

Board ID Tutorial 3 - Certifications

Introduction

This tutorial is designed to provide an introductory overview of types of security certifications.

Contents

BOARD ID TUTORIAL 3 - CERTIFICATIONS	1
INTRODUCTION	1
CONTENTS	1
CERTIFICATIONS.....	2
FIPS 140-2 CERTIFICATION.....	2
COMMON CRITERIA (CC) CERTIFICATION	3

Certifications

Certifications are used to ensure a minimal level of guaranteed security:

- They are often limited to components of a system, not the entire system. So if a component is secure, the weak link could be outside the component, rendering the component the least important part of the system from a security perspective
- Security certifications are general guidelines and are most often not good enough to ensure a system is secure. Detailed attacks (i.e., a framework for determining the security level) need to be analyzed separately with regard to the component and the whole system.
- Certifications typically include a specific piece of hardware with a specific version of firmware/software/applet running. If the hardware has an operating system, the Hardware + OS can be certified, but the certification will typically also have to include the application software
- If a component is not certified, it doesn't mean it doesn't have a high level of security, it just hasn't gone through the certification process. This process can take 6 – 18 months.
- The end customer ultimately decides if a component or system requires certification in their purchasing decision. In most cases, the customer is not familiar with the details of certifications, security design, and attack scenarios, thus it is difficult for them to assess the quality of security of a product (vs. the OEM who has much more knowledge). A certification only provides some level of comfort that a component of the system has a certain level of security. The customer may make their purchasing decision to include a certified part because of regulatory requirements or because they feel it limits their liability to do so.

Common certifications include:

FIPS 140-2 Certification

US government certification of cryptographic modules: It does not generally apply to the solution (e.g. application software, system design). Generally used for government applications, but commercial users may require FIPS certifications.

Increasing levels of security:

- **Level 1 - Basic**
 - Production grade component
 - Follows best practices (no egregious security violations)
- **Level 2 – Tamper Evidence**
 - Provides clear evidence of tampering (e.g. damaged packaging or seal)

- Role based authentication to get access to security assets
- **Level 3 – Tamper Resistant**
 - Will resist physical attacks
 - User based authentication to get access to security assets (sensitive data)
 - Separation (physical or logical) of the communications in and out of the module between security assets and other information (e.g. control information)
- **Level 4 – Tamper Resistant in any environment condition**
 - Same as level 3, but will also provide Tamper Resistance in very hostile environments (e.g. high and low temperature)

Note that Level 3 and 4 do not specify the type of physical attacks for which the device must be tamper resistant. For example a part may be able to resist the attack where a hacker drills open the part using various probes, but not be able to resist an attack where the hacker has \$500K worth of equipment such as a scanning electron microscope, special X-ray equipment, etc. Some parts will resist any attack (e.g. Smart Cards). One party might not care about the \$500K hacker scenario, but the other party may possess military secrets and may care.

Furthermore there are certain attacks which are not physical attacks via drilling open the part, but include tasks such as measuring the electromagnetic field around the part, or delays in response times to cryptographic operations which could yield information about secrets. There are enough determined hackers available who spend a great deal of time developing attacks against common parts which are manufactured in high volumes, to make such seemingly bizarre attack scenarios feasible.

Common Criteria (CC) Certification

Common Criteria differs from FIPS in several ways:

- International standard
- More broad than FIPS as it may apply to an entire system vs. a cryptographic module. (However, CC is commonly used for cryptographic modules and other components due to the difficulty in evaluating security around an entire system).
- Defines a framework (common language and process) for evaluating security. It does NOT establish any security features or levels
- The “EAL level” (see below) establishes increasing levels of rigor around the process of evaluating security. A high EAL level does not guarantee a high level of security, nor does a low EAL level indicate a low level of security. The security level depends on what security level is defined.
- ISO9000

Common Criteria framework summary:

Documents are generated by the vendor or community who wishes to receive a certification. The security levels are defined in these documents.

- **Target of Evaluation (TOE)**
 - Indicates what is being evaluated. For example, a security module or the entire system.
- **Security requirements/implementation** (each document builds on the previous)
 - **Protection Profile (PP)**
 - A document that contains the security requirements that will be evaluated. The required security level can be defined here.
 - **Security Target (ST)**
 - A document that indicates the particular security features/properties that will be used to implement the security requirements in the PP.
 - **Security Functional Requirements (SFRs)**
 - A document which indicates which security functions will be provided to implement the features/properties in the ST.
 - Indicates how these functions will be implemented
 - The document may indicate a well known protocol or algorithm
- **Evaluation Assurance Level (EAL)**
 - Provides an indicate of how rigorous the evaluation of the TOE has been against the Security Requirements/Implementation (PP, ST, SFRs)
 - Does not imply a level of security, the level of security is defined in the Security Requirements/Implementation documents.
 - EAL levels (as certified by a 3rd party):
 - **Level 1 – Functionally Tested**
 - Tests for correct operation, but not security
 - **Level 2 – Structurally Tested**
 - The vendor or developer provides information to the evaluator as to the design and test results of the TOE.
 - Contains information limited to that that which would be provided to an average commercial customer (e.g. not rigorous, not necessarily complete, not secret)
 - **Level 3 - Methodically Tested and Checked**
 - The TOE is rigorously evaluated
 - However, the results are not used to re-engineer the system, they are used to make modifications to the existing system to ensure a “moderate” level of security.
 - **Level 4 - Methodically Designed, Tested and Reviewed**
 - Similar to Level 3, except modifications are made to ensure a “moderate” to “high” level of security.
 - Does not include re-engineering the system, but may include modifications to the system using rigorous security technology components

- **Level 5 - Semiformally Designed and Tested**
 - The TOE is rigorously evaluated very early in the design cycle with the intention of engineering the system for security
 - It is intended that the addition of security would not significantly increase costs vs. a normal rigorous general design.
- **Level 6 - Semiformally Verified Design and Tested**
 - Similar to Level 5, but the addition of security is expected to include a significant increase in cost for a premium product
- **Level 7 - Formally Verified Design and Tested**
 - Similar to Level 5, but the additional of security is expected to include a very significant increase in cost for very high risk environments

EAL levels could be summarized as:

- **Level 1 and 2** – Low security
- **Level 3 and 4** – Moderate/high security where security is not designed in (it is added)
- **Levels 5, 6, 7** – High security is designed in. Increasing levels of security/cost

More Resources

<http://america.renesas.com/boardid>