ETSI The Standards People

IoT Conference 2023

Testing the cybersecurity of the Internet of Things with the help of EN 303 645 as a Market Surveillance Authority

Presented by: Gürkan Kirca

Dutch Authority for Digital Infrastructure
Ministry of Economic Affairs and Climate Policy

06/07/2023

Index

- Who are we?
- Whats wrong with IoT?
- Radio Equipment Directive
- IoT testlab – Objective, configuration and costs
- EN 303 645 standard
- Findings on PV inverters and Home Gateway
- Verdict
- Future projects

About myself

Gürkan Kirca, 26 year old

(IoT) Inspector, Market Surveillance Department

@ Dutch Authority for Digital Infrastructure

h yÅrÑ â vP

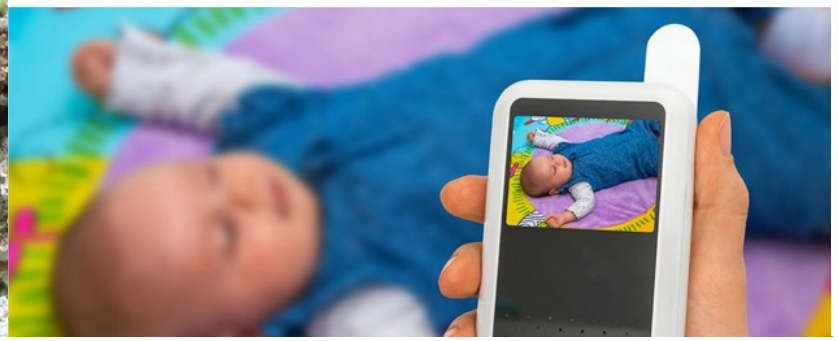
- Dutch Authority for Digital Infrastructure
- Part of the Ministry of Economic Affairs and Climate Policy
- Mission: “Keeping the Netherlands safely connected”
- +/- 450 colleagues, in Groningen and Amersfoort

Whats wrong with IoT?

Innovations

How a fish tank helped hack a casino

Hacker terrorizes family by hijacking baby monitor



'Internet of things' or 'vulnerability of everything'? Japan will hack its own citizens to find out

By James Griffiths, CNN

Updated 0259 GMT (1059 HKT) February 2, 2019

Hackers leave Finnish residents cold after DDoS attack knocks out heating systems

- The attack is believed to have lasted for a week, starting in late October and enc November.

This pretty blond doll could be spying on your family

Black Hat USA 2015: The full story of how that Jeep was hacked

Radio Equipment Directive

Article 3.3 (d, e, f) of the Radio Equipment Directive states:

- **(d)** radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service;
- **(e)** radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected;
- **(f)** radio equipment supports certain features ensuring protection from fraud.

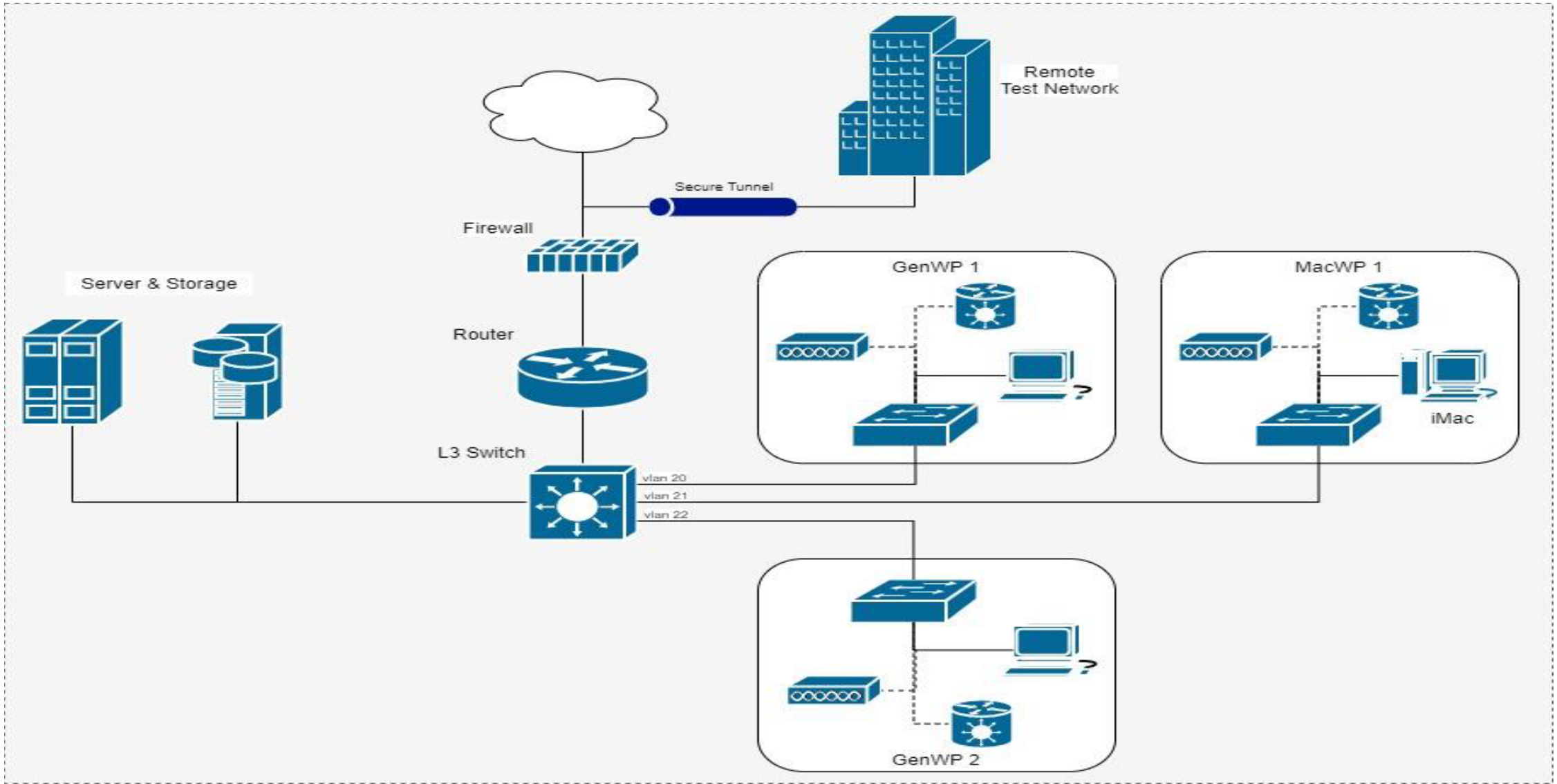
“Digital Safe Products” program

- New program within our organization, built from scratch, whole new area, “pioneering”.
- Digital Safe Products has in scope:
  - Standardization;
  - Normalization;
  - Building of Internet of Things Test Lab and testing IoT products on cyber security;
  - Reporting point for “unsafe smart products;
  - Talking with branche organisations to create “awareness” of what’s coming with the RED 3.3DEF;
  - Talking with Notified Bodies to gather knowledge.

IoT Testlab - Objective

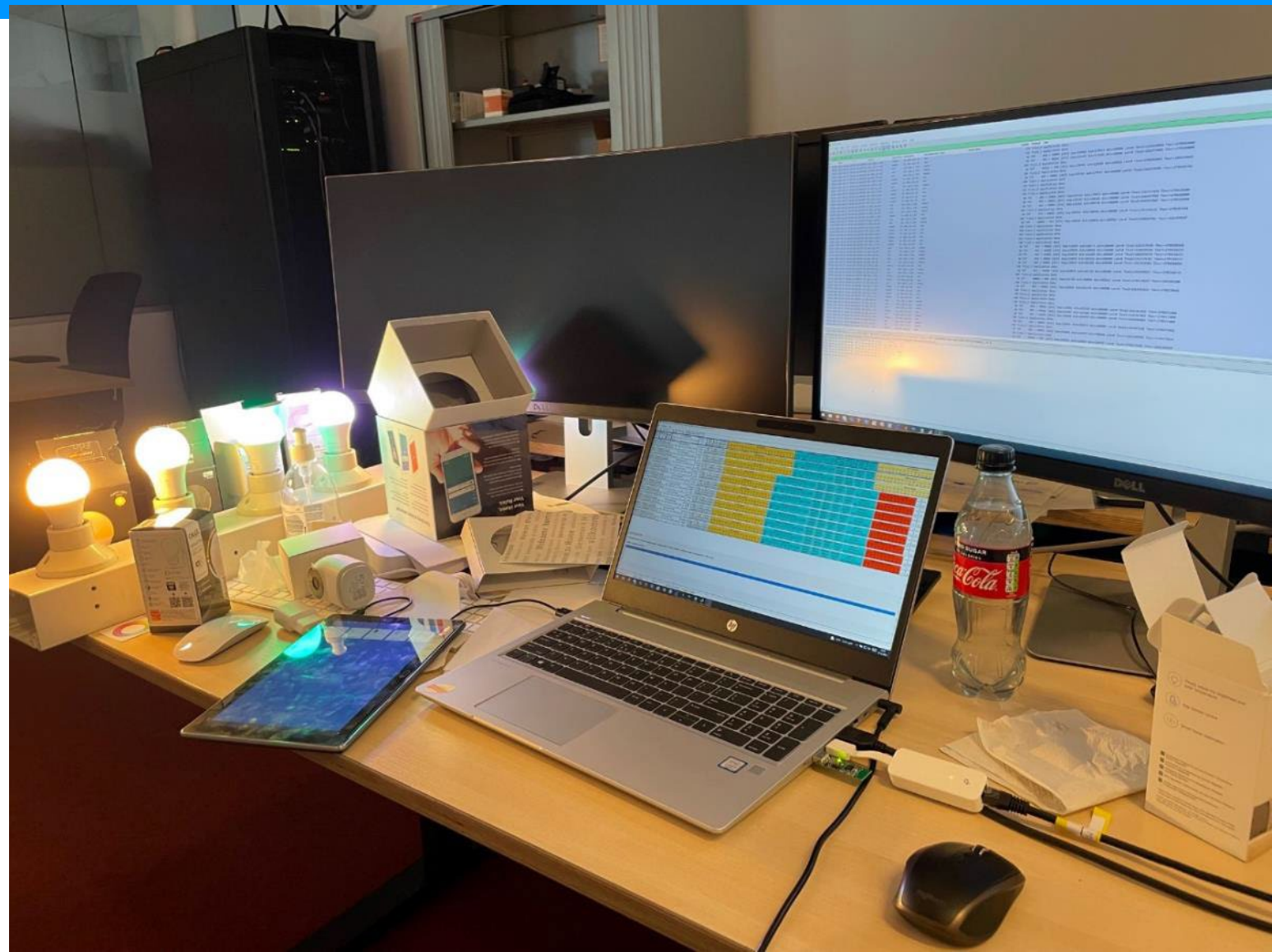
- Market surveillance/regulation/enforcement
- Gather knowledge
- No certifying
- Verifying testability of regulations
- Measurements were performed using:
  - Baseline requirements from EN 303 645 V2.1.1.
  - Conformance assessment based on TS 103 701 V1.1.1.
    - TS 103 848 for “Home Gateway”
  - Guidance with the help of TR 103 621 V2.1.1.

IoT Testlab - Configuration



IoT Testlab - Costs

- "IoT Testing laboratory"
- Networking: €4000~
- Server: €5000~
- Workplace: €10000~
- Software: €10000~
- 2 ➔ 4 FTE ethical hackers / testers
- 0.2 FTE system engineer (for basic IT maintenance and management)
- **It does not only cost money to build this, but also a lot of time!**



Standard

ETSI EN 303 645 V2.1.1 (2020-06)

CYBER;
Cyber Security for Consumer Internet of Things:
Baseline Requirements

EN 303 645 Provisions categories

- Cyber security provisions for consumer IoT:
  1. No universal default passwords
  2. Implement a means to manage reports of vulnerabilities
  3. Keep software updated
  4. Securely store sensitive security parameters
  5. Communicate securely
  6. Minimize exposed surface attacks
  7. Ensure software integrity
  8. Ensure that personal data is secure
  9. Make systems resilient to outages
  10. Examine system telemetry data
  11. Make it easy for users to delete user data
  12. Make installation and maintenance of dev
  13. Validate input data
- Data protection provisions for consumer IoT

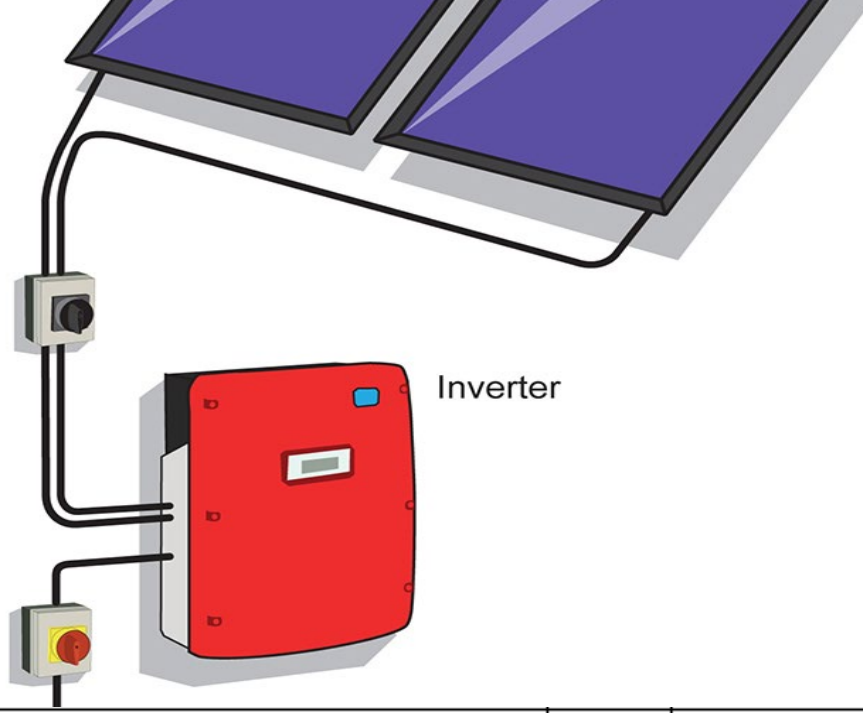
Test Report – Password example

5. Results: Passwords

5.1 Test descriptions

The scope of this test is to measure how the device handles various situations regarding passwords.
The following tests related to passwords will be applied:

Provision	Condition	Result	Internal notes
5.1-1	Where passwords are used and, in any state, other than the factory default, all consumer IoT device passwords shall be unique per device or defined by the user.	Fail	Standard login credentials present.
	Password is unique per device.	Fail	Standard login credentials present.
	Password can be set by user.	Fail	Standard login credentials can't be changed. Can change the password for the app.
5.1-2	Where pre-installed unique per device passwords are used, these shall be generated with a mechanism that reduces the risk of automated attacks against a class or type of device.	Fail	Standard login credentials present.



5.1-3	Authentication mechanisms used to authenticate users against a device shall use best practice cryptography, appropriate to the properties of the technology, risk, and usage.	Fail	No encryption is being used.
5.1-4	Where a user can authenticate against a device, the device shall provide to the user or an administrator a simple mechanism to change the authentication value used.	Fail	Standard login credentials can't be changed. Can change the password for the app.
5.1-5	When the device is not a constrained device, it shall have a mechanism available which makes bruteforce attacks on authentication mechanisms via network interfaces impracticable.	Fail	Bruteforce attacks are possible on both the app and the inverter.

Findings on PV inverters

Category	Product 1	Product 2	Product 3	Product 4	Product 5	Product 6	Product 7	Product 8
Passwords	✗	✗	✗	✗	✓	✗	✗	✗
Reports of vulnerabilities	✗	✗	✗	✗	✗	✗	✗	✗
Updates	✗	✗	✗	✗	✗	✗	✗	✗
Securely store security parameters	—	—	—	—	—	—	—	—
Communicate securely	✗	✓	✗	✓	✓	✗	✓	✗
Minimize exposed attack surfaces	✗	✓	✓	✓	✓	✓	✗	✗
Secure personal data	✓	✓	✓	✓	✓	✗	✓	✓
Delete user data	✓	✓	✓	✗	✓	✗	✓	✓
Validate input data	✓	✓	—	—	✓	✓	—	✓
Data protection	✓	✓	✗	✓	✓	✗	✗	✓

✓ = Pass

✗ = Fail

— = N/A

Findings on PV inverters

NOS Nieuws Sport Live

rtl nieuws 19 ° 55 km

Omvormers slecht beveiligd

Zonnepanelen eenvoudig te hacken: risico voor woningen én stroomnet

Door Stan Hulsen
30 mei 2023 03:41 • Aangepast 30 mei 2023 06:51

NOS Nieuws • Dinsdag 30 mei, 10:07

Zonnepanelen gevoelig voor hacks en storingen: 'Hack stroomnet is realistisch'

Menu nrc

Luister naar 04:50

Zonnestroominstallatie kwetsbaar voor hacks en storingen

Cybercrime Omvormers die energie van zonnepanelen omzetten in stroom voor koelkasten en koffiezetapparaten, blijken makkelijk te hacken.

Koen Marée 30 mei 2023 Leestijd 2 minuten

GHACD

Findings on routers

Categorieën	Router 1	Router 2	Router 3	Router 4	Router 5	Router 6	Router 7	Router 8	Router 9
Passwords	✗	✓	✗	✓	✗	✓	✗	✗	✗
Reports of vulnerabilities	✓	✓	✓	✓	✓	✓	✓	✓	✓
Updates	✗	✗	✗	✗	✗	✗	✗	✗	✗
Communicate securely	✓	✓	✗	✓	✓	✓	✓	✗	✓
Minimize exposed attack surfaces	✓	✓	✗	✓	✓	✓	✓	✓	✓
Secure personal data	✓	✓	✓	✓	✓	✓	✓	✗	✓
Delete user data	✓	✓	✓	✓	✓	✓	✓	✓	✓
Validate input data	✓	✓	✓	✓	✓	✓	✓	✓	✓
Data protection	✓	✓	✓	✓	✓	✓	✓	✓	✓

✓ = Pass

✗ = Fail

— = N/A

Digital threats are a fact of life

Hacker terrorizes family by hijacking baby monitor

Babymonitor example

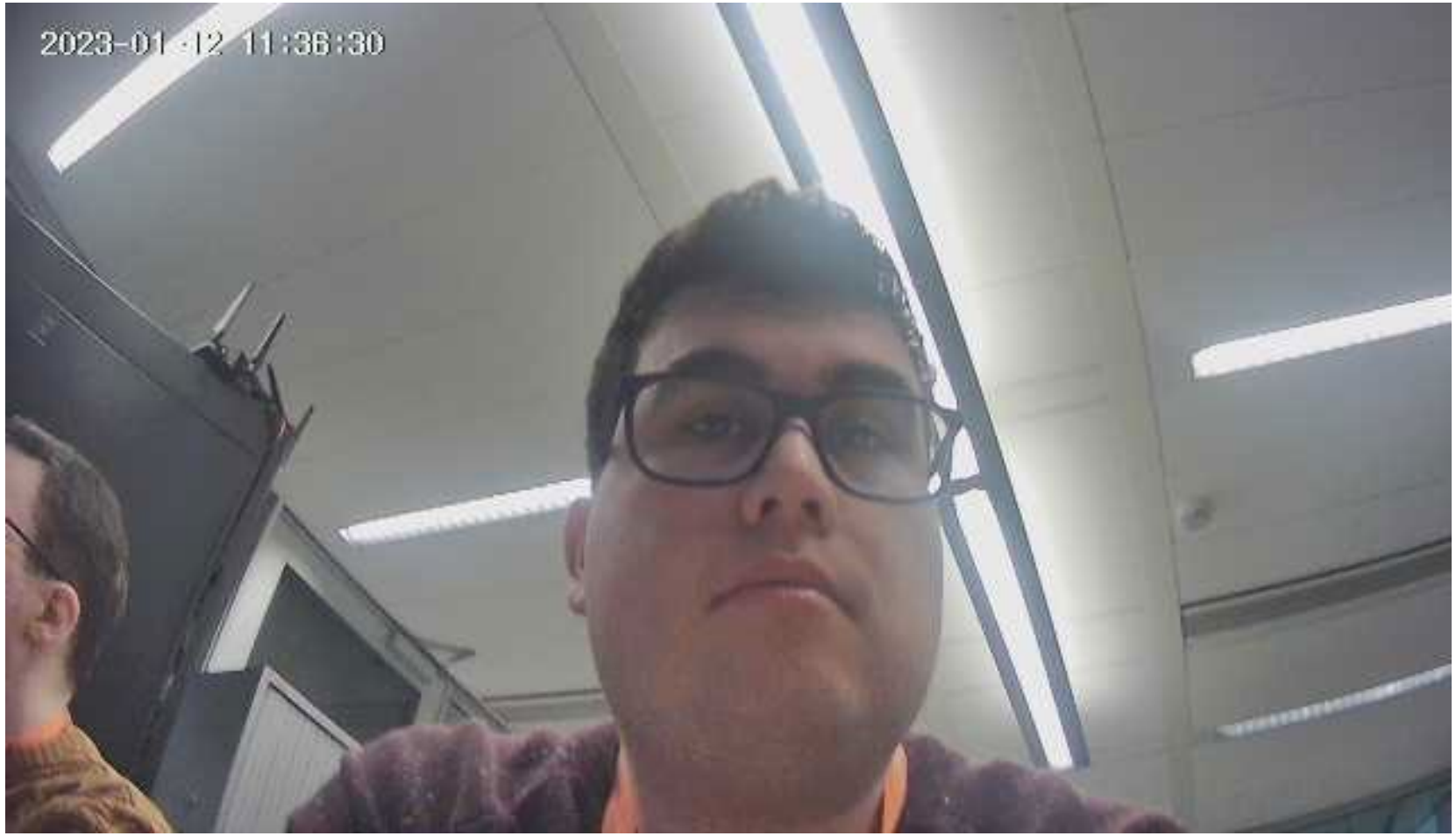
Summary o

- IP address: 47.254.187.21
- City: **Frankfurt Am Main**
- Region name: Hessen
- Country name: Germany

PUT /alertImage/101557783/103405931/103405931-20221205134127-661689.jpg

1143	2022-12-05 12:41:29,345297	47.254.187.21	192.16 .2.36	TCP	66	[TCP Dup ACK 1124#3] 80 → 58856 [ACK] Seq=309 Ack=17743 Win=69632 Len=0 SLE=15421 SRE=16721
1144	2022-12-05 12:41:29,345297	47.254.187.21	192.168.2.36	TCP	60	80 → 58856 [ACK] Seq=309 Ack=18863 Win=72704 Len=0
1145	2022-12-05 12:41:29,345540	47.254.187.21	192.168.2.36	TCP	60	80 → 58856 [ACK] Seq=309 Ack=20163 Win=75776 Len=0
1146	2022-12-05 12:41:29,345540	47.254.187.21	192.168.2.36	TCP	60	80 → 58856 [ACK] Seq=309 Ack=21463 Win=78336 Len=0
1147	2022-12-05 12:41:29,348019	192.168.2.36	47.254.187.21	TCP	1354	58856 → 80 [ACK] Seq=33163 Ack=309 Win=17132 Len=1300 [TCP segment of a reassembled PDU]
1148	2022-12-05 12:41:29,348256	192.168.2.36	47.254.187.21	HTTP/JSON	934 ✓	PUT /alertImage/101557783/103405931/103405931-20221205134127-661689.jpg HTTP/1.1 , JavaScript Object Notation (application/json)
1149	2022-12-05 12:41:29,352128	47.254.187.21	192.168.2.36	TCP	60	80 → 58856 [ACK] Seq=309 Ack=22763 Win=81408 Len=0
1150	2022-12-05 12:41:29,352128	47.254.187.21	192.168.2.36	TCP	60	80 → 58856 [ACK] Seq=309 Ack=24063 Win=84480 Len=0
1151	2022-12-05 12:41:29,352355	47.254.187.21	192.168.2.36	TCP	60	80 → 58856 [ACK] Seq=309 Ack=25363 Win=87040 Len=0
1152	2022-12-05 12:41:29,357980	47.254.187.21	192.168.2.36	TCP	60	80 → 58856 [ACK] Seq=309 Ack=26663 Win=90112 Len=0
1153	2022-12-05 12:41:29,357980	47.254.187.21	192.168.2.36	TCP	60	80 → 58856 [ACK] Seq=309 Ack=27963 Win=93184 Len=0
1154	2022-12-05 12:41:29,358209	47.254.187.21	192.168.2.36	TCP	60	80 → 58856 [ACK] Seq=309 Ack=29263 Win=95744 Len=0
1155	2022-12-05 12:41:29,363856	47.254.187.21	192.168.2.36	TCP	60	80 → 58856 [ACK] Seq=309 Ack=30563 Win=98816 Len=0
1156	2022-12-05 12:41:29,363856	47.254.187.21	192.168.2.36	TCP	60	80 → 58856 [ACK] Seq=309 Ack=31863 Win=101888 Len=0
1157	2022-12-05 12:41:29,364084	47.254.187.21	192.168.2.36	TCP	60	80 → 58856 [ACK] Seq=309 Ack=33163 Win=104960 Len=0
1158	2022-12-05 12:41:29,385534	47.254.187.21	192.168.2.36	TCP	60	80 → 58856 [ACK] Seq=309 Ack=34463 Win=107520 Len=0
1159	2022-12-05 12:41:29,398599	47.254.187.21	192.168.2.36	TCP	60	80 → 58856 [ACK] Seq=309 Ack=35343 Win=110592 Len=0
1160	2022-12-05 12:41:29,398599	47.254.187.21	192.168.2.36	HTTP	362	HTTP/1.1 200 OK
1161	2022-12-05 12:41:29,404881	192.168.2.36	47.254.187.21	TCP	60	58856 → 80 [FIN, ACK] Seq=35343 Ack=617 Win=17132 Len=0
1162	2022-12-05 12:41:29,406482	192.168.2.36	192.168.2.1	DNS	94	Standard query 0x001c AAAA apis-eu-frankfurt.cloudedge360.com
1163	2022-12-05 12:41:29,447530	47.254.187.21	192.168.2.36	TCP	60	80 → 58856 [FIN, ACK] Seq=617 Ack=35344 Win=110592 Len=0
1164	2022-12-05 12:41:29,449776	192.168.2.36	47.254.187.21	TCP	60	58856 → 80 [ACK] Seq=35344 Ack=618 Win=17132 Len=0
1165	2022-12-05 12:41:29,550533	192.168.2.1	192.168.2.36	DNS	254	Standard query response 0x001c AAAA apis-eu-frankfurt.cloudedge360.com CNAME meari-eu-slb-cloudedge360-52676689.eu-central-1.elb.ama

Babymonitor example



Conclusion

- EN 303 645 V2.1.1 is a great guideline to test consumer IoT on cybersecurity:
  - Provisions are written in an understandable language.
  - The categories within this standard are relevant to increase the baseline cybersecurity of consumer IoT.
  - Generic, purposeful requirements and best practices.
- TS 103 701 V1.1.1 makes it clear what the expectations are and how this should be assessed.
- TR 103 621 V2.1.1 has good examples for each provision.
- **The essential requirements of the RED are leading!**
- **Preparation for the CRA.**

Reflection, takeaways, learnings

- It takes time to build an Internet of Things testing lab. **Start on time to build yours!**
- Finding the right people with the right knowledge is a challenge.
- Important to send a signal to the industry that Market Surveillance Authorities are looking at this.
- Not a completely new method of working, more focus on IoT. Not only focus on cybersecurity but also administrative research and writing a research report.

Future projects

- Prepare ourself even further as market surveillance authority to test consumer IoT products on cyber security.
- Look at more products that could pose a **risk** such as **childcare, renewable energy** and **Operational Technology**

Thank you

- iot-lab@rdi.nl
- gurkan.kirca@rdi.nl