Bluetoothin tietoturva

Eero Kaipiainen

Helsinki 4. maaliskuuta 2003

Tietoturvallisuus nykyaikaisessa liiketoimintaympäristössä -seminaari: laajennettu tiivistelmä

HELSINGIN YLIOPISTO
Tietojenkäsittelytieteen laitos

Bluetooth on teknologia langattomaan kommunikointiin. Bluetoothin kehitys aloitettiin Bluetooth Special Interest Group (SIG) nimisessä ryhmässä vuonna 1998. Bluetoothin päämääränä on yhdistää erilaisia laitteita langattomasti. Yleisimpiä tapoja yhdistää laitteita Bluetoothilla on esimerkiksi matkapuhelimen ja kannettavan tietokoneen tai taskutietokoneen (PDA) kytkeminen. Bluetoothilla voidaan muodostaa myös niin sanottuja "ad hoc" -verkkoja, joissa korkeintaan kahdeksan laitetta voi kommunikoida keskenään. Bluetoothin käyttöä rajoittaa sen kantama, joka tällä hetkellä on noin kymmenen metriä. Bluetoothia voidana käyttää esimerkiksi työpaikoilla tai kotona. Työpaikkalla voidaan Bluetooth-laitteiden avulla lähettää luottamuksellista tai salaista tietoa, jolloin tarvitaan tietoturvaa.

Bluetooth-laitteet jaetaan kolmeen luokkaan sen perusteella, että millä taajudella niiden lähetys toimii. Ensimmäiseen luokkaan kuuluvat sellaiset laitteet, joiden kantama on sata metriä ja lähetysteho on 100 mW. Toisessa luokkaan määritellään laitteet, joilla kantama on kymmenen metriä ja lähetysteho on 1 - 2,5 mW. Kolmanteen luokkaan kuuluvat laitteet, joiden lähetysteho on 1 mW ja kantama on 0,1 - 1 metriä.

Bluetooth tarjoaa useita tapoja salata tietoa ja tunnistaa käyttäjä. Se käyttää PIN-koodien yhdistelmää (engl. Personal Identification Number PIN) ja laitteiden osoitteita niiden tunnistamiseen. Bluetoothin käyttämä lähetystapa tarjoaa jonkin asteista suojaa, koska lähetystaajuus voi vaihdella 2.4 GHz kaista-alueella, jolloin vain sen kanssa synkronoiduilla vastaanottajilla on mahdollisuus vastaanottaa tietoa. Tätä tekniikkaa kutsutaan FHSS-tekniikaksi (engl. fast frequency spread spectrum).

Bluetooth käyttää niin sanottua valtuutusta (engl. authorisation) ja tunnistamista (engl. authentication) käyttäjien, laitteiden ja niiden oikeuksien määrittelemiseen. Valtuutuksella tarkoitetaan tapahtumaketjua, jossa jokin laite haluaa käyttää palvelua, joka sijaitsee toisella laitteella. Tällöin palvelua pyytävään laitteen on täytettevä luotettavan laitteen tunnusmerkit eli laitteen on täytynyt tunnistautua. Laitteiden luottamustasoista kerrotaan lisää myöhemmin. Turvamanageri ylläpitää tietoa laitteden ja palveluiden tietoturvatasoista. Se päättää laitteiden yhteyden muodostamisesta, sen katkaisemisesta, tunnistamisen tai salauksen tarpeellisuudesta. Lisäksi se alustaa luotettavan yhteyden toiseen laitteeseen tarpeen mukaan ja kysyy käyttäjältä PIN-koodia.

Bluetooth sisältää turvatasoja, joita voivat hyödyntää laitteet ja palvelut. Laitteilla on kaksi luottamustasoa: luotettava ja epäluotettava. Laite ei välttämättä saa käyttää kaikkia palveluita, jos se on määritelty epäluotettavaksi. Luotettavalla laitteella on vapaa pääsy kaikkiin palveluihin. Uusi laite on aina epäluotettava. Lisäksi Bluetooth käyttää turvatiloja laitteille. Matalimmassa turvatilassa laite ei tarjoa mitään turvaa ja korkeimassa tasossa laite tarjoaa täyden turvan. Kun yhteys on muodostettu laitteiden välille, käyttäjä voi valita tietoturvatason käyttämälleen palvelulle kolmesta vaihtoehdosta tai niiden yhdistelmistä. Vaihtoehdot ovat valtuutus, tunnistaminen tai salaus.

Linkkikerroksella tapahtuu laitteiden välinen tunnistaminen ja tiedon salaus. Laitteilla on julkinen yksikäsitteinen osoite ja kaksi salaista avainta: tunnistusavain ja salausavain. Muita käytettäviä avaimia ovat linkkiavaimet ja PIN-koodi. Linkkiavaimia on useita ja niitä käytetään tilanteen mukaan. Salausavain muodostetaan käytössä olevasta linkkiavaimesta.

Bluetoothissa tunnistaminen tapahtuu kaksivaiheisen avainten vaihtoprotokollan avulla. Protokolla käyttää symmetrisiä avaimia eli onnistunut tunnistaminen perustuu siihen, että kumpikin laitteista jakaa saman avaimen.

Bluetoothin lähettämä tieto salataan käyttämällä neljää LFSR:ää (engl. linear feedback shift registers), joiden kokonaispituus on 128 bittiä. Avainten muodostaminen ja laitteiden tunnistaminen tapahtuu SAFER+ -salausalgoritmilla.

Lopuksi esitellään muutamia mahdollisia hyökkäystapoja Bluetoothia vastaan. Ensimmäisessä hyökkäystyyppissä hyökkääjä voi saada laitteiden tunnistusavaimet, linkkiavaimet ja salausavaimet hyökkäyksen kohteena olevasta laitteesta. Tällöin hyökkääjä voi kuunnella salaa laitteiden välistä liikennettä. Hyökkäys voidaan toteuttaa kokeilemalla PIN-avaimia tai niin sanottua kolmannen persoonan hyökkäystä (engl. middle-person-attack). Toisessa hyökkäystyypissä yritetään kartoittaa laitteiden fyysinen sijainti. Tämä saattaa olla kiusallista joillekin käyttäjille. Kolmannessa tapauksessa on mahdollista murtaa Bluetoothin käyttämä salaustapa.

Lähteet

1 (Gehrmann, Nyberg, “Enhancements to Bluetooth baseband security”, Nordsec ’01)

2 Markus Jakobsson and Susanne Wetzel, “Security Weaknesses in Bluetooth”, Lucent Technologies - Bell Labs, Information Sciences Research Center

3 Jyrki Oraskari, “Bluetooth versus WLAN IEEE 802.11x”, Department of Computer Science And Engineering, Helsinki University of Technology

4 Marjaana Träsbäck, “Security of Bluetooth: An overview of Bluetooth Security”, Department of Electrical and Communications Engineering, Helsinki University of Technology

5 J.T Vainio, “Bluetooth security”, Proceedings of Helsinki University of Technology, Telecommunications Software And Multimedia Laboratory, Seminar on Internetworking: Ad Hoc Networking

6 Bluetooth Specification, www.bluetooth.com/dev/specifications.asp