Crypto Engineering

Elisabeth Oswald

Part 1 — The role of testing, validation, verification, evaluation and certification

Outline

Making sense of terminology

Types of Security Certification Schemes
- Common Criteria
- FIPS 140-3

Over to you

WORTSALAT

No matter what we develop (e.g. a specification, an API, software, hardware), there comes the time when we need to ensure that the "thing does what it is supposed to".

There are a number of terms that people use for a range of ways of what "it is supposed to" means. Many people use them interchangeably, my take on them is as follows

Testing:	Given a set of properties (aka test cases), does the thing meet the properties? (Are we building the thing correctly?)
Validation:	Given the requirements, does the "thing" meet the requirements? (Are we building the right "thing"?)
Verification:	Given a set of formal definitions, does the "thing" satisfy these definitions? (Are we building the "thing" as per our specification?)

Evaluation and Certification

Many products require some form of certification to prove that they meet some (minimum) standards before they can be sold.

Many products use certification to boost their market value.

Evaluation precedes certification: only if a product passes an evaluation regime it can be certified. During evaluation, a product is tested based on the evaluation regime, and this may require e.g. some form of (formal) verification.

Security sensitive products (e.g. the chip on a credit or debit card, point of sales terminals, etc.) can only enter the marked after certification.

CERTIFICATION

The idea is that, based on some (independent) evaluation, a trustworthy "body" issues a certificate (i.e. a written notice that confirms that the product satisfies some well specified requirements).

This idea long precedes the security industry, and is applicable to all sorts of products, services and even organisations.

Security certification and evaluation schemes depend on the respective market, e.g.

- pay TV: DVB standard (no explicit evaluation regime)
- credit/debit cards: EMV standard (evaluation largely via CC)
- passports/ID documents: ICAO standard (evaluation largely via CC)

Evaluation schemes for software/hardware are the Common Criteria (CC) in Europe, and FIPS 140-3 in US/Canada/Japan.

Certification vs Evaluation

Certification is the process of producing a recognised “stamp of approval”; typically a vendor contacts a certification body (a government agency, or some industry body), and an independent evaluator.

Evaluation is part of certification: an (independent) lab/company carries out a set of tests as mandated in the certification scheme that are aligned to some standard

Some markets/schemes follow public standards such as Common Criteria methodology or FIPS 140-3, others are completely not transparent.

Certification Setup

Typically an evaluation has three parties interacting with each other:

Vendor/Sponsor: the party that wishes to obtain a security certification for a product

Certifier: an institution that may issue security certificates

Evaluator: an evaluation lab of the vendor's choice

Certification bodies typically oversee the process and they will interact with the evaluator to ensure that they get a sufficiently detailed evaluation report. They can demand extra tests if they see fit.

Evaluators often have to be certified for a scheme: i.e. they have to undergo a few test before they are accepted by Certifiers.

Certification Schemes vs. Standards

CC (and FIPS 140, which we will cover as well) have been “translated” into international standards.

CC $\equiv$ ISO 15408 (plus additional documents/standards)

FIPS 140 $\equiv$ ISO/IEC 19790:2012; ISO/IEC 24759:2014; with physical attacks covered in ISO 17825 (non-invasive attack methods) and ISO 20085-1 and ISO 20085-2 (setups). FIPS 140-2 is still a “self contained” document, but FIPS 140-3 refers to the named ISO standards plus has a separate set of “special publications" (SP 800-140) that can overwrite parts of the ISO documents.

No worries, we won’t be reading these documents; not just because this would be a course on its own but also because whilst these documents are public, they need to be paid for.

Overview

Making sense of terminology

Types of Security Certification Schemes
- Common Criteria
- FIPS 140-3

Over to you

COMMON CRITERIA: SMART CARDS

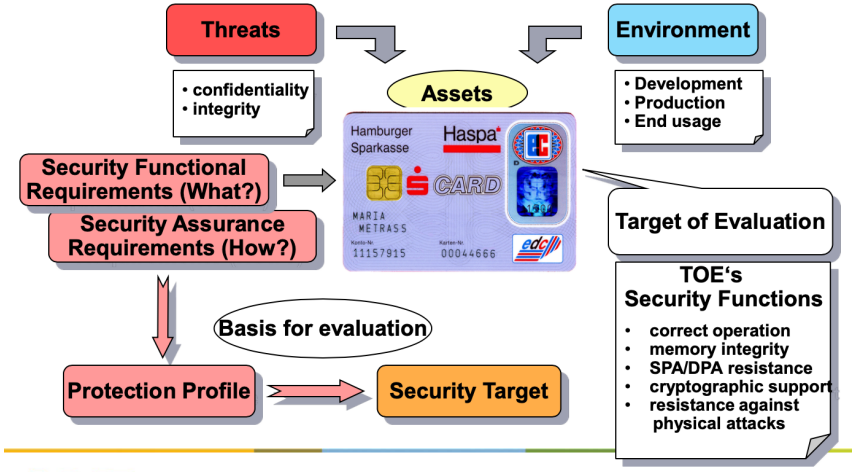

Figure: Taken from M. Medwed's Talks at a 2014 Summer School (NXP)

Evaluation Assurance Levels (EALs)

There are a number of different levels: they relate to the effort going into the evaluation, not the security of the product!

- EAL 1: Functionally tested
- EAL 2: Structurally tested
- EAL 3: Methodically tested and checked
- EAL 4: Methodically designed, tested, and reviewed
- EAL 5: Semiformally designed, and tested
- EAL 6: Semiformally verified, designed, and tested
- EAL 7: Formally verified, designed, and tested

It is possible to pick one level and "augment" (this is then indicated with a "+") it with specific requirements from a higher level.

PAPERWORK

CC evaluations are complex and governed by several documents. The product which is being certified is called the Target of Evaluation (TOE). For a TOE two documents are of relevance: the Protection Profile (PP) and the Security Target (ST).

The Protection Profile is a generic document for a category of product (e.g. Travel documents, Java Cards, IC, ...), often created by a user community. It provides an implementation independent specification of security requirements for a "class of devices": it lists threats, security objectives, assumptions, security functional requirements (SFRs), security assurance requirements (SARs) and rationales.

The Security Target details the secure implementation of the TOE and may use (or not) a PP as reference. It uniquely identifies the product and describes the assets, the threats, the security objectives (both on the TOE and on the environment), the perimeter of the evaluation, the SFRs and the life cycle. Vendors often make the Security Target details available to their customers.

PAPERWORK

Protection profile example (as accepted/certified by the German BSI)
`https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0084.html`

Other examples: `https://www.commoncriteriaportal.org/pps/`

Example for a Security Target: `https://www.commoncriteriaportal.org/files/epfiles/anssi_cible2017_44en.pdf`

CC Evaluation

During the Common Criteria evaluation process, vendors must state an envisioned security level, the (EAL). The EAL indicates a minimal level for each subclass (development process, guidance, conformity of security target, vulnerability assessment, ...) that will be taken into account during the evaluation.

Among all subclasses, the more relevant for practical security is AVA_VAN (vulnerability assessment), with levels going from 1 (resistance to basic attackers) to 5 (resistance to attackers with high attack potential). It describes the search for vulnerabilities and define a rating scale for attacks, depending on the means of the adversary.

So who decides on the “attack potential” of an adversary?

Focusing on smart cards: ISCI

The International Security Certification Initiative (ISCI) brings together stakeholders from every aspect of smart card security evaluations: certification bodies, evaluation laboratories, hardware vendors, software vendors, card vendors and service providers.

ISCI has two working groups: ISCI-WG1, which aims to define methodology and best practice for smart security device evaluation, and ISCI-WG2 (also known as JHAS), which defines and maintains the state of the art in potential attacks against smart security devices.

Two documents are essential for the evaluation of smart cards. The “Application of Attack Potential to Smart Cards” provides a “rating system” for attacks.

The “Attack Methods for Smart Cards and Similar Devices” is a confidential document and describes attack vectors that are considered “relevant”.

The same rating scheme is also used by EMVCo (a “derivative” of the CC approach).

Common Criteria: AVA_VAN subclass

- AVA_VAN.1 Vulnerability survey (TOE Resistance against Basic Attack Potential)
- AVA_VAN.2 (Unstructured) Vulnerability analysis (TOE Resistance against Basic AP)
- AVA_VAN.3 Focused vulnerability analysis (TOE Resistance against Enhanced-Basic AP)
- AVA_VAN.4 Methodical vulnerability analysis (TOE Resistance against Moderate AP)
- AVA_VAN.5 Advanced methodical vulnerability analysis (TOE Resistance against High AP)

Overview

Making sense of terminology

Types of Security Certification Schemes
- Common Criteria
- FIPS 140-3

Over to you

FIPS 140

The Federal Information Processing Standard (140-2, and, from late 2020 on, FIPS 140-3) specifies the security requirements for cryptographic modules.

It has four increasing, qualitative levels intended to cover a wide range of potential applications and environments.

It provides minimal requirements, with only four different evaluation levels. On levels one and two, the evaluator does not have to consider physical attacks. Only at levels three and four power, timing and EM attacks come into play.

FIPS 140-3 covers side-channel attacks via a link to several ISO standards: a side-channel test regime is given in ISO/IEC 17825:2016, with setups and calibration defined in ISO/IEC 20085-1 and 20085-2 (NIST special publications SP800-140 A-F may modify these in the future).

Cryptographic Module Validation Programme (CMVP)

FIPS 140-3 is an integral part of the CMVP: `https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program`

"The goal of the CMVP is to promote the use of validated cryptographic modules and provide Federal agencies with a security metric to use in procuring equipment containing validated cryptographic modules. " (taken from above URL)

Currently there is a transition from FIPS 140-2 to FIPS 140-3: the latter takes side channels into consideration.

CMVP

Before any CMVP mandated testing happens, any crypto algorithms are checked within the CAVP (A=Algorithm).

FIPS 140 specifies security requirements for cryptographic devices that encrypt and decrypt data, generate cryptographic keys, perform hashing, execute key agreement using industry standard protocols, and generate or verify digital signatures.

“FIPS 140 validation is mandatory for vendors selling cryptography into the US and Canadian governments. US government agencies consider cryptography that is not FIPS-validated as clear text. ” (taken from `https://www.oracle.com/corporate/security-practices/assurance/development/external-security-evaluations/fips/`).

CMVP Process

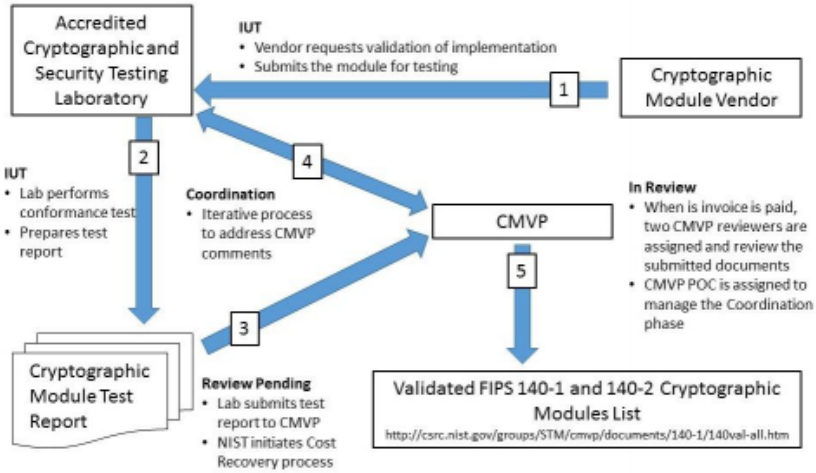

Figure: Taken from CMVP Website

CMVP AIMS FOR "CONFORMANCE TESTING"

The perhaps crucial difference to CC is that NIST/FIPS do not aim to ascertain the "true security level" of a product, but they mean to specify some minimum standards only that a product should satisfy (at level X, higher is better).

Level 1: No physical security mechanisms are required in the module beyond the requirement for production-grade equipment.

Level 2: Tamper evident physical security. Level 2 provides for role-based authentication. It allows software cryptography in multi-user timeshared systems.

Level 3: Tamper resistant physical security. Level 3 provides for identity-based authentication.

Level 4: Physical security provides an envelope of protection around the cryptographic module.

Conformance testing w.r.t. implementation attacks

FIPS 140-3 (via ISO 17825) puts forward some clear attack methods and leakage detection tests that a device needs to undergo.

Thus there is no attempt to capture the true security level, instead one tests w.r.t. some well defined attack scenarios.

The advantage of this is that it's quick and easy and therefore cheap.

The disadvantage is that the methods that are specified are very basic, and the leakage detection methodolgy is flawed (together with a colleague I authored a research paper that explains how and why and presented it at Asiacrypt 2019)

Because of this there is a revision now on the way for ISO 17825.

Complementary Reading and Watching

This course consists not just of material that I produced, but I also want you to benefit from a range of existing other materials from some fantastic researchers out there.

- I suggest you have a look at what a certification report from a CC evaluation looks like, e.g. look at this one: `https://www.commoncriteriaportal.org/files/epfiles/1040a_pdf.pdf`
- NXP have an online training about smart card certification for their customers `https://www.nxp.com/design/training/smart-card-security-countering-side-channel-and-fault-attacks-TIP-PART-4-SECURITY-EVALUATION-AND-CERTIFICATION`

The intended learning goals are that you get and overview of the two different philosophies for certification in the context of crypto/security and that you have some familiarity w.r.t. the terms and concepts used in specific contexts.