Common Criteria

Matthias Brüstle
<m@mbsks.franken.de>

Kommunikationsnetz Franken e.V.

Früher: Orange Book ⇔ ITSEC

- USA
  - Sicherheitsniveaus wie B2 oder C2
  - Bekannt: Windows NT-Zertifikat
- Europa
  - Sicherheitsniveau: Niedrig, Mittel, Hoch
  - Vertrauensniveau: E1 bis E6

Heute: Common Criteria

- Weltweit
  - Sicherheitsniveau: Niedrig, Mittel, Hoch
  - Vertrauensniveau: EAL1 bis EAL7 (Evaluation Assurance Level)

Juhu!

Naja, nicht so ganz Juhu

- Common Criteria nicht wirklich akzeptiert in USA
  - Bei Chipkarten: FIPS 140-2 Validation (!)
- Internationale Anerkennung von Zertifikaten nur bis EAL4 (bzw. EAL4+)
- CC-Standards sind wie die Bibel: anpaßbar und interpretierbar
  $\Rightarrow$ Nationale Unterschiede

Wie ist nun Common Criteria so?

- Kunde:
  - Kann in einem Schema Bedrohungen und Sicherheitsbedürfnisse darlegen (Protection Profile, PP)
  - Für Bedürfnisse (Security Functional Requirements, SFRs) flexibles und erweiterbares Bausteinsystem
  - Abdeckung der Bedrohungen und Ziele (Threads, Objectives) durch SFRs
  - PP wird geprüft

Wie ist nun Common Criteria so? (2)

- Hersteller:
  - Kann sich auf Protection Profile beziehen
  - Deckt Bedrohungen/Ziele mit Sicherheits-funktionen (Security Functions, SFs) ab
  - Verfeinerung der SFs
    - Abhängig vom EAL
    - Ab EAL4 bis zum Quellcode
  - Betrachtung des ganzen Lebenszykluses
  - Das ganze wird ebenfalls geprüft

Wen gibt es bei CC alles?

- Entwickler:
  - Produktentwickler: Produkt und Dokumente
  - Kunde: Protection Profile
- Evaluator: Prüft und schreibt Berichte
- Zertifizierer: Überwacht (Vergleichbarkeit) und stellt Zertifikat aus
- Eventuell Sponsor: Bezahlt die Zertifizierung

Protection Profile

- TOE Description
- TOE Security Environment
  - Was ist zu schützen? (Assets)
  - Assumptions: A.Pers_Agent „Personalisierer signiert die Daten“
  - Threads: T.Forgery „Pass wird gefälscht“
  - Organisational security policies: P.Manufact „gesicherter Herstellungsprozess“

Protection Profile (2)

- Security Objectives

  TOE: OT.Data_Int „Datenintegrität und Schutz gegen überschreiben“

  Environment: OE.Pass_Auth_Sign „CA zum Signieren“

- Security Requirements (SFRs)
  - TOE: FDP_ACF.1.4 „Terminals dürfen keine Daten verändern können“ (DP: Data Protection, ACF: Access Control Function)
  - Environment

Protection Profile (3)

- Security Assurance Requirements
  - EAL4 augmented by ADV_IMP.2, ALC_DVS.2
- Rationale
  - Abdeckung von Threads durch Objectives
  - Abdeckung von Objectives durch SFRs
  - Konsistenz, Sicherheitslevel

Security Functional Requirements Bausteine aus CC part 2

- Part 2: Katalog mit SFRs (>300 Seiten)
- SFRs auch selbst definierbar, z.B. FPT_EMSEC (ProTection/EManation)
- FDP_ACF.1.4:
  The TSF shall explicitly deny access of subjects to objects based on the [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].

Veröffentlichte PPs

BSI, DCSSI, etc. veröffentlichen PPs, z.B.:

- Software based Personal Firewall for home internet use
- Automatic Cash Dispenser / Teller
- Machine Readable Travel Document (BSI)
- Smartcard Integrated Circuit PP (DCSSI)
- Waste Bin Identification
- Secure Signature - Creation Device

Security Target / ST

- Sehr ähnlich wie PP strukturiert
- Kann sich auf ein oder mehrere PPs beziehen, muß aber nicht
- Wichtigster Unterschied zum PP
  - Einführung relativ abstrakter Sicherheitsfunktionen (Security Function, (T)SF)
  - Abdeckung der Security Functional Requirements (aus PP oder eigene) durch diese SFs

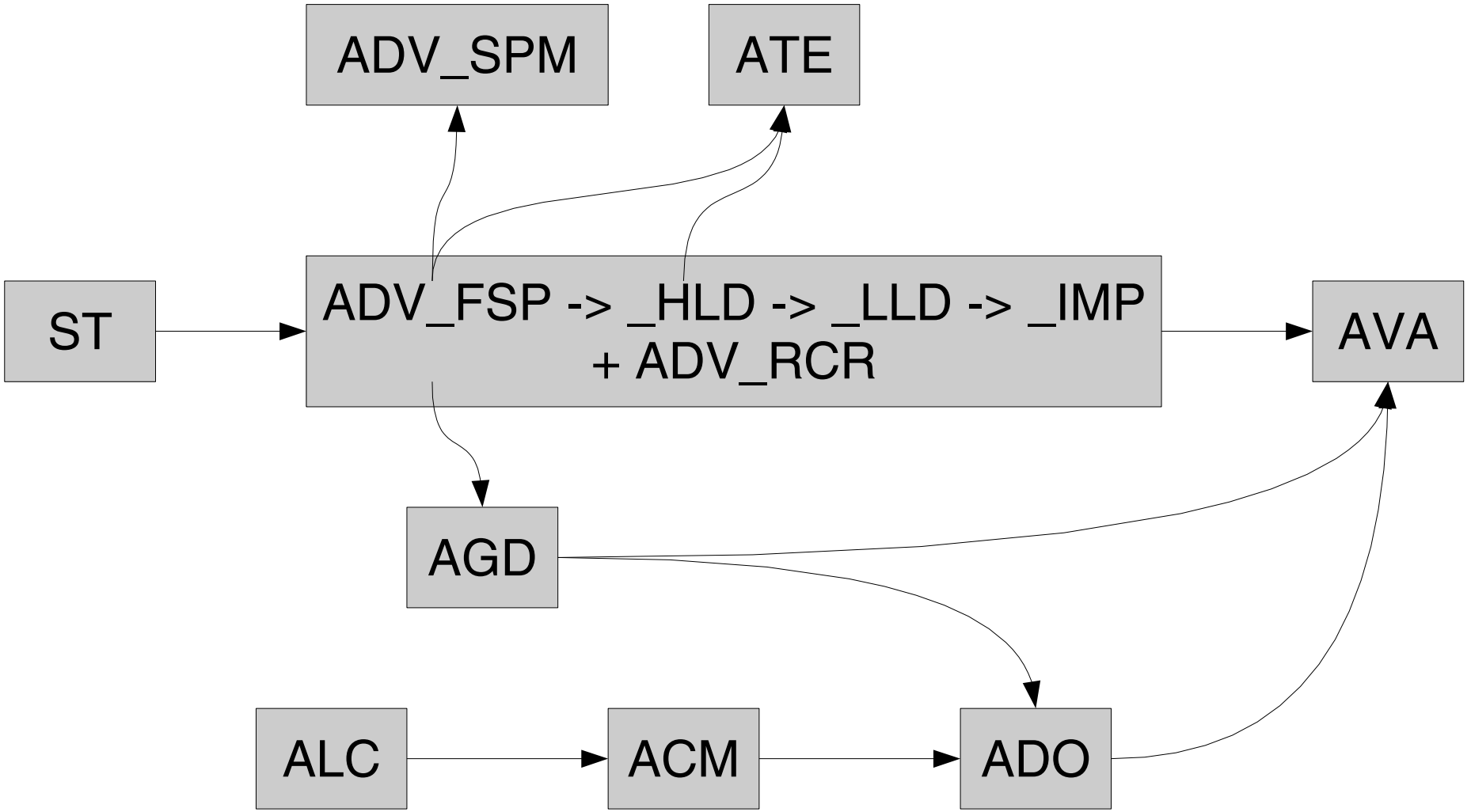
Sonstige Arbeit für den Entwickler

- Part 3: Assurance Requirements
- Assurance Classes
  - ACM: Configuration Management
  - ADO: Delivery and Operation
  - ADV: Development
  - AGD: Guidance Documents
  - ALC: Life Cycle Support
  - ATE: Tests
  - AVA: Vulnerability Assessment

Für EAL4(+)

- ACM_AUT.1
- ACM_CAP.4
- ACM_SCP.2
- ADO_DEL.2
- ADO_IGS.1
- ADV_FSP.2
- ADV_HLD.2
- ADV_IMP.1 -> .2
- ADV_LLD.1
- ADV_RCR.1
- ADV_SPM.1
- AGD_ADM.1
- AGD_USR.1
- ALC_DVS.1 -> .2
- ALC_LCD.1
- ALC_TAT.1
- ATE_COV.2
- ATE_DPT.1
- ATE_FUN.1
- ATE_IND.2
- AVA_MSU.2
- AVA_SOF.1
- AVA_VLA.2 (-> .4)

Abhängigkeiten



Composite Evaluation

- Chipkarte besteht aus Hardware und Software
- 2-stufige Evaluierung:
  1. Zertifizierung der Hardware, z.B. AT90SC12872RCFT Rev. L fnord, nach einem Hardware-PP
  2. Zertifizierung der Software auf der zertifizierten Hardware

Aufwand für EAL4+

- Zeit: (vielleicht) 3 Monate bis (ohne Probleme) 1-2 Jahre
- Kosten: Mittlerer sechsstelliger Euro-Betrag
- Papier:
  - Hersteller: ein ziemlich dickes Buch
  - Evaluator: ein ziemlich dickes Buch
  - Zertifizierer: vermutlich ein dünnes Buch

Vorteile

- Man hat die Chance sich zur Sicherheit Gedanken zu machen (PP/ST/FSP)
- Für Kunden: Von unabhängiger Stelle wurde geprüft:
  - Produkt
  - Handbücher
  - Entwicklungsumgebung
  - Test des Produkts

Nachteile

- Sehr großer Aufwand, der nur für weniger Produkte finanzierbar ist
- Preis/Leistungs-Verhältnis könnte man sicherlich verbessern
- Produkt natürlich immer noch nicht fehlerfrei

Zusammenfassung

- Entwickler:
  - Müssen sich auf sehr viel Arbeit einstellen.
  - Durch die Abhängigkeiten der Dokumente und die vielen Beteiligten gibt es viele Gelegenheiten für Verzögerungen
- Kunden
  - Unbedingt ST des Produktes ansehen, da Hersteller sich nicht auf ein PP beziehen muß und eine Popel-Zertifizierung machen kann
  - Garantiert einen gewissen Qualitätsstandard

Dokumente

- Common Criteria for Information Technology Security Evaluation, Version 2.3 bzw. Version 3.1 Revision 1
  - Part 1: Introduction and general model
  - Part 2: Security functional requirements
  - Part 3: Security assurance requirements
- Common Methodology for Information Technology Security Evaluation, Version 2.3 bzw. Version 3.1 Revision 1

Web

- www.commoncriteriaportal.org
- www.bsi.de/zertifiz/index.htm
- www.dcssi.fr
- csrc.nist.gov/cryptval/140-2.htm
-

Wühlen in der Praxis

Zum Abschluß der Blick in richtige Dokumente:

- MRTD-PP
- Beispiel-Dokumente vom BSI

Mahlzeit

Matthias Brüstle
<m@mbsks.franken.de>

Kommunikationsnetz Franken e.V.