20-07-09

Proposal from ARGE SDL WP E Cyber -2

Based on ETSI EN 303 645 V2.1.0 2020-4

5.7 Software integrity

- The SDL device shall verify its software using secure boot mechanisms.
- The integrity check shall be based on a hardware root of trust by utilizing secure storage of encryption/signature keys.
  (only applicable for security level High)
- When applying SW updates on the HW elements (locks, readers, etc.) integrity and authenticity checks must be implemented before applying updates on the firmware.
- Microprocessor reprogramming is disabled. Once the processor is programmed and tested, it is "locked" or "disabled" to avoid reprogramming.

Ex: Firmware hash is generated and signed by manufacturer. Public key of manufacturer is stored in the secure area of the boot loader, so that boot loader may verify authenticity of firmware.

Ex: Firmware is encrypted with symmetric key stored in the inaccessible area of the boot loader.

Ex: Access to firmware update is only possible via special mode that is limited to administrator or password / encryption key that is unique to the device and which is stored in the inaccessible area of the boot loader. Firmware is not continuously or regularly monitored for integrity.

If physical access to CPU is possible, the CPU shall only be erased entirely and a new firmware may be uploaded without bootloader, so that the firmware cannot be modified. During this process the security relevant cryptographic keys are deleted automatically.

If security checks for software integrity fail, the administrator shall be alerted.

- The device shall detect and alert the user of unauthorized change.
- lf an unauthorized change is detected to the software, it shall fallback lo the prior sw and an shall send alert lo the Administration/ User SW /Hosting SW where applicable

Test methods /Validation Software integrity

- A declaration or formal procedure showing how is the authenticity and integrity of the firmware update is applied on the product (encryption, hash etc.)
- Description of implementation?
- A declaration or formal procedure showing how is this being applied on the product.
- Try lo update with inappropriate SW

5.8 Secure personal data

- The confidentiality of personal data transiting and communicated between the SDL and a service, especially associated services, shall be protected, Personal data in transit must be encrypted with best practice cryptography.
- Personal information that is stored on registration servers (e.g. phone numbers) shall be protected. In the case where reading access to registration servers is allowed by mobile phone app then the information is regarded as insecure. In this case, further measures are necessary to prevent unauthorized access to this data
- Personal data in the cloud background system shall be protected by standard means.
- When audit trails are transmitted, they shall be end 2 end encrypted.
- Privacy policy shall be available for customers
- All services of the cloud background system shall be kept up to date.
- All data that is stored on the cloud server or on the locally installed server that may be accessed by a software or by an app using built in credentials is considered insecure because apps and software may be disassembled or reverse engineered
- Audit trails that are usually stored on the SDL are considered sensitive personal data.
- Cloud services and mobile apps shall comply with GDPR requirements (consent lo processing, protection of data, information about stored data, deletion on request) .

Find solution for access logs and deletion requirements according to GDPR.

Test methods /Validation Personal data

- Personal Data Privacy policy shall be available for customers (specifying which personal data is being processed on the systems and how it is protected, also whether the manufacturer has access lo the personal data or not)
- Analyse communication between elements processing personal data and ensure **it** is encrypted (e.g. between the mobapp and the backend with TLS).
- Documentation of cloud service and mobile app

5.9 Resilient telemetry data systems

- The SDL devices shall remain operating and locally functional in the case of a loss of network access and shall recover cleanly in the case of restoration of a loss of power.
- In the event of power loss, SDL shall regain its normal operating state within 1 minute after regaining power.
- In the event of an outage of network or power, the customer must be able to open a door, so lock shall remain operating.
- In the event of network connection lost, the SDL shall work in offline mode and shall at least unlock for special emergency users.
- The device shall have a backup solution on how to operate the lock in case the main power fails.

- Device behaves securely after a denial of service attack
- Network and power losses shall be documented in a special part of the audit trail storage so that they cannot be overwritten by normal operations.
- In the case where the SDL is permanently and directly connected to a network, it shall locally store all data that it usually transmits through the network during a power loss and send this locally stored information once it regains network connectivity

Test methods /Validation resilient telemetry data systems

The device must have a backup solution on how to operate the lock in case the main power fails.

- Verify that the locks can operate in the event of a network or power outage (e.g. remove batteries from the gateway and ensure lock can be open)
- Disconnect from network and operate
- Conduct DDoS attack against devices (e.g. using a Bluetooth client against the lock). After the DDoS is finished, the lock must become fully operative.

5.10 Telemetry data system

- If telemetry data is collected from SDL devices and services, such as usage and measurement data, it shall be examined for security anomalies.
- The owner of the lock shall have the possibility to consent to collecting telemetries data from the lock and the mobile app**.** Based on telemetries data from the lock and the app checks for anomalies (e.g. failed updates) the operator is notified about security anomalies.
- This shall apply lo the use of mobapp - cloud interfaces

Option

- Telemetry data that is sent to the cloud background system **may** be checked for anomalies by artificial intelligence. When anomalies are detected, the owner/administrator shall be alerted

Test methods /Validation telemetry data system

- Provoke a failed update, check operator notification.
- Confirm whether mobapp events are being registered and monitored by the manufacturer on the cloud infrastructure.

5.11 Delete user data

- The SDL shall have a simple process to set it to factory state with all personal data, cryptographic keys, project specific data erased.
- Users shall be given clear instructions on how to delete their personal data.
- Users shall be provided with clear confirmation that personal data has been deleted from services, devices and applications.

Option

- Normal individual users that are authorized to unlock the door **may** not have the possibility to erase themselves from all memories and databases because of immutable audit trail (inconsistency with 5.11).

Test methods /Validation of delete user data

- Decommissioning process for HW components (locks, readers etc.) must be defined and available for end-users (e.g. secure destruction, send the components back lo the manufacturer etc.)
- For deleting data on the cloud infrastructure including logs etc., there must be a procedure available for sending this request lo the manufacturer.
- For deleting data stored on the mob app, the app deinstallation process should be sufficient?
- Check confirmation
- Check wizard

5.12 Installation and maintenance

- The manufacturer shall provide users with guidance on how to securely set up their device. Security options shall be explained during the installation procedure itself with all advantages and disadvantages.
- The manufacturer shall provide users with guidance on how to check whether their device is securely set up. Secure configurations should be enforced (there is not option for customers to install / operate insecurely)
- The mobile app / admin SW provides a wizard lo setup the device where a subset of configuration options with the common defaults already specified and with appropriate security options already turned on by default**.**

Option

- Installation and maintenance of SDL **should** involve minimal number of choices and decisions by the user. If there are several choices, the decisions **should** follow security best practice shall be the default.
- A security check of the security settings **may** be performed at any time and its result shall be displayed to the administrator

Test methods /Validation of installation and maintenance process

- Check wizard.
- Check user manual. Installation process must be clear and available for end users.
- Ensure that there are only secure ways for configuration.

5.13 Input data

- The SDL software shall validate data input via user interfaces or transferred via Application Programming Interfaces (APIs) or between networks in services and devices.
- This is to avoid allowing malformed request into the application and avoid security issues
- All input data shall be checked for validity by the background cloud system services itself (not only by the input mask on the browser). All numerical data bounds shall be checked.
- The overall length of data packets shall be checked and packets with incorrect lengths shall be discarded to prevent buffer overflow hacks.
- Interfaces provided to integrators shall check the validity of numerical data bounds as well as packet lengths.
- Data entered via internet forms / mobile phone forms shall be routinely “sanitized” (i.e. stripped from dangerous characters like backslashes, slashes, apostrophes).

Test methods /Validation input data

- SW implementation documentation
- Verify input validation (conducting penetration test against SW which basically consists in finding implementation bugs using malformed /semi-malformed data injection in an automated fashion and/or reviewing source code to ensure input validation is conducted).

ADDITIONAL REQUIREMENTS: OWASP FOR IOT.

- Community for defining security methodology / standards for Web application and IoT.
- All these principles must be tested with a penetration tests / vulnerability scanning for hardware elements + software.
- E.g. access controls and authentication tests, session management, input validation, open ports, tampering, etc.
- The new smart lock standard should specify the set of technical tests to be conducted to achieve the certificate

Some references:
https://owasp.org/www-project-web-security-testing- guide/assets/archive/OWASP Web Application Penetration Checklist_v1 1.pdf

https://owasp org/www-chapter-pune/IoT Device Pentest by Shubham Chougule.QQf

ADDITIONAL REQUIREMENTS: ENISA Candidate scheme v1.0 - 01/07/2020