Teksti: Matti Järvinen

Epäilyttääkö etäluku

Matti Järvinen työskentelee KPMG:llä tietoturva-asiantuntijana. Hänellä on kokemusta tietoturvan kehittämisestä ja tarkastamisesta sekä teknisestä sekä hallinnollisesta näkökulmasta. Matti on valmistunut Diplomi-insinööriksi Teknillisestä Korkeakoulusta tietotekniikan osastolta. Lisäsi hänellä on kansainvälisesti arvostettu tietoturva-ammattilaisten CISSP-sertifikaatti.

Yhteystiedot:
Matti Järvinen
matti.jarvinen@kpmg.fi
+358 (0)20 760 3398

KPMG on maailmanlaajuinen asiantuntijaorganisaatio, jonka tehtävänä on muuttaa tietoa arvoksi asiakkailleen, henkilöstölleen ja pääomamarkkinoille. KPMG:n palvelutarjontaan kuuluvat tilintarkastus, vero- ja neuvontapalvelut. Neuvontapalveluiden osana toimiva tietoturvapalvelut yksikkö tarjoaa monipuolisia, eri tietoturvan osa-alueisiin liittyviä koulutus, neuvonta ja auditointipalveluita, jotka perustuvat hyviksi havaittuihin käytäntöihin ja työmenetelmiin.

RFID on menetelmä, joka mahdollistaa tiedon etäluvun ja tallennuksen. Se on jo tällä hetkellä laajasti käytössä ja sen käytön ennakoidaan kasvavan räjähdysmäisesti tulevina vuosina. Tämä artikkeli kertoo lyhyesti RFID-teknologiasta, sen sovelluksista, mm. *biopassista* ja yleisesti siihen liittyvistä tietoturvaongelmista ja niiden mahdollisista ratkaisuista.

Mikä on RFID?

RFID (Radio Frequency Identification) on menetelmä, tiedon etälukuun ja tallennukseen. Järjestelmä koostuu RFID-tunnisteista ja RFID-lukijasta. RFID tunniste on pieni tietoa sisältävä laite, joka voidaan sisällyttää esimerkiksi tuotteisiin valmistusvaiheessa tai liittää niihin myöhemmin. RFID-lukija on laite, jolla voidaan lukea (ja mahdollisti kirjoittaa) RFID tunnisteisiin tallennettua tietoa.

Osassa RFID-tunnisteista niihin asetettu tieto on pysyvää, eli sitä ei pysty myöhemmin muuttamaan. Hieman monimutkaisimmissa RFID-tunnisteissa tiedon pystyy muuttamaan myöhemmin. RFID-tunnisteita on kahta tyyppiä: passiivisia, jotka eivät sisällä omaa virtalähdettä, ja aktiivisia, jotka sisältävät oman virtalähteen. Näiden lisäksi on tarjolla myös puolipassiivisia tunnisteita. Näissä on oma virtalähde, mutta ei omaa lähetintä.

Passiivisissa RFID-tunnisteissa tarvittava virta saadaan lukijalaitteelta, joka välittää virtaa magneettikentän välityksellä RFID-tunnisteeseen. Tunnisteet voivat sisältää ID-numeron lisäksi pienen määrän muuta tietoa. Virtalähteen puuttumisen vuoksi tunnisteet voivat olla hyvinkin pieniä, kuten Hitachin µ-Chip, jonka koko on vain 0.15x0.15mm ja paksuus 7.5 mikrometriä. Passiivisten RFID-tunnisteiden käyttöetäisyys voi käytetystä standardista riippuen olla muutamasta senttimetristä muutamaan metriin.

Aktiivisissa RFID-tunnisteissa oleva virtalähde mahdollistaa käyttösäteen kasvun kymmeniin metreihin ja ne voivat sisältää huomattavasti enemmän tietoa kuin passiiviset tunnisteet. Lisäksi niihin voidaan rakentaa logiikkaa, joka mahdollistaa turvallisen istunnon muodostamisen. Aktiiviset RFID-tunnisteet ovat tällä hetkellä kooltaan suunnilleen kolikon kokoisia.

Sovellukset

RFID-menetelmiä pidetään teknologiana, joka tulee leviämään hyvin laajaan käyttöön. Jo nykyään sitä käytetään monessa paikassa helpottamaan tunnistamista. Taulussa 1 on yhteenveto muutamista erilaisista RFID-sirujen sovelluksista.

RFID ja biopassi

Monimutkaisesta sovelluksesta hyvänä esimerkkinä on suomessa elokuussa 2006 käyttöön otetut biopassit, jotka sisältävät RFID-tunnisteen. Tällä hetkellä siihen tallennetaan passin tietosivulta passin haltijan tiedot, passin numeron ja kasvokuvan. Myöhemmin passeihin lisätään sormenjälkitiedot. Samankaltaisia passeja on otettu käyttöön jo monessa muussakin maassa.

Biopasseissa on käytetty passiivista RFID-sirua, mutta ne ovat kuitenkin riittävän monimutkaisia, jotta niissä on pystytty toteuttamaan tietoturvaominaisuuksia. Passeissa käytetään Basic Access Control (BAC) -protokollaa, joka tarkoittaa sitä, että ennen kuin passit antavat tietoa sen haltijasta, täytyy lukijalaitteelle syöttää niin sanottu Machine Readable Zone (MRZ) -tieto, joka lukee passissa ja joka voidaan lukea koneellisesti. Tämä tarkoittaa sitä, että passista ei voi lukea helposti tietoja ilman passin omistajan suostumusta. BAC -protokollassa ja monessa sen toteutuksessa on kuitenkin heikkouksia ja Eurooppalaisissa passeissa onkin otettu käyttöön Extended Access Control menetelmä, joka lisää tietoturvaa julkisen avaimen menetelmällä. Tällöin RFID-lukijalaite todistaa passille olevansa laillinen lukijalaite ennen kuin passi antaa tietoja lukijalaitteelle. RFID-sirujen vaihtaminen passilla on estetty niin sanotulla aktiivisella autentikaatiolla.

Biopassissa on siis monia tietoturvaominaisuuksia, jotka suojaavat passin omistajaa sekä estävät passien väärentämisen. Tietoturvaominaisuudet ovat periaatteellisella tasolla riittäviä, mutta niistä ei ole saatavilla tarkempia tietoja, kuten suomen tapaa luoda MRZ-kenttä passiin. Näitä tarkempia tietoja tarvittaisiin, jotta pysyttäisiin paremmin analysoimaan tietoturvaa.

Taulu 1.
RFID -sovelluksia

Liikenne ja Joukkoliikenne
- Pääkaupunkiseudun matkakortti
- Tietullit
Tuotteiden seuranta
- Tällä hetkellä käytetään suurempien erien tunnistamisessa
- Suunnitteilla laajentaminen siten, että jokaisessa tuotteessa olisi RFID -siru
Aitouden todistaminen ja pääsykontrolli
- Biopassi otettu suomessa käyttöön 2006
- Lääketeollisuus pyrkii estämään RFID:n avulla tuoteväärennöksiä
- Auton ovien avaus ja ajonestolaitteet
Eläimet ja ihmiset
- Karjan ja kotieläinten tunnistaminen
- Vankien seuranta
- Potilastietojen tallentaminen

Biopassit ovat laitteita, joissa voidaan perustellusti käyttää hieman kalliimpia RFID-tunnisteita ja siten pystyä toteuttamaan monimutkaisia tietoturvaominaisuuksia.

RFID viivakoodin korvaajaksi

Toisessa ääripäässä RFID-tunnisteiden käyttötapauksia on niiden käyttö kuluttajatuotteissa viivakoodin sijaan. Jokaiseen tuotteeseen sisällytettävä RFID-tunniste mahdollistaisi tuotteiden yksilökohtaisen seurannan nykyisen tuotekohtaisen seurannan sijaan. Lisäksi kassojen toiminta voisi tehostua, sillä RFID tunnisteen lukeminen on tehokkaampaa kuin viivakoodien lukeminen ja niitä voidaan lukea useampia yhdellä kertaa. Suunnitelmissa on jopa kassojen korvaaminen itsepalveluperiaatteella toimiviksi.

Mikäli viivakoodit korvataan RFID-tunnisteilla, tulee tunniste todennäköisesti sisältämään vain tuotteen ID-numeron, joten ne eivät varsinaisesti sisällä luottamuksellista tietoa. Kaupalle olennaista on tällöin se, että tunnistetta ei pystytä irrottamaan tai muuttamaan, sillä tällöin maksun yhteydessä toiminta hidastuu, jos hintatietoa täytyy etsiä manuaalisesti tai tuotteesta veloitetaan väärä hinta.

Kuluttajalle ongelma muodostuu siitä, että RFID-siru jatkaa toimintaansa ostotilanteen jälkeen. Halvoissa tunnisteissa ei ole minkäänlaista estoa niiden sisältämän tiedon lukemiselle, joten kuka tahansa pystyy niissä olevan tiedon lukemaan. Tällöin esimerkiksi lenkkikengissä olevan sirun tieto pystytään lukemaan oston jälkeenkin ja siten mahdollisesti saamaan kuluttajan näkökulmasta arkaluontoista tietoa.

Tunnisteen ID-numero pysyy samana, jolloin sen käyttäjää pystytään mahdollisesti seuraamaan. Kuluttaja voisi rikkoa sirun oston jälkeen, jolloin sen tiedon lukeminen ei ole enää mahdollista. Ongelmaksi tulee se, että siru on pyritty tekemään mahdollisimman vahvaksi, jotta sitä ei pystyttäisi kaupassa rikkomaan sekä se, että siru voi olla hyvinkin pieni, eikä sitä pystytä mahdollisesti tuotteesta löytämään. Parempi ratkaisu olisi se, että ostotilanteessa kaupan kassa lähettäisi sirulle käskyn tuhota itsensä. Tällöin tosin tuhokoodi tulisi olla tuotekohtainen, jotta hyökkääjä ei pystyisi halutessaan tuhoamaan RFID-tunnisteita.

Tietoturvanäkökulmia

RFID-tunnisteita on hyvin monenlaisia ja yksinkertaisimmat passiiviset laitteet ovat hyvin erilaisia verrattuna monimutkaisimpiin aktiivisiin tunnisteisiin. Niillä onkin siten eritasoiset valmiudet ratkaista tietoturvaan liittyviä ongelmia. Uhat tietoturvalle koskevat kuitenkin ainakin osittain kaikkia laitteita. Seuraavassa käsitellään yleisimpiä RFID-järjestelmään liittyviä uhkia.

1. **Tiedon lukeminen käyttäjän tietämättä.** RFID-tunnisteet eivät monestikaan suojaa tietojansa millään tavalla, vaan mikä tahansa lukijalaite, joka on sopivan etäisyyden päässä, voi lukea tunnisteen sisällön. Laitteet eivät yleensä myöskään ilmoita milloin niiden tietoja luetaan, joten lukeminen voi tapahtua käyttäjän tiedostamatta. Monesti tunnisteet sisältävät vain koodin, jolla ei suoraan pystytä tekemään mitään tietoturvaa vaarantavaa. Ongelma muodostuu silloin, kun tunnisteelle tallennetaan tietoa, joka on arkaluontoista tai jota voidaan käyttää hyväksi arkaluontoisen tiedon hankkimisessa.
2. **RFID-tunnisteiden seuranta.** RFID-tunnisteista saadaan usein riittävä tieto, jolla voidaan yksilöidä tunniste henkilöön joka sitä kantaa tai muuten kuljettaa mukanaan. Tällöin sopiviin paikkoihin sijoitetuilla lukijalaitteilla voidaan seurata ihmisten liikkeitä.
3. **RFID-tunnisteiden väärentäminen.** Käyttämällä uudelleenkirjoitettavaa RFID-tunnistetta, hyökkääjä voi pystyä väärentämään tunnisteen sisällön.
4. **Toistoon perustuvat hyökkäykset.** Hyökkääjä voi pystyä kaappaamaan RFID-tunnisteen ja lukijan välisen liikenteen ja käyttämään tätä kaapattua keskustelua myöhemmin hyväkseen esimerkiksi tunnistautumisessa johonkin palveluun.
5. **Palvelunestohyökkäykset.** RFID-tunnisteiden toiminnan pystyy estämään monella eri tavalla, kuten laittamalla tunnisteen metalliseen kuoreen (Faradayn häkkiin), lähettämällä estosignaalin tai lähettämällä tunnisteelle käskyn tuhota itsensä.
6. **Vääränlaisen tiedon syöttämiseen perustuvat hyökkäykset.** RFID-lukijan tieto on usein syöte taustajärjestelmälle, kuten varastonhallintajärjestelmälle. Hyökkääjä voi pystyä käyttämään taustajärjestelmässä olevia tietoturvaongelmia muokkaamalla RFID-tunnisteen sisältämää tietoa siten, että se on erilaista kuin järjestelmä sen olettaa olevan. Ongelmat ovat silloin hyvin samankaltaisia kuin tällä hetkellä WWW-järjestelmissä olevat ongelmat.

Ratkaisuja tietoturvaongelmiin

Jokaisen RFID-järjestelmän kehityksessä täytyy ottaa huomioon kyseisen järjestelmän luonne ja sen omat tietoturvaan liittyvät ongelmat. Analyysissä tulee ottaa huomioon esimerkiksi käsiteltävän tiedon luonne, käytettävän RFID-tunnisteen kyvykkyys ja käyttäjien tarpeet yksityisyydelle.

RFID-järjestelmän tietoturvaongelmiin on pyritty löytämään ratkaisuja esimerkiksi seuraavilla menetelmillä

1. **RFID-tunnisteen sulkeminen.** Tunnistetta tarvitaan monesti vain tiettyyn pisteeseen saakka, esimerkiksi ostotilanteessa tietoa tarvitaan yksilöimään tuote, mutta sen jälkeen tunnisteesta vain haittaa kuluttajan yksityisyyden suojan kannalta. RFID-tunnisteilla voisi olla yksilöllinen salasana, jonka antamalla se tuhoutuisi lopullisesti.
2. **Faradayn häkki.** RFID-tunniste voitaisiin

sulkea Faradayn häkkiin silloin, kun sitä ei tarvita. Tällöin sen käyttö käyttäjän tietämättä olisi paljon haastavampaa. Tätä ratkaisua voitaisiin käyttää esimerkiksi biopassin yhteydessä lisäämällä metallinen kansisivu.

3. **Kryptografia.** Aktiiviseen RFID-tunnisteeseen voidaan sisällyttää logiikkaa, jolla voidaan tehdä turvallinen istunto tunnisteen ja lukijan välillä. Vasta istunnon muodostettua voidaan lukijalle kertoa varsinaista tietoa RFID-tunnisteesta. Ongelmana kryptografian käytössä on se, että useimmat RFID-tunnisteet ovat vielä liian yksinkertaisia, jotta niillä voitaisiin käyttää päteviä kryptografisia menetelmiä.

4. **RFID-tunnisteen tiedon kierrättäminen.** RFID-tunniste mahdollistaa henkilöiden seurannan, sillä niiden ID-numero pysyy samana. Mikäli toiminnallisuutta muutetaan siten, että ID-numero muuttuu joka kerta kun se luetaan, muuttuisi seuraaminen paljon hankalammaksi. Tämä tosin hankaloittaa RFID-tunnisteen lukemista, sillä lukijalla ja tunnisteella tulisi molemmilla olla tiedossa algoritmi, jolla seuraava ID-numero muodostetaan. Lisäksi tunnisteen kierrättäminen vaatii logiikkaa RFID-tunnisteelta, eikä sitä ole helppo tehdä passiivisiin tunnisteisiin.

Yhteenveto

RFID on teknologia, joka on jo nyt laajasti käytössä ja jonka käyttö laajenee jo lähitulevaisuudessa huomattavasti RFID-tunnisteiden hinnan halvetessa. Tietoturva on yksi osa-alue, joka on saanut julkisuutta tunnisteiden yleistymisen myötä ja kuluttajilla on huoli oman yksityisyyden suojan kapenemisesta. Sovelluksissa tulisikin, kuten missä tahansa muussa rakennettavassa sovelluksessa, ottaa huomioon tietoturva jo aikaisessa suunnitteluvaiheessa. RFID-tunnisteiden yhteydessä suurimman ongelman muodostaa sirujen toimintojen yksinkertaisuus, joka ei monesti mahdollista haluttujen tietoturvaominaisuuksien lisäämistä.

Teksti: Markus Tahvanainen
Kai Tarkka

RFID muuttaa varastosta kotiin

Kirjoittajien esittelyt seuraavalla sivulla.

RFID:n (radio frequency identification) yhteydessä puhutaan perinteisesti vain yritysten logistiikasta ja varastojen seurannasta. Se on kuitenkin vain puolet totuudesta. Tulevaisuudessa RFID on mukana meidän kaikkien arjessamme. Kohdusta hautaan.

RFID-sovellukset voisivat hyvin olla osa arkeamme jo nyt. Teknisesti se olisi mahdollista. Maailma ei vain ole ajatukselle vielä kypsä. Muutaman sentin hintainen yksittäinen RFID-siru ei ole enää ainakaan kustannuskysymys.

Yksilönsuojasta on RFID-sirujen kanssa huolehdittava. Äärimmäisyyksiin vietynä yksilönsuojan korostaminen rajoittaa kuitenkin kehitystyötä merkittävästi. Isoveljen valvontaa ei varmasti kukaan halua lisää eikä vastasyntyneille lapsille tulevaisuuden Suomessakaan asenneta sci-fi-elokuvista tutulla tavalla RFID-sirua takaraivoon. Ei ainakaan vastoin heidän tai vanhempiensa tahtoa. Jos käyttäjä itse hyväksyy RFID-teknologian hyödyntämisen, niin sen pitäisi riittää hyväksynnäksi myös lainsäätäjälle.

Miltä tulevaisuuden arki näyttää RFID-sirujen näkökulmasta? Seuraavat kolme tarinaa kertovat tulevaisuuden koululaisen, tietotyöläisen ja seniorikansalaisen elämästä RFID-maailman keskellä.

Vilma 16 v: Koululaisen reput ja pelivehkeet vihdoinkin tallessa

Vilma, 16-vuotta, herää aamulla kotoaan. Hetki vetelehtimistä sängyssä, vaatteet päälle ja kylpyhuoneeseen. Vilman paidannapissa oleva RFID-siru kertoo talon tietojärjestelmälle missä tyttö milloinkin liikkuu, jolloin valot syttyvät ja sammuvat tarpeen mukaan. Kylpyhuoneessa Vilmaa odottaa vaaka, joka tunnistaa tytön. Paino on pudonnut muutaman gramman eilisestä, joten Vilma päättää syödä aamiaiseksi suklaavanukkaan. Vaaka mittaa myös rasvaprosentin eikä koneella ole siitä mitään huomautettavaa.

Aamiaisen jälkeen Vilman koulureppu vilauttaa repun läpässä olevaa vihreää valoa, kun kaikki sinä päivänä tarvittavat koulukirjat ovat repussa. Kassi olalle ja bussiin. Bussin tietojärjestelmä kuittaa Vilman bussin käyttäjäksi. Erillisiä matkakortteja ei tarvita.

Apua allergioihin

Koulurakennukseen saapuessaan koulun tietojärjestelmä noteeraa Vilman saapumisen koulun tiloihin ja omaan luokkaansa. Saapumisesta lähtee myös tieto kodin tietojärjestelmään. Vilma on siis päässyt turvallisesti perille. Ensimmäisen tunnin historiankokeessa RFID-nappi kertoo opiskelupisteen tietokoneelle, että koevastauksen antaja on