

Bluetooth-tekniikan soveltaminen tunnistuksessa

Tulevaisuuden langattomat avaimet



Bluetooth based authentication

More and more personal mobile devices are equipped with Bluetooth. These devices usually belong to Bluetooth power class 2, which gives them a range of approximately 10 meters. Personal nature of mobile devices and an adequate wireless range of Bluetooth make them suitable for user authentication.

Wireless authentication brings several challenges to the authentication system. The traditional threats of wired networks, network sniffing and impersonation, are also a problem for the wireless network.

Handheld devices also have a limited memory and processor capacity compared to personal computers. For this reason, authentication system may have to be a compromise between the needed security level and the processing capacity.

In its simplest form Bluetooth based authentication can be based on the Bluetooth device address. A certain Bluetooth device must be close to the authentication service, when the user tries to use the service. The service can be a "log on" daemon of a computer or an access control service.

Most of the time the presence of a Bluetooth device is not enough for the user authentication and more sophisticated approaches need to be used. The use of certificates makes the authentication more general. Certificates may contain both device and service dependent parts, e.g. certificate may be granted for certain Bluetooth device or is limited to certain operations.

Different authentication methods have been used in Bluetooth based access control system. The project Short Range Radio Technologies is part of TEKES (the National Technology Agency in Finland) NETS program and the contact person is Jari Porras (jari.porras@lut.fi).



Kuva: Veijo Ojanperä

Langaton Bluetooth-tekniikka yleistyy ja tuo mukanaan mahdollisuuden käyttää henkilökohtaisia laitteita apuna käyttäjän tunnistuksessa. Monipuolinen, aina mukana kulkeva avain on houkutteleva ajatus. Miten Bluetooth-laitteet soveltuvat tunnistukseen, ja mitä asioita tulisi ottaa huomioon tunnistusjärjestelmää suunniteltaessa? Kuinka voidaan ehkäistä aikaa vievän Bluetooth-laitehaun vaikutus?

Bluetooth on lyhyen kantaman langaton radiotekniikka, joka on vähitellen yleistynyt kuluttajatasen laitteissa. Monissa matkapuhelimeissa ja kämmentietokoneissa Bluetooth-toiminto on joko sisäänrakennettuna tai saatavissa erillisenä lisävarusteena.

Suuri osa Bluetooth-laitteista kuuluu lähetyshoitoaan Bluetoothiin luokkaan 2, eli laitteiden lähettämän radiosignaalin kantomatka on vain noin 10 metriä.

vaatimuksia myös käytettävälle tunnistusmenetelmälle. Salasanaa tai muuta salaisuutta ei saisi lähettää radiotien yli, sillä arka luonteisen tiedon nuuskiminen on yksi perinteisimpiä uhkia verkon turvallisuudelle. Nuuskimisen lisäksi toiseksi tekeytymisen uhka tulee ottaa huomioon myös langattomassa verkossa, vaikkakin Bluetoothin osalta yksilölliset laiteosoitteet tekevät tekeytymisestä vaikeampaa.

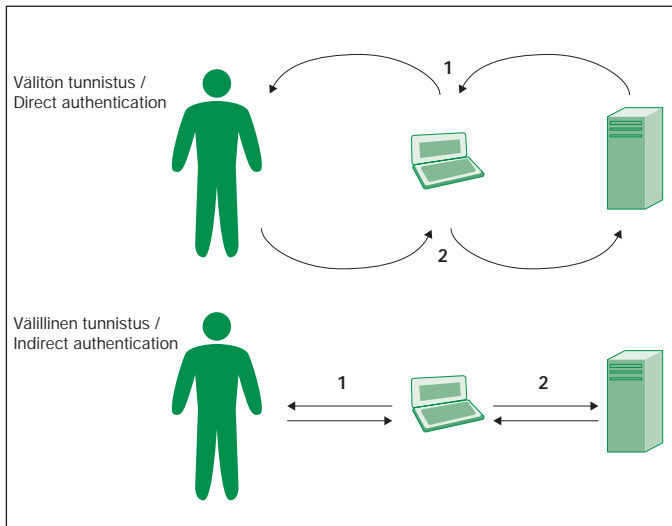
Pienten päätelaitteiden prosessoritehot ovat yleensä vain murto-osia pöytätietokoneiden tehoihin verrattuna. Käytettävän tunnistusmenetelmän tulisikin vaatia päätelaitteelta mahdollisimman vähän laskentatehoa, mutta kuitenkin toteuttaa sovelluksen suhteen riittävä turvataso. Usein ratkaisussa joudutaan tekemään kompromissi näiden ominaisuuksien välille.

Langattoman päätelaitteen avulla tapahtuva tunnistus voi olla välitön tai välillinen. Välittömässä tunnistuksessa päätelaitte ainoastaan välittää palvelulta tulevan pyynnön käyttäjälle ja vastauksen käyttäjältä palvelulle. Välillisessä tunnistuksessa käyttäjä kirjautuu ensin laitteelle, minkä jälkeen tunnistuspalveluiden kyselyt voidaan kohdistaa käyttäjän sijasta laitteeseen. Laite toimii siten käyttäjän tunnisteena.

Laitteen ja palvelun välinen tunnistuskysely on nopeampaa ja sujuvampaa kuin tunnistus, jossa vaaditaan käyttäjän syötettä. Käyttäjän ja laitteen välisessä tunnistuksessa voidaan käyttää PIN-koodia, salasanaa tai erillistä fyysistä todistetta, kuten esimerkiksi henkilökorttia. Palvelu tunnistaa laitteen joko pelkätään sen osoitteen perusteella tai haaste-vastaus-periaatteella. Palvelun kriittisyys määrittää pitkälti käytettävän menetelmän.

Bluetooth-määrittelyyn kuuluva perustunnistus tapahtuu PIN-koodin, toisen osapuolen Bluetooth-laiteosoitteen ja satunnaisluvun avulla. Radiotien yli lähetetään haasteena satunnaisluku, johon toinen laite vas-

Langaton tunnistus
Langattoman verkon käyttö tunnistuskäytössä tuo mukanaan



Välitön tunnistus. Laite vain ohjaa tunnistuspyynnön käyttäjälle ja vastauksen palvelulle. **Välillinen tunnistus.** Laite tunnistaa käyttäjän ja palvelu laitteen.

Direct authentication. Device directs the request to the user and the response back to the service. Indirect authentication. The Device identifies its user and the service identifies the device.

taa. Salaisuuksia ei lähetetä Bluetooth-yhteyden yli, mikä tekee menetelmästä soveltuvan langattomaan tunnistukseen. PIN-koodin avulla tapahtuva tunnistus ei ole kuitenkaan joka tilanteessa riittävän sujuvaa ja käytännöllistä.

Läsnäolo riittää

Yksinkertaisimmillaan Bluetooth-laitetta voi käyttää käyttäjän tunnistuksessa tarkistamalla tunnistuksen yhteydessä laitteen läsnäolo. Bluetooth-laitteen läsnäoloa voidaan vaatia esimerkiksi tietokoneen sisäänkirjautumisessa, joko ainoana tunnistusmenetelmänä tai perinteisen salasanan lisäksi.

Tunnistuksessa lähetetään tietokoneella oleviin käyttäjän tietoihin tallennettuun Bluetooth-laitteeseen nimikysely, ja tarkistetaan, tuleeko kyselyyn vastausta. Koska Bluetooth-laitteet ovat tallessa käyttäjätiedoissa, ei laitetta tarvitse hakea Bluetooth-laitekyselyllä. Nimikyselyn avulla tehtävässä tunnistuksessa ei ole tärkeää laitteen palauttama nimi, vaan se, että vastaus tiettyyn osoitteeseen lähetetystä kyselystä tulee.

Tällainen lisätunnistus on erittäin helppo toteuttaa, ja se lisää tietokoneen turvasoa pelkkään sisäänkirjautumisen salasankyselyyn verrattuna. Bluetooth-puhelimelta se ei vaadi mitään Bluetooth-perusominaisuuksien lisäksi, sillä jokainen Bluetooth-laite osaa vastata laitteen nimikyselyyn.

Käyttöjärjestelmään tuki on helppo toteuttaa, jos käyttöjärjestelmän kirjautumista vaativat

ohjelmat tukevat keskitettyä ja modulaarista tunnistusohjelmistoa. Toiminto voidaan toteuttaa esimerkiksi monissa Unix-käyttöjärjestelmissä toimivan Pluggable Authentication Modules -ohjelmiston (PAM) avulla. Eri PAM-moduulit, tässä tapauksessa Bluetooth PAM -moduuli, huolehtivat tunnistuksen yksityiskohdista. Tunnistusta vaativille ohjelmille PAM-moduulit näkyvät yhtenä kirjastona. Jokaiselle PAM-tunnistusta käytävälle ohjelmalle voidaan kuitenkin määrittellä erilaiset vaatimukset käyttäjän kirjautumisen hyväksymiseksi.

Sertifikaatilla monikäyttöisyyttä

Sertifikaattien avulla voidaan Bluetooth-tunnistusta käyttää

monipuolisesti. Tunnistuksen yhteydessä tunnistuspalvelulle siirrettävällä sertifikaatilla voidaan kertoa, mihin palveluihin sen haltijalla on sertifikaatin myöntäjän lupa. Tällöin palveluihin ei tarvitse etukäteen määrittellä, kenellä on oikeus niiden käyttöön. Sertifikaatin myöntäjän tulee olla luotettu tunnistuspalveluiden keskuudessa. Sertifikaatin toiminta perustuu julkisen avaimen menetelmään, jossa sertifikaatin myöntäjä allekirjoittaa sertifikaatin yksityisellä avaimellaan, ja tunnistuspalvelu varmistaa sertifikaatin oikeellisuuden myöntäjän julkisella avaimella. Sertifikaatin tietoja ei voi muuttaa ilman myöntäjän yksityistä avainta.

Sertifikaatin käyttöoikeuden myöntäjä voi määrittellä sertifikaatin henkilö- ja laitetietoja tarpeen mukaan. Myös tieto sertifikaatin käyttöoikeudesta määrittellään siihen mukaan. Bluetooth-käytössä on tärkeää lisätä laitteen Bluetooth-osoite sertifikaatin tietoihin. Tällä tavalla saadaan valmius sertifikaatin tunnistuskäyttöön Bluetooth-osoitteen perusteella. Tapahtumatiotojen tallennusta varten myös sertifikaatin haltijan henkilötiedot ovat tärkeitä sertifikaatissa.

Varastetut tai kadonneet laitteet voidaan poistaa käytöstä lisäämällä tieto kadonneista laitteista tunnistuspalvelun estolistaan. Palvelu tarkistaa tunnistuksen yhteydessä, ettei yhteyttä otavan laitteen osoite ole tässä listassa. Mikäli osoite löytyy listasta, tunnistus hylätään, vaikka se muuten olisikin hyväksyttävissä.

Haaste-vastaus varmuudeksi

Mikäli pelkkä Bluetooth-laite-osoitteen tarkistus tuntuu liian

vähäiseltä tunnistuskäytössä, voidaan tarkistaa haaste-vastaus-periaatteella, että käyttäjä todellakin on sertifikaattiin liittyvän avainparin omistaja. Sertifikaatti sisältää käyttäjän julkisen avaimen, jolla tunnistuspalvelu voi salata haasteviestin.

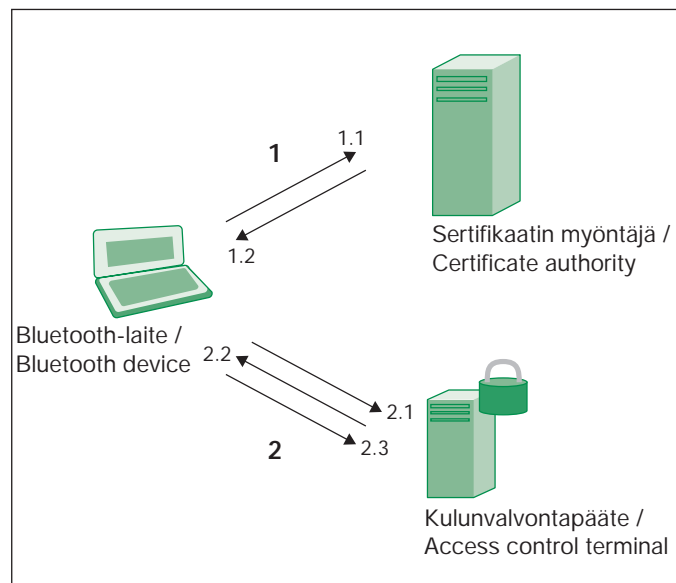
Palvelu lähettää haasteviestin sertifikaatin Bluetooth-osoitteen perusteella käyttäjän laitteelle ja muodostaa haasteesta yksisuuntaisella tiivistefunktiolla tiiviste. Haaste puretaan käyttäjän laitteesta käyttäjän yksityisellä avaimella. Laite lähettää sovitulla tiivistealgoritmilla muodostamansa vastauksen takaisin päätteelle. Palvelu tarkistaa vastauksen vertaamalla saapunutta tiivistettä itse muodostamaansa tiivisteeseen. Jos ne ovat samat, tunnistus hyväksytään.

Kulunvalvontasovellus

Kulunvalvontasovelluksessa tavoitteena oli suunnitella ja toteuttaa järjestelmä, jossa henkilöiden käyttämät Bluetooth-päätelaitteet, esimerkiksi matkapuhelimet ja kämmentietokoneet, toimivat avaimina. Järjestelmän kulunvalvontapäätteillä ei tarvitse olla erillistä yhteyttä käyttöoikeustietokantaan, koska käyttäjien oikeudet lähetetään avauspyyntöjen mukana sertifikaatissa.

Laitteen liittäminen järjestelmään alkaa avainparin luomisella. Yksityinen avain tallennetaan päätelaitteen muistiin, ja sen avulla luodaan sertifikaattipyynnö. Sertifikaattipyynnö lähetetään sertifikaatin myöntäjälle, joka on tunnettu ja luotettu taho. Sertifikaattipyynnö allekirjoitetaan sertifikaatiksi ja lähetetään takaisin laitteelle. Allekirjoituksen yhteydessä sertifikaattiin lisätään käyttäjän henkilötiedot, avainlaitteen Bluetooth-osoite ja tunnukset niistä lukoista, jotka käyttäjällä on oikeus avata.

Avaustilanteessa käyttäjä lähettää avauspyynnön kulunvalvontapäätteelle avainlaitteeseen tallennettujen Bluetooth-osoit-



- Kulunvalvontajärjestelmä**
- 1.1 Sertifikaattipyynnö
 - 1.2 Hyväksytty sertifikaatti
 - 2.1 Avauspyynnö (sertifikaatti)
 - 2.2 Haaste
 - 2.3 Vastaus (tiiviste)

- Access control system**
- 1.1 Certificate request
 - 1.2 Authorized certificate
 - 2.1 Unlock request (certificate)
 - 2.2 Challenge
 - 2.3 Response (hash)

Sanasto

PIN-koodi/Salanasana:

Salainen tunnus, jolla käyttäjä kirjautuu laitteelleen.

Haaste/Vastaus:

Muodostetaan palvelun lähettämään satunnaiseen haasteeseen ennalta sovitulla menetelmällä vastaus, joka lähetetään takaisin palvelimelle. Palvelin tarkistaa vastauksen oikeellisuuden. Salanasanaa ei tarvitse lähettää verkon yli.

Bluetooth-laitekysely:

Laitekyselyllä haetaan lähistöllä olevat Bluetooth-laitteet, jotka ovat haettavissa-tilassa. Laitekysely kestää tavallisesti useita sekunteja.

Bluetooth-nimikysely:

Pyydetään tietyn Bluetooth-laitteen laitenimi Bluetooth-osoitteen perusteella. Nimikyselyn toiminta on nopeampaa kuin laitekysely.

PAM, Pluggable Authentication Modules:

Tunnistustoimintoja tekevien kirjastojen kokoelma, josta valitaan sopivat toiminnot jokaiselle tunnistusta vaativalle ohjelmalle. Ohjelmille moduulit näkyvät yhtenä kirjastona.

Sertifikaatti:

Sidos käyttäjän tietojen ja käyttäjän julkisen avaimen välille muodossa, jossa sertifikaatin tietoja ei voi muuttaa ilman sen myöntäjän salaista avainta.

Julkisen avaimen menetelmä:

Käytetään avainparia, jonka toinen avain on vain avainparin omistajan tiedossa, toinen julkisesti levityksessä. Allekirjoitus tehdään yksityisellä avaimella ja puretaan julkisella avaimella. Salauksen voi tehdä julkisella avaimella ja purkaa yksityisellä avaimella.

teiden perusteella. Avaustilanteissa ei tarvita hidasta Bluetooth-laitihakua päätteiden osoitteiden selvitykseen, joten yhteydenmuodostus onnistuu nopeasti.

Avauspyynnössä on halutun lukon tunnus ja laitteen sertifikaatti. Kulunvalvontapäätte tarkistaa myöntäjän julkisella avaimella sertifikaatin oikeellisuuden. Samalla tarkistetaan,

onko sertifikaatin sisältämä Bluetooth-osoite varmasti sama kuin yhteyttä ottavan laitteen osoite, ja onko kyseisen lukon tunnus sertifikaatin lukkolistassa.

Mikäli edellä mainitut asiat ovat kunnossa, päätte purkaa sertifikaatista käyttäjän julkisen avaimen. Avaimella salataan haaste, jonka kulunvalvontapäätte lähettää käyttäjän Bluetooth-laitteelle. Laite purkaa vastaanotetun haasteen salauksen yksityisellä avaimellaan ja lähettää haasteesta muodostamansa tiivisteen vastauksena kulunvalvontapäätteelle. Mikäli kulunvalvontapäätteen saama vastaus on sama kuin päätteen alkuperäisestä haasteesta itse muodostama tiiviste, päätte avaa lukon. ●

Aiheesta enemmän

Bluetooth:

www.bluetooth.com

PAM:

www.opengroup.org/tech/rfc/mirror-rfc/rfc86.0.txt

Julkisen avaimen menetelmä:

www.ietf.org/html.charters/pkix-charter.html

LKRT:

www.it.lut.fi/project/lkrt

Taustat

Kirjoittajat: Arto Hämäläinen, LKRT-hankkeen projektipäällikkö, Pekka Jäppinen, Bluetooth-asiantuntija, Jari Porras, professori ja LKRT-hankkeen vastuullinen johtaja.

Yhteyshenkilö:

jari.porras@lut.fi
Tietoliikennetekniikan laitos, Lappeenrannan teknillinen korkeakoulu

Tutkimus: LKRT (Lyhyen kantaman radiotekniikat).

Yhteistyössä: Abloy, Aldata Industries, Digia, Elektrobit, Ericsson, Wificom Technologies, Satakunnan puhelin, UPM-Kymmene.

Teknologiaohjelma: NETS