TIETOTURVAN PERUSTEET

T. Karvi

Tammikuu 2013

Johdanto

Kurssi perustuu oppikirjaan

- Michael T. Goodrich, Roberto Tamassia: Introduction to Computer Security. Pearson 2011.

Kirjaa käydään läpi luku luvulta lukuunottamatta lukua 2, jota käsitellään pintapuolisemmin kuin muita lukuja. Ei myöskään käsitellä käyttöjärjestelmien ja tietoliikenteen perusteita, jotka oletetaan tunnetuiksi.

Luku 1: Peruskäsitteitä I

- Tietoturva määritellään kolmen käsitteen avulla: luottamuksellisuus, eheys, käytettävyys.
- **Luottamuksellisuus** toteutetaan salauksen, pääsynvalvonnan, todennuksen, valtuutuksen ja fyysisen turvallisuuden avulla.
- Tietoaineiston **eheys** varmistetaan varmuuskopioilla, tarkistussummilla ja tietoja korjaavilla koodeilla.
- **Käytettävyys** varmistetaan fyysisellä suojauksella ja kaksinkertaistamalla laitteistoja (RAID-levyt, varakoneet).

A.A.A I

- Edellisten käsitteiden lisäksi nykyaikaisessa tietoturvatutkimuksessa ja -käytännössä käytetään vielä "kolmea A:ta": assurance, authenticity, anonymity.
- **Assurance** eli **varmuus** viittaa siihen, miten luottamus saadaan aikaan ja miten sitä ylläpidetään tietokonesysteemeissä. Luottamus on hankala määritellä täsmällisesti, mutta se liittyy siihen, että ihmiset tai systeemit toimivat siten kuten oletamme. Luottamus syntyy seuraavien tekijöiden yhteispelistä:
  - Käyttösäännöt määräävät, miten tulisi toimia.
  - Oikeudet kuvaavat, mitä saa tehdä.
  - Suojaukset takaavat, että oikeuksia ei rikota tai käytetä väärin.
- **Authenticity** eli autenttisuus tarkoittaa menetelmiä, jotka varmistavat, että käskyt, politiikat ja käyttöluvat tulevat oikeilta tahoilta.

A.A.A II

- Autenttisuuteen kuuluu kiistämättömyys eli ominaisuus, ettei määräyksen antaja tai tehtävän hyväksyjä voi kiistää jälkeenpäin antaneensa määräystä tai hyväksyneensä tehtävää.
- Autenttisuus ja kiistämättömyys saadaan aikaan digitaalisella allekirjoituksella, joka toteutetaan käytännössä julkisen avaimen salauksen avulla.
- Digitaaliset allekirjoitukset takaavat alkuperän lisäksi eheyden, ts. ettei dokumenttia ole millään tavoin muutettu.

- Monissa tapauksissa tarvitaan myös **anonymiteettiä**. Jos aina toimittaisiin todellisen identiteettin varassa, digitaalisessa maailmassa olisi helppoa yhdistää erilaisia tietoja, jotka yhdessä murentaisivat yksilön suojaa. Jos organisaatio haluaa julkistaa tietoja jäsenistään, yleensä oletetaan, että se tapahtuu yksityisyyttä suojaten. Tähän tavoitteeseen pääsemiseksi organisaatio voi tehdä seuraavaa:

A.A.A III

- Kooste (aggregation): Tiedot voidaan kerätä useasta yksilöstä, jonka jälkeen julkaistaan vain keskiarvoja tai summia. Näin yksilöt eivät paljastu.
- Sekoitus: Jos sekoitetaan tapahtumia, tietoja tai yhteyksiä niin, ettei tietuetta voida yhdistää kehenkään yksilöön, saavutetaan yksityisyyden suoja. Edelletyksenä on, että yksilöön liittyvät tiedot voidaan kuitenkin koota, mutta siten, ettei identiteetti paljastu.
- Sovellustason välimuistit eli proxit: Nämä ovat luotettuja agentteja, jotka suorittavat tehtäviä yksilön puolesta siten, etteivät toimenpiteet paljasta yksilöä. Vrt. internet-proxit, joiden kautta pääsee katsomaan sivuja, jotka virallisesti on kielletty.
- Pseudonyymit: Kuvitteellisia identiteettejä, joita voidaan käyttää kommunikoidessa ja tapahtumien yhteydessä. Vrt. sosiaaliset verkot, joissa voi seikkailla paljastamatta identiteettiään.

Uhat ja hyökkäykset

- *Salakuuntelu.*
- *Muuntelu*, jossa tietoja muunnellaan ilman, että vastaanottaja sitä huomaa.
- *Palvelunesto*.
- *Toiseksi tekeytyminen*. Tähän kuuluu tietojen kalastelu (phishing) väärällä identiteetillä ja huijaaminen (spoofing) lähettämälllä esimerkiksi paketteja väärennetyllä lähdeosoitteella.
- *Kiistäminen* (repudiation), jolloin kiistetään, että ollaan saatu tietoa tai allekirjoitettu jotain.
- *Korrelaatio* ja *jäljitys*. Yhdistetään useita tietolähteitä ja tietovirtoja yrittäen näin paljastaa tietyn tietovirran tai tiedon. Tämä on hyökkäys anonymiteettiä vastaan.

Turvallisen suunnittelun periaatteet I

Seuraavassa esitellään kymmenen yleistä periaatetta, joita tulisi soveltaa turvallisuuteen liittyvissä projekteissa. Nämä yleiset periaatteet on laadittu varhain (Salzer and Schroeder, 1975), mutta periaatteet ovat kestäneet aikaa yllättävän hyvin.

Määritelmä

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

Jos määrittelyt ja toteutukset ovat yksinkertaisia, virheitä on todennäköisesti vähemmän. Monimutkaiset mekanismit usein tekevät oletuksia systeemistä ja ympäristöstä. Jos nämä oletukset ovat virheellisiä, ilmaantuu turvaongelmia.

Turvallisen suunnittelun periaatteet II

Määritelmä

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

Erityisesti objektiin pääsystä ei ole mitään oletusarvoja tai oletusoikeuksia. Jos subjekti ei onnistu viemään objektiin kohdistuvaa operaatiota loppuun, sen pitäisi purkaa tehdyt osaoperaatiot ennen lopettamistaan. Näin systeemi pysyy turvallisena vaikka ohjelma keskeytyisi.

Turvallisen suunnittelun periaatteet III

Määritelmä

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

Aina kun subjekti yrittää lukea objektin, käyttöjärjestelmän tulisi toimia välittäjänä. Ensiksikin KJ päättää, onko subjektilla oikeus lukea objekti. Jos on, KJ tarjoaa resurssit lukemiseen. Jos subjekti yrittää lukea samaa objektia uudestaan, taas tulisi tehdä tarkistus. Useimmat systeemit eivät toista tarkistuksia. Ne tallentavat ensimmäisen tarkistuksen tuloksen ja nojautuvat tähän uuden pyynnön yhteydessä.

Turvallisen suunnittelun periaatteet IV

Määritelmä

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

Näin useat tahot ja tutkimusryhmät voivat tarkistaa systeemin ja mahdolliset heikkoudet ja virheet löytyvät paremmin ja ajoissa.

Turvallisen suunnittelun periaatteet V

Määritelmä

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

Esimerkiksi Berkeleyn UNIX:ssa käyttäjät eivät voi vaihtaa käyttäjätiliään juureksi, ellei kaksi ehtoa ole voimassa. Ensimmäinen ehto on, että käyttäjä tuntee juuren salasanan. Toinen ehto on, että käyttäjä kuuluu wheel-ryhmään (GID 0). Molempien ehtojen tulee olla voimassa.
Periaate tarkoittaa nykyään myös sitä, että systeemin komponentit tulisi erottaa toisistaa siten, ettei yhteeen komponenttiin tehty tietomurto johda koko järjestelmän tietoturvan murtumiseen.

Turvallisen suunnittelun periaatteet VI

Määritelmä

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

Turvallisen suunnittelun periaatteet VII

Määritelmä

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

Jos esimerkiksi tiedosto täytyy jakaa usean käyttäjän kanssa, niin näillä käyttäjillä tulisi olla erilliset pääsykanavat tiedostoon.

Turvallisen suunnittelun periaatteet VIII

Määritelmä

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

Käytännössä turvamekanismit lisäävät jonkin verran vaivaa, mutta lisäyksen tulisi olla kohtuullista. Turvamekanismien toteutus vaatii myös laskentaresursseja, joita kaikissa sovelluksissa ei ole riittävästi. Siten turvallisuusvaatimuksista on tällaisissa tapauksissa tingittävä. Esimerkiksi verkkokerrokseen tarvittaisiin vahvoja todennusmenetelmiä, mutta raskaan liikenteen yhteydessä vahvat todennusmenetelmät eivät ole toistaiseksi olleet mahdollisia.

Turvallisen suunnittelun periaatteet IX

Määritelmä

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

Näin esim. opiskelijatietojen suojaaminen muutoksilta ei vaatisi yhtä paljon resursseja kuin sotilaallisten tietojen suojelu. Tämän periaatteen noudattaminen on hieman vaikeaa, sillä se mikä tänään tuntuu raskaalta laskennalta saattaa muutamassa vuodessa muuttua helposti toteutettavaksi.

Turvallisen suunnittelun periaatteet X

Määritelmä

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

Esimerkiksi valvontakameroiden käyttöönotto voi olla halvempi ja yhtä hyvä ratkaisu kuin ovien ja ikkunoiden vahvistaminen. Samoin palvelimet voivat rekisteröidä kaiken liikenteen, joka liittyy tiedostoihin, sähköpostiin ja verkossa surffailuun.
On tosin myönnettävä, ettei tämä periaate sovi täysin tietokoneympäristöön, sillä taitava murtautuja voi peittää tehokkaasti jälkensä.

Pääsynvalvontamallit I

- Pääsynvalvonta on ensimmäiseksi järjestettävä asia verkkoympäristössä.
- Pääsynvalvonnassa on ensiksi määriteltävä, ketkä saavat käyttöoikeuden mihinkin järjestelmän osaan. Eli ensiksi on määriteltävä pääsynvalvonnan politiikka.
- Sen jälkeen on otettava käyttöön mekanismi, turvamekanismi, jonka avulla toteutetaan valittu politiikka.
- Tämä politiikan ja sen toteutusmekanismin erottelu selventää määrittelyjä. On esimerkiksi mahdollista käyttää yleisiä politiikkakieliä määrittelemään oikeuksia, joita sitten valvotaan käyttöjärjestelmän ja sovellusohjelmistojen suomien mekanismien avulla.

Pääsynvalvonnan tyypit I

Pääsynvalvonnan tyypit voidaan jaotella kolmeen tai neljään perustyyppiin.

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).

Yksilöpohjaisessa pääsynvalvonnassa pääsyoikeudet perustuvat subjektin ja objektin identiteettiin. Identiteetti on tässä avainsana: objektin omistaja asettaa pääsyrajoitukset määrittelemällä, kuka saa pääsyn objektiin. Määrittely perustuu subjektien identiteettiin.

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.

Esimerkiksi käyttöjärjestelmä pakottaa noudattamaan sääntöpohjaista pääsynvalvontaa, ainakin tietyissä tilanteissa. Ei subjekti eikä objektin omistaja voi määritellä, kuka saa pääsyoikeuden.
Sääntöpohjaisella järjestelmällä estetään mm. Troijan hevosten kautta tapahtuva tietojen vuoto.

Määritelmä

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

Tässä politiikassa objektin, esimerkiksi tiedoston, luoja päättää, kenellä on pääsyoikeus tiedostoon. Tiedoston omistaja ei voi tätä muuttaa.

Lisäksi voidaan määritellä roolipohjainen pääsynvalvonta. Oikeuksia ei myönnetä yksittäiselle subjektille, vaan roolille, jonka eri subjektit voivat ottaa sallittujen sääntöjen puitteissa. Roolin kohdalla voidaan puolestaan noudattaa edellä mainittuja kolmea pääsynvalvontatyyppiä.

Monentasoinen pääsynvalvonta

Tällaiset järjestelmät ovat MAC-järjestelmän erikoistapauksia. Ideana on, että määritellään turvallisuuustavoite ja tiedonkulku järjestetään niin, että tavoite saavutetaan. Seuraavassa mainitaan muutamia tällaisia järjestelmiä nimeltä; yksityiskohdat sivuutetaan.

- *Bell-LaPadula- eli BLP- ja Biba-malli*: BLP:ssä tiedonkulku korkeammalta turvallisuustasolta alemmalle estetään. Alemman tason toimijat voivat modifioida ylemmän tason tietoja, mutta eivät voi lukea niitä. Muuttaminen aiheuttaa eheysongelmia, joita Biban malli yrittää korjata.
- *Kiinanmuuri*: Vuodelta 1989. Tavoitteena rajoittaa tiedonkulkua organisaatiossa, joka käsittelee kilpailevien yritysten tietoja.
- *Clarkin ja Wilsonin malli*: Soveltuu tilanteisiin, jossa tiedon eheys on tärkeämpi kuin luottamuksellisuus.

Pääsynvalvontamekanismit I

- Pääsynvalvontamekanismeja on useita. Käyttöjärjestelmä huolehtii osittain pääsynvalvonnasta, ainakin tiedostojen suhteen.
- Mekanismit voivat perustua pääsymatriiseihin, pääsylistoihin tai valtakirjoihin (capabilities). Näitä voisi kutsua pääsynvalvontamalleiksi. Malli olisi siis pääsynvalvontatyypin ja varsinaisen toteutuksen välimaastossa.
- Pääsynvalvontamatriisissa on rivit edustavat subjekteja ja sarakkeet objekteja. Kussakin matriisin alkiossa on tieto, mitä subjekti voi tehdä objektille. Matriisi mahdollistaa nopean tarkistuksen, mutta se kasvaa herkästi liian suureksi.
- Pääsynvalvontalistassa on jokainen matriisin sarake omana listanaan ilman tyhjiä paikkoja. Tämä säästää tilaa, mutta on hankalaa nähdä nopeasti subjektin kaikki oikeudet.

Pääsynvalvontamekanismit II

- Valtakirjassa on lista jokaista subjektia kohti ja listassa on objektit, joihin subjektilla on oikeuksia.
- Viime aikoina huomiota on saanut kryptografinen pääsynvalvonta, CAC. Se pyrkii samaan kuin monentasoiset mallit, mutta yleisemmin. Menetelmät perustuvat salakirjoitukseen ja erilaisiin avaimiin (ryhmäavaimet, hierarkkiset avaimet yms).

Yleistä salasanoista I

- Tavallisin todennusmekanismi perustuu salasanoihin. Tosin kriittisissä sovelluksissa voidaan käyttää biometrisiä tunnisteita salasanojen sijasta.
- Salasanat näyttävät tarjoavan hyvän suojan ulkopuolisia vastaan, joskin niiden huolimaton valinta ja käyttö saattavat aiheuttaa riskejä.
- Lisäksi ohjelmistoissa on otettava huomioon muutamia yksinkertaisia asioita. Ohjelmisto ei saa esimerkiksi kysyä käyttäjätunnusta ja ilmoittaa heti, että se on väärin. Tällöin tunkeutuja saisi tietoonsa, että tunnus ei ole oikea. Sen sijaan parempi on kysyä sekä käyttäjätunnusta että salasanaa ja ilmoittaa vasta sitten, jos jompi kumpi on virheellinen. Tällöin tunkeutuja ei saa tietoonsa, kumpi on virheellinen, tunnus vai salasana.

Yleistä salasanoista II

- Salasanojen lisäksi voidaan käyttää muitakin tekijöitä käyttäjän identifioimiseen. Voidaan esimerkiksi ottaa huomioon aika, vaikka virka-aika, jolloin sisäänkirjoittautuminen on mahdollista. Virka-ajan ulkopuolella pääsy kielletään.

Hyökkäykset salasanoja vastaan I

- Ensimmäinen yritys on kokeilla systemaattisesti erilaisia salasanoja samalla käyttäjätunnuksella. Tämä on varsin tehokas menetelmä, sillä kone kykenee arvaamaan suunnattoman määrän lyhyessä ajassa ja monet valitsevat heikkoja salasanoja (liian lyhyitä, luonnollisen kielen sanoja, liian yksinkertaisia modifikaatioita).
  Nykyään ohjelmistot torjuvat näitä hyökkäyksiä hidastamalla salasanojen tarkistusta, jos samalle tunnukselle yritetään antaa väärä salasana useaan kertaan.
- Anastetaan salasanatiedosto. Yleensä salasanat eivät ole selväkielisessä muodossa salasanatiedostossa, joten edelleen joudutaan systemaattisesti testaamaan eri vaihtoehtoja. Nykyään tähän on kuitenkin olemassa tehokkaita menetelmiä. Esimerkiksi tiivisteitä voidaan laskea etukäteen ja tulosten tallettamiseen käytetään sateenkaaritauluja.

Hyökkäykset salasanoja vastaan II

- Sosiaalinen urkinta on kolmas vaihtoehto. Tekeydytään joksikin auktoriteetiksi ja udellaan salasanoja ”alaisilta”. Myös sähköpostikyselyt ovat arkipäivää.

Salasanojen valinta I

Yllä kuvattujen selvittämisyritysten vaikeuttamiseksi salasanojen valinnassa suositellaan seuraavien seikkojen huomioimista:

- Käytä muitakin merkkejä kuin kirjaimia A-Ö.
- Valitse pitkiä salasanoja. Kombinatorinen räjähdys alkaa, kun pituus ylittää 5-6 merkin pituuden, mutta hyvä salasana paljon pitempi. Nykyään suositus on vähintään 8 tai 10 merkkiä.
- Vältä todellisia nimiä ja sanoja.
- Valitse epätodennäköinen salasana. Kehitä jonkinlainen muistisääntö salasanan muistamiseksi.
- Vaihda salasana säännöllisesti. Tällä tavoin estetään kauan kestävät systemaattiset salasanan murtoyritykset.

Salasanojen valinta II

- Älä kirjoita salasanaa muistiin. Tämä sääntö alkaa tosin menettää pätevyyttään, sillä erilaisten tunnusten määrä alkaa olla jo niin suuri, että jonkinlaista kirjanpitoa tarvitaan. Pidä kuitenkin salasanalistat hyvässä tallessa.
- Älä kerro salasanaa kenellekään toiselle.