TIETOTURVAN PERUSTEET: KERTAUSTA

T. Karvi

Helmikuu 2012

Turvallisuuskoulutus turvallisuusjohdolle I

Organisaatioiden turvallisuus on hyvin laaja alue, josta tietoturvallisuus muodostaa vain pienen osan. Erään entisen kaupallisen turvallisuuskurssin asioita:

- Turvallisuus yrityksen tai organisaation toiminnassa ja turvallisuuden johtaminen.
- Turvallisuusriskien tunnistaminen ja hallintakeinot.
- Turvallisuustoiminnan lainsäädännöllinen viitekehys.
- Turvallisuusviestintä ja -tiedottaminen, turvallisuuskoulutus.
- Tuotannon ja toiminnan turvallisuus.
- Työturvallisuus.
- Pelastustoiminta.
- Ympäristöturvallisuus.
- Varautuminen ja jatkuvuussuunnittelu.

Turvallisuuskoulutus turvallisuusjohdolle II

- Tietoturvallisuus.
- Tietotekninen turvallisuus.
- Tilaturvallisuus- ja turvallisuusvalvonta.
- Taloushallinnon ja varainhoidon turvallisuus.
- Henkilöturvallisuus ja ulkomaantoimintojen turvallisuus.
- Security Management.
- Turvallisuussuunnitelmat ja -projektit.
- Turvallisuuden kehittäminen ja johtaminen.

Erään entisen kaupallisen tietoturvallisuuden koulutusohjelman sisältö I

- Tietoturvallisuus organisaation toiminnan osana.
- Tietoturvallisuutta koskeva lainsäädäntö ja viranomaistoiminta.
- Riskien tunnistaminen ja hallintakeinot.
- Tietoaineistojen luokitus ja valvonta.
- Järjestelmien kehittäminen ja ylläpidon turvallisuus.
- Laitteistojen ja ohjelmistojen turvallisuus.
- Salaustekniikat ja niiden hallinta.
- Tietoliikenneturvallisuus.
- Henkilöturvallisuus.
- Fyysinen turvallisuus.
- Käyttöturvallisuus ja tietojärjestelmien palveluiden hankinta.
- Liiketoiminnan jatkuvuuden hallinta.

Erään entisen kaupallisen tietoturvallisuuden koulutusohjelman sisältö II

- Tietoturvallisuuden tarkastaminen ja kehittäminen.

Huomattakoon, että näillä kursseilla ei ole käsitelty turvallista ohjelmistosuunnittelua, ohjelmiston toteutusta ja testausta eikä turvaprotokollia.

CISSP I

Certified Information System Security Professional (CISSP) -sertifikaatteja myöntää voittoa tavoittelematon organisaatio International Information Systems Security Certification Corsortium eli ISC, jonka tutkintoja Suomessa järjestää Tietoturva ry. Koe kestää kuusi tuntia ja se sisältää 250 monivalintakysymystä oheisilta aihealoilta. Jotta kokeeseen voisi osallistua, osallistujalla on oltava vähintään kolmen vuoden yhtäjaksoinen työkokemus joltain alla mainituista aihealueista välittömästi koetta edeltävältä ajalta. Jotta sertifikaatti pysyisi voimassa, on kolmen vuoden aikana kerättävä täydennyspisteitä.

- Access Control
- Telecommunications and Network Security
- Information Security Governance and Risk Management
- Software Development Security
- Cryptography

CISSP II

- Security Architecture and Design
- Operations Security
- Business Continuity and Disaster Recovery Planning
- Legal, Regulations, Investigations and Compliance
- Physical (Environmental) Security

Muita sertifikaatteja on olemassa runsaasti, yli 60. Etsi esim. hakusanoilla *information security certifications*.

Luku 1: Peruskäsitteitä I

- Muista, että tietoturva määritellään kolmen käsitteen avulla: luottamuksellisuus, eheys, käytettävyys. Miten nämä toteutetaan?
- Muista vielä, että edellisten käsitteiden lisäksi nykyaikaisessa tietoturvatutkimuksessa ja -käytännössä käytetään vielä "kolmea A:ta": assurance, authenticity, anonymity.
- Muista turvallisen suunnittelun kymmenen periaatetta:

Määritelmä

I. Taloudellisen mekanismin periaate *sanoo, että turvamekanismin tulisi olla niin yksinkertainen kuin mahdollista.*

Määritelmä

II. Oletuskiellon periaate *sanoo että subjektilta pitää kieltää pääsy objektiin, ellei subjektille ole eksplisiittisesti sallittu pääsyä siihen.*

Määritelmä

III. Täydellisen välityksen periaate *(complete mediation) vaatii, että kaikkien pääsyjen kohdalla tulee tarkistaa, että pääsy on todella sallittu.*

Määritelmä

IV. Avoimen suunnittelun periaate *sanoo, että turva-arkkitehtuurin ja turvasuunnittelun tulisi olla julkinen. Salaista saisi olla salaiset avaimet.*

Määritelmä

V. Oikeuksien erottamisen periaate *sanoo, että systeemin ei pitäisi antaa oikeuksia yhden ehdon perusteella.*

Määritelmä

VI. Pienimmän oikeuden periaatteen *mukaan subjektille tulee antaa vain ne oikeudet, joita hän välttämättä tarvitsee tehtävän suorittamiseen.*

Määritelmä

VII. Pienimmän yhteisen mekanismin periaate *sanoo, ettei resursseihin pääsyä valvovia mekanismeja pidä jakaa muiden kanssa.*

Määritelmä

VIII. Psykologisen hyväksyttävyyden periaate *sanoo, että turvamekanismin ei tule vaikeuttaa resurssien käyttöä verrattuna tilanteeseen, jossa mekanismia ei käytetä.*

Määritelmä

IX. Työmääräperiaatteen *mukaan hyökkäyksen torjuntaan kulutettavat resurssit tulisi olla verrannollisia hyökkääjän resursseihin.*

Määritelmä

X. Tallennusperiaatteen *mukaan on toisinaan parempi vain rekisteröidä tietomurto ja kerätä siitä tietoja kuin yrittää estää se.*

- Muista pääsynvalvonnan tyypit:

Määritelmä

Jos yksittäinen käyttäjä, yleensä objektin omistaja, voi asettaa objektin käyttöoikeudet, kysymyksessä on yksilöpohjainen pääsynvalvonta (engl. discretionary access control eli DAC, tai identity-based access control).

Määritelmä

Sääntöpohjainen pääsynvalvonta (engl. mandatory access control, rule-based access control) on sellainen keskitetty järjestelmä, että objektit on luokitelty hierarkkisille tasoille objektin turvavaatimusten mukaisesti (esim. top secret, secret, confidential), subjekteille on asetettu turvatasot ja subjektilla on pääsy objektiin, jos subjekti-objekti -pari täyttää ennalta määritellyt turvallisuusehdot hierarkioiden ja turvatasojen perusteella. Siten systeemi valvoo, kuka pääsee käsiksi objekteihin, eikä yksittäinen käyttäjä voi tätä muuttaa.

Määritelmä

Luontipohjainen pääsynvalvonta (engl. originator controlled, ORGON) perustuu objektin luojan määrityksiin.

Lisäksi roolipohjainen pääsynvalvonta (RBAC).

Luku 1: Peruskäsitteitä VI

- Muista pääsynvalvontamekanismien "tietorakenteet" pääsymatriisit, pääsylistat ja valtakirjat (capabilities). Erityisesti pääsynvalvontapolitiikan ja -mekanismin erottaminen hyödyllistä.

- Osaa selittää, mitä tarkoittaa jonosalaus, lohkosalaus, julkisen avaimen salaus.
- Osaa selittää ketjutustekniikat ECB, CBC, CFB, CTR. Osaa analysoida tiedonsiirtovirheiden vaikutusta. Ymmärrä kaavoja kuten

$$\begin{aligned} D_K(C'_n) \oplus C_{n-1} &= \tilde{Q}_n, \\ D_K(C_{n+1}) \oplus C'_n &= Q'_{n+1}, \\ D_K(C_{n+2}) \oplus C'_{n+1} &= Q_{n+2}. \end{aligned}$$

Luku 2: Kryptgrafian perusteita II

- Muista julkisen avaimen salauskaava

$$C = M^e \mod n.$$

  Purkuun käytetään kaavaa

$$M = C^d \mod n = (M^e)^d \mod n = M^{ed} \mod n.$$

  Osaa laskea potenssiinkorotuksia moduloaritmetiikassa käyttäen ominaisuuksia

$$(ab) \mod n = (a \mod n)(b \mod n) \mod n.$$

- Sanoma allekirjoitetaan "salaamalla"se lähettäjän salaisella avaimella D_{K_s}. Muista myös, että yleensä allekirjoitetaan tiiviste koko sanoman sijasta.
- Muista tiivistefunktioilta vaadittavat ominaisuudet:

Luku 2: Kryptgrafian perusteita III

1. $h(M)$ voidaan laskea minkä pituiselle M tahansa.
2. $h(M)$ on kiinteän pituinen.
3. $h(M)$ on helppo laskea.
4. Jos annetaan y, ei ole helppoa löytää sellaista M:ää, että $h(M) = y$. Eli h on *alkukuvaresistentti* (h has preimage resistance).
5. Jos on annettu y ja M_1, ei ole helppoa löytää sellaista $M_2 \neq M_1$, että $h(M_1) = h(M_2)$. Eli h on *injektiotyyppinen* (h has second preimage resistance).
6. On vaikeaa löytää mitään paria (M, M'), jolle $h(M) = h(M')$. Eli h on *törmäysresistentti* (collision resistance).

- Muista tilanne tiivistefunktioiden kohdalla: perinteellisiä tiivistefunktioita MD5, SHA-1, SHA-2, RIPEMD-160 ei pidetä enää turvallisina:
  Paraikaa ollaan kehittämässä SHA-3:ta, ja sen pitäisi tulla markkinoille tänä vuonna. MD5 (pituus 128 bittiä) on ehdottomasti vanhentunut, SHA-1:tä (160 b) ei myöskään ole suositeltu enää

vähään aikaan. Sen sijaan SHA-2 -versiot (224, 256, 384, 512 bittiä) toiminevat vielä käytännössä jonkin aikaa.

- Muista MAC: tiivistefunktio plus salainen avain.
- Muista suositellut avainten pituudet symmetrisessä ja epäsymmetrisessä salauksessa sekä tiivisteen suositeltu pituus.

Luku 3: Käyttöjärjestelmien turvallisuus I

- Muista käynnistysjärjestys ja BIOS-vaiheen salasana. Virransäästötilan haavoittuvuudet (live CD attack eli käyttöjärjestelmä ladataan ulkoiselta medialta kuten CD:ltä, jonka jälkeen kovalevy luetaan ohittaen alkuperäisen KJ:n suojaukset).
- Kirjausten merkitys, erilaiset lokitiedostot ovat hyödyllisiä (system, application, security).
- Muista komennot ps, top, pstree, kill Unixissa ja Task Manager, Process Explorer Windowsissa (available from Microsoft Sysinternals).
- Osaa selittää virtuaalimuistin haavoittuvuudet ja varautumisen näiden hyväksikäyttöön.
- Selitä salasanojen valintakriteerit, tyypillisimmät hyökkäykset salasanoja vastaan, salasanojen suolaus.
- Osaa kuvailla salasanojen välitysmekanismin periaatteen asiakkaalta palvelimelle. Ei yksityiskohtia.

Luku 3: Käyttöjärjestelmien turvallisuus II

- Osaa käyttää chmod-käskyä Unixissa.
- Osaa selittää todellisen ja efektiivisen UID:n määritelmän ja kuvailla käyttötilanteita, joissa näitä joudutaan vuoroin käyttämään setuid-bitin kanssa.
- Osaa kuvailla tiedostonimien tyypit: inode, tiedostokuvaaja, absoluuttinen ja suhteellinen polkunimi.
- Osaa antaa esimerkin symbolisten linkkien vaaroista. Tietää, miten symboliset linkit käyttäytyvät tiedostokomentojen yhteydessä.
- Osaa selittää linkityksen ja DLL-injektion.
- Osaa selittää puskurin ylivuotohyökkäysten periaatteet ja vastatoimenpiteitä.

Luku 4: Haittaohjelmat I

- Osaa haittaohjelmien terminologian ja osaa sanoa, minkä tyyppinen haittaohjelma on aiheuttanut vahinkoa missäkin tilanteessa.
- Osaa kuvailla virusten luokittelun.
- Osaa luetella puolustuksia sisäisiä hyökkäyksiä vastaan.
- Osaa luetella haittaohjelmien torjuntamenetelmiä ja -käytäntöjä.

Luku 5: Verkkojen turvallisuus I I

- Oletuksena on, että omaa kokonaiskuvan tietoliikenneverkoista ja tuntee pääpiirteiltään ARP:n IP:n, TCP:n ja DNS:n toiminnan.
- Osaa selittää ARP-haavoittuvuuden ja esittää torjuntamenetelmiä ARP-hyökkäystä vastaan.
- Osaa selittää IP-huijauksen ja miten sitä voi yrittää torjua.
- Osaa selittää torjuntakeinoja pakettien sieppauksen estämiseksi.
- Osaa selittää TCP-istunnon kaappauksen ja miten sitä on torjuttu.
- Palvelunestohyökkäyksistä pitäisi muistaa vain SYN-tulvitus ja ehdotuksia sen torjumiseksi.
- Muista myös ehdotukset, miten protokollia pitäisi suunnitella palvelunestohyökkäysten vaikeuttamiseksi.

Luku 6: Verkkojen turvallisuus II I

- Osaa selittää nimipalvelun käteismuistin myrkytystekniikat ja miten niitä on pyritty vaikeuttamaan. DNSSECin periaate.
- Osaa kuvailla palomuurityypit ja osaa antaa esimerkkejä erilaisista palomuurikonfiguraatioista.
- Osaa kuvailla SSH:n aseman protokollapinossa, sen tuottamat palvelut ja sen perusrakenteen.
- Osaa vastata kysymyksiin "Mikä on varmenne?"ja "Miten ja mihin tarkoitukseen varmenteita käytetään?". Osaa selittää, miten varmenteiden allekirjoitukset käytännössä usein joudutaan verifioimaan (eli etsimään jokin CA, johon lähettäjä ja vastaanottaja luottavat ja joka on kummankin varmenteen varmenneketjun huipulla).
- Osaa selittää, miten varmenteet käytännössä toimitetaan käyttäjille.

Luku 6: Verkkojen turvallisuus II II

- Osaa selittää varmenteisiin liittyviä ongelmia: todennus, muttei valtuutusta, varmenteiden jakelu, peruutuslistat, varmenneketjut.
- Varmenteisiin liittyviä protokollia, erityisesti OCSP.
- IPsec: yleisarkkitehtuuri (AH, ESP, SAD, SPD, SA, SPI).
- Osaa selittää pakettien rakenteen AH:n ja ESP:n yhteydessä kuljetus-ja tunnelimoodissa IPv4:ssä. Myös kun ESP:tä ja AH:ta käytetään yhdessä.
- Osaa kiritisoida IPsec:iä.