Protecting your Assets: IP Protection – essential to protect your business and your customers

By Stephan Spitz, Chief Strategy Officer, Secure Thingz

Counterfeit components in IoT hugely impact market and reputation

Consumer brands have long had issues with counterfeit goods and cloning. But in the world of connected devices, the consequence of grey market components has the potential to create much more damage to the market, to brand reputation and to safety. The internet of things (IoT) is clearly beneficial to many aspects of business process improvements, driving efficiency, reducing downtime, and much more, in almost every industry vertical. However, the fact that devices are connected via the internet means there are multiple points within the network that could also be affected.

It is a major concern when manufacturers do not have full visibility of the authenticity of devices and products within the supply chain. In a 2018 Deloitte survey[1] of 500 procurement leaders from 39 countries, it was found that supply chain transparency is poor, with 65% of them having limited or no visibility beyond their tier one suppliers.

Counterfeit components are a safety risk

In addition, counterfeit components are a safety risk. It cannot be guaranteed that the Software IP on the final device has no modifications or that the underlying hardware offers the same reliability and robustness as specified by the OEM. Stolen IP can be modified in a fraudulent manner and can contain backdoors and side channels. The lack of integrity means modified Software IP can potentially enter connected safety-critical systems, a good example, of which is a modern car. If a cloned component is introduced and does not meet the original component's specifications, the equipment it is monitoring may end up not meeting the necessary operating requirements, especially if the newly introduced counterfeit components have poorer characteristics than the original device.

Depending on the system or application which relies on these components, there could be many different outcomes which can have significant unintended consequences. For example, in a car, it could result in failures in safety critical functions that are integral to autonomous driving systems[2]. These failures could be due to incorrect monitoring of environmental parameters and tolerances that are necessary to avoid accidents.

Another area of concern is in the health care sector. If compromised devices, that rely on accurate measurement of body parameters, cause incorrect dosage of medicines; patients could end up being severely harmed or even resulting in death because of modified software IP producing incorrect results.

In general, a distributed supply chain bears the risk that software IP can be intercepted by hackers to introduce backdoors and malicious code.

1) https://www2.deloitte.com/global/en/pages/strategy-operations/articles/global-cpo-survey.html
2) https://www.techradar.com/news/cybersecurity-as-important-as-brakes-for-future-cars-jaguar-land-rover-ceo-sayscpo-survey.html

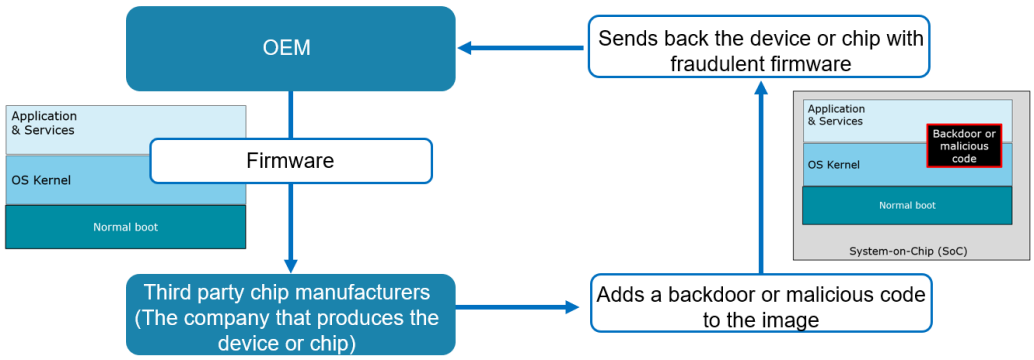

Fig. 1 Attacker can modify software IP, which is not integrity protected

Functional Safety and IP Protection

C-Trust offers efficient IP protection based on state-of-the art cryptography. A digital signature ensures integrity and authenticity of the firmware by binding it to a Secure Boot Manager (SBM) provided by Secure Thingz. This SBM itself is protected from modifications by the chip hardware and personalized by a public key, which allows an integrity check and a verification of the authenticity of the safety-critical firmware.

A confidentiality protection mechanism can be added that cryptographically encrypts the safety-critical firmware. This prevents reverse engineering and theft of software IP, because it is end-to-end encrypted from the development environment (IAR Systems Embedded Workbench with C-Trust) through to the point at which the software is booted and executed on the System-on-Chip (SoC).

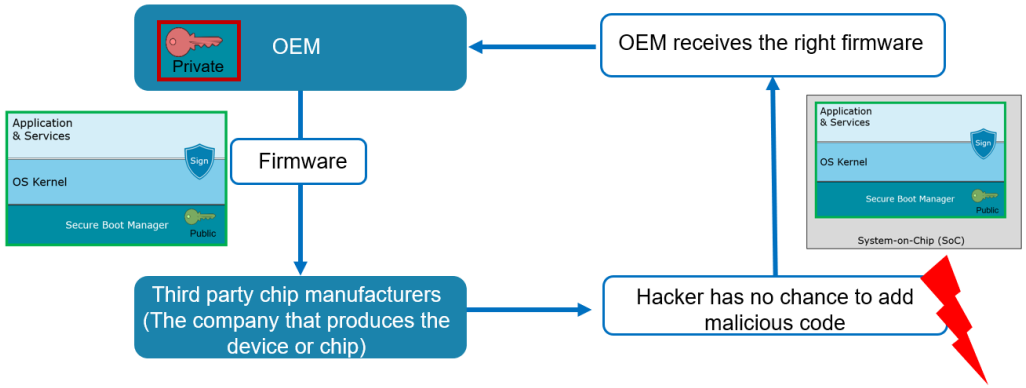

Fig. 2 Efficient prevention of fraudulent modifications by sealing the software IP with a digital signature

IP Protection with C-Trust

A key design requirement of C-Trust is to simplify the development process. Adding IP Protection to an application does not require the development engineer to be a crypto expert or have knowledge of the management of cryptographic keys. In an out-of-the-box wizard the IP Protection feature can be configured in a few simple steps. IP Protection settings such as “Basic signature checking” are available which protect the software IP from modifications and allows only authenticated firmware to be booted. It is possible to enhance this feature by selecting “Full encryption” of the firmware, which adds additional protection against reverse engineering and IP theft.

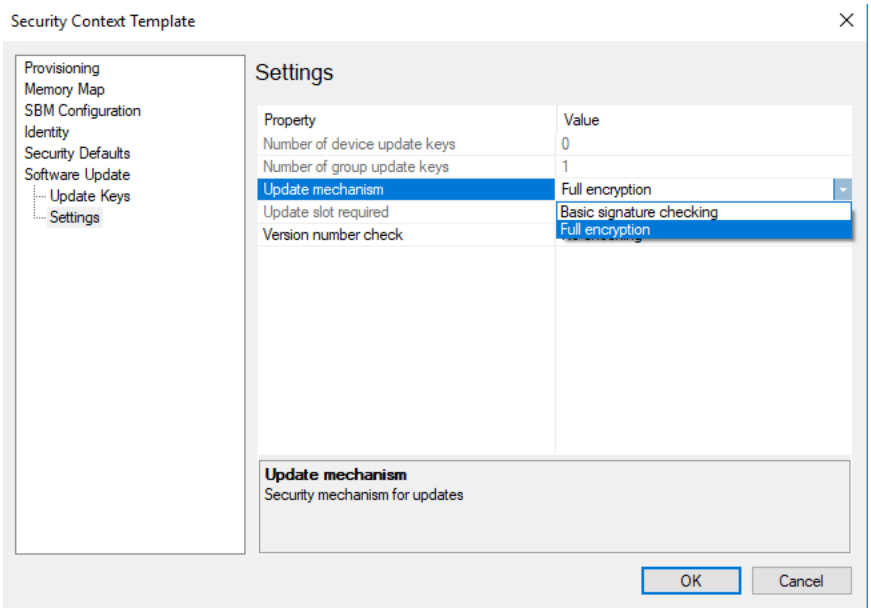

Fig. 3 Wizard to configure IP Protection feature which checks the authenticity and integrity (Basic signature checking) or confidentiality protection (Full encryption)

A further configuration option is the protection of downgrading the firmware to an older version (also known as anti-rollback). The "Version number check" feature prevents firmware updates from using older versions which may have security vulnerabilities. This feature prevents attackers from taking advantage of any security flaws in older firmware versions.

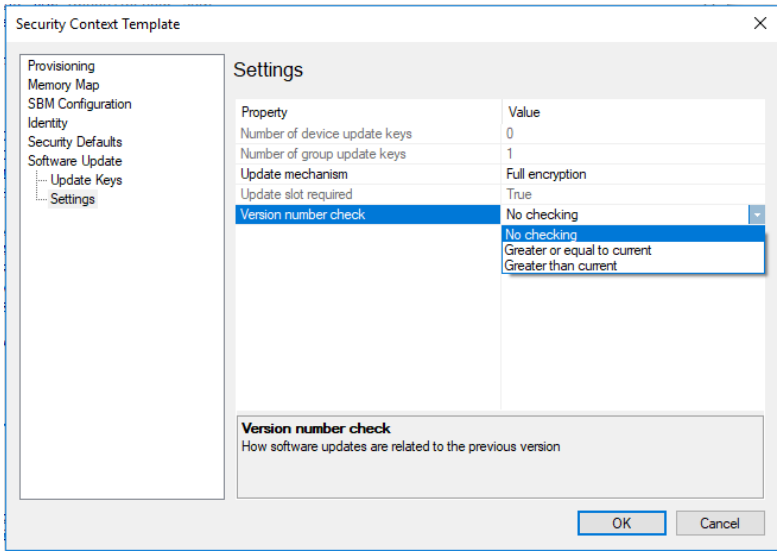

Fig. 4 Wizard to configure version number checking to avoid an attack based on an older firmware version

How to protect intellectual property is an increasing concern for many companies, being the core of the business assets. Embedded application work and development are often considered critical investments and might comprise several man years of resources and efforts before any product launch. Companies can easily increase the protection of their investments significantly with C-Trust, by implementing foundation security measures such as signing and encrypting the codebase and with anti-rollback policies to avoid firmware downgrade.