.. IoT Security Initiative Cybersecurity Principles of IoT

- Main
-
- Guidance
    - Cybersecurity Principles of IoT
    - Security Design Best Practices
    - Privacy Design Best Practices
    - Product Security Launch checklist
    - Secure-Me: D-OPSEC
- Device-SLA
- Attacker M.O.

Cybersecurity Principles of IoT v1.1

The 22 principles cited below establish a guiding foundation for how to operationalize Internet of Things systems and services so that key security and privacy elements are taken into account for the end-to-end solution.

A note on the term "Device"

For our purposes here, we will consider a “device” as being any standalone embedded system that has external wired or wireless communication capabilities integrated.

Principle 1

An end-to-end solution is designed, developed, operated and managed according to industry-best-practice security and privacy guidelines.

Principle 2

A device has a security rating established and identified by its manufacturer using the Device Security Rating System (DSRS) or similar model.

principle 3

Secure SDLC best practices and supporting tools are utilized for all software in the end-to-end solution.

PRINCIPLE 4

Systems and applications in the end-to-end solution are validated with security vulnerability testing prior to production release.

PRINCIPLE 5

To remain in operation, a deployed and functional device has a known and identifiable owner.

PRINCIPLE 6

To remain in operation, a deployed and functional device always has a known and identifiable operator/maintainer.

PRINCIPLE 7

A device is clearly marked with the short link of its corresponding Device Security Level Agreement (DSLA).

PRINCIPLE 8

The public vulnerability disclosure contact details are clearly identified on both the manufacturers Device Security Level Agreement (DSLA) page and any solution web sites.

PRINCIPLE 9

The Device Security Level Agreement (DSLA) identifies the public security or safety alerts filed for the device historically to date.

PRINCIPLE 10

The software update support timespan and frequency are clearly identified in the manufacturers Device Security Level Agreement (DSLA) page.

PRINCIPLE 11

All device Industry use classifications, with the allowed exception of "Consumer," provide a software patch update support timespan of not less than 6 years from manufacture date.

PRINCIPLE 12

The Device Security Level Agreement (DSLA) for a device identifies the software update mechanism as either Direct-Physical, Remote-Network-Automatic, or Remote-Network-Manual facilitated.

PRINCIPLE 13

The Device Security Level Agreement (DSLA) for a device identifies the firmware versioning history.

PRINCIPLE 14

A device with inbound network services running is supported with remote-network firmware updates by the manufacturer in order to remain in an operational state.

PRINCIPLE 15

A device without a User Interface notification system and without an owner/operator patch notification system implements Remote-Network-Automatic firmware updates.

PRINCIPLE 16

A device with a system classification of "Gateway" implements Remote-Network-Automatic firmware updates.

PRINCIPLE 17

A device storing personal or operationally sensitive information integrates data wipe capabilities into its design and architecture for standard use and decommissioning scenarios.

PRINCIPLE 18

Devices supporting sensitive or safety-critical functions are designed and architected to continue safe and secure operation during communications interruption or failure.

PRINCIPLE 19

A device is designed and architected to protect personal privacy through data collection transparency and anonymization of user activity.

PRINCIPLE 20

A device clearly identifies the collection or processing of personally identifiable data in the Device Support-Level Agreement (DSLA).

PRINCIPLE 21

A device in active use to identify and/or track persons and their activity is overtly identified as such to the public in the devices operating environment.

PRINCIPLE 22

A published Device Security Level Agreement (DSLA) is maintained once initially created to provide the change history of material modifications to this public information.