Laajennettu tiivistelmä

Langattomien laitteiden ja sovellusten tietoturva

Helsinki, 4.3.2003
Tea Silander, *tea.silander@cs.helsinki.fi*
Tietoturva nykyaikaisessa liiketoimintaympäristössä -seminaari
Tietojenkäsittelytieteen laitos
HELSINGIN YLIOPISTO

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.
Strategia-analyytikot monien muiden markkinatutkimusryhmien tavoin uskovat langattomien laitteiden määrän ylittävän miljardi laitetta vuoteen 2004 mennessä. 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. Myös langattomiin laitteisiin sekä näille tarjottaviin palveluihin voidaan kohdistaa palvelunestohyökkäyksiä. Lisäksi laitteiden tyypilliset ominaisuudet aiheuttavat ongelmia esimerkiksi fyysisen tietoturvan ja laskentatehokkuuden kannalta.

Langattomat laitteet siirtyvät monien erilaisten, mahdollisesti epäluotettavien tietoliikenneverkkojen läpi, joista ne saavat palvelua ja joissa ne suorittavat datan vaihtoa. Tällöin informaatiota voidaan varastaa tai muuttaa ilman että käyttäjä edes huomaa tätä.

McAfee Securityn apulaistoimitusjohtajan Arvind Narain ennustaa, että vaikkei tietoturvauhkia mobiiliverkoissa koeta vielä todellisesti, tulevat ne kasvamaan huomattavasti lähivuosina kehittyneemmän teknologian yleistyessä, jolloin mobiilikentän kiinnostavuus herää myös hakkereissa ja virusten tekijöiden parissa.

2 Langattoman tiedonsiirron ominaispiirteitä

Langattomat laitteet saattavat parantaa yrityksen työntekijöiden tuottavuutta, mutta aiheuttavat yritykselle uusia huomioonotettavia riskejä, koska laitteet kykenevät tallettamaan ja siirtämään yritykseen liittyvää tietoa sekä langattomissa että langallisissa verkoissa. Lan-

gattomalla tiedonsiirrolla on ominaispiirteitä, jotka johtuvat 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 käytetystä langattomasta siirtomediasta.

Langallisessa tiedonsiirrossa:

- siirto pitkin fyysistä linkkiä
- suuri siirtonopeus
- pieni virhetodennäköisyys

Langattomassa tiedonsiirrossa:

- siirto käyttäen radio- tai infrapuna-aaltoja
- matala ja laadultaan vaihteleva siirtonopeus
- suuri virhetodennäköisyys
- päästä päähän -kommunikointi (*point-to-point*) tai epämääräinen tai heikosti määritetty lähetyskantama

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. Nämä protokollat eivät myöskään ota huomioon sitä, että siirtonopeus voi välillä hidastua merkittävästi tai yhteys katketa kokonaan ja käyttäjän identiteetti voidaan väärentää.
Langattomassa tiedonsiirrossa on otettava huomioon myös se, että langattoman kommunikoinnin siirtomedia, radioaallot on rajallinen

resurssi, joka on kaikkien kuultavissa ja siten erittäin herkkä erilaisille hyökkäyksille sekä salakuuntelulle.

2.2 Langattomien laitteiden ominaisuudet

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 laitteiden pieni koko aiheuttaa niiden toiminnalle rajoitteita. Laitteiden käytön kannalta on ongelmallista se, että niillä on yleensä varsin rajallinen virtalähde ja ne ovat laskennallisesti tehottomia laitteita, joilla on kannettavia lukuunottamatta rajallinen muisti ja tietoliikennekapasiteetti. Tämän lisäksi laitteilla saattaa olla hyvin rajallinen näyttö, joka ei välttämättä kykene näyttämään käyttäjän haluamaa sisältöä.

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. Usein langattomat laitteet kykenevät kommunikoimaan toistensa kanssa rajallisen alueen sisällä käyttäen infrapuna- tai radioaaltoja.

Langattomilla laitteilla itsellään on niiden luonteesta johtuen monia tietoturvauhkia:

Langattomien laitteiden on niiden pienestä koosta johtuen todennäköistä kadota, jäädä ilman valvontaa tai tulla varastetuksi.
Käyttäjän autentikointi saatetaan kytkeä pois, joka yleensä on default-asetus, paljastaen laitteen sisältö kenelle tahansa, joka saa laitteen haltuunsa. Vaikkakin käyttäjän autentikointi olisi käytössä, saattaa autentikointimekanismi olla heikko tai helposti kierrettävissä.
Langaton tiedonsiirto voidaan siepata ja jos dataa ei ole salattu tai salaus on tehty viallisella protokollalla voidaan datan sisältö saada

selville.
Yrityksen on hankalaa ellei mahdotonta valvoa työntekijöidensä langattomien laitteiden siirtymistä yrityksen verkkoon ja sieltä jälleen ulos.

4 Palvelunestohyökkäykset

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.

Hyökkäys voi kohdistua esimerkiksi radioaaltoihin. Radioaaltojen rajallinen määrä tekee siitä langattoman tiedonsiirron pullonkaulan ja näin potentiaalisen palvelunestohyökkäyksen kohteen. Siirtomedian allokointi ja valvonta kontrollit 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.

5 Session kaappaaminen, Man-in-the-middle

Langattomissa verkoissa transaktio voidaan keskeyttää ja käynnistää uudelleen, eikä osapuolien autentikointia usein suoriteta tällöin uudelleen. Myös yhteyden muodostaminen uudelleen vain "päivittämällä"(*refresh*) selainta saattaa sisältää riskejä. Molemmissa tapauksissa pyynnöt (*request*) voidaan ohjata uudelleen ja palauttaa vahingollista koodia odotetun datan sijaan.
Monet SSL:n (Secure Socket Layer) ja WTSL:n (Wireless Transport Security Layer) kaupalliset versiot eivät suorita osapuolien autentikointia tai sertifikaattien tarkistusta uudelleen kun yhteys on jo kertaalleen muodostettu.

Myös paikallisuutta voidaan hyödyntää session kaappaamisessa. Jos hakkeri saa lähimmän DNS-nimipalvelimen ohjaamaan tietyn osa-

kevälittäjän sivustolle tulevat pyynnöt omalle peilisivustolleen, saa hän haltuunsa kyseisen DNS-palvelimen alueella osakevälittäjän palvelua käyttävien käyttäjien tietoja, kuten tilinumeroita. Langattoman verkon käyttö tarjoaa lisäksi hakkereille hyvän suojan, sillä langattomat laitteet vaeltavat langattomien alueiden välillä, niillä ei ole mitään tiettyä maantieteellistä kiintopistettä ja laitteet saattavat olla poiskytkettyinä (*offline*) verkosta, jolloin ne ovat vaikeasti tavoitettavissa.

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 domainien 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.

Viitteet

[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] Geng, X., Huang, Y., Whinston, A. B.
Defending Wireless Infrastructure Against the Challenge of DDoS Attacks,

Mobile Networks and Applications, Vol. 7, No. 3, p. 213-223, 2002

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

[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

[NiL02] Nichols, R.K., Lekkas, P.C.
Wireless Security: Models, Threats, and Solutions,
Mc Graw-Hill, 2002

[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