

# **LUOTTAMUKSELLISUUDEN JA TODENNUKSEN PERUSTEET SEKÄ KERBEROS- TODENNUSPROTOKOLLA**

Markus Pakkala

Opinnäytetyö  
Joulukuu 2010  
Tietojenkäsittelyn koulutusohjelma  
Tietoverkkopalveluiden suuntautumisvaihtoehto  
Tampereen ammattikorkeakoulu

## TIIVISTELMÄ

Tampereen ammattikorkeakoulu  
Tietojenkäsittelyn koulutusohjelma  
Tietoverkkopalveluiden suuntautumisvaihtoehto

PAKKALA, MARKUS: Luottamuksellisuuden ja todennuksen perusteet sekä Kerberos-todennusprotokollan toiminta

Opinnäytetyö 38 s.  
Joulukuu 2010

---

Opinnäytetyön tilaajana toimi Avanor Oy. Tutkimusongelmana oli ottaa selvää ja raportoida kahden tietoturvan suuren periaatteen, luottamuksellisuuden ja todennuksen perusteista sekä niiden käytännön haasteista. Lisäksi oli määrä esitellä Kerberos-todennusprotokolla, tutkia sen toimintaa ja mahdollisia uhkia sen luotettavalle toiminnalle. Opinnäytetyön tarkoitus oli tuottaa edellä mainituista aiheista selkeä esitys, joka on lukijalleen hyödyksi sinällään. Tavoitteena oli antaa tiedollisia valmiuksia tutkia käsiteltyjä aiheita omatoimisesti. Työ on laadullinen tutkimus, jonka aineistona toimi alan kirjallisuus.

Luottamuksellisuuden tarkoitus on tiedon lukemisen ja muokkaamisen salliminen vain siihen oikeudet omistaville käyttäjille. Motiivit tiedon luottamuksellisuuden säilyttämiseen ovat lähinnä kaksijakoisia. Todennuksen tarkoitus määritellään kirjallisuudessa eri osapuolten henkilöllisyyden tai aitouden varmistamiseksi. Tietoturvan muiden osalueiden kannalta luotettava todennus on elintärkeää. Perusteita todennukselle on kolme: tieto, esine ja ominaisuus. Yksittäisistä todennusperusteista löytyy vakaviakin ongelmia. Kerberos-todennusprotokolla on niin sanottu luotettu kolmas osapuoli, joka hallinnoi käyttäjien ja palveluiden todennusta tietoverkossa. Kerberosin kautta tapahtuva todennus ja viestinnän turvallisuus perustuvat lipuiksi kutsuttuihin uniikkeihin viesteihin ja viestinnän salaamiseen. Muutamat protokollan rakenteisiin perustuvat hyökkäykset ja laitteistoihin kohdistuvat tietomurrot ovat tärkeitä ottaa huomioon.

Tutkimuksen myötä opinnäytetyössä tultiin siihen johtopäätökseen, että luottamuksellisuuden ja todennuksen oikea toteutus on tietoturvalle olennaista ja että Kerberos on haavoittuvuudestaan huolimatta pätevä työkalu todennukseen.

---

Asiasanat: Luottamuksellisuus, todennus, Kerberos, tietoturva.

## ABSTRACT

Tampereen ammattikorkeakoulu  
Tampere University of Applied Sciences  
Degree Programme in Business Information Systems  
Specialisation option of Network Services

PAKKALA, MARKUS: Principles of Confidentiality and Authentication, Operation of Kerberos Authentication Protocol

Bachelor's thesis 38 pages  
December 2010

---

This thesis was commissioned by Avantor Oy. The goal was to find out about confidentiality and authentication and report about their principles and challenges in practice. Also, the thesis was to present the Kerberos authentication protocol and study how it works and what possible threats there are to its reliable functioning. The purpose of the thesis was to produce an understandable presentation of the aforementioned topics for the benefit of its readers. Another objective of the thesis was to provide its readers with basic knowledge of the topics so they can find more information and study further on their own. The research method of this thesis was qualitative research. The information was gathered from professional literature.

The study showed that confidentiality as a data security principle means that only authorized users have the access to read and modify data. The motives for retaining confidentiality are twofold. The meaning of authentication was defined in the literature as to confirm the identities or the validity of the communicating parties. Reliable authentication is vital for other fields of data security to function properly. There are three methods to authenticate the user. The methods are using something that the user knows, something that the user holds and something that the user is. There are notable security hazards in only using exclusively any one of the three methods. Kerberos authentication protocol is a so-called trusted third party that governs the authentication of the users and the services in a network. Authentication and communication security via Kerberos are based on unique messages called tickets and encrypting the communication between the parties. There are few attacks against the protocol itself and against the hardware that the protocol runs on which should be taken into account by the administrator.

The findings indicate that the proper implementation of the two principles, confidentiality and authentication, is essential to data security. Also, it is clear that Kerberos is a valid tool for authentication in computer networks if its vulnerabilities are acknowledged.

---

Key words: Confidentiality, authentication, Kerberos, data security.

## ESIPUHE

Opiskeluvuosieni ja opinnäytetyöprosessini aikana lukuisat ihmiset ovat olleet apunani ja tahdon muistaa heitä muutamalla sanalla. Kiitän opinnäytetyöni oikoluvusta ja rakastavasta tuesta vaimoani Teijaa. Samoin kiitän tuesta vanhempiani Irmaa ja Teuvoa sekä isoveljeäni Markoa perheineen. Monet ystäväni Peräseinäjoelta, kiitos teille ystävyystänne ja yhteisistä hetkistä. Erityisterveiset ”kolhoositovereille” Vilelle ja Ilarille! Tampereen Evankelisille opiskelijoille ja ystäville sieltä lämmin kiitos mahdollisuudesta oppia ja kasvaa yhdessä. Kunnianosoitukseni ja kiitokseni myös Lasselle ja Annelle heidän panoksestaan Sley:n opiskelijatyölle.

Avanor Oy:lle ja Janne Ala-Siurulle kiitokset työharjoittelupaikasta ja opinnäytetyön tilaamisesta.

Tampereella joulukuussa 2010

Markus Pakkala

## SISÄLLYS

1 JOHDANTO.....	6
2 LUOTTAMUKSELLISUUS.....	8
2.1 Tietoturva käsitteenä.....	8
2.2 Luottamuksellisuus käsitteenä.....	8
2.3 Salaus tietoturvan työkaluna.....	9
2.3.1 Symmetrinen salaus.....	10
2.3.2 Epäsymmetrinen salaus.....	11
3 TODENNUS.....	13
3.1 Todennuksen tarkoitus.....	13
3.2 Luotettavan todennuksen perusteet.....	14
3.3 Haasteet.....	16
3.3.1 Jokapäiväinen ongelma.....	16
3.3.2 Tieto.....	17
3.3.3 Esine.....	17
3.3.4 Ominaisuus.....	18
3.3.5 Vastauksia haasteisiin.....	18
4 KERBEROS.....	20
4.1 Taustaa.....	20
4.2 Protokollan toiminta.....	21
4.2.1 Yleistä.....	21
4.2.2 Käyttäjä aloittaa protokollan.....	23
4.2.3 Todennuspalvelu prosessoi pyynnön.....	24
4.2.4 Käyttäjä vastaanottaa istuntoavaimen ja lipun.....	25
4.2.5 Lippupalvelu prosessoi pyynnön.....	26
4.2.6 Käyttäjä vastaanottaa uuden istuntoavaimen ja palvelulipun.....	27
4.2.7 Palvelin vastaanottaa viestin.....	27
4.3 Hyökkäykset.....	28
4.3.1 Protokollan tietoturvauhat.....	29
4.3.2 Hyökkäykset Kerberosta vastaan.....	32
5 POHDINTA.....	34
5.1 Lopputulokset.....	34
5.2 Johtopäätökset ja kehittämis ehdotukset.....	35
LÄHTEET.....	38

## 1 JOHDANTO

Tietoturvan näkökulma on ollut jatkuvasti läsnä opiskellessani tietoverkkopalveluiden suuntautumisvaihtoehdossa. Aihepiiristä kumpuaa monia mahdollisuuksia tarkastella tietoturvan vaatimuksia ja haasteita, joita ilmenee ihmisten käyttäessä tietojärjestelmiä, jotka parhaimmillaankin ovat epätäydellisiä. Aihe on kiinnostanut minua jo ennen saapumistani opiskelijaksi Tampereen ammattikorkeakouluun. Tietoturvan keskeisimpien käsitteiden esittely ja selvennys pyörivät mielessäni tutustuessani Kerberokseen. Kerberos-todennusprotokolla osoittautui alan standardiksi, mutta opiskeluissani en ollut siihen törmännyt. Havaitsin myös ettei Kerberosta ole juurikaan tuotu esiin alan opinnäytetöissä. Se oli puute, jonka halusin korjata. Näin opinnäytetyön aihe viimein nivoutui yhteen katsauksesta Kerberokseen ja sen taustalla vaikuttavien tietoturvan ydinalueiden esittelystä.

Työharjoittelupaikassani, Avanor Oy:ssä, ehdotukseni opinnäytetyön aiheeksi otettiin vastaan hyvin. Avanor on suomalainen internetmediayhtiö, jolla on kokemusta internetliiketoiminnasta jo vuodesta 1997. Yhtiön liiketoiminta keskittyy nopeiden ja helppokäyttöisten internetpalveluiden tuottamiseen. Avanor työllistää mm. IT-alan, markkinoinnin ja henkilöstöjohton opiskelijoita vuoden ympäri. Yhtiön kotipaikka on Oulu, työharjoittelujaksoni suoritin etätyönä.

Opinnäytetyössäni otan selvää kahdesta tietoturvan peruseriaatteesta, tiedon luottamuksellisuudesta ja luotettavasta todennuksesta, niiden perusteista ja merkityksestä käytännössä. Näiden lisäksi tarkastelen käytännössä hyväksi todettua järjestelmää käyttäjien todennukseen ja luottamuksellisuuden säilyttämiseen, Kerberos-todennusprotokollaa. Varsinkin Kerberosta käsitellessä suomenkielisen termin perässä sulkeissa on myös englanninkielinen termi hahmottamisen helpottamiseksi. Opinnäytetyöni edetessä kerroon muun muassa miten tiedon vuotamisesta voi joutua vaikeuksiin lain kanssa, mitkä kolme metodia ovat käytettävissä käyttäjän todentamiseen ja mitkä ovat Kerberosin heikkoja kohtia.

Luottamuksellisuus tarvitsee tuekseen lyhyen luonnehdinnan tietoturvan käsitteestä. Samoin luottamuksellisuus, todennus ja Kerberos yhdessä hyötyvät yleisimpien nykyaikaisten salaustekniikoiden suuntaa antavasta, suppeasta esittelystä. Tietoturvan yleisistä periaatteista ja salaustekniikoista on kirjoitettu paljon hyviä tietokirjoja, joten en opin-

näytetyössäni paneudu näihin aihealueisiin sen enempiä kuin mitä on käsillä olevan asian kannalta välttämätöntä.

Työni tarkoituksena on tuottaa mainituista aiheista selkeä esitys, joka on tavallisen IT-alan opiskelijan ja työntekijän ymmärrettävissä. Opinnäytetyöni tavoitteena on että luetuun tämän raportin lukijalla on perustavanlaatuinen käsitys tarkasteltavista teemoista ja valmiudet syventyä niitä tarkemmin käsitteleviin teoksiin.

Opinnäytetyöni on tutkimusotteeltaan laadullinen eli kvalitatiivinen tutkimus. Tutkimustyypiltään se on tapaustutkimus. Käsiteltäviä tapauksia ovat toisaalta abstraktimmat luottamuksellisuuden ja todennuksen kokonaisuudet, toisaalta konkreettisempi Kerberos ohjelmistotuotteena. Tietoa tapauksista kerättiin kirjallisista ja sähköisistä asiantuntija- ja ammattilaislähteistä. Tapauksia käsittelevää lähdekirjallisuutta hain ensisijaisesti paikallisten korkeakoulujen kirjastoista. Tietoturvan opinnoissa ja yleisen alan harrastuksen myötä minulla on jonkin verran omakohtaista tietoa ja näkemystä luottamuksellisuuden ja todennuksen käsitteistä ja käytännöistä. Tietoa kerättiin lähes koko kirjoitusprosessin ajan. Alkuvaiheessa hyödynnettiin laajempia perusteoksia leipätekstin muodostamiseksi. Kirjoittamisen edistyessä käytettiin aiheeseen erikoistunutta lähdekirjallisuutta. Tutkimusaiheestani ei ollut mielekästä kerätä omaa aineistoa, sillä tarvittava tieto oli jo saatavilla ja esimerkiksi haastatteluilla ei olisi tuotettu uutta tietoa aihealueesta. Uuden tiedon löytäminen näin tutkituista aiheista olisi ainakin vaatinut laajoja resursseja ja työmäärää, joka ei olisi järkevä ammattikorkeakoulun opinnäytetyön puitteissa.

Opinnäytetyöni analysointimenetelmä on sisällönanalyysi. Kirjallisuuteen pohjautuvassa tutkimuksessa sisällönanalyysi on sopiva työkalu, sillä sen tavoitteena on lähdemateriaalin analysointi systemaattisesti ja objektiivisesti. Sisällönanalyysin tarkoitus on luoda sanallinen ja selkeä kuvaus tutkittavasta ilmiöstä, mikä sopii hyvin yhteen opinnäytetyöni tarkoituksen kanssa. Tätä menetelmää käyttämällä lähtökohtani on selkeyden luominen aineistoon, että aiheesta voitaisiin tehdä luotettavia johtopäätöksiä.

## 2 LUOTTAMUKSELLISUUS

### 2.1 Tietoturva käsitteenä

Tietoturvasta puhuttaessa se monesti rinnastetaan läheisesti salauksen kanssa. Yleinen mielipide on, että tietoturvan tarkoitus on pitää tiedot salassa ja että salaustekniikat on kehitetty juuri tätä tarkoitusta varten. Todellisuudessa tietoturvassa on kyse suuremmista asioista. Tietoturvan tavoitteena on puolustaa tietojenkäsittelyä monilta erilaisilta riskeiltä ja suojata tietoja luvattomalta hallinnoinnilta. (Järvinen 2003, 29.)

Jotkut uhista ovat luonteeltaan teknisiä. Tieto voi esimerkiksi pirstaloitua käyttökeltomaksi kiintolevyllä tai kiintolevyn hajoaminen voi johtaa tietojen pysyvään menetykseen ja palveluiden keskeytymiseen ilman tarvittavia varotoimenpiteitä. Useimmiten riskit ovat kuitenkin seurausta ihmisten toiminnasta järjestelmässä. Ulkopuoliset hyökkääjät pyrkivät sisään tietojärjestelmiin voidakseen varastaa arkaluontoista tietoa tai tuhota sen sitä. Hyökkääjät voivat yrittää saada koko järjestelmän haltuunsa käyttääkseen sitä omaksi hyödykseen tai rampauttaakseen sen toiminnan kokonaan. Myös yrityksen omat työntekijät voivat kiireessä, huolimattaan tai osaamattaan tehdä virheitä, jotka vaarantavat verkon ja tietojen turvallisuuden. (Järvinen 2003, 29.)

Ulkopuolisen hyökkääjän tarvitsee harvoin turvautua salauksenmurtotekniikoihin yrittäessään kaapata luottamuksellisia tietoja. Yleensä järjestelmän salasanan urkkiminen muilla keinoin on paljon vaivattomampaa. Krakkerin (engl. cracker, luvattomasti tietojärjestelmään murtautuva henkilö) näkökulmasta parhaimmillaan tiedon hankkiminen vaatii vain puhelinoiton jollekin yrityksen työntekijälle tekeytyen toiseksi työntekijäksi, joka tarvitsee salasanaa johonkin toimenpiteeseen. (Järvinen 2003, 29.) Tämänkaltaisista todennuksen ongelmista kerrotaan lisää luvussa 3.4.1 Jokapäiväinen ongelma.

### 2.2 Luottamuksellisuus käsitteenä

Tietoturvan on perinteisesti nähty koostuvan kolmesta osa-alueesta, jotka tunnetaan lyhenteellä CIA. Lyhenne tulee englanninkielisistä termeistä confidentiality (luottamuksellisuus), integrity (eheys) ja availability (saatavuus). Nämä yleisperiaatteet koskevat



tietoa sen kaikissa muodoissa, oli tieto sitten tiedostoina (dokumentit, ohjelmat ja www-sivut), tiedonsiirtona (sähköposti, Internet-yhteys) tai kasana bittejä tietokoneen keskusmuistissa. (Järvinen 2002, 22.)

Tiedon luottamuksellisuus merkitsee tiedon lukemisen ja muokkaamisen sallimista vain niille henkilöille, joille on myönnetty siihen oikeudet. Muilta pääsy tietoihin evätään. Luottamuksellisuuden motiivina on usein organisaation tai käyttäjän oma etu, toisin sanoen arkaluontoisen tiedon leviämisen estäminen. Tällaista tietoa voivat olla esimerkiksi tuotekehittelytiedot tai tekeillä olevat kauppasopimukset, joiden paljastumisella voisi olla negatiivisia vaikutuksia. Joissain tapauksissa tiedon luottamuksellisuudesta määrää laki. Esimerkiksi pörssiyhtiöiden on pidettävä tiedotteensa salassa julkaisuhetkeen asti rangaistuksen uhalla, että sijoittajilla olisi yhtäläiset mahdollisuudet toimia. Henkilötietolaki velvoittaa rekisterinpitäjän suojelemaan keräämiänsä tietoja niin, etteivät ulkopuoliset saa niitä haltuunsa. (Paavilainen 1998, 8-9; Järvinen 2003, 29.) Henkilötietolain (1999) määrittelemä henkilörekisteri voi olla esimerkiksi yrityksen ylläpitämä yhteystiedoista koostuva asiakasrekisteri tai terveydenhuollon ylläpitämä hoitotiedoista koostuva potilasrekisteri (Tietosuojavaltuutetun toimisto 2010).

Salaus ja todennus liittyvät läheisesti luottamuksellisuuteen. Tiedon muokkaamiseen valtuutettujen käyttäjien tunnistamiseksi heidät täytyy ensin todentaa. Tiedon suojaamiseksi ulkopuolisilta tarvitaan salausta. Riittävän turvallinen salausten menetelmä takaa tiedon säästymisen paljastumiselta, jos joku salakuuntelee tiedonsiirtoa tai varastaa fyysisen laitteen, jolla tieto sijaitsee. (Järvinen 2003, 30.)

### 2.3 Salaus tietoturvan työkaluna

Vaikka salaus on vain marginaalinen osa tietoturvaa, on hyvä tuntea yleisimmät salausten menetelmät, joihin lähes kaikki tärkeän tiedon salaus ja todennuksen turvallisuus nykyisin perustuu. Nämä päämenetelmät ovat symmetrinen ja epäsymmetrinen salaus. Alaluvuissa käytetään muutamia termejä, jotka on syytä avata. Salaukseen liittyen avaimella tarkoitetaan tietoa, joka määrittelee salausalgoritmin lopputuloksen ja joka tarvitaan salausten prosessin läpiviemiseksi. Avain voidaan koneellisesti muodostaa vaikkapa salasanan muodossa olevasta helposti muistettavasta merkkijonosta. Selvätekillä tarkoitetaan al-

kuperäistä viestiä ennen sen salaamista. Salatekstillä vastavuoroisesti salattua tekstiä, jota ei pystytä tulkitsemaan ilman salauksen purkamista. (Järvinen 2003, 47–48.)

### 2.3.1 Symmetrinen salaus

Symmetrinen salaus (symmetric-key encryption) perustuu 1940 -luvulla matemaatikko Claude Shannonin esittämään ajatukseen hyvän salaimen toiminnasta. Oleellista tälle toiminnalle oli sotkeminen ja hajauttaminen. Sotkeminen tarkoittaa selvätekstin ja salatekstin välisen yhteyden sotkemista niin, ettei selvätekstin merkistä ole pääteltävissä vastaava salatekstin merkki. Hajauttaminen taas tarkoittaa selvätekstin vaikutuksen hajauttamista mahdollisimman laajalle niin, että pienet muutokset aiheuttavat suurta varianssia salatekstissä peittäen selvätekstin toistuvat kohdat ja säännönmukaisuudet. (Järvinen 2003, 77.) Symmetrisen salauksen nimitys johtuu sen toimintamallista. Symmetrinen salausalgoritmi käyttää tiedon salaamiseen ja salauksen purkamiseen samaa avainta.

Symmetriset salaimet voidaan jakaa vielä kahteen kategoriaan, lohko- ja jonosalaimiin. Lohkosalain käsittelee selvätekstiä lohkoina, jotka salataan aina samalla avaimella. Tavallisia lohkon kokoja ovat 64 ja 128 bittiä, tietokoneen kahden potensseihin perustuvasta tietojenkäsittelystä johtuen. Pitkät lohkot ovat turvallisempia, mutta ne vaativat enemmän muistia ja ovat ongelmallisia salattavan tietomäärän ollessa hyvin pieni. Esi-merkki tunnetusta lohkosalaimesta on AES (Advanced Encryption Standard, tunnettu myös nimellä Rijndael). (Järvinen 2003, 77–78, 96.)

Jonosalain taas käsittelee tietoa pienissä yksiköissä, bitti tai merkki kerrallaan, mutta avain vaihtuu joka salausoperaation jälkeen. Salaus tapahtuu yhdistämällä sillä hetkellä käytössä oleva avain ja selväteksti XOR -operaatiolla salatekstiksi. XOR on looginen operaatio, jonka ulostulo on yksi, jos jompikumpi kahdesta syötteestä on yksi. Vastavasti ulostulo on nolla, jos molemmat syötteet ovat nolla tai yksi. Taulukko tuloksista on seuraavalla sivulla (taulukko 1). Tämä operaatio yhdessä jatkuvasti vaihtuvan avaimen kanssa sotkee alkuperäisen selväkielisen tekstin tehokkaasti. Avainjono, josta uusia avaimia ammennetaan, muodostetaan algoritmilla, joka alustetaan ennalta valitulla avaimella. Tunnetuin jonosalain on RC4 (Rivest Cipher 4). (Järvinen 2003, 71, 77–78, 98.)

TAULUKKO 1. XOR-operaation tulokset

Syöte A	Syöte B	Ulostulo A XOR B
0	0	0
0	1	1
1	0	1
1	1	0

### 2.3.2 Epäsymmetrinen salaus

Ennen tietokoneaikaa kaikki salaustekniikat jouduttiin perustamaan lähettäjän ja vastaanottajan yhteiseen salausavaimen. Symmetrinen salaus jatkaa tätä perinnettä. Tietokoneiden yleistyessä tuli mahdolliseksi kehittää uudenlainen salaustekniikka, jossa salausavain voi olla julkinen kunhan purkuavain on salainen. Näiden kahden avaimen erillaisuudesta johtuen tätä tekniikkaa kutsutaan epäsymmetriseksi salaukseksi (public-key encryption). (Järvinen 2003, 131.)

Epäsymmetrinen salaustekniikka pohjautuu yksisuuntaisiin funktioihin, matemaattisiin toimituksiin, joiden tuloksesta ei voi päätellä alkuarvoja. Tarvitaan kuitenkin tapa, jolla funktio saadaan ajettua päinvastaiseen suuntaan. Tätä tapaa sanotaan salaluukuksi (trap-door). Salaluukun tunteva pystyy laskemaan funktion myös toisinpäin vaikka ulkopuoliselle se näyttää yksisuuntaiselta. Yhdysvaltalaiset tutkijat Whitfield Diffie ja Marty Hellman julkaisivat vuonna 1976 kehittämänsä tavan sopia avaimesta suojaamattoman yhteyden yli. Menetelmä tultiin tuntemaan Diffie-Hellman -avaintenvaihtoprotokollan nimellä. Syvemmin matemaattisiin perusteisiin menemättä Diffie-Hellman -protokolla käyttää hyväkseen alkuluvun moduloa, joka on helppo laskea yhteen suuntaan, mutta vielä nykyiselläkin tietämyksellä käänteinen laskutoimitus, diskreetti logaritmi, on liki mahdoton tehtävä. Diffien ja Hellmanin työn perusteella teoreetikot Ronald Rivest, Adi Shamir ja Leonard Adleman kehittivät vuonna 1978 epäsymmetrisistä salausmenetelmistä ehkä tunnetuimman, RSA-salausalgoritmin. (Järvinen 2003, 116–118, 131–132, 137–138; Stallings 2003, 268.)

Epäsymmetrisessä salauksessa käytetään kahta avainta, julkista (public key) ja yksityistä (private key). Ne ovat matemaattisesti yhteydessä toisiinsa, mutta sillä tavoin, että julkisesta avaimesta on erittäin vaikeaa johtaa yksityistä avainta. Julkisen avaimen voit siten huoletta antaa kaikkien tietoon, sillä salauksen pätevyys perustuu yksityisen avaimen pysymiseen salassa. Salattu viestintä toimii siten, että jokaisella henkilöllä on oma avainparinsa. Esimerkkihenkilö Bellalle lähetettävä tieto salataan Bellan julkisella avaimella. Julkisella avaimella salatun viestin voi purkaa ainoastaan sen kanssa liitoksissa olevalla yksityisellä avaimella. Jos Bella haluaa vastata turvallisesti viestin lähettäjälle, Akiille, hän salaa vastauksensa viestin Akin julkisella avaimella. Näin viestin voi purkaa vain Aki yksityisellä avaimellaan. Salattuaan viestin julkisella avaimella edes viestin lähettäjä ei saa sitä enää purettua, vaan salaus aukeaa ainoastaan yksityisellä avaimella. (Järvinen 2003, 132.) Epäsymmetristä salausta voisi verrata kirjeen jättämiseen lukittuun postilaatikkoon. Postinkantaja voi jättää laatikkoon kirjeen, mutta sen voi saada sieltä ulos vain postilaatikon omistaja avaimellaan.

Julkisen avaimen menetelmä poistaa ongelman, joka ilmenee yhteiseen salaisuuteen perustuvassa salauksessa. Salausavaimen vaihtamisesta tulee pelkkä ilmoitusasia, sillä yhteistä salaisuutta ei tarvita. Jos Aki haluaa vaihtaa avaimensa, hän luo uuden avainparin. Sitten hän tallettaa yksityisen avaimen ja tiedottaa uudesta julkisesta avaimesta sähköpostilla tai www-sivuillaan Bellalle ja muille ihmisille, joiden kanssa hän on tekemisissä. Avaimet toimivat itsenäisesti, joten Akin avainparin vaihto ei aiheuta muille toimenpiteitä omien avaimiensa suhteen. (Järvinen 2003, 133.)

### 3 TODENNUS

#### 3.1 Todennuksen tarkoitus

Todennus (authentication, suomeksi puhutaan myös autentikaatiosta) ei välttämättä ole kaikille terminä kovin selkeä, mutta kyseessä on arkipäiväinen ilmiö. Luultavasti tänäkin päivänä olet todentanut useita ihmisiä ja laitteita. Kun työkaveri tulee käytävällä vastaan, havainnoit jo parinkymmenen askeleen päästä tutun henkilön lähestymisen ja tervehdit. Pankkiautomaatilla käydessäsi toteat sen värin olevan tuttu oranssi, laitteen päällä lukee ”Otto” ja se sijaitsee tutussa paikassa, joten voit huoletta käyttää sitä. Jos puoliso soittaa, tunnistat hänet äänestä.

Todennuksen tavoitteena on varmistaa, että eri osapuolet todella ovat keitä he väittävät olevansa. Ihmisten kohdalla kyse on henkilöllisyydestä ja tietokoneiden sekä palveluiden tapauksessa niiden aitoudesta. Luotettavasta todennuksesta riippuvat enemmän ja vähemmän kaikki muut tietoturvan osa-alueet. Jos todennusprosessi on ylimalkainen ja täynnä aukkoja, ei tiedon luottamuksellisuudella, salauksella tai lähetysmenetelmällä ole mitään väliä. Todennuksen pettäessä ovi on apposen auki ja kuka tahansa voi paitsi lukea, myös muokata tietoja, jotka alun perin olivat tarkoitettuja vain valikoiduille ihmisille organisaation sisällä. (Järvinen 2003, 33–34.)

Toisaalta taas onnistuneen todennuksen jälkeen käyttäjän on päästävä sisään järjestelmään kuten on tarkoituskin. Se ei kuitenkaan tarkoita, että kuka tahansa tietojärjestelmän luvallinen käyttäjä saisi täydet valtuudet tehdä mitä haluaa. Huolto- ja muutostöimenpiteitä varten on ylläpitokäyttäjiä, joilla on tavallista käyttäjää laajemmat valtuudet toimia järjestelmässä. Tämä on todennuksen läheisen naapurin, valtuutuksen (authorization), alaa. Sikäli kun todennuksen lopputulos on joko sisään tai ei, valtuutus on hienojakoisempi jaotteluväline käyttäjien oikeuksien hallinnoimisessa. Valtuutus yhdessä todennuksen kanssa muodostaa suuren osan tietojärjestelmien tietoturvasta. Nämä kaksi konseptia yhdistyvät termissä pääsynvalvonta (access control). (Stamp 2006, 153–154.)

Todentaminen on siis varsin kriittinen tekijä tietoturvan alalla. Tilannetta ei varsinaisesti helpota se, että luotettava todentaminen on varsin vaativa tehtävä. Tavallisen arjen keskellä tapahtuvat todennustoimenpiteet ovat usein varmuudeltaan hataria. Näin oli myös

tietoteknisen kehityksen alkuvuosina, sillä tietokoneen käyttö oli hankalaa ja se vaati suorastaan erillisen koulutuksen. Toiseksi, tietokoneen käyttö oli mahdollista harvoille, yleensä tietojenkäsittelytieteen tutkijoille tai yritysmaailmassa alan erityisasiantuntijoille.

Neljännessä luvussa esiteltävä Kerberos-todennusprotokolla kehitettiin 1980-luvun lopussa todelliseen tarpeeseen. Keskustietokoneeseen pohjautuva malli oli murtumassa. Myös Massachusetts Institute of Technology, yhdysvaltalainen teknillinen yliopisto, havahtui tähän. Entisten keskustietokoneeseen kytkettyjen ”tyhmien päätteiden” sijasta alettiin käyttämään henkilökohtaisia tietokoneita (PC, Personal Computer). Opiskelijat olivat kuitenkin teknisen kehityksen tasalla ja käyttivät koneita verkkoliikenteen kaappaamiseen ja selväkielisenä verkossa välitettyjä salasanoja löydettyään tekeytyivät muiksi käyttäjiksi. Laaja yksittäisten tietokoneiden verkko ei ollut enää samalla tavoin ylläpitäjien hallinnassa ja hakkeroinnin myötä tilanne kävi sietämättömäksi. Luotiin työkalu ihmisten todentamiseen ilman salasanojen menettämisen vaaraa, Kerberos. (Garman 2003, 3–5.)

### 3.2 Luotettavan todennuksen perusteet

Nyt kun tiedetään mistä todennuksessa on kyse, voidaan siirtyä askel eteenpäin ja tarkastella todennuksen perusteita. Kun tavoitteena on eri ihmisten tai laitteiden tunnistaminen varmasti, voisi loogisesti päätellä, että todennuksen on pakko perustua johonkin sellaiseen tekijään, joka on vain yhdellä todennettavalla. Tekijät, joihin todennus perustuu, voidaan luokitella kolmeen eri kategoriaan (Järvinen 2003, 35–36). Todennuksen perusteet ovat esiteltyinä seuraavassa kuvassa (kuvio 1).



KUVIO 1. Todennuksen perusteet

Ensimmäinen kategorია on tieto. Tarkemmin määriteltynä salainen tieto, joka on vain todennettavan ja todentajan tiedossa. Tietoteknisissä yhteyksissä yleisin todennustapa on salasana ja tähän periaatteeseen myös Kerberosin toiminta perustuu. Yleisesti tietojärjestelmään ensin tunnistaudutaan antamalla käyttäjänimi, joka usein voi käytännössä katsoen olla yleistä tietoa. Siksi todennus tapahtuu tunnukseen liitettyllä salasanalla. Salasanojen käyttö on suosittua, koska se on helppoa ja halpaa. Niiden käyttäminen poistaa kalliit investointitarpeet avaimiin tai tunnistuskortteihin ja niiden lukkoihin ja lukulaitteisiin. (Järvinen 2003, 35.) Nämä lienevät tärkeimmät syyt siihen miksi salasanoja käytetään kaikkialla, myös Kerberosin todennusprosesseissa.

Toinen mahdollisuus on hallussa oleva esine. Tässäkin tapauksessa on kyse menetelmästä, jota käytetään hyvin yleisesti. Lukkoon sopiva avain tai lukulaitteen hyväksymäkortti todentaa sisään pyrkivän henkilön. Edellisessä kappaleessa mainittujen panostusten lisäksi haasteena on tehdä todentavasta esineestä mahdollisimman kopiointi- ja väärennyskelvoton. (Järvinen 2003, 35.) Jos lukon saa auki hiuspinnillä, ovi on tarpeeton.

Kolmantena todennustapana on yksilöllinen ominaisuus. Kyseessä on todennusmetodi, joka on meihin ihmisiin sisäänkirjoitettuna. Jokapäiväisessä kanssakäymisessä todennuksemme perustuu muiden ihmisten ulkonäköön, olemukseen ja ääneen. Tällaista todennusta teemme jatkuvasti sen kummempia ajattelematta, sillä aivomme ovat siihen harjaantuneet. (Järvinen 2003, 36.) Voi kuitenkin olla, että uusien vaatteiden tai flunssaisen äänen takia emme heti tunnista tuttujamme. Ihmisen luontevinkin todennusmetodi pettää joskus.

### 3.3 Haasteet

#### 3.3.1 Jokapäiväinen ongelma

Arkinen esimerkki valottaa todennuksien ongelmia. Useimmat ostotapahtumat kauppoissa tapahtuvat nykyisin pankki- tai luottokortilla. Uuden mallin mukaisia kortinlukijoita, joissa todennus tapahtuu PIN -koodilla, on kuitenkin vasta harvassa. Useimmiten kuitaus tapahtuu vieläkin perinteisellä ”rallikuskinimmarilla”, sillä yleensä mihinkään tarkempaan ei ole aikaa. Jos ostos on tarpeeksi iso, myyjä pyytää nähdäkseen henkilöllisyystodistuksen tai kysyy henkilötunnuksen loppuosaa. Jo lähi-Siwan kassalla törmäämme todennusongelmiin. (Järvinen 2003, 38.)

Tunnettu fakta on, että kukaan ei näytä omalta itseltään ajokortin tai passin kuvassa. Ajan kuluessa kuvaushetkestä tilanne vain kärjistyy. Harva lentokenttävirkillijakaan kuitenkaan pysäyttää matkustajan, joka on eri näköinen kuin kuva papereissa. Samoin henkilötunnuksen loppuosa on todennusmetodina yhtä luotettava kuin ihmisten puheet ylipäättänsä, jos sitä ei tarkisteta henkilöllisyystodistuksesta. Henkilötunnus sinänsä ei myöskään ole valtakunnan salaisuus, vaan se ajelehtii lukuisissa hakemuksissa ja julkisissakin asiapapereissa ihmisen yksilöivänä tunnisteena. Toki henkilötunnuksen tallentamista on rajoitettu tietoturvasyistä, mutta viimeistään kaupan kassalla salaisuus paljastuu. (Järvinen 2003, 38.) Facebook-salasanaansa ei monikaan kailottaisi samalla tavalla lähikaupassa.



### 3.3.2 Tieto

Luotettavan todennuksen perusteissa käytiin läpi kolme mahdollisuutta todennukseen: tieto, esine ja ominaisuus. Jos tarkastelemme ensimmäisenä tietoa, joka yleensä tarkoittaa salasanaa, joudumme myöntämään ettei kyseessä ole mikään pomminvarma konsepti. Salasana on digitaalista informaatiota palvelimilla ja tietokannoissa ja sellaisena sitä pystyy kopioimaan vaikka loputtomasti. Vaarana on myöskin, että salasana voi paljastua vahingossa tai se kaapataan käyttäjältä hänen ymmärtämättään. Tämä on mahdollista vaikkapa tietokoneelle pesiytyneen kirjoitusta tallentavan haittaohjelman kautta. (Järvinen 2003, 35.)

Myös tiedon urkkiminen sosiaalisen manipuloinnin (social engineering) avulla on hyvin tehokasta. Kalliista teknisistä turvajärjestelyistä ei ole apua, jos hakkeri soittaa yrityksen työntekijälle tekeytyen ylläpito-osaston työntekijäksi ja pyytää käyttäjätunnusta ja salasanaa ”ongelman korjaamista” varten. Tunnettu entinen hakkeri ja nykyinen tietoturvakonsultti Kevin Mitnick totesikin tietomurroissa sosiaalisen manipuloinnin puhelimesta niin tehokkaaksi keinoksi että hänen todella harvoin tarvitsi yrittää teknisesti murtautua yritysten tietojärjestelmiin. Kaiken lisäksi on vaara, että käyttäjä voi unohtaa salasanansa, käyttää heikkoa salasanaa tai kirjoittaa sen paperilapulle kaikkien nähtäville. (Schneier 2000, 266–267.)

### 3.3.3 Esine

Todentava esine on nimensä mukainen. Sillä todennetaan, mutta se ei ota kantaa siihen kuka sitä käyttää. Avain tai avainkortti ei yleensä ole millään tavalla sidottu haltijaansa. Molemmista voidaan sitä paitsi tehdä vähällä vaivalla kopioita. Aina ei tarvitse nähdä niinkään paljon vaivaa, sillä avaimen voi aina varastaa tai haltija voi luovuttaa sen vapaaehtoisesti hämărăhommiin. Todennuksen kannalta olisikin ensiarvoisen tärkeää saada avain sidottua käyttäjänsä ja suunnitella siitä mahdollisimman vaikeasti kopioitava. (Järvinen 2003, 35.)

Todentavan esineen riskeihin on luettava myös, kuten salasanankin tapauksessa, käyttäjän laiskuus. Jos yrityksen tietokoneelle kirjaudutaan laittamalla avainkortti lukijaan, on

hyvin suuri todennäköisyys, että ainakin joku käyttäjä jättää avainkorttinsa lukijaan pysyvästi. (Schneier 2000, 146.)

#### 3.3.4 Ominaisuus

Kuten luotettavan todennuksen perusteissa todettiin, yksilölliseen ominaisuuteen perustuva todennus on ihmisille luonteva ja arkinen tapa tunnistaa asioita ja ihmisiä. On kuitenkin riski, että tämä todennus voi pettää ja syitä on useita. Emme näe tuttua kiireessä, tuttumme näyttää erilaiselta tai luulemme vaikkapa jotakuta vierasta tutuksi ja tervehdimme epähuomiossa häntä. Ihmismieli on aikojen saatossa sopeutunut tunnistamaan varsinkin ihmisiä äänen, ulkonäön ja elekielen perusteella. Ääni tai ulkonäkö voidaan digitoida tietokoneelle ja verrata niitä sitten todennettavan henkilön ominaisuuksiin. Tätä kutsutaan biometriseksi tunnistukseksi. Jos ihminen ei kuitenkaan ole aukoton tunnistuksissaan, miten tietokone voisi olla? (Järvinen 2003, 36.) Tietokoneelta puuttuu harkinta- ja sopeutumiskyky sen suhteen miten tunnistettava henkilö on piirteiltään muuttunut ajan kuluessa.

Ongelmia on myös käänteiseen suuntaan tapahtuvassa todentamisessa. Verkkopankin palvelimella ei ole kasvoja, ääntä tai muutenkaan aistein havaittavaa tunnusmerkkiä, jota vertailla sen kanssa millainen luotetun palvelimen pitäisi olla. Huolestuttavampaa on se, että myös käsillä olevien laitteiden tunnistaminen on hankalaa. Jos joku vaihtaisi työ-kannettavasi toiseen samanlaiseen yön aikana ja olisi kopioinut alkuperäisen koneen kiintolevyltä kaikki tiedot uuteen, huomaisitko sitä seuraavana aamuna? Huijaus voisi jatkua pitkäänkin käyttäjän huomaamatta. Vaikeinta on kuitenkin ohjelmien kanssa. On mahdotonta sanoa mikä kasa bittejä ohjelman muotoon kasattuna on aito ja alkuperäinen hyötyohjelma ja mikä on hakkeroitu versio, jossa on takaportti arkaluontoisten tietojen nuuskimista varten. (Järvinen 2003, 36.)

#### 3.3.5 Vastauksia haasteisiin

Näiden edellä olevien esimerkkien ei ole tarkoitus ahdistaa ja luoda hallitsematonta turvallisuuden tunnetta, vaan toimia muistutuksena siitä, että mihinkään yksittäiseen to-

dennusperusteeseen ei ole syytä luottaa sokeasti. Ratkaisuna yksittäisten metodien turvattomuudelle korkeampaa turvatasoa vaativissa sovelluksissa käytetään käyttäjän todentamiseen kahta tai jopa kaikkia kolmea menetelmää (Järvinen 2003, 38).

Pankkikortti ja kännykän SIM-kortti ovat hyviä esimerkkejä tällaisesta turvallisuusajattelusta. Pankkikortti ja SIM-kortti toimivat todentavina esineinä, mutta niiden käyttöön pankkiautomaatilla ja kännykässä tarvitaan todentava tieto, PIN-koodi. Sama pätee verkkopankin käyttämiseen, jossa todennus perustuu pankin lähettämään listaan kertakäyttöisiä tunnuslukuja (esine) ja seuraavaan käyttämättömään numeroon (tieto). (Järvinen 2003, 38.)

Tärkeiden esineiden aitoutta pyritään turvaamaan teknisillä järjestelyillä. Käytännössä kaikissa maailman setelirahoissa on vesileima tai turvalanka tai molemmat. Luottokorteissa ja ohjelmistolevyissä käytetään vaikeasti väärennettäviä hologrammeja. Varsinaisesti kyseessä ei ole todentaminen yksilölliseen ominaisuuteen perustuen, vaan siitä että esineen valmistaja todistaa omistavansa jotain, joka voi olla vain aidolla valmistajalla. (Järvinen 2003, 38.)

## 4 KERBEROS

### 4.1 Taustaa

Kreikkalaisessa mytologiassa Kerberos oli kolmipäiseksi kuvattu valtava vahtikoira Haadeen eli manalan portilla. Tämän hirvityksen tehtävänä oli pitää vainajat sisällä ja elävät ihmiset ulkopuolella. Tässä tehtävässä Kerberos ei aina täysin onnistunut, vaan Herakles viimeisenä urotyönään paini vahtikoiran sopuisaksi ja toi tämän hetkeksi mukanaan tämänpuoleiseen maailmaan. Myös monet muut tarujen sankarit kävivät manalassa ja tulivat takaisin. Kerberos saattoi olla hurja peto, mutta tuonpuoleisen pääsynvalvonnassa oli huomattavia ongelmia. Kerberosen moderni vastine on kuitenkin maineeltaan ja toimintavarmuudeltaan myyttistä esi-isäänsä paljon parempi.

Massachusetts Institute of Technology (MIT) käynnisti vuonna 1983 Project Athena -nimellä tunnetun projektin, jonka tavoitteena oli tutkia uusien tietoteknisten mahdollisuuksien tuomista kiinteäksi osaksi opetusta. Vuonna 1991 päättyneen projektin lopputulos oli Athena, MIT:n kampuksenlaajuinen tietokoneverkko. (MIT 2010.) Tämän projektin sivutuotteina syntyi myös uutta teknologiaa talon sisällä, yhtenä näistä Kerberos-todennusprotokolla pääsynvalvontaa varten. Ensimmäiset kolme versiota olivat ainoastaan MIT:n sisäisessä käytössä. Kun neljäs versio julkistettiin 1980-luvun lopussa, siitä tuli nopeasti suosittu. Sen sisältämien muutamien turvallisuusaukkojen takia pian tämän jälkeen julkaistiin Kerberosen viides versio. Kerberos on saavuttanut käytössä eri sovelluksissa ja alustoilla niin suuren suosion, että siitä on tullut käytännössä alan standardi. (Todorov 2007, 387.) MIT:n versio Kerberosesta on vapaa ohjelmisto eli sen kopioiminen, käyttäminen, muokkaaminen ja levittäminen on sallittua. (About - Frequently asked... 2010.)

Kerberos perustuu suurelta osin yhdysvaltalaisen tutkijoiden Roger Needhamin ja Michael Schroederin vuonna 1978 julkaisemaan tutkimukseen. Siinä Needham ja Schroeder (1978, 993–999) hahmottelivat protokollan turvalliseen todennukseen tietokoneverkossa. Tämä protokolla tultiin tuntemaan nimellä Needham-Schroeder -protokolla ja sen periaatteisiin Kerberosenkin kehitys tukeutui. Needham-Schroeder -protokollasta siirtyi Kerberoseseen monet peruskonseptit, kuten todennuspalvelin, luotettu kolmas osa-

puoli, joka toimii käyttäjän ja kohderesurssin välissä, samoin kuin käyttäjän itsetodennus purkamalla todennuspalvelimen lähettämä salattu viesti. Needham ja Schroeder määrittelivät tutkimuksessaan useita oletuksia, joihin pohjaten he suunnittelivat protokollansa. Yksi näistä oletuksista oli hyökkääjän mahdollisuus salakuunnella ja kaapata verkon liikennettä ja injektoida siihen omia viestejään. Tätä tekijät kuvailivat äärinäkökulmana, vaikka nykyisin se on muodostunut rutiiniolettamukseksi turvallisen verkkoprotokollan suunnittelussa. (Garman 2003, 24–25.) Myös tämän näkökulman huomioon ottaminen käy ilmi Kerberosin toiminnassa, jota kuvaillaan seuraavassa luvussa.

## 4.2 Protokollan toiminta

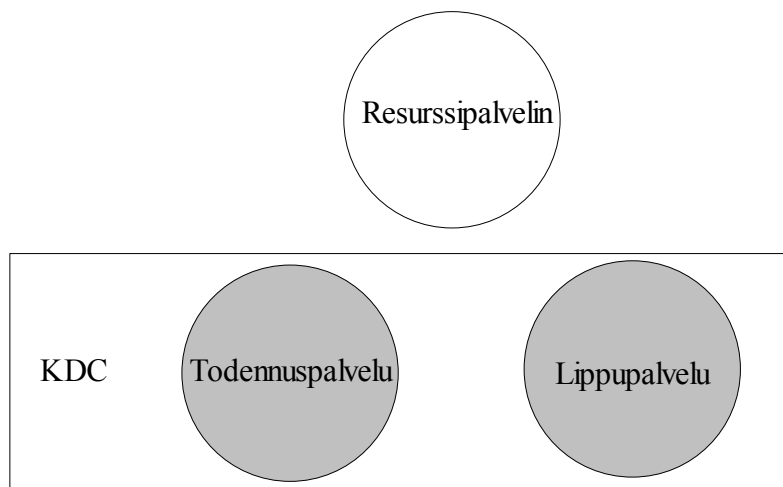
### 4.2.1 Yleistä

Kerberos on todennusprotokolla, joka perustuu luotetun kolmannen osapuolen malliin. Tämä tarkoittaa sitä, että todennus toimii keskitetysti Kerberos-palvelimen kautta. Verkossa olevat tietokoneet ja palvelut luottavat tähän palvelimeen todentajana keskinäisessä kanssakäymisessään ja kaikki todennuspyynnöt kulkevat sen kautta. (Garman 2003, 6.)

Kerberos -palvelu toimii TCP/IP -verkon portinvartijana sallien pääsyn resursseihin, joita se valvoo. Kerberosin toiminnan periaatteisiin kuuluu kertakirjautuminen (single sign-on). Käyttäjän tarvitsee kirjautua sisään vain kerran käyttääkseen Kerberosin valvomia resursseja. Protokollan käynnistymisessä tapahtuneen todennuksen jälkeen Kerberos todentaa käyttäjän muille osapuolille lipuiksi (tickets) kutsuttuja viestejä käyttämällä kirjautumisen voimassaoloaikana. Kerberos käyttää viestintänsä suojaamisessa symmetristä salausta. Alun perin käytetty salausalgoritmi oli 56-bittinen DES, mutta luotettavammat algoritmit ovat osittain ottaneet sen paikan. Käyttäjätodennus perustuu salassa pidettäviin käyttäjä- ja palvelukohtaisiin avaimiin. Kerberosella on tiedossaan kaikkien käyttäjien, palveluiden ja palvelimien avaimet, joten sen kautta osapuolet voivat varmentua toistensa henkilöllisyydestä. Tätä kutsutaan keskinäiseksi todennukseksi (mutual authentication). (Schneier 1996, 566; Garman 2003, 6.)

Kerberos muodostaa todennusvaiheessa viestejä, jotka on salattu todennusta pyytävän osapuolen avaimella eikä niitä siten voi periaatteessa avata kuin henkilö, jolle viesti on tarkoitettu. Tarvetta lähettää salasanaa verkon yli ei siis ole. Todennus tapahtuu käyttäjän omalla koneella purkamalla Kerberosin lähettämän viestin salaus ja vastaamalla siihen. Varsinaista kommunikointia varten Kerberos muodostaa osapuolille istuntokohtaisen avaimen, jolla liikenne salataan. Istuntoavain (session key) on kertakäyttöinen, yhtä istuntoa varten, ja se tuhotaan istunnon päätteeksi. (Schneier 1996, 566.)

Kerberosin kolme ”päättä” ovat todennuspalvelu (Authentication Service), lippupalvelu (Ticket Granting Service) ja resurssit, jotka ovat Kerberosin pääsynvalvonnan kohteena (kuvio 2). Todennus- ja lippupalvelusta käytetään yhteisnimitystä avainjakelukeskus (Key Distribution Center) ja yleisesti lyhennettä KDC. Fyysisesti KDC:n palvelut yleensä sijaitsevat pienemmissä verkoissa samalla palvelimella. (Todorov 2003, 388.)



KUVIO 2. Kerberosin kolme ”päättä”

Pääpiirteissään todentamisprosessi menee seuraavasti: käyttäjä (principal) esittelee itsensä ja kertoo todennuspalvelulle haluavansa asioida lippupalvelun kanssa ja vastaanottaa siltä lipun (Ticket Granting Ticket). Käyttäjä esittää lippunsa lippupalvelulle ja pyytää pääsyä resursseihin. Jos käyttäjällä on oikeus käyttää pyytämäänsä resurssia ja kaikki on kunnossa, lippupalvelu antaa käyttäjälle palvelulipun (Server Ticket). Käyttäjä todentaa palvelulipulla itsensä palvelimelle ja käyttää resurssia. (Schneier 1996, 567.)

Seuraavissa luvuissa esitellään todennuksen kulkua askeleittain yksinkertaisen mallin mukaan, jossa käyttävät ovat saman Kerberos-palvelimen alaisuudessa. Seuraavassa taulukossa on protokollan viestien sisällön kuvaamisessa käytetyt merkit (taulukko 2).

TAULUKKO 2. Merkkien selitys (Schneier 1996, 567, muokattu)

Merkki	Selitys
k	Käyttäjä
p	Palvelin
o	Käyttäjän verkko-osoite
v	Lipun voimassaolon alku- ja loppuaika
l	Aikaleima
va	Lisäävain istuntoa varten (valinnainen)
ett	Esitodennustieto
tp	Todennuspalvelu
lp	Lippupalvelu
$A_x$	Käyttäjän $x$ avain (salasana)
$A_{x,y}$	Istuntoavain $x$ :lle ja $y$ :lle
$\{z\}_{A_x}$	Viesti $z$ salattuna $x$ :n avaimella
$L_{x,y}$	Lippu $x$ :lle $y$ :n käyttöä varten
$T_{x,y}$	Todennusviesti $x$ :ltä $y$ :lle

#### 4.2.2 Käyttäjä aloittaa protokollan

Oletetaan tilanne, jossa käyttäjä nimeltä Keijo haluaa päästä asioimaan tiedostopalvelimelle, jonka verkkonimi on Pentti. Käyttäjä Keijo ja palvelin Pentti kuuluvat verkossa saman Kerberos-palvelimen alueelle (realm). Toisin sanoen molemmat luottavat tähän Kerberos-palvelimeen ja ovat rekisteröineet salasansansa sille. Myös Kerberosta käytävillä sovelluksilla ja palvelimilla täytyy olla salasana todennusta varten. Keijo aloittaa prosessin ja lähettää todennuspalvelulle selväkielisen viestin, jossa hän ilmoittaa oman identiteettinsä ja halutun yhteyden kohteen. Viestin sisältö yksinkertaistetusti on:

$k, [ett], tp$

Tässä vaiheessa kohteena on lippupalvelu, joka myöntää lippuja käyttäjille resurssien käyttöön. Tämä viesti tunnetaan nimellä todennuspalvelupyyntö (Authentication Service request) tai lyhenteellä AS\_REQ. (Schneier 1996, 569; Graff 2001, 48; Garman 2003, 31; Todorov 2003, 395.)

Jos Kerberos-palvelin vaatii esitodennusta (pre-authentication), käyttäjän on ennen todennuspalvelupyyntöä todennettava itsensä lähettämällä todennuspalvelupyynnön sisältä esitodennustieto. Yleisimmin käytetty esitodennustieto on tyypiltään PA-ENC-TIMESTAMP, joka sisältää aikaleiman salattuna käyttäjän avaimella. Tällä pyritään estämään tarpeettomien todennuspalvelupyyntöjen tehtailu hyökkäystarkoituksessa. Jos esitodennusta vaaditaan Kerberos-palvelimen puolelta, mutta käyttäjä aloittaa todennuspalvelupyynnöllä ilman esitodennustietoa, Kerberos-palvelin vastaa KRB\_ERROR -viestillä eikä käsittele todennuspalvelupyyntöä. (Garman 2003, 43; Todorov 2003, 398.)

Vaikka tässä esityksessä viitataan hänen tekemisiinsä, todellisuudessa Keijon ei tarvitse itse aktiivisesti lähettää Kerberokseen liittyviä viestejä, vaan niiden muodostaminen ja lähettäminen tapahtuu automaattisesti. Samoin Kerberokselta tulevien viestien käsittely tapahtuu automaattisesti. Keijon todelliseksi osuudeksi jää salasanana syöttäminen käyttöliittymään.

#### 4.2.3 Todennuspalvelu prosessoi pyynnön

Todennuspalvelu ottaa vastaan Keijon pyynnön. Todennuspalvelu aloittaa sen käsittelyn luomalla istuntoavaimen, jolla yhteys Keijon ja palvelimen välillä salataan. Todennuspalvelu salaa istuntoavaimen Keijon avaimella, ettei kukaan muu pääsisi siihen käsiksi. (Schneier 1996, 569; Garman 2003, 32.)

Seuraavaksi todennuspalvelu luo lipun, jolla käyttäjä todentaa itsensä lippupalvelulle. Lipun sisältö on tämä:

$$L_{k, lp} = lp, \{k, o, v, A_{k, lp}\}A_{lp}$$



Voimassaolon alku- ja loppuaika muodostavat turvallisuustekijän nimeltä tuoreus. Näiden kahden ajan perusteella voidaan varmistua siitä, että esitetty lippu ei ole hyökkäys, jossa ajetaan palvelimelle viesti, joka on kopioitu verkkoliikenteestä aikaisemmin (replay attack). Näiden kahden arvon myötä lippu vanhenee säädetyn ajan päästä ja muuttuu käyttökelvottomaksi. Mitä lyhyemmäksi voimassaoloaika säädetään, sitä vaikeammaksi ulkopuolinen väärinkäyttö muodostuu. Samalla kuitenkin ruuhka verkossa ja KDC:llä kasvaa, kun lippuja joudutaan uusimaan useammin. (Schneier 1996, 568; Graff 2001, 50; Garman 2003, 33.)

Istuntoavain on tärkeä väline, jonka jakaminen todennettujen osapuolten kesken on protokollan tavoite. Istuntoavaimella salatuin viestein osapuolet voivat kommunikoida ulkopuolisten katseilta suojassa. (Graff 2001, 50; Garman 2003, 33.)

Lippu salataan lippupalvelun avaimella. Todennuspalvelu yhdistää nämä viestiksi, jonka sisältö on:

$$\{A_{k, lp}\}A_{k, lp} \{L_{k, lp}\}A_{lp}$$

Tämän jälkeen todennuspalvelu lähettää tämän todennuspalveluvastauksen (Authentication Service reply) eli AS\_REP -viestin Keijolle. (Schneier 1996, 568–569; Garman 2003, 33; Todorov 2003, 395.)

#### 4.2.4 Käyttäjä vastaanottaa istuntoavaimen ja lipun

Keijo vastaanottaa todennuspalvelun lähettämät salatut viestit ja purkaa istuntoavaimen sisältävän viestin salauksen omalla avaimellaan. Näin tekemällä Keijo todentaa itsensä. Vaikka jokin ulkopuolinen hyökkääjä olisikin kaapannut tämän viestin, siitä ei ole mitään hyötyä ilman Keijon salasanaa. Keijo laittaa istuntoavaimen ja salatun lipun talteen. Näitä hän voi käyttää niin kauan kuin lippu on voimassa. (Schneier 1996, 569; Garman 2003, 33.)

Nyt Keijo lähettää erityisen todennusviestin (authenticator) yhdessä lipun kanssa Kerberosin lippupalvelulle. Todennusviestillä Keijo näyttää toteen lippupalvelulle olevansa todella Keijo, sillä todennusviesti on salattu istuntoavaimella. Aikaleima on turvameka-

nismi, jonka ansiosta hyökkääjä ei voi käyttää verkosta kaapattua todennusviestiä lipun kanssa myöhemmin. Todennusviesti on kertakäyttöinen ja muodoltaan:

$$T_{k,p} = \{k, l, va\}_{A_{k,lp}}$$

Viesti lippupalvelulle kokonaisuudessaan:

$$\{T_{k,p}\}_{A_{k,lp}}, \{L_{k,lp}\}_{A_{lp}}$$

Viesti on nimeltään lippupalvelupyynnö (Ticket Granting Service request) eli TGS\_REQ. Seuraavaksi Keijo lähettää tämän viestin lippupalvelulle. (Schneier 1996, 568–569; Garman 2003, 33; Todorov 2003, 399.)

#### 4.2.5 Lippupalvelu prosessoi pyynnön

Käyttäjän on hankittava oma lippu jokaista resurssia varten, jota hän haluaa käyttää. Lippupalvelun tehtävänä on myöntää käyttäjille lippuja resurssien käyttämistä varten. Lippupalvelu ottaa vastaan Keijon viestin, joka koostuu todennusviestistä ja lipusta. Lippupalvelu purkaa lipun, jonka todennuspalvelu oli salannut lippupalvelun avaimella. Lipun sisällä ollutta istuntoavainta käyttäen lippupalvelu pystyy avaamaan Keijon todennusviestin. Sitten se vertailee todennusviestin ja lipun tietoja, käyttäjän verkko-osoitetta osoitteeseen, josta viesti tuli ja aikaleimaa nykyhetkeen. Jos tiedot ovat kunnossa pyynnön käsittely jatkuu. (Schneier 1996, 569; Garman 2003, 33.)

Aikaleimoja tarkastellessa Kerberos olettaa, että sen kanssa kommunikoivien koneiden kellot ovat synkronoidut vähintään muutaman minuutin tarkkuudella. Lippupalvelu kohtelee palvelupyynnöä hyökkäysyrityksenä, jos viestissä oleva kellonaika on liian kaukana menneisyydessä tai tulevaisuudessa. Lippupalvelu pitää kirjaa myös voimassaolevista todennusviesteistä, joten palvelupyynnöt kertaalleen esitetyllä lipulla ja aikaleimalla voidaan ohittaa. (Schneier 1996, 569–570.)

Lippupalvelu luo uuden istuntoavaimen Keijon ja Pentti-palvelimen välistä kommunikointia varten ja salaa sen Keijon ja lippupalvelun käyttämällä istuntoavaimella. Lippupalvelu luo myös palvelulipun, jolla Keijo voi todentaa itsensä Pentti-palvelimelle. Palvelulippu on muodoltaan samanlainen edellisen lipun kanssa, mutta eroaa siitä vähän si-

sällöltään. Kohteena on nyt tavoiteltu palvelin, uusi istuntoavain on mukana ja lippu on salattu palvelimen avaimella:

$$L_{k,p} = p, \{k, o, v, A_{k,p}\}A_p$$

Näistä lippupalvelu koostaa viestin:

$$\{A_{k,p}\}A_{k,lp}, \{L_{k,p}\}A_p$$

Lippupalvelu lähettää tämän lippupalveluvastauksen (Ticket Granting Service reply) eli TGS\_REP -viestin Keijolle. (Schneier 1996, 568–569; Garman 2003, 33; Todorov 2003, 399.)

#### 4.2.6 Käyttäjä vastaanottaa uuden istuntoavaimen ja palvelulipun

Otettuaan vastaan palvelulipun ja purettuaan viestistä uuden istuntoavaimen Keijo on valmis ottamaan yhteyttä palvelimeen ja todentamaan itsensä sille. Hän luo palvelimelle samankaltaisen viestin kuin lippupalvelulle. Ensin Keijo luo uuden todennusviestin, joka on muodoltaan ja sisällöltään vastaava kuin edellinen ja salaa sen hänen ja palvelimen välisellä istuntoavaimella. Yhdessä uusi todennusviesti ja palvelulippu muodostavat sovelluspyynnön (Application request) eli AP\_REQ -viestin:

$$\{T_{k,p}\}A_{k,p}, \{L_{k,p}\}A_p$$

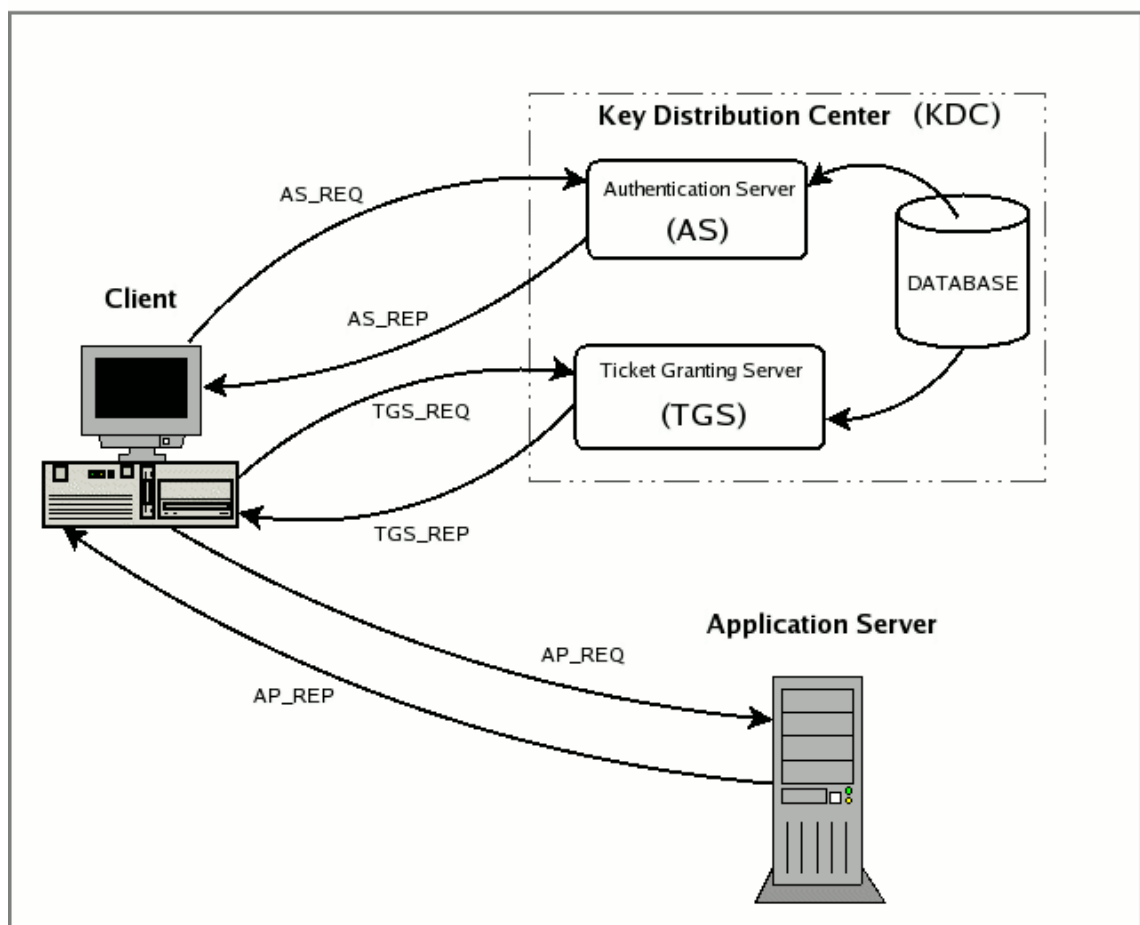
Tämän viestin Keijo lähettää nyt Pentti-palvelimelle. (Schneier 1996, 568–570; Garman 2003, 33; Todorov 2003, 401.)

#### 4.2.7 Palvelin vastaanottaa viestin

Palvelin vastaanottaa Keijon viestin, purkaa ensin avaimellaan lipun ja purkaa siitä saamallaan istuntoavaimella todennusviestin. Kuten lippupalvelu edellä, se myös tarkistaa käyttäjän verkko-osoitteen ja aikaleiman. Jos kaikki on kunnossa, palvelin tietää, että Kerberosin mukaan Keijona esiintyvä käyttäjä todella on Keijo. Jos palvelimen täytyy myös viestiä takaisin käyttäjälle, kuten tässä esimerkissämme, Pentti-palvelin lähettää Keijolle viestin, jossa on aikaleima salattuna istuntoavaimella. Vastausviesti on sovel-

lusvastaus (Application reply) eli AP\_REP. Näin myös Keijo voi varmistua, että hänen viestinsä vastaanotti oikea palvelin, sillä se pystyi purkamaan lipun ja todennusviestin. Tästä eteenpäin Keijo ja Pentti voivat kommunikoida käyttäen yhteistä istuntoavaintaan. (Schneier 1996, 570; Todorov 2003, 401.)

Seuraavassa piirroksessa on yhteenveto Kerberos-pohjaisen todennuksen vaiheista (kuvio 3). Yhteenvetona lippujen liikkeistä mainittakoon, että käyttäjä (kuvassa Client) saa AS\_REP -viestissä lipun, TGS\_REP -viestissä palvelulipun ja AP\_REQ -viestissä esittää palvelulipun palvelimelle (kuvassa Application Server).



KUVIO 3. Kerberos-todennuksen kulku (Kerberos Protocol Tutorial 2010)

### 4.3 Hyökkäykset

Teoriassa Kerberos on erittäin varma tapa todentaa käyttäjiä. Koska teoria ja käytäntö kuitenkin ovat kaksi eri asiaa, on hyvä olla tietoinen muutamista käytännön ongelmista

Kerberos-toteutuksissa. Kerberos ei pitkästä kehityshistoriastaan huolimatta ole täydellinen, mutta ohjelmakoodin avoimen luonteen vuoksi ongelmat ovat olleet helpompia löytää suljettuihin ohjelmistoihin verrattuna. On muistettava, että Kerberos on ainoastaan todennuspalvelu, eikä se voi estää esimerkiksi virheellisesti toimivista palvelinohjelmistoista, inhimillisistä virheistä tai huonoista salasanoista johtuvia vaaratilanteita. (Garman 2003, 100.)

#### 4.3.1 Protokollan tietoturvaohauat

Jo Kerberosen neljäs versio jakoi alun perin lippuja kaikille, jotka niitä pyysivät. Todennus tapahtuu sitten purkamalla salaus tästä lipusta oikealla avaimella. Koko järjestelmän toiminta riippuu tästä. Hyökkääjä voi siis pyytää KDC-palvelimelta lippua kohteen käyttäjänimellä. Vaikka ilman salasanaa ei ole mahdollisuutta suoraan murtaa salausta, sen purkamiseen voi käyttää sanakirjahyökkäystä (dictionary attack). Sanakirjahyökkäyksessä syötetään lista yleisesti käytettyjä salasanoja murto-ohjelmaan, joka yrittää purkaa viestin kokeilemalla kaikkia listalla olevia salasanoja. On myös mahdollista käyttää ohjelmaa, joka yrittää arvata salasanaa ns. raan voiman menetelmällä (brute-force attack), jolloin murto-ohjelma kokeilee kaikkia mahdollisia merkkijohdistelmia salasanan löytämiseksi. (Garman 2003, 104.)

Näiden menetelmien käyttö on mahdollista, sillä on yleisessä tiedossa, että lipun sisällä on tiettyä selväkielistä tekstiä, kuten merkkijono tgt. Kerberosen lippupalvelun käyttäjänimi taas on aina krbtgt, joka voidaan löytää viestistä onnistuneen murren jälkeen. Itse murto-ohjelman kirjoittaminen on varsin yksinkertaista ohjelmoijalle, sillä prosessi on yksinkertainen. Hyökkääjän työtä helpottaa se, että näitä hyökkäyksiä voi ajaa kaikessa rauhassa omalla koneellaan ilman että joutuisi olemaan koko ajan yhteydessä Kerberosseen. Hyökkääjä voi aluksi tilailla nipun lippuja KDC-palvelimelta ja ryhtyä sitten murtaamaan niiden salausta. (Garman 2003, 104.)

Salausjärjestelmissä on siirrytty kohti pidempiä salausavaimia näiden hyökkäysten mitätöimiseksi. Prosessoreiden ja pilvilaskentatekniikan kehityksen myötä kuitenkin käytettävissä oleva laskentateho lisääntyy vuosi vuodelta dramaattisesti. Pilvilaskennalla tarkoitetaan suurta laskentatehoa vaativien tehtävien hajauttamista verkon yli suurelle jou-

kolle tietokoneita. Tämänkaltainen kehitys johtaa siihen, että jo lähitulevaisuudessa salaukset, joiden murtamista nyt pidetään utopistisena voivat olla murrettavissa tarpeeksi nopeasti salasanojen hyödyntämiseksi. Keksimisensä aikaan varsin turvallinen salausalgoritmi 56-bittinen DES, jota Kerberosin alunperin käytti, on nykyisin turvallisuusris-ki. Raa'an voiman menetelmää käyttäen se oli ensimmäistä kertaa mahdollista murtaa alle vuorokaudessa jo vuonna 1999. (Garman 2003, 104–105.)

Kerberoksen viidennessä versiossa tätä uhkaa on torjuttu sellaisilla ominaisuuksilla, kuten vaihtoehtoisten salausalgoritmien tuella ja esitodennuksella. On kuitenkin huomatta-va, että uudistukset eivät täysin poista edellä kuvailtujen hyökkäysten riskiä. Jos verkos-sa on useampia eri Kerberos -toteutuksia palvelimien ja päätteiden kesken, vaikkapa MIT-toteutuksen mukaiset KDC-palvelimet ja Windows-päätteet, niin kommunikoinnis-sa voidaan käyttää vain yhteistä salausta. MIT -toteutus Kerberoksesta tukee kolminker-taista DES-salausta, mutta Windows -päätteet eivät, joten viestiliikenteessä on käytettä-vä normaalia DES-salausta. Esitodennuksen ollessa käytössä hyökkääjä ei voi enää suo-raan pyytää lippuja KDC-palvelimelta, mutta hän voi salakuunnella verkon liikennettä ja siepata käyttäjille kulkevia lippuja murtamista varten. Tämän lisäksi monet toteutuk-set eivät vakioasetuksilla pakota käyttäjää esitodentamaan itseään. (Garman 2003, 106.)

Toistohyökkäyksessä (replay attack) hyökkääjä salakuuntelee verkon liikennettä ja sieppaa käyttäjältä palvelimelle menossa olevan lipun ja lähettää sen myöhemmin pal-velimelle tarkoituksenaan imitoida käyttäjää. Tässä tapauksessa hyökkääjän ei tarvitse murtaa salasanaa verkon resurssien väärinkäyttämiseksi. Tällaista hyökkäystä vastaan Kerberoksessa on useampia sisäänrakennettuja ominaisuuksia, jotka vaikeuttavat toisto-hyökkäyksen käyttöä. Ensimmäinen näistä on lippujen osoitekenttä. Lippuihin merki-tään käyttäjän tietokoneen verkko-osoite, jota KDC-palvelin vertaa lipun lähettäjän osoitteeseen. Tämä estää toistohyökkäyksen toisesta osoitteesta. On kuitenkin huomatta-va, että hyökkääjän on mahdollista vaihtaa tietokoneensa osoitetta käyttäjän tietokonetta vastaavaksi, jos osoite on tiedossa. Toiseksi, lipun osoitekentän voi jättää myös tyhjäk-si, jolloin lippu kelpaa vaikka se tulisi mistä verkko-osoitteesta. (Garman 2003, 106–107.)

Toinen ominaisuus toistohyökkäyksen estämiseksi on todennusviestin aikaleima, jota KDC-palvelin vertaa nykyhetkeen. Jos aikaleima ja KDC-palvelimen kellonaika ovat

viiden minuutin sisällä, lippu kelpaa. Tarkoituksena on mahdollistaa lievä heitto kellonajassa verkon tietokoneiden kesken. Viisi minuuttia on kuitenkin enemmän kuin tarpeeksi hyökkäyksen tekemiseksi varsinkin jos hyökkääjä on ohjelmallisesti automatisoinut lippujen keruun ja lähetyksen. (Garman 2003, 108.)

Viimeisenä teknisenä keinona toistohyökkäystä vastaan Kerberos säilyttää tietoja käytetyistä todennusviesteistä välimuistissa. Toistovälimuistia (replay cache) pitää jokainen Kerberosin alainen palvelu erikseen. Kun palvelu saa todennusviestin, se vertaa sitä toistovälimuistiinsa ja jos samaa todennusviestiä on jo käytetty, se hylkää saapuneen palvelupyynnön. Muussa tapauksessa se hyväksyy pyynnön ja lisää todennusviestin tiedot toistovälimuistiin. (Garman 2003, 108.) Tämä aiheuttaa sen, että hyökkääjän on paitsi kaapattava lippu todennusviesteineen myös estää sen kulkeminen KDC-palvelimelle ennen omaa hyökkäysyritystään.

Kolmas uhka Kerberosta kohtaan protokollana on hyökkäys, joka tunnetaan nimellä epärehellinen välittäjä (man-in-the-middle attack). Kyseessä on hyökkäys, joka on riski kaikille protokollille, jotka pyrkivät todentamaan yhteyden eri päissä olevat toimijat. Epärehellinen välittäjä on toistohyökkäyksen kaltainen aktiivinen hyökkäys, joka vaatii onnistuakseen hyökkääjältä mahdollisuuden vakoilla hyökkäyksen kohteena olevan verkon liikennettä ja lähettää omia viestejä. Tällaista viestien syöttämistä kutsutaan spoofaukseksi (engl. spoof; huijaus, väärennös). Hyökkäyksen tarkoituksena on imitoida palvelinta ja saattaa käyttäjä uskomaan olemaan normaalissa yhteydessä palvelimeen, jonka kanssa hän haluaa asioida. Sen jälkeen kun hyökkääjä on ottanut istunnon haltuunsa hän voi halutessaan päästää käyttäjän ja oikean palvelimen välillä kulkevan liikenteen läpi sellaisenaan tai lisätä, poistaa ja muokata kulkevia viestejä. Hyökkäyksen nimi juontuu tästä hyökkääjän asemasta käyttäjän ja palvelimen välillä. (Garman 2003, 108.)

Uhkaa pienentää se, että Kerberosin toimintamalli on epärehellinen välittäjä -hyökkäyksiä torjuva. Palvelimeen yhdistävän käyttäjän lisäksi Kerberos todentaa myös palvelimen identiteetin keskinäisen todennuksen periaatteen mukaan. Koska Kerberos pitää hallussaan kaikkien osapuolten salausavaimia ja salaa muodostamansa istuntoavaimet niillä, hyökkääjä ei pääse istuntoavaimeen käsiksi ilman oikeaa salasanaa. Keskinäisen todennuksen myötä käyttäjä voi varmistua palvelun aitoudesta, sillä palvelu todentaa itsensä purkamalla KDC-palvelimen muodostaman lipun, ottamalla siitä istuntoavaimen

ja salaamalla istuntoavaimella vastauksensa käyttäjälle. Jos palvelu ei onnistu vastaamaan oikein, yhteys katkaistaan. (Garman 2003, 108–109.)

#### 4.3.2 Hyökkäykset Kerberosta vastaan

Pääkäyttäjätason oikeuksien (root-level privileges) vaarantuminen KDC-palvelimella antaa hyökkääjälle esteettömän pääsyn koko todennusjärjestelmään. Kerberosin tietokanta on kylläkin salattu pääavaimella, mutta pääavainta säilytetään KDC:n kiintolevyllä ettei KDC-palvelun käynnistyessä olisi tarvetta syöttää tätä avainta. Lisäksi kaikki Kerberos-toteutukset tarjoavat pääkäyttäjälle vikasietoisen pääsyn Kerberos-tietokantaan. Käytännössä koko järjestelmä on vaarassa, jos hyökkääjä löytää keinon hyödyntää pääkäyttäjaoikeuksia KDC:llä. (Garman 2003, 101.)

Jos hyökkääjä onnistuu saamaan tietoonsa Kerberosin ylläpitokäyttäjän salasanan, hänellä on siinäkin tapauksessa täydet oikeudet toimia Kerberosin tietokannassa. Useimmat KDC-toteutukset sallivat ylläpitäjän ottavan etäyhteydellä vedoksen tietokannan sisällöstä varmuuskopiointia varten ja tätä toimintoa voidaan käyttää väärin salasanan vaarantuessa. Hyökkääjä voi halutessaan myös poistaa ja lisätä käyttäjiä tietokantaan mielensä mukaan. Ylläpitokäyttäjien määrää tulisikin rajoittaa mahdollisimman paljon ja huolehtia salasanoiden koskevien menettelytapojen olevan turvallisella tasolla. Salasanoiden tulisi olla riittävän monimutkaisia ja niitä tulisi vaihtaa säännöllisesti. (Garman 2003, 101.)

Hyökkääjän saadessa pääkäyttäjätason oikeudet palvelimella kaikki Kerberosta todennukseen käyttävät palvelut ovat vaarassa. Hyökkääjä pääsee purkamaan salattua liikennettä käyttäjien ja palvelimella toimivien palveluiden välillä, mikä on ilmeinen tietoturvariski. Jotkut palvelut, kuten verkkotiedostojärjestelmä AFS, jakavat samat Kerberos-käyttäjätiedot kaikkien palvelua pyörittävien palvelimien kesken. Näin hyökkääjä voi hallita kaikkea kyseisen palvelun ja käyttäjien välistä Kerberosin salaamaa liikennettä. (Garman 2003, 101.)

Pääkäyttäjätason oikeuksien haltuunotto käyttäjän tietokoneella taas antaa hyökkääjälle pääsyn voimassaoleviin lippuihin tietokoneen muistissa. Liput tosin ovat voimassa vain rajoitetun ajan, joten kyseessä ei ole yhtä suuri riski kuin käyttäjän salasanan paljastues-



sa. Tällöin hyökkääjä voisi imitoida luvallista käyttäjää salasanan vaihtamiseen asti, mikä huonosti harkitulla salasanapolitiikalla voi kestää kauankin. (Garman 2003, 101.)

Näistä riskeistä tulisi oppia se, että Kerberosen käyttöönotto ei tee verkosta läpitunke-  
matonta hyökkääjille. Vaikka todennus onkin paremmissa käsissä, ei ole syytä laimin-  
lyödä verkon yleistä turvallisuutta. Minkä tahansa tietokoneen haavoittuvuus voi johtaa  
vakaviin seurauksiin myös Kerberosen luotettavan toiminnan kannalta.

## 5 POHDINTA

### 5.1 Lopputulokset

Opinnäytetyössäni käytiin läpi muutamia tietoturvan perusperiaatteita, luottamuksellisuus ja todennus, ja näiden periaatteiden käytännön sovellus, Kerberos-protokolla. Seuraavaksi kertaan tuloksia, joihin päädyin aineiston pohjalta.

Luottamuksellisuus on yksi kolmesta tietoturvan lähtökohdista yhdessä tiedon eheyden ja saatavuuden kanssa. Luottamuksellisuudella tarkoitetaan tiedon suojaamista ulkopuolisten lukemiselta ja muokkaamiselta ja näiden toimintojen sallimista käyttäjille, joilla on niihin oikeus. Yleisin motiivi tiedon luottamuksellisuuden säilyttämiseen on arkaluontoisten tietojen suojeleminen ulkopuolisilta. Myös laki saattaa asettaa vaatimuksia tiedon suojelemiselle. Käyttäjien luotettava todentaminen ja erilaiset salaustekniikat ovat tärkeitä apuvälineitä luottamuksellisuuden säilyttämisessä.

Todennuksen tarkoitus on varmistaa eri osapuolten henkilöllisyys, jos kyse on ihmisistä, tai aitous, jos kyse on tietokoneista tai palveluista. Muut tietoturvan osa-alueet ovat eri tavoin riippuvaisia luotettavasta todennuksesta. Todennus voi perustua johonkin seuraavista kolmesta tekijästä: tieto, esine ja ominaisuus. Todentava tieto voi olla esimerkiksi salasana, joka on helppo ja halpa käyttää todennukseen, mutta on riskialtis urkkimiselle tai unohtamiselle. Yleisin esine todennuskäytössä on avain. Avaimen kaltainen fyysinen esine kuitenkin on usein helposti kopioitavissa eikä se ole sidottu käyttäjäänsä. Yksilölliseen ominaisuuteen perustuva todennus käyttää hyväkseen esimerkiksi ihmisen ääntä tai ulkonäköä tunnistukseen. Ihmisen yksilölliset ominaisuudet kuitenkin muuttuvat ajan kuluessa ja laitteilla tai ohjelmilla ei sellaisia olekaan. Vaadittaessa varmempaa todennusta onkin järkevää käyttää yhdistelmää joistakin kahdesta tai kaikista kolmesta tekijästä.

Kerberos on MIT:ssä kehitetty todennusprotokolla, jonka toiminta perustuu luotettuun kolmanteen osapuoleen, tässä tapauksessa Kerberos-palvelimeen, joka hallinnoi käyttäjien ja palveluiden todennusta ja turvallista kommunikointia. Kerberos käyttää todennuksessa hyväkseen käyttäjän avaimella salattuja viestejä, joiden onnistunut purkaminen todentaa käyttäjän. Lipuiksi kutsutuin viestein Kerberos ja käyttäjä neuvottelevat

pääsystä käyttämään haluttua resurssia. Kerberos myös muodostaa istuntokohtaisen avaimen Kerberos-asiakkaiden välisen viestinnän salaamiseen.

Lyhyesti selitettynä käyttäjän todentaminen ja pääsy käyttämään palvelua, esimerkiksi tiedostopalvelinta, tapahtuu kolmessa vaiheessa. Käyttäjä esittelee itsensä ja kertoo todennuspalvelulle haluavansa asioida lippupalvelun kanssa ja vastaanottaa lipun. Käyttäjä esittää lippunsa lippupalvelulle ja pyytää pääsyä resursseihin. Jos käyttäjällä on oikeus käyttää pyytämäänsä resurssia, lippupalvelu antaa käyttäjälle palvelulipun. Käyttäjä todentaa palvelulipulla itsensä palvelimelle ja käyttää resurssia. Kerberosin myytiseen kolmipäiseen hirviöön viittaava nimi on tullut näistä kolmesta kuvitellusta ”päästä”, todennuspalvelu, lippupalvelu ja resurssipalvelin.

Kerberoksella on turvallisuusriskinsä, jotka on tiedostettava. Ensinnäkin Kerberosin todennus on lopulta vain niin luotettava, kuin käytetty salausalgoritmi ja -avain, sillä käyttäjän salasana voi olla murrettavissa sanakirjahyökkäyksellä tai raa’an voiman menetelmällä. Toinen uhka on toistohyökkäys, jossa hyökkääjä kaappaa käyttäjältä lähteneen lipun ja imitoi sen avulla käyttäjää. Tätä torjutaan lipun osoitekentällä, todennusviestin aikaleimalla ja toistovälimuistilla. Kolmas huomattavista protokollan tietoturva-uhista on epärehellinen välittäjä -hyökkäys. Siinä hyökkääjä asettuu hallinnoimaan liikennettä käyttäjän ja imitoi palvelinta, johon käyttäjä haluaa suojatun yhteyden. Keskinäisen todennuksen periaate, jossa molemmat osapuolet todennetaan Kerberosin kautta hillitsee tätä ongelmaa. Näiden lisäksi murtautumiset Kerberos-palveluille elintärkeille tietokoneille ovat riski todennuksen luotettavalle toiminnalle.

## 5.2 Johtopäätökset ja kehittämisehdotukset

Tutkimuksen perusteella voi sanoa, että luottamuksellisuuden ja todennuksen perusteiden sisäistäminen on alan toimijoille elintärkeää. Jo opiskeluvaiheessa olisi syytä kiinnittää huomiota näihin turvallisen tietojenkäsittelyn rakennuspalikoihin. Todennusperusteihin soisin perehdyttävän alan opinnoissa. Tutkittaessa Kerberos osoittautui syystäkin alansa standardiksi. Kerberosessa otetaan huomioon monet perinteiset uhkatekijät ja oikein hoidettuna se kestää haavoittuvuushyökkäykset. MIT:n toteutuksen lähdekoodin vapaa levitys on kantanut hedelmää ohjelmiston laajana levinneisyytenä ja siitä eteen-

päin kehitettyinä toteutuksina. Koulutukseni puolesta Kerberokseen tutustuttiin Käyttöjärjestelmien palvelut -opintojaksolla, mutta ikävä kyllä en ollut silloin paikalla.

Mielestäni esittelemieni aiheiden käsittely onnistui hyvin käytettävissä olleeseen aikaan nähden. Harmittelen sitä, ettei aika riittänyt tarkastella syvemmin joitain luottamuksellisuuteen ja todennukseen liittyviä kysymyksiä, kuten luottamuksen merkitystä tietojenkäsittelyssä. Voiko koskaan olla täysin varma siitä kuka linjan toisessa päässä on? Tarvitseeko täydelliseen varmuuteen edes pyrkiä? Nämä kysymykset eivät välttämättä olisi mahtuneet aiheen rajaukseen, mutta olisivat valottaneet tietojenkäsittelyn inhimillistä puolta. Ehkä joku muu voisi ottaa ajatuksesta kiinni ja viedä sitä eteenpäin. Kerberosta olisi ollut hyvä tutkia myös käytännön työn kautta, esimerkiksi koulun omassa opetusverkossa. Yhdessä työharjoittelun kanssa aika käytännön puoleen ei kuitenkaan olisi riittänyt, sillä mikään harvoin menee niin kuin on tarkoitus.

Materiaalia käsitellyistä aihealueista olisi löytynyt enemmänkin. Lähteet ovat osin iäkkäitä, mutta tietoturvan peruseriaatteet eivät onneksi ole juurikaan muuttuneet, vaikka kehitys IT-alalla on ollut hurjaa. Kerberoksen osalta yhdyn Jason Garmanin kirjansa esipuheessa lausumiin sanoihin turhautumisesta Kerberoksen käytännöllisen dokumentaation puutteesta. Hänen lukuisat muistiinpanonsa kehittyivät lopulta hienoksi tietopakettiksi, jota lämpimästi suosittelen Kerberoksen kanssa työskenteleville. Jos parempi yleisesitys Kerberoksesta on sittemmin julkaistu, otan tiedon siitä vastaan ilomielin.

Suurin osa teoksista oli englanninkielisiä, kuten saattaa olettaakin, mutta niihin tutustuminen oli varsin mieluista tehtävää. Johdannossa jo mainitsinkin ja tekstiä lukiessa huomaa, että useissa kohdissa suomenkielisen termin perässä on sulkeissa alkuperäinen englanninkielinen termi. Tähän ratkaisuun päädyin selkeyden takia. Monista, etenkin Kerberokseen liittyvistä, teknisistä termeistä ei ollut tarjolla vakiintunutta suomennosta. Tästä syystä päädyin tekemään useiden termien osalta suomennokset itse raportin kielen yhtenäistämiseksi. Jätin kuitenkin englanninkielisen termin kääntämieni ja monien vakiintuneidenkin käsitteiden perään näkyville, että myöhemmin luettaessa kansainvälistä alan kirjallisuutta lukijan olisi mahdollista tunnistaa keskeiset termit ilman suurempaa kummastelua.

Opinnäytetyöni tarkoituksena oli tuottaa luottamuksellisuudesta, todennuksesta ja Kerberoksesta selkeä esitys, joka on tavallisen IT-alan opiskelijan ja työntekijän ymmärret-

tävissä. Tavoitteena oli että luettuaan tämän raportin lukijalla on perustavanlaatuinen käsitys käsitellyistä teemoista ja valmiudet syventyä niitä tarkemmin käsitteleviin teoksiin. Esittelin työtäni alalla työskenteleville tuttaville ja saamani palautteen perusteella päädyin siihen tulokseen, että tarkoitus ja tavoite täyttyivät hyvin. Rakenne ja kieliasu ovat selkeitä ja olen niihin itsekin hyvin tyytyväinen. Voin luovuttaa työni tilaajalle hyvillä mielin.

On täysin varmaa, että oma tietämykseni opinnäytetyöni aihepiiristä lisääntyi. Uskon olevani tämän prosessin jälkeen valmiimpi arvioimaan todennuskäytäntöjä ja ymmärtämään olemassa olevia ratkaisuja paremmin. Tultuani tutuksi Kerberoksen kanssa, voin nyt perehtyä sen toimintaan syvemmin teknisellä tasolla ja käytännön kautta tuotanto-verkoissa.

## LÄHTEET

### Kirjalliset lähteet

Garman, J. 2003. Kerberos: The Definitive Guide. Sebastopol, USA: O'Reilly Media, Inc.

Graff, J. 2001. Cryptography and E-Commerce. New York, USA: John Wiley & Sons, Inc.

Henkilötietolaki 22.4.1999/523

Järvinen, P. 2002. Tietoturva & yksityisyys. Jyväskylä: Docendo Finland Oy.

Järvinen, P. 2003. Salausmenetelmät. Jyväskylä: Docendo Finland Oy

Needham, R., Scroeder, M. 1978. Using Encryption for Authentication in Large Networks of Computers. Communications of the ACM 21 (12), 993–999.

Paavilainen, J. 1998. Tietoturva. Jyväskylä: Suomen Atk-kustannus Oy.

Schneier, B. 1996. Applied Cryptography. Protocols, Algorithms, and Source Code in C. 2. painos. New York, USA: John Wiley & Sons, Inc.

Schneier, B. 2000. Secrets & Lies. Digital Security in a Networked World. New York, USA: John Wiley & Sons, Inc.

Stallings, W. 2003. Cryptography and Network Security. Principles and practices. 3. painos. Upper Saddle River, USA: Pearson Education, Inc.

Stamp, M. 2006. Information Security. Principles and practice. New York, USA: John Wiley & Sons, Inc.

Todorov, D. 2007. Mechanics of User Identification and Authentication. Fundamentals of Identity Management. New York, USA: Auerbach Publications

### Sähköiset lähteet

MIT. 2010. Athena history (1983 - present) from A to Z. Luettu 7.9.2010. <http://web.mit.edu/acs/athena.html>

The MIT Kerberos Consortium. 2010. About - Frequently asked questions about the MIT Kerberos Consortium. Luettu 20.10.2010. <http://www.kerberos.org/about/FAQ.html>

The MIT Kerberos Consortium. 2010. Kerberos Protocol Tutorial. Luettu 4.11.2010. <http://www.kerberos.org/software/tutorial.html>

Tietosuojavaltuutetun toimisto. 2010. Tietoa rekisterinpitäjälle. Luettu 11.10.2010. <http://www.tietosuoja.fi/1698.htm#kohta5>