CC's place in the security market
Security market as seen from evaluation methodologies
Common Criteria

Development → Usage
Developed product focus

Development

Usage
Deployed product focus

Development → Usage
Process focus

Development

SDL

ISO 2700x
SAS 70

Usage
Evaluation methodologies (single focus)
Broader focus

Development ➔ Usage
Common Criteria

Development → Usage
Re-use of earlier work in the CC evaluation
Re-use of earlier work in the CC evaluation
Re-use of CC in further certification

Development

Usage

CMMI®
ISO 2700x
SAS 70

ScanAlert™
OWASP

HACKER SAFE
TESTED DAILY 01-JAN
Problem area

Common Criteria

Development

Usage

13
Problem area

Exactly this TOE performs the SFRs if the guidance is followed (offer valid to SARs only)
Problem area

Exactly this TOE performs the SFRs if the guidance is followed (offer valid to SARs only)

Usage

certified isn’t it?
“is secure” manuals??
attacker level
Evaluator

Slowly getting into the box
by Greencolander
@ flickr.com CC-BY
Evaluation methodology

Evaluator
Assurance limits
Assumptions
Human mistakes
Claims
Assurance limits
AVA_VAN.x

Assumptions
Objectives for the environment (guidance)

Claims
SFRs
TOE scope

Human mistakes
Assumptions

...everyone knows, when you make an assumption, you make an ass out of "u" and "umption".

Mitch Henessey – The Long Kiss Goodnight
Assumptions: OSes (Windows, Linux, ...)

A.CONNECT
All connections to peripheral devices reside within the controlled access facilities. The TOE only addresses security concerns related to the manipulation of the TOE through its authorized access points. Internal communication paths to access points such as terminals are assumed to be adequately protected.

A.PEER
Any other systems with which the TOE communicates are assumed to be under the same management control and operate under the same security policy constraints. The TOE is applicable to networked or distributed environments only if the entire network operates under the same constraints and resides within a single management domain.

A.COOP
Authorized users possess the necessary authorization to access at least some of the information managed by the TOE and are expected to act in a cooperating manner in a benign environment.

A.PROTECT
The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
Assumptions: OSes (Windows, Linux, ...)

A.CONNECT
All connections to peripheral devices reside within the controlled access facilities. The TOE only addresses security concerns related to the manipulation of the TOE through its authorized access points such as terminals are assumed to be adequately protected.

A.PEER
Any other systems with which the TOE communicates are assumed to be under the same management control and operate under the same security policy constraints. The TOE is applicable to networked or distributed environments only if the entire network operates under the same constraints.

A.COOP
Authorized users possess the necessary authorization to access at least some of the information managed by the TOE and are expected to act in a cooperating manner in a benign environment.

A.PROTECT
The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

Only allow access to keyboard, mouse and display

No connections to the outside world

Users are smart and do not press “yes” on any question, run malware, ...

No touching of the hardware
Assumptions: OSes (Windows, Linux, ...)

A.CONNECT
All connections to peripheral devices reside within the controlled access facilities. The TOE only addresses security concerns related to the management of the TOE through its authorized access points such as terminals are assumed to be adequately protected.

A.PEER
Any other systems with which the TOE communicates are assumed to be under the same management control and operate under the same security policy constraints. The TOE is applicable to networked or distributed environments only if the entire network operates under the same constraints and resides within a single management domain.

A.COOP
Authorized users possess the necessary authorization to access at least some of the information managed by the TOE and are expected to act in a cooperating manner in a benign environment.

A.PROTECT
The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

Source: Protection Profiles CAPP / LSPP
Cold war government threat model

Physical protection
Distance to attackers
Trusted personnel
Highly compartmentalized networks
Real world attacks: a big gap

- CVE-2010-0729: A certain Red Hat patch for the Linux kernel in Red Hat Enterprise Linux (RHEL) 4 on the ia64 platform allows local users to use ptrace on an arbitrary process, and consequently gain privileges, via vectors related to a missing ptrace_check_attach call.

- CVE-2010-0723: The gfs2 lock function in the Linux kernel before 2.6.34-rc1-next-20100312, and the gfs_lock function in the Linux kernel on Re, not properly remove POSIX locks on files if permission, which allows local users to cause a denial of service (CPU consumption and application hang) or information leakage (purple in Finch in RHEL before 2.6.6, which used, does not properly parse nicknames and remote attackers to cause a denial of service (SMP), does not properly restrict writing of key information to reduce denial of service attacks (SMP) and remote attackers to cause a denial of service (application crash) via a long string in the SRC attribute of a (1) IMG or (2) FRAME element.

- CVE-2010-0719: Stack-based buffer overflow in VBScript in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2, when Internet Explorer is used, might allow user-assisted remote attackers to execute arbitrary code via a long string in the fourth argument (aka helpfile argument) to the LoadLibrary function, leading to code execution when the F1 key is pressed, a different vulnerability than CVE-2010-0483.

- CVE-2010-0718: Buffer overflow in Microsoft Windows Media Player 9 and 11.0.3721.2445 allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a
Assumptions: OSes (Windows, Linux, ...)

A.CONNECT
All connections to peripheral devices reside within the controlled access facilities. The TOE only addresses security concerns related to the manipulation of the TOE through its authorized access points such as terminals are assumed to be adequately protected.

A.PEER
Any other systems with which the TOE communicates are assumed to be under the same management control and operate under the same security policy constraints. The TOE is applicable to networked or distributed environments only if the entire network operates under the same constraints and resides within a single management domain.

A.COOP
Authorized users possess the necessary authorization to access at least some of the information managed by the TOE and are expected to act in a cooperating manner in a benign environment.

A.PROTECT
The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

Source: Protection Profiles CAPP / LSPP

Users are smart and do NOT press “yes” on any question, run malware, ...

No touching of the hardware
Assumptions: smartcards

A.Process-Sec-IC Protection during Packaging, Finishing and Personalisation
It is assumed that security procedures are used after delivery of the TOE by the TOE Manufacturer up to delivery to the endconsumer to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use).

A.Plat-Appl Usage of Hardware Platform
The Security IC Embedded Software is designed so that the requirements from the following documents are met: (i) TOE guidance documents (refer to the Common Criteria assurance class AGD) such as the hardware data sheet, and the hardware application notes, and (ii) findings of the TOE evaluation reports relevant for the Security IC Embedded Software as documented in the certification report

A.Resp-Appl Treatment of User Data
All User Data are owned by Security IC Embedded Software. Therefore, it must be assumed that security relevant User Data (especially cryptographic keys) are treated by the Security IC Embedded Software as defined for its specific application context.
Assumptions: smartcards

A. Process-Sec-IC Protection during Packaging, Finishing and Personalisation

It is assumed that security procedures are used after delivery of the TOE by the TOE Manufacturer up to delivery to the endconsumer to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use).

A. Plat-Appl Usage of Hardware Platform

The Security IC Embedded Software is designed so that the requirements from the following documents are met: (i) TOE guidance documents such as the hardware application notes, and (ii) findings of the TOE evaluation reports relevant for the Security IC Embedded Software as documented in the certification report.

A. Resp-Appl Treatment of User Data

All User Data are owned by Security IC Embedded Software. Therefore, it must be assumed that security relevant User Data (especially cryptographic keys) are treated by the Security IC Embedded Software as defined for its specific application context.

Careful when personalizing

Follow the programmer guidelines

Software: Don’t output data you want to keep secret
Assumptions: smartcards

A.Process-Sec-IC Protection during Packaging, Finishing and Personalisation

It is assumed that security procedures are used after delivery of the TOE by the TOE Manufacturer up to delivery to the endconsumer to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use).

A.Plat-Appl Usage of Hardware Platform

The Security IC Embedded Software is designed so that the requirements from the following documents are met: (i) TOE guidance documents such as the hardware data sheet, and the hardware application notes, and (ii) findings of the TOE evaluation reports relevant for the Security IC Embedded Software as documented in the certification report.

A.Resp-Appl Treatment of User Data

All User Data are owned by Security IC Embedded Software. Therefore, it must be assumed that security relevant User Data (especially cryptographic keys) are treated by the Security IC Embedded Software as defined for its specific application context.

Careful when personalizing

Follow the programmer guidelines

Software: Don’t output data you want to keep secret
Assumptions

Keep the assumptions
realistic
minimal
extremely clear
... also in the manuals!
FIPS-140 meets USB-sticks: Claims ("SFRs" and "TOE scope")
Use a proper crypto algorithm
(~FCS_COP)

(Environment will do the rest)
FIPS-140 meets USB-sticks
FIPS-140 meets USB-sticks

Human inputs a good key (i.e. it is large, random and unique)
FIPS-140 meets USB-sticks

Human inputs a good key (i.e. it is large, random and unique)
FIPS-140 meets USB-sticks

Human inputs a good key (i.e. it is large, random and unique)
FIPS-140 meets USB-sticks

Instant hack

Figure 4: Proof-of-Concept software tool of the SySS GmbH
FIPS-140 meets USB-sticks: Claims and Assumptions

FIPS-140 level 2 requirements broken?
FIPS-140 meets USB-sticks: Claims and Assumptions

FIPS-140 level 2 requirements broken?

Stick still does AES with provided key (does not know key is not unique)
Claims: TOE Scope, SFRs, real world use

Keep the claims
  close to actual end-user use
  clear what is not included

Keep the scope realistic
  No scope tricks
Assurance limits

Assumptions

Human mistakes

Claims
Re-usable CC certifications

Clear on claims
  No trickery with TOE scope
  SFRs == used functionality

Realistic objectives for the environment
  As limited as possible
  Very clear they need to be done

Real vulnerability analysis
Security IC Platform Protection Profile

Version 1.0
15.06.2007

developed by

Atmel
Infineon Technologies AG
NXP Semiconductors
Renesas Technology Europe Ltd.
STMicroelectronics

Operating System Protection Profile

Common Criteria Protection Profile
BSI-CC-PP-0067
Version 2.0

????
Wouter Slegers

CREATIVE SOLUTIONS

YOUR

WOUTER@ YOURCREATIVESOLUTIONS.NL
+31-6-24721971
Attributions

“Slowly getting into the box” by Greencolander @ flickr.com CC-BY

“IMG_4284” by babbagecabbage @ flickr.com CC-BY

Images and trademarks of respective owners, used under fair use to illustrate the discussion