Shield

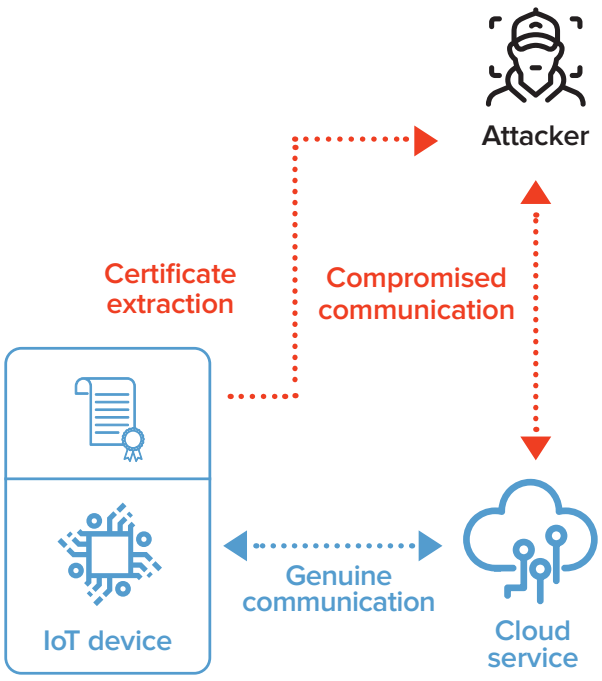
RESECURE YOUR IoT DEVICES AT ANY TIME

Protect your data from security breach and your intellectual property from theft over a simple firmware update (Over-the-Air).

AGILE BOLT-ON-SECURITY ENHANCING THE SECURITY OF DEPLOYED DEVICES

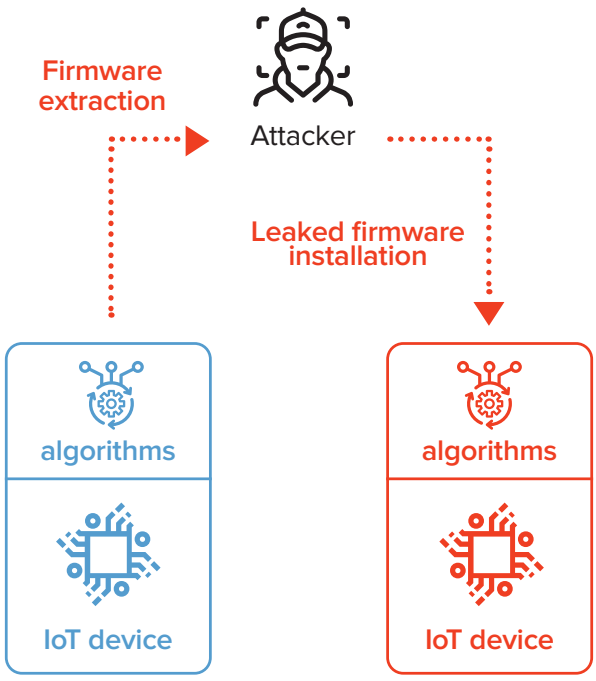
Secure storage of secrets

Cloud platforms such as AWS IoT and Microsoft Azure IoT bring tremendous value to device fleet managers and device makers by bringing advanced off-the-shelf features and building blocks. Brownfield devices are, however, often **ill-equipped to securely store authentication tokens** of these cloud platforms (in the absence of a TPM). An attacker having access to these tokens could **compromise the whole IoT fleet, damaging business revenues and company reputation**.



Supply-chain IP protection

Device firmware represents precious Intellectual Property, containing Machine learning models, algorithms, proprietary data, etc. As device owners rely on third parties to produce their devices, they are consequently **exposed to Intellectual Property (IP) leakage** when sending their firmware. To counter IP leakage, **static and dynamic protections** must be implemented in the firmware to ensure that a third party cannot reuse the firmware on another device **or steal its data**.



Quarkslab

Active modules

- **Data Protection :** Secure storage of secrets (cloud authentication tokens)
- **App Protection :** Supply-chain IP protection

Key features	Key benefits
Secure storage of secrets (OAUTH, API Keys, x509, tokens, credentials, PII data, etc.) ▶ An abstraction layer for secrets storage - Software-based solution, with software cryptography (white-box cryptography) - Does not need a TPM ▶ Deployment modes - SDK (C library) **Supply-chain IP Protection** ▶ Combination of static and dynamic protections (more than 30 available) ▶ Languages supported: - C/C++/Java/Objective-C/Swift - Possibility of custom development to add languages ▶ Targeted Architectures: - Mobile/Embedded and desktop architectures (ARM/ARM64/x86/x64) - Suitable for constrained environments - Support of a specific architecture on demand	▶ Prevent data leaks and security breaches by securely storing all sensitive and business-related data (cloud connection tokens, keys, billable data...) ▶ Enhance your device fleet security posture without having to replace brownfield devices ▶ Easily re-secure an IoT fleet spanning several generations with different hardware ▶ Protect your business revenues and Intellectual Property by preventing device counterfeiting

RE-SECURE YOUR IOT DEVICES NOW, PROTECT YOUR REVENUE !

Reach out to our experts for a consultation

quarkslab.com/contact