Common Criteria

Juha-Pekka Leskinen

Helsingin yliopisto

Tietoturva nykyaikaisessa liiketoimintaympäristössä –seminaari

10.4.2003

Common Criteria

Juha-Pekka Leskinen

Tietoturva nykyaikaisessa liiketoimintaympäristössä -seminaari

HELSINGIN YLIOPISTO

Tietojenkäsittelytieteen laitos

10.4.2003, 25 sivua

Seminaarityössä selvitetään Common Criteria –tietoturvastandardin taustat, tarkoitus ja peruskäsitteet. Lisäksi selvitetään Common Criteriaa kokeilleen ryhmän kokemuksia. Seminaarityön ote on opetuksellinen, varsinaista tieteellistä tutkimusta ei ole työn aikana tehty. Tutkimus on tehty analysoimalla tieteellisiä kirjoituksia, konferenssijulkaisuja, Common Criteria –standardointidokumentteja ja muuta Common Criterian käyttöön liittyvää materiaalia. Työn tarkoituksena on selvittää lukijalle mikä Common Criteria on, mitkä ovat sen peruskäsitteet ja mitä sen käytöllä on tarkoitus saada aikaan. Lisäksi kuvataan joitakin Common Criterian käytössä esiintyneitä ongelmia.

Aiheluokat: (The ACM Computing Classification System 1998): K.6.5, K.4.4, D.4.6

Avainsanat: Common Criteria

Sisällys

1. Mikä Common Criteria on

Common Criteria on tietotekniikkatuotteiden tietoturvallisuustason määrittely- ja evaluointistandardi, jota ovat kehittäneet eri maiden kansalliset turvallisuus- ja standardointiorganisaatiot. Kaikilla suurilla CC:tä kehittäneillä mailla on ollut jokin kansallisesti tai käytössä ollut turvallisuusstandardi, jota on käytetty esim. evaluoitaessa tietoteknisten ratkaisujen turvallisuustasoa. Syynä Common Criterian kehittämiseen näistä kansallisista standardeista on ollut tarve kehittää yhteinen menettelytapa. Aktiivisesti CC:tä kehittämässä ovat olleet Kanada, Ranska, Saksa, Hollanti, Iso-Britannia ja Yhdysvallat [Gui99]. Jotta Common Criteriasta saataisiin laajalle levinnyt kansainvälinen standardi, ovat sitä kehittäneet maat toimineet niin, että Common Criteria v.2.1 on saatu hyväksyttyä ISO 15408 -standardiksi [Gui99].

Kansallisten standardien kehittyminen kohti Common Criteria –standardia [Int].

1980 TCSEC USA

1991 ITSEC Eurooppa

1993 TCSEC+ITSEC=CTCPEC Canada

1993 FC USA

1996 Common Criteria v. 1.0

1998 Common Criteria v. 2.0

1998 Common Criteria v. 2.1 = ISO 15408

Common Criteria sisältää joukon vaatimuksia, joita voi käyttää määritettäessä jonkin tietotekniikkatuotteen tietoturvavaatimuksia. Lisäksi se määrittelee evaluointimenettelyn, jonka avulla voidaan arvioida tietotekniikkatuotteiden tietoturvan tasoa. Common Criterian tarkoituksena on tarjota yhtenäinen menettelytapa, jonka avulla tietotekniikkatuotteiden tietoturvatasoa voidaan evaluoida. Näin tuotteen ostaja voi valita joukosta sellaisia tuotteita, jotka on arvioitu standardoidulla tavalla. Eräs-

nä tarpeena Common Criterian käytölle nähdään tilanne, jossa suurta tietoturvan tasoa vaativia tietojärjestelmiä rakennetaan niin, että tietojärjestelmä rakentuu sekä juuri kyseiseen tarpeeseen rakennetuista osista että ns. valmisohjelmistoista [Mar02]. Toisaalta ohjelmistoyrityksille tarjoutuu yhtenäinen tapa määrittää tuotteensa tietoturvallisuustaso. Näin ajatellaan sekä ostajan että ohjelmistoyrityksen hyötyvän.

Kannattaa huomata, että Common Criterian määrittelemä evaluointimenettely ei takaa ehdotonta tietoturvallisuutta. Käytännössä se tarkoittaa, että tuotteen tietoturvavaatimukset on määritelty, tuote on evaluoitu ja evaluoinnin tulokset on dokumentoitu ennalta sovitulla tavalla. Common Criteria määrittää myös joukon tietoturvallisuustasoja, joihin evaluoidut tuotteet voidaan sijoittaa. Näin kuluttaja voi valita, minkä tasoisen tuotteen hän haluaa hankkia ja toisaalta helpommin arvioida täyttääkö jokin tuote ne tietoturvatarpeet, jotka hänellä on [Gui99]. Common Criterian käyttö ei edellytä tarkasteltun kohteena olevalta tuotteelta mitään tiettyä toteutustekniikkaa [Mar02]. Tuote voi olla esim. rakennettu millä ohjelmointikielellä hyvänsä.

Common Criterian määritysdokumentit on jaettu kolmeen erilliseen osaan, joissa kuvataan Common Criterian yleismalli, tietoturvallisuuden toiminnalliset vaatimukset ja tuotteen vaatimuksen toteutuminen. Common Criterian peruskäsitteitä ovat: Protection Profile (PP), Security Target (ST) ja Target of Evaluation (TOE).

1.1. Protection Profile

Protection Profile määrittelee kuvaustavan ja menettelyn, jonka avulla organisaatio tai kuluttaja voi määrittää tietoturvavaatimuksia. Nämä vaatimukset ovat yleisiä vaatimuksia, joita ei ole välttämättä vielä liitetty mihinkään tiettyyn tuotteeseen. Protection Profile on myös riippumaton siitä, millä

teknologilla, ohjelmointikielellä yms. tuote on toteutettu. Tavoitteena on kuvata Protection Profile niin, että sen avulla voidaan asettaa jonkin tietyn tuoteryhmän tai palvelun yhteiset tietoturvavaatimukset. Näitä vaatimuksia voi sitten käyttää aina arvioitaessa tähän ryhmään kuuluvien tuotteiden tietoturvallisuuden tasoa. Protection Profiileja on kehitetty valmiiksi eri tuoteryhmiä kuten palomuureja, tietokantajärjestelmiä yms. varten.

Protection Profilen kuvauksen aloittaa johdanto-osuus, jossa kuvataan mitä PP:n on tarkoitus kuvata. Seuraavaksi kuvataan tietoturvatavoitteet (Security Objectives). Tietoturvatavoitteet ovat niitä asioita, joita organisaatio haluaa tavoitella yleisesti ottaen, yleensä johonkin tietoturvauhkaan liittyen.

Protection Profilessa kuvataan myös yleisesti millaiseen tuotteeseen tai tuoteryhmään vaatimuksia kohdennetaan. Käytännössä tämä tarkoittaa, että esim. kuvataan PP:n vaatimusten kohteena olevat palomuuriohjelmistot tms. kokonaisuus. Lisäksi kuvataan tietojenkäsittelytoiminnan taholta tulevat toiminnalliset vaatimukset koskien jotain evaluoitavaa tuotetta tai tuoteryhmää. Nämä vaatimukset ovat joko itse organisaatiossa kehitettyjä tai ne on voitu kerätä käyttämällä valmiiksi rakennettuja [Int] PP-paketteja.

Kuvaukseen kuuluu vielä kuvaus (TOE Security Environment) siitä, millaisessa ympäristössä evaluoinnin kohdetta aiotaan käyttää. Se kuvaa ympäristöön liittyvät tietoturvatavoitteet ja luettelee tärkeimmät toimintaympäristön henkilöstöön sekä tekniseen ympäristöön liittyvät oletukset. Myös oletetut ympäristöön liittyvät uhat, hyökkääjät ja hyökkäyskohteet kuvataan tässä osiossa. Myös sellaiset organisaation tietoturvapolitiikkaan liittyvät asiat, jotka evaluointeja tehtäessä on tiedettävä luetellaan tässä.

1.2. Security Target

Security Target (ST) määrittää kuvaustavan ja menettelyn, jonka avulla organisaatio voi määrittää johonkin tiettyyn tuotteeseen liittyviä tietoturvavaatimuksia. Sitä käytetään myös evaluoitaessa tuotteita ja kuvattaessa sitä, täyttääkö tietty tuote edeltäkäsin määriteltyjä tietoturvavaatimuksia. Yksi Security Target voi liittyä yhteen tai useampaan Protection Profileen.

Security Target sisältää Protection Profilen lailla ensin johdannon (introduction), jossa kuvataan yleisesti ST:hen liittyviä asioita. Johdannon lisäksi kuvataan tietoturvatavoitteet (Security Objectives), jossa luetellaan niitä tavoitteita, joita tuotteen tulee toteuttaa. Tavoitteet pyritään löytämään arvioimalla mahdollisia tietoturvauhkia [Int] ja miettimällä, miten niihin pystytään vastaamaan.

ST:ssä kuvataan myös evaluoinnin kohde (TOE Description). Tavoitteena on auttaa evaluoinnin suorittamisessa niin, että siinä on kuvattu evaluoinnin kohteelta vaadittavat tietoturvavaatimukset. Lisäksi tässä kohdassa kuvataan miten evaluoinnin kohteena olevaa tuotetta on tarkoitus käyttää ja sen yleisiä tietotekniikkaominaisuuksia.

Security Target –kuvaukseen kuuluu myös kuvaus tietotekniikkavaatimuksista (IT Security Requirements), kuvaus siitä, millaisessa ympäristössä evaluoinnin kohdetta aiotaan käyttää sekä mahdolliset kuvaukset Protection Profilen käyttöön liittyvistä asioista (PP Claims). Kuvauksessa tietotekniikkavaatimuksista kerrotaaan evaluoitavan tuotteen toiminnalliset- ja tietoturvavaatimukset.

Kuten PP:ssä, kuvaukseen kuuluu vielä kuvaus evaluointiympäristöstä (TOE Security Environment). Se kuvaa ympäristöön liittyvät tietoturvatavoitteet ja luettelee tärkeimmät toimintaympäristön henkilöstöön sekä tekniseen ympäristöön liittyvät oletukset. Myös oletetut ympäristöön liittyvät uhat, hyökkääjät ja hyökkäyskohteet sekä organisaation tietoturvapolitiikka kuvataan tässä osiossa.

Security Target –kuvauksessa on paljon sellaisia kohtia joita on jo lueteltu Protection Profile –kuvauksessa. Tarkoitus ei suinkaan ole toistaa samoja määrityksiä kahteen dokumenttiin. ST-kuvauksessa voi siis viitata PP-kuvauksen tietoihin silloin, kun ei ole olemassa väärinymmärryksen mahdollisuutta [Int].

1.3. Target of Evaluation

Target of Evaluation on tuote, tietojärjestelmä tai sen osa jonka tietoturvaominaisuuksia tai soveltuvuutta organisaatioon arvioidaan. TOE voi olla myös tällaisen järjestelmän osajärjestelmä. Common Criteria määrittää kolme ryhmää, joille standardi on kohdistettu: TOE käyttäjät, TOE kehittäjät ja TOE evaluoijat [CCI99a]. Standardi pyrkii siis helpottamaan näiden ryhmien toimintaa kehitettäessä ja valittaessa TOE –tuotteita.

1.4. Luokkajärjestelmä

Common Criteria -järjestelmä määrittelee joukon tietoturvavaatimuksia, joita voidaan käyttää hyväksi evaluoitaessa tuotteita ja rakennettaessa omia vaatimusmäärittelyjä. Vaatimukset on luokiteltu hierarkkisesti luokkiin (class), perheisiin (family) ja komponentteihin (component) [CCI99b]. Komponentteja voidaan vielä ryhmitellä paketeiksi (package) niin, että yhteen pakettiin kuuluu komponentteja eri perheistä.

Ennalta määriteltyjä komponenttiluokkia ovat:

- Audit
- Cryptographic Support
- Communications
- User Data Protection
- Identification and Authentication
- Security Management
- Privacy
- Protection of the TOE Security Functions
- Resource Utilisation
- TOE Access
- Trusted Path/Channels

Luokka on komponenttijärjestelmän korkein taso. Luokkia on jaettu perheisiin niin, että kukin perhe sisältää samo tietoturvallisuuteen liittyviä asioita, mutta eri näkökulmasta tarkasteltuna. Erilaisia perheitä saman luokan sisällä voivat olla esim. saman asian tarkastelu tiedot tuottamisen, analyysin tai tapahtumien tallettamisen näkökulmasta [Gui99].

1.5. Evaluation Assurance Levels

Common Criteria määrittelee erityiset tietoturvavaatimusten toteutumistasot (Evaluation Assurance Levels, EAL), joita voi käyttää määriteltäessä tietoturvavaatimusten toteutumista tietyn tuotteen tai tuoteryhmän osalta. Tasoja on seitsemän (EAL1-EAL7) vaatimusten muuttuessa tiukemmiksi siirryttäessä tasolta EAL1 tasolle EAL7.

EAL-tasoja ovat:

- EAL1 - funktionaalisesti testattu
- EAL2 - rakenteellisesti testattu
- EAL3 - menetelmällisesti testattu ja tarkistettu
- EAL4 - menetelmällisesti suunniteltu, testattu ja katselmoitu
- EAL5 - semiformaalisti suunniteltu ja testattu
- EAL6 - semiformaalisti verifioitu, suunniteltu ja testattu
- EAL7 - formaalisti verifioitu, suunniteltu ja testattu

EAL1 - funktionaalisesti testattu

EAL1 evaluaatio on tarkoitus pystyä toteuttamaan ilman ulkopuolista apua. Kuluttaja tai yritys pystyy toteuttamaan arvioinnin niin, ettei siihen tarvita esim. sovelluksen kehittäjien apua. Evaluointitaso on myös sellainen, ettei evaluoinnin suorittamiseen kulu kovin paljon aikaa eikä henkilöresursseja.

EAL2 - rakenteellisesti testattu

EAL2 -tason evaluointi vaatii yhteistyötä sovelluksen kehittäneen tahon kanssa. Evaluoinnin suorittamiseksi sovelluskehittäjältä tarvitaan informaatiota sovelluksen rakenteesta. Evaluointi ei kuitenkaan vaadi vielä merkittävästi keskustelua ohjelmansuunnittelijoiden ja evaluoinnin tekijöiden välillä, eikä sovelluksen rakenteen kovin yksityiskohtaista selvittelyä. EAL2 -tason tavoitteleminen ei vielä vaadi sen huomioonottamista ohjelmiston suunnitteluvaiheesa

EAL2 -tasoa käytetään silloin, kun tarvitaan vielä suhteellisen matalaa tai keskitasoista tietoturvan tasoa, tyypillisesti sellaisessa ympäristössä, jossa evaluoitavat ohjelmistokomponentit ovat jo olemassa. Tällainen tilanne saattaa olla esimerkiksi arvioitaessa olemassaolevia järjestelmiä tai milloin ei ole mahdollista pitää yhteyttä sovelluksen kehittäjien kanssa.

EAL3 - menetelmällisesti testattu ja tarkistettu

EAL3 -taso sallii ohjelmistokehittäjän soveltaa tietoturvasuunnitteluperiaatteita ohjelmistoa rakentaessaan niin, että hän ei kuitenkaan joudu vielä muuttamaan ohjelmiston normaalia sovelluskehitysmenettelyä. Niinpä sillä voidaan saavuttaa kohtalainen tietoturvan taso ilman korkeaksi nousevia kehityskustannuksia. Evaluoinnin aikana EAL3 -tason saavuttaminen vaatii ns. "grey-box" -ohjelmistotestauksen tekoa ja järjestelmällistä tietoturvaheikkouksien hakemista.

EAL4 - menetelmällisesti suunniteltu, testattu ja katselmoitu

Sovelluksen kehittäjä noudattaa tietoturvallisuusperiaatteita sovellusta rakentaessaan. Sovellussuunnittelijan ei kuitenkaan tarvitse olla erikoistunut tietoturvakysymyksiin. Sovellettavat periaatteet ovat ns. normaalisti kaupallisessa ohjelmistonkehittämisessä käytettäviä menetelmiä. Niiden käyttäminen ei siis vielä edellytä erityistaitoja.

EAL4 -taso on korkein tietoturvan taso, joka voidaan saavuttaa niin, että sovelluskehityksessä ei vielä jouduta muuttamaan olemassaolevaa sovellusten rakennusprosessia tai -menetelmää. Sillä voidaan saavuttaa kohtalainen tietoturvan taso, mutta vastapainoksi sovelluskehityksen kustannukset jo kasvavat, joskaan ei vielä merkittäviksi.

EAL5 - semiformaalisti suunniteltu ja testattu

EAL5 taso vaatii sovelluskehittäjää käyttämään hyväksi todettuja kehityskäytäntöjä kehittäessään ohjelmistoa. Hän käyttää apunaan erityisiä turvallisuustekniikoita (security engineering techniques). Ohjelmiston suunnittelulta ja kehittämiseltä vaaditaan, että jo ohjelmistoa kehitettäessä tavoitellaan EAL5 -tason toteuttamista.

EAL5 -tason tavoittelemisesta syntyy kustannuksia, mutta ei vielä kovin suuria. Kustannukset syntyvät lähinnä järjestelmällisestä tietoturvan huomioonottamisesta jo ohjelmiston tekovaiheessa sekä erityisten tietoturvatekniikoiden toteuttamisesta. EAL5 -tasoa käytetään silloin, kun tavoitteena on kohtalaisen suuri, erillisesti todettu tietoturvallisuustaso suhteellisesti vaatimattomilla kehityskustannuksilla.

Ohjelmistoa evaluoitaessa on tietoturvallisuuden tasoa testattava ja haettava siitä puutteita. Erityisesti evaluoinnin aikana testataan ja haetaan sellaisia heikkouksia, jotka mahdollistavat tietomurron tekemisen. Evaluoinnin aikana varaudutaan siihen, että ohjelmisto joutuu kohtalaisen taitavan tietomurtoyrityksen kohteeksi.

EAL6 - semiformaalisti verifioitu, suunniteltu ja testattu

EAL6 -tasolla sovelluskehittäjä käyttää hyväksi todettuja kehityskäytäntöjä kehittäessään ohjelmistoa. Hän käyttää apunaan erityisiä turvallisuustekniikoita jo ohjelmistoa suunnitellessaan. Ohjelmiston suunnittelun tavoitteena on korkean turvallisuustason ohjelmisto.

Ohjelmistoa evaluoitaessa on tietoturvallisuuden tasoa testattava ja haettava siitä puutteita. Erityisesti evaluoinnin aikana testataan ja haetaan sellaisia heikkouksia, jotka mahdollistavat tietomurron tekemisen. Evaluoinnin aikana varaudutaan siihen, että ohjelmisto joutuu taitavan tietomurtoyrityksen kohteeksi.

EAL7 - formaalisti verifioitu, suunniteltu ja testattu

EAL7 -tasoa tavoitellaan silloin, kun rakennetaan erittäin korkean riskitason sovelluksia. Tällöin sovelluskehityskustannukset ovat korkeita, mutta korkea riskitaso vaatii tuotteelta niin paljon, että sovelluskehityskustannukset ovat oikeutettuja.

Käytännössä EAL7 -tason saavuttaminen vaatii tiukan formaalin analysoinnin toteuttamista ohjelmiston suunnittelu- ja evaluointivaiheessa. Lisäksi ohjelmiston kompleksisuus on suunnittelukustannusten kasvamisesta huolimatta minimoitava. Ohjelmistoa evaluoitaessa vaaditaan ns. "white-box" -testauksen toteuttamista.

EAL-tasojen, US TCSEC ja Eurooppalaisen ITSEC -järjestelmän vertailu [Int]:

EAL-taso	US TCSEC	ITSEC
-	D:Minimal Protection	E0
EAL1	-	-
EAL2	C1:Discretionary Security Protection	E1
EAL3	C2:Controlled Access Protection	E2
EAL4	B1:Labeled Security Protection	E3
EAL5	B2:Structured Protection	E4
EAL6	B3:Security Domains	E5
EAL7	A1:Verified Design	E6

2. Common Criterian hyödyntäminen ohjelmistotyössä

Common Criterian hyödyntämisessä ehdotetaan seuraavaa lähestymistapaa [Far02]:

- ota Common Criterian termistö käyttöön tietoturvaan liittyvissä evaluointiprosesseissa
- tee tietoturvariskien kartoituksesta osa normaalia vaatimusmäärittelymenettelyä
- ota Security Target –kuvausten tekeminen osaksi normaalia suunnittelumenettelyä
- ohjeista ja tue tietoturvanäkökohtien huomioonottamista jo tuotteen suunnitteluvaiheessa

Common Criterian hyödyntäminen sovelluksen suunnittelu- ja rakentamisvaiheessa nostaa todennäköisesti systeemityön kiinteitä kustannuksia [Far02]. Niinpä kustannusten nousu tulee perustella tuotteen tietoturvallisuuden tason nousulla. Tällöinkin tulee harkita sitä, ovatko tuotteen tietoturvallisuusnäkökohdat asiakkaalle niin tärkeitä, että ne oikeuttavat tuotteen rakentamisaikaisten kustannusten nousun. Liiketoiminnasta vastaavat henkilöt voivat esimerkiksi jaotella tuotteet sellaisiin, joissa asiakkaalle määräävänä tai jopa kriittisenä tekijänä on tuotteen hinta ja niihin tuotteisiin joissa tietoturvaominaisuudet ovat määrääviä. On olemassa sovellusalueita, joissa turvallisuustekijät ovat jopa lainsäädännön sanelemia, esimerkiksi Yhdysvalloissa ns. Defence customer –tilanteissa [Far02].

3. Evaluoinnin toteuttaminen

Evaluoinnissa verrataan tietotekniikkatuotteen tai tietojärjestelmän soveltuvuutta ennalta määriteltyihin vaatimuksiin [Int]. Common Criteria määrittelee termin ”Common Criteria evaluointi” seuraavasti: Common Criteria evaluointi on sellainen evaluointi, jossa käytetään Common Criteriaa pohjana evaluoitaessa tietoteknisiä turvaominaisuuksia [Int]. Tarkoituksena on saada eri aikana ja eri henkilöiden tekemät evaluoinnin tulokset vertailukelpoisiksi keskenään. Tämä tapahtuu käyttämällä standardoitua menettelytapaa niin tietoturvamääritysten kuvaamisessa, evaluoinnin tekemisessä kuin tulosten kirjaamisessakin. Common Criteria määrittelee PP, ST ja TOE –evaluoinnit. Tässä dokumentissa keskitytään TOE –evaluointiin.

3.1. Tuotteen evaluointimenettely

Tuotteen evaluointi eli TOE -evaluointi on evaluointi, jossa tarkastellaan jotain tietoteknistä tuotetta. Tuotetta vertaillaan ennalta valittuihin PP- ja ST – määrityksiin. Tarkastelussa pyritään selvittämään miten hyvin tuote täyttää nämä määritykset. Evaluoinnin aikana kuvataan tehdyt havainnot ja johtopäätökset. Evaluoinnin jälkeen päätetään evaluoinnin hyväksymisestä sekä siitä millainen EAL –taso tuotteelle määritetään. Evaluoinnin suorittamista varten on luotu menetelmä nimeltään Common Evaluation Methodology (CEM). Menetelmässä ohjeistetaan yksityiskohtaisesti ne periaatteet ja prosessit, joiden mukaan evaluointi suoritetaan. Sen mukaan evaluointi on jaettu useisiin vaiheisiin. CEM esittää evaluoinnin suorituksen pääosin seuraavasti:

1. evaluoinnin syötteiden määrittäminen
    - varmistuttava siitä, että kaikki evaluointia varten tarvittava materiaali on saatavilla
    - kaiken evaluoinnissa käytettävän tiedon dokumentointi

- testien dokumentointi
- tuotteen dokumentaation hankkiminen
- lähdekoodin hankkiminen
- materiaalin käsittelystä, suojaamisesta ja hävittämisestä sopiminen

2. evaluoinnin tulosteiden määrittäminen
    - havaintoraportti (Observation Report)
        - käytetään tietyn evaluoinnin aikana syntyneen havainnon käsittelyyn
        - kuvaa toiminnon, johon havainto liittyy
        - kuvaa havainnon
        - kuvaa havainnon vakavuusasteen
        - kuvaa sen, kenen vastuulla on esim. havaintoon liittyvien ongelmien ratkaiseminen
    - tekninen raportti evaluoinnista (Evaluation Technical Report)
        - kuvaa evaluoinnin johtopäätökset tekniseltä kannalta
        - evaluoinnissa käytetyt menettelytavat, tekniikat ja välineet
        - evaluoinnissa käytetyt mittarit, kriteerit ja johtopäätökset
        - evaluoinnin tulokset, johtopäätökset ja suositukset

3. kuhunkin EAL-tasoon liittyvät evaluointiohjeet
    - miten ST – ja PP –evaluoinnit tehdään
    - erityiset ohjeet eri osa-alueen evaluoimiseksi
    - miten evaluointi poikkeaa alempien EAL-tasojen evaluoinneista

3.2. Evaluoinnin toteuttaminen

Evaluoinnin suorittaa yleensä riippumaton organisaatio tai yritys, joka on erikoistunut tietoturvaevaluointien tekemiseen [Bis03]. Tällaiset organisaatiot tietysti laskuttavat työstään. Evaluointiin kuuluu evaluointisuunnitelma, jonka noudattamista valvoo evaluointilautakunta (evaluation board). Jotta tuotteen evaluointi onnistuisi hyvin, on työtä myös koordinoitava. Sekä tuotteen valmistajan, että evaluointiorganisaation edustajien on ainakin korkeammilla EAL -tasoilla keskusteltava keskenään tuotteen rakenteen selvittämiseksi evaluointia tekeville henkilöille.

Evaluointi tehdään yleensä jollakin tietyllä tai tietyillä laite- ja ohjelmistokoonpanoilla. Paras tilanne on, jos evaluointi voidaan suorittaa kaikilla niillä ohjelmisto- ja laitekokoonpanoilla, joilla tuotetta tullaan myös käyttämään [Gui99]. Käytännössä tämä ei tietenkään ole aina mahdollista tai edes tarkoituksenmukaista.

Evaluoinnin valmistuttua evaluointia tehnyt organisaatio esittää tulokset evaluoinnin hyväksyjälle (validation agent). Vasta tämä hyväksyjäagentti päättää miten evaluoinnin aikana tehtyihin havaintoihin suhtaudutaan [Bis03]. Agentti voi joko päättää hyväksyä tai hylätä evaluoinnin tulokset. Agentti myös päättää mikä EAL –taso tuotteelle myönnetään. Kannattaa huomata, että tuotteen evaluointi ei sinänsä takaa tuotteen laadukkuutta. Se takaa ainoastaan, että tuote on katselmoitu tietyn käytännön (Common Criteria) mukaisesti [Gui99].

Evaluoinnin kustannukset muodostuvat evaluointiorganisaatiolle maksetuista maksuista, mahdollisen sertifioinnin maksuista ja koko prosessista muodostuvista sisäisistä kustannuksista.

4. Common Criteria Suomessa ja muualla

Common Criteriaa ovat kehittäneet eri maiden kansalliset turvallisuus- ja standardointiorganisaatiot. Aktiivisesti mukana ovat olleet Kanada, Ranska, Saksa, Hollanti, Iso-Britannia ja Yhdysvallat [Gui99]. Tuntuu siltä, että myös tällä hetkellä aktiivisimmin Common Criteriaa tukevat organisaatiot löytyvät näistä maista. EU:n piirissä on aloitettu keskustelu siirtymisestä Common Criterian käyttöön. Myös Suomessa esiintyy spekulointia Common Criterian käyttöönotosta: ”myös Suomeen pyritään luomaan tällaista tukea antava järjestelmä” [Kan98].

Common Criteria- sertifioinneille on olemassa ns. vastavuoroisen hyväksynnän menettely. Sen mukaan kerran sertifioitua tuotetta ei tarvitse uudestaan sertifioida toisessa menettelyn hyväksyneessä maassa. Menettelysopimuksen on allekirjoittanut 14 valtiota (Australia, Englanti, Espanja, Hollanti, Italia, Israel, Kanada, Kreikka, Norja, Ranska, Saksa, Suomi, Uusi-Seelanti, Yhdysvallat) [Par01]. Suomessa ei ole Common Criteria- tietoturvallisuussertifiointeja tekevää elintä. Suomi kuuluukin ns. sertifikaattien kuluttajamaihin (Certificate Consuming Member).

Suomalaisista yrityksistä ainoastaan Setec on (15.3.2001 mennessä) sertifioinut tuotteitaan tietoturvallisuuden arviointijärjestelmän mukaisesti. Nämä sertifioinnit on tehty Saksassa ITSEC –arviointikriteeristön mukaisesti [Par01]. Suomessa tietoturvallisuuden järjestelyt ja sääntely on yleisesti todettu olevan ”hyvää kansainvälistä tasoa” [Pur00]. Tietojärjestelmien tietoturvallisuuden hallinnolliset järjestelmät –raportissa vuodelta 2000 todetaan kansainvälisen standardoinnin kehittymisen edellyttävän kuitenkin myös Suomessa nykyistä tarkempaa standardien huomioon ottamista.

5. Case: Common Criteria –evaluointikokemuksia Australiasta

Australian Information Security Evaluation Program (AISEP) on käyttänyt Common Criteria –evaluointeja ohjelmistotuotteiden evaluointiin [Apt02]. AISEP on evaluoinut yhteensä 17 tuotetta viimeisen kahden vuoden aikana. Työn aikana syntyneitä kokemuksia on esitetty vuoden 2002 International Common Criteria Conference -konferenssissa. Olen tähän kerännyt yhteenvedon konferenssijulkaisussa esitetyistä tärkeimmistä havainnoista.

5.1. Havaitut ongelmat

Evaluointeja tehneet henkilöt ovat havainneet tiettyjen asioiden aiheuttavan ongelmia jatkuvasti. Tällaisia asioita ovat:

- evaluoinnin kohteen määrittely
- evaluoinnin kohteen koostuminen useasta tuotteesta
- yhden tuoteryhmän koostuminen useasta evaluoinnin kohteesta
- evaluoinnin kohteen erottaminen muusta tuotteesta
- tuotteen rakenteen ymmärtäminen
- organisaation tietoturvapolitiikkaan liittyvät ongelmat
- tietotekniikkaympäristöön liittyvät tietoturvamääritykset

Kohteen määrittelyssä ongelmana on, että sovelluskehittäjän on vaikea määritellä tarkkaan mikä on tietoturvaevaluoinnin kohde. Ongelmat ilmenevät määriteltäessä sitä mikä tarkkaan ottaen on evaluoitava tuote, miten tuotetta käytetään ja millainen on tuotteen normaali konfiguraatio.

Evaluoinnin kohde voi tosiasiallisesti koostua useasta eri tuotteesta tai sillä voi olla riippuvuussuhteita muihin tuotteisiin. Tämä on noussut käytännön työssä ongelmaksi. Miten esimerkiksi erotetaan

tuote sen käyttämistä yleisistä luokkakirjastoista? Tuleeko myös luokkakirjastot evaluoida? Entä jos ne käyttävät jotain toisia kirjastoja tai käyttöjärjestelmäpalveluja ? Tietoturvatuotteita evaluoitaessa käytännön esimerkkinä ovat erilaiset kryptografisia palveluja tarjoavat yleiset kirjastot ja moduulit sekä niitä käyttävät ohjelmistot. AIESEP on havainnut, että ongelman ratkaiseminen vaatii evaluointeja suorittavalta henkilöstöltä hyvää näkemystä tuotteesta ja sen rakenteesta. Tällöin voidaan päättää mihin muihin tuotteisiin asti evaluointeja tulee ulottaa.

Vastaavan tyyppinen ongelma ilmenee silloin, kun tuote tai tuoteryhmä koostuu useasta tuotteesta, jotka ovat itsessään sellaisia kokonaisuuksia, että ne ovat myös itsenäisiä evaluoinnin kohteita. Ongelmatilanne tulee esiin myös silloin, kun tuotetta voidaan ajaa useassa eri varusohjelmistoympäristössä. Evaluointeja suorittavien henkilöiden täytyy tällöin pystyä tekemään päätös siitä, ovatko eri ympäristöissä ajettavat ohjelmistot sama tuote vai kaksi erillistä tuotetta. Esimerkkinä mainitaan tapaus, jossa samasta ohjelmistosta oli olemassa versio kolmelle eri käyttöjärjestelmälle. Evaluoinnin aikana kävi ilmi, että vaikka kyseessä oli (piti olla) sama tuote, eri käyttöjärjestelmissä toimivissa versioissa oli niin paljon eroja, että evaluoinnin kannalta ”melkein ainoa yhtäläinen asia tuotteissa oli niiden nimi” [Apt02].

Usein evaluointia tehtäessä on tarpeen testata vain tiettyä osaa tuotteesta. AIESEP on havainnut tämän ongelmalliseksi, koska tietotekniikkatuotteessa esim. sovelluksen osan tai sen toiminnan erottaminen muusta tuotteesta on vaikeaa ja usein jopa mahdotonta. Joka tapauksessa tällaisen erottamisen tekeminen vaatii selkeää ymmärrystä evaluoitavan tuotteen rakenteesta. Käytännössä on havaittu, että ainakin alemmilla EAL -tasoilla toimittaessa ohjelmistot rakennetaan niin, ettei tuotteen rakenteesta ole käytettävissä riittävän tarkalla tasolla olevaa dokumentaatiota. Tyypillinen ohjelmiston mukana toimitettu dokumentaatio on tarkoitettu yksinomaan tuotteen käyttämisen, ei sen rakenteen ymmärtämisen avuksi. Niinpä evaluointia suorittavat henkilöt joutuvat hankkimaan tie-

don käyttämällä tuotetta ja analysoimalla sen rakennetta tällä tavalla sekä keskustelemalla tuotteen rakentaneen ohjelmistonkehitysryhmän kanssa.

Ongelmia Common Criteria –evaluoinnin tekemisessä muodostaa myös tietoturvauhan ja organisaation tietotekniikkaympäristön tason määrittely. ”Suurimmassa osassa evaluointeja meillä oli ongelmia tietoturvauhan määrittelyn kanssa” [Apt02]. Näyttää siltä, että käytännön työssä ongelmaksi muodostuu määritellä mitkä asiat muodostavat uhan turvallisuudelle. Samaten ongelma on suhtautuminen siihen, miten tuotteen tekijät olivat määritelleet tuotteen soveltuvuuden erilaisiin organisaatioiden tietoturvapolitiikkoihin ja -infrastruktuureihin. Ongelmaksi oli muodostunut tapaus, jossa yleisille markkinoille rakennetun tuotteen dokumentaatiossa oli määritelty millaisen tietoturvapolitiikan omaaville yrityksille tuote on suunnattu. Voidaanko tuote tällöin ottaa käyttöön vain niissä yrityksissä joissa on kyseiseen määritykseen soveltuva tietoturvapolitiikka ? Tämä tuo esille liian tiukasti tehtyjen määrittelyjen mukanaan tuoman ongelman.

5.2. Yhteenveto evaluoinneista

AIESEP koki että sen kohtaamat ongelmat olivat sellaisia, jotka ratkeavat Common Criterian kehitystyön myötä. Ongelmat liittyivät suurelta osin menettelytapojen vakiintumattomuuteen, henkilöiden kokemattomuuteen ja syvällisen ymmärtämyksen puutteeseen. Common Criterian käytöstä tehtiin seuraavia yleisluontoisia huomioita.

Common Criteria on suhteellisen uusi tapa suorittaa tietoturvallisuusevaluointeja. Etenkin sovelluskehittäjät eivät vielä tunne menettelyä ja siihen liittyviä vaatimuksia. Lisäksi ainakin AIESEP:n kohdemaassa (Australia) evaluointeja tekevä yhteisö on suhteellisen pieni ja kokematon. Osa ongelmista aiheutuu tästä kokemuksen puutteesta. Kokemustensa perusteella ryhmä väittää Common

Criteria –evaluoinnin Security Target –kuvauksen tekemisen olevan myös selvästi työläämpää kuin vastaavan ITSEC –evaluoinnin kuvauksen.

6. Yhteenveto

Common Criteria on tietotekniikkatuotteiden tietoturvallisuustason määrittely- ja evaluointistandardi (ISO 15408). Common Criteria määrittää valmiiksi joukon vaatimuksia, joita voi käyttää määritettäessä tietotekniikkatuotteen tietoturvavaatimuksia. Lisäksi se määrittelee evaluointimenettelyn, jonka avulla voi arvioida ja määrittää tietotekniikkatuotteiden tietoturvan tasoa. Common Criteria määrittää myös joukon tietoturvallisuustasoja, joihin evaluoidut tuotteet voidaan sijoittaa.

Common Criteria- evaluointimenettelyn käyttäminen ei sinällään takaa tietoturvallisuutta. Se tarkoittaa vain, että tuotteen tietoturvavaatimukset on määritelty, tuote on evaluoitu ja evaluoinnin tulokset on dokumentoitu ennalta sovitulla tavalla.

Suomessa ei ole Common Criteria- tietoturvallisuussertifiointeja tekevää elintä ja niinpä Suomi kuuluukin ns. sertifikaattien kuluttajamaihin (Certificate Consuming Member). Suomi on allekirjoittanut ns. vastavuoroisen hyväksynnän menettelysopimuksen. Sen mukaan kerran Common Criteria –menettelyn mukaan sertifioitua tuotetta ei tarvitse uudestaan sertifioida toisessa menettelyn hyväksyneessä maassa.

Common Criterian käyttö on ilmeisen työlästä ja vaatii syvällistä perehtymistä standardiin. Eräät Common Criteria –evaluointeja tehneet henkilöt ovat myös kokeneet ongelmia, joiden he uskovat ratkeavan vasta Common Criterian kehitystyön myötä. Ongelmat ovat liittyneet ilmeisesti myös menettelytapojen vakiintumattomuuteen ja ihmisten kokemattomuuteen Common Criterian käytössä.

Lähteet

Apt02 Apted A., Carthigaser M., Lowe C., Common Problems with the Common Criteria, 3rd International Common Criteria Conference, March, 2002, 1-23.

Bis03 Bishop Matt, Computer Security, Addison Wesley, 2003, s. 601.

CCI99a Common Criteria for Information Technology Security Evaluation, Part1:Introduction and general model, Version 2.1, CCIMB-99-031, elokuu 1999, s 9.

CCI99b Common Criteria for Information Technology Security Evaluation, Part2:Security functional requirements, Version 2.1, CCIMB-99-032, elokuu 1999, s. 9.

Far02 Farkas A., Walsh C., A Perspective of the Common Criteria in Modern IT Business, 3rd International Common Criteria Conference, May, 2002, 1-8.

Gui99 Common Criteria User Guide, Syntegra, Oct, 1999.

Int Common Criteria An Introduction, Syntegra.

Kan98 Kansikas Aarno, Tietoturvallisuusluokitukset, Systeemityö 3/98, Maaliskuu, 1998, s. 9.

Mar02 Marquet B., Gustave C., Common Criteria: A Foundation for a Comprehensive Security Framework, 3rd International Common Criteria Conference, May, 2002.

Par01 Parmes Rauli et al., Tietojärjestelmien tietoturvallisuuden hallinnolliset järjestelyt, Liikenne- ja viestintäministeriön mietintöjä ja muistioita B 20/2001, 15.3.2001, liite 2 s. 3.

Pur00 Purhonen Mika et al., Tietojärjestelmien tietoturvallisuuden hallinnolliset järjestelyt, Puolustustaloudellinen suunnittelukunta, 15.5.2000, s. 11-18.