Security Conference 2022

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

GÜrkan Kirca

04/10/2022

Index

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

About myself

Gürkan Kirca, 26 year old

(IoT) Inspector, Market Surveillance Department

@ Agentschap Telecom /

Dutch Radiocommunications Agency

Who are we?

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

Definition Internet of Things

Definition Gartner:

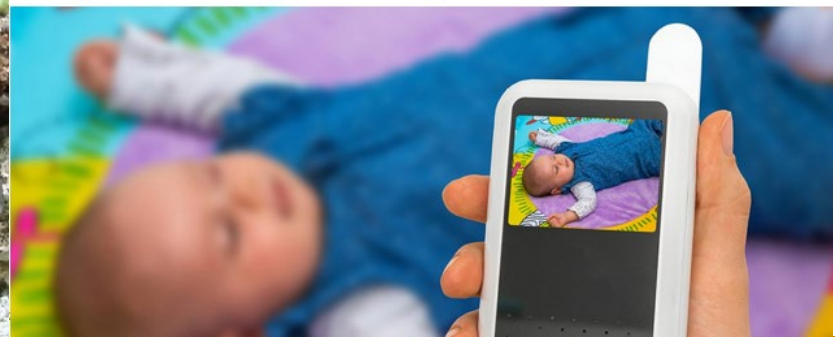
“The Internet of Things (IoT) is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment.”

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

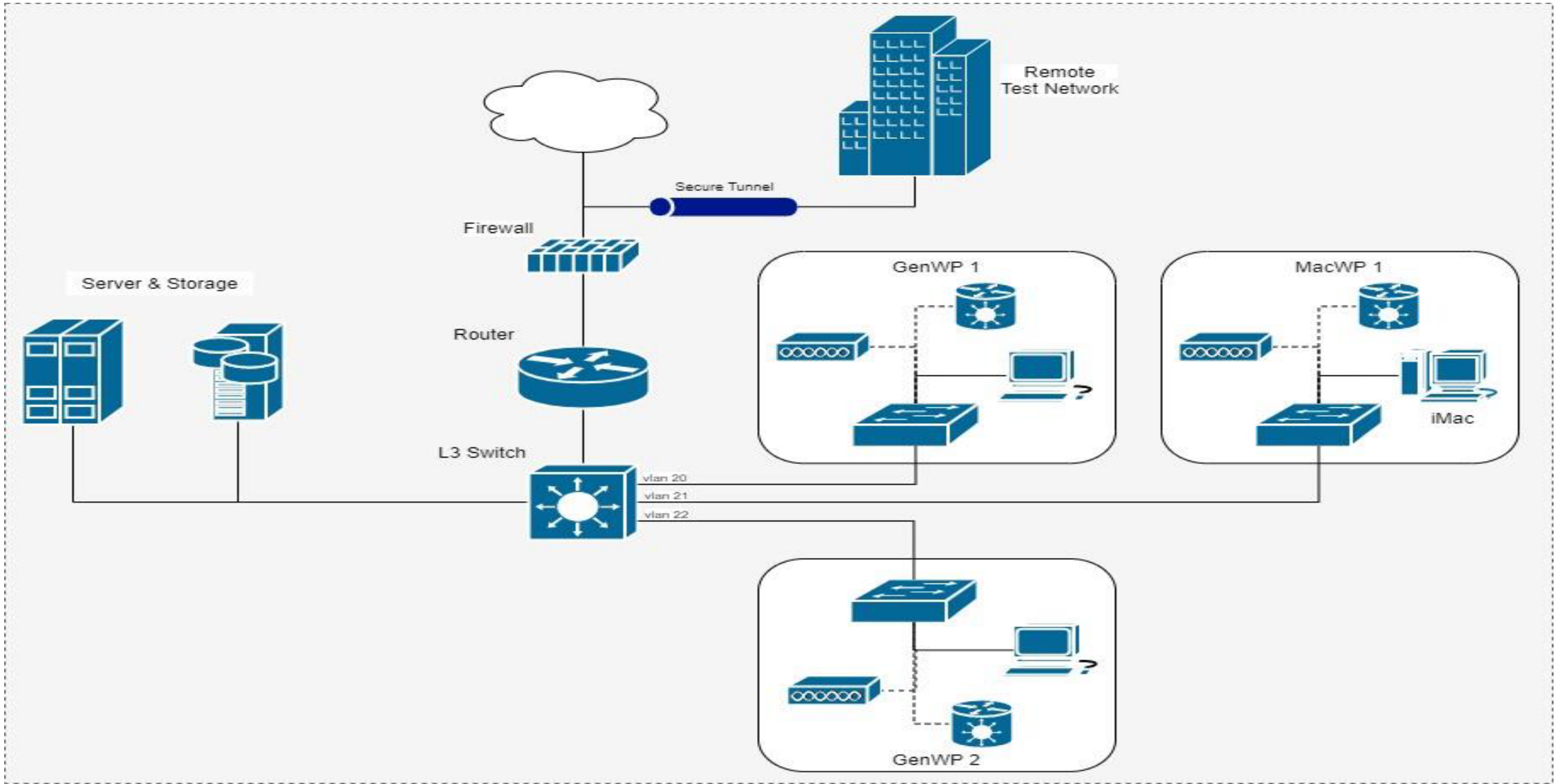
Whats wrong with IoT?

Insteon Kills Servers Without Warning, Bricks Smart Home Devices

IoT Testlab - Objective

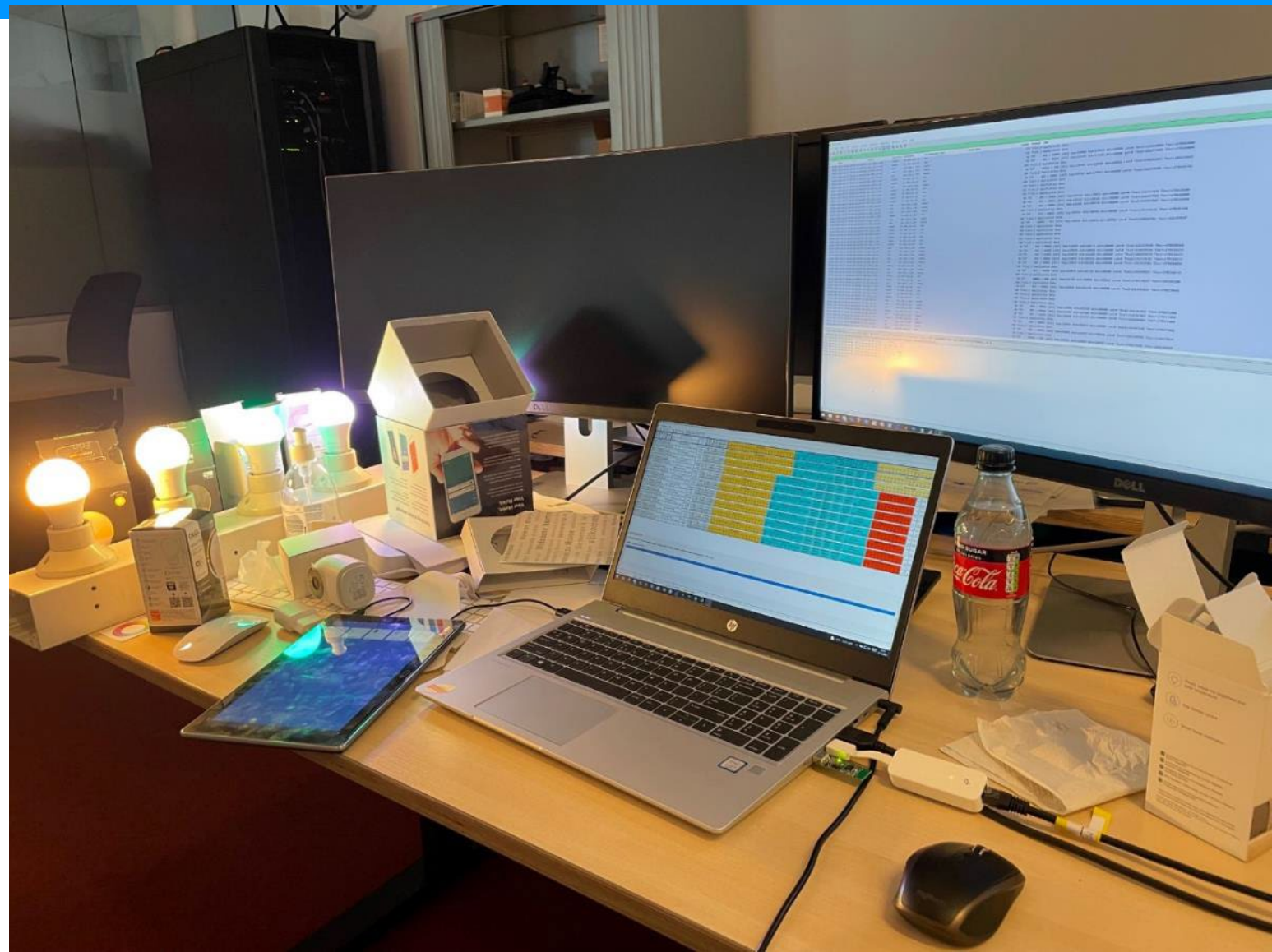
- **Market surveillance/regulation/enforcement**
- **Gather knowledge**
- **No certifying**
- **Verifying testability of regulations**
- **Measurements were performed using:**
  - **Baseline requirements from EN 303 645 V2.1.1.**
  - **Conformance assessment based on TS 103 701 V1.1.1.**

IoT Testlab - Configuration



IoT Testlab - Costs

- "IoT Testing laboratory"
- Networking: €4000~
- Server: €5000~
- Workplace: €10000~
- Total under €20000
- 2 FTE ethical hackers
- 0.2 FTE system engineer (for basic IT maintenance and management)



Radio Equipment Directive (RED)

Article 3.3 (d, e, f, i) of the Radio Equipment Directive states:
“…
(d) radio equipment does not harm the network or its functioning nor misuse network r esources, thereby causing an unacceptable degradation of service;
(e) radio equipment incorporates safeguards to ensure that the personal data and priva cy of the user and of the subscriber are protected;
(f) radio equipment supports certain features ensuring protection from fraud;
…
(i) radio equipment supports certain features in order to ensure that software can only be loaded into the radio equipment where the compliance of the combination of the ra dio equipment and software has been demonstrated. ”

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 devices easy
  13. Validate input data
- Data protection provisions for consumer IoT

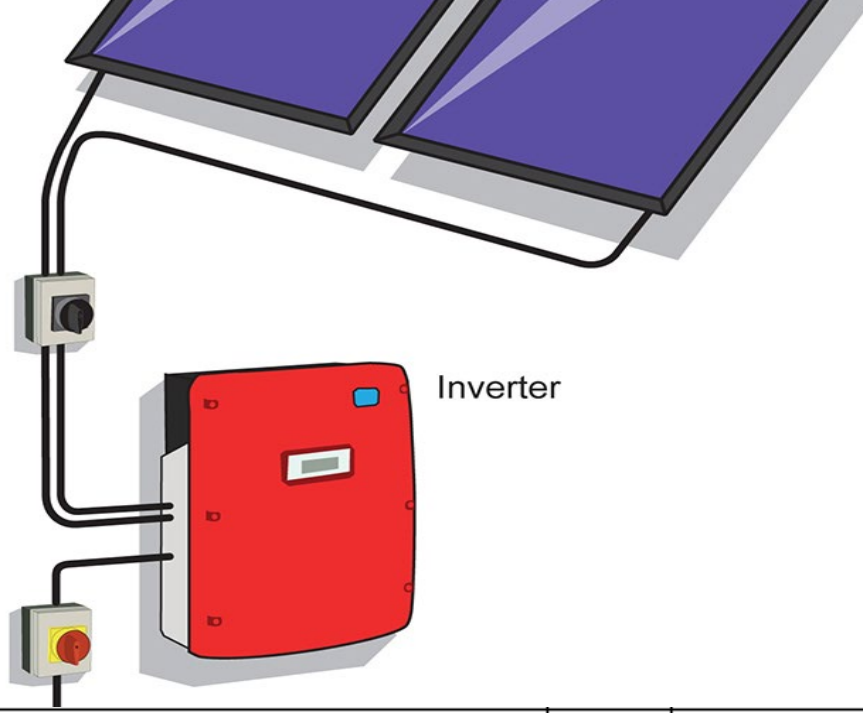
Test Report – Password example

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

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.**

Future projects

- **Testing of 2/3/4/5G wireless connected devices.**
  - **Electric vehicle charging points**
  - **Cars/bikes**
  - **Sensors/Industrial IoT**
  - **Smart meters**
- **Smartphones (TS 103 732, Consumer Mobile Device Protection Profile)**
- **“Home Gateway” (TS 103 848, Cyber Security for Home Gateways, vertical from Consumer Internet of Things)**
- **“Smart toys”**

Thank you

- info@agentschaptelecom.nl
- Gurkan.Kirca@agentschaptelecom.nl