hyväksymispäivä arvosana

arvostelija

Langattomien laitteiden tietoturva

Tea Silander

Helsinki 19.4.2003

HELSINGIN YLIOPISTO
Tietojenkäsittelytieteen laitos

Matemaattis-luonnontieteellinen | Tietojenkäsittelytieteen laitos

Tekijä — Författare — Author
Tea Silander

Työn nimi — Arbetets titel — Title

Langattomien laitteiden tietoturva

Oppiaine — Läroämne — Subject
tietojenkäsittelytiede

Työn laji — Arbetets art — Level	Aika — Datum — Month and year	Sivumäärä — Sidoantal — Number of pages
aine	19.4.2003	15 sivua

Tiivistelmä — Referat — Abstract

Langattoman tietojenkäsittelyn osuus nykyaikaisessa liiketoimintaympäristössä on kasvanut viimeisten vuosien aikana huomattavasti. Siirtyminen langattomaan ympäristöön on tuonut tietoturvan alalle uusia uhkia, jotka ovat tyypillisiä vain langattomalle siirtomedialle ja tätä mediaa käyttäville päätelaitteille.

Uudet uhkat kohdistuvat esimerkiksi käytettyyn siirtomediaan, laitteiden sisältämän tiedon turvaamiseen sekä luotettavuuteen. Esimerkiksi radioaallot ovat haavoittuvaisempia palvelunestohyökkäyksille ja liikenteen salakuuntelulle sekä väärentämiselle kuin fyysisen linkin yli tapahtuva tiedonsiirto.

Tämä artikkeli käsittelee langattoman tiedonsiirron ominaisuuksia ja sen mukanaan tuomia uusia uhkia.

Avainsanat — Nyckelord — Keywords
tietoturva, langattomat laitteet

Säilytyspaikka — Förvaringsställe — Where deposited

Muita tietoja — övriga uppgifter — Additional information

Sisältö

1 Johdanto

Nykypäivän tietojenkäsittely on siirtynyt yhä suuremmaksi osaksi langattomiin laitteisiin, kuten kannettaviin tietokoneisiin, PDA-laitteisiin (Personal Digital Assistent) sekä älypuhelimiin, joilla käyttäjä voi kommunikoinnin lisäksi selata tietoa ja ladata sovelluksia Internetissä [JKG02, Lea00]. Strategia-analyytikot monien muiden markkinatutkimusryhmien tavoin uskovat langattomien laitteiden määrän ylittävän miljardi laitetta vuoteen 2004 mennessä [GhS01]. Siirtyminen langattomaan ympäristöön on tuonut tietoturvan alalle uusia uhkia, jotka ovat tyypillisiä vain langattomalle siirtomedialle ja tätä mediaa käyttäville päätelaitteille [GhS01]. Uudet uhkat kohdistuvat esimerkiksi käytettyyn siirtomediaan, laitteiden sisältämän tiedon turvaamiseen sekä luotettavuuteen. Myös langattomiin laitteisiin sekä näille tarjottaviin palveluihin voidaan kohdistaa palvelunestohyökkäyksiä. Lisäksi laitteiden tyypilliset ominaisuudet aiheuttavat ongelmia esimerkiksi fyysisen tietoturvan ja laskentatehokkuuden kannalta [RHC02].

Langattomat laitteet siirtyvät monien erilaisten, mahdollisesti epäluotettavien tietoliikenneverkkojen läpi, joista ne saavat palvelua ja joissa ne suorittavat datan vaihtoa [GhS01]. Tällöin informaatiota voidaan varastaa tai muuttaa ilman että käyttäjä edes huomaa tätä. Uusien teknologioiden myötä tulevien hyötyjen mukana seuraa myös riskejä [Kel02]. Uudet käyttöönotetut teknologiat mahdollistavat uudet keinot petoksille ja varkauksille. McAfee Securityn apulaistoimitusjohtajan Arvind Narainin mukaan tietoturvauhkia ei mobiiliverkoissa koeta vielä todellisesti, vaan ne tulevat kasvamaan huomattavasti lähivuosina kehittyneemmän teknologian yleistyessä, jolloin mobiilikentän kiinnostavuus herää myös hakkereissa ja virusten tekijöiden parissa.

Luvussa kaksi käsitellään langattoman ja langallisen tiedonsiirron eroja, sekä langattomaan tiedonsiirtoon käytettyjen laitteiden ominaispiirteitä. Luvussa kolme esitellään laitteisiin kohdistuvia tietoturvauhkia ja eräs näihin ongelmiin esitelty ratkaisu. Luvussa neljä kerrotaan millaisia palvelunestohyökkäyksiä langattomiin laitteisiin, siirtomediaan tai laitteille tarjottuihin palveluihin ja palveluntarjoajiin voi esiintyä. Viides luku esittelee session kaappaamiseen ja vastapuolen väliin pääsyyn liittyviä tietoturvauhkia. Kuudes luku on yhteenveto.

2 Langattomuuden mukanaan tuomia eroja

Langattomalla laitteella tarkoitetaan kannettavaa tietokonetta tai muuta langatonta laitetta, joka käyttää jotakin käyttöjärjestelmää. Tässä yhteydessä langaton laite myös liikkuva. Langattomat laitteet saattavat parantaa yrityksen työntekijöiden tuottavuutta [JKG02], mutta aiheuttavat yritykselle uusia huomioonotettavia riskejä, koska laitteet kykenevät tallettamaan ja siirtämään yritykseen liittyvää tietoa sekä langattomissa että langallisissa verkoissa. Langattomalla tiedonsiirrolla on langalliseen verrattuna ominaispiirteitä, jotka johtuvat lähinnä käytetystä siirtomediasta sekä laitteiden ominaisuuksista.

2.1 Langaton siirtomedia

Langattoman (*wireless*) ja langallisen (*wired*) tietoliikenteen välillä on olennaisia eroja, jotka sulkevat pois osan langalliseen tiedonsiirtoon suunnitelluista tietoturvaprotokollista [Per98]. Erot johtuvat lähinnä langattomien verkkojen käyttäjän liikkuvuudesta sekä kommunikointiin käytetyn langattomasta siirtomediasta [GhS01, GHW02].

Langallisessa tiedonsiirrossa:

- siirto pitkin fyysistä linkkiä
- suuri siirtonopeus
- pieni virhetodennäköisyys

Langattomassa tiedonsiirrossa:

- siirto käyttäen erilaisia tekniikoita, useimmiten radioaaltoja
- siirron kustannukset suuret verrattuna tiedonsiirtoon käyttäen langallista linkkiä
- matala ja mahdollisesti laadultaan vaihteleva siirtonopeus
- suuri virhetodennäköisyys

- päästä päähän -kommunikointi (*point-to-point*) tai epämääräinen tai heikosti määritetty lähetyskantama

Langattomassa tiedonsiirrossa hyödynnetään erilaisia tekniikoita, muun muassa mikroaalto- ja infrapunataajuudella toimiviat sekä lasertekniikkaa hyödyntävää. Näillä tekniikoilla on erilaiset ominaisuudet, jotka voivat tuottaa ongelmia, suurimpina rajoittimina siirtomatka, siirtokapasiteetti sekä näköyhteys. Käytettäessä infrapunavaloa siirtokeinona ongelmaksi muodostuu auringon- ja keinovalon sisältämä infrapunasäteily, joka aiheuttaa häiriöitä. Yleensä infrapunayhteyksiä käytetäänkin vain hyvin lyhyillä yhteyksillä esimerkiksi kannettavan tietokoneen ja printterin välillä, jolloin päästään kohtalaiseen siirtonopeuteen.

Johtuen langattomaan tiedonsiirtoon käytetyistä tekniikoista, kommunikointia voivat häiritä toiset käyttäjät, muut laitteet, pahantahtoiset hakkerit tai luonnonilmiöt [GHW02]. Osa olemassa olevista langalliseen tietoliikenteeseen suunnitelluista protokollista on käyttökelvottomia siksi, että ne olettavat laitteiden olevan laskennallisesti kykeneviä turvaamaan yhteyden, esimerkiksi suorittamalla julkisen avaimen SSL-operaatioita [RHC02]. Nämä protokollat eivät myöskään ota huomioon sitä, että siirtonopeus voi välillä hidastua merkittävästi tai yhteys katketa kokonaan ja käyttäjän identiteetti voidaan väärentää [JKG02].

Langattomassa tiedonsiirrossa on otettava huomioon se, että käytettäessä radioaaltoja langattomaan tiedonsiirtoon, radioaallot on rajallinen resurssi, joka on kaikkien kuultavissa ja siten erittäin herkkä erilaisille hyökkäyksille sekä salakuuntelulle [GHW02]. Vaikka tällä hetkellä suurin osa langattomista verkoista toimivatkin 2,45 GHz:in taajuusalueella, tulee toiminta tulevaisuudessa oletettavasti siirtymään luvanvaraisille taajuuksille. Syynä tähän on jo nyt useiden muidenkin sovellusten toimiminen samalla alueella, joten alueen käydessä ruuhkaiseksi, ei sillä käytettäville laitteille voida taata häiriötöntä toimintaa.

2.2 Langattomat laitteet

Langattomat laitteet, kuten PDA:t on tarkoituksellisesti pyritty suunnittelemaan mahdollisimman pieniksi ja kevyiksi, jotta käyttäjä todella kykenee kuljettamaan laitetta mukanaan ja työskentelemään sillä paikasta riippumatta. Kuitenkin lait-

teiden pieni koko aiheuttaa niiden toiminnalle rajoitteita [JKG02].

Laitteiden käytön kannalta on ongelmallista se, että niillä on yleensä varsin rajallinen virtalähde ja ne ovat laskennallisesti tehottomia laitteita, joilla on kannettavia lukuun ottamatta rajallinen muisti ja tietoliikennekapasiteetti [RHC02]. Tämän lisäksi laitteilla saattaa olla hyvin rajallinen näyttö, joka ei välttämättä kykene näyttämään käyttäjän haluamaa sisältöä. Lisäksi pienikokoisten langattomien laitteiden kuten PDA-laitteiden ja puhelimien laskentakapasiteetin rajallisuus vaikuttaa niiden mahdollisuuksiin salata niiden sisältämä tai lähettämä tieto riittävän hyvin. Esimerkiksi 3Com Palm Pilot V -laittelta kuluu standardi SSL-kättely vaiheen suorittamiseen useita sekunteja [RHC02]. Tämän kaltainen viive yhteyden muodostamisessa on erittäin epäsuotava langattomissa ympäristöissä, varsinkin silloin kun yhteys on huono.

3 Langattomiin laitteisiin liittyvät tietoturvauhat

Langattomille laitteille on tyypillistä se, että ne ovat kooltaan pieniä, niillä on rajallinen muisti ja laskentateho, rajallinen käyttöliittymä ja näyttö sekä keinot synkronoida tietonsa esimerkiksi pöytäkoneen kanssa [JKG02]. Koska langattomat laitteet ovat yleensä käyttäjänsä omistuksessa, syöttävät käyttäjät henkilökohtaista tietoa niihin paljon luottavaisemmin kuin esimerkiksi työpaikkojensa koneisiin, joita työnantaja saattaa valvoa [GhS01]. Usein langattomat laitteet kykenevät kommunikoimaan toistensa kanssa rajallisen alueen sisällä käyttäen infrapuna- tai radioaaltoja [JKG02].

Langattomilla laitteilla itsellään on niiden luonteesta johtuen monia tietoturvauhkia. Langattomien laitteiden on kiinteisiin koneisiin verrattuna pienestä koostaan johtuen todennäköistä kadota, jäädä ilman valvontaa tai tulla varastetuksi [GhS01, JKG02]. Käyttäjän tunnistusmekanismi, kuten salasanakysely saatetaan kytkeä pois, jolloin laitteen sisältö paljastuu kenelle tahansa, joka saa laitteen haltuunsa [JKG02]. Tunnistusmekanismin poiskytkeminen saattaa olla jopa oletusasetus ja vaikka käyttäjän tunnistus olisikin käytössä, saattaa autentikointimekanismi olla heikko tai helposti kierrettävissä. Langattoman laitteen sisältämä tieto saattaa olla löytäjälleen arvotonta, mutta käyttäjälleen korvaamatonta kadotessaan, varsinkin kun laitteen sisältämästä tiedosta ei ole tehty varmuuskopioita [GhS01]. Yritykselle kuuluvan langattoman laitteen joutuessa varkauden kohteeksi on riski, että laitteen varastanut henkilö pääsee laitteella käsiksi esimerkiksi yrityksen tietojärjestelmään, postipalvelimelle tai muihin tietokantoihin ja saa tätä kautta käsiinsä salaista tai yritykselle haitallista tietoa.

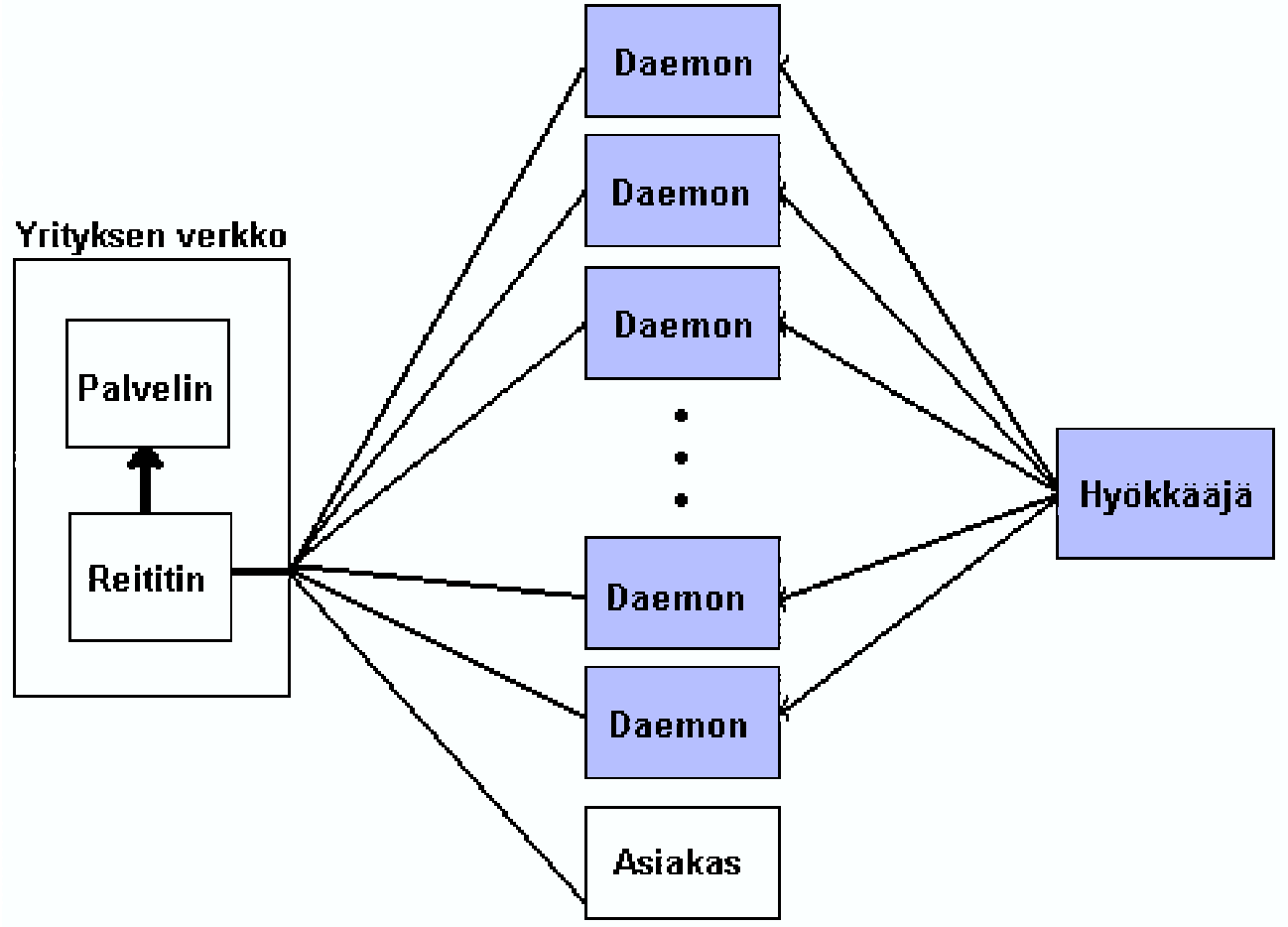
Langaton tiedonsiirto voidaan siepata ja jos dataa ei ole salattu tai salaus on tehty viallisella protokollalla voidaan viestien sisältö saada selville [JKG02]. Yrityksen on hankalaa ellei mahdotonta valvoa työntekijöidensä langattomien laitteiden siirtymistä yrityksen verkkoon ja sieltä jälleen ulos. Esimerkiksi työntekijän suorittama PDA-laitteen synkronointi yrityksen verkossa olevan pöytäkoneensa kanssa muodostaa riskin yrityksen verkolle [JKG02]. Haitallista koodia sisältävä PDA-laite ohittaa työntekijän matkassa fyysisesti yrityksen palomuurin ja sen sisältämät tietoturvaohjelmistot. Haitallinen koodi pääsee näin leviämään yrityksen verkon sisällä siirryttyään ensin yhteen pöytäkoneista synkronoinnin yhteydessä.

Johtavilta teollisuusyrityksiltä kerätyistä ohjeista on muodostettu 15 askeleen ohjeet järjestelmänvalvojille, joilla saavutetaan riittävä tietoturvan taso langattomissa ympäristöissä [Kel02]. Ohjeiden mukaan langattomien laitteiden tietoturvaa saadaan parannettua olennaisesti muuttamalla tuotteen oletus- tai tehdasasetuksia. Kaikki laitteet tulisi myös varustaa virustentorjuntaohjelmistolla, joka tulee päivittää riittävän usein. Esimerkiksi yritysten ja julkisten organisaatioiden tulisi tarjota verkkoaan käyttäville työntekijöilleen tällainen ohjelmisto ja päivityspaketit.

Langattomissa laitteissa osa riskeistä liittyy ohjelmistoalustaan (*platform*) [GhS01]. Varsinkin PDA-laitteiden eräs suuri ongelmana nykyisten langattomien laitteiden kanssa on varman autentikointimekanismin puute. Esimerkiksi kehitteillä olevat biometriset tunnistuskeinot ovat varma tapa tunnistaa kunkin laitteen omistaja [GhS01, JKG02]. Alustan tulisi tarjota muistin suojaus prosesseilta sekä hiekkalaatikko epäluotettavan koodin suorittamiseen [GhS01]. Huomiota tulee myös kiinnittää ohjelmistoalustan tiedostonpääsynvalvontaan ja kernelin suojaukseen.

Eräänä ratkaisuna langattomien laitteiden ominaisuuksien mukanaan tuomiin ongelmiin on esitetty digitaalisia sertifikaatteja [JKG02]. Tietoturva- tai järjestelmävastaajan muodostettua sertifikaatin, tämä tallennetaan joko työntekijöiden pöytäkoneisiin tai yrityksen sertifikaattipalvelimelle. Käyttäjän suorittaessa langattoman laitteensa synkronoinnin tai muita operaatioita, järjestelmä tarkistaa ensin onko kyseisellä laitteella voimassaoleva sertifikaatti. Jos sertifikaattia ei ole tai se ei ole voimassa, tietyt laitteen suorittamat tehtävät ovat estetty. Käyttäjän hankkiessa sertifikaatin langattomalle laitteelle, sertifikaatti astuu voimaan kun laitteen asetukset ovat nostettu sertifikaatin esittämälle tasolle. Sertifikaatin hyvänä puolena on se, että samat politiikat saadaan jaettua eri laitteille. Huonona puolena on kuitenkin se, että sertifikaatin vaatimukset kertova politiikkataulu (*policy table*) on laitteen keskusmuistissa, jolloin sitä pystytään väärentämään.

4 Palvelunestohyökkäykset



Kuva 1: Hajautettu palvelunestohyökkäys [GHW02].

Palvelunestohyökkäyksessä hyökkääjä ei koskaan yritä murtautua uhrinsa systeemiin, vaan hyökkäyksen tavoitteena on saattaa käyttäjän järjestelmä tilaan, jossa sen käyttö on normaalia hitaampaa tai täysin estetty [GHW02, ITE02]. Kuvassa 1 esitetty hajautettu palvelunestohyökkäys (*Distributed Denial-of-Service, DDoS*) on edistyneempi muoto palvelunestohyökkäyksestä [GHW02]. Kuten nimi kertoo, hajautetussa palvelunestohyökkäyksessä hyökkäys tapahtuu monen koneen voimin, jotka ovat hajautettu verkon yli. Hyökkäyksen torjuminen on vaikeampaa, sillä torjuttava liikenne tulee useasta osoitteesta, eikä näitä kyetä erottamaan oikeista palvelupyynnöistä. Hajautettua palvelunestohyökkäystä varten hyökkääjä tarvitsee käyttöönsä useita koneita (*zombie, daemon computers*), joiden omistajat yleensä ovat täysin tietämättömiä osallisuudestaan palvelunestohyökkäykseen. On olemassa monia työkaluja [GHW02], joiden avulla hyökkääjä saa zom-

biekoneet automaattisesti lähettämään synkronisesti liikennettä kohteeseen, joka usein estää oikeiden käyttäjien pääsyn palveluun. Kaikki nämä työkalut ovat saatavilla lähdekoodeineen ja uusia versioita ilmestyy jatkuvasti.

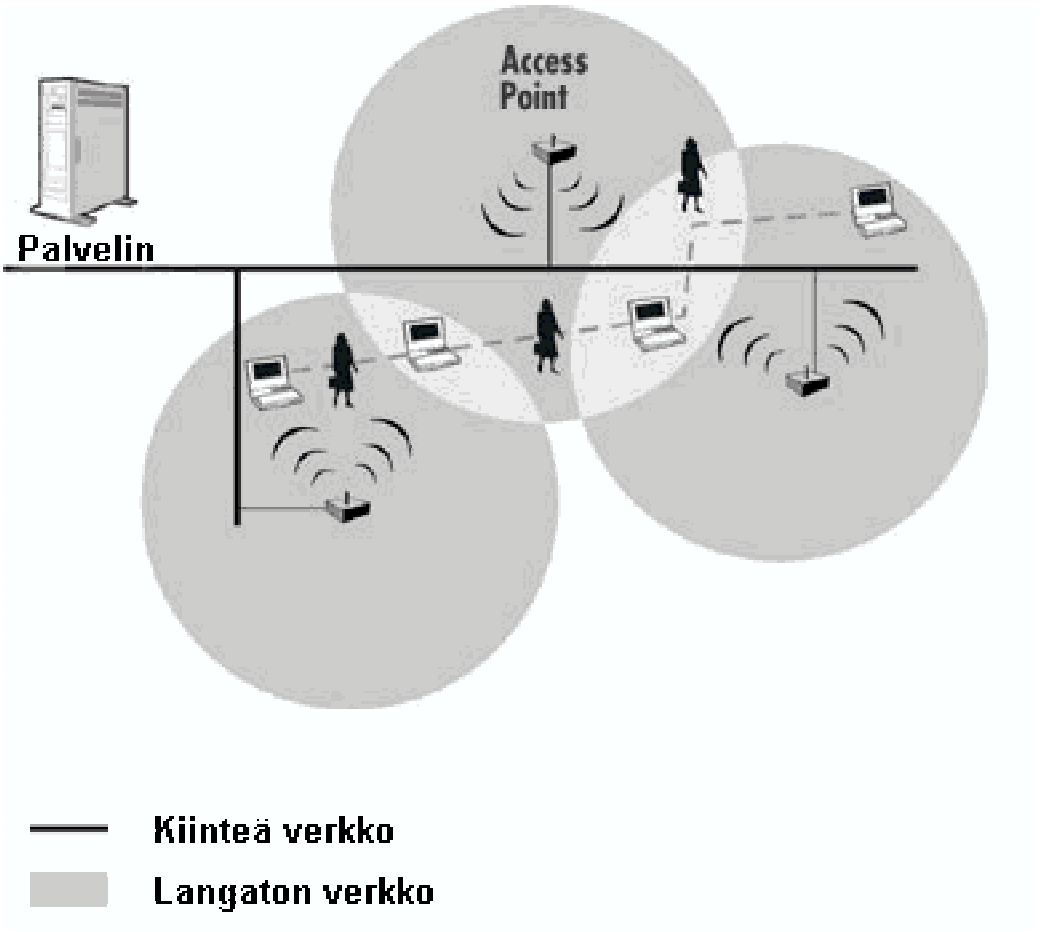
Hyökkääjä voi myös käyttää korkeataajuisia radiosignaaleja tuottavaa laitetta estääkseen langattomia laitteita toimimasta [ITE02]. Laitteen tuottamat radiosignaalit sotkevat lähialueen langattomien laitteiden radiosignaalit niin etteivät ne kykene kommunikoimaan.

Internet voidaan jakaa karkeasti kolmen tyyppisiin verkkoihin sovellusten mallien perusteella [GHW02]. Mallit ovat langaton laajennettu Internet (*Wireless Extended Internet*), johon myös langaton lähiverkko (*Wireless Local Area Network, WLAN*) kuuluu, langaton portraaliverkko (*Wireless Portral Network*), jossa asiakkaalle tarjotaan palveluita sekä langattomat ad hoc -verkot.

4.1 Langaton laajennettu Internet

Käytettäessä langatonta tekniikkaa langallisen Internetin jatkeena kyseessä on langaton laajennettu Internet [GHW02]. Langattomat palvelun tarjoajat (*Internet Service Provider, ISP*) tarjoavat langattomille laitteille pääsyn kiinteään verkkoon radiokanavan (*radio frequency, RF*) kautta. Kiinteässä ja langattomassa verkossa ovat käytössä asiakas-palvelin -arkkitehtuuri sekä kuljetuskerroksen protokollat (yleensä TCP). Langaton laajennettu Internet poikkeaa kiinteästä verkosta mm. verkkorakenteessa, joka on esitetty kuvassa 2. Verkon langaton osa on yhdistetty kiinteään verkkoon pääsypisteillä (*access point*). Myös langaton laajennettu Internet on haavoittuvainen hajautetulle palvelunestohyökkäykselle [GHW02]. Hyökkäykset voivat kohdistua liikennettä käsitteleviin laitteisiin, epäsymmetriseen rakenteeseen, sekä radioaaltoihin.

Langattomissa verkoissa on laitteita, jotka käsittelevät, tai joiden kautta kulkee suuri osa verkon liikenteestä [GHW02]. Tällaisiin liikennettä kerääviin laitteisiin (*devices using aggregated traffic*) kohdistettu palvelunestohyökkäys lamaannuttaa helposti suuren osa verkosta. Tällaisia laitteita ovat esimerkiksi tukiasemat ja pääsypisteet. Näiden laitteiden toimintaa voi hidastaa esimerkiksi lähettämällä



Kuva 2: Langaton laajennettu Intenet.

jatkuvaa liikennettä laitteille.

Langattoman verkon epäsymmetrisellä rakenteella (*asymmetric structure*) tarkoitetaan langattoman laajennetun Internetin tapauksessa sitä, että verkon langaton osuus on huomattavasti tehottomampi verrattuna kiinteään verkkoon. Langattomissa laitteissa on vähemmän laskentatehoa ja kommunikointikykyä kuin kiinteissä laitteissa [GHW02, JKG02]. Hajautettu palvelunestohyökkäys voi helposti lamaannuttaa langattomat laitteet suurelta alueelta, vaikka hyökkäykseen käytettäisiinkin harvoja, mutta tehokkaita koneita [GHW02]. Langattoman Internetin sisältöpalvelimet, kuten WAP-, Instant Message - sekä pelipalvelimet ovat usein optimoitu vastaamaan palvelupyyntöihin nopeasti olettamalla niille käsiteltäväksi saapuvien palvelupyyntöjen määrä pieneksi. Varsinkin tämä tekee niistä erittäin herkkiä palvelunestohyökkäyksille.

Radiospektriin voidaan kohdistaa palvelunestohyökkäyksiä [GHW02]. Radioaaltojen rajallinen määrä tekee siitä langattoman tiedonsiirron pullonkaulan ja näin potentiaalisen palvelunestohyökkäyksen kohteen . Siirtomedian allokointi ja valvontakontrollit nojaavat stokastisiin teorioihin, jotka olettavat etteivät kaikki käyttäjät käytä laitteitaan samaan aikaan. Tästä johtuen verkon todellinen siirtokapasiteetti saattaa olla paljon pienempi kuin kaikkien verkon laitteiden yhteenlaskettu kapasiteetti. Lähettämällä riittävän määrän normaalia liikennettä simuloivaa liikennettä verkkoon kykenee hyökkääjä sotkemaan radioaaltoja niin että oikeiden asiakkaiden liikenne sotkeutuu.

4.2 Langattomat portraaliverkot

Eniten julkisuutta saanut langaton portraaliverkko on oletettavasti NTT DoCoMo, jossa lähes 5,9 miljoonaa käyttäjää käytti i-mode -palveluita neljän viimeisen kuukauden aikana vuonna 2000 [GHW02]. Langattomien portraaliverkkojen suuren suosion takia niistä on tullut potentiaalinen palvelunestohyökkäyksen kohde. Langattomat portraaliverkot perustuvat yleensä asiakas-palvelin -arkkitehtuuriin. Asiakkaat ovat yleensä matka- tai älypuhelimia sekä PDA-laitteita.

Langattomiin portraaliverkkoihin voidaan kohdistaa hyökkäyksia esimerkiksi radiospektrin kautta [GHW02]. Portraaliverkot käyttävät yleensä olemassa olevia matkapuhelinverkkoja, joissa yksi tukiasema huolehtii oman solunsa liikenteestä. Suurissa kaupungeissa tai tapahtumissa syntyy tilanteita, joissa tukiasema ei pysty huolehtimaan kaikesta liikenteestä, jolloin matkapuhelimella ei saa yhteyttä verkkoon. Tämän kaltaista luonnollista ruuhkaa matkimalla hyökkääjä voi lamaannuttaa alueen tukiaseman, jolloin asiakkaat eivät saa yhteyttä verkkoon eivätkä pääse käyttämään portraaliverkon palveluita.

Jos hyökkääjä pääsee portraaliverkon sisälle on mahdollista yrittää lamaannuttaa portraaliverkon tarjoamia palveluita lähettämällä riittävän määrän palvelupyyntöjä [GHW02]. Tämä on kuitenkin erittäin vaikeaa, sillä kaikista arvokkaimmille palveluille on yleensä varattu täysin erilliset kommunikointikanavat ja palveluiden käyttöastetta valvotaan tarkasti.

Langattomissa portraaliverkoissa TCP/IP-yhdyskäytävä kääntää langattomien asiakkaiden lähettämän liikenteen TCP/IP-protokollien muotoon ja päinvastoin [GHW02]. Yhdyskäytävällä tulee olla riittävästi laskenta- ja tiedonsiirtotehoa, jotta se selviää kuormastaan. Jos yhdyskäytävä jostakin syystä menee epäkuntoon, on portraaliverkko tällöin eristetty muusta Internetistä. Tällöin Internetin tarjoamat palvelut ovat portraaliverkon asiakkaiden saavuttamattomissa.

4.3 Langattomat ad-hoc -verkot

On myös tilanteita, jolloin joukko käyttäjiä haluaa kommunikoida vapaasti, ilman infrastruktuuriverkkoa [GHW02]. Tällöin kyseessä on ad-hoc -verkko. Ad-hoc-verkossa työasemat kommunikoivat suoraan toistensa kanssa ja yhteys voi rakentua ilman järjestelmänhallintaa. Välimatkat ovat tällaisilla yhteyksillä hyvin rajatut, riippuen lähinnä siirtotekniikasta. Ad-hoc -verkoista on tullut merkittävä sovellus ryhmäkommunikoinnissa ja sitä käytetään esimerkiksi kokouksissa tiedon välittämiseen [GhS01].

Ad-hoc -verkossa kukin solmu toimii oman alueensa reitittimenä [GhS01]. Hyökkääjä saattaa asettaa ad-hoc -verkkoon solmun, joka välittää muille solmuille väärää reititystietoa. Tällöin ad-hoc -verkko saattaa kaatua tai hyökkääjä saattaa ohjata kaiken liikenteen kulkemaan yhden solmun kautta.

5 Session kaappaaminen, Man-in-the-Middle

Luvussa kolme esitellyn 15 askeleen listan mukaan järjestelmänvalvojan on ehdottoman tärkeää muuttaa verkon reitittimeen tai pääsypisteeseen tehtaalla asetetut oletusasetukset ja salasanat, sillä yleensä hakkerit yrittävät ensimmäisenä juuri näitä salasanoja yrittäessään luvatonta pääsyä esimerkiksi yrityksen verkkoon [Kel02]. Esimerkiksi suurin osa langattoman verkon pääsypisteistä lähettää oletusarvoisesti SSID:tään (Service Set ID) säännöllisin väliajoin, jotta asiakaskoneet löytäisivät sen [ITE02]. SSID-tunnuksen selville saava hakkeri voi asettaa langattoman asiakaspäätteen verkkoon, jolla hakkeri pystyy matkimaan oikeaa asiakasta saadakseen riittävän paljon informaatiota hyökkäystä varten.

Koska langattomissa verkoissa tieto siirretään ilmassa käyttäen sähkömagneettista säteilyä, on selvää, että se leviää väistämättä jossain määrin ympäristöön [GHW02]. Tässä on eri tekniikoilla taas eronsa. Radioaallot kulkevat jopa useiden kilometrien päähän ja käytännössä kaikki siirrettävä tieto on jaettu kaikkien lähialueella olevien kanssa. Teollisuusyrityksiltä kerättyjen 15 askeleen ohjeiden mukaan tähän voidaan vaikuttaa pääsypisteiden sijoittelulla [Kel02]. Jos pääsypisteet sijoitetaan ikkunoiden välittömään läheisyyteen, on ulos heijastuva signaali huomattavasti vahvempi, kuin jos ne olisivat sijoitettu rakennuksen keskelle. Toinen keino pulman selvittämiseen on salauksen käyttö [GuM98]. Teknisesti salaus voidaan sijoittaa mihin tahansa kerrokseen, tehokkain se kuitenkin on alemmissa kerroksissa. Käytännössä esimerkiksi tavallinen WLAN-verkon turvallinen käyttö vaatii salatun verkkokerroksen. Salakuuntelu on WLANin tapauksessa kuitenkin vaikeaa, sillä radiosignaali perustuu hajaspektritekniikkaan ja yhteys toimii useimmiten salattuna PPTP- tai IPSec -tunnelin läpi.

Langattoman verkon käyttö hyökkäykseen tarjoaa hakkereille hyvän suojan kiinnijoutumiselle [GhS01]. Koska langattomat laitteet vaeltavat langattomien alueiden välillä, niillä ei ole mitään tiettyä maantieteellistä kiintopistettä ja ne voivat olla välillä poiskytkettyinä verkosta (*offline*), jolloin ne ovat vaikeasti tavoitettavissa. Tällöin hyökkäyksen suorittaneen laitteen jäljittäminen on paljon vaikeampaa verrattuna kiinteään verkkoon.

5.1 Man-in-the-Middle

Man in the middle -hyökkäyksellä tarkoitetaan tilannetta, jossa kolmas osapuoli eli hakkeri kaappaa ja mahdollisesti väärentää kommunikoivien osapuolien viestejä [Kel02]. Hakkeri voi toteuttaa hyökkäyksen esimerkiksi sijoittamalla pääsypisteen riittävän lähelle kohdetta [ITE02]. Käyttäjän käyttäjätunnus ja salasana paljastuvat kolmannelle osapuolelle, kun kohde on yhteydessä tähän väärennettyyn access-pointiin. Kuitenkin hakkerin on oltava silloin kohteensa verkon sisällä tai välittömässä läheisyydessä, jotta pääsypiste olisi lähempänä kuin kohteen lähin. Tältä riskiltä voi 15 askeleen ohjeen riittävän tietoturvatason saavuttamiseksi mukaan turvautua suunnittelemalla verkon pääsypisteiden sijoittelun riittävän tarkasti sekä kiinnittämällä riittävän paljon huomiota fyysiseen tietoturvaan [Kel02].

GSM-tekniikkaan perustuvassa tiedonsiirrossa man-in-the-middle -hyökkäyksen toteuttaminen on vieläkin helpompaa, sillä laitteen ottaessa yhteyttä tukiasemaan laite identifioi itsensä, mutta tuliaseman ei tarvitse suorittaa vastaavaa operaatiota [Kel02]. Hyökkääjän tarvitsee vain sijoittaa kannettava tietokone ja siihen kytketty, hieman muunneltu GSM-puhelin tukiaseman ja hyökkäyksen kohteen väliin. Kannettava kone ja GSM-puhelin toimivat kuten tukiasema ja lähettävät tunnustaan lähellä sijaitseville puhelimille. Koska tuliaseman ei tarvitse identifioida itseään siihen yhteyttä ottaneelle asiakkaalle, saa hyökkääjä haltuunsa asiakkaiden tunnuksia ja voi käyttää näitä tunnuksia esimerkiksi uhrinsa salakuunteluun.

5.2 Session kaappaaminen

Session kaappaamisessa on kyse siitä, että hakkeri kaappaa viestejä ja syöttää verkkoon väärennettyjä viestejä [ITE02]. Langattomissa verkoissa transaktio voidaan keskeyttää ja käynnistää uudelleen, eikä osapuolien autentikointia usein suoriteta tällöin uudelleen [GhS01]. Myös yhteyden muodostaminen uudelleen vain päivittämällä (*refresh*) selainta saattaa sisältää riskejä. Molemmissa tapauksissa pyynnöt (*request*) voidaan ohjata uudelleen ja palauttaa väärennettyjä viestejä tai jopa vahingollista koodia odotetun datan sijaan. Monet SSL:n (Secure Socket Layer) ja WTSL:n (Wireless Transport Layer Security) kaupalliset versiot eivät suorita osapuolien autentikointia tai sertifikaattien tarkistusta uudelleen kun yh-

teys on jo kertaalleen muodostettu.

Session kaappaaminen voidaan myös suorittaa esimerkiksi DNS-palvelimen (Domain Name Server) kautta. Jos hakkeri saa lähimmän DNS-nimipalvelimen ohjaamaan tietyn osakevälittäjän sivustolle tulevat pyynnöt omalle peilisivustolleen, saa hän haltuunsa kyseisen DNS-palvelimen alueella osakevälittäjän palvelua käyttävien käyttäjien tietoja, kuten tilinumeroita ja osakemääriä [GhS01].

6 Yhteenveto

Tässä artikkelissa käsiteltiin langattoman tiedonsiirron mukanaan tuomia uusia tietoturvauhkia. Verrattuna perinteiseen langalliseen tiedonsiirtoon, langattoman tiedonsiirron tekee erilaiseksi käyttäjän liikkuvuus ja langaton tiedonsiirtomedia. Kun käyttäjä liikkuu siirtäessään tietoa, kulkee hän erilasten verkkojen alueella, joiden tietoturvapolitiikat voivat olla hyvinkin erilaisia. Siirrettäessä tietoa langattomissa verkoissa tulisi tietoturvakysymyksissä ottaa huomioon käytetty tiedonsiirtomedia. Radioaallot ovat haavoittuvaisempia palvelunestohyökkäyksille ja liikenteen salakuuntelulle sekä väärentämiselle kuin fyysisen linkin yli tapahtuva tiedonsiirto. Laitteiden fyysiset ominaisuudet altistavat laitteet palvelunestohyökkäyksien tai jopa varkauden kohteeksi herkemmin kuin perinteiset pöytäkoneet. Myös hyökkääjän jäljittäminen on vaikeampaa langattomissa ympäristöissä, sillä langattomat laitteet liikkuvat verkkojen välillä ja ovat toisinaan poiskytkettyinä verkosta.

Lähteet

GhS01 Ghosh, A. K., Swaminatha, T. M.
Software Security and Privacy Risks in Mobile E-Commerce,
Communications of the ACM, Vol. 4, No. 2, s. 51-57, February 2001.

GHW02 eng, X., Huang, Y., Whinston, A. B.,
Defending Wireless Infrastructure Against the Challenge of DDoS Attacks Mobile Networks and Applications,
Vol. 7, No. 3, s. 213-223, 2002.

GuM98 Gupta, V., Montenegro, G.
Secure and Mobile Networking,
Mobile Networks and Applications, Vol. 3, s. 381-390, 1998.

ITE02 IT in Education project
Wireless LAN Security,
The Government is HKSAR, Education Department, Infrastructure Division, December 2002.

JKG02 Jansen, W. A., Karygiannis, T., Gavrila, S., Korolev, V.
Assigning and Enforcing Security Policies on Handheld Devices,
Proceedings of the Canadian Information Technology Security Symposium, May 2002.

Kel02 Kellerman, T.
Mobile Risk Management: E-finance in the Wireless Environment,
Financial Sector Discussion Paper, The World Bank, May 2002.

Lea00 Leavitt, N.
Malicious Code Moves to Mobile Devices,
IEEE Computer Society, p. 16-19, December 2000.

Per98 Perkins, C. E.,
Mobile Networking in the Internet,
Mobile Networks and Applications, Vol. 3, s. 319-334, 1998.

RHC02 Ross, S.J., Hill, J.L., Chen, M.Y., Joseph, A.D., Culler, D.E., Brewer, E.A.
A Composable Framework for Secure Multi-Modal Access to Internet Services from Post-PC Devices,
Mobile Networks and Applications, Vol. 7, p. 389 - 406, 2002.