VAASAN AMMATTIKORKEAKOULU
VASA YRKESHÖGSKOLA
UNIVERSITY OF APPLIED SCIENCES

Markus Koivisto

Tiedon salaus ja tietoliikenteen suojaus

Liiketalous ja matkailu
2012

VAASAN AMMATTIKORKEAKOULU
Tietojenkäsittelyn koulutusohjelma

TIIVISTELMÄ

Tekijä	Markus Koivisto
Opinnäytetyön nimi	Tiedon salaus ja tietoliikenteen suojaus
Vuosi	2012
Kieli	Suomi
Sivumäärä	57
Ohjaaja	Antti Mäkitalo

Työssäni selvitän kannettavan tietokoneen, älypuhelimien ja tablettitietokoneiden tietoturvaan liittyviä asioita. Vastaan myös kysymykseen, kuinka suojata tietokone yleisessä verkossa. Työssä käydään myös läpi erilaisia salaustekniikoita ja algoritmejä, joilla saadaan turvattua tietokoneella oleva tieto. Käsittelen myös langattomia verkkoja niiden suuren käytön ja kasvun takia.

Salauksesta käsitellään niin symmetrinen salaus kuin epäsymmetrinen salaus. Symmetrisessä salausosiossa käydään läpi DES- ja AES-salaukset. Epäsymmetrisessä osiossa käydään läpi RSA- ja Diffie-Hellman-salaukset. Tutkimus on aineistolähtöinen ja aineistona käytin kahdeksaa kirjaa, mukaan lukien Ciscon verkkoakatemian ensimmäisen ja toisen vuosikurssin kirjoja.

Työn teoriaosassa keskitytään salausalgoritmeihin, kovalevyn ohjelmalliseen salaukseen sekä varmuuskopiointiin. Käytännön osassa keskitytään langattoman verkon tietoturvaan, älypuhelimien ja tablettitietokoneiden tietoturvaan, etätyöskentelyyn VPN:n avulla sekä esitellään Prey-ohjelmisto, jolla kadonneen tietokoneen voi löytää.

Avainsanat Tietoturva, Tietoliikenne, Salaus, WLAN, VPN

VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES
Tietojenkäsittelyn koulutusohjelma

ABSTRACT

Author	Markus Koivisto
Title	Data Encryption and Telecommunication Security
Year	2012
Language	Finnish
Pages	57
Name of Supervisor	Antti Mäkitalo

In this thesis information security for laptops, smartphones and tablet computers was studied, Also, the answer to the question how to protect your computer in open networks was examined. The thesis looked into different cryptographic techniques and algorithms, which can secure data on one's computer. Still, wireless networks were examined due to their high use and accelerated growth.

For encryption symmetric and asymmetric encryption were considered. In symmetric encryption DES and AES encryptions were examined. For asymmetric encryption RSA and Diffie-Hellman were looked onto. The thesis is literature based and for material eight books, including the Cisco Network Academy year one and year two study books were used.

The theoretical part of the study focused on the encryption algorithms, hard drive encryption as well as backup. The practical section focused on wireless network security as well as, smartphone and tablet PC security. Also, working from home using a VPN and demonstrating program called Prey that users can use to find their lost computers, was studied.

Keywords Data Security, Telecommunication, Encryption, WLAN, VPN

Sisällys

TIIVISTELMÄ
ABSTRACT
Käsiteluettelo

1. Johdanto 9

2. Tutkimuksen tavoitteet 10

3. Symmetrinen salaus 11

3.1. DES 11

3.2. AES 13

4. Epäsymmetrinen salaus 15

4.1. RSA 15

4.2. Diffie-Hellman 16

5. Kovalevyn salaus 18

6. Kannettavan työaseman suojaus langattomassa verkossa 21

6.1. IEEE 802.11, a, b, g ja n 21

6.2. SSID 22

6.3. MAC-osoitteet 23

6.4. WEP 24

6.5. WPA 25

6.6. WPA2 26

6.7. RADIUS 27

6.8. Bluetooth 28

7. Etätyöskentely kannettavalla (VPN) 30

7.1. IPSec 31

7.2. L2TP 31

7.3. PPTP 32

7.4. SSL VPN 32

8. Älypuhelimien ja tablettikoneiden tietoturva 34

8.1. iOS-käyttöjärjestelmä 35

8.2. iPad 35

8.3. iOS 5.1-tietoturva 36

8.4. F-Secure 40

9. Tietojen ja ohjelmistojen varmuuskopiointi 41

9.1. RAID 0,1 ja 5 41

9.2. Cobian-varmuuskopiointi 44

10. Varastetun kannettavan löytäminen etäohjelmiston avulla 48

11. Johtopäätökset 52

12. LÄHTEET 54

Käsiteluettelo

AES (Advanced Encryption Standard) lohkosalausjärjestelmä, jota käytetään tietotekniikassa.

Algoritmi on tarkasti määritelty vaihesarja, jota seuraamalla voidaan ratkaista tietty ongelma.

CRYPTOcard on niin sanottu haaste-vaste-laskin. Käyttäjä kirjautuu ensin sovellukseen käyttäjätunnuksellaan ja staattisella salasanallaan, minkä jälkeen tunnistusjärjestelmä esittää ruudulla haasteen. Käyttäjä näppäilee haasteen tunnistuslaitteeseensa, joka laskee vasteen ja näyttää sen lcd-näytössään. Käyttäjä kopioi laitteen laskeman vasteen työasemalleen, ja tunnistusjärjestelmä voi todeta käyttäjän hallussa olevan tunnukseensa sidotun laitteen.

Epäsymmetrinen salaus sisältää kaksi avainta, joista toinen on julkinen avain ja toinen salainen avain. Julkisella avaimella salattu viesti voidaan purkaa salaisella avaimella ja päinvastoin.

IEEE 802.11 (Institute of Electrical and Electronics Engineers) on standardi langattomille WLAN-verkoille.

iOS (aiemmin iPhone OS) on Applen kehittämä käyttöjärjestelmä, joka on käytössä Applen iPhone, iPod touch, iPod Nano ja iPad-laitteissa.

IPSec (IP Security Architecture) on joukko TCP/IP-perheeseen kuuluvia tietoliikenneprotokollia internet-yhteyksien turvaamiseen. Nämä protokollat tarjoavat salauksen, osapuolten todennuksen ja tiedon eheyden varmistamisen.

L2TP on Microsoftin ja Ciscon kehittämä VPN-tunnelointiprotokolla. L2TP on yhdistelmä L2F:stä ja PPTP:stä.

PPTP (Point-to-Point Tunneling Protocol) on VPN-tunnelointiprotokolla, joka pohjautuu PPP-protokollaan. Se on alun perin tarkoitettu yrityksen ulkopuolella

olevien Windows-työasemien kytkeytymiseen Windows-palvelimille julkisen verkon yli.

RADIUS (Remote Authentication Dial In User Service) on aikoinaan suunniteltu sisäänsoittopalveluissa tapahtuvaan tunnistukseen, jossa se on nykyäänkin laajassa käytössä.

securID on Security Dynamics-yhtiön kehittämä mekanismi, jolla todennetaan käyttäjän oikeus verkkoresursseihin.

S/MIME Secure MIME eli S/MIME on standardi, joka määrittelee sähköpostin salauksen ja allekirjoittamisen julkisen avaimen salausta käyttäen. Sen avulla voidaan varmistaa viestin luottamuksellisuus (ei sivullisten tietoon), alkuperäisyys (kuka on viestin laatija) ja muuttumattomuus.

SSID on lyhenne sanoista Service Set IDentifier, joka tarkoittaa langattoman lähiverkon verkkotunnusta. Sen avulla voidaan erottaa samalla alueella olevat WLAN-verkot toisistaan ja kytkeytyä haluttuun verkkoon.

SSL v3 on kolmas versio salausprotokollasta, jolla voidaan suojata internet-sovellusten tietoliikenne IP-verkkojen yli.

SSL VPN (Secure Sockets Layer) VPN (Virtual Private Network) on tekniikka, jossa otetaan VPN-yhteys SSL-yhteyden yli suljettuun verkkoon etätyöasemalta tai yhdistetään kaksi suljettua verkkoa keskenään.

Symmetrinen salaus tarkoittaa, että viesti salataan ja salaus puretaan samalla avaimella. Salauksen purkamiseen tarvittava avain on suoraan johdettavissa salausavaimesta.

VPN (Virtual Private Network) on tapa, jolla yhdistetään useampia yrityksen verkkoja julkisen verkon yli muodostaen näennäisesti yksityisen verkon.

Wi-Fi on WLAN-tuotteista käytetty kaupallinen nimi. Wi-Fi on *Wi-Fi Alliancen* tavaramerkki, jota jäsenet käyttävät määritellyn laatutason symbolina.

WLAN (Wireless Local Area Network) on langaton lähiverkkotekniikka, jolla yhdistetään erilaiset verkkolaitteet toisiinsa ilman kaapeleita.

WPA (Wi-Fi Protected Access**)** on tietoturvatekniikka, joka kehiteltiin korvaamaan WEP-salauksen ongelmat.

1. Johdanto

Kannettavien tietokoneiden, älypuhelimien ja tablettitietokoneiden yleistyessä niiden tietoturva on entistä tärkeämpi asia. Erilaiset salausalgoritmit auttavat käyttäjiä suojaamaan tärkeän ja korvaamattoman tiedon sekä auttavat lähettämään tietoa salatussa muodossa avoimissa verkoissa. Jos pelkän tiedoston salaaminen ei ole riittävä keino, voidaan koko kovalevyn sisältö salata. Tähän on olemassa monenlaisia ohjelmia, tässä työssä on niistä esitelty TrueCrypt-ohjelma. Salauksen lisäksi on tärkeää muistaa varmuuskopiointi. Varmuuskopiointi pitää suorittaa yrityksissä päivittäin. Varmuuskopioita pitää olla vähintään kaksi ja niistä toinen kaukana alkuperäisestä laitteesta tulipalon ja varkausuhan takia.

Langattomat verkot ovat viime aikana yleistyneet vauhdilla, tämä on tehnyt niistä aika ajoin erittäin turvattomia. Langattomien verkkojen yleistyminen vuosituhannen vaihteessa toi mukanaan suuren huolen niiden turvallisuudesta. Aluksi kehiteltiin WEP-salaus, se kuitenkin murrettiin muutaman vuoden sisällä sen lyhyen salausavaimen ansiosta. Tällä hetkellä turvallisin langaton verkko on suojattu WPA2-salauksella. WPA2:ssa käytetään AES-salausalgoritmia, jonka purkamiseen ei ole keksitty tehokasta keinoa.

Nykypäivänä kotoa työskentely VPN-yhteyttä käyttäen on suosittua. Tässäkin tapauksessa tietoturva on suurena vaikuttajana. Salattuna VPN-yhteys tarvitsee käyttäjän koneelta sertifikaatin, jonka avulla todennetaan käyttäjä.

2. Tutkimuksen tavoitteet

Tutkimuksen tavoitteena on selventää tiedon salauksen eri tapoja ja käytäntöjä. Tavoitteena on myös tietoverkkojen eri suojausmenetelmien käytännön selvitys. Työssäni syvennyn tiedon salaamiseen ja langattomien verkkojen tekniikoihin. Tutkimuksessani käyn läpi myös tietojen varmistamisen sekä etäyhteydet.

Tutkimuskysymyksiä:

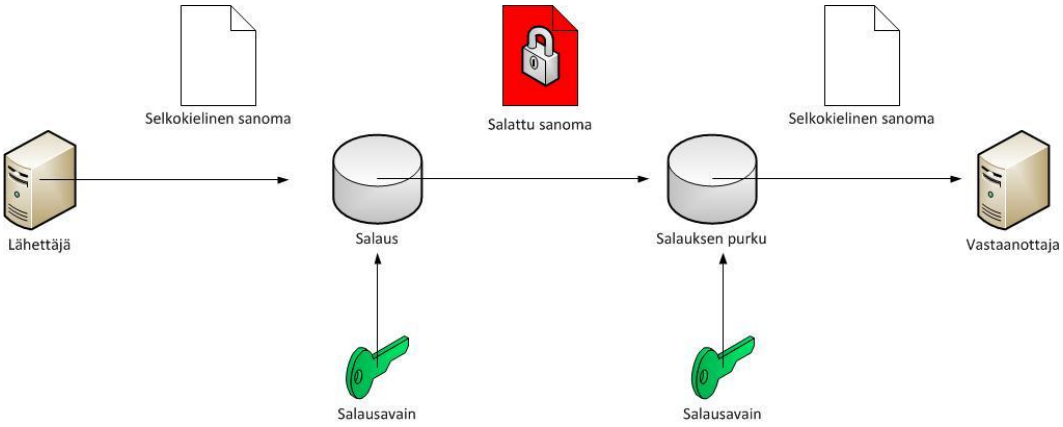
1. Kuinka tietokoneen saa suojattua langattomassa verkossa?

2. Miten suojaan tietokoneen niin, että voin tehdä etätöitä?

3. Kuinka suojaan tietokoneella olevan tiedon?

3. Symmetrinen salaus

”Symmetrisessä salauksessa viestin salauksen purkamiseen tarvittava avain on suoraan johdettavissa salausavaimesta.” Symmetrisessä salauksessa viesti salataan ja salaus puretaan samalla avaimella. (Kuva 1) Symmetriset salausalgoritmit jaetaan jono- ja lohkosalaajiin. (Viestintävirasto 2007)



Kuva 1. Esimerkki symmetrisestä salauksesta.

3.1. DES

DES (Data Encryption Standard) on kehitetty vuonna 1977. Se on pohjimmiltaan muutettu ja yksinkertaistettu versio IBM:n kehittämästä LUCIFER-salausjärjestelmästä. DES:iä on käytetty esimerkiksi pankkien sovelluksissa, jossa salaus on erittäin tärkeää. (Kerttula 1998, 114.)

DES on symmetrisen avaimen salaaja, koska se käyttää samaa avainta tiedon salaamiseen ja purkamiseen. DES:iä kutsutaan 64 bitin salaajaksi, mutta todellisuudessa siinä käytetään 56 bittiä salaukseen ja loput 8 bittiä tarvitaan pariteettiin. Pariteetti on yksinkertainen keino laskea tarkistussumma, eli jos pariteetti on oikein, tiedetään salauksessa käytetyn 56 bitin olevan myös eheä. (Internet-Computer-Security.com 2012)

DES on nykypäivänä jo vanhentunutta teknologiaa sen lyhyen salausavaimen vuoksi (56 bittiä). DES:iin on kuitenkin vuosien aikana investoitu miljardeja, jo-

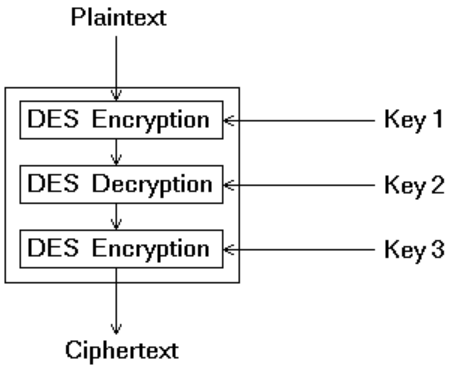
ten sen päivitettyyn versioon Triple-DES (3-DES) voi vielä tänäkin päivänä törmätä.

DES-algoritmi pystytään nykypäivänä murtamaan ”raa’an voiman” murtomenetelmää käyttäen. Raakaa voimaa käyttämällä DES:in voi murtaa yhden vuorokauden aikana. DES-algoritmin murtamisen helppous piilee sen salausavaimen lyhyydessä, tämän takia on kehitetty monisalaajia kuten Triple-DES.

Triple-DES tarkoittaa kolmea DES-salauksen käyttöä peräkkäin. Triple-DES:iä voidaan käyttää kolmella eri tavalla:

- Kolme salausta peräkkäin kolmella eri avaimella
- Salaus-purku-salaus-operaatio kolmella eri avaimella
- Samat kuin edelliset, mutta ensimmäinen ja kolmas DES käyttää samaa avainta. (Kerttula 1998, 114, 127, 130.)

Kolmella avaimella salaus toimii niin, että ensiksi luodaan kaksi 56 bitin avainta. Ensimmäinen salaus tehdään avaimella yksi, sitten salaus puretaan avaimella kaksi ja lopuksi salataan avaimella kolme. Näin saadaan aikaan vahva salaus. (Kuva 2)



Kuva 2. Triple-DES-salauksen toiminto. (Tropical software 2012)

3.2. AES

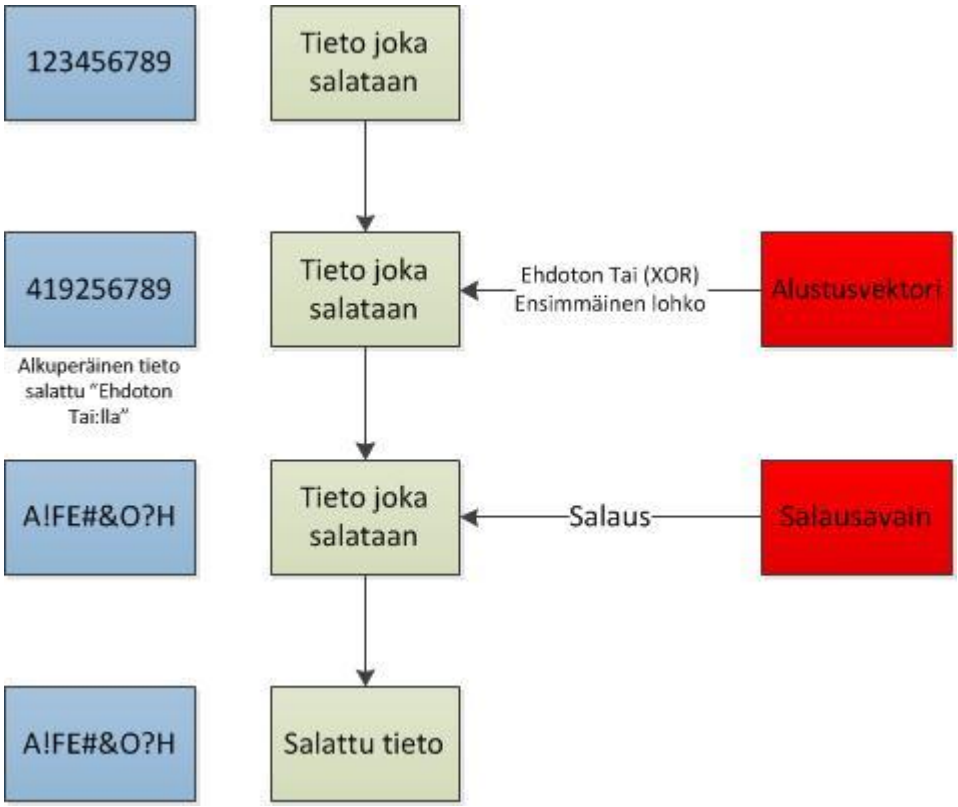
Yhdysvaltain hallitus kehitti AES (Advanced Encryption Standard)-salakirjoitusmenetelmän omaan käyttöönsä korvaamaan DES-algoritmin. AES on myöhemmin julkaistu myös yleiseen käyttöön. AES käyttää Rijndael-algoritmia, joka on salaisen avaimen tulosalaaja ja käyttää 128-, 192- tai 256-bittistä avainta. Lohkon koko ei ole riippuvainen avaimen koosta, lohko voi olla 128-, 192- tai 256-bittinen.

Rijndael-algoritmi jakaa selväkielisanoman lohkon sekä salakirjoitusavaimen omiin taulukkoihinsa, joista jokaisessa on neljä riviä ja niiden sarakkeiden määrä lasketaan jakamalla lohkon tai avaimen pituus 32:lla. Taulukon alkiot täytetään sarake kerrallaan joko lohkon tai avaimen tavuilla. ”Rijndael-algoritmi käyttää useaa salauskierrosta, joiden lukumäärä valitaan lohkotaulukon sarakkeiden lukumäärän tai avaintaulukon sarakkeiden lukumäärän perusteella siten, että neljä saraketta tarkoittaa kymmentä salauskierrosta, kuusi saraketta tarkoittaa kahtatoista kierrosta ja kahdeksan saraketta tarkoittaa neljäätoista salauskierrosta.” (Hakala, Vainio & Vuorinen, 2006, 382)

Sitten avaimesta tehdään kierrosavaimet jokaiselle salauskierrokselle myös lopuksi tehtävälle ylimääräiselle kierrokselle. ”Sen jälkeen lohkotaulukon alkioita muutetaan avaimen alkioiden perusteella, minkä jälkeen suoritetaan salauskierrokset.” (Hakala, Vainio & Vuorinen 2006, 382.)

AES-algoritmi koostuu neljästä tasosta, jotka muodostavat yhden kierroksen. Ensimmäisen tason muutos on ”ei lineaarinen” tavun korvaaminen jokaiselle lohkon tavulle. Toinen taso siirtää syklisesti tavun lohkon sisällä. Kolmannen tason muutos ryhmittää neljä tavua yhteen, luoden neljän termin polymonin ja moninkertaistaa polymonit kiinteän polymonin mod (x^4+1) avulla. Neljännen tason muutos lisää kierrosavaimen, joka sisältää datalohkon. (VOCAL Technologies Ltd. 2012)

Kuvassa 3 on selkeytetty AES-algoritmin toimintaa.

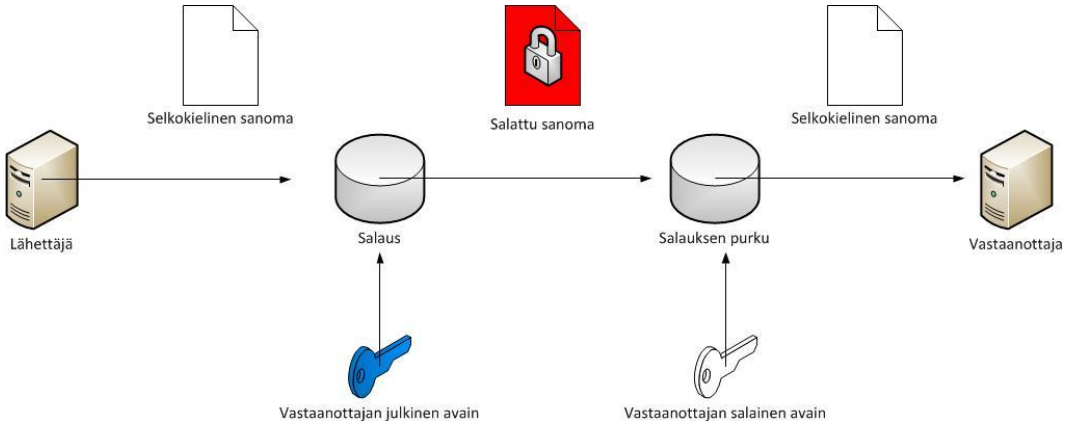


Kuva 3. AES-salauksen vaiheet. (QuinStreet Inc. 2012)

Ensiksi luodaan salaus ja salauksenpurkumuunnoksia, käyttäen alustusvektoria ja salausavainta. ”Ehdoton tai” muuttaa alustusvektorin ensimmäisen lohkon arvolla, ennen kuin todellinen salaus tapahtuu. ”Ehdottoman tai:n” tarkoitus on pitää salatut arvot ainutlaatuisina, vaikka arvot, joita salataan, olisivat samanlaisia. (QuinStreet Inc. 2012)

4. Epäsymmetrinen salaus

”Epäsymmetrisessä salauksessa käytetään avainparia, joista toinen avain on julkinen (public key) ja toinen vastaavasti yksityinen (private key).” (Kuva 4) Avaimet ovat yhteensopivia siten, että julkisella avaimella salattu viesti voidaan purkaa yksityisellä avaimella ja päinvastoin. (Viestintävirasto 2007) Epäsymmetristä salausta kutsutaan myös julkisen avaimen salaamiseksi.



Kuva 4. Esimerkki epäsymmetrisestä salauksesta.

4.1. RSA

RSA on R. Rivest, A. Shamir ja L. Adlemanin vuonna 1977 keksimä ja julkaisema julkisen avaimen kryptosysteemi. RSA:ta voidaan käyttää salaukseen, digitaaliseen allekirjoitukseen ja avainten jakeluun. RSA on lohkosalaaja, siinä selväkieliset sanomat ja salasanomat ovat kokonaislukuja, sanomat muutetaan kokonaisluvuiksi jollain yksikäsitteisellä tavalla. (Kerttula 1998, 173.)

RSA-algoritmi perustuu modulaariseen potenssinkorotukseen. Numeroiden e, d ja N arvot valitaan niin, että jos A on vähemmän kuin N, sitten käytetään lausetta (A^e mod N) d mod N = A. Tämä tarkoittaa sitä, että A:n pystyy salaamaan käyttämällä e:n arvoa ja purkamaan käyttämällä d:n arvoa. Numeroparit (e, N) tunnetaan julkisena avaimena. Numeroparit (d, N) tunnetaan salaisena avaimena. Numero e on julkinen eksponentti, mod on jakojäännös eli modulo, numero d on

salainen eksponentti ja N on moduuli. Kun RSA:ssa puhutaan avaimen pituudesta, tarkoitetaan sillä moduulin pituutta. (Cryptography World 2012.)

RSA:ta kutsutaan myös epäsymmetriseksi salausalgoritmiksi. Sitä käytetään mm. elektronisessa kaupankäynnissä. RSA oletetaan turvalliseksi, koska erittäin suurien alkulukujen tekijöihin jako on vaikeaa. RSA:ta käytetään myös viestien allekirjoittamiseen, jolloin viestistä lasketaan tiiviste tiivistefunktion avulla. Tämän jälkeen ”tiiviste salataan julkisella allekirjoitusavaimella.” Viestin allekirjoitusta tarkistettaessa pitää vanha tiiviste purkaa, jonka jälkeen viestistä lasketaan uusi tiiviste. Jos vanha ja uusi tiiviste ovat samanlaisia, niin tiedetään, ettei viesti ole muuttunut matkalla. (Hakala ym. 2006, 382–383.)

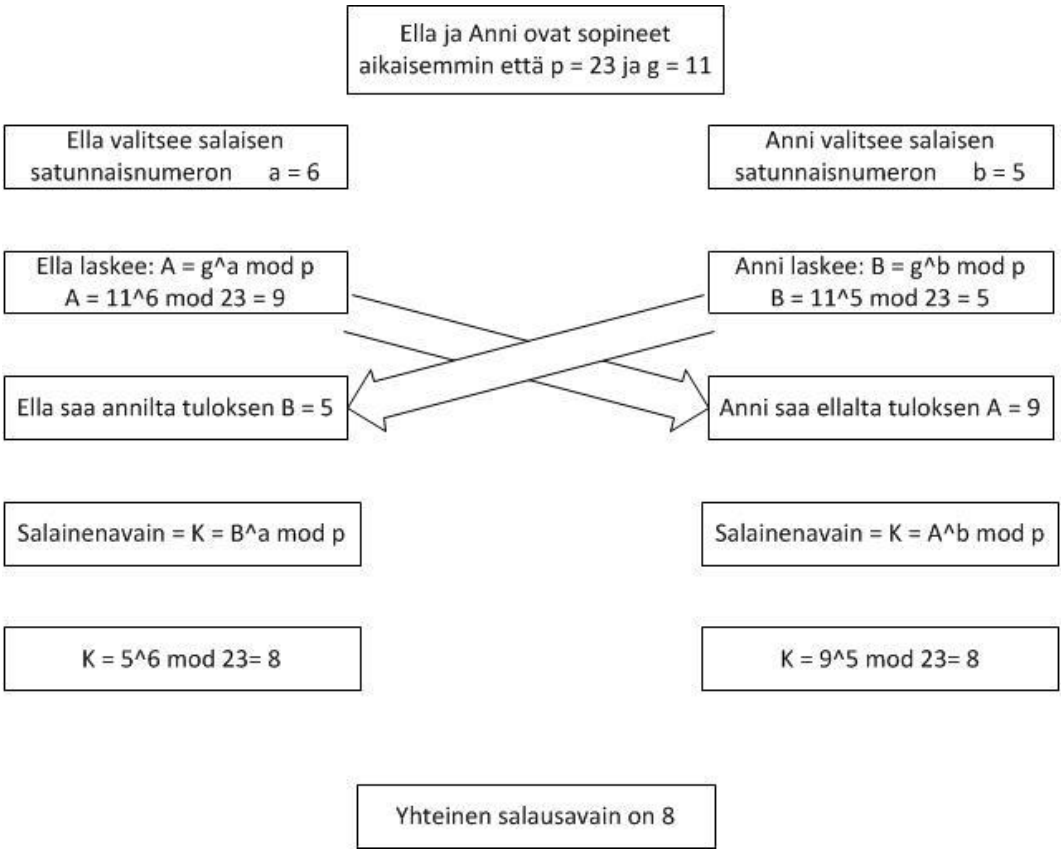
4.2. Diffie-Hellman

Whitfield Diffie ja Martin Hellmanin algoritmi määrittelee turvallisen mekanismin symmetriseen avainten jakeluun. Diffie-Hellman-protokolla ratkaisee salaisen avaimen lähettämisen turvallisesti vastaanottajalle. Kumpikin osapuoli voi saada avaimen vaihtamatta ollenkaan salaista informaatiota.

Yleisesti kuvattuna Diffie-Hellman toimii niin, että osapuolet sopivat keskenään kahdesta suuresta vähintään 150-numeroisesta luvusta. Koska luvuilla on oltava tiettyjä matemaattisia ominaisuuksia, on suositeltavaa, että toinen osapuoli valitsee molemmat luvut ja ilmoittaa näistä vastapuolelle. Olkoot vastapuolet nimeltään Ella ja Anni. Ella voi valita molemmat luvut ja ilmoittaa ne Annille osana yleistä keskustelua, salakuuntelija ei hyödy mitenkään näistä luvuista, vaikka saisikin ne tietoonsa.

Seuraavaksi Ella ja Anni valitsevat itsenäisesti oman suuren luvun satunnaisesti. Luvun tulee olla vähintään 150-numeroinen, ja tämä numero on pidettävä salassa. ”Tämän jälkeen molemmat syöttävät salaiset lukunsa ja kaksi aikaisemmin valittua lukua määrättyyn yksinkertaiseen eksponenttifunktioon.” Ella ja Anni vaihtavat avoimesti saamansa tulokset, ”minkä jälkeen molemmat suorittavat vastaavantyyppiset eksponenttilaskut toisiltaan saamilla luvuilla.” (Kerttula 1998, 168–169.)

Laskennan tuloksena Ella ja Anni saavat identtisen luvun, jota voidaan käyttää salaisena avaimena. (Kuva 5) Tätä avainta käyttäen osapuolet voivat käyttää mitä tahansa salaisen avaimen menetelmää viestien salaamiseen. (Kerttula 1998, 168–169.)



Kuva 5. Esimerkki Diffie-Hellman-algoritmin käytöstä.

5. Kovalevyn salaus

Salaamalla kannettavan kovalevy estetään ulkopuolisten pääsy koneelle talletettuihin tietoihin. Jos kovalevyä ei ole salattu, voi ulkopuolinen päästä tiedostoihin käsiksi esimerkiksi liittämällä kovalevyn toiseen koneeseen. BIOS-salasanalla voidaan myös suojata koneella olevaa tietoa, tosin se ei ammattilaiselle ole niinkään este kuin pieni haitta, sillä ”BIOS-salasanan murtaminen/muuttaminen on kohtuullisen helppoa.” (Laaksonen, Nevasalo & Tomula 2006, 196.)

Käyttöjärjestelmässä voi olla valmiina salausohjelmisto, esimerkiksi Windows Vista ja Windows 7 -käyttöjärjestelmien Enterprise- ja Ultimate-versioissa on Bitlocker-ohjelma sisäänrakennettuna.

TrueCrypt-ohjelmisto on tarkoitettu kovalevyn salaamiseen. TrueCrypt on ilmainen avoimen lähdekoodin ohjelmisto, jolla voi salata kovalevyltä joko osion tai koko levyn. TrueCrypt voi myös salata osion tai levyn, johon Windows on asennettu. Kun käyttäjä käynnistää koneen, niin TrueCrypt pyytää salasanaa ennen kuin se antaa tietokoneen ladata Windowsin. Salasana pyydetään myös, kun Windowsin sisältämältä levyltä yritetään lukea tietoa, samoin kuin sinne kirjoitettaessakin. Salaus toimii automaattisesti reaaliajassa ja näkymättömästi.

Ensimmäisellä käyttökerralla TrueCrypt pakottaa käyttäjän tekemään ns. pelastuslevyn. Pelastuslevyllä on neljä eri toimintoa:

1. Sen avulla voidaan palauttaa käynnistyssektori, eli jos tietokone ei jostain syystä suostu käynnistymään, niin käynnistyssektorissa voi olla jokin vika.

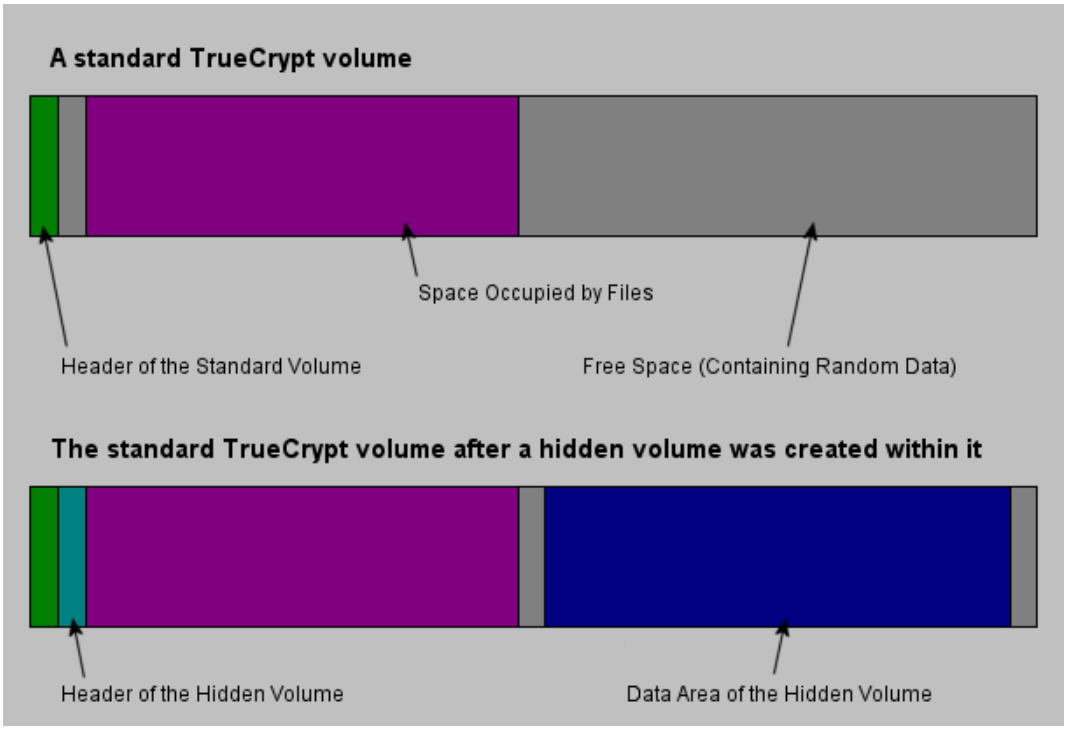
2. Jos TrueCryptin käynnistyslatain on vioittunut, tai jos ei halua pitää käynnistyslatainta kovalevyllä.

3. Jos syöttää oikean salasanan, mutta TrueCrypt väittää sen olevan väärä, voi pääavain tai jokin muu kriittinen tieto olla vääristynyttä. Pelas-

tuslevy antaa mahdollisuuden korjata pääavaimen ja vääristyneen tiedon.

4. Jos Windows on vioittunut, niin pelastuslevyn avulla voidaan salaus purkaa kyseiseltä osiolta tai levyltä.

TrueCrypt:in avulla voidaan myös luoda piilotettu asema. (Kuva 6) Tämä tapahtuu niin, että ensiksi luodaan normaali salattu asema jonka sisään luodaan toinen piilotettu asema. Tämä on mahdollista sen takia, että koska TrueCrypt täyttää salatun aseman vapaan tilan satunnaisella tiedolla, eli se näyttää aina täydeltä asemalta. Piilotettu asema luodaan tämän satunnaisen tiedon tilalle, mutta koska piilotettu asema on myös salattu, niin se ei tule näkyviin esimerkiksi kovalevyn asetuksista, koska se imitoi tyhjää tilaa.



Kuva 6. Kuva piilotetusta asemasta. (TrueCrypt Developers Association 2012.)

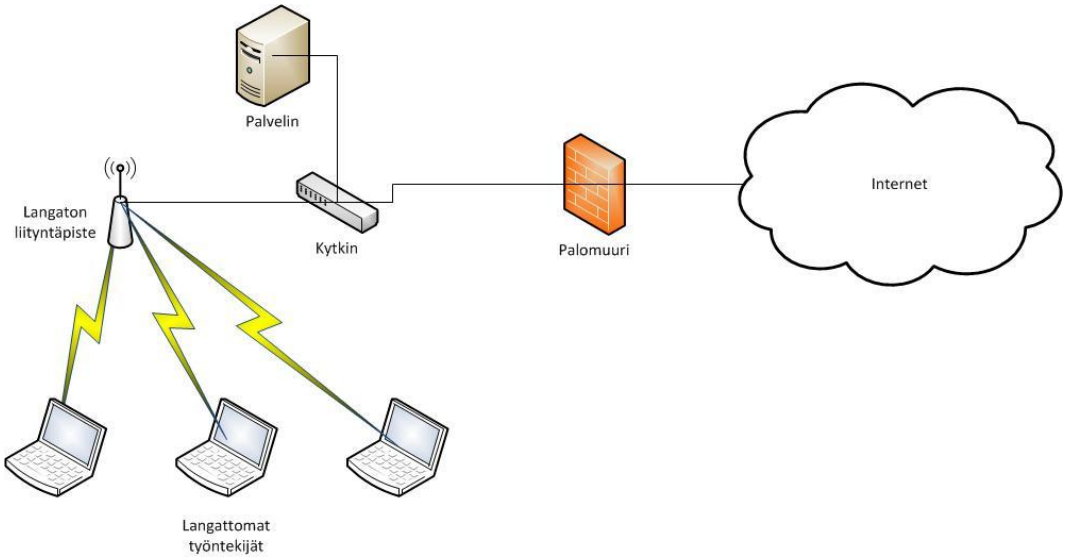
Rinnakkainen salaus ja purku on mahdollista. jos tietokoneen prosessorissa on useampi ydin. Salauksessa otetaan iso kimpale tietoa ja jaetaan se pienempiin osiin. Osia muodostetaan yhtä monta kuin on prosessorin ytimiä. Sitten jokaisella

ytimelle annetaan oma pala tiedosta, joka sen pitää purkaa. Purkaus tapahtuu siis kaikissa ytimissä yhtä aikaa. Samaa käytäntöä käytetään salauksen purkamisessa.

Jotkut prosessorit tukevat laitekiihdytettyä AES-salausta. Tämä on tyypillisesti 4-8 kertaa nopeampaa, kuin pelkkä ohjelmistokohtainen salaus samalla prosessorilla. TrueCrypt käyttää salaukseen AES-, Serpent- ja Twofish-salausalgoritmejä. Käyttäjä saa itse valita, mitä näistä käyttää vai haluaako käyttää näiden yhdistelmää. (TrueCrypt Developers Association, 2012)

6. Kannettavan työaseman suojaus langattomassa verkossa

Tietoturva langattomassa verkossa on tärkeä asia, tietomurtoja kohdistuu kaikkiin internetissä oleviin koneisiin ja etenkin langattomassa verkossa olevaan koneeseen on helppo yrittää murtautua. Seuraavissa luvuissa kerrotaan, kuinka langattomassa verkossa olevan koneen voi yrittää suojata ja minkälaisia WLAN-tekniikoita on nykypäivänä käytössä.



Kuva 7. Yrityksen langaton sisäverkko (WLAN).

6.1. IEEE 802.11, a, b, g ja n

Vuonna 1997 the Institute of Electrical and Electronics Engineers (IEEE) loi ensimmäisen WLAN-standardin ja antoi sille nimeksi 802.11. 802.11sta nopeus oli maksimissaan 2 mb/s, mutta hitaan nopeuden takia tätä standardia ei otettu yleiseen käyttöön.

Ensimmäinen hyväksytty WLAN-standardi oli 802.11b. Tämä b-standardi käyttää 2,4 GHz:n taajuutta ja on teoreettiselta maksiminopeudeltaan 11 mb/s. Todellinen nopeus on 5 mb/s. Melkein samaan aikaan kun b-standardi julkistettiin tuli myös 802.11a-standardi. A-standardi on muuten samanlainen kuin b, mutta se käyttää 5 GHz:n taajuutta. Loppujen lopuksi b-standardi voitti, koska sen 2,4 GHz piiri oli helpompi ja halvempi valmistaa.

Vuonna 2003 julkaistiin 802.11g-standardi. Uusi standardi julkistettiin, koska haluttiin nostaa tiedonsiirron nopeutta. G-standardin teoreettinen maksiminopeus on 54 mb/s, mutta todellinen nopeus on 24 mb/s ja se myös käyttää 2,4 GHz:n taajuutta. Vuonna 2009 standardoitiin n-standardi. Tämäkin standardi luotiin nopeuden noston takia. N-standardissa on kaksitaajuustoiminto, mikä tarkoittaa sitä, että 2,4 GHz:n ja 5 GHz:n taajuuksia käytetään samaan aikaan. N-standardin laitteissa on vähintään kaksi antennia. Teoreettinen maksiminopeus on 600 mb/s ja todellinen nopeus on 100–200 mb/s. (Adrio Communications Ltd. 2012)

Standardi	Vuosi	Taajuus	Tiedonsiirtokapasiteetti	Kantama
802.11	1997	2,4 GHz	1-2 Mb/s	20m sisällä 100m ulkona
802.11a	1999	5 GHz	54 Mb/s	35m sisällä 120m ulkona
802.11b	1999	2,4 GHz	11 Mb/s	35m sisällä 140m ulkona
802.11g	2003	2,4 GHz	54 Mb/s	38m sisällä 140m ulkona
802.11n	2009	2,4 GHz / 5 GHz	100-200 Mb/s	70m sisällä 250m ulkona

Kuva 8. Taulukko WLAN-standardeista.

6.2. SSID

SSID (Service Set IDentifier) on langattoman lähiverkon identifioima nimike. Sen avulla käyttäjät tietävät, mihin verkkoon he ovat liittymässä. Langattoman verkon tukiasema kuuluttaa SSID:tä koko ajan, jotta tietokoneella tai muulla Wi-Fi-verkkoa käytettävällä laitteella löytämään. SSID on 32 bittiä pitkä aakkosnumeerinen sarja, käyttäjälle se kuitenkin näytetään luettavalla ASCII-formaatilla. Järjestelmänvalvoja voi määrittää SSID:n nimen haluamakseen, jotta se voidaan helposti erottaa muista langattomista verkoista.

Suurin osa tukiasemista tukee useamman SSID:n lähettämisen samaan aikaan. Tämän avulla voidaan luoda virtuaaliliityntäpiste. Jokaiselle liityntäpisteelle voidaan luoda omat turvallisuus- ja verkkomääritykset. Tämä sopii hyvin esimerkiksi

yrityksille, jotka haluavat tarjota asiakkailleen pääsyn internetiin yrityksen sisällä, mutta ei pääsyä yrityksen sisäiseen lähiverkkoon.

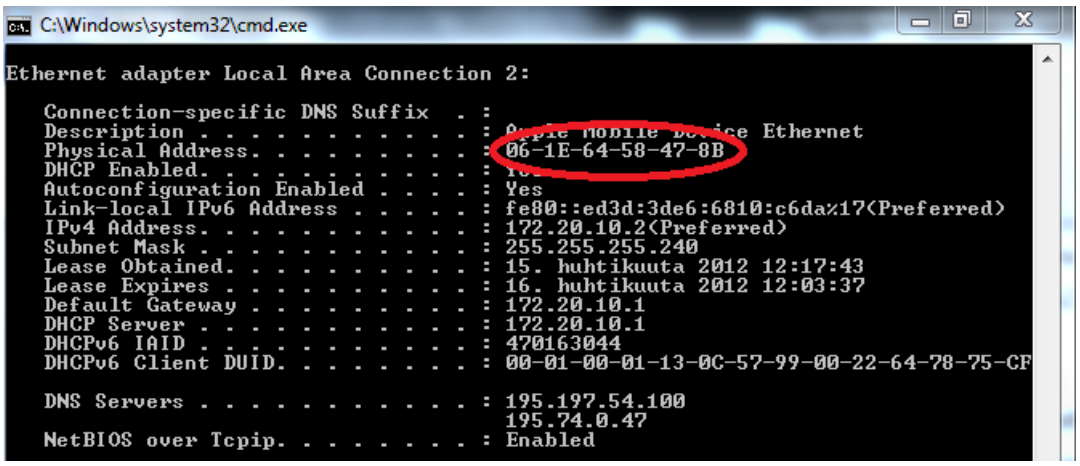
SSID:n avoimen lähetyksen voi kytkeä pois päältä, tämä luo vähän turvallisuutta langattomaan verkkoon. Käyttäjän on muistettava piilotetun SSID:n nimi, mikäli hän haluaa liittyä verkkoon. Piilotettu SSID:n turvallisuus on nykypäivänä kuitenkin pelkkä harhakuva, sen voi helposti löytää nuuskintaohjelmistoilla kuten Kismet. Langattoman lähiverkon turvallisuutta voidaan vähän parantaa, jos SSID on piilotettu ja verkko on suojattu esim. WPA2-suojauksella. (Tech-FAQ)

6.3. MAC-osoitteet

”Jokainen tietokone identifioi itsensä ainutkertaisesti.” Jokaisella verkon tietokoneella on oma fyysinen osoite, jota kutsutaan MAC-osoitteeksi (Media Access Control). MAC-osoite sijaitsee tietokoneen verkkokortilla. ”MAC-osoite on 48-bittinen osoite, joka ilmaistaan kahtenatoista heksadesimaalilukuna.” Ensimmäiset kuusi lukua muodostavat valmistajan tunnisteen ja loput kuusi ilmoittavat valmistajien liitännän sarjanumeron.

Jokaiselle verkkokortille annetaan tehtaalla oma fyysinen osoite, MAC-osoite on ohjelmoitu verkkokortin sirulle. MAC-osoite voidaan kirjoittaa kahdessa eri muodossa: 0000.0c12.3456 tai 00-00-0c-12-34-56. (Kuva 9) MAC-osoitteet ovat verkon yksi keskeisimmistä osista, ilman MAC-osoitteita tietokoneet eivät pystyisi tunnistamaan itseään ja toisiaan. MAC-osoite antaa isännille pysyvän, ainutkertaisen nimen. Toisin kuin IPv4-osoitteet, MAC-osoitteet eivät ihan heti lopu sillä MAC-osoitteita on kaikkiaan 2 triljoonaa kappaletta. (Holttinen Ciscon verkkoakatemia - 1. vuosi 2002, 219–220.)

Tukiasemalle on olemassa oma MAC-suodatus. Tukiasemalle käyttäjä määrittelee listalle kaikki ne MAC-osoitteet, josta liikenne sallitaan. Tämä on kuitenkin työlästä ja aikaa vievää puuhaa, jonka takia näitä listoja ei enää yritysmaailmassa käytetä.



Kuva 9. Verkkokortin MAC-osoite.

6.4. WEP

”WEP-salaus (Wired Equivalent Privacy) on alkuperäinen, IEEE 802.11-standardiin kuuluva tukiaseman ja pääteaseman välisen liikenteen salaukseen käytettävä menetelmä.” (Hovatta, Kiviniemi & Somiska 2005, 28–29) WEP-salaus on käytettävissä niin vanhoissa kuin uusissakin laitteissa. WEP-salauksen huonona puolena on sen heikkous, se voidaan nykypäivänä helposti murtaa. Näiden heikkouksien takia WEP-salausta ei suositella yrityskäyttöön, mutta kotikäytössä se on parempi kuin täysin salaamaton yhteys.

WEP-salauksen toimintaperiaate on, että tukiasemaan ja päätelaitteeseen asetetaan salausavain. Useimmiten salausavain on sama kaikissa päätelaitteissa. Salausavain on pituudeltaan 104 bitin mittainen. WLAN-laitteen konfiguraatiokäytöliittymässä avaimen pituus on 128 bittiä, tämä on sen takia, että avaimeen lisätään 24 bitin mittainen aloitusvektori.

Salausavain voi olla mikä tahansa 13 merkin mittainen yhdistelmä. Salausavain voidaan ilmoittaa myös HEX-muodossa, jolloin se muodostuu 26:sta HEX-merkistä. Lähetettävä data salataan avaimen avulla lähetyspäässä ja puretaan vastaanottopäässä sekä varmistetaan datan koskemattomuus.

WEP-salauksen heikkoudet mahdollistavat passiivisen hyökkäyksen WLAN-verkkoon. WLAN-verkkoon murtautujan tarvitsee vain kuunnella ja kerätä verkon

salattua liikennettä saadakseen salausavaimen haltuunsa. Kerättyään liikennettä tarpeeksi murtautuja voi muutamassa minuutissa murtautua verkkoon internetistä löytyvillä murtotyökaluilla. Liikenteen tarvittava määrä vaihtelee sadoista megatavuista gigatavuun saakka.

”Myös käyttäjän tunnistamiseen eli autentikointiin WEP on huono ratkaisu. WEP itsestään ei tarjoa mahdollisuutta yksittäisen käyttäjän autentikoimiseksi.” Tunnistamiseen on käytetty tukiasemien pääsylistoja eli MAC-osoitelistoja. Listoihin kirjataan kaikkien päätelaitteiden MAC-osoitteet yksitellen, joten ylläpito on erittäin työlästä. Lisäksi MAC-osoitteen pystyy vaihtamaan ohjelmallisesti ja näin päästään kiertämään pääsylista. (Hovatta, Kiviniemi & Somiska 2005, 28–29.)

6.5. WPA

WPA (Wi-Fi Protected Access) on kehittyneempi salausmuoto WLAN-verkoille. WPA:ssa on WEP-salauksessa havaitut puutteet korjattu ja otettu mukaan käyttäjän autentikointi. ”WPA:ssa salausavain vaihdetaan automaattisesti 10000 paketin välein.” (Hakala ym. 2006, 297.)

WPA:sta on olemassa kaksi eri versiota, joista toinen on tarkoitettu koti- ja pientoimistokäyttöön (WPA-Personal) ja toinen isompien yritysten käyttöön (WPA-Enterprise). Erot näiden välillä ovat käyttäjien autentikoinnin toteutuksessa.

WPA-salaus käyttää TKIP (Temporary Key Integrity Protocol) -protokollaa. WPA:ta käytettäessä liikenne salataan pidemmillä ja pakettikohtaisesti vaihtuvilla salausavaimilla, täten WEP:issä ilmenneet salauksen murtomenetelmät eivät enää toimi.

Kotikäytössä käyttäjän tunnistamiseen käytetään WPA-PSK (Pre Shared Key) -menetelmää, eli WLAN-tukiasemaa konfiguroidessa annetaan jokin salausavain, jolla päästään liittymään verkkoon. Tämä avain on kaikilla käyttäjillä sama. Yrityskäytössä yksittäisen salasanan käyttö on epäkäytännöllistä, joten WPA-Enterprice -laitteissa käytetään erillistä autentikointipalvelinta. Palvelimelle mää-

ritellään jokaiselle käyttäjälle oma käyttäjätunnus-salasanapari, jolla päästään kirjautumaan verkkoon, tunnisteena voi käyttää myös digitaalisia varmenteita.

Autentikointi suoritetaan RADIUS-palvelimen avulla. RADIUS-palvelin voi olla yhteydessä yrityksen AD (Active Directory) -hakemistopalveluun, täten WLAN-verkkoon kirjautumiseen käytetään yrityksen lähiverkon tunnisteita kirjauduttaessa.

WPA:n käytössä on todettu heikkouksia, mutta sitä voidaan pitää käyttökelpoisena ratkaisuna langattoman verkon tietoturvan toteuttamiseen. WPA:n heikkoudet ovat ilmenneet kotikäytössä. Käytössä on ollut liian lyhyt salasana tai se on pystytty arvaamaan helposti. (Hovatta ym. 2005, 29–30.)

6.6. WPA2

”WPA2 on viimeisin ja kehittynein ratkaisu WLAN-verkkojen salaamiseen.” WPA2 on monelta osin samanlainen kuin WPA. Suurin ero on salauksen menetelmässä, WPA2:ssa käytetään TKIP:in sijasta AES-menetelmää. AES (Advanced Encryption Standard) on vahva salausmenetelmä, AES vaatii suurta suoritustehoa niin tukiasemalta kuin päätelaitteeltakin. WPA2:sta on myös kaksi eri versiota, WPA2-Enterprice ja WPA2-Personal. Toiminnaltaan nämä ovat samanlaisia kuin WPA:n versiot. Enterprice tarvitsee palvelimen autentikoimiseen, kun taas Personal käyttää määritettyä salasanaa. Tietoturvan kannalta WPA2 on tällä hetkellä kannattavin ratkaisu suojata niin yrityksen kuin kodinkin verkko. (Hovatta ym. 2005, 30.)

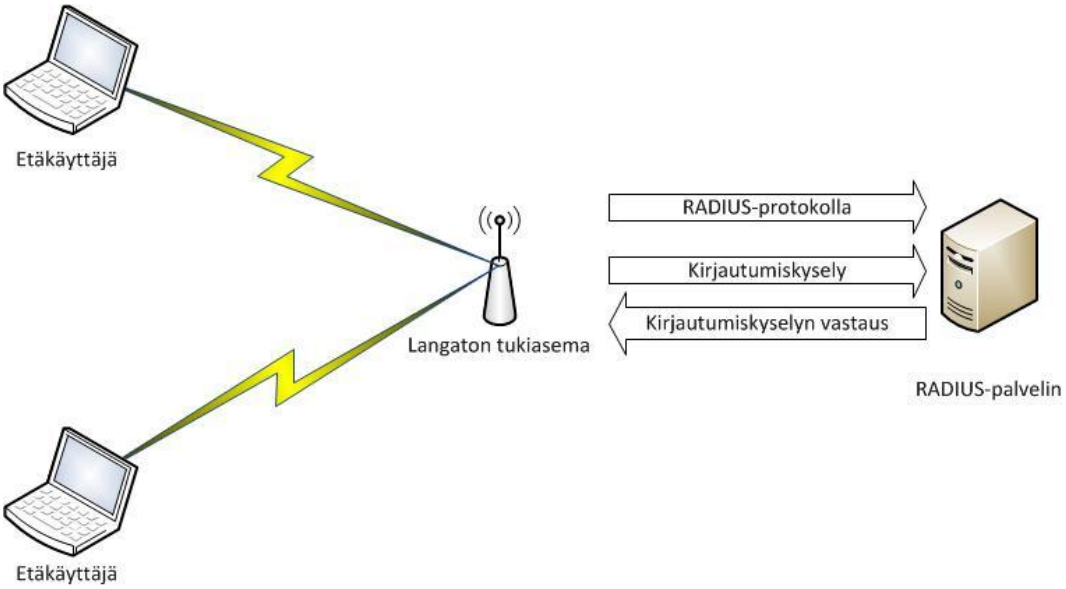
WPA2 tarjoaa korkeamman luokan tietoturvan kuin WPA, koska AES-salausalgoritmi on vahvempi kuin TKIP-algoritmi. WPA2 luo uudet salausavaimet jokaiselle yhteydelle, ja salausavaimet, joita käytetään asiakaskoneen kanssa, ovat ainutlaatuisia kyseiselle asiakkaalle. Jokainen lähetetty paketti salataan uniikilla salausavaimella, jolloin turvallisuus paranee, koska avainten uudelleen käyttöä ei ole. (Cisco Systems Inc.)

6.7. RADIUS

RADIUS (Remote Authentication Dial-In User Service) on niin sanottu laillisuustarkistuspalvelin. RADIUS-palvelin voi tarkistaa joko käyttäjän tiedot salasanojen tai sertifikaattien avulla tai järjestelmän MAC-osoitteen kautta laillisuuden. ”Teoriassa langattoman asiakkaan ei sallita liittyvän verkkoon, ennen kuin tämä tapahtuma on valmis”. RADIUS tarkistaa käyttäjien henkilöllisyydet tietokannoista. (Dell Inc.)

RADIUS-palvelin tukee monia metodeja käyttäjän tunnistamiseen. Kun palvelimelle annetaan käyttäjänimi ja alkuperäinen salasana, niin se tukee PPP-, PAP- tai CHAP-protokollia. Tyypillisesti käyttäjän sisäänkirjautuminen tapahtuu pääsykyselyllä. Tämä kysely lähetetään NAS-palvelimelle, josta se ohjautuu RADIUS-palvelimelle. Kyselyyn palvelin voi vastata joko myöntävästi tai kieltävästi riippuen siitä, onko käyttäjällä oikeus kirjautua käyttäjätunnuksellaan. Kun RADIUS-palvelin on saanut kirjautumiskyselyn NAS-palvelimelta, alkaa RADIUS tarkistamaan tietokannastaan käyttäjänimeä. Jos käyttäjänimeä ei tietokannasta löydy, lähettää palvelin kieltävän vastauksen kyselyyn. Tähän vastaukseen voidaan liittää myös sanallinen syy, miksi kirjautuminen estettiin. RADIUS-palvelimella on todennus ja valtuutus yhdistettynä toisiinsa. Jos käyttäjänimi löytyy ja salasana on oikein, lähetetään hyväksyntäviesti, ja viestin mukana lähetetään lista parametreista, joita käyttäjä voi istunnon aikana käyttää. (Kuva 10)

Kirjanpitotoiminto RADIUS-palvelimessa sallii datan lähetyksen istunnon alku- ja loppuvaiheessa. Kirjanpidossa käy ilmi käytettyjen resurssien määrä, kuten käytetyn ajan ja tiedonsiirron määrä. Internetpalveluntarjoaja voi käyttää tätä toimintoa hyväkseen tietoturvallisuuden ja/tai laskutuksen kannalta. (Cisco Systems Inc.)



Kuva 10. Kirjautuminen käyttäen RADIUS-palvelinta.

6.8. Bluetooth

Bluetooth-teknologia keksittiin vuonna 1994, sitä kehittivät Ericssonin insinöörit. Vuonna 1998 joukko yrityksiä sopi yhteistyöstä käyttää bluetoothia valmistamissaan laitteissa, ja näin muodostui Bluetooth Special Interest Group (SIG). Tämä tarkoittaa sitä, ettei yksikään yritys omista Bluetoothia, mutta moni SIG:in yritys kehittää yhdessä Bluetoothia.

Bluetoothin langaton teknologia on rakennettu moneen eri tuotteeseen, aina autoista kännyköihin ja tietokoneisiin. Bluetoothin avulla pystytään jakamaan ääntä, musiikkia, valokuvia, videoita ja muuta informaatiota langattomasti kahden laiteparin välillä. (Bluetooth SIG, Inc. 2012)

Bluetooth on niin sanottu Personal Area Network (PAN), sen etäisyys riippuu millaista Bluetooth radiota käytetään.

- Luokan yksi radio – käytetään pääsiassa teollisuuskäytössä. Kantama 100 metriä.

- Luokan kaksi radio – yleisemmin käytössä mobiililaitteissa. Kantama 10 metriä.

- Luokan kolme radio – kantama 1 metri.

Bluetooth toimii lisensoimattoman teollisuuden, tieteen ja lääketieteen kaistalla 2,4 – 2,485 GHz. (Bluetooth SIG, Inc. 2012)

7. Etätyöskentely kannettavalla (VPN)

VPN (Virtual Private Network) on verkon liikenteen salausratkaisu. VPN-yhteys muodostetaan VPN-asiakasohjelmiston ja VPN-päätepisteen välille. Salaus toteutetaan useimmiten IPSec-protokollaa käyttäen. VPN-yhteydellä otetaan yhteys internetin välityksellä kotoa yrityksen sisäverkkoon. Tämän avulla työntekijä voi tehdä töitään kotoa käsin turvallisesti salatun yhteyden läpi. VPN:ää käytettäessä yleisessä ja avoimessa WLAN-verkossa voidaan esimerkiksi sähköposti tarkistaa salattuna, kun ensin kirjaudutaan yrityksen sisäverkkoon ja sen kautta luetaan sähköposti. (Hovatta ym. 2005, 30.)

Käyttäjän autentikointi takaa, että vain luvalliset käyttäjät voivat päästä käsiksi verkon resursseihin. Etäkäyttäjän tunnistamiseen voidaan käytetään RADIUS-palvelinta. (Kerttula 1998, 233–234.)

VPN-tyyppejä on kolmea, ja ne ovat.

- Access VPN (tunnetaan myös nimellä Client VPN) sallii etäyhteyden yrityksen sisäverkkoon jaetun infrastruktuurin kautta samoin käytännöin kuin yksityinen verkko. Access VPN tukee DSL- sekä mobiili IP- ja kaapelitekniikoita. Näiden avulla mobiilikäyttäjät ja etätyöpaikat voivat turvallisesti muodostaa yhteyden verkkoon. (Kuva 11)

- Intranet VPN (tunnetaan myös nimellä Site to Site VPN) yhdistää yrityksen kaikki etätoimipaikat yhteen intranetiin jaetun infrastruktuurin avulla. Internetoperaattoreilta voi ostaa tähän tarkoitukseen soveltuvan yhteyden.

- Extranet VPN yhdistää kaikki yrityksen kumppanit samaan yrityksen intranetiin. Tähän voi myös operaattorilta ostaa soveltavan yhteyden.

Tyypillisesti VPN muodostuu maantieteellisesti hajallaan olevista aliverkoista, jotka kuuluvat kaikki saman yrityksen toimialueeseen. ”Verkkoja yhdistää jaettu infrastruktuuri, joka on niiden hallinnan ulkopuolella.” VPN:n turvallisuus riippuu sen toteutuksessa käytettävästä teknologiasta. Jos liikenne on salattu yhteisessä

infrastruktuurissa tehtävän siirron ajaksi, on VPN-aliverkkojen yhteys suhteellisen korkeaa tasoa. (Holttinen 2002, 541–542, 544.)

7.1. IPSec

Internet Protocol Security käyttää salattuja turvallisuuspalveluita suojaamaan liikenneyhteyksiä IP-verkoissa. IPSec tukee verkkotason todennusta, tiedon alkuperän todennusta, tiedon eheyttä, tietojen luottamuksellisuutta salauksessa sekä uusinta suojausta. (Microsoft Inc. 2012)

Transport mode eli liikennetila on IPSec:in oletustila, sitä käytetään päästä päähän tietoliikenteeseen, esimerkiksi kommunikaatio on asiakaskoneen ja palvelimen välillä. Kun liikennetilaa käytetään, IPSec salaa vain IP-kuorman. Liikennetila tarjoaa suojan IP-kuormalle AH (Authentication Header) tai ESP (Encapsulating Security Payload) -tunnisteen läpi. Yleensä IP-kuormat ovat TCP-segmenttejä, UDP-viestejä tai ICMP-viestejä. (Microsoft Inc. 2005)

Tunnel mode on tunnelointitila; kun tunnelointitilaa käytetään IPSec salaa IP-tunnisteen ja kuorman. Tunnelointitila tarjoaa turvan koko IP-paketille käsittelemällä sitä AH- tai ESP -kuormana. Tunnelointitilassa koko IP-paketti on kapseloitu AH- tai ESP –tunnisteella sekä lisäksi IP-tunnisteella. Uloimman IP-tunnisteen IP-osoitteet ovat tunnelin päätepisteet ja kapseloidun IP-tunnisteen ovat perimmäinen lähde ja kohdeosoitteet. IPSec tunnelointitila on käyttökelpoinen suojaamaan liikennettä eri verkkojen välillä, kun liikenteen on kuljettava epäluotettavan verkon läpi. (Microsoft Inc. 2005)

7.2. L2TP

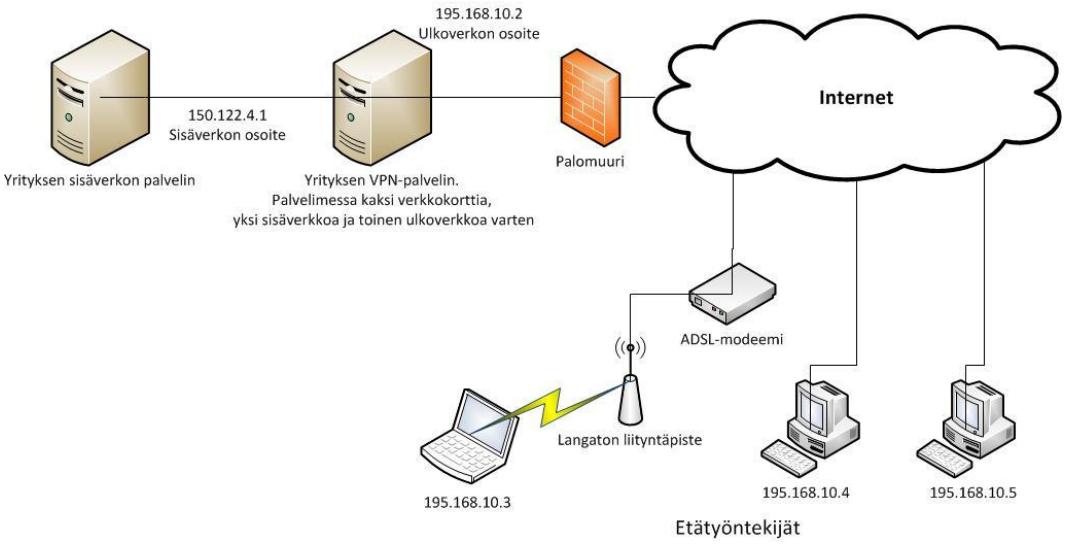
Layer Two Tunneling Protocol on laajennus PPTP:lle, jota internet-palveluntarjoajat käyttävät toteuttaakseen VPN-verkon internetin yli. L2TP yhdistää parhaimmat piirteet kahdesta muusta tunnelointiprotokollasta: Microsoftin PPTP ja Cisco Systems:in L2F:n. L2TP muodostuu kahdesta keskeisestä osasta. Ne ovat: L2TP Access Concentrator (LAC), tämä on laite joka fyysisesti sulkee linjan. Sekä L2TP Network Server (LNS), joka päättää ja mahdollisesti todentaa PPP-virran. (TechTarget 2012)

7.3. PPTP

Point-to-Point Tunneling Protocol on protokolla, joka mahdollistaa turvallisen tiedonsiirron etäasiakkaan ja yrityksen palvelimen välille luoden VPN-yhteyden TCP/IP-verkon kautta. PPTP tukee moniprotokollaratkaisua sekä VPN-verkkoa yli avoimen verkon, kuten internet. (Microsoft Inc. 2012)

7.4. SSL VPN

SSL VPN on VPN:n muoto, jota voidaan käyttää normaalilla web-selaimella. IPSeciin verrrattuna SSL VPN ei tarvitse omaa asiakasohjelmiston asennusta käyttäjän tietokoneelle. SSL VPN antaa etäkäyttäjälle käyttömahdollisuuden palvelinsovelluksille sekä sisäisiin verkkoyhteyksiin. SSL VPN koostuu yhdestä tai useammasta VPN-laitteesta, joihin käyttäjä muodostaa yhteyden web-selaimella. Liikenne web-selaimen ja SSL VPN-laitteen välillä on suojattu SSL-protokollalla tai sen seuraajalla TLS-protokollalla. (TechTarget, 2012)



Kuva 11. Yrityksen VPN-verkko.

IPSec VPN:n käyttöön pitää asiakaskoneeseen asentaa erillinen ohjelmisto. Tämän ohjelmiston avulla käyttäjä pystyy käyttämään kokonaan yrityksen sisäverkkoa. Yrityksessä pitääkin miettiä, halutaanko käyttäjälle antaa koko verkko käytettäväksi, vai vain pääsy eri ohjelmiin ja tiedostoihin. Jos halutaan rajata etätyön-

tekijät käyttämään vain joitain ohjelmia, niin SSL VPN on hyvä vaihtoehto salatulle VPN-yhteydelle. SSL VPN:ä voidaan käyttää suoraan selaimessa, eli erillistä asiakasohjelmistoa ei tarvita. Koska suurimpaan osaan nettiselaimista on sisäänrakennettu SSL VPN-mahdollisuus, voi etätyöskentelijä käyttää tätä tekniikkaa helposti hyväkseen. Pääsyn hallinta on SSL VPN:n yksi suurimmista ominaisuuksista. Toimimalla istuntokerroksella ja antamalla käyttöoikeudet tarkkoihin ohjelmiin SSL VPN voidaan räätälöidä kullekin etätyöntekijälle omanlaiseksi. (Tippit Inc. 2012)

8. Älypuhelimien ja tablettikoneiden tietoturva

Mobiililaitteet ovat nousemassa merkittäviksi uhiksi tietoturvan kannalta. Varsinkin älypuhelimiin tallennetaan paljon tietoa. Sähköpostin käyttö näillä mobiililaitteilla on lisännyt tiedon määrää suuresti. Mobiililaitteita uhkaavat erilaiset haittaohjelmat, ja suositeltavaa onkin asentaa anti-virusohjelma ja palomuuri mobiililaitteeseen jos sellainen on tarjolla. (Heljaste 2008, 71.)

Mobiililaitteesta on tärkeää pitää huolta, sen kuljettamista suositellaan esimerkiksi taskussa tai käsimatkatavarana lentokoneessa, josta se on vaikea varastaa. Laite voidaan myös suojata salasanalla, jolloin siihen ei helposti pääse käsiksi. Mobiililaitteet voi myös merkitä siten, että ne on helppo palauttaa oikealle omistajalle. Palautuspalveluita tarjoavat mm. vartiointiliikkeet.

Älypuhelimille, tablettikoneille, USB-muisteille ja iPod-musiikkisoittimille on kaikille omat salausohjelmansa. Salausohjelmaa valittaessa kannattaa huomioida seuraavia seikkoja:

- Hidastaako salaus laitteen toimintaa? Jos hidastaa, niin kuinka paljon?
- Onko salausohjelman käyttö helppoa? Käyttäjältä ei saa vaatia muita toimia kuin järjestelmään kirjautuminen.
- Tukeeko ohjelma keskitettyä ylläpitoa sekä helpdesk-toimintaa? HelpDeskin avulla voidaan unohtunut salasana turvallisesti uusia.
- Ohjelmiston pitää salata kaikki tiedostot ja tiedot.
- ”Käyttämättä olleet laitteet tulee automaattisesti lukita tietyn ajan kuluttua.” (Laaksonen ym. 2006, 220–221.)

Olen tässä työssä keskittynyt Applen iOS-käyttöjärjestelmään, koska se on minulle tutuin mobiilikäyttöjärjestelmä.

8.1. iOS-käyttöjärjestelmä

iOS on Applen iPhone-, iPad- ja iPod Touch -laitteiden käyttöjärjestelmä. iOS on kosketusnäytöllinen mobiilikäyttöjärjestelmä, joka pystyy tunnistamaan kaksi kosketusta samanaikaisesti. Käyttöliittymä on suunniteltu sormilla käytettäväksi, joten styluskynää ei tarvita. iOS-käyttöjärjestelmässä ohjelmat ovat työpöydällä 4 x 4 ruudukolla, eli 16 ohjelmaa per sivu, sekä alapalkissa pysyvästi neljä ohjelmaa. (Kuva 12) iOS sisältää perusohjelmat, joita ovat kello, laskin, muistio, sähköposti, sää, kartat, kamera, kalenteri yms. App Store:sta voidaan ladata erilaisia ohjelmia, joita on tarjolla yli 500 000, kaikkea peleistä hyötyohjelmiin.

Kuva 12. iPhone iOS 5.1-työpöytä.

8.2. iPad

iPad on Applen suunnittelema tablettitietokone. iPad:iä voisi sanoa isoksi iPod:iksi. iPad:issä on 9,7 tuuman retina-näyttö ja sen tarkkuus on 2048 x 1536. Prosessorina iPad:issä on Applen oma A5X-prosessori, joka sisältää neliytimisen näytönohjaimen. iPad:issä on 5 megapikselin iSight-kamera, jonka avulla

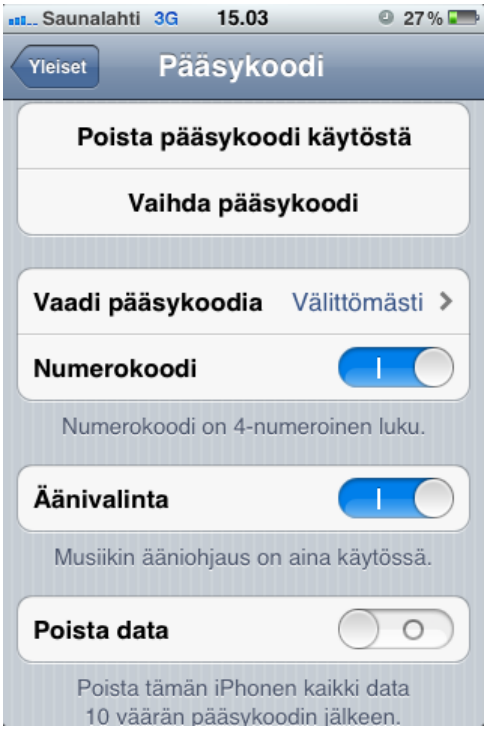
onnistuu 1080p HD-videon ja valokuvien ottaminen. iPad tukee Wi-Fi b-, g- ja n -tekniikoita, sekä bluetooth-tekniikkaa.

8.3. iOS 5.1-tietoturva

iOS tietoturva perustuu kerroksittain rakennettuun turvallisuuteen. Kerroksia on neljä kappaletta.

- Laiteturvallisuus
- Dataturvallisuus
- Verkkoturvallisuus
- Ohjelmistoturvallisuus

Laiteturvallisuudessa käytetään salasanaa turvaamaan laite. Sen avulla pystytään pitämään laite suojattuna muilta käyttäjiltä. Salasanan muodostamisen voi käyttäjä itse määritellä, kuinka pitkä se on ja millaisia merkkejä saa käyttää. Salasanalle voi myös määritellä sen maksimaalisen käyttöiän sekä kirjautumisyritysten maksimimäärän. (Kuva 13)



Kuva 13. Kuva pääsykoodisivusta.

iOS:n rajoitusasetuksista voidaan määritellä kaikki ohjelmat, jotka annetaan käyttäjälle käyttöön, esimerkiksi nettiselaimen käytön voi kieltää. Rajoitusasetuksista voidaan myös määritellä millaisia muutoksia esimerkiksi sähköpostitileihin voidaan tehdä. Myös ohjelmien sisällä tehdyt ostokset voidaan kieltää rajoitusasetuksista. (Kuva 14)

Kuva 14. Kuva rajoitukset-sivusta.

Dataturvallisuus on iOS:n yksi tärkeimmistä alueista. Laitteella säilytettävä tieto voidaan salata ja langattomasti viestittävä tieto salataan myös. Jos laite katoaa tai se varastetaan, voidaan laitteen tiedot tuhota etäohjelmalla, laitteen voi myös kytkeä pois päältä etäohjelmalla. iOS-laitteen tiedot on salattu AES-salauksella, joka käyttää 256-bittistä avainta salaukseen. Salaus on aina päällä, eikä käyttäjä pysty sitä itse ottamaan pois päältä. iOS tukee myös S/MIME-salausta sähköpostin lähetyksessä ja vastaanotossa.

Verkkoturvallisuus iOS-laitteissa on erittäin laaja. Laitteisiin sisäänrakennettuna on Cisco IPSec, L2TP, PPTP VPN, SSL VPN, SSL/TLS, WPA/WPA2, RSA securID ja CRYPTOcard. iOS tukee SSL v3:a, se käynnistyy automaattisesti selainta ja sähköpostia käytettäessä. WPA2 käyttää 128-bittistä AES-salausta, joten langatonta verkkoa voi käyttää turvallisesti niin kotona kuin töissäkin.

Ohjelmistoturvallisuus takaa sen, että ohjelmia ei päästä muuttamaan. Ohjelmaa käynnistettäessä pyydetään salasanaa, jos sellainen on asetettu. Ohjelmistot koodataan siten, että ne eivät pääse käsiksi käyttäjän muihin tietoihin tai muihin oh-

jelmiin. Kaikki uudet ohjelmat pitää tarkistuttaa, tämä tapahtuu Apple-yrityksen puolesta. Ohjelmaa ei päästetä App Storeen, ennen sen tarkistusta. (Apple Inc, 2012)

Älypuhelimilla pystytään myös käyttämään VPN-verkkoa. Älypuhelimen VPN-toimintoa käytettäessä voidaan sillä lähettää tärkeät sähköpostit turvallisesti sekä selata nettiä turvallisesti.

PPTP VPN määrittely iOS 5.1 laitteelle (Kuva 15).

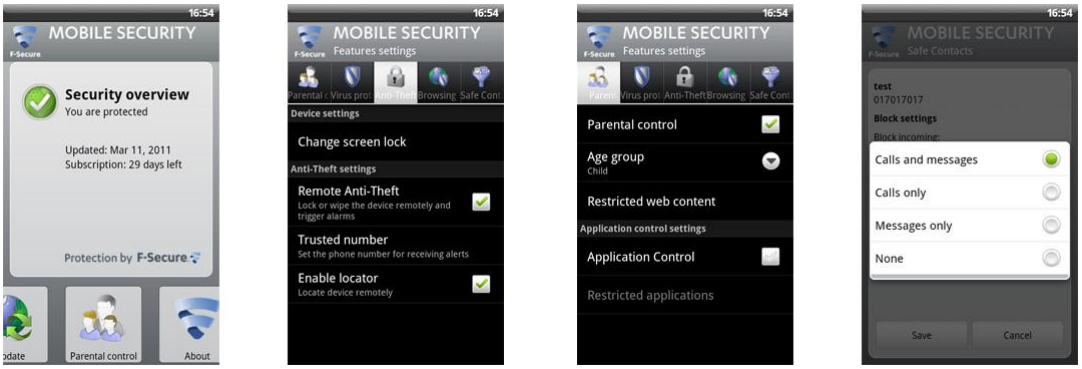
Kuva 15. iPhone VPN-määrittely ja käyttöönotto.

iPhone:n varmuuskopiointi tapahtuu iTunes-ohjelman avulla. Puhelin liitetään tietokoneeseen USB-johdolla. Heti kun tietokone tunnistaa puhelimen, käynnistyy iTunes automaattisesti ja alkaa varmuuskopioimaan puhelimen sisältöä tietokoneelle. Iphonen palautus tapahtuu myös iTunes-ohjelmalla. Kun puhelin on yhdistetty tietokoneeseen, niin painetaan palauta nappia iTunes-ohjelmasta, jolloin palautus käynnistyy. iTunes palauttaa aina uusimman varmuuskopion puhelimesta. (Kuva 16)

Kuva 16. iTunes-ohjelmisto.

8.4. F-Secure

F-Secure mobile security on älypuhelimiin tarkoitettu ohjelmisto. Sen avulla voit suojata puhelimen viruksilta ja haittaohjelmilta. Sillä voi myös suojata henkilöllisyyttä verkossa, paikantaa varastetun puhelimen, paikantaa lapsen sijainti puhelimen välityksellä sekä estää puhelut ja tekstiviestit, joita ei haluta vastaanottaa.



Kuva 17. Mobile Security käytössä Windows-puhelimella. (F-Secure Oyj)

Mobile Security on saatavilla Android-, Symbian- ja Windows Mobile käyttöjärjestelmille. Mobile Security maksaa 29,95 euroa 12 kuukautta tai 49,95 euroa 24 kuukautta per puhelin. (F-Secure Oyj)

9. Tietojen ja ohjelmistojen varmuuskopiointi

Työn yhtenä tavoitteena on myös tiedon suojaamisen näkökulma. Tässä luvussa on käsitelty suojaamista varmuuskopioinnin ja RAID:in kautta.

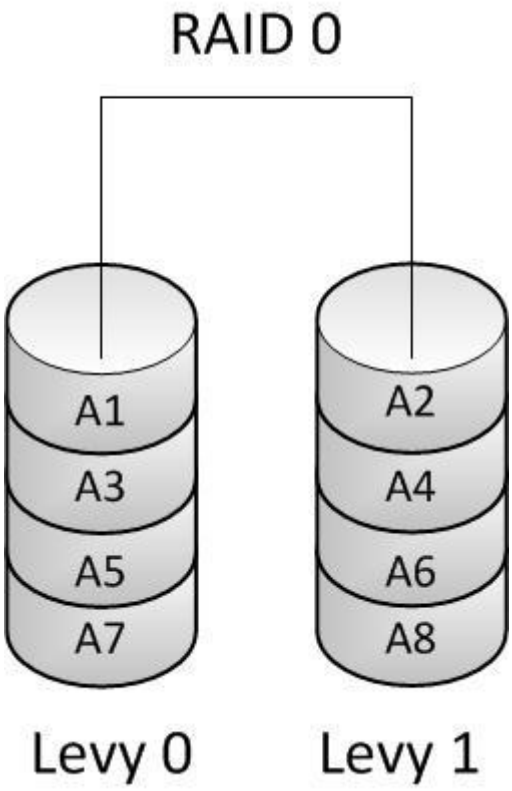
Varmuuskopioinnilla halutaan varmistaa, että kaikki tietokoneella oleva tieto on varmasti tallessa ja palautuskelpoisena. Jos alkuperäiset tiedot on tuhottu tai kadotettu, voidaan varmuuskopiot ottaa käyttöön ja näin päästään jatkamaan työntekoa nopeasti. Varmuuskopioinnin tekemättä jättäminen on kuin vuoren kiipeäminen ilman köyttä. Jos ja kun jotain tapahtuu, niin pahimmassa tapauksessa voidaan menettää rahanarvoista tietoa suuria määriä. Jos on kyseessä suurempi yritys, niin varmuuskopioinnin voi suorittaa automaattisesti. Yrityksissä kannattaa suorittaa varmuuskopiointi kerran päivässä kaikista tiedostoista ja ohjelmistoista.

Varmuuskopioiden säilyttäminen ja testaus on yksi suurimmista seikoista, tämä vain valitettavan usein jää liian vähälle huomiolle. Varmuuskopiot pitää säilyttää eri tilassa kuin ajan tasalla oleva tieto. Jos esimerkiksi varmuuskopioidaan ulkoiselle muistille, kuten muistitikku tai ulkoinen kovalevy, se pitää varmuuskopioinnin jälkeen siirtää pois varmistettavan koneen luota mielellään aivan eri rakennukseen. Varmuuskopion siirtäminen varmistaa sen, ettei varas tai tulipalo tuhoa alkuperäistä tietoa ja varmuuskopiota samalla kertaa. Varmuuskopio on myös hyvä testata ulkopuolisella koneella, jotta voidaan olla varmoja sen toimivuudesta. Tällä tavoin estetään kysymys: mikä sitten avuksi kun alkuperäinen tieto on varastettu ja varmuuskopio ei toimi? (Miettinen 1999, 239–240.)

9.1. RAID 0,1 ja 5

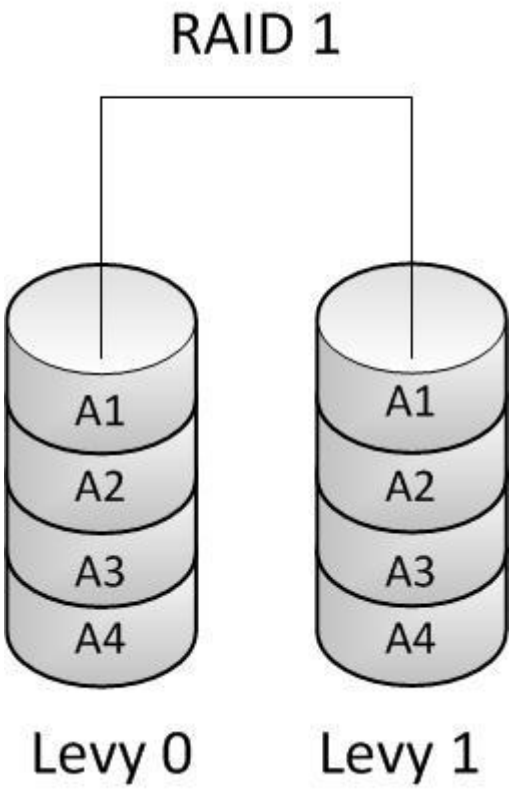
Redundant Array of Independent (or Inexpensive) Disks on luokka kiintolevyjä, jotka yhdistävät kaksi tai useampia asemia vikasietoisuuden ja suorituskyvyn parantamiseen. RAID-levyasemia käytetään usein palvelimissa, mutta välttämätön kotikoneissa. RAID mahdollistaa saman tiedon tallentamisen useissa askeleissa suorituskyvyn parantamiseksi. RAID-tasoja on monia erilaisia.

RAID 0 mahdollistaa tiedon jaon useammalle levylle, mutta ei sisällä ylimääräistä kopiota tiedosta. (Kuva 18) Tämä parantaa suorituskykyä, mutta ei vikasietoisuutta. Jos yksikin levy rikkoutuu, kaikki tiedot menetetään.



Kuva 18. RAID 0-kaavio.

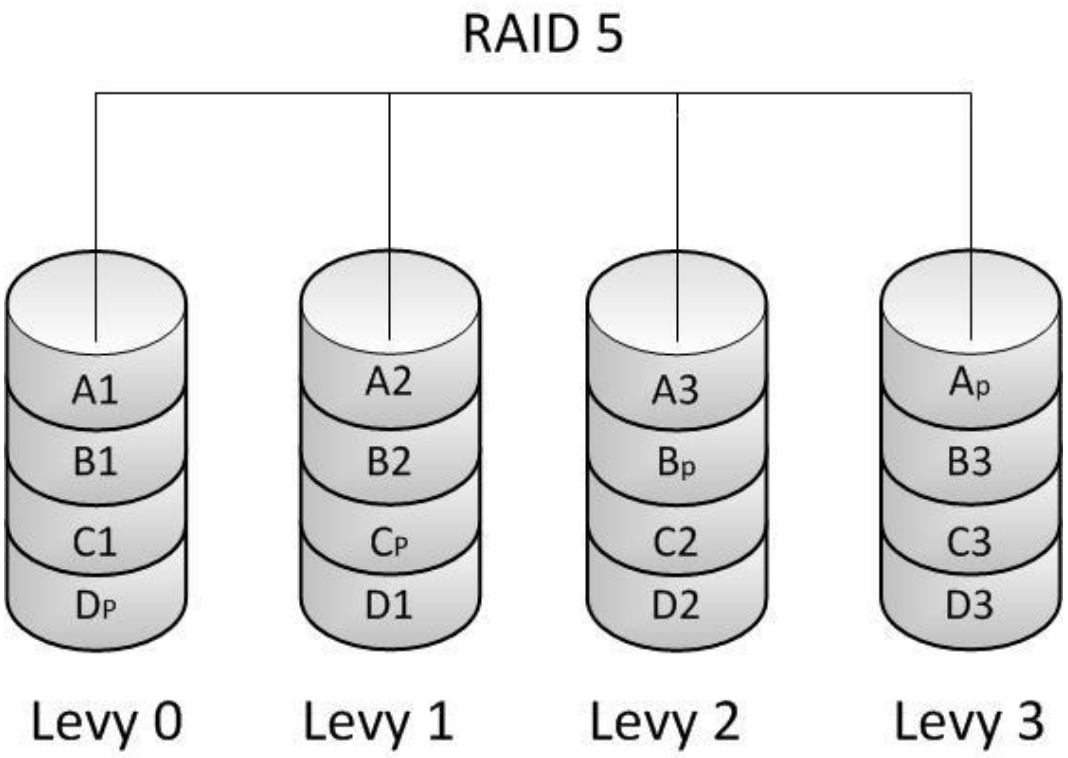
RAID 1 tarjoaa levyn peilauksen, taso yksi mahdollistaa kaksinkertaisen luku- ja kirjoitusnopeuden yhdelle levylle. Levyn tiedot peilataan toiselle levylle, näin saadaan turvallisuutta levyn rikkoutumisia vastaan. (Kuva 19)



Kuva 19. RAID 1-kaavio.

RAID 5 mahdollistaa tiedon jaon tavun tasolla sekä virheenkorjaustiedon. Tämä johtaa erinomaiseen suorituskykyyn ja vikasietoisuuteen. (Kuva 20) Taso viisi on yksi suosituimmista RAID-toteutuksista. (QuinStreet Inc. 2012)

RAID 5:tä käytetään yrityksissä tiedon varmistukseen. RAID 5 on käytössä yrityksen palvelimissa, joihin varmuuskopioidaan kaikki yrityksen tiedot.

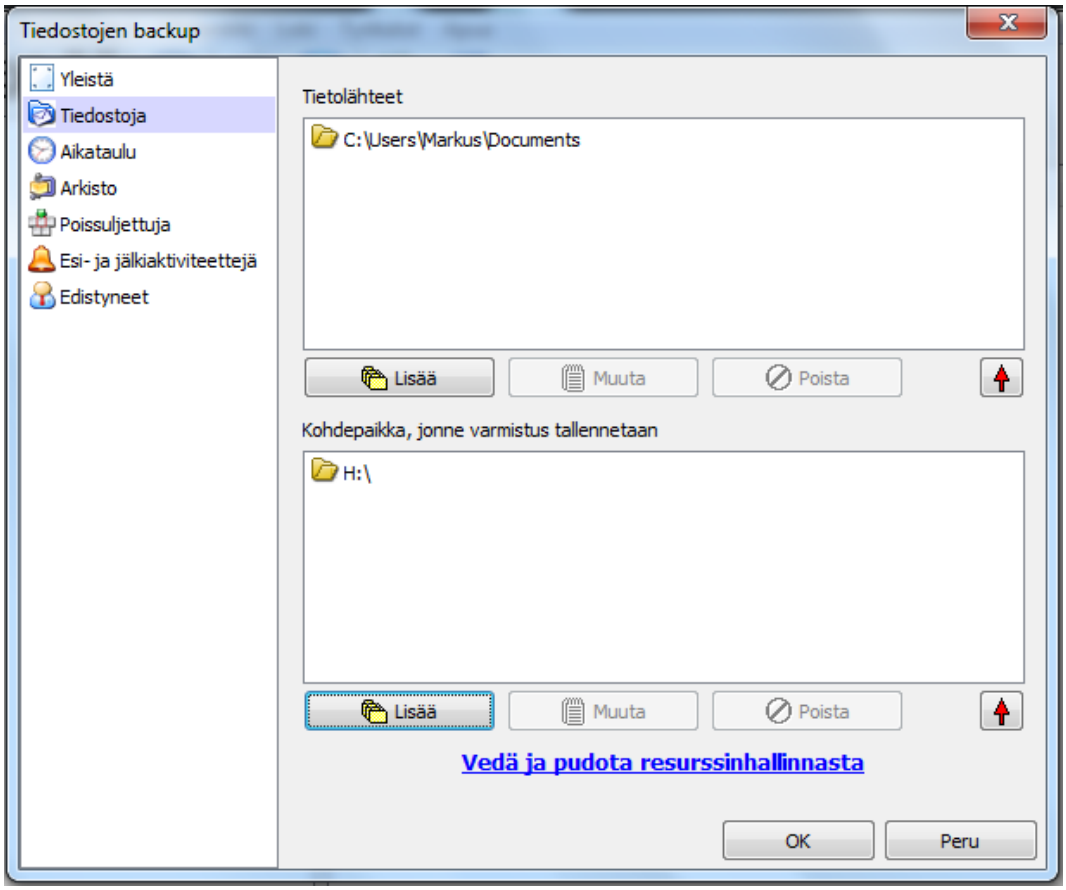


Kuva 20. RAID 5-kaavio.

9.2. Cobian-varmuuskopiointi

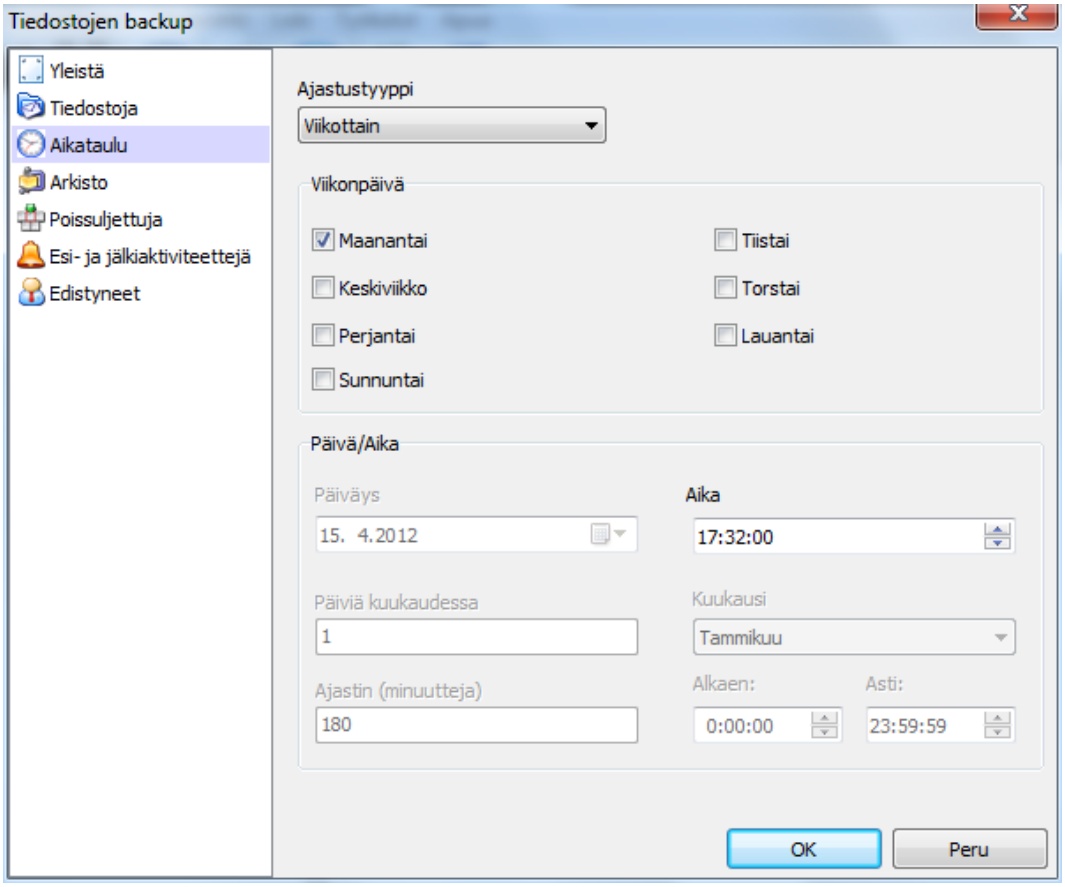
Cobian-ohjelmalla voi yritys varmuuskopioida tärkeät tiedostot helposti. Ohjelman asennuksen jälkeen Cobian pitää konfiguroida. Konfigurointi pitää tehdä vain kerran, sen jälkeen Cobian ottaa varmuuskopioinnit käyttäjän määrittämänä ajankohtana. Konfiguroinnissa käyttäjä määrittelee, mitkä kansiot ja tiedostot kopioidaan ja mihin varmuuskopio talletetaan, sekä koska varmuuskopiointi tehdään esimerkiksi joka päivä klo 17.00.

Tiedostoja-kohdasta valitaan, mitä kopioidaan ja mihin kopioidaan. Tässä tapauksessa olen valinnut, että Documents-kansio varmuuskopioidaan muistitikulle (Asema H:\ ). (Kuva 21)



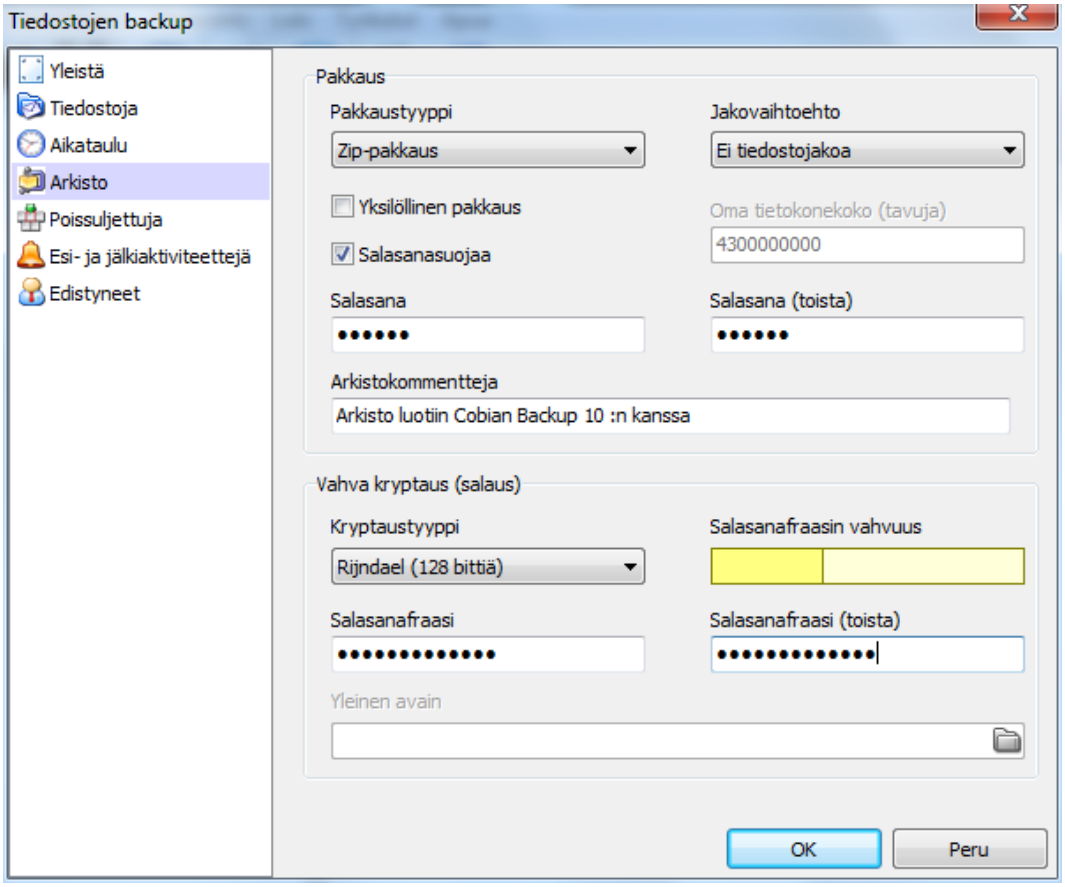
Kuva 21. Valitaan kansiot, jotka varmuuskopioidaan.

Aikataulu-välilehdeltä saadaan valita, kuinka usein varmuuskopiointi tehdään; valitsin kerran viikossa maanantaisin. Ajastustyypiksi voi valita myös esimerkiksi kerran tunnissa tai kerran kuukaudessa. Kellonajan saa myös itse määritellä. Yrityksen kannattaa määrittää kellonaika vähän sen jälkeen, kun työpäivä on loppunut. (Kuva 22)



Kuva 22. Aikataulutus varmuuskopioinnille.

Arkistovälilehdeltä voidaan valita pakkaustapa ja sille salasana sekä salaustyyppi. Salaustyyppinä on valittavana Rijndael, DES, RSA-Rijndael sekä Blowfish. Itselleni valitsin Rijndael-algoritmin ja annoin sille salasanan. (Kuva 23)



Kuva 23. Pakkaus- ja salaustyypit.

Tämän jälkeen voidaan painaa OK, jolloin Cobian kerää tiedot yhteen sivuun. Tältä sivulta näemme kaiken, mitä käyttäjä on määritellyt. Nyt Cobianin määrittely on valmis ja sen voi jättää automaattisesti ottamaan varmuuskopioita.

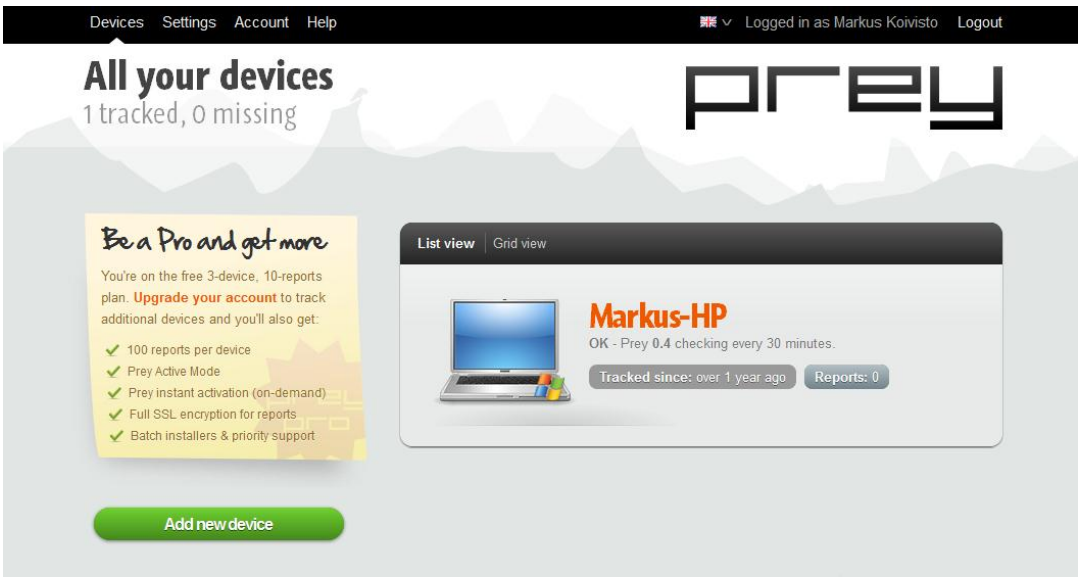
Varmuuskopion palautus Cobianilla on helppoa, koska Cobian pakkaa kaikki tiedostot, jotka varmuuskopioidaan. Palautus tapahtuu siis purkamalla varmuuskopion zip-paketti käyttäjän haluamaan kansioon. Zip-paketin purkamiseen käyttäjä tarvitsee WinZip-ohjelman.

10. Varastetun kannettavan löytäminen etäohjelmiston avulla

Työn yhtenä aiheena on tiedon suojaaminen. Sen takia esittelen tässä luvussa ohjelmiston, jonka avulla voi varastetun kannettavan yrittää löytää.

Varastetun tai hukassa olevan tietokoneen, älypuhelimen tai tablettitietokoneen voi löytää Prey-nimisen ohjelman avulla. Prey on avoimen lähdekoodin ohjelmisto. Preyn normaali asennus on ilmainen, ja sen avulla käyttäjä voi valvoa kolmea eri laitetta. (Kuva 24) Preystä on olemassa myös Pro-versio niille, jotka haluavat suojata enemmän kuin kolme laitetta. Prey Pro on maksullinen, esimerkiksi kymmenen laitteen suojaus maksaa 15 dollaria kuukaudessa. Suurin luokka on 500 laitteen suojaus, joka maksaa 399 dollaria kuukaudessa.

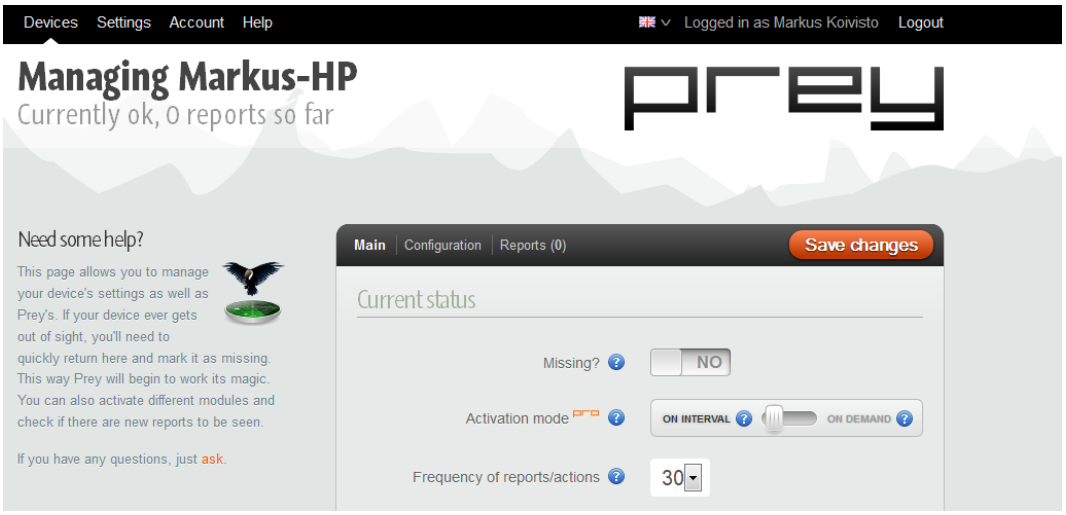
Preyn toiminta perustuu agenttiohjelman asennukseen, ja ohjelman voi asentaa tietokoneelle tai älypuhelimeen. Asennuksen jälkeen ohjelma käy koko ajan, mutta se ei kuitenkaan käytä tietokoneen resursseja juuri ollenkaan, ennen kuin se aktivoidaan internetsivulta löytyvällä ohjauspaneelilla.



Kuva 24. Lista kaikista laitteista, joita Prey:llä seurataan.

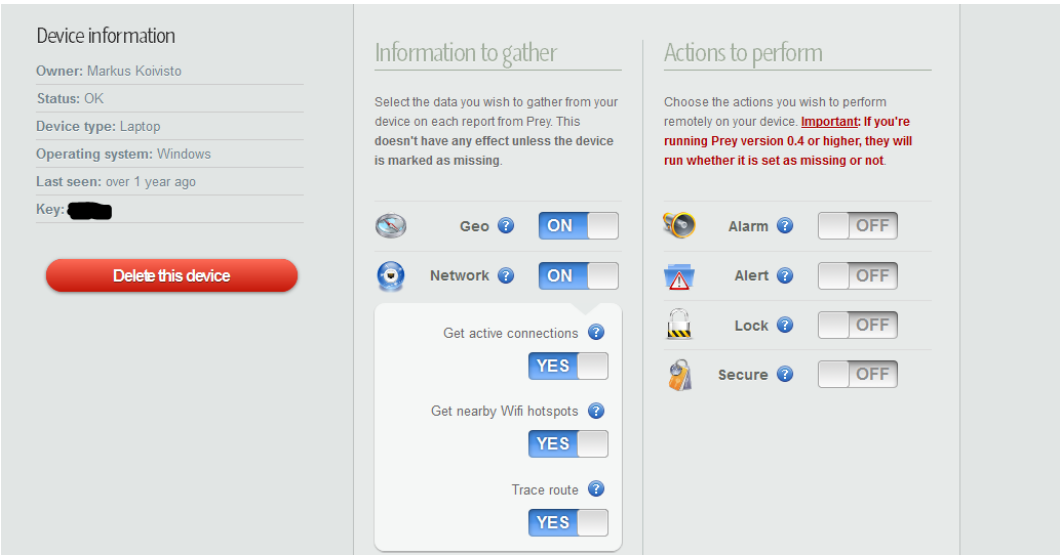
Preyn ohjauspaneelissa on monia eri toimintoja, joilla voidaan yrittää varastettu tietokone löytää. Ensiksi laite pitää merkitä kadonneeksi, tämä jälkeen Prey alkaa

keräämään tietoa kyseisestä laitteesta. Aktivointitilasta on valittuna ”on interval”-toiminto. Tämä tarkoittaa sitä, että kun Prey seuraavan kerran käynnistyy, niin se alkaa lähettämään tietoa varastetusta laitteesta. Aktivointitilan ”on demand”-toiminto on vain maksaville asiakkaille. Raporttien ja toimintojen esiintymistiheys on valittavissa aina 10 minuutista 40 minuuttiin. (Kuva 25)



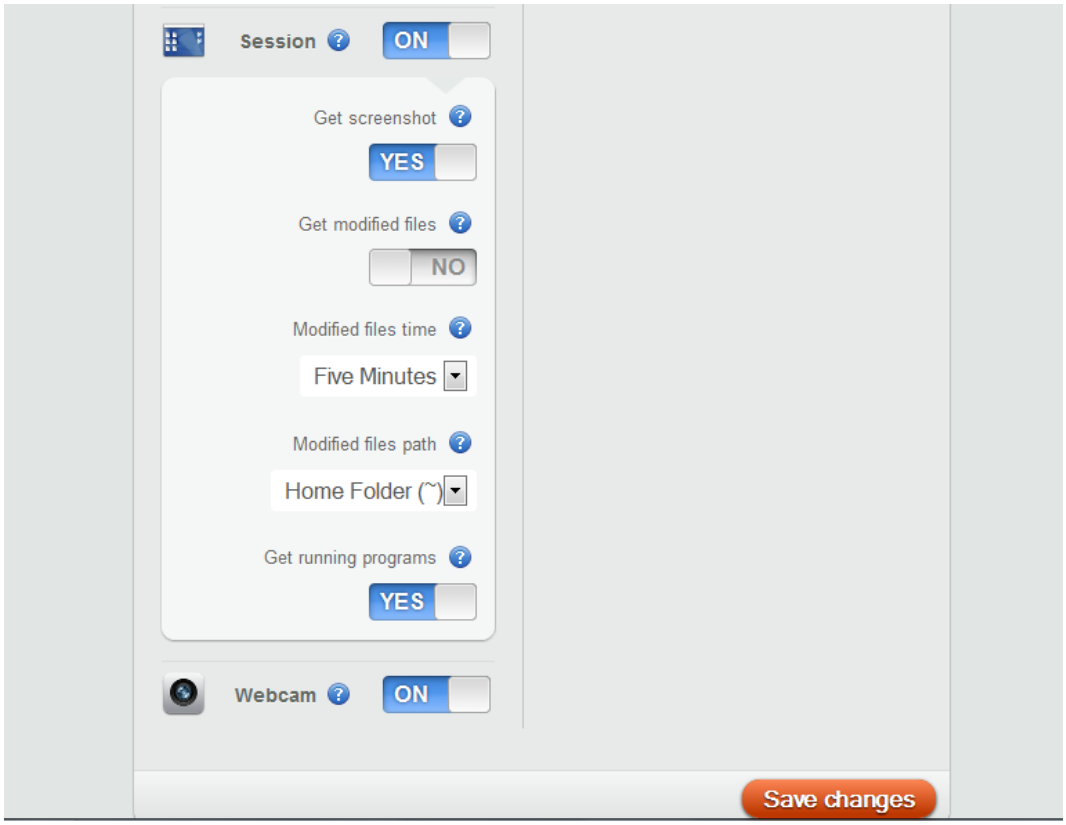
Kuva 25. Ohjauspaneelisivun yläosa.

Varastettua tietokonetta voi yrittää etsiä maantieteellisen sijainnin avulla. Prey etsii konetta sen sisäisen GPS-paikantimen avulla tai lähimmän Wi-Fi-verkon avulla. Preyn kautta voi myös lähettää koneelle erilaisia toimintoja. Hälytystoiminnon avulla tietokone pitää kovaa ääntä 30 sekunnin ajan. Varoitussignaalin avulla voidaan varkaalle näyttää viesti koneen ruudulla, tai vaihtoehtoisesti vaihtaa taustakuvaa. Lukituksen avulla tietokone voidaan kokonaan lukita, kunnes annetaan oikea salasana. Salasanan saa itse määrittää Preyn ohjauspaneelissa. Suojaustoiminnolla voidaan piilottaa sähköpostit, tuhota selaimen cookiet ja salasanat kaikilta käyttäjiltä. (Kuva 26)



Kuva 26. Ohjauspaneelisivun keskikohta.

Istunto kerää tietoa sekä ottaa kuvakaappauksen työpöydästä. Muutetuista tiedostoista saadaan myös tehtyä lista. Listan päivitystiheyttä voidaan muuttaa: se voi olla viisi minuuttia, kolmekymmentä minuuttia, yksi tunti tai kolme tuntia. Ohjauspaneelissa pitää myös määritellä, mitä kansiota seurataan. Käytössä olevista ohjelmista saadaan myös tehtyä listaus. Web-kameralla voidaan yrittää ottaa varkaasta kuva olettaen, että tietokoneessa on kamera. (Kuva 27) (Fork Ltd. 2012)



Kuva 27. Ohjauspaneelisivun alareuna.

11. Johtopäätökset

Kannettavien laitteiden tietoturva on nykypäivänä hyvällä tasolla. Käyttäjältä ei vaadita erityisosaamista tiedon turvassa pitämisessä. Tietoturva on rakennettu laitteen perustoiminnoksi ja mahdollisimman helpoksi käyttää. Nykyään kaikki laitteet ovat jo niin tehokkaita, ettei salausta ja salauksen purkamista edes huomaa. AES on tällä hetkellä erittäin suosittu salausalgoritmi, se on vielä turvallinen, mutta aika näyttää kuinka kauan.

Langattomat verkot jatkavat kasvuaan vuosi toisensa perään. Niiden tuoma helppokäyttöisyys ja liikunnallinen vapaus on tehnyt niistä korvaamattomia. Langattomia verkkoja päivitetään koko ajan nopeammiksi ja turvallisimmiksi, viimeisin standardisoitu laajennus on 802.11n. 802.11n standardoitiin syyskuussa 2009, ja se on tällä hetkellä nopein langaton verkkostandardi. Langattomat verkot ovat turvallisia, jos ne on suojattu WPA2-suojauksella. WPA2 on tänä päivänä turvallisin salausmenetelmä.

Jokaisen työntekijän pitäisi osata olla tietoturvan kannalta varovainen. Yrityksen sisäverkko voi olla hyvin suojattuna ulkoisilta uhilta, mutta se pystytään ohittamaan jos työntekijä käyttää esimerkiksi muistitikkua työnsä teossa. Kotoa tuotu muistitikku voi sisältää jonkun haittaohjelman, ja kun sen liittää työpaikan tietokoneeseen, niin muuten turvallinen verkko on nyt ohitettu ja pahimmassa tapauksessa saastutettu haittaohjelmalla.

Tietoturva on erittäin laaja alue, sen päivittäminen on tärkeää. Työpaikoilla pitää työntekijät kouluttaa tietoturvan eri osioihin. Näin saadaan parannettua yrityksen sisäistä tietoturvaa. Pitää myös muistaa, että vaikka langattomat verkot ovat käyttäjäystävällisiä, on langallinen verkko silti se paras vaihtoehto tietoturvan kannalta.

Tiedostojen salaus ja etenkin varmuuskopiointi on yksi tärkeimmistä asioista, joita yrityksessä voidaan tehdä. Varmuuskopiointi on myös hyvä opetella kotioloihin, sillä kadotettu tieto on aina kallista, jos ei rahallisesti niin ajallisesti. Varmuusko-

piointi on siinä mielessä helppoa, että kun varmuuskopiointiohjelman on kerran konfiguroinut, niin se voidaan jättää tulevaisuudessa automaattisesti ottamaan varmuuskopioita. Netistä löytyy monia eri varmuuskopiointipalveluita, joista käyttäjä maksaa vain tarvitsemastaan kovalevytilasta. Koneella oleva korvaamaton tieto on myös hyvä salata esim. AES-salauksella.

Etätyönteko kotoa on nykypäivää, joten VPN-yhteyden suojaus on tärkeä asia. Vaikkakin VPN-yhteys on salattu, niin tietokone kannattaa suojata palomuurilla ja virustutkalla mahdollisia uhkia varten.

12. LÄHTEET

Kirjat

Hakala M. Vainio M. & Vuorinen O. (2006). *Tietoturvallisuuden käsikirja.* Porvoo: Docendo Finland Oy.

Heljaste J.-M. (2008). *Yrityksen turvallisuusopas.* Helsinki: Gummerus Kirjapaino Oy.

Holttinen J. (2002). *Ciscon verkkoakatemia - 1. vuosi.* Helsinki: Edita Publishing Oy.

Holttinen J. (2002). *Ciscon verkkoakatemia - 2. vuosi.* Helsinki: IT Press.

Hovatta T. Kiviniemi J. & Somiska J. (2005). *WLAN-tekniikat ja -käyttösovellukset toimitilakiinteistössä.* Espoo: Sähkötieto ry.

Kerttula E. (1998). *Tietoverkkojen tietoturva.* Helsinki: Liikenneministeriö.

Laaksonen M. Nevasalo T. & Tomula K. (2006). *Yrityksen Tietoturvakäsikirja.* Helsinki: Oy Nordprint Ab.

Miettinen J. E. (1999). *Tietoturvallisuuden johtaminen.* Helsinki: Kauppakaari Oyj ja Juha E. Miettinen.

Elektroniset julkaisut

Adrio Communications Ltd. (2012). *Radio-Electronics*. Haettu 15. Huhtikuu 2012 osoitteesta IEEE 802.11 standards tutorial: http://www.radio-electronics .com/info/wireless/wi-fi/ieee-802-11-standards-tutorial.php

Apple Inc. (2012). *iPhone in Business: Secure your data.* Haettu 19. Maaliskuu 2012 osoitteesta iPhone in Business: http://images.apple.com /iphone /business/docs/iOS_Security.pdf

Bluetooth SIG, Inc. (2012). *How It Works*. Haettu 28. Huhtikuu 2012 osoitteesta Fast Facts: http://www.bluetooth.com/Pages/Fast-Facts.aspx

Bluetooth SIG, Inc. (2012). *How It Works*. Haettu 28. Huhtikuu 2012 osoitteesta Bluetooth Basics: http://www.bluetooth.com/Pages/Basics.aspx

Cisco Systems Inc. *Authentication Protocols*. Haettu 4. Huhtikuu 2012 osoitteesta How Does RADIUS Work?: http://www.cisco.com /en/US /tech /tk59 /technologies_tech_note09186a00800945cc.shtml

Cisco Systems Inc. *Wireless, LAN (WLAN).* Haettu 4. Huhtikuu 2012 osoitteesta Wi-Fi Protected Access 2 (WPA 2) Configuration Example: http://www.cisco.com/en/US/tech/tk722/tk809/technologies_configuration _example09186a008054339e.shtml

Cryptography World. (2012). *Cryptographic Algorithms*. Haettu 14. Huhtikuu 2012 osoitteesta RSA: http://www.cryptographyworld.com/rsa.htm

Dell Inc. *Support Home Page*. Haettu 4. Huhtikuu 2012 osoitteesta 802.1x-laillisuustarkistus: http://support.dell.com/support /edocs/network/P94583 /fin/security.htm

Fork Ltd. (2012). *Prey, a project by Fork Ltd.* Haettu 17. Maaliskuu 2012 osoitteesta Prey: http://preyproject.com/

F-Secure Oyj. *F-Secure Mobile Security*. Haettu 17. Maaliskuu 2012 osoitteesta Mobile Security yleistä: http://www.f-secure.com/fi/web /home_fi /protection/mobile-security/overview

nternet-Computer-Security.com. (2012). *Computer Security Guide for Home and Network Users*. Haettu 10. Huhtikuu 2012 osoitteesta DES tutorial - VPN Encryption explained: http://www.internet-computer-security.com/VPN-Guide/DES.html

Microsoft Inc. (21. Tammikuu 2005). *IPSec Protocol Types*. Haettu 28. Huhtikuu 2012 osoitteesta Transport mode: http://technet.microsoft.com/en-us /library/cc739674%28v=ws.10%29.aspx

Microsoft Inc. (21. Tammikuu 2005). *IPSec Protocol Types*. Haettu 28. Huhtikuu 2012 osoitteesta Tunnel mode: http://technet.microsoft.com/en-us /library /cc737154%28v=ws.10%29.aspx

Microsoft Inc. (2012). *Networking and Access Technologies*. Haettu 20. Huhtikuu 2012 osoitteesta IPsec: http://technet.microsoft.com/en-us/network /bb531150

Microsoft Inc. (2012). *Planning to Install Windows NT Server*. Haettu 20. Huhtikuu 2012 osoitteesta Understanding PPTP (Windows NT 4.0): http://technet.microsoft.com/en-us/library/cc768084.aspx

QuinStreet Inc. (2012). *Implementing Encrypted SQL Server Database Columns with .NET*. Haettu 8. Toukokuu 2012 osoitteesta Introducing AES Encryption: http://www.devx.com/dbzone/Article/26726/0/page/2

QuinStreet Inc. (2012). *Webopedia*. Haettu 21. Huhtikuu 2012 osoitteesta RAID: http://www.webopedia.com/TERM/R/RAID.html

Tech-FAQ. (2012). Haettu 19. Maaliskuu 2012 osoitteesta Tech-FAQ: http://www.tech-faq.com/ssid.html

TechTarget. (2012). *EnterpriseWAN Topics*. Haettu 20. Huhtikuu 2012 osoitteesta Layer Two Tunneling Protocol (L2TP): http://searchenterprisewan.techtarget.com/definition/Layer-Two-Tunneling-Protocol

TechTarget. (2012). *Security Resources*. Haettu 20. Huhtikuu 2012 osoitteesta SSL VPN (Secure Sockets Layer virtual private network): http://searchsecurity.techtarget.com/definition/SSL-VPN

Tippit Inc. (5. Huhtikuu 2007). *Featured Articles*. (C. Waxer, Toimittaja) Haettu 16. Huhtikuu 2012 osoitteesta Moving to SSL VPN: http://www.itsecurity.com/features/beyond-ipsec-move-sslvpn-040507/

Tropical software. (20. Huhtikuu 2012). *des3p1.gif*. http://www.tropsoft.com/strongenc/des3.htm.

TrueCrypt Developers Association. (14. Helmikuu 2012). *TrueCrypt: Free open-source disk encryption software for Windows 7/Vista/XP, Mac OS X, and Linux*. Haettu 19. Maaliskuu 2012 osoitteesta TrueCrypt -sivusto: http://www.truecrypt.org/

Viestintävirasto. (27. Syyskuu 2007). *Tietoturva ja -suoja*. Haettu 21. Huhtikuu 2012 osoitteesta Salausmenetelmät: http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/salausmenetelmat/symmetrinensalaus.html

VOCAL Technologies Ltd. (2012). *Cryptography*. Haettu 10. Huhtikuu 2012 osoitteesta Advanced Encryption Standard (AES): http://www.vocal.com/cryptography/aes.html

VOCAL Technologies, Ltd. (2012). *Cryptography*. Haettu 10. Huhtikuu 2012 osoitteesta Data Encryption Standard (DES): http://www.vocal.com/cryptography/des.html