Hogyan fejlesszünk, vásároljunk, integráljunk biztonságos IoT eszközöket

Molnár Ferenc Tamás, CCLab

Debrecen, 2022.11.04.

CCLAB

THE AGILE CYBERSECURITY LAB


AARGH!
CloudPets

NEMZETI KONZULTÁCIÓ A KIBERBIZTONSÁGRÓL

Egyetért ön azzal, hogy bűnözői csoportok a magyar adófizetők pénzéből telepítsenek kiberfegyvereket a háztartásokba, melyekkel a magyar családokat elzárhatják az energiától, ivóvíztől és az internetkapcsolattól?

IGEN ☐ **NEM** ☐

Ki figyeljen erre?

- Eszközgyártó (biztonságos terméket fejlesszen)
- Forgalmazó (csak tanúsított terméket értékesítsen)
- Infrastruktúra-szolgáltató (csak tanúsított terméket engedjen a hálózatára)
- Platform-szolgáltató (biztonságos terméket fejlesszen, rendszert üzemeltessen, auditáltassa magát)
- Felügyelő hatóság (megfelelőségi kontrollokat írjon elő, felügyelje a szolgáltatókat)
- Megfelelőségértékelő szervezetek
- Felhasználók (tőlük ne várjunk semmit)

Mi a biztonságos?

- Hogy definiálni tudjuk, ahhoz 2 dolog kell
  - Követelményrendszer (pl. Common Criteria)
  - Vizsgálati módszertan (pl. CEM, OWASP Web Security Testing Guide)
- És még egy - Megfelelőségértékelési rendszer
  - Ne kelljen mindent nekünk megvizsgálni
  - Laborok, tanúsító szervezetek, akkreditáló és felügyelő szervezetek

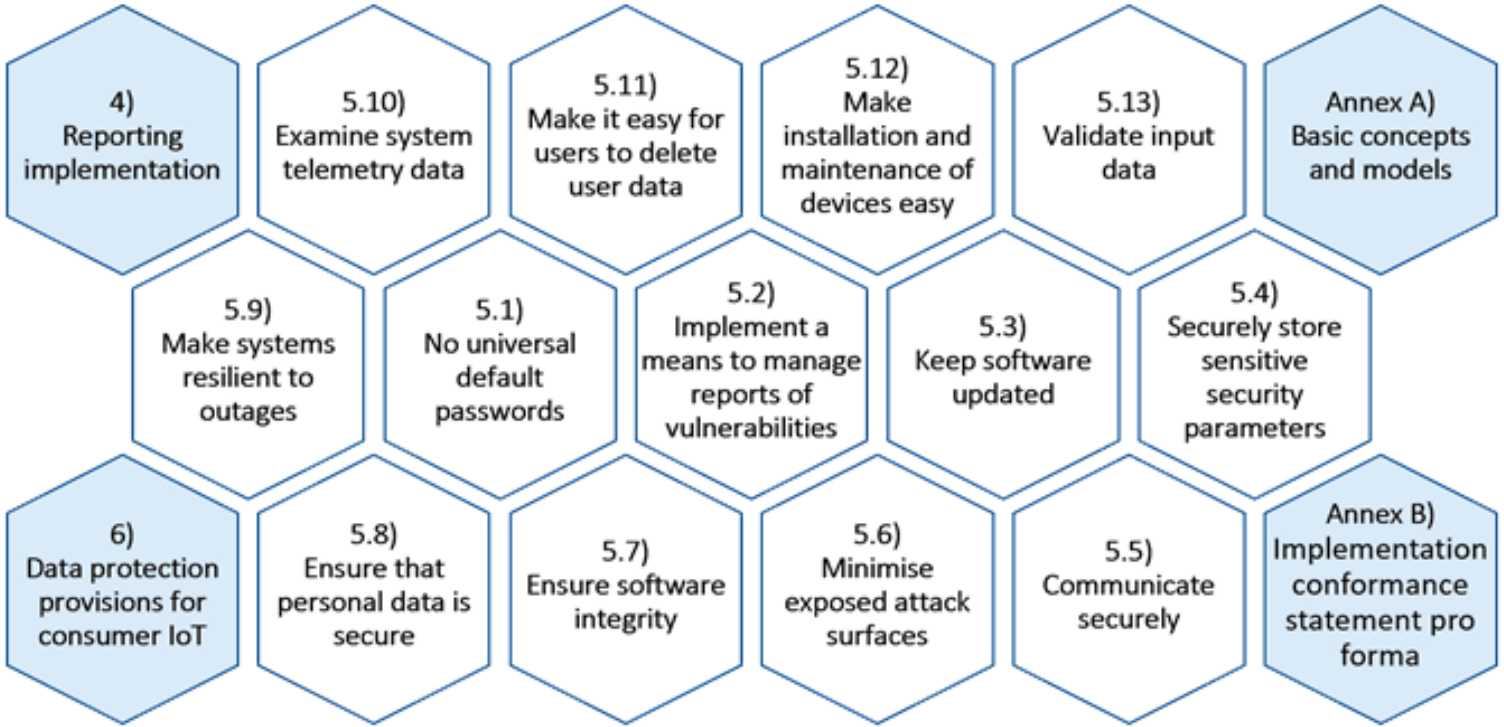
Hogyan érdemes felépíteni

- Egységes követelményrendszer, rétegezett felépítés
- TPM Chip CC EAL5-6
- Broadband router, smart meter gateway CC EAL4
- Home gateway, smart meter CC EAL2-3 (NDcPP)
- Cloud service, EUCS (European Cybersecurity Certification Scheme for Cloud Services)
- Consumer IoT eszköz, ETSI EN 303 645

Consumer IoT kiberbiztonság - ETSI EN 303 645

- Cyber Security for Consumer Internet of Things: **Baseline** Requirements
- Nulláról az egész jóra húzza a szintet
- Minden jelentősebb ismert támadásra ad választ (pl. Mirai botnet)
- Átfogóan lefedi a kiberbiztonsági és adatvédelmi jó gyakorlatokat
- Pragmatikus megközelítés hogy elérhető legyen a KKV szektornak

Tartalomjegyzék



5 Cyber security provisions for consumer IoT

5.1 No universal default passwords

Provision 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.

NOTE 1: There are many mechanisms used for performing authentication, and passwords are not the only mechanism for authenticating a user to a device. However if they are used, following best practice on passwords is encouraged according to NIST Special Publication 800-63B [i.3]. Using passwords for machine to machine authentication is generally not appropriate.

Many consumer IoT devices are sold with universal default usernames and passwords (such as "admin, admin") for user interfaces through to network protocols. Continued usage of universal default values has been the source of many security issues in IoT [i.17] and the practice needs to be discontinued. The above provision can be achieved by the use of pre-installed passwords that are unique per device and/or by requiring the user to choose a password that follows best practice as part of initialization, or by some other method that does not use passwords.

EXAMPLE 1: During initialization a device generates certificates that are used to authenticate a user to the device via an associated service like a mobile application.

To increase security, multi-factor authentication, such as use of a password plus OTP procedure, can be used to better protect the device or an associated service. Device security can further be strengthened by having unique and immutable identities.

Provision 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.

EXAMPLE 2: Pre-installed passwords are sufficiently randomized.

As a counter-example, passwords with incremental counters (such as "password1", "password2" and so on) are easily guessable. Further, using a password that is related in an obvious way to public information (sent over the air or within a network), such as MAC address or Wi-Fi® SSID, can allow for password retrieval using automated means.

Supporting documents

- ETSI TS 103 848
  - Cyber Security for Home Gateways
  - extending ETSI EN 303 645
- ETSI TR 103 621
  - Guide to Cyber Security for Consumer Internet of Things
  - Provision 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". (ETSI EN 303 645 [i.1]).
  - Example 1: The consumer IoT device password for the factory default state is printed on a sticker under the device casing. During the initialization phase, the user is requested to provide a new password and the procedure cannot complete without the new password being different from the default state password.

Konklúzió

- Ha Európa a piac, Consumer IoT a termék
- Akkor az ETSI EN 303 645 a kötelező olvasmány

THE AGILE CYBERSECURITY LAB