Challenges in the design of Hardware Security Modules that protect high level classified information to achieve a security certification with the highest security level

Ángel Custodio Espinar

TECNOBIT – Oesía Group

Valdepeñas (Ciudad Real), Spain

acustodio@oesia.com

Abstract

A Hardware Security Module (HSM) is an electronic device that protects valuable information mainly by using cryptographic mechanisms. The HSM also implements a set of security measures to protect the information, the keys, the parameters, the implementation of these cryptographic mechanisms and all the security functions from all the possible threats. In the case of military or governmental information, this valuable information is classified following a classification system with different levels depending on the value of the information or the outcomes of the compromise of this information. Each nation or organization defines its own security domain (national, NATO, European Union…). A security certification is always required for a HSM to be allowed to process classified information. This certification process is always done by the National Security Agency (NSA) of the nation of the manufacturer of the HSM, but in the case of organizations like NATO or EU, a second evaluation is done by another agency from the organization (SECAN in the case of NATO) or by the NSA of a second nation (a nation member of AQUA in the case of the EU).

The security requirements requested in this certification process depend on the security level of the HSM. This security level depends on two factors: the classification level and the threat level of the environment where the HSM is going to be operated. The highest threat level happens when the HSM is operated on the field, without any external protection. The HSM is assigned with the highest security level when the classification level of the information and the threat level are the highest. The higher the security level, the stricter and more difficult to fulfil the security requirements.

In this talk we present the main challenges that the HSM manufacturer companies face when designing a HSM that protect high level classified information to achieve a security certification with the highest security level. We must fulfil all the security requirements but, at the same time, we must fulfil Size, Weight and Power (SWaP) requirements and also usability and logistics requirements imposed by our customers. Many times, these requirements collide with the security requirements, making this engineering activity extremely challenging. Sometimes, the NSA is very conservative and does not allow the implementation of state-of-the-art security measures improving the fulfilment of the other requirements because they consider they are not mature enough (for example PUF functions). Moreover, we must provide exhaustive evidences of the implementation of each security function. This makes impossible to use components that implement security functions when the company that manufactures the component does not want to provide detailed technical information to support the certification or when its NSA does not allow it, considering that this information would be provided directly to the NSA in charge of the certification. This situation makes impossible to include that component in the design and forces us to make an alternative implementation of that security function, normally in a more complex, more costly, and less optimal way. Finally, the situation is even worse when the HSM must protect EU classified information because there is a requirement to use only components designed and manufactured in an EU nation when they are used to implement critical security functions. This requirement complicates the selection of hardware components because of the lack of EU manufactured integrated circuits.