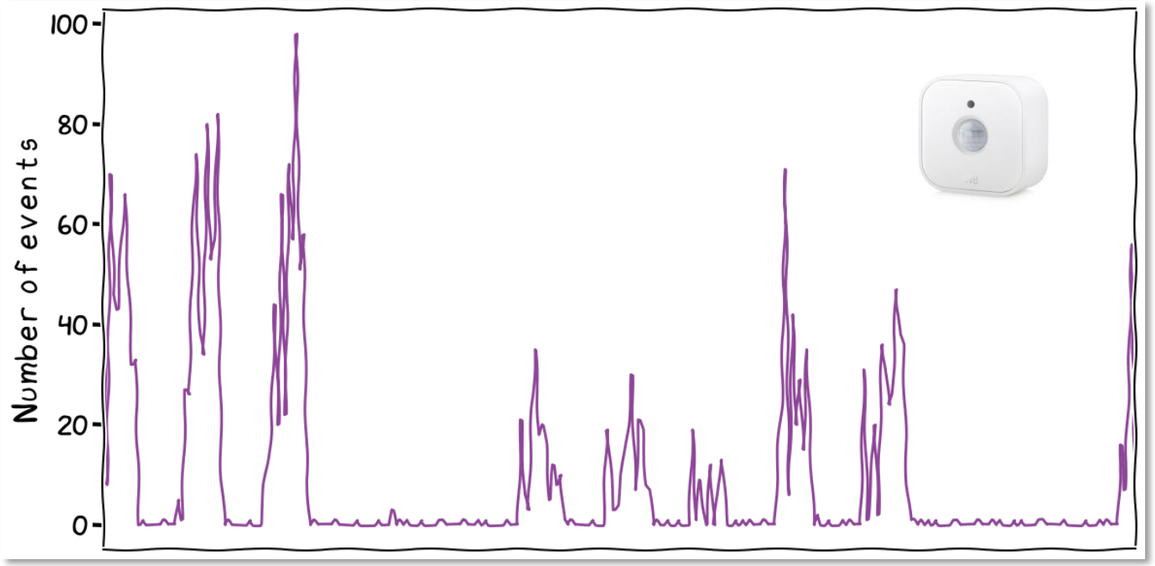
Noticeable correlations



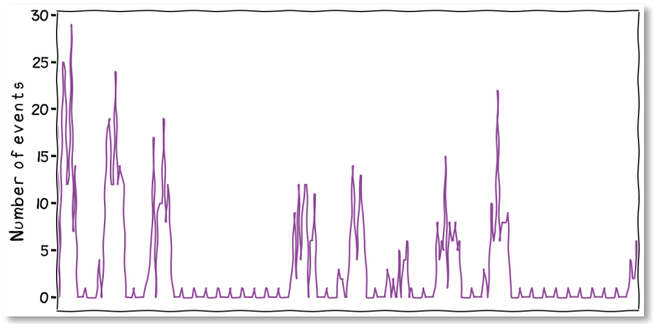


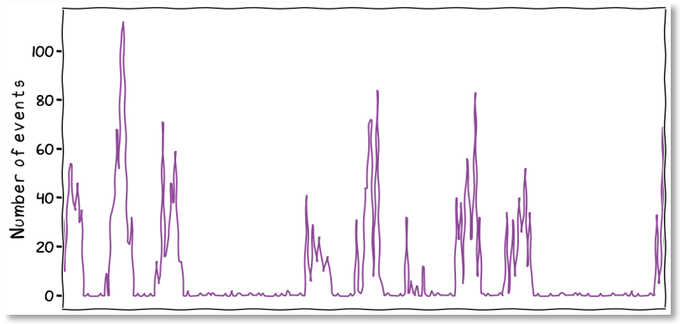
Seem identical, but are from different devices / types

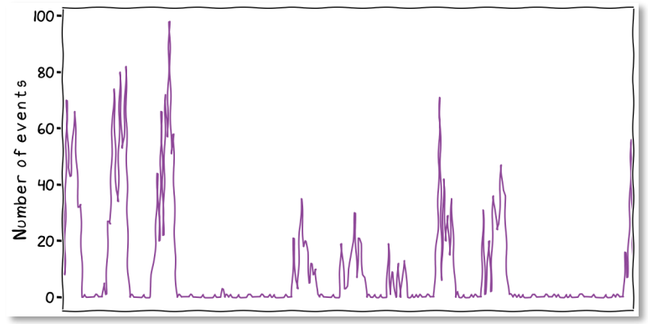




Reverse engineering automations







. . .

Smart Plug 1

On/Off

Smart Lock

Lock/
Unlock

Smart Plug 2

On/Off

Smart Light 1

Change
Color
Warm K

Smart Light 1

Change
Intensity

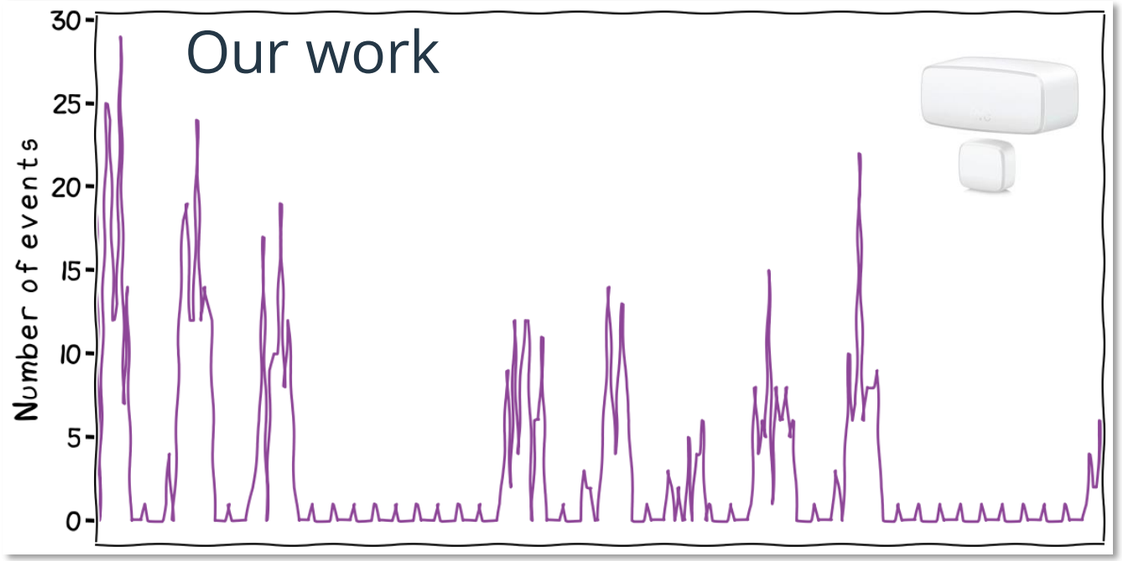
Smart Light 2

Change
Color
Cool K

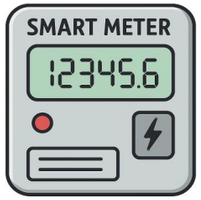
Smart Light 2

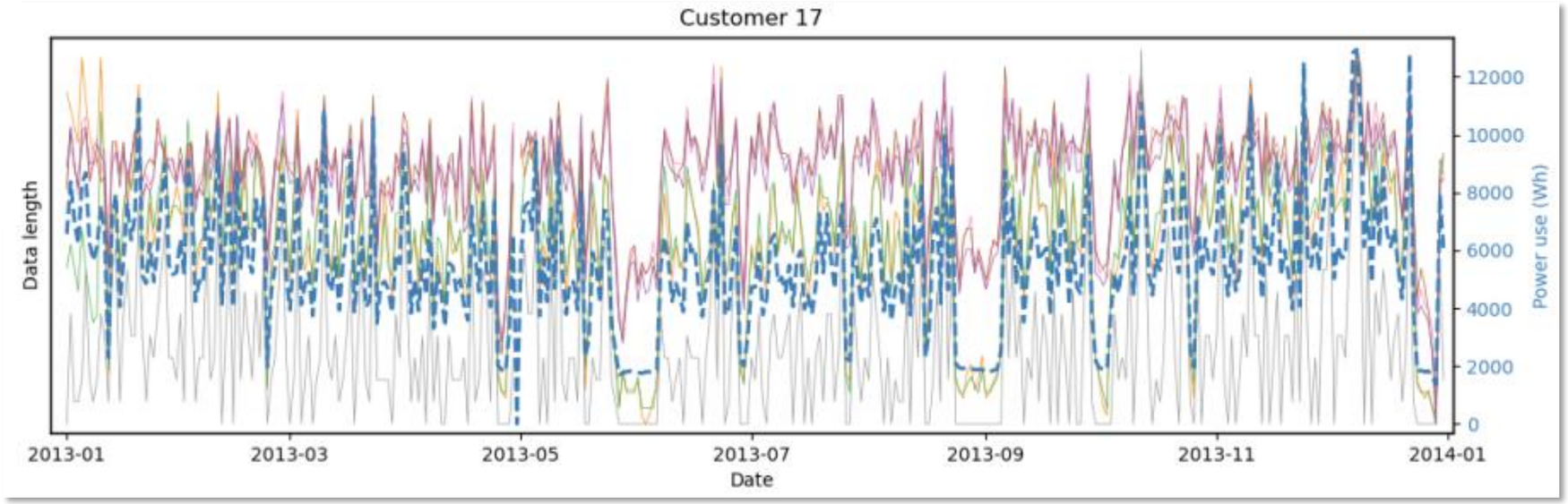
Change
Intensity

Going back in time: smart meters



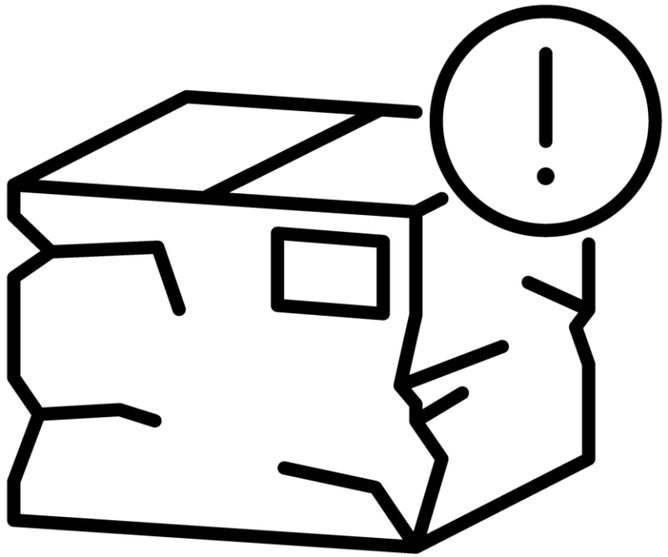
"A mistake repeated more than once is a choice."
(Paulo Coelho)





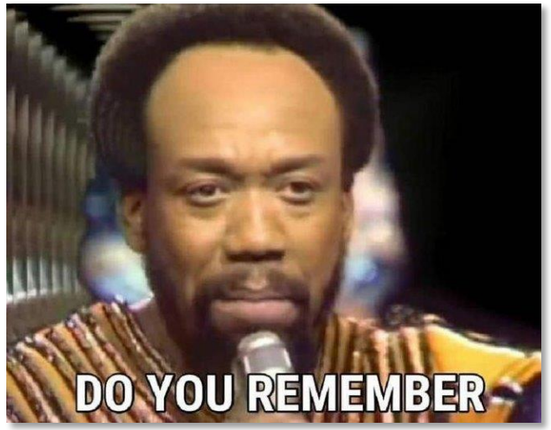
Pol Van Aubel, Erik Poll: *Compromised Through Compression - Privacy Implications of Smart Meter Traffic Analysis*. SecureComm (2) 2021, pp. 317-337

What about fixing this?



Encryption

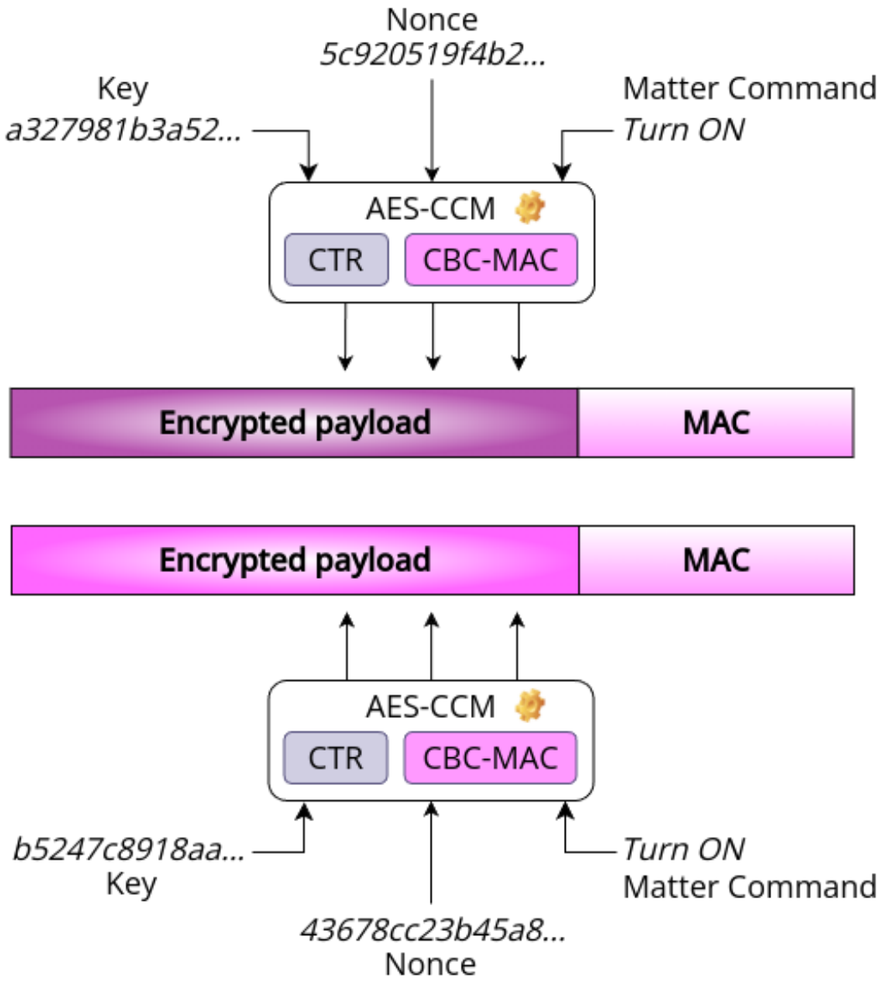
- One crypto scheme
- No crypto negotiation, no crypto agility



Today

=

Next week



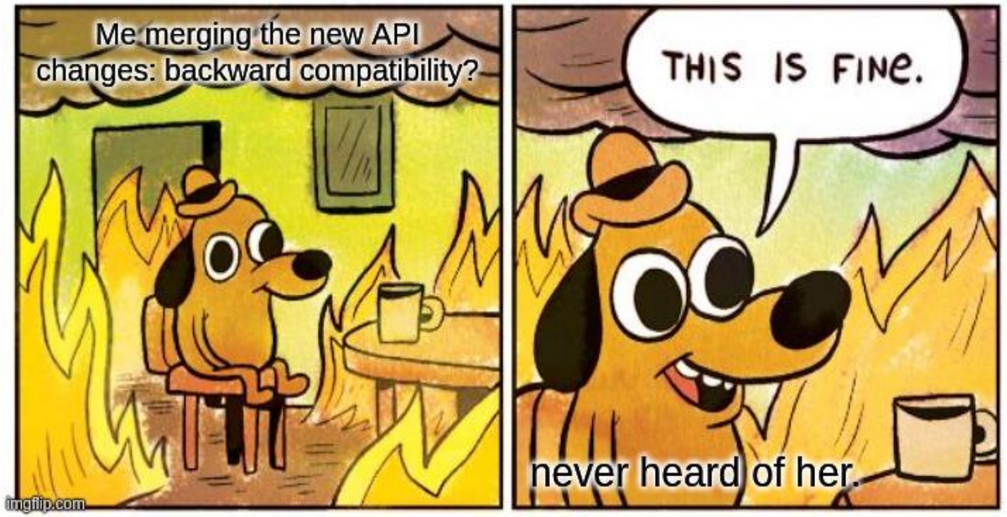
What about fixing this?

1. Start fix

2. Add random padding

   Use uniform packet sizes

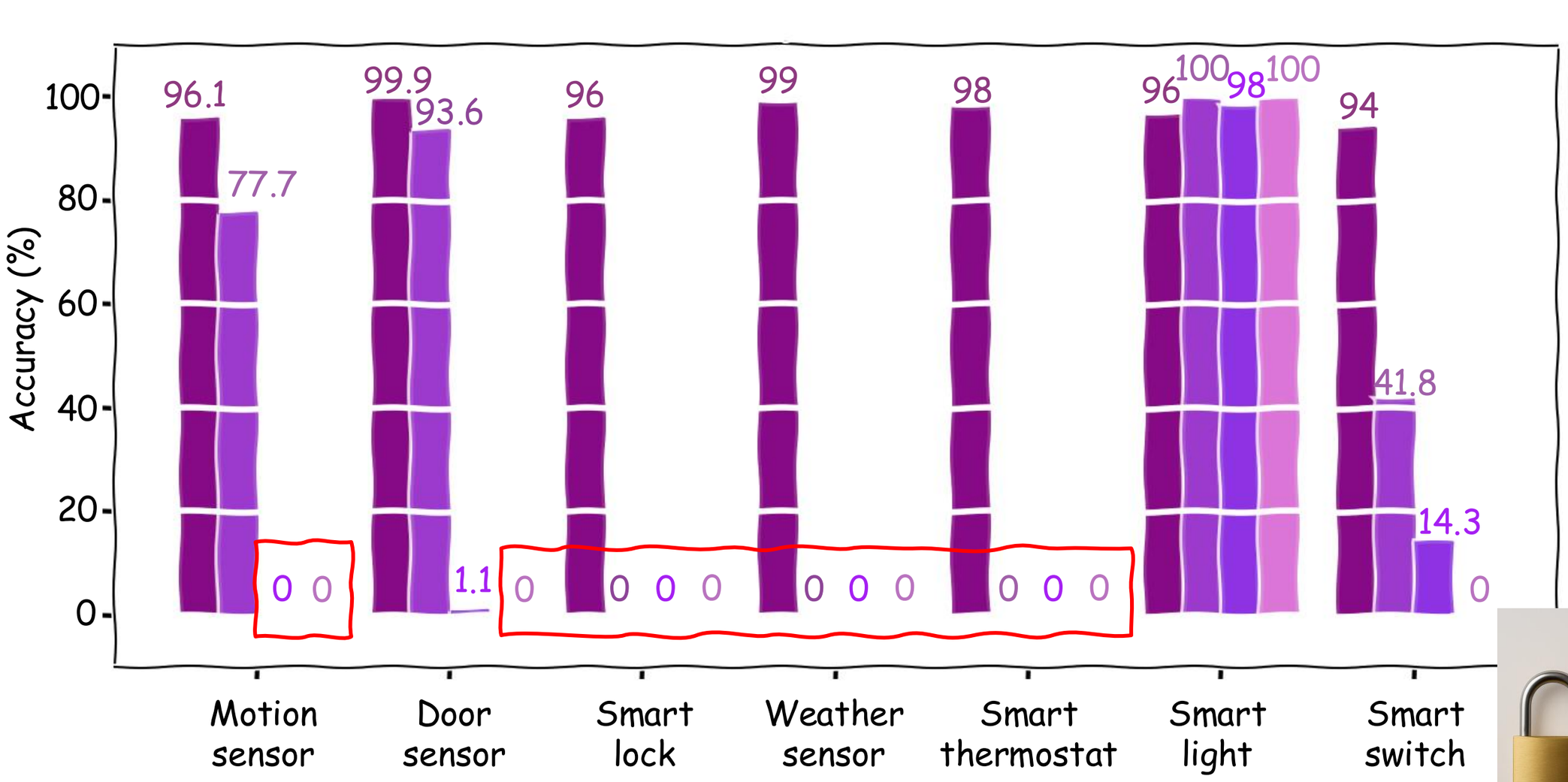
   Solutions from other fields

3. 

Karel Dhondt, et al. "*A run a day won't keep the hacker away: Inference Attacks on Endpoint Privacy Zones in Fitness Tracking Social Networks*", **Black Hat Asia**, 2023.

Depending on version, feasible or not

Random perturbation of packet sizes



Perturbation level

- no pert
- 5-10 pert
- 10-20 pert
- 20-40 pert

Drop of accuracy

↓

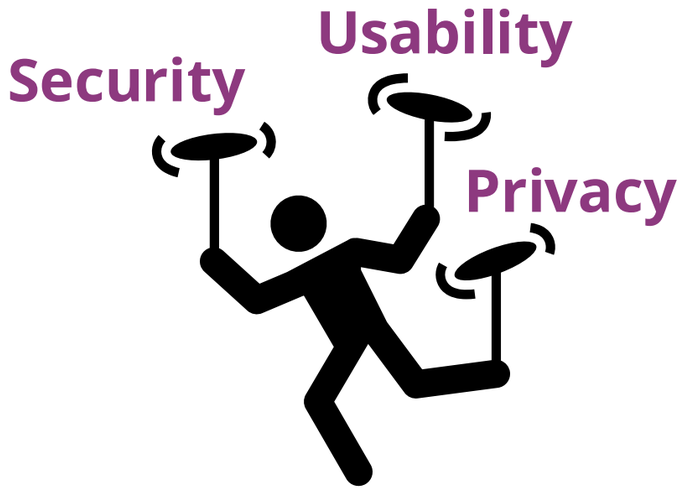
Missclassifications

Uniform packet sizes

Use uniform packet sizes

(not perfect, has drawbacks)

Terminology: **packet size quantization**
Each packet size is rounded up to its nearest multiple of 100 bytes



Could work: our simulations show a drop to **39.72%** (from 97.02%) overall accuracy

- We wanted **security by design**? We got it!
- The **overhead is huge** – Thread is already struggling
- Additional overhead for privacy? **Dramatic impact** on Thread-based communications and battery devices

Lessons learned & actionable items

Lessons learned – context

EU legislation:

Cyber Resilience Act (CRA)

2024/2847

REGULATION (EU) 2024/2847 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 23 October 2024

GDPR

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 27 April 2016

EU CRA: products with digital elements: *"… are also to contribute to enhancing the protection of personal data and privacy of individuals."*

GDPR: does not mention packet sizes directly, but indirectly: personal data or personally identifiable information (PII), which includes *any information that can be linked to an identifiable individual, either directly or indirectly*

The interaction between users and devices poses
significant risks to user behavior profiling,
that is, indirect **user identification** (via Matter packet analysis)

Lessons learned

- In the context of EU legislation, the protocol (standard?) **might be in trouble** (person identification via Matter traffic analysis was not investigated)

- Padding may not be a viable solution, as (some) communications (e.g., Thread) are **already overwhelmed** by Matter traffic

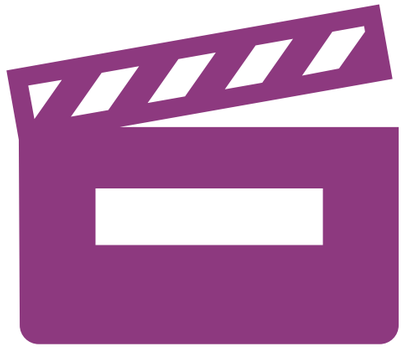
- We have an issue that is waiting for a solution; unfortunately, it is standard-specific, so **it affects all Matter devices**
  - Possible solution: transform not only the packets but the data themselves?

- The standard / protocols are young, so the **time to protect privacy** is now!

Actionable items

1. **Device owners:** as with any software, upgrade, upgrade, upgrade to at least Matter 1.3 – that is, if you have the resources :) - and wait for the fix

2. **Academia & industry:** analyze the standard / protocols, keep reporting issues; hopefully, this will place sufficient pressure to ensure privacy is protected



3. **Standard creators:** very good job at providing security, but users also value their privacy; also consider privacy as a requirement when designing new protocols

Thank you!

Kristopher Schlett, Béla Genge

kris.schlett13@gmail.com, bgenge@bitdefender.com

TU/e EINDHOVEN UNIVERSITY OF TECHNOLOGY

Bitdefender