psacertified™

10 Security Goals

The most common IoT hacks can easily be prevented by following security best practice. The 10 security goals provide a foundation for IoT products. They are in the DNA of PSA Certified and inform the whole framework and evaluation scheme.

Unique Identification

To interact with a particular device, a unique identity should be assigned to the device and this identity should be attestable. This identity facilitates trusted interaction with the device for example, exchanging data and managing the device.

Security Lifecycle

Devices should support security lifecycle that depends upon software versions, run-time status, hardware configuration, status of debug ports and the product lifecycle phase. Each security state of the security lifecycle should be attestable and may impact access to the device.

Attestation

Attestation is the evidence of the device's properties, including the identity and lifecycle security state of the device. The device identification and attestation data should be part of a device verification process using a trusted third party.

Secure Boot

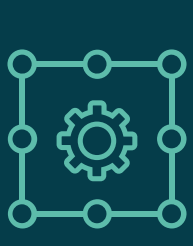
To ensure only authorized software can be executed on a device, secure boot and secure loading processes are required. Unauthorized boot code should be detected and prevented. If the software cannot compromise the device, unauthorized software may be allowed.

Secure Update

Secure updates are required in order to provide security or feature updates to devices. Only authentic and legitimate firmware should be updated on the device. Authentication, at the time of download, may be performed however, the execution of the update must be authorized via secure boot.

Anti-Rollback

Preventing rollback to previous software versions is essential to ensure that previous versions of the code can't be reinstated. Rollback should be possible for recovery purposes only when authorized.



Isolation

Isolation aims to prevent one service from compromising other services. This is done by isolating trusted services from one another, from less trusted services and from un-trusted services.

Interaction

Devices should support interaction over isolation boundaries to enable the isolated services to be functional. The interfaces must not allow the system to be compromised. It may be required to keep the data confidential. Interaction should be considered both within the device and between the device and the outside world.

Secure Storage

To prevent private data being cloned or revealed outside the trusted service or device, it must be uniquely bound to them. Confidentiality and integrity of private data is typically achieved using keys, which themselves need to be bound to the device and service.

Cryptographic / Trusted Services

A minimal set of trusted services and cryptographic operations should be implemented as the building blocks of a trusted device. These should support critical functions including security lifecycle, isolation, secure storage, attestation, secure boot, secure loading and binding of data.

The 10 security goals provide a baseline for PSA Certified Level 1 evaluation, helping you showcase your security capabilities.

Learn more about PSA Certified here