Position Paper by Trusted Objects
May 2020

Software and IP Protection for OEM

Introduction

The term "software and IP protection" refers to the protection of OEM's software code against security breaches. The purpose of this position paper is to analyze the vulnerabilities leading to software and IP hacking and theft, to look at the different solutions and their gaps and to finally introduce a new concept adapted to embedded systems.

Software and IP protection: a major concern for OEM executives

As the risk of security breaches is growing, it is no surprise that the management and protection of the software and IP have become major concerns for OEM executives.

The average direct revenue loss per security breach is now **exceeding $3m (*)** on top of which, indirect damages such as company brand reputation, safety and services efficiency can result from a weak protection of software and IP.

Vulnerabilities analysis

When referring to software and IP protection, the main vulnerabilities occur, 1) during the device manufacturing process, 2) on the off-the-shelf device and 3) during the OTA (Over The Air) software update.

1) <u>During the device manufacturing process</u>
   In many cases, software and IP are programmed into the devices in clear, without any protection. Very often, code, data and secret keys are sent in clear mode to the programming equipment or encrypted with a key that can be easily recovered. Furthermore, code, data and secret keys are usually stored in the programming engine, sometimes for an unlimited period.

2) <u>On the off-the shelf device</u>
   3rd parties can take advantage of the software vulnerabilities and use hacking techniques including reverse engineering, code dumping or code tampering to create cloned devices. Reverse engineering based on side-channel attacks can be done with a $500 tool with basic instructions available on the web.

3) <u>During the OTA software update</u>
   In order to perform OTA software updates securely, a secure channel must be established between the servers and the devices. Unfortunately, many software products still do not use proper authentication, leaving this channel open to exploitation.

(*): *figures from Accenture.*

Position Paper by Trusted Objects
May 2020

Existing solutions and gaps

Security technologies have been deployed for decades to protect data and software, including state-of-the art cryptography, digital signature, secure boot, obfuscation of executables, to name just a few examples.

However, there are still some gaps with those existing solutions for embedded systems:

1) Security in silos

   A security chain is as weak as its weakness element. Should the security measures not address the 3 vulnerabilities mentioned above, like security at the manufacturing level for instance, it will create a hole in the security chain to protect software IP.

2) Impact on the device performances

   Most of the security solutions have been developed for systems with high computing capabilities, such as servers, PC, smartphones, etc…
   Embedded systems have specific constraints in terms of computing performances, size of code, power consumption. As a result, many solutions are significantly downgrading the performance of the embedded system (speed, power consumption).

3) Cost effectiveness
   Security is always a trade-off between cost and risk. Since the risks are not always well identified, OEM will be naturally looking for the cheaper solution.

New concepts for software and IP Protection

New solutions have been developed for software and IP protection at the device level, taking into account the constraints of embedded systems without compromising on security.

Additionally, some players can now provide a full set of security solutions ensuring a seamless protection all along the “chain of trust”.

Secure libraries based on cryptography and obfuscation techniques have proven to be efficient against reverse engineering, and easy to implement.

Centralized solutions for secure programming are getting user friendly and easy to implement, at effective cost.

Trusted Objects

Trusted Objects has pioneered new concepts and innovative solutions for software and IP protection, including secure libraries, secure programming and secure boot for OTA secure software update.

Trusted Objects has also partnered with **System General** to have TOPS, its secure programming solution, qualified on System General programming equipment.

www.trusted-objects.com

www.sg.com.tw