TUNNELOITU LÄHIVERKKO

YRITYKSEN IP-KAMERAVALVONTA

LAHDEN AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma
Tietoliikennetekniikan suuntautumisvaihtoehto

Opinnäytetyö

Kevät 2007

Aleksi Manninen

LAHDEN AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma
Aleksi Manninen: Tunneloitu lähiverkko
Tietoliikennetekniikan opinnäytetyö 42 sivua
Kevät 2007

TIIVISTELMÄ

Opinnäytetyössä tutkittiin mahdollisuuksia suojatun tunnelin luomiseksi internetin yli. VPN-tunneli tarvittiin Riimikko Ay:n liikekiinteistön IP-kameravalvontajärjestelmän etähallintaa varten.

Etäyhteys voidaan luoda monin eri keinoin. On olemassa erilaisia VPN-reitittimiä ja ohjelmistoja. Opinnäytetyössä keskityttiin ohjelmallisten VPN-ratkaisujen salaus- ja tunnistusmenetelmiin. VPN-tunnelointiprotokollat eroavat toisistaan paketointi- ja salausratkaisujen puolesta.

PPTP on eri valmistajien yhteystyönä kehitetty VPN-ratkaisu. PPTP on vanha protokolla, joka ollut käytössä jo yli kymmenen vuotta. Salaus PPTP:ssa on hoidettu Microsoftin muunnelmalla RC4-salauksesta ja todennukseen voi käyttää salaamatonta käyttäjätunnussalasanaparia tai kehittyneempiä avaimen vaihtomenetelmiä, joissa vaihdetaan hajautusalgoritmeilla tuotettuja tiivistelmiä avaimista eikä itse avaimia. IPsec on IP-liikenteen suojaamisen tarkoitettu arkkitehtuuri. IPsec ei määrittele salaukseen ja avaimen vaihtoon käytettäviä algoritmeja vaan se määrittelee ainoastaan tavan, miten salattu data kapseloidaan.

VPN-protokollaksi valittiin PPTP, joka asennettiin Linux-palvelimeen, ja yhteys järjestelmään voidaan ottaa Windowsin omalla PPTP-asiakasohjelmalla. Järjestelmä on varmatoiminen, halpa ja helposti muokattavissa.

Avainsanat: VPN, tunnelointi, PPTP, IPsec, etähallinta, etäkäyttö

LAHDEN AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma
Aleksi Manninen: Tunneled local area network
Bachelor's thesis on information technology 42 pages
Spring 2007

ABSTRACT

This thesis researched possibilities for secure tunnels over the Internet. A confidential tunnel was needed to control remotely Riimikko store's surveillance system.

These private channels can be created in many different ways. For instance many vendors provide VPN routers and software companies like Microsoft offer VPN client softwares. In this thesis was concentrated in VPN softwares and their encrypting algorithms and encapsulations.

PPTP is the first VPN solution that uses the Internet to transfer confidential information securely. It was created by vendor consortium. PPTP relies on RC4 encrypting algorithm and authentication can be made with a insecurely transferred password or with a message digest that is created by an hash algorithm. IPsec is a architecture that is created to secure IP traffic. It doesn't define algorithms or protocols which should be used to encrypt information and authenticate the tunnel's end-points. IPsec however defines how encrypted messages must be encapsulated.

PPTP was selected the protocol to be used to create VPN. PPTP server was installed on Linux-server and it could be contacted with the PPTP client software that comes with Windows operating systems. The system is stable and cheap and modified easily.

Key words: VPN, tunneling, PPTP, IPsec, remote control, remote use

SISÄLLYS

LYHENNELUETTELO

ADSL	Asymmetric Digital Subscriber Line, laajakaistatekniikka
AES	Advanced Encyption Standard, vahva salausstandardi
AH	Authentication Header, paketin autentikointi standardi
ASCII	American Standard Code for Information Interchange
ATM	Asynchronous Transfer Mode, tietoliikennejärjestelmä
CHAP	Challenge-Handshake Authentication Protocol, autentikointiprotokolla
DES	Data Encryption Standard, salausprotokolla
DNS	Domain Name System, nimipalvelujärjestelmä
EFF	Electronic Frontier Foundation, tietotekniikan etujärjestö
ESP	Encapsulating Security Payload, salausprotokolla
FTP	File Transfer Protocol, tiedonsiirtoprotokolla
GRE	Generic Routing Encapsulation, kapselointistandardi
HMAC	keyed-hash message authentication code, protokolla tiivistealgoritmien käyttöön
HTML	Hypertext Markup Language, linkitykseen pystyvä tekstin kuvauskieli
ICV	Integrity Check Value, eheyden tarkistus arvo ESP-paketeissa
IETF	The Internet Engineering Task Force, standardointijärjestö
IKE	Internet Key Exchange, salausavaimen vaihtoprotokolla
IP	Internet Protocol, pakettipohjainen tiedonsiirtoprotokolla
IPsec	IP security architecture, VPN-protokolla
IPv6	IP version 6, IP:n uusi versio
JPG	Joint Photographic Group, häviöllinen kuvaformaatti
Kbps	Kilo bits per second, tietoliikennenopeuden mittäyksikkö
L2TP	Layer 2 Tunneling Protocol, tunnelointiprotokolla
MB	Mega Byte, tietotekniikan tilayksikkö
Mbps	Mega Byte per second, tietoliikennenopeuden mittayksikkö
MD5	Message Digest 5, tiivistealgoritmi
MPPE	Microsoft Point-to-Point Encryption, salausmenetelmä
MS-CHAPv1	Microsoft CHAP version 1, autentikointiprotokolla
MS-CHAPv2	Microsoft CHAP version 2, autentikointiprotokolla
NAPT	Network Address and Port Transfer, osoitteen muuntostandardi
PAP	Password Authentication Protocol, autentikointistandardi
PC	Personal Computer, tietokone
PPP	Point-to-Point Protocol, Tunnelointiprotokolla
PPTP	Point-to-Point Tunneling Protocol, VPN-protokolla
RC4	Rivest Chiper 4, salausalgoritmi
RFC	Request For Comment, standardointidokumentti
RSA	Rivest Shamir Adleman, salausalgoritmi ja tietoturvayritys
SA	Security Association, kahden laitteen välinen turvallisuusinformaatio
SHA	Secure Hash Algorithm, tiiviste-algoritmi
TCP	Transmission Control Protocol, tiedonsiirtoprotokolla
WLAN	Wireless Local Area Network, Langaton lähiverkko
VPN	Virtual Private Network, Turvallinen verkko internetin yli
WWW	World Wide Web, internet-palvelimien muodostama järjestelmä

1 JOHDANTO

Riimikko on yli 20 vuotta Vanhassa Porvoossa toiminut lahjatavaraliike. Yritys myy mm. miniatyyrejä, retroleluja, nukkekoteja ja niiden kalusteita. Koska kyseessä on pieni perheyritys, ei varkaudenesto- eikä valvontakameralaitteistoja ole ollut aiemmin varaa eikä myyntiartikkeleiden jälleenmyyntiarvon vuoksi ole ollut tarvetta hankkia. Yrityksen omistajien mukaan yleisimmin liikkeestä häviää alle 5 euron esineitä, mutta liikkeessä myydään myös useiden satojen eurojen arvoisia esineitä. Tästä näpistelystä haluttiin nyt päästä eroon ja päädyttiin tallentavien valvontakameroiden hankintaan, joista pystyttäisiin seuraamaan hyllystä häviävää tavaraa ja pelottelemaan näpistelijöitä. Kamerat myös ennalta ehkäisevät ryöstöjä.

Valvonta ja tallennus haluttiin täysin automaattiseksi ja vikasietoiseksi ja videota piti voida tarkastella reaaliaikaisesti niin paikan päällä kuin etänäkin. Järjestelmän laitteistokustannukset haluttiin pitää mahdollisimman pieninä. Järjestelmä oli saatava myös mahdollisimman helpoksi huoltaa ja päivitykset haluttiin automaattiseksi.

Ongelmana oli, miten tallennus ja etävalvonta saataisiin suoritettua mahdollisimman halvalla, turvallisesti ja käyttäjäystävällisesti. Opinnäytetyö tutki mahdollisuuksia kameroiden reaaliaikaiseen seuraamiseen ja tallentuneiden valvontakuvien tarkasteluun etänä.

Idea valvonnan järjestämisestä liikkeeseen ei ole uusi, vaan sitä on pohdittu usean vuoden ajan. Itse ehdotus valvonnan ja siihen liittyvän etäyhteyden toteuttamiselle tuli syksyllä 2006 ja valvonnan toivottiin olevan käytössä ennen seuraavaa liikkeen kesäruuhkaa, jonka aiheuttavat luokkaretkeläiset ja turistit.

2 VPN

2.1 Yleiskuvaus

VPN (Virtual Private Network) on tekniikka, jolla pystytään yhdistämään fyysisesti erillisiä IP (Internet Protocol) -lähiverkkoja ja työasemia toisiinsa turvallisesti ulkoisen verkon yli. VPN sana on käytössä myös muissa kuin IP-verkoissa, kuten ATM- (Asynchronous Transfer Mode) ja Frame Relay -verkoissa, mutta opinnäytetyössä keskityttiin vain IP-verkkojen VPN-yhteyksiin, koska kaikki tarvittavat sovellukset ja verkot toimivat IP-pohjaisesti (Perlmutter & Zarkower 2001, 11).

> VPN on tietoliikenneverkko, joka on rakennettu yrityksen yksityiseen käyttöön jaetun julkisen infrastruktuurin välityksellä. Tämä määritelmä kattaa kaksi ensisijaista sovellusta: etäyhteydet ja eri toimipaikkojen väliset yhteydet. (Perlmutter & Zarkower 2001, 10.)

Yksityinen käyttö tarkoittaa käytännössä sitä, että liikenne VPN:n sisällä tapahtuu salattuna ja todennettuna. Verkon laitteiden ja käyttäjien on pystyttävä luottamaan siihen, ettei liikennettä muuteta tai salakuunnella. Tämä onnistuu vain vahvalla salauksella, käyttäjän tunnistuksella ja informaation eheyden varmistamisella.

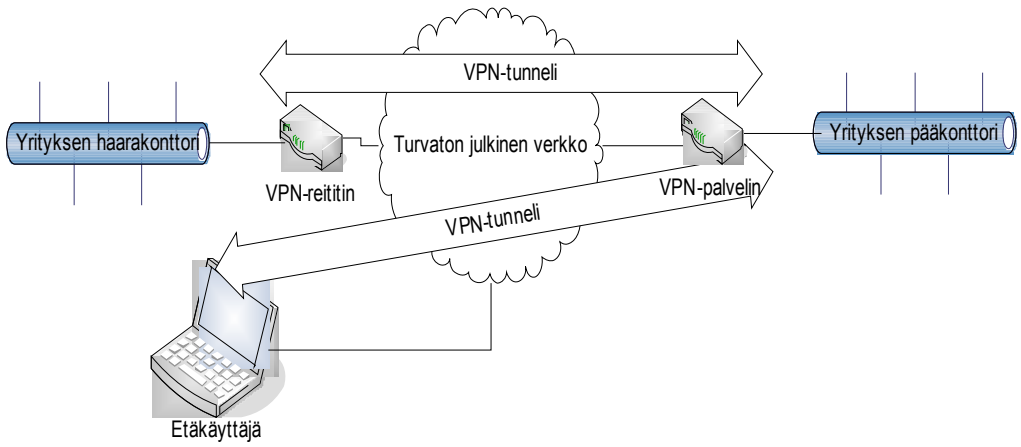
2.2 VPN -tyypit

VPN -yhteydet voidaan luoda monella tavalla ja moneen eri tarkoitukseen. Useat valmistajat tarjoavat VPN-palomuurilaitteistoja, joihin voidaan ottaa yhteys toisella VPN-palomuurilaitteella tai VPN-ohjelmistolla. Useat ohjelmistoyritykset tarjoavat myös täysin ohjelmallisia VPN-ratkaisuja. Kaikissa ratkaisuissa on yhteistä käyttäjän tunnistus ja salattu liikenne päätepisteiden välillä.

Laitteisto-VPN:n hyötynä on toimintavarmuus, keskitetty hallinta, käyttäjälle läpinäkyvyys ja muiden resurssien säästäminen(Perlmutter & Zarkower 2000, 91). Laitteisto-VPN haittana on usein hinta ja asiakkaan riippuvuus yhdestä laitteistotoimittajasta.

Ohjelmisto-VPN:n hyötynä on laaja levinneisyys, joka johtuu paljolti siitä että Microsoft on liittänyt käyttöjärjestelmiinsä tuen PPTP (Point-to-Point Tunneling Protocol) ja IPsec (Internet Protocol security architecture) protokollille (Perlmutter & Zarkower 2000, 115). Ohjelmallisesti tuotettu VPN on helposti käytettävissä ympäri maailmaa, koska siinä ei tarvita erillistä laitetta hoitamaan yhteyden muodostusta ja salausta. Etätyöntekijän tarvitsee vain tunnistautua VPN-palvelimelle.

VPN-yhteyksien käyttö voidaan karkeasti jakaa kahteen osaan: yksittäisen laitteen liittäminen yrityksen verkkoon ja yrityksen haarakonttorien yhdistäminen. Yleensä haarakonttorien yhdistämiseen käytetään kahta VPN-reititintä, kun yksittäisen laitteen ja konttorin verkon yhdistämiseen käytetään VPN -ohjelmaa ja VPN-reititintä tai -palvelinta. Näitä tunnelityyppejä voidaan käyttää myös samanaikaisesti (KUVIO 1).



KUVIO 1. VPN-tunnelityypit

2.3 Autentikointi ja datan eheys

Jotta VPN -tunneli voidaan rakentaa, on VPN-palvelimen pystyttävä tunnistamaan yhteyden pyytäjät. Autentikointiin eli tunnistukseen voidaan käyttää eri menetelmiä, jotka voidaan jakaa viiteen kategoriaan:

1. Mitä käyttäjällä on (esim. älykortti, avain)?
2. Mitä käyttäjä tietää (esim. salasana)?
3. Mitä käyttäjä on (esim. sormenjälki, iiris)?
4. Mitä käyttäjä tekee (esim. allekirjoitus, kirjoitustyyli)?
5. Missä käyttäjä on (esim. päätelaite, satelliittipaikannus)?

Vahvaksi tunnistusta voidaan sanoa jos käytetään vähintään kahta kategoriaa samanaikaisesti. Esimerkiksi käyttäjä tunnistautuu laitteelle sormenjäljellään ja salasanalla. (Gollman, D. 1999, 26-28.)

Kolmannet osapuolet voivat muuttaa viestiä, jos viestien eheyttä ei varmisteta millään tavoin. Viestien eheys voidaan varmistaa muodostamalla viestistä tiivistelmä ja salaamalla se (katso 2.4). Tiivistelmien tekoon käytetään hajautusalgoritmeja, jotka pystyvät tekemään mistä tahansa merkkijonosta (esim. tekstin pätkä) tietyn mittaisen summan. Esimerkiksi suosittu hajautusalgoritmi MD5 (Message Digest algorithm 5) tuottaa mistä tahansa merkkijonosta 128 bittisen tiivistelmän (Schneider, B. 1996, 436). Tiivistelmä on helppo luoda ja se on aina samanlainen, mutta muodostetusta tiivistelmästä on erittäin vaikea palauttaa alkuperäistä tekstiä. Esimerkiksi sanan ”cat” MD5-tiivistelmä on heksakoodattuna ”d077f244def8a70e5ea758bd8352fcd8” (Wikipedia, 2007a). Toinen yleisesti käytetty hajautusalgoritmi on SHA-1 (Secure Hash Algorithm). Kuten muussakin tietoturvassa, mikään tekniikka ei ole veden pitävää ja uusia hajautusalgoritmeja kehitellään koko ajan ja esimerkiksi SHA:sta on tullut jo useita uusia versioita kuten SHA-256, SHA-384 ja SHA-512 (National Institute of Standards and Technology 2002, 3).

PAP (Password Authentication Protocol) on yksinkertainen salasana-käyttäjätunnus -autentikointimetodi, jossa palvelimelle lähetetään käyttäjätunnukset ja salasanat selkokielisenä ASCII-merkkijonoina (American Standard Code for Information Interchange). Tämä autentikointimetodi on erittäin turvaton, koska kolmannet osapuolet voivat kaapata autentikointiviestit verkosta ja näin saavat suoraan käyttäjätunnuksen ja salasanan.

CHAP (Challenge-Handshake Authentication Protocol) on kolmiosainen autentikointiprotokolla. Alustavan yhteyden jälkeen palvelin lähettää autentikointihaasteen päätelaitteelle, johon päätelaite vastaa salasanasta tuotetulla tiivistelmällä. Jos palvelimen vastaanottama tiivistelmä vastaa palvelimella olevaa salasanaa, vastaa palvelin päätelaitteelle yhteyden hyväksymisestä. Jos tiivistelmä on väärä, vastataan yhteyden hylkäämisellä.

MS-CHAP (Microsoft Challenge-Handshake Authentication Protocol) on Microsoftin muunnelma CHAP protokollasta. MS-CHAP:sta löydettyjen haavoittuvuuksien vuoksi nykyisin suositellaan käytettäväksi MS-CHAP:n versiota 2. Microsoftin uudesta käyttöjärjestelmästä, Windows Vistasta, on otettu pois MS-CHAPv1 -tuki (Microsoft, 2007a).

MS-CHAPv2 viesteissä kulkeva informaatio:

1. tunnistajan haaste: session tunnistenumero ja haastemerkkijono
2. tunnistettavan tiivistevastaus: käyttäjätunnus, vertaishaastemerkkijono sekä haastemerkkijonosta, session tunnistenumerosta ja salasanasmerkkijonosta muodostettu tiiviste
3. tunnistajan vastaus: hylkäys- tai hyväksymisvastaus sekä autentikoitu vastaus joka on muodostettu haastemerkkijonosta, vertaishaastemerkkijonosta ja asiakkaasta ja salasanasmerkkijonosta.

Tunnistaja laskee vielä tunnistajan vastauksesta onko tunnistaja oikea ja jatkaa tai sulkee yhteyden sen mukaan. (Microsoft, 2007b.)

HMAC (Keyed-Hashing for Message Authentication) on autentikointiprotokolla, joka käyttää CHAP:n tavoin hajautusalgoritmia tunnistukseen. HMAC muokkaa tiivisteen ulkopuolisesta salasanasta ja ulkopuolisen hajautusalgoritmin tuottamasta tiivisteestä. Tämä ulkopuolinen tiiviste voi olla tehty millä vain hajautusalgoritmilla, kuten SHA-1:lla tai MD5:llä. Jotta tiedettäisiin mitä hajautusalgritmia missäkin HMAC-sovelluksessa käytetään, on sovittu, että hajautusalgoritmi mainitaan protokollan perässä (esimerkiksi HMAC-MD5). (RFC 2104 1997, 2-6.)

2.4 Salaus

2.4.1 Salaus VPN-yhteyksissä

VPN-yhteydet muodostetaan julkisen verkon yli, josta on mahdollista kaapata ohikulkevia viestejä, joten pelkkä käyttäjän tunnistus ei riitä takaamaan turvallista tiedonsiirtoa. Turvallinen tiedonsiirto pystytään takaamaan hyvällä tunnistuksella ja vahvalla salauksella. Vahvan salauksen määritelmä muuttuu sitä mukaa kun edellisiä salausmenetelmiä murretaan. Salausmenetelmät voidaan jakaa kahteen kategoriaan niiden salauksen ja salauksen purun tapojen mukaan: symmetrisen avaimen ja julkisen avaimen algoritmeihin.

2.4.2 Symmetrisen avaimen salausmenetelmät

Symmetriset lohkosalaimet jakavat selkokielisen datan lohkoihin, jotka jokainen muutetaan salakieliseksi monimutkaisten matemaattisten operaatioiden avulla. Symmetriseksi salauksen tekee se että samalla avaimella voidaan salata ja purkaa salaus. Tunnetuimmat symmetrisen avaimen lohkosalaimet ovat DES (Data Encryption Standard), DES:n kehitelty versio 3DES ja AES (Advanced Encryption Standard).

DES jakaa datan 64-bitin lohkoihin, ja myös sen avaimen pituus on 64 bittiä. Avaimen 64 bitistä vain 56 bittiä käytetään algoritmissa, loput 8 bittiä on virheen tarkistusta varten. 1970-luvulla standardoitu DES-salaus on murrettu julkisesti useaan otteeseen, eikä sitä pidetä enää vahvana salauksena. EFF (Electronic Frontier Foundation) mursi ensimmäisenä DES-salauksen julkisesti vuonna 1998. DES:n jatkokehitetty versio 3DES on vielä murtamatta. 3DES on käytännössä kolme peräkkäistä DES -salainta peräkkäin. (Gollman, D. 1999, 212-214; RFC 4772 2006, 2.)

AES on DES:n korvaaja Yhdysvaltojen hallinnon lohkosalaimena. AES käyttää Rijndael-algoritmia salauksessa. Lohkojen koko on 128 bittiä, ja avain voi olla 128, 192 tai 256 bittinen. Yhdysvallat on pitänyt AES-salausta murtamattomana, ja kesäkuussa 2003 National Security Agency ilmoitti että AES-salausta käytetään salaisten ja erittäin salaisten asiakirjojen salausmenetelmänä (CNSS 2003, 2).

Lohkosalaimien vastakohtana on jonosalaimet, jotka eivät kokoa informaatiota salattaviin lohkoihin vaan salaavat datan suoraan. Tunnetuimpia ja käytetyimpiä jonosalaimia on Ron Rivestin vuonna 1987 RSA (Rivest, Shamir, Adleman) Security Inc.:lle kehittämä RC4 (Rivest Chiper 4). RC4 on noin kymmenen kertaa nopeampi salausmenetelmä kuin DES. Salausalgoritmi oli liikesalaisuus vuoteen 1994 asti, kunnes se vuoti julkisuuteen ja nykyään se on vapaassa

käytössä. RC4:sta käytetään muun muassa MPPE (Microsoft Point-to-Point Encryption), SSH (Secure Shell) ja WPA (Wi-Fi Protected Access)-salauksessa. (Schneier, B. 1996, 397-398.)

2.4.3 Julkisen avaimen salausmenetelmät ja avainten vaihto

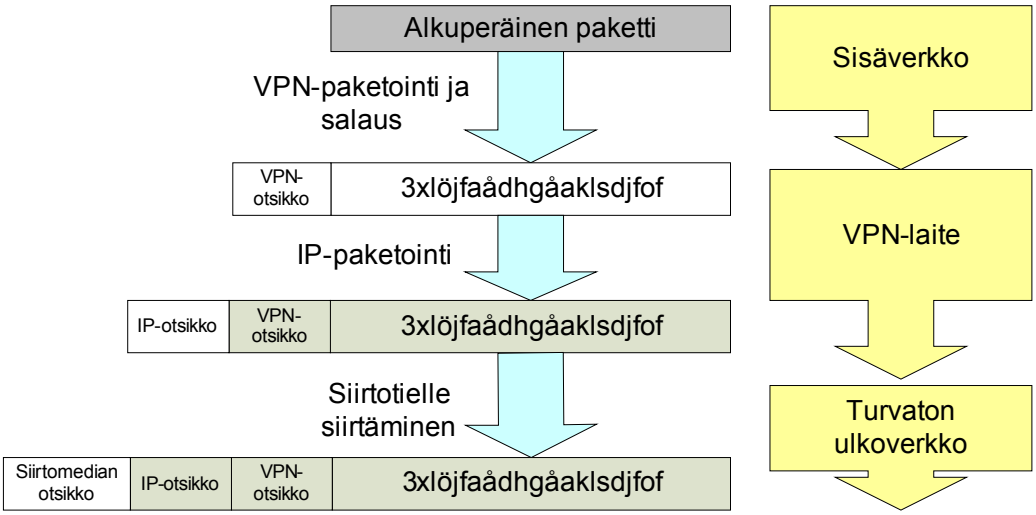
Vuonna 1976 Whitfield Diffie, Martin Hellman ja Ralph Merkle kehittivät salausmenetelmän jonka nimeksi vakiintui Diffie-Hellman. Tämä oli ensimmäinen käytännöllinen julkisen avaimen salausmenetelmä. Toisinaan julkisen avaimen algoritmeja kutsutaan epäsymmetrisen avaimen algoritmeiksi, mikä johtuu salauksen luonteesta. Salattava data suojataan yhdellä avaimella, ja salaus puretaan toisella. Näitä avaimia kutsutaan salaiseksi avaimeksi ja julkiseksi avaimeksi. Julkinen avain on, kuten nimestä voi päätellä, julkista tietoa ja salainen avain on vastaavasti pidettävä salassa. Salainen avain on matemaattisesti linkitettävissä julkisen avaimen kanssa, mutta salaisen avaimen selvittäminen on erittäin hankalaa tätä kautta ja vaatii äärimmäisen suuria prosessoritehoja. Nykyisellä tekniikalla vahvojen asymmetrisien avaimien purkuun voi mennä vuosia. Julkista avainta käyttämällä voidaan salata haluttu informaatio, esimerkiksi tiedosto, mutta sillä ei voida enää avata kyseistä tiedostoa. Salaisella avaimella tiedosto voidaan taas purkaa. Tämä tekniikka poisti tarpeen salausavaimien jakamiselle suojaamattomia yhteyksiä käyttäen kuten avaimien lähettämisen postissa. (RSA Laboratories, 2007.)

Diffie-Hellman kehitettiin siirtämään salainen avain kahden maantieteellisesti kaukana olevan tahon välillä turvallisesti, ja tämän jälkeen voitaisiin siirtyä käyttämään symmetrisen avaimen salaimia tahojen väliseen liikennöintiin. Esimerkiksi Matti haluaa salatun yhteyden Maijan kanssa. Matti ja Maija sopivat käyttävänsä alkulukua $p=23$ ja primitiivistä alkiota $g=5$. Maija valitsee satunnaisen luvun $a=6$ ja Matti valitsee satunnaisen luvun $b=15$. Nyt Maija laskee $g^a \bmod p = 5^6 \bmod 23 = 8$ ja lähettää tämän numeron Matille. Matti laskee $g^b \bmod$

$p = 5^{15} \bmod 23 = 19$ ja lähettää tämän numeron Maijalle. Maija laskee $(g^b \bmod p)^a \bmod p$ ja saa tulokseksi *2*. Matti laskee taasen $(g^a \bmod p)^b \bmod p$ ja saa tulokseksi myös *2*. Tulosnumero on nyt symmetrinen avain, joka on saatu turvallisesti jaettua molemmille osapuolilla ja voidaan aloittaa symmetrisesti salattu dataliikenne. Kun luvut valitaan tarpeeksi suuriksi, on tätä algoritmia miltei mahdotonta murtaa laskemalla käyttäen nykyistä tekniikkaa. (Gollmann, D. 1999, 218.)

2.5 VPN-paketit ja kapselointi

VPN-tunnelin toiseen päähän suunnattu paketti ensin salataan sovitulla salausmenetelmällä ja annetaan VPN-tyypin vaatima otsikko. Koko paketti kapseloidaan sen jälkeen siirtotielle sopivaksi paketiksi lähettävässä VPN-laitteessa. Internetissä informaatio kulkee IP-paketeissa jolloin VPN-paketitkin täytyy kapseloida IP-paketeiksi, jotta reitittimet osaisivat käsitellä paketteja ja ohjata paketit oikeisiin osoitteisiin. Koko VPN-paketti datoineen ja osoitteineen kulkee salattuna IP-paketin sisällä VPN-tunnelin sisällä (KUVIO 2). IP-paketille annetaan kohdeosoitteeksi VPN-tunnelin toinen pää. (Perlmutter & Zarkower 2001, 13.)



KUVIO 2. Yleiskuvaus VPN-paketin kapseloinnista

Toisessa päässä tunnistetaan saapuvan IP-paketin tulevan VPN-tunnelista VPN-otsikon ja TCP (Transmission Control Protocol) porttinumeron avulla. Vastaanottava VPN -laite purkaa salauksen ja lähettää sen eteenpäin alkuperäisessä muodossaan joko yksityisverkkoon tai laitteen omalle sovellukselle riippuen paketin kohteesta.

2.6 VPN-yhteyksien muodostuminen

VPN-laitteiden pitää selvittää yhteiset pelisäännöt ja hoidettava tunnistukset, ennen kuin voidaan aloittaa dataliikenne näiden laitteiden välillä. Eri VPN-protokollat hoitavat nämä yhteyksien muodostamiset hieman eri tavoin, mutta pääperiaatteet ovat kaikissa samankaltaisia. Ensin varmistetaan, että vastapäässä on

VPN-tunnelointiin kykenevä laite ja tämän jälkeen laitteet keskustelevat yhteyden ohjauksesta. Kun ohjaus on kunnossa, siirrytään tunnistusprosessiin. Tunnistuksen jälkeen laitteet voivat aloittaa salatun dataliikenteen.

No.	Time	Source	Destination	Protocol	Info
3	0.000515	192.168.254.35	192.168.254.1	TCP	3605 > pptp [SYN] Seq=0 Len=0 MSS=1460
4	0.001090	192.168.254.1	192.168.254.35	TCP	pptp > 3605 [SYN, ACK] Seq=0 Ack=1 Win=
5	0.001228	192.168.254.35	192.168.254.1	PPTP	Start-Control-Connection-Request
6	0.001497	192.168.254.1	192.168.254.35	TCP	pptp > 3605 [ACK] Seq=1 Ack=157 Win=643
7	0.006327	192.168.254.1	192.168.254.35	PPTP	Start-Control-Connection-Reply
8	0.006471	192.168.254.35	192.168.254.1	PPTP	Outgoing-Call-Request
12	0.023020	192.168.254.1	192.168.254.35	PPTP	Outgoing-Call-Reply
13	0.023257	192.168.254.1	192.168.254.35	PPP LCP	Configuration Request
14	0.028470	192.168.254.35	192.168.254.1	PPTP	Set-Link-Info
17	0.039783	192.168.254.35	192.168.254.1	PPP LCP	Configuration Request
18	0.041164	192.168.254.1	192.168.254.35	PPP LCP	Configuration Reject
19	0.041516	192.168.254.35	192.168.254.1	PPP LCP	Configuration Request
20	0.042276	192.168.254.1	192.168.254.35	PPP LCP	Configuration Ack
23	0.066676	192.168.254.1	192.168.254.35	TCP	pptp > 3605 [ACK] Seq=189 Ack=349 Win=7
24	0.144260	192.168.254.35	192.168.254.1	GRE	Encapsulated PPP
27	3.022901	192.168.254.1	192.168.254.35	PPP LCP	Configuration Request
28	3.023498	192.168.254.35	192.168.254.1	PPP LCP	Configuration Ack
29	3.023797	192.168.254.35	192.168.254.1	PPTP	Set-Link-Info
30	3.023975	192.168.254.1	192.168.254.35	TCP	pptp > 3605 [ACK] Seq=189 Ack=373 Win=7
31	3.024259	192.168.254.35	192.168.254.1	PPP LCP	Identification
32	3.024491	192.168.254.35	192.168.254.1	PPP LCP	Identification
33	3.025069	192.168.254.1	192.168.254.35	PPP LCP	Echo Request
34	3.025346	192.168.254.35	192.168.254.1	PPP LCP	Echo Reply
35	3.025484	192.168.254.1	192.168.254.35	PPP CHA	Challenge (NAME=' [redacted] ', VALUE=0x5951BC
36	3.025998	192.168.254.35	192.168.254.1	PPP CHA	Response (NAME= [redacted] , VALUE=0x7712C66
37	3.031186	192.168.254.1	192.168.254.35	PPP CHA	Success (MESSAGE='S=B8C6D7CCA580DF74BF7

KUVIO 3. PPTP-yhteyden muodostus (kuvakaappaus Etherreal-ohjelmasta)

2.7 PPTP

PPTP on VPN-protokolla, joka on tullut suosituksi Microsoftin Windows käyttöjärjestelmissä olevan tuen vuoksi. Microsoft on muutaman muun yrityksen kanssa (mm. 3Com ja Ascend) kehitellyt PPTP:n. PPTP oli markkinoiden ensimmäinen tekniikka, joka käytti internetiä etäyhteyksien luontiin, kun aiemmin etäyhteydet olivat operaattoreilta vuokrattuja linjoja. (RFC 2637 1999, 1; Perlmutter & Zarkower 2000, 115.)

Autentikointiin PPTP:ssä voidaan käyttää älykorttia, MD5-haastetta, PAP:ia, CHAP:ia tai MS-CHAP:eja. Salaus Microsoftin PPTP:ssä on toteutettu MPPE-tekniikka käyttäen. MPPE käyttää RSA RC4 -koodausta ja se tukee 40 bittisiä, 56 bittisiä ja 128 bittisiä avaimia, jotka vaihtuvat tietyin väliajoin. (RFC 3078 2001, 3.)

PPTP:n toiminta perustuu kahdenlaisiin paketteihin: TCP:ssä kulkeviin kontrollipaketteihin ja IP:n päällä kulkeviin GRE (General Routing Encapsulation) kapseloituihin datapaketteihin. Kontrollipaketilla otetaan yhteys PPTP-palvelimen TCP-porttiin 1723, joka vastaa yhteyden hyväksymisellä (KUVIO 3, kaksi ensimmäistä riviä). (Perlmutter & Zarkower 2000, 116.) Kontrollipaketteja on IETF:n (Internet Engineering Task Force) RFC (Request For Comment) 2637:n mukaan määritelty 15 kappaletta (TAULUKKO 1).

TAULUKKO 1. PPTP -kontrolliviestit

Nimi	***Nro***	***Selitys***
Start-Control-Connection-Request	1	Kontrolliyhteyden avauspyyntö
Start-Control-Connection-Reply	2	Kontrolliyhteyden avauksen hyväksyminen
Stop-Control-Connection-Request	3	Kontrolliyhteyden sulun pyyntö
Stop-Control-Connection-Reply	4	Kontrolliyhteyden sulun hyväksyminen
Echo-Request	5	Vastauspyyntö
Echo-Reply	6	Vastaus
Outgoing-Call-Request	7	Palvelimen datanlähetyspyyntö
Outgoing-Call-Reply	8	Palvelimen datalähetyksen hyväksyminen
Incoming-Call-Request	9	Asiakkaan datalähetyksenpyyntö
Incoming-Call-Reply	10	Asiakkaan datalähetyksen hyväksyminen
Incoming-Call-Connected	11	Asiakkaan kuittaus lähetyksen hyväksymiselle
Call-Clear-Request	12	Datalähetyksen lopetuspyyntö
Call-Disconnect-Notify	13	Katkaisun hyväksyminen
WAN-Error-Notify	14	Asiakkaan virheilmoitus
Set-Link-Info	15	Palvelimen yhteysasetusviesti

Kontrollipakettien koot, tiedot ja muodot vaihtelevat kontrollityypin mukaan. Kontrollipaketeissa ei ole virheenkorjausta, koska paketit kulkevat TCP:n sisällä jossa on itsessään virheenkorjaus. Mahdollisia virhetilanteita, kuten TCP-yhteyden katkeamista, varten on kuitenkin protokollaan lisätty virheistä toipumismenettelyjä. (RFC 2637 1999, 37-39.)

TAULUKKO 2: Start-Control-Connection-Request -paketti

Viestin pituus (16 bittiä) Paketin pituus	PPP paketin tyyppi (16 bittiä) 1 = kontrollipaketti
Maaginen keksi (32 bittiä) 0x1A2B3C4D käytetään synkronoinnin varmistamiseen	
Kontrollipaketin tyyppi 1 = Start-Control-Connection-Request	Varattu0 Arvo = 0
Protokollaversio riippuu laitteista	Varattu1 Arvo = 0
Raamitusmahdollisuudet 1 = asynkroniset raamit tuettuna 2 = synkroniset raamit tuettuna	
Kantomahdollisuudet 1 = analoginen liitäntä tuettuna 2 = digitaalinen liitäntä tuettuna	
Kanavien maksimimäärä Yhtäaikaisten yhteyksien maksimi	Laitteiston revisio-numero
Laitenimi (64 tavua) (host name)	
Valmistajan nimi (64 tavua) (Vendor name)	

Dataliikenne PPTP:ssä kulkee PPP (Point-to Point Protocol)-paketeissa joista on otettu pois liikenteenohjaus ja virheenkorjaus. PPP-paketit on pakattu GRE-paketteihin, ja GRE-paketit kulkevat IP:n päällä. PPTP:n GRE-otsikot eivät ole täysin RFC 1701 ja 1702 määritellyn GRE-standardin mukaisia, vaan niitä on hieman muokattu paremman kontrollin vuoksi. PPTP:ssä on käytössä liukuvat ikkunat eli tekniikka, joka parantaa verkon tehokkuutta. Liukuvat ikkunat mahdollistaa useamman paketin lähetyksen peräkkäin ilman, että ensimmäisestäkään paketista on tullut kuittausta. Jokaisen paketin kuittaukseen ei myöskään tarvitse lähettää omaa viestiä, vaan yhdellä viestillä voidaan kuitata useampi paketti saapuneeksi. (RFC 2637 1999, 46-49.)

PPTP hyvinä puolina on laaja käyttäjäkunta ja käyttömahdollisuuksien

monipuolisuus. PPTP:lle on mahdollista helposti lisätä tuki muillekin tekniikoille kuin IP-pohjaisille. Muiden tekniikoiden lähettäminen tunnelin läpi vaatii kuitenkin VPN-laitteilta tuen näille tekniikoille. (Perlmutter & Zarkower 2000, 115.)

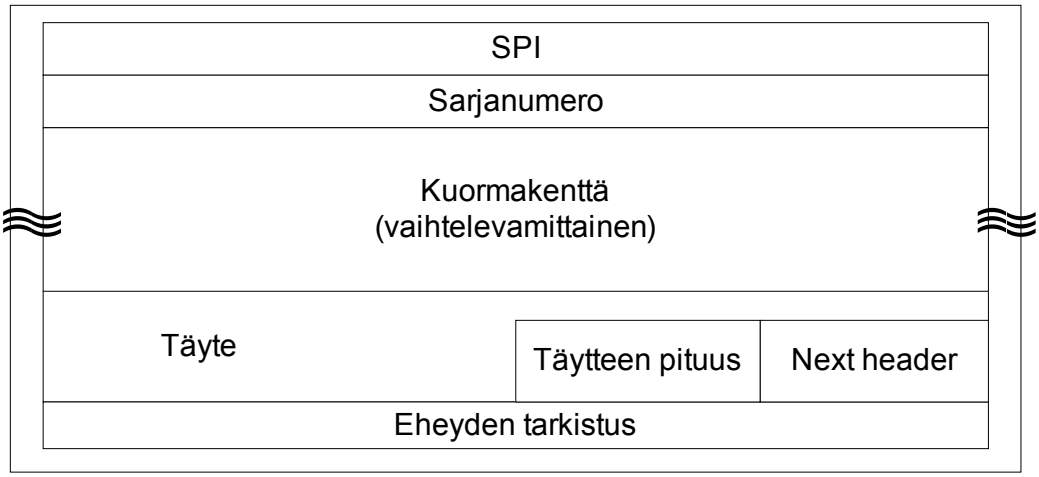
2.8 IPsec -tunnelointi

IPsec (Internet Protocol security architecture) on nimensä mukaisesti IP:n turvallisuusarkkitehtuuri, ja se koostuu useasta protokollasta. IPsec on liitetty kiinteästi IPv6:en (Internet Protocol version 6). IPv6:n tullessa käyttöön IPsec:n käyttö lisääntyy huomattavasti, ja mahdollisesti muut VPN-menetelmät marginalisoituvat tai katoavat kokonaan. IPsec:n standardointi on vielä keskeneräinen, ja tällä hetkellä on menossa IETF:n kolmas RFC-kierros. Ensimmäiset ehdotukset tulivat vuonna 1995 (RFC 1825-1829), seuraavat dokumentit tulivat 1998 (RFC 2401-2412) ja uusin painos tuli joulukuussa 2005. Vasta viimeisen painoksen myötä päädyttiin nykyiseen kirjoitusmuotoon ”IPsec” eikä aiemmin käytettyyn ”IPSec”:iin.

IPsec muodostuu kolmesta osasta. AH:sta (Authentication Header), KE:stä (Key Exchange) ja ESP:sta (Encapsulating Security Payload). AH:n tehtävänä on varmistaa informaation aitous muttei salata sitä ja koska ESP:ta voidaan käyttää samaan tarkoitukseen, on AH hieman ylimääräisenä tässä arkkitehtuurissa. Opinnäytetyössä keskityttiin tunneleiden luomiseen, minkä vuoksi AH on sivuutettu kokonaan. (RFC 4301 2005, 9.)

Avainten vaihtoon suositellaan käytettäväksi IKE:a (Internet Key Exchange). IKE:n tehtävänä on hoitaa tunnelin molempiin päihin avaimet turvallisesti ja automaattisesti, jotta ESP toimisi läpinäkyvästi. Tämän lisäksi IKE hoitaa tunnistuksen IPsec:lle. Nämä tunnistukset ja avaimet tunnetaan nimellä SA (Security association), ja ne muodostetaan aina samanaikaisesti pareittain tunnelin

molempiin päihin. SA:a käytetään tunnistamaan ja liittämään toisiinsa yhteydet, henkilöllisyydet, salaukset ja avaimet. Ensimmäisessä vaiheessa, jota kutsutaan IKE_SA_INIT -nimellä, tunnelin päätelaiteet neuvottelevat salausmenetelmän, vaihtavat kertakäyttöavaimet ja tekevät Diffie-Hellman muunnokset. Kun tämä on tehty, voivat päätelaitteet autentikoida edelliset viestit ja lähettää IKE_SA_INIT:n tuloksena saatujen avainten avulla salattuna henkilöllisyytensä, sertifikaattinsa ja luoda ensimmäinen SA ESP:n käyttöön. Tätä prosessi tunnetaan nimellä IKE_AUTH. IKE:en on määritelty myös kaksi muuta viestiparityyppiä. Kaikki IKE:n viestit perustuvat pyyntö-vastaus -pareihin. Nämä muut viestiparit ovat CREATE_CHILD_SA, jolla voidaan luoda uusia SA-pareja ja INFORMATIONAL, jota käytetään muun muassa vikatilojen ilmoittamiseen ja avaimien tuhoamiseen. Nämä viestit ovat salattuja. IKE toimii UDP (User Datagram Protocol) porttien 500 ja 4500 välityksellä. (RFC 4306 2005, 6-11,25.)



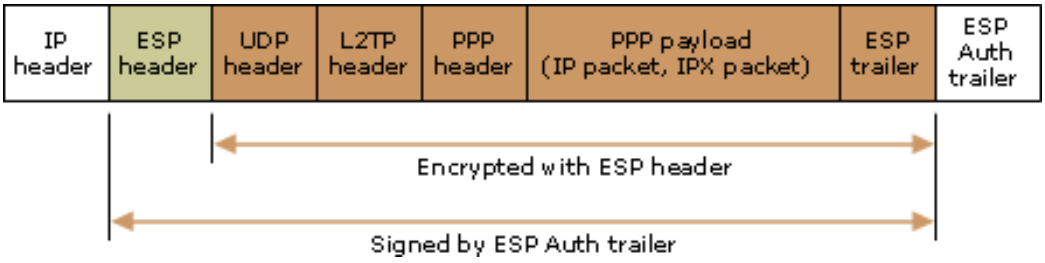
KUVIO 4: Yksinkertainen ESP-paketti

ESP määrittelee, kuinka salaus liitetään IPsec:iin, muttei määrittele mitä, algoritmeja salauksessa tulisi käyttää. ESP:n käyttö onnistuu, vasta kun avaintenvaihtoprosessi on hoidettu ja molemmilla osapuolilla on SA:t. ESP-salauksen tunnistaa IP-paketin otsikosta. IPv4 otsikon protokollakentässä ja vastaavasti IPv6 otsikon

”Next Header”-kentässä täytyy olla ”50”, jotta se osataan tunnistaa salatuksi viestiksi. Itse ESP-otsikko IP:n sisällä alkaa nelitavuisella SPI (Security Parameters Index), kentällä jossa määritellään vastaanottajan SA (KUVIO 4). Seuraavaksi otsikossa on 32 bittinen sarjanumero, jolla pystytään varmistamaan, että kaikki suojatut paketit ovat päässeet perille oikeassa järjestyksessä. Nopeissa yhteyksissä on mahdollista käyttää 64 bittistä sarjanumeroa. Nämä mainitut kentät ovat pakollisia. ESP-paketissa seuraavaksi tulee kuormakenttä ja mahdolliset lisäkentät. Näiden koko riippuu siirtotien ja valitun kryptografian vaatimuksista. Lopuksi pakettiin tulee ”Next Header”-kenttä joka kertoo kuorman IP-tyypin (IPv4, TCP jne) ja SA:n niin vaatiessa loppuun lisätään ICV-kenttä (Integrity Check Value), jolla pystytään varmentamaan tiedon eheys. (RFC 4303 2005, 9-16, 19, 21.)

IPsec:n hyvänä puolena on riippumattomuus salaus- ja avaimenvaihtometodeista joka lisää IPsec:n elinkaarta, kun ei tarvitse koko arkkitehtuuria heittää romukoppaan, jos tietystä salausalgoritmista löytyy turva-aukkoja. IPsec:ssä on kuitenkin yhteensopivuuden varmistamiseksi määritelty että kaikkien laitteiden on ainakin tuettava 3DES salausta ja HMAC-SHA1-tunnistusta (RFC 4305 2005, 3). Nykyisin useat verkot ja järjestelmät pyritään luomaan yhteensopivuuden vuoksi täysin IP-pohjaisiksi, ja näin IPsec sopisi erinomaisesti hoitamaan näiden verkkojen salauksen, kun laitteiden ei tarvitse osata useita eri kapselointimenetelmiä. Kun 3DES ja HMAC-SHA1 pystytään murtamaan järkevässä ajassa, joudutaan IPsec:a ehkä päivittämään, mutta siitä ei välttämättä tarvitse kokonaan luopua.

Windowsin IPsec-asiakasohjelma paketoi datan ensin L2TP-pakettiin (Layer Two Tunneling Protocol) ja sitten vasta ESP-pakettiin. Siksi Windows käyttää ”L2TP/IPsec VPN” -nimeä IPsec-tunnelointimetodistaan. L2TP/IPsec ja PPTP on siitä samanlaisia, että molemmat paketoivat ensin datan PPP-pakettiin ja lisäävät siihen oman protokollansa vaatimat otsikot. (Microsoft 2007c; RFC 3193 2001.)



KUVIO 5. L2TP/IPsec -paketti (Microsoft 2007c)

3 JÄRJESTELMÄN TUKITEKNIIKAT

3.1 Linux

Linux-käyttöjärjestelmän kehitti suomalainen Linus Torvalds vuonna 1991. Linux on Unix-käyttöjärjestelmän pohjalta tehty vapaan lähdekoodin käyttöjärjestelmä, jonka hyötyinä ovat turvallisuus, keveys ja nopeus. Linux oli ensimmäisiä suosittuja vapaan lähdekoodin ohjelmistoja. Linux on moniajo- ja monikäyttäjäkäyttöjärjestelmä. Turvallisuudesta on viime aikoina ollut keskustelua, kun hakkerit ovat kiinnostuneet yhä kasvavasta Linux-kannasta. Helppokäyttöisyyteen ja graafiseen käyttöliittymään on viime aikoina painotettu huomattavasti jotta Linux olisi helpompi omaksua myös koti- ja toimistokäyttöön, kun aiemmin Linux on ollut lähinnä palvelimien käyttöjärjestelmä.

Linuxista on liikkeellä satoja jakeluita, joissa on yleensä sama Linux-ydin, mutta muut ohjelmat voivat olla hyvinkin erilaisia. Osa jakeluista ovat myös maksullisia. Jotkut jakelut tulevat graafisen käyttöliittymän kanssa ja toiset eivät. Myös jakelun asentaminen, komennot ja jakeluihin saatavat lisäohjelmat voivat olla

erilaisia. Näitä jakeluita ovat mm. Debian, Gentoo, Ubuntu, Mandriva ja Fedora Core.

3.2 Tiedoston siirto

FTP (File Transfer Protocol) on yksinkertainen ja tehokas IP-verkon tiedostonsiirtoprotokolla, joka toimii asiakas-palvelin -mallin mukaisesti. Sitä käytetään yleensä isompien tiedostojen siirtoon internetin yli. Esimerkiksi internet-sivut siirretään perinteisesti FTP:llä palvelimelle. FTP tukee käyttäjän tunnistusta mutta vain selkokielisenä siirrettynä. Myös dataliikenne on salaamatonta. Protokollaan on tästä syystä liitetty lisäosa, jonka avulla voidaan salata niin kirjautumisviestit kuin dataliikennekin.

FTP-liikennettä on kahdenlaista: ohjausliikennettä joka kulkee TCP-portin 21 kautta ja dataliikennettä, joka kulkee TCP-portin 20 kautta. FTP-palvelin voi toimia myös passiivisessa tilassa jolloin dataliikenne kulkee satunnaisen TCP-portin kautta. Ohjausliikenne on suojaamattomassa muodossa telnet-liikennettä asiakkaalta palvelimelle, ja sitä käytetään ohjaamaan FTP:n dataliikennettä (TAULUKKO 3).

TAULUKKO 3: Yleisiä FTP-käskyjä

Käsky	***Selitys***
USER	Lähetä käyttäjätunnus
PASS	Lähetä salasana
LIST	Listaa etäkansion tiedot
RETR/GET	Hae etätiedosto
DELE	Poista etätiedosto
STOR/PUT	Lähetä tiedosto etäkoneelle
CWD	Vaihda etäkansiota
ABOR	Katkaise tiedostonsiirto

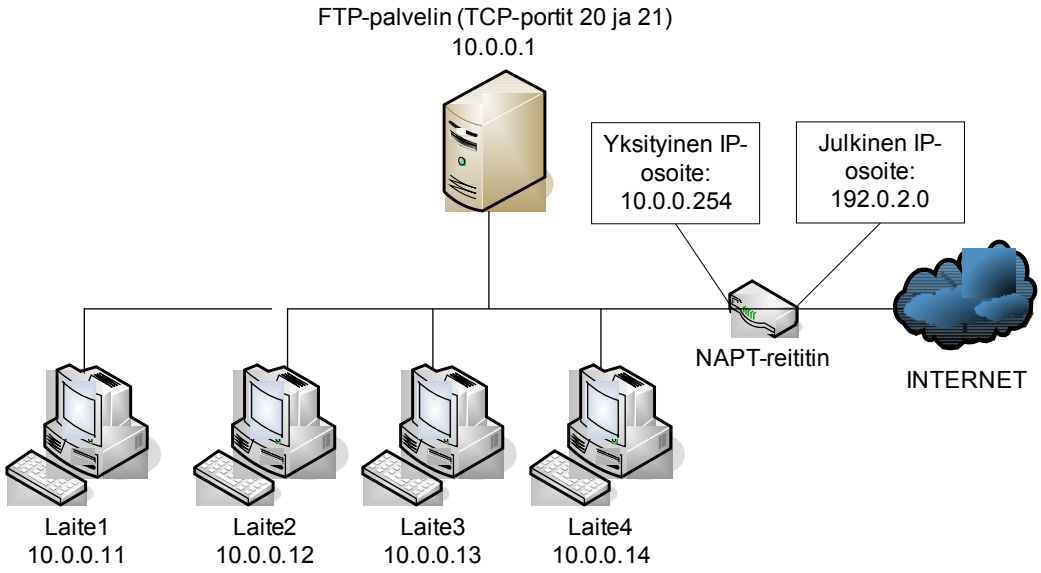
3.3 NAPT

NAPT (Network Address and Port Translation) on tekniikka, jolla pystytään piilottamaan yhden verkon IP-osoitteet toisen verkon IP-osoitteen taakse porttinumeroiden avulla. Tekniikkaa käytetään IP-osoitteiden säästämiseksi ja palomuurin apuna. NAPT toimii reitittimissä kahden verkon yhdyspisteissä.

IP-osoitteiden säästäminen on tärkeää varsinkin internetissä, kun laitemäärät vain kasvavat ja IPv4-osoitteet eivät riitä loputtomiin. IPv6 -tekniikka poistaa nämä ongelmat, kuten myös tarpeen NAPT -tekniikalle, mutta siihen asti on NAPT tuiki tärkeä apuväline ip-verkkojen toiminnalle (RFC 2373 1998, 2-3).

NAPT:ssa on siis kiinni kaksi verkkoa, joita kutsutaan sisä- ja ulkoverkoiksi. Sisäverkolla tarkoitetaan yleensä yrityksen lähiverkkoa, jossa saattaa olla satojakin koneita kiinni. Ulkoverkko on yleensä julkinen internet. Sisäverkon laitteille annetaan osoitteet omasta sisäverkoille määritetystä osoiteavaruudesta, ja NAPT-reititin saa sisäverkon osoitteen lisäksi myös yhden ulkoisen verkon osoitteen. Kaikki sisältä ulospäin menevä liikenne kulkee NAPT-reitittimen kautta, ja reititin pystyy valvomaan kaikkea läpikulkevaa liikennettä. NAPT:n toiminta perustuu siihen, että NAPT-reititin muokkaa läpikulkevien IP-pakettien otsikoita, niin että ulospäin lähtevien pakettien lähettäjäkentäksi laitetaan NAPT-reitittimen oma ulkoinen osoite. Näin internetistä tuleva paluuviesti löytää perille NAPT-reitittimelle. NAPT-reititin osaa lähettää lähettää paluuviestin oikeaan osoitteeseen porttinumeron perusteella. NAPT:n täytyy myös laskea uudelleen otsikon tarkistussumma, jottei vastaanottaja huomaisi otsikon muuntelua ja luulisi sitä laittomasti manipuloiduksi. NAPT toimii siis vain, jos yhteyden aloittajana on sisäverkon laite. Jos sisäverkossa on jokin palvelu, johon pitää päästä internetistä käsin, pitää sen palvelun käyttämä porttinumero ja IP-osoite kertoa

manuaalisesti NAPT:lle, jotta se osaa reitittää sisään tulevat yhteydet oikealle laitteelle. Kuvion 6 esimerkissä NAPT-reitittimelle täytyy kertoa, että ulkoverkosta osoitteen 192.0.2.0 TCP-portteihin 20 ja 21 tuleva liikenne täytyy ohjata sisäverkon osoitteeseen 10.0.0.1, jotta palvelin pystyisi tarjoamaan FTP-palveluita ulkoverkon käyttöön.



KUVIO 6. Esimerkki NAPT-verkotuksesta

4 KAMERAVALVONTA

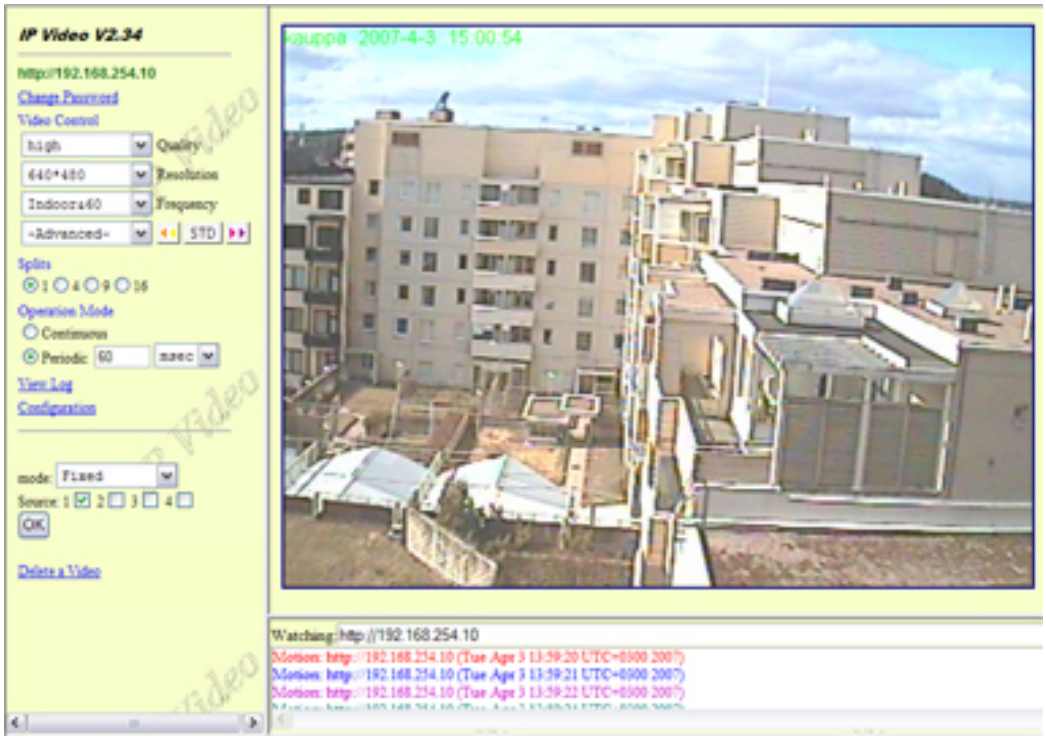
4.1 Reaaliaikainen seuranta

Kameravalvontajärjestelmä rakennettiin Aviosys:n IP Video 9100a:n (KUVIO 7) ympärille. IP Video 9100a:ssa on neljä RCA-video sisääntuloa, yksi RCA-äänitulo, verkkokortti, FTP-lähetysohjelma ja www-palvelin. Www-palvelimen avulla voidaan tarkastella kaikkia neljää videosyötettä samanaikaisesti internet-selaimella. Www-palvelin pystyi näyttämään videot Java-sovelluksen, ActiveX:n tai päivittyvien JPG-kuvien (Joint Photographic Experts Group) avulla. Www-palvelimessa on myös kaksitasoinen käyttäjätunnistus: toinen katselua ja toinen asetusten muuttamista varten.

KUVIO 7. Aviosys IP Video 9100a (Aviosys 2005)

Katselutunnuksilla pääsi näkemään videosyötteet ja konfiguraatiot muttei muuttamaan niitä. Hallintasivuja oli kahdenlaisia: ActiveX:llä tuotettu hallinta ja

html-sivuilla tuotettu hallinta. Hallinnassa pystyttiin määrittelemään, mitä kameraa seurataan, millä tarkkuudella ja taajuudella, ja kuinka usein kameran kuva päivittyy www-sivulla vai toimiiko reaaliaikaisesti. Täysin reaaliaikaisesta ei voida kuitenkaan puhua, kun IP Video 9100a:ta menee aikaa analogisen syötteen konvertoinnissa digitaaliseksi ja sivun siirto vie myös oman aikansa. Lähiverkossa videon näyttämiseen puolesta kolmeen sekuntiin riippuen videon tarkkuudesta. Kameroiden valoisuutta, kontrastia ja muita video-ominaisuuksia voitiin myös säätää www-hallinnan kautta. Kuvan jakaminen neljään osaan onnistui myös, jos halusi seurata jokaista kameraa yhtä aikaa. ActiveX:n kautta hallinta oli nopeaa ja intuitiivista, kun pääosan säädöistä pystyi hoitamaan etusivulta videokuvan viereltä (KUVIO 8), kun vastaavasti html-hallinta oli sekava ja hidas. Muutoksen html:n kautta piti tehdä erillisillä sivuilla, ja tehdyt muutokset näki vasta palattuaan videosivulle.



KUVIO 8. Kuvakaappaus ActiveX-hallinnasta

4.2 Kuvien tallennus ja tarkastelu

IP Video 9100a:ssa oli myös liikkeen tunnistusominaisuus. Laite vertaili kahta määritellyin väliajoin ottamia kuvia ja jos kuvat erosivat toisistaan, laite pystyi lähettämään viimeisimmän kuvan FTP:llä palvelimelle ja/tai sähköpostiin. Koska tässä tapauksessa kyseessä oli liiketilojen valvonta, joka perustuu liiketunnistukseen, olisivat sähköpostiosoitteet olleet pian tukossa. IP Video 9100a:n sisäinen FTP-asiakasohjelmisto pystyi anonyyminä lähettämiseen tai vaihtoehtoisesti käyttäjätunnus-salasana parin avulla tunnistautumaan palvelimelle.

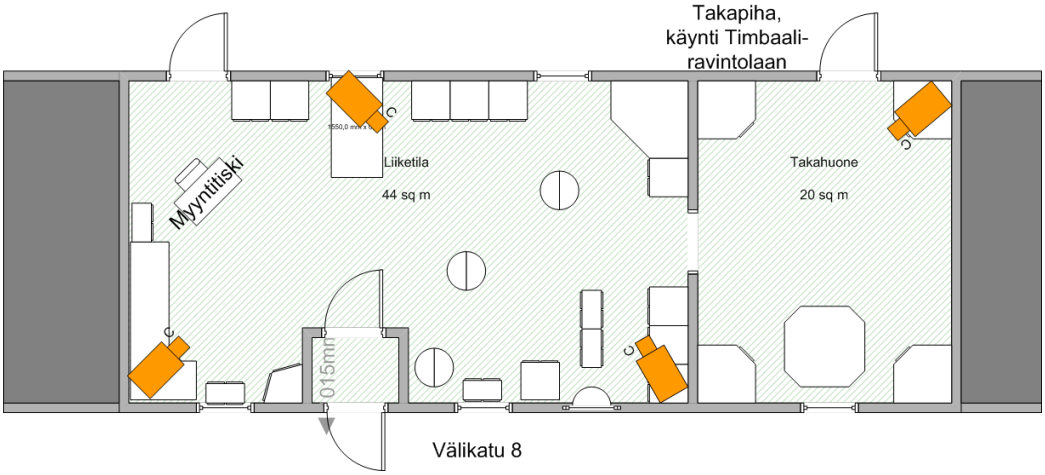
Järjestelmä asetettiin lähettämään kuvia 6 sekunnin välein, jos kuvissa näkyi liikettä. Todettiin liikkeen henkilökunnan kanssa, että tämä aikaväli riittäisi siihen, että kaikki liikkeessä käyvät ihmiset tallentuisivat kameralle ja mahdollisesti pystyttäisiin kuvista varmistamaan, onko hyllyistä hävinnyt esineitä. Laskujen ja testausten mukaan selvitettiin että palvelimen kiintolevylle mahtui miltei kahden kuukauden kuvat. Päätettiin, että kuukausi oli riittävän pitkä aika säilyttää tallenteita ja hankittiin ulkopuolista apua kirjoittamaan pieni ajastettu ohjelma, joka tuhoaa yli kuukauden vanhat kuvakansiot. Kuvat tallentuivat palvelimelle päiväyksen mukaan omiin kansioihin. Kansion nimet olivat ”mm_dd_yyyy” muodossa, ja kuvat saivat nimensä kellonajan mukaan ”hh_mm_ss_GMT.jpg” muodossa. Kuvia pystyttiin tarkistelemaan etänä muodostamalla ensin VPN-tunneli palvelimeen ja sieltä FTP-ohjelmalla hakemalla halutut kuvat.

5 VERKON SUUNNITTELU JA RAKENNUS

5.1 Lähtökohta

Liiketiloissa oli puhelinliittymä, johon oli liitetty puhelin ja modeemiyhteydellä toimiva pankkikortin varmennuslaite. Sonera, paikallisen puhelinverkon omistaja, ilmoitti voivansa asentaa ADSL (Asymmetric Digital Subscriber Line) -laajakaistan kiinteistöön. Porvoon Energia tarjosi langatonta laajakaistaa WLAN (Wireless Local Area Network) -tekniikalla toteutettuna. Etäyhteydet liikkeeseen ja sen kameravalvontaan tulisi useimmiten kotitoimistosta, jossa oli jo asennettuna Soneran tarjoama 512 kbps ADSL-liittymä.

Liikkeen pinta-ala on 64 neliötä kahdessa huoneessa ja molemmissa huoneissa on asiakkaille tarkoitettu ovi. Suurempi noin 44 neliöinen huone on myyntialuetta, jossa pyörivät korttitelineet toimivat näköesteinä ja tekevät tilasta sokkeloisen. Tästä syystä tarvittiin useita kameroita, jotta saatiin kaikki alueet kuvattua. Takahuoneessa olevan oven takia oli sinnekin saatava kamera kuvaamaan mahdollisia varkaita. Kameroiden sijoittelua rajoittavat työntekijöiden yksilön suojalait. Asia otettiin huomioon, eikä yhdestäkään kamerasta ei ole mahdollista nähdä myyntitiskin taakse. Muut tilat liikkeessä lasketaan yleisiksi tiloiksi, ja näiden kuvaaminen on lain mukaan sallittu.



KUVIO 9. Riimikon pohjapiirros kamera-asetteluineen

5.2 Huomioitavat seikat

Järjestelmää rakennettaessa haluttiin uudistaa myös pankkikorttien varmennusjärjestelmä. Entisen modeemiyhteyden tilalle haluttiin laajakaistainen varmennusjärjestelmä hoitamaan kasvavaa pankki- ja luottokorttiliikennettä. Puhelinyhteyden haluttiin pysyvän paikallaan ja analogisena.

Valvontajärjestelmän tuottamat kuvat täytyi saada siirrettyä ja tallennettua vaivattomasti ja häiritsemättä muita toimintoja, kuten pankkiliikennettä. Järjestelmä tuottaa vuorokaudessa 30-60 MB (Mega Byte) kuvia verkkoon. Kuvien määrä on suhteessa päivän vilkkauteen. Tallennuskapasiteetti oli rajallinen.

Tarvittaessa tietyn päivän kuvat voitaisiin tarkastaa jälkeenpäin etäyhteyden avulla. Etäyhteyden avulla piti pystyä seuraamaan myös reaaliaikaista valvontakameroiden tuottamaa videosyötettä. Etäyhteyden avulla piti olla mahdollista myös hallita palvelinta ja muita verkon laitteita.

5.3 Tunnelointitekniikan valinta

Kotitoimiston koneilla oli valmiiksi Windows-käyttöjärjestelmät eikä haluttu turhaan lisätä ohjelmia, joten päätettiin valita Windowsin valmiiksi tukema VPN-tekniikka. Näitä tekniikoita ovat PPTP ja IPsec. PPTP on ensimmäinen VPN-protokolla, joka toimi Internetin välityksellä, kun IPsec on vielä hiottavana oleva protokolla, jonka suosio on kovassa kasvussa.

IPsec on lisäämässä suosiotaan hurjasti IP verkoissa monipuolisten salaus- ja tunnistusmetodiensa ansiosta. IPsec määrittelee yhden pakollisen salausprotokollan ja yhden pakollisen tunnistusprotokollan, mutta IPsec:ssa voidaan käyttää mitä tahansa salausta ja tunnistusta, kunhan tunnelin molemmat päät tukevat niitä tekniikoita. IPsec tuki on otettu alusta lähtien huomioon myös IPv6-protokollaa suunniteltaessa, ja jos IPv6 joskus otetaan käyttöön, lisääntyy IPsec:n käyttö räjähdysmäisesti.

PPTP:n salausmenetelmät ovat onnistuneet pysymään suhteellisen turvallisena eikä järkevästi hyödynnettäviä menetelmiä salauksen purkuun ole olemassa. ”Järkevästi hyödynnettävällä” tarkoitetaan tässä ajallisesti mielekästä ja kohtuullisilla resursseilla. PPTP:n vahvin suojaus koostuu MS-CHAPv2- ja MPPE-128-protokollista.

Useat laitevalmistajat ja ohjelmistotalot luottavat IPsec:n turvallisuuteen ja useita IPsec-tunnelointisovelluksia on markkinoilla, vaikka standardi on epäilyttävän uusi. Tästä kertoo sekin, että arkkitehtuurissa on päällekkäiset protokollat. AH ja ESP ovat molemmat luotu varmentamaan otsikko. PPTP on taas vanha ja testattu protokolla, jonka salaus on vieläkin riittävällä tasolla. Myös ohjelmistot ja laitteistot ovat PPTP:ssä hyvin testattuja, ja lastentaudeista on päästy jo eroon. Tunnelointiprotokollaksi valittiin siis luotettavaksi osoittautunut PPTP-protokolla.

5.4 Verkon suunnittelu

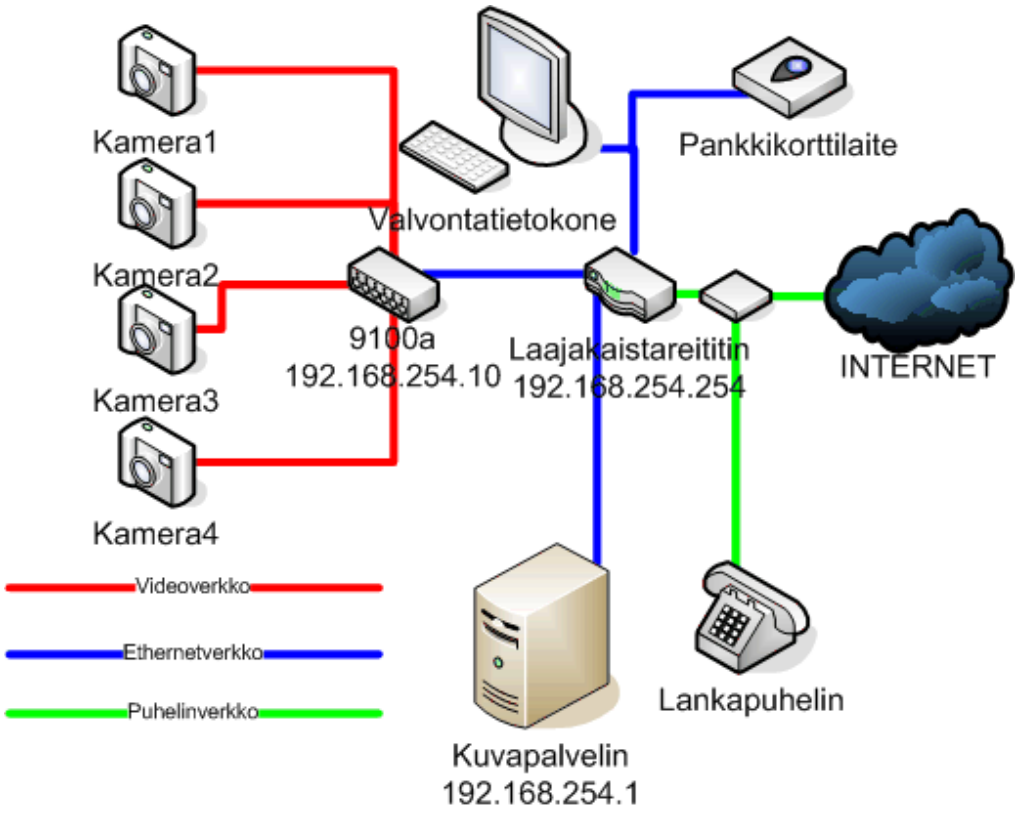
Järjestelmän aiheuttaman liikenteen vuoksi päätettiin asentaa tallennuslaitteisto paikallisesti liikkeeseen, ettei kamerajärjestelmän liikenne häiritsisi liiketoiminnan kannalta tärkeää pankkikorttiliikennettä. Resurssien vähyyden vuoksi päädyttiin ratkaisuun jossa mahdollisimman moni palvelu toimisi yhdessä laitteessa. Tämä myös helpotti verkonkin suunnittelua kun laitemäärät pysyisivät aisoissa.

Kiinteästi liikkeeseen asennettavia laitteita oli IP-kamerajärjestelmä, tallennuslaitteisto, reaaliaikaista seurantaa varten tietokone, pankkikortin varmennin ja laajakaistareititin. Puhelin tulisi pysymään paikallaan, ja IP-kamera järjestelmään kuuluu neljä analogista videokameraa ja IP Video 9100a -palvelin. Kaikki mahdolliset johdot vedettiin suojaputkissa ullakon kautta, jolloin ulkopuolisilla ei ole mahdollista päästä johtoihin käsiksi. Ainoat näkyvät osat kameravalvonnasta ovat kamerat.

Verkkotopologiaksi päädyttiin ottamaan tähtimalli (KUVIO 10) sen vikasietoisuuden ja yksinkertaisuuden vuoksi. Kaikki muut verkkolaitteet liitettiin reitittimeen. Ainoa kriittinen laite, joka olisi siis pystynyt sammuttamaan koko järjestelmän, oli laajakaistareititin. Sen vuoksi hankittiin varareititin, joka voitaisiin vaihtaa nopeasti alkuperäisen reitittimen tilalle tarvittaessa.

Ulkolinjaksi valittiin Soneran tarjoama 512kbps ADSL -laajakaista. ADSL oli edullisempia ja varmatoimisempi kuin langaton internet, varsinkin kun liikekiinteistö sijaitsi langattoman tukiaseman kantaman raja-alueella. Langattoman internetin toiminta olisi voinut olla epävarmaa huonolla säällä. Laajakaistareitittimen palomuuriominaisuudet otettiin käyttöön ja estettiin muun muassa sisääntuleva liikenne. TCP-portille 1723 tuleva liikenne ohjattiin NAPT:n avulla VPN-palvelimelle, joka on PPTP:n käyttämä oletusportti. Näin palvelimen muut palvelut, kuten FTP ja SSH olivat piilossa ulkopuolisilta ja käytössä vain sisäverkossa tai VPN-tunnelin kautta. Tämä esti myös suoran pääsyn Internetistä kame-

ravalvonnan www-palvelimelle.



KUVIO 10. Liikkeen verkkokuva

5.5 Ohjelmistovalinnat ja asennus

Ohjelmistovalinnat päätettiin tehdä mahdollisimman paljon vapaan lähdekoodin ja turvallisuuden kannalta. Resurssien säästämiseksi vapaa lähdekoodi luonnollinen valinta.

Linuxin valitseminen VPN- ja FTP-palvelimeksi oli helppo Linuxin ilmaisuuden ja vapaan lähdekoodin vuoksi. Resurssien säästämisen vuoksi päädyttiin käyttämään vanhaa Pentium II -prosessoria käyttävää tietokonetta joka myöskin osaltaan helpotti päätöstä käyttää resurssipihiä Linuxia. Jakelua päätettäessä oli tärkeää helppokäyttöisyys ja suosio Linux-asiantuntijoiden keskuudessa. Debianiin pohjautuva Ubuntu mainittiin niin useassa lähteessä luotettavana, helppona ja suosittuna ettei sille löytynyt loppujen lopuksi haastajia. Käyttöjärjestelmäksi valittiin Ubuntu Edgy, joka oli valintahetkellä Ubuntun uusin versio. Ubuntu oli tunnettu helposta asennuksesta ja oli huojentavaa todeta että kerrankin mainospuheet pitivät paikkansa. Asennus sujui nopeasti ja yksinkertaisesti. Automaattisten suojauspäivitysten käyttöönotto oli myös helppoa ja yksiselitteistä. Kun alkuasennus oli tehty, siirryttiin käyttämään SSH-yhteyttä, jonka avulla muut asennukset suoritettiin. Lisäohjelmien asentaminen oli helppoa käyttäen valmiita ohjelmistovarastoja (repositories) joista löytyi suurin osa tarvittavista lisäohjelmista, ja ubuntuguide.org internet-sivu tarjosi yksinkertaiset ohjeet niiden ohjelmien asennukseen.

PPTP-ohjelmiston valinta oli helppoa, kun Windows-yhteensopiva PPTP-palvelinohjelmistoja oli rajallinen määrä ja kaikkien ohjelmistojen turvallisuus vaikutti päälle päin hyvin hoidetulta. PPTP-tunnelointipalvelimeksi valittiin vapaan lähdekoodin Poptop. Ohjelman asennus oli yksinkertaista käyttäen Ubuntun automaattista lataus/asennus-ohjelmaa (apt-get). Kun asennus oli suoritettu, alkoi asentamista hieman monimutkaisempi konfigurointiosuus, johon löytyi kylläkin useita asennusohjeita. ”/etc/ppp/pptpd-options” -tiedostosta löytyi vaihtoehdot

autentikoinnin ja salauksen toteutukselle. Oletuksena salaus toteutettiin MPPE-128 -tekniikalla, joka vaatii MS-CHAPv2:n autentikoinnin ja koska tämä on varmin salaus- ja autentikointimetodi PPTP:ssä, jätettiin oletusarvot voimaan. Tiedostoon olisi ollut myös mahdollista asettaa käsin DNS-palvelimien (Domain Name System) osoitteet, mutta koska tämä olisi lisännyt mahdollisuuden netissä surffailuun tunnelin läpi, kommentoitiin dns-osoitteet. Tämä esti mahdollisuuden vahingossa tunnelin läpi surffaamiseen ja jätti tunnelin vain valvontajärjestelmän käyttöön. Konfiguraatiotiedostosta ”/etc/pptpd.conf” vaihdettiin local-ip ja remote-ip arvot. Local-ip kohtaan asetettiin PPTP-palvelimen oma osoite, ja remote-ip kohtaan asetettiin lähiverkosta viiden osoitteen segmentti. Näitä viittä osoitetta palvelin jakoi dynaamisesti PPTP-yhteyttä haluaville laitteille. Tämä rajoitti myös yhtäaikaiset PPTP-yhteydet viiteen kappaleeseen. ”/etc/ppp/chap-secrets”-tiedostoon kirjoitettiin rivi, johon tuli etäkäyttäjän käyttäjätunnus, palvelimen käyttäjätunnus, salasana ja lopuksi olisi voinut rajata sallitut IP-osoitteet, mutta kiinteiden IP-osoitteiden puutteen vuoksi sitä ei voitu tehdä. Windows-asiakasohjelman käyttöönotto oli yksinkertaista Poptopin ja Microsoftin ohjeiden avulla. Käytännössä tämä tapahtui luomalla uusi yhteys, joka määriteltiin PPTP VPN yhteydeksi ja määriteltiin autentikointitavaksi MS-CHAPv2 ja salaukseksi varmin mahdollinen MPPE-128.

Tiedostonsiirtoa kameravalvonnasta kovalevylle, ja kovalevyltä etäkäyttöä varten tarvittiin myös FTP-palvelinohjelma. Jälleen vapaa lähdekoodi ja turvallisuus ratkaisivat asian ja päädyttiin VSFTP:hen (Very Secure FTP). Muun muassa OpenBSD:n ja Redhat-jakelun kotisivut käyttävät VSFTP:tä tiedoston jakeluun. VSFTP konfiguroitiin niin, että vain kirjautumalla pääsi lukemaan ja kirjoittamaan palvelimelle. Ohjelmassa oli optio, että vain salatuilla yhteyksillä pääsisi kirjautumaan FTP-palveluun, mutta IP Video 9100a tue salattuja yhteyksiä. VSFTP:n konfigurointitiedosto ”/etc/vsftpd.conf/” on kommentoitu hyvin yksiselitteiseksi eikä tilaa virhekonfiguroinneille juuri jää.

Palvelin-Linuxille asennettiin myös Samba-tiedostopalvelin. Tämä asennettiin, jotta paikan päällä liikkeessä olisi helppo tarkastella palvelimelle tallentuneita

kuvia. Samba-tiedostopalvelimella olevia tiedostoja voi tarkastella Windows-käyttöjärjestelmään kuuluvalla Explorer-tiedostoselaimella. Explorerin käyttöliittymä ja toiminta on valmiiksi tuttua liikkeen henkilökunnalle, eikä henkilökunnan näin ollen tarvitse opetella uusien ohjelmien käyttöä. Samban toiminta on liian hidasta, jotta sitä voitaisiin luontevasti käyttää Internetin yli.

5.6 Valvontajärjestelmän toimivuus

VPN-tunneli on toimiva ratkaisu, kun halutaan etäyhteyksiä yrityksen verkkoon, ja nykyisillä hinnoilla valmiit VPN-reitittimet ovat käteviä vaihtoehtoja tällaiselle ohjelmallisesti suoritetulle VPN/Linux-palvelimelle, joskin ohjelmallinen ratkaisu on helpommin ja halvemmalla päivitettävissä, kun salaus todetaan liian kevyeksi.

GFI LANguard Network Security Scanner 8.0 verkkotutka ei löytynyt verkosta vakavia turva-aukkoja (ainoastaan tarpeellisten palvelujen portit), joten verkon turvallisuus on ainakin päällisin puolin kunnossa. Linuxin automaattiset turvapäivitykset pitävät palvelimen turvallisuudesta huolen jatkossakin, ja laajakaistareitittimen palomuuri onnistuu pitämään selvimmät verkkohyökkäykset kurissa.

Kvanttitietokoneiden on sanottu murtavan kaikki nykyiset salaukset ja teorioita monen nykyisin varmojen salausten purkamiseen ovat olemassa. Tällaiseen valvontajärjestelmään valitut salausmenetelmät ja muut turvallisuusominaisuudet ovat riittävän vahvoja, mutta verkkoihin, joissa liikkuu liikesalauksia ja muuta arkaluontoista informaatiota, otettaisiin käyttöön enemmän kulunvalvontaa ja mahdollisesti vahvempi salaus sekä varmistettaisiin salasanojen olevan riittävän monimutkaisia.

Nykyään 512 kbps ADSL-laajakaistaa pidetään suhteellisen hitaana, kun mobiililaitteisiin, kuten kännyköihinkin, on saatavilla 2 Mbps:n nopeudella toimivia

langattomia laajakaistoja. ADSL:n hitaus rajoittaa jonkin verran valvontajärjestelmän toimivuutta ja lisäksi salaus ja salauksen purku tunnelin päissä vievät oman aikansa. Nämä viiveet eivät kuitenkaan ole mitenkään ratkaisevan suuria, eikä niitä välttämättä edes huomaa.

6 YHTEENVETO

Tavoitteena oli rakentaa mahdollisimman huokea ja helppokäyttöinen etäyhteys yrityksen liiketilojen valvontakamerajärjestelmään. Etäyhteydellä piti päästä käsiksi niin kameroiden reaaliaikaiseen videosyötteisiin kuin myös järjestelmän liiketunnistuksen avulla FTP-palvelimelle tallennettuihin kuviin. Yhteyksien kustannukset koostuivat lähinnä uudesta laajakaistaliittymästä, reitittimistä ja verkkokaapeleista, kun palvelimeksi valittiin vanha PC-kone, jolla ei nykypäivänä ole mitään rahallista arvoa.

Verkon suunnittelussa otettiin huomioon liiketoiminnalle elintärkeä pankki- ja luottokorttien todennusjärjestelmä, ja etäkäyttö ja valvonta tehtiin mahdollisimman vähän ulkokaistaa vieväksi. Kameroiden tuottamista videoista IP Video 9100a tunnisti liikkeen ja lähetti muuttuneet kuvat 6 sekunnin välein FTP-palvelimelle. Ulkokaistan säästämiseksi tämä toteutettiin FTP-palvelimen sijoittamisella lähiverkkoon, jolloin tallennettavat valvontakuvat eivät veisi rajallista laajakaistan kapasiteettia pankkiliikenteeltä. Tarvittaessa tietyn päivän kuvat voitiin hakea etäyhteyden avulla FTP-palvelimelta, joka aiheuttaisi vain hetkellistä liikennettä. Reaaliaikainen kameravalvonnan etähallinta hidastaa huomattavasti verkkoa, eikä sitä voi suositella käytettäväksi ruuhka-aikoina. Koska kaikki laitteet käyttävät standardiliityntöjä niin fyysisesti kuin protokolliensakin puolesta, on laitteet helppo vaihtaa tulevaisuudessa uudempiin ja parempiin. Esimerkiksi IP Video 9100a on mahdollista vaihtaa laitteeseen, joka tukee useampaa

kameraa ja videotallennusta, kun IP Video 9100a pystyy vain kuvien tallentamiseen, VPN/FTP-palvelimelle voi tarvittaessa vaihtaa tehokkaamman koneen, lisätä muistia ja kovalevytilaa. Näin palvelimelle voisi asentaa useampia palveluita, kuten varastokirjanpitotietokannan, kassaohjelman jne.

Ubuntun valitseminen käyttöjärjestelmäksi oli oiva valinta käytön helppouden vuoksi. Ubuntu-käyttöjärjestelmän asennus palvelimelle oli jopa helpompaa kuin Windowsin asennus. Debianista tuttu apt-get-asennusohjelma oli äärimmäisen tärkeä apuväline ohjelma-asennuksissa. Asennusohjelman ansiosta tarvitsi tietää vain asennettavan ohjelman nimi, ja apt-get haki itse ohjelman internetistä ja asensi sen valmiiksi. Omaksi työksi jäi vain ohjelmien konfigurointi. Näin sain tietokoneelle asennettua VSFTP:n, Poptopin ja Samban.

Kamerat suunnattiin liikkeessä niin että saatiin mahdollisimman kattavasti kuvattua koko liike kuitenkaan rikkomatta työntekijän yksityisyyden suojalakeja. Asiakkaille vapaassa takahuoneessa olevan oven vuoksi tarvittiin kamera myös sinne, joten kolme kameraa sijoitettiin suurempaan kadun puoleiseen tilaan ja yksi oven yläpuolelle takahuoneeseen. Johdot kameroista vedettiin kovissa muoviputkissa ullakolle, joten ulkopuoliset eivät pääse niihin käsiksi.

Etäyhteyden luonti PPTP:tä käyttäen oli alun testausvaiheen jälkeen helppoa ja yksinkertaista. Konfiguraatiotiedostoissa oli suurimmalta osalta hyvin dokumentoidut ja yksiselitteiset asetusvaihtoehdot. Esimerkiksi autentikointimetodien valinta hoitui konfiguraatiotiedoston riveillä: ”refuse PAP, refuse CHAP, require MS-CHAPv2”. Poptopin kotisivuilta löytyivät yksinkertaiset ohjeet yhteyden muodostukseen Microsoftin asiakasohjelmalla. Kotitoimiston tietokoneen työpöydälle asetettu pikakuvake mahdollisti nopean ja vaivattoman yhteyden PPTP-palvelimeen ja sitä kautta koko valvontakamerajärjestelmään. FTP toimi täysin mukisematta, ja tiedostojen vieminen ja hakeminen palvelimelta sujui helposti, kun muisti salasana- käyttäjätunnusparin. FTP-palveluun pääsee käsiksi salaamattomana ja SSH-salatulla yhteydellä. Reaaliaikainen kameravalvonta ja

valvonnan hallinta ei ole nettisurffailua vaikeampaa IP Video 9100a:n kätevän www-hallinnan vuoksi.

Etäyhteyden turvallisuus riippuu enemmän käyttäjien tietoturvakäytännöistä ja salatun tiedon arvosta kuin salausalgoritmeista: säilyttääkö käyttäjä tunnuksiaan lompakossa, puhelimessa, koneen vieressä vai muistissaan, ja käytetäänkö samoja tunnuksia kaikissa mahdollisissa yhteyksissä kuten pankissa ja irc-galleriassa. Vaikka salausalgoritmit murretaankin ennen pitkään, on ohjelmallisesti tuotettu VPN helppo ja nopea vaihtaa käyttämään vahvempaa salausta ja tarvittaessa eri tekniikkaa. Halutessa etäyhteystekniikka voidaan vaihtaa etäyhteyden avulla, eikä paikan päällä tarvitse käydä ollenkaan. Ensin otetaan etäyhteys vanhalla tekniikalla ja asennetaan sekä konfiguroidaan uusi tekniikka sekä lopuksi otetaan yhteys uudella tekniikalla ja poistetaan vanha.

Kokonaisuudessaan järjestelmä on toimiva, tarpeeksi turvallinen ja helppokäyttöinen. Valvonnan hyödyllisyys jää historian näytettäväksi. Luultavasti ”nauhoittava videovalvonta” -tarrat ovissa ja ikkunoissa tuottavat enemmän tulosta kuin itse kameravalvonta. Tarpeen vaatiessa VPN-tunnelia voidaan käyttää liiketoiminnan tukemiseksi hyvinkin erilaisin tavoin. Verkkoliikennettä lisättäessä on kuitenkin tärkeää varmistaa laajakaistan nopeuden riittävyys. Laajakaistojen hintojen laskiessa alenee kynnys hankkia muita käyttökohteita tunnelille.

IPv6:n tullessa laajaan käyttöön kannattaa IP Video 9100a vaihtaa jykevämpään IPv6-laitteeseen. Palvelimelle kannattaa samalla vaihtaa VPN-tekniikaksi IPsec, koska IPv6-protokollassa on suora tuki IPsec-tekniikalle. IPsec:lle on saatavilla myös PPTP:tä vahvempia salausmetodeja, mikä lisää tunneloinnin käyttöikää. IPv6 on ollut tulossa jo monta vuotta, mutta operaattorit ja laitteisto- sekä ohjelmistovalmistajat ovat olleet hyvin hiljaisia viime ajat käyttöönottoaikatauluista, joten tämä ei ole mitenkään ajankohtaista. IPv6-IPv4-muunnoksien käyttäminen tuhlaa resursseja, eikä niiden käyttäminen ole siksi järkevää.

LÄHTEET

Aviosys. 2005 [elektroninen dokumentti]. IP Video 9100(A) User Guide. Käyttöopas.

CNSS. 2003 [verkkodokumentti]. Policy No. 15, Fact Sheet No. 1 [viitattu 27.3.2007]. saatavissa: http://www.cnss.gov/Assets/pdf/cnssp_15_fs.pdf

National Institute of Standards and Technology. 2002 [verkkodokumentti]. Federal Information Prosessing Standards Publication 180-2 [viitattu 5.4.2007]. saatavissa: http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf

Microsoft. 2007a [verkkodokumentti]. The MS-CHAP version 1 authentication protocol has been deprecated in Windows Vista [viitattu 27.3.2007]. saatavissa: http://support.microsoft.com/kb/926170

Microsoft. 2007b [verkkodokumentti]. MS-CHAP authentication method [viitattu 26.3.2007]. saatavissa: http://www.microsoft.com/technet/isa/2004/help/FW_MSChap.mspx?mfr=truev

Microsoft. 2007c [verkkodokumentti]. Virtual private networking with IPSec [viitattu 5.4.207]. saatavissa: http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/sag_ipsectunnel.mspx?mfr=true

RFC 2104. 1997 [verkkojulkaisu]. HMAC: Keyed-Hashing for Message Authentication [viitattu 3.4.2007]. saatavissa: http://www.ietf.org

RFC 2373. 1998 [verkkojulkaisu]. IP Version 6 Addressing Architecture [viitattu 2.4.2007]. saatavissa: http://www.ietf.org

RFC 2637. 1999 [verkkojulkaisu]. Point-to-Point Tunneling Protocol (PPTP) [viitattu 28.3.2007]. saatavissa: http://www.ietf.org

RFC 3078. 2001 [verkkojulkaisu]. Microsoft Point-To-Point Encryption (MPPE) Protocol [viitattu 2.4.2007]. saatavissa: http://www.ietf.org

RFC 3193. 2001 [verkkojulkaisu]. Securing L2TP using IPsec [viitattu 4.42007]. saatavissa: http://www.ietf.org

RFC 4301. 2005 [verkkojulkaisu]. Security Architecture for the Internet Protocol [viitattu 29.3.2007]. Saatavissa: http://www.ietf.org

RFC 4303. 2005 [verkkojulkaisu]. IP Encapsulating Security Payload (ESP) [viitattu 29.3.2007]. Saatavissa: http://www.ietf.org

RFC 4305. 2005 [verkkojulkaisu]. Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH) [viitattu 29.32007]. Saatavissa: http://www.ietf.org

RFC 4306. 2005 [verkkojulkaisu]. Internet Key Exchange (IKEv2) Protocol [viitattu 29.32007]. Saatavissa: http://www.ietf.org

RFC 4772. 2006 [verkkojulkaisu]. Security Implications of Using the Data Encryption Standard (DES) [viitattu 2.4.2007]. Saatavissa: http://www.ietf.org

RSA Laboratories. 2007 [verkkodokumentti]. 2.1.1 What is public-key cryptography? [viitattu 27.3.2007]. Saatavissa: http://www.rsa.com/rsalabs/node.asp?id=2165

Wikipedia. 2007a [verkkodokumentti]. MD5 [viitattu 26.3.2007]. Saatavissa: http://fi.wikipedia.org/wiki/MD5

Perlmutter, P. & Zarkower, J. 2000, Virtuaaliset yksityisverkot. Edita Oyj, Helsinki

Gollmann, D. 1999, Computer Security. John Wiley & Sons Ltd, West Sussex, England

Schneider, B. 1996, Applied Cryptography – Protocols, Algorithms, and Source Code in C. John Wiley & Sons, Inc, Yhdysvallat