Evaluationskriterien
und
Zertifizierungsstrukturen

Seminar IT Security
WS 2003/2004

Normen Rohde
163432

Abstract

Hinter der Frage welche Kriterien bei der Prüfung eines IT-Systems auf seine Sicherheit anzulegen sind, verbirgt sich mehr als ein Katalog von Sicherheitsfunktionen. Neben den unterschiedlichen Einsatzgebieten und damit auch unterschiedlichen Bedrohungspotentialen sollten die Hersteller auch die Möglichkeit haben bestimmten Bedrohungspotentialen unterschiedlich zu begegnen. Mit den Common Criteria wurde 1998 ein internationaler Standart veröffentlicht der Herstellern, Verbrauchern, und externen Gutachtern dabei hilft, die Vertrauenswürdigkeit eines IT-Systems im Hinblick auf seine Sicherheit zu evaluieren.
In einer Evaluierung wird geprüft ob alle notwendigen Sicherheitsfunktionen vorhanden sind und ob deren Funktionalität auch „vertrauenswürdig" ist.
In der vorliegenden Arbeit wird im 1.Teil erläutert wie man die notwendigen Sicherheitsfunktionen bestimmt und wie „Vertrauenswürdigkeit" in diesem Kontext zu verstehen ist.
Im 2.Teil wird auf die Zertifizierung eines IT-Systems eingegangen. Es werden zunächst die Hintergründe vorgestellt, die eine solche Zertifizierung sinnvoll erscheinen lassen, danach die Beteiligten, der Ablauf und die benötigten Dokumente.

1. Evaluationskriterien

Einleitung

Unter Evaluationskriterien werden die Anforderungen verstanden an ein IT-System (oder eines Teiles davon) verstanden, die dieses bei einer Zertifizierung[1] zu erfüllen hat.
Die Kriterien die für eine solche Prüfung herangezogen werden lassen sich in 2 Klassen unterteilen:

1. Anforderungen an die Funktionalität
2. Anforderungen an die Vertrauenswürdigkeit der Funktionalität

Im Kapitel 1.1 wird darauf eingegangen wie die Common Criteria bei der Identifizierung der Bedrohungspotentiale helfen und wie der Katalog der Sicherheitsanforderungen zu benutzen ist.
Im Kapitel 1.2 wird auf die verschiedenen Klassen eingegangen die die Vertrauenswürdigkeit eines Produktes beeinflussen. Es werden danach die von den CC vordefinierten Pakete vorgestellt, die einen schnellen und einfachen Vergleich der Vertrauenswürdigkeit verschiedener Softwareprodukte ermöglichen.

1.1. Funktionelle Anforderungen

Eine Evaluierung der Sicherheit eines IT-Systems kann nur auf Grundlage der identifizierten Bedrohungspotentiale erfolgen. Deshalb werden auch die Dokumente geprüft, in denen der Weg zu den konkreten Sicherheitsanforderungen dokumentiert ist. Die CC bieten mit den Security Targets (1.1.1 Sicherheitsvorgaben) einen standartisierten Aufbau für eine solche Dokumentation. Um diesen Sicherheitsanforderungen zu entsprechen bieten die CC im Teil 2 einen umfangreichen Katalog von Sicherheitskomponenten die im Abschnitt 1.1.2 und 1.2.3 erläutert werden. Im Abschnitt 1.1.4 wird auf Abhängigkeiten zwischen diesen Komponenten eingegangen.

[1] siehe Teil 2

1.1.1. Sicherheitsvorgaben

Die Sicherheitsvorgaben enthalten die Sicherheitsanforderungen für einen konkreten EVG. Nach einer Einführung in das Dokument folgt die Beschreibung des EVG und der Sicherheitsumgebung. Die Beschreibung der Umgebung geht auf getroffene Annahmen, identifizierte Bedrohungen und Sicherheitsrichtlinien innerhalb der Organisation ein.
Anschließend werden die Sicherheitsziele für den EVG und seine Umgebung formuliert. Im nächsten Punkt werden diese zu konkreten Anforderungen an die Funktionsweise von Sicherheitsfunktionen und deren Vertrauenswürdigkeit weiter präzisiert.
Danach können Verweise auf bestehende Schutzprofile folgen die dieser EVG ebenfalls erfüllen soll. Abschließend werden nochmals die Hintergründe für die Auswahl der Sicherheitsziele, der Anforderungen und die gewählte Spezifikation zusammenfassend dargelegt.

1.1.2 Benutzung des Teil 2 der CC

Im Teil 2 der CC befindet sich eine vollständige Auflistung aller für ein sicheres IT System relevanten Komponenten. Diese werden in Funktionsfamilien und Klassen aufgeteilt.
Eine Klasse stellt einen konkreten Sicherheitsaspekt des zu untersuchenden Produktes dar. Alle Familien einer Klasse widmen sich diesem Sicherheitsbereich, allerdings mit unterschiedlicher Zielsetzung. Die Komponenten einer Familie haben wiederum alle die gleiche Zielsetzung, wirken aber in unterschiedlicher Stärke.
Um die Informationen in den CC effektiv nutzen zu können, ist es wichtig den Aufbau der Erklärungen zu verstehen :

1. Familienname
   Er besteht aus einem 7-stelligen mnemonischen Code, der in den ersten 3 Buchstaben den Klassennamen enthält, gefolgt von einem Unterstrich. Die letzen 3 Buchstaben charakterisieren den Namen der Funktionsfamilie.

2. Familienverhalten
   Hier werden die Sicherheitsziele aufgeführt die mit dieser Funktionsfamilie abgedeckt werden sollen. Hier werden auch alle in den Komponenten der Familie enthaltenen Sicherheitsanforderungen kurz zusammengefasst.

3. Komponentenabstufung
   Hier wird graphisch dargestellt, wie die Komponenten in der Familie voneinander abhängen. Horizontal am weitesten rechts dargestellte Kästchen enthalten die stärksten Sicherheitsanforderungen und beinhalten die Anforderungen der linkstehenden Komponenten. Die vertikale Ordnung listet die Komponenten hinsichtlich ihrer verschiedenen Aufgaben auf, um die Sicherheitsziele der Familie zu erfüllen.

4. optionale Managementhinweise
   Hier werden Hinweise für die Festlegung der Sicherheitsvorgaben geliefert

5. Protokollierung
   Hier werden Situationen beschrieben in denen der Benutzer eine Protokollausgabe erwarten kann. Das natürlich nur, sofern die Protokollierung sicherheitsrelevanter Ereignisse ein Bestandteil der Sicherheitsanforderungen ist, was allerdings bei den meisten der bisher in Deutschland evaluierten Produkte der Fall ist[2].

[2] mit Ausnahme der Smartcards Vgl [1] S.15

6. detaillierte Informationen zu den einzelnen Komponenten:

- Komponentenname
- Auflistung der Hierarchien, die aber bereits aus der Komponentenabstufung bei der Beschreibung des Familienverhaltens bekannt sind.
- enthaltene Elemente: Elemente bilden die elementarste Sicherheitsanforderung, wo eine weitere Aufteilung keinen Sinn machen würde. Für die Erstellung von Sicherheitsvorgaben müssen immer alle Elemente einer Komponente in ein Sicherheitspaket aufgenommen werden.
- Abhängigkeiten
  Die sichere Funktionalität einiger Komponenten hängt von der Benutzung anderer Komponenten ab. Dies können entweder funktionale Komponenten sein oder auch bestimmte Anforderungen an die Vertrauenswürdigkeit.

1.1.3 Funktionale Sicherheitsanforderungen

Wie bereits beschrieben, enthalten die CC eine Auflistung aller für ein sicheres IT System nutzbaren Komponenten. Die Gliederung erfolgt durch Klassen die aus Funktionsfamilien bestehen. Nachfolgend werden die 11 Klassen der CC vorgestellt.

Alle 5 Familien der Klasse FAU (Security audit) widmen sich den Anforderungen an das Erkennen, Aufzeichnen, Speichern und Analysieren von Informationen zu sicherheitsrelevanten Aktivitäten.

Die Klasse FCO (Communication) enthält 2 Familien die Anforderungen festlegen, dass sowohl die Urheberschaft als auch der Empfang einer Nachricht nicht bestritten werden kann.

Die 2 Familien der Klasse FCS (Cryptographic support) decken Sicherheitsfunktionen auch von Familien anderer Klassen ab (z.B. Authentizität, Nichtabstreitbarkeit...)

Die 13 Familien der Klasse FDP (User Data Protection) widmen sich dem Schutz der Benutzerdaten aus unterschiedlicher Perspektive. Zwei Familien widmen sich grundsätzlichen Richtlinien zum Schutz der Daten, 6 Familien stellen verschiedene Formen des konkreten Datenschutzes dar, 3 Familien der Datenspeicherung und dem Austausch von Daten. Die letzten beiden Familien behandeln Aspekte der Kommunikation innerhalb der Sicherheitsfunktionen.

Die 6 Familien der Klasse FIA (Identification and authentication) bilden die Grundlage für die Wirksamkeit von anderen Sicherheitsfunktionen.

In der Klasse FMT (Security Managment) bieten die CC 6 Familien an, um das Verwalten der Sicherheitsfunktionen am EVG sicher zu gestalten.

In der Klasse FPR (Privacy) werden 6 Familien aufgezählt die Anforderungen zum Schutz des Benutzers beinhalten. Diese zielen insbesondere auf die Geheimhaltung der Identität eines Benutzers ab, damit diese nicht mißbräuchlich verwendet werden kann.

Die Klasse FPT (Protection TSF) enthält 16 Familien mit Anforderungen an den Schutz der Sicherheitsfunktionen des EVG.

In der Klasse FRU (Resource utilisation) legen 3 Familien Anforderungen an die Verfügbarkeit und die Aufteilung von Systemressourcen fest.

In der Klasse FTA (TOE access) werden Anforderungen zur Kontrolle einer Benutzersitzung festgelegt.

In der Klasse FTP (Trusted Path) werden in 2 Familien Anforderungen an einen vertrauenswürdigen Kommunikationsweg zwischen dem Benutzer und den Sicherheitsfunktionen des EVG aufgelistet.

1.1.4 Abhängigkeiten

Abhängigkeiten entstehen wenn die Sicherheit einer Komponente auf das Vorhandensein eine andere Komponente aufbaut. Diese Abhängigkeiten sind häufig zwischen funktionalen Komponenten vorhanden aber es bestehen auch Abhängigkeiten innerhalb der Komponenten zur Vertrauenswürdigkeit und sogar zwischen funktionalen und vertrauensfördernden Komponenten.
Ein Beispiel für eine offensichtliche Abhängigkeit zwischen funktionalen Komponenten ist die User Authentifizierung (FIA_UAU.1) die eine Identifikation der User (FIA_UID.1) voraussetzt.
Diese Abhängigkeiten sind teilweise nicht so offensichtlich, müssen aber bei der Einrichtung eines sicheren IT Systems unbedingt beachtet werden. Die CC unterstützen das Entdecken von Abhängigkeiten, indem diese ausführlich in den Komponentenbeschreibungen dokumentiert werden.

1.2 Vertrauenswürdigkeit

Der Begriff der „Vertrauenswürdigkeit“ soll ausdrücken wie sorgfältig ein Produkt entwickelt wurde und wie sehr sich ein Benutzer auf die angebotene Sicherheitsfunktionalität verlassen kann. Die CC unterscheiden 8 Bereiche (Klassen) die die Vertrauenswürdigkeit beeinflussen. Diese werden im Abschnitt 1.2.1 vorgestellt. Im Abschnitt 1.2.2 wird der häufig benutzte Begriff Evaluation Assurance Level erklärt.

1.2.1 Klassen

Im Teil 3 der CC werden verschiedene Komponenten, die Vertrauen in ein Softwareprodukt steigern aufgelistet und nach Klassen und Familien geordnet. Die 8 Klassen bilden die gröbste Strukturierung und stehen für den Bereich wo das Vertrauen in die Software gestärkt werden soll. Folgende 8 Klassen werden in den CC aufgelistet:
Mit Hilfe der Klasse ACM (Configruation Management) soll sichergestellt werden, das die Dokumentationen der Sicherheitsfunktionen mit dem tatsächlich geprüften EVG übereinstimmen.
In der Klasse ADO (Delivery and operation) sind Anforderungen definiert, die sich auf Transport, Installation, Anlauf und Betrieb des EVG beziehen. Insbesondere soll sichergestellt werden das keine Manipulationen an den Sicherheitsfunktionen während dieser Phasen vorgenommen werden können.
Durch die Klasse ADV (Development) werden Anforderungen an die Darstellung festgelegt, wie die funktionalen Anforderungen durch schrittweise Verfeinerung zu der dem Evaluator vorliegenden Implementation geführt haben.
In der Klasse AGD (Guidance support) werden Anforderungen an die Verständlichkeit und Vollständigkeit der Handbücher (für Systemverwalter und Benutzer) aufgelistet.

Die Anforderungen an die Verfolgbarkeit des EVG über seinen ganzen Lebenszyklus hinweg werden in der Klasse ALC (Life cycle support) festgelegt.
In der Klasse ATE (Tests) sind Anforderungen an das Testen definiert so dass nachgewiesen werden kann, dass der EVG seine Sicherheitsanforderungen erfüllt.
In der Klasse AVA (Vulnerability assesssment) sind Anforderungen an die Schwachstellen-bewertung dargelegt. Schwachstellen betreffen potentielle Sicherheitslücken die sich aus der Konstruktion, dem Betrieb, dem Missbrauch oder einer falschen Konfiguration des EVG ergeben könnten.
Durch die Klasse AMA (Maintenance of assurance) werden Anforderungen an die Aufrechterhaltung der Vertrauenswürdigkeit festgelegt.

Innerhalb der 8 Klassen befinden sich insgesamt 30 Familien. Diese Familie stehen für einen konkreten Ansatz die Vertrauenswürdigkeit in das Produkt zu steigern.
Der Evaluator prüft ob die für eine bestimmte Vertrauenswürdigkeitsstufe (die vom Hersteller festgelegt wurde) notwendigen Dokumente vollständig vorliegen und ob der EVG tatsächlich den dort beschriebenen Eigenschaften entspricht.

1.2.2 Vertrauenswürdigkeitsstufe (Evaluation Assurance Level)

Eine Vertrauenswürdigkeitsstufe ist ein Paket aus den unter 1.1.1 beschrieben Komponenten.
Die CC unterscheiden 8 Vertrauenswürdigkeitsstufen. Während auf der Stufe 0 die Vertrauenswürdigkeit als unzulänglich eingeschätzt wird, sichert die Stufe 8 die Vertrauenswürdigkeit durch formale Verifikation.
Die Evaluierung einer Sicherheitsfunktionalität erfolgt immer unter dem Gesichtspunkt einer Vertrauenswürdigkeitsstufe.
Grundlage für die Entscheidung über die gewünschte Vertrauenswürdigkeitsstufe ist der Verwendungszweck des Produktes. Folgende Fragen kann sich der Antragsteller bei der Auswahl stellen:
Wie sehr möchte ich die Vertrauenswürdigkeit der Funktionalität steigern ?
Wie wichtig ist die unabhängige Bestätigung der Qualität (Werbeffekt) ?
Existieren rechtliche oder organisatorische Mindestgrenzen ? (Chipkartenlesegeräte...)
Welche zusätzlichen Kosten dürfen maximal entstehen ?
(einmalige Zertifizierung: 50.000 – mehrere Millionen EUR)
Wieviel Zeit habe ich maximal ? Wegen der ggf. langen Evaluationszeit sollte möglichst schon zu Beginn der Produktentwicklung mit dem Prüfungsprozess begonnen werden. (Sonst ist das Produkt bei Erteilung des Zertifikates bereits vom Markt überholt)

2. Zertifizierung

2.1. Hintergründe

Die Zertifizierung von sicheren IT Systemen gewinnt zunehmend praktische Bedeutung:

1. Durch die steigende Nutzung von IT im Geschäftsverkehr wächst der Sicherheitsbedarf der Anwender. Durch die Zertifizierung erhält der Anwender eine neutrale Einschätzung der Vertrauenswürdigkeit in ein IT-System.

2. In einem wild gewachsenem Markt der Softwareentwicklung ist es für Hersteller wichtig, die Qualität hochwertiger Produkte für den Kunden fassbar zu machen. Ein zertifiziertes IT-System setzt eine strukturierte Softwareentwicklung voraus und macht diese für die Kunden des Herstellers sichtbar.

Die Common Criteria, nachfolgend als CC bezeichnet, wurden 1998 als internationaler Standard[3] zur Prüfung und Bewertung von IT-Sicherheit fertiggestellt. Die CC in der aktuellen Version 2.1 bilden die Grundlage für den hier beschriebenen Zertifizierungsprozess.

2.2. Beteiligte

Für eine Zertifizierung kommen Vertragsverhältnisse zwischen den folgenden 3 Parteien zustande:

1. Antragsteller (typischerweise der IT-Hersteller)
2. Evaluator (Prüflabor)
3. Zertifizierer (BSI oder eine der drei in Deutschland ansässigen privaten Zertifizierungsstellen)

2.3. Ablauf der Zertifizierung

Der Antragsteller schliest mit der Prüfstelle einen Evaluierungsvertrag, anschließend stellt er beim BSI (oder einer privaten Zertifizierungsstelle) einen Zertifizierungsantrag. Der Zertifizierer benennt Prüfbegleiter, die den Evaluierungsprozess begleiten um ein einheitliches Vorgehen und vergleichbare Bewertungen sicherzustellen. Der Antragsteller stellt sein Produkt und die notwendigen Dokumente dem Prüflabor zur Verfügung. Nach erfolgreicher Evaluierung wird ein Bericht an die Zertifizierungsstelle abgegeben, die dann ein Zertifikat erteilen kann. Nachfolgend wird auf diese Phasen näher eingegangen.

2.3.1 Vorbereiten der Evaluation

Die Vorbereitungsphase spielt eine zentrale Rolle im Zertifizierungsprozess. Nicht beachtete Aspekte in der Vorbereitungsphase ziehen eine Kette von Fehlern nach sich, die den Zertifizierungsprozess mit hohen Folgekosten belasten.
Ergebnisse der Vorbereitungsphase sind die Sicherheitsvorgaben und die Produktdokumentation die dem Evaluator zur Prüfung eingereicht werden.
Da an diese beiden Artefakten die Evaluationskriterien klar erkennbar sind, werden diese in Kapitel 2 und 3 gesondert behandelt.

[3] ISO/IEC 15408

2.3.2 Evaluation

Die für die Prüfung notwendigen Dokumente sind die Sicherheitsvorgaben und sämtliche zum EVG gehörenden Produktdokumentationen.
Optional, doch empfehlenswert ist die Vorlage eines Schutzprofils. Auf dieses Dokument wird unter Punkt 2.1 näher eingegangen.
Zu Beginn findet eine Prüfung der Sicherheitsvorgaben, ggf. auf Grundlage des evaluierten Schutzprofils statt. Danach folgt die Evaluierung des eigentlichen EVG. Bei Unklarheiten kann der Antragsteller eine Review-Sitzung beantragen. Ziel dieses Reviews ist eine Korrektur des EVG. Die Zertifizierungsstelle begleitet die Evaluation um durch ein einheitliches Vorgehen die Vergleichbarkeit mit anderen EVG sicherzustellen
Der Prüfungszeitraum kann sich je nach Gegenstand über Monate oder sogar Jahre hinziehen.
Die Evaluationsstelle erstellt einen Evaluationsbericht (**E**valuation **T**echnical **R**eport) in zweifacher Ausfertigung: für den Antragsteller und für die Zertifizierungsstelle.

2.3.3 Zertifizierung

Der von der Evaluationsstelle erstellte Bericht mit positivem Gutachten wird für die Zertifizierung benötigt. Soll der Zertifizierungsreport veröffentlicht werden, wird dafür die Zustimmung des Antragstellers benötigt.
Bei erfolgreicher Evaluation erstellt die Zertifizierungsstelle einen Zertifizierungsreport der zu der Erteilung des Zertifikats führt. Wenn die Zustimmung des Antragstellers vorliegt, wird dieser Report veröffentlicht und internationale Partnerbehörden werden über das erteilte Zertifkat benachrichtigt.

2.3.4 Nachbetreuung

Nach erfolgreicher Zertifizierung berät die Zertifizierungsstelle den Antragsteller über die Re-Zertifizierung neuer Versionen des Produktes. Die Re-Zertifizierung benutzt die bereits vorliegenden Evaluierungsdokumente und ist deshalb preiswerter und schneller.

2.4 Benötigte Dokumente

2.4.1 Sicherheitsvorgaben (Security Targets)

In dem bereits in Abschnitt 1.1.1 vorgestellten Dokument werden ausführlich identifizierte Bedrohungen, Sicherheitsziele, Sicherheitsanforderungen und Spezifikationen zu Funktionalität und Vertrauenswürdigkeit festgehalten. Die erforderliche Form ist im Anhang C des 1. Teils der CC aufgeführt. Inhaltlich bauen die Sicherheitsvorgaben auf ein ggf. vorhandenes Schutzprofil auf. Sollte dies noch nicht vorhanden sein, werden die Sicherheitsvorgaben in Zusammenarbeit mit dem BSI erarbeitet. Wichtiger Bestandteil der Sicherheitsvorgaben ist die Auswahl der Vertrauenswürdigkeitsstufe. Auf diese wird im Unterabschnitt 2.4.3 näher eingegangen. Sicherheitsvorgaben werden vom Evaluator auf Vollständigkeit geprüft und dienen anschließend als Grundlage zur Prüfung der Produktdokumentationen. In den Sicherheitsvorgaben kann auf ein Schutzprofil verwiesen werden das mit dem IT-Produkt abgedeckt werden soll.

2.4.2 Schutzprofil (Protection Profile)

Ein Schutzprofil ist nicht zwingend für die Evaluierung erforderlich. Falls in den Sicherheitsvorgaben ein Verweis auf ein Schutzprofil vorhanden ist muss dieses mitgeliefert werden.
Das Schutzprofil sollte idealerweise vom Anwender dem IT Hersteller zur Verfügung gestellt werden. In diesem Dokument wird eine implementierungsunabhängige Menge von IT

Sicherheitsanforderungen aufgestellt. Das BSI hat für einige typische Softwareprodukte Statistiken aufgestellt, welche Sicherheitsanforderungen in bisherigen Zertifizierungsverfahren für diese Produktkategorien gefordert wurden.
Die formale Gliederung des Schutzprofils sollte den Empfehlungen der CC im Teil 1 Anhang B folgen:

EVG Beschreibung	APE_DES
Sicherheitsumgebung	APE_ENV
PP-Einführung	APE_INT
Sicherheitsziele	APE_OBJ
EVG-Sicherheitsanforderungen	APE_REQ
Explizit: IT Sicherheitsanforderungen	APE_SRE

2.4.3 Produktdokumentation

Die für die Evaluierung notwendige Produktdokumentation enthält die vollständige Sammlung aller bei der Produktherstellung angefallenen für die Evaluierung relevanten Dokumente. Zentraler Bestandteil der Produktdokumentation ist die Darlegung, wie die in den Sicherheitsvorgaben geforderten Sicherheitsfunktionen realisiert wurden. Welche anderen Dokumente für die Produktdokumentation benötigt werden hängt davon ab, für welche Stufe an Vertrauenswürdigkeit das Produkt zertifiziert werden soll.
Für eine Zertifizierung mit der Vertrauenswürdigkeitsstufe 1 werden beispielsweise die Nachweise für die nachfolgend aufgelisteten Eigenschaften gefordert:
- eine Versionsverwaltung muss bei dem zu evaluierenden Produkt zur Anwendung gekommen sein (ACM_CAP.1)
- es muss eine vollständige Dokumentation vorliegen wie der Anwender eine sichere Installation für das Produkt durchführen kann. (ADO_IGS.1)
- alle Sicherheitsfunktionen müssen auf hohem Abstraktionsniveau spezifiziert worden sein. (Benutzerschnittstelle...) (ADV_FSP.1)
- der Entwickler muss informell darlegen, dass jede konkrete Darstellungsform einer Sicherheitsfunktion mit der abstrakteren Darstellung übereinstimmt. (ADV_RCR.1)
- Handbücher für den Administrator (AGD_ADM.1) und für den Anwender müssen vorhanden sein (AGD_USR.1)
- Funktionsorientierte Testverfahren müssen vom Entwickler angewandt worden sein. (ATE_IND.1)

Glossar
EAL Evaluation Assurance Level (Vertrauenswürdigkeitsstufe)
EVG Evaluationsgegenstand
TOE Target of Evaluation (=EVG)

Quellen:
[1.] IT Sicherheit auf Basis der Common Criteria www.bsi.bund.de
[2.] Zertifizierung mehrseitiger IT-Sicherheit Kai Ranneberg Viewg, 1998
[3.] Common Criteria Version 2.1 Bundesamt für Sicherheit in der Informationstechnik
[4.] Homepage des Common Criteria Projektes www.commoncriteria.org