Lappeenrannan teknillinen yliopisto
Tuotantotalouden tiedekunta
Tietotekniikan koulutusohjelma

Kandidaatintyö

Ilpo Hiienkoski

RFID-TEKNOLOGIA KULUNVALVONNASSA

Työn tarkastaja: TkT Ari Happonen

Työn ohjaaja: TkT Ari Happonen

TIIVISTELMÄ

Lappeenrannan teknillinen yliopisto
Tuotantotalouden tiedekunta
Tietotekniikan koulutusohjelma

Ilpo Hiienkoski

RFID-TEKNOLOGIA KULUNVALVONNASSA

Kandidaatintyö

2014

41 sivua, 6 kuvaa, 5 taulukoa

Työn tarkastaja: TkT Ari Happonen
Työn ohjaaja: TkT Ari Happonen

Hakusanat: RFID, radio frequency identification, kulunvalvonta, access control

Tämä kandidaatintutkielma on kirjallisuuskatsaus, joka käsittelee RFID-teknologian hyöndyntämistä kulunvalvonnassa. Työssä perehdytään pintapuolisesti itse teknologiaan, ja luodaan katsaus kulunvalvontaan. Työn pääaihe on kuitenkin kulunvalvonnan ja RFID:n yhdistyminen: miten RFID:tä hyödynnetään kulunvalvonnan toteutuksissa ympäri maailmaa. Työssä tarkastellaan RFID:n vahvuuksia, sekä heikkouksia kulunvalvonnan suhteen. Tämän lisäksi pyritään luomaan kuva nykyisistä ja tulevista implementaatioista. Viimeinen tärkeä työn osa-alue on turvallisuus. RFID:tä käytetään korkeankin turvatason kulunvalvontaratkaisuissa ja tällöin turvallisuuden maksimoiminen on ensiarvoisen tärkeää.

ABSTRACT

Lappeenranta University of Technology
Faculty of Technology and Management
Computer Science Degree Program

Ilpo Hiienkoski

RFID-TECHNOLOGY IN ACCESS CONTROL SYSTEMS

Bachelor of Science Thesis

2014

41 pages, 6 pictures, 5 tables

Thesis Examiner: TkT Ari Happonen
Thesis Supervisor: TkT Ari Happonen

Keywords: RFID, radio frequency identification, access control

This bachelor thesis is a review of how RFID-technology is being used in access control applications. The thesis takes a short look in RFID-technology and access control individually. The main point of the thesis however, is the cross section of these two concepts: How is RFID used in access control applications around the world. The thesis examines RFID's strengths and weaknesses from access control's perpective, and tries to build a picture of current and future implementations. The last important theme of the thesis is security: RFID is being used in access control applications that require a very high level of security. In these implementations minimizing risks and maximizing security are of topmost priority.

SISÄLLYSLUETTELO

SYMBOLI- JA LYHENNELUETTELO SEKÄ TERMIEN AVAUS

ACL	Access control list, lista, joka määrittelee eri osapuolten käyttöoikeudet jossakin järjestelmässä.
Bugi	Ohjelmointi, tai sunnitteluvirhe.
Data	Datalla viitataan binäärimuodossa olevaan tietoon, joka sijaitsee esimerkiksi muistisirun sisällä.
DOS	Denial of service, eli palvelunestohyökkäys. Hyökkäys, jossa pyritään estämään käyttäjien tai laiteiden pääsy johonkin palveluun tai järjestelmään.
DES	Data Encryption Standard, Salausmenetelmä jonka lohkon pituus on 64 bittiä ja avaimen pituus 56 bittiä.
HF	High Frequency, eli korkeataajuuksinen. 3 – 30MHz.
HSL	Helsingin Seudun Liikenne, Helsingin ja ympäryskuntien julkista liikenettä hallinnoiva yhtymä.
ISM	Industrial, Scientific, Medical, eli taajuusalue joka on varattu teollisuuden, tieteen ja lääketieteen tarpeisiin ja on vapaasti käytettävissä maailmanlaajuisesti.
Kbps	Kilobittiä per sekunti, datansiirtonopeus.
Keystream	Salaukseen käytetty pseudorandom avainvirta, joka generoidaan yleensä sarjoitetusta siemenestä, eli seedista.

Kulunvalvonta	Ihmisten kulun seuraaminen jollekkin alueelle, ja sieltä pois. Kulunvalvontaan usein liittyy kulun rajoittamista.
LF	Low Frequency, eli matalataajuuksinen. LF radiotaajuudet ovat 30-300kHz.
Middleware	Väliohjelmisto, eli eri järjestelmien välinen kerros. Yleensä tällä tarkoitetaan ohjelmistokerrosta, joka vastaa järjestelmien välisestä kommunikaatiosta.
NFC	Near Field Communication, Pääosin laitteiden, esimerkiksi älypuhelinten parittamisessa käytetty teknologia, joka käyttää hyväkseen radiosignaaleja. Toimii nimensä mukaisesti lyhyillä fyysisillä etäisyyksillä.
RFID	Radio Frequency Identification
P2P	Peer- to- peer, kommunikaatiomuoto jossa jokainen osapuoli toimii sekä palvelimena, että asiakkaana.
SQL	Structured Query Language, relaatiotietokannan hallintaan kehitetty kyselykieli.
SWOT	Strengths, Weaknesses, Opportunities, Threats. Nelikenttäanalyysi, jolla kartoitetaan tarkasteltavan kohteen vahvuuksia ja heikkouksia.
Stream Cipher	Salaustekniikka, jossa viesti salataan merkki kerrallaan käyttäen hyväksi pseudorandomia avainvirtaa.
Tagi	RFID-järjestelmän osa, antennilla varustettu laite joka vastaa lukulaitteen pyyntöihin ja sisältää tagityypin ja tarkoituksen mukaan erilaista tietoa.

UHF	Ultra High Frequency, eli erittäin korkeataajuuksinen.
WLAN	Wireless Local Area Network

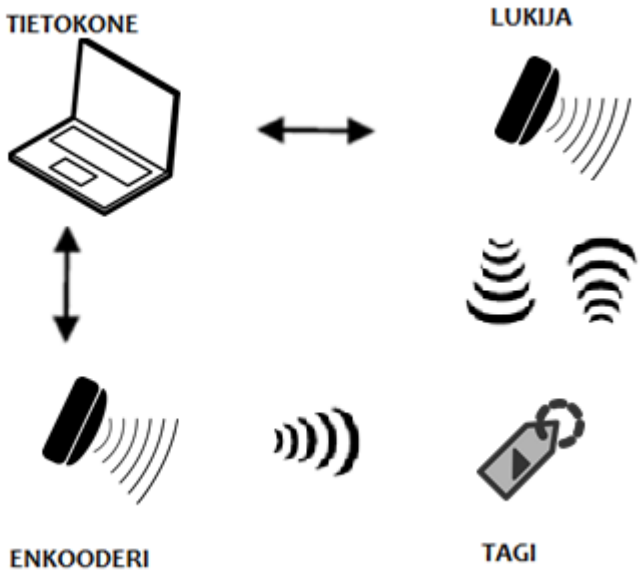
JOHDANTO

RFID:n (Radio Frequency Identification) käyttö kulunvalvonnassa on nykyisin erittäin yleistä. Teknologiaa käytetään seuraamaan ja rajoittamaan erilaisten järjestelmien käyttöä aina yksittäisten rakennuksien kulunvalvonnasta suuren skaalan lippujärjestelmiin. RFID on kehittynyt vuosien varrella erittäin paljon ja erilaisia implementaatioita on valtava määrä. Yksinkertaisista ja suurikokoisista kulkukorteista on tullut pieniä ja käteviä tageja joissa on kehittyneitä datanprosessointiominaisuuksia. RFID-teknologian yleistyessä sen turvallisuudesta on tullut keskeinen huomion kohde. Erityisesti vanhat RFID-järjestelmät ovat monesti haavoittuvia erilaisilla hyökkäyksille.

Tämän kandidaatintyön tarkoitus on selvittää, miten RFID-teknologiaa hyödynnetään tällä hetkellä, ja voidaan tulevaisuudessa hyödyntää kulunvalvonnassa. Tarkastelussa on itse teknologia, sen heikkoudet ja vahvuudet, sekä miten nämä vaikuttavat kulunvalvontaan. Koska RFID:tä käytetään korkeankin turvatason vaativien kohteiden kulunvalontaan, yksi työn tärkeimmistä teemoista on tietoturva ja turvallisuus. Ensimmäisessä luvussa esitellään lyhyesti RFID-teknologia, ja sen toimintaperiaate, sekä luodaan katsaus kulunvalvontaan. Myöhemmin samaisessa luvussa esitellään tutkimuskysymykset, ja tarkempi työn rakenne.

1.1 Tausta

RFID- termillä voidaan periaatteessa kuvata mitä tahansa tunnistusjärjestelmää jossa komponenttien välinen kommunikaatio tapahtuu radioaaltojen ja/tai magneettikenttien avulla. Tyypilliseen RFID-järjestelmään kuuluu tagi(t), lukija, enkooderi ja tietokone. Enkooderi on laite jolla voidaan muokata tagien sisältämää tietoa, tai kirjoittaa uusia tageja. Järjestelmän oiminta perustuu lukijan lähettämään radiosignaalin, johon tagi vastaa. Fyysistä kontaktia tagin ja lukijan välillä ei tarvita, ja tagin voi sisällyttää esimerkiksi kulkukorttiin. [1] Kuva 1 havainnollistaa RFID:n toimintaa:



Kuva 1. RFID-järjestelmän toiminta

Kulunvalvonnalla (access control) takoitetaan ihmisten kulun valvomista ja rajoittamista tietyllä fyysisellä alueella. Käsite kattaa myös erilaisten järjestelmien ja laitteiden käytön valvonnan, joskin nämä implementaatiot ovat harvinaisempia.

Aluetta valvottaessa kulunvalvontajärjestelmään kuuluu aina vähintään kaksi komponenttia: valvottava alue, sekä valvontapiste jossa ihmisten kulkuoikeus takistetaan. Valvontapisteen kautta ihmiset siirtyvät aluueelle ja sieltä pois. Valvottava alue voi olla esimerkiksi aidattu alue, tai rakennus. Valvontapiste olisi vastaavasti portti tai ovi, jonka kautta alueelle kuljetaan.

Kuten mainittu, joskus kulunvalvontajärjestelmään sisältyvät myös käyttöoikeudet erilaisiin laitteisiin tai järjestelmiin. Tällöin kulunvalvontajärjestelmän piirissä oleviin laitteisiin saadaan käyttöoikeus samalla tavalla kuin siirryttäessä alueelta toiselle. Esimerkkinä toimii hyvin esimerkiksi kopiokoneen käyttö: Kopiokone sijaitsee alueella, jolle kulkua valvotaan RFID-kulunvalvontajärjestelmällä. Koneen ominaisuuksiin kuuluu käyttäjän tunnistaminen RFID-tagin perusteella. Ideaalisesti alueella olevat valtuutetut käyttäjät voivat tällöin tunnistautua ja käyttää kopiokonetta samalla tagilla, millä he tulivat valvotulle alueelle.

RFID istuu kulunvalvonnan sovelluksiin erittäin hyvin. RFID-kulunvalvontajärjestelmään kuuluvat tagi, lukija, tietokone, valvontapiste, enkooderi, sekä valvottava alue. Tagi voidaan sisällyttää esimerkiksi kulkukorttiin. Malliskenaario voisi olla esimerkiksi seuraavanlainen: Kulkukortin omistaja näyttää tagin sisältävää korttiaan lukijalaitteelle, joka puolestaan lukee tagin sisältämän tiedon, kun kortti on lukuetäisyydellä. Tagin sisältämän tiedon perusteella lukija lähettää portin lukkoon yhdistetylle tietokoneelle tiedon tagin sisällöstä. Portti avantaan vain, jos tagin sisältämä data oikeuttaa kulkulupaan.

1.2 Tavoitteet ja rajaukset

Työn korkeimman tason tavoite on tutkia RFID-teknologiaa kulunvalvonnan näkökulmasta. Tavoite on kartoittaa nykyisia implementaatioita, markkinatilannetta, sekä selvittää, voidaanko teknologiaa tulevaisuudessa soveltaa laajemminkin kulunvalvonnan alalla tutkimalla tämän hetken uusinta teknologiaa.

Työssä pyritään vastaamaan seuraaviin tutkimuskysymyksiin:

1. Miten RFID teknologiaa hyödynnetään, ja tullaan hyödyntämään kulunvalvonnassa?
2. Onko RFID- teknologia kulunvalvonnan näkökulmasta turvallisempi, tai kustannustehokkaampi kuin muut teknologiat?
3. Onko RFID- teknologialla heikkouksia kulunvalvonnan suhteen, ja voidaanko näitä heikkouksia korjata tai ohittaa?

Työssä keskitytään RFID teknologiaan kulunvalvonnan yhteydessä. Tarkastelun ulkopuolelle jätetään tuotantoketjujen ja mateliaalinseurannan implementaatiot, mutta näissä käytetyn teknologian soveltuvuus kulunvalvonnan implementaatioihin kuuluu tutkimuksen piiriin. Implementaatioita ja markkinatilannetta tarkastellaan maailmanlaajuisesti, mutta pääpaino on länsimaiden alueella.

1.3 Työn rakenne

Luvussa 2 käsitellään kulunvalvontaa ja RFID-teknologiaa hieman syvemmin yhdessä ja erikseen. Tämän jälkeen samassa luvussa vertaillaan erilaisia RFID-teknologian piirteitä

ja pohditaan miten ne soveltuvat kulunvalvonnan tarpeisiin. Luvussa 3 esitellään käytännön implementaatioita. Luvussa 4 pohditaan, mihin suuntaan RFID-kulunvalvonta on kehittymässä. Luvussa 5 tehdään reflektio tehdystä työstä ja sen haasteista. Lopuksi luvussa 6 tehdään yhteenveto työstä.

1.4 Tutkimusmenetelmät

Materiaaleina ja lähteinä käytetään tieteellisiä artikkeleita mm. Google Scholarista, sekä kyseiseen teknologiaan liittyvää kirjallisuutta Lappeenrannan teknillisen yliopiston tiedekirjastosta, sekä muista yliopistoista. Lähteiden perusteella kootaan ensin yleiskuva RFID:n toiminnasta, sekä kulunvalvonnasta. Tämän jälkeen pohditaan RFID:n luomia mahdollisuuksia sekä implikaatioita kulunvalvonnan suhteen. Käytännön implementaatioiden arvioimiseen käytetään SWOT-analyysia.

2 RFID-TEKNOLOGIA JA KULUNVALVONTA

2.1 Sähköinen kulunvalvonta

Kulunvalvonnan tarkoitus on rajoittaa henkilöiden pääsyä tietylle alueelle. Tavoite on sallia pääsy tietyiltä henkilöiltä, ja estää se muilta. Tämä tarkoittaa sitä, että henkilöt on valvontapisteessä tunnistettava jollakin keinolla.

Sähköisen kulunvalvonnan tavoite on tarjota vaihtoehto mekaanisille avainjärjestelmille sähköisten tunnisteiden avulla. Tällöin itse lukot voivat olla yksinkertaisempia ja halvempia, sillä lukkojen uusintasarjoituksia ei tarvitse tehdä tunnisteen hävitessä. Järjestelmässä mekaanisten avaimien määrä on pieni ja niitten haltijat on tarkkaan määritelty. Näitä avaimia käytetään yleensä vain erikoistapauksissa, jossa sähköinen tunniste ei toimi. Tämä sen takia, että sähköisen kulunvalvontajärjestelmän keskeinen toiminto, eli kulkutietojen tallentaminen ei toimi, jos tunnistetta ei lueta. Turvakameroilla tai tukijärjestelmällä, jossa lukon avaaminen jättää merkinnän erilliseen järjestelmään, voidaan parantaa käyttökatkon aikaista valvontaa. [3] RFID-teknologia on tasaisesti syrjäyttämässä vanhempia kulunvalvontajärjestelmiä, jotka perustuivat pääosin magneettiraitakortteihin, ja viivakoodeihin.

Magneettiraitakortteihin perustuvassa järjestelmässä tunnisteen virkaa toimittaa magneettiraita, joka ajetaan lukijan läpi. Perinteisen magneettiraidan suurin heikkous piilee turvallisuudenpuutteessa, sillä se on hyvin helppo kopioida. Tämän takia magneettiraitoihin perustuva kulunvalvontajärjestelmä tarvitsee tukijärjestelmiä, kuten raitakohtaisen koodin, joka syötetään manuaalisesti raidan luvun yhteydessä. Uusia teknologioita jotka yksilöivät magneettiraitoja, ja täten estävät kopioinnin on kuitenkin olemassa. [4] Turvallisuudessa RFID ja magneettiraidat ovat jotakuinkin tasoissa: Yksinkertaisia tageja ja magneettiraitoja on helppo kopioida, mutta tarvittaessa ne voidaan myös suojata hyvin, ja kopioinnista näin erittäin haastavaa.

Viivakoodeja käytettäessä esiintyy sama turvallisuusongelma, kuin magneettiraidoissakin: viivakoodi on helpo kopioida. Tämän takia myös viivakoodit tarvitsevat tukijärjestelmiä,

jotta niiden avulla voitaisiin luoda turvallinen kulunvalvontajärjestelmä. Viivakoodia luettaessa kortin ei tarvitse olla lukijassa kiinni, mutta tekniikan optisen luonteen takia koodin ja lukijan välinen näköyhteys on oltava hyvä. RFID luottaa radioaaltoihin, joten lukijan ja tagin välissä voi olla tagityypistä ja lukijasta riippuen huomattava määräkin materiaalia. [1] Radioaallot liikkuvat tyhjiössä valonnopeudella. Tämän aaltoluonteen takia luettava kohde voi myös liikkua varsin kovaa vauhtia. Tämä on tärkeä etu liikenteen valvonnassa, sillä esimerkiksi RFID:llä varustetun rekan tagin voi lukea kymmenienkin metrien päästä, rekan liikkuessa.

Kulunvalvonnassa voidaan myös käyttää biometrisia tunnisteita, kuten sormenjälkiä tai silmänpohjantunnistusta. Nämä järjestelmät ovat käyttökelpoisia kohteissa, jossa turvatason pitää olla erittäin korkea. Yleiseen käyttöön biometrinen tunnistus ei sovellu yhtä hyvin kuin RFID. Ogelmina ovat järjestelmän korkeampi hinta, tunnistuskeinon hidas ja epäkäytännöllinen lukutapa, sekä tunnistetietojen päivittämisen ja muuttamisen vaikeus. [3]

2.2 RFID:n vahvuudet kulunvalvonnan näkökulmasta

RFID:n vahvuuksiin kilpaileviin teknologioihin verrattuna kuuluu lukuvarmuus: Tagin lukeminen on helppoa ja vaivatonta, ja sen lukeminen onnistuu lähes aina. Magneettiraitaa tai biometrista tunnistusta käytettäessä lukuvarmuus on pienempi, sillä lukutapahtuma on alttiimpi ulkoisille häiriötekijöille. Magneettiraita voi olla likainen, jolloin luku estyy. Sormenjälkeä luettessa ihminen voi tehdä virheen ja painaa esimerkiksi sormensa lukijalle väärällä tavalla. [1]

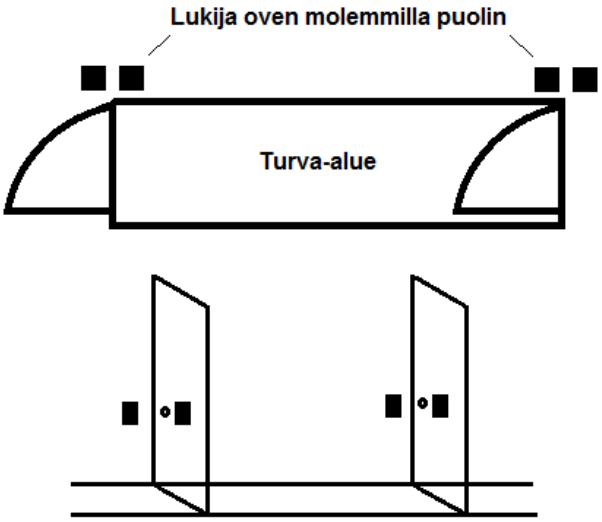
RFID:n eduksi voidaan tietyissä tapauksissa laskea myös hinta. Järjestelmän implementoiminen ja tagien valmistamienen ovat magneettiraitaa tai viivakoodia kalliimpia, mutta tietyissä tapauksissa pitkällä tähtäimellä tagien kestävyys ja uudelleenkäytettävyys ovat hintaetu. [4]

Suurin etu muihin teknologioihin nähden on kuitenkin käyttäjäystävällisyys. Tagi on helppo lukea ja se voidaan muotoilla tarpeen mukaan lähes minkälaiseksi vain. Lukutapa on keskeinen asia käytettävyyden kannalta: Koska tagin ei tarvitse olla kosketuksissa

lukijaan, RFID on erittäin nopea valvontakeino. Magneettiraidat täytyy ajaa lukijan läpi ja viivakoodit asettaa oikeaan asentoon lukijaan nähden. RFID:tä käytettäessä riittää että tagi viedään lukijan lähelle, tai vain kuljetaan tagin kanssa lukijan ohi. [1,3,4]

2.3 RFID:n käyttö ja sen haasteet kulunvalvonnassa

Kulunvalvonnassa itsessään on muutama haaste, jotka tulee ottaa huomioon valvontajärjestelmää suunniteltaessa. Kulkulupia voidaan periaatteessa väärentää tai kopioida, tai niitä voidaan varastaa, jolloin ei-toivottu henkilö pääsee tunkeutumaan alueelle. Toinen selvä ongelma on vanavedessä pysyminen, eli valtuutetun henkilön seuraaminen esimerkiksi portin läpi valvotulle alueelle. Kolmas ongelma on järjestelmän toiminta hätätilanteessa: Järjestelmän on taattava apuhenkilöiden pääsy alueelle hätätilanteessa, mutta tästä ei kuitenkaan saa muodostua turva-aukkoa. [2] RFID-teknologia ei suoranaisesti tarjoa yleistason ratkaisua näihin ongelmiin, mutta niiden ohi voidaan päästä. Seuraamista alueelle voidaan estää esimerkiksi jonkinlaisella suojavyöhykkeellä, kuten esimerkiksi kahdella erillisellä ovella. Molemmat ovet voivat vaatia RFID-tunnistuksen, jolloin sisään pääsee vain yksi henkilö kerrallaan, kuten kuva 2 näyttää. Paloturvallisuuden vuoksi tällaista ratkaisua ei juuri voida käyttää suljetuissa sisätiloissa. Sopiva sovelluskohde voisi olla esimerkiksi tiukasti vartioidun teollisuusaluueen pääportti.



Kuva 2. Valvontajärjestelmän turva-alue

Julkisen liikenteen ollessa kyseessä, väärinkäyttäjiin kohdistuva sakkorangaistus voi olla riittävä vaihtoehto: Matkustajavirran kulkua ei ole hyvä hidastaa useilla porteilla, sillä tällöin koko järjestelmän toiminta hidastuisi. Laiturialueelle pääsee ilmankin lippua. Tarkastajien suorittamat pistotarkastukset ja sakkojen antaminen kuitenkin monesti riittävät väärinkäyttäjien määrän aisoissa pitämiseen.

Kulkulupien väärentäminen on todellinen huoli tageja kirjoitettaessa. Passiivisissa tageissa ei lähes koskaan ole tiedonsalausta, joten ne ovat haavoittuvaisia kopioinnille, joskin niiden lukuetäisyydet ovat yleensä varsin pieniä. Tagien etäluku on silti periaatteessa mahdollista. Normaalilla, tehorajojen puitteissa toimivalla lukijalla tagien etäluku on hankalaa. [2] Potentiaalinen skenaario olisi ehkä täyteen ahdettu ruuhkametro: Tässä ympäristössä lukijalaitteen kanssa pääsisi tarpeeksi lähelle kohteita ilman epäilyttävää käyttäytymistä. Jos tehorajat hylätään, voidaan lukijan kantomatkaa kasvattaa jonkin verran. Tällöin tagien etäluku olisi periaatteessa mahdollista kävelykadullakin. [2] Edellä mainitut skenaariot pätevät vain suojaamattomiin tageihin.

Käyttäjäystävällisyys tekee RFID:stä ideaalisen vaihtoehdon kun halutaan valvoa suuria ihmismassoja. Esimerkkinä tästä on Etelä-Korean Daegussa sijaitseva metro. Järjestelmässä matkustaja ostaa ennen matkaa automaatista pienen kolikkomaisen passiivisen RFID-tagin. Tätä tagia käyttämällä hän pääsee portista sisään laiturialueelle. Matkustaja voi nyt matkustaa minne haluaa. Päämäärässään hän jää normaalisti pois ja nousee ylös asemaan. Seuraavaksi hän syöttää tagin palautusluukkuun, jossa oleva lukija rekisteröi tagin palautetuksi ja päästää matkustajan pois laiturialueelta. Ratkaisu on nopea sekä helppokäyttöinen. Kestävien, muovipäällysteisten tagien takia ratkaisu on myös edullisempi, kuin jatkuvasti uusien kertakäyttöisten lippujen tulostaminen.

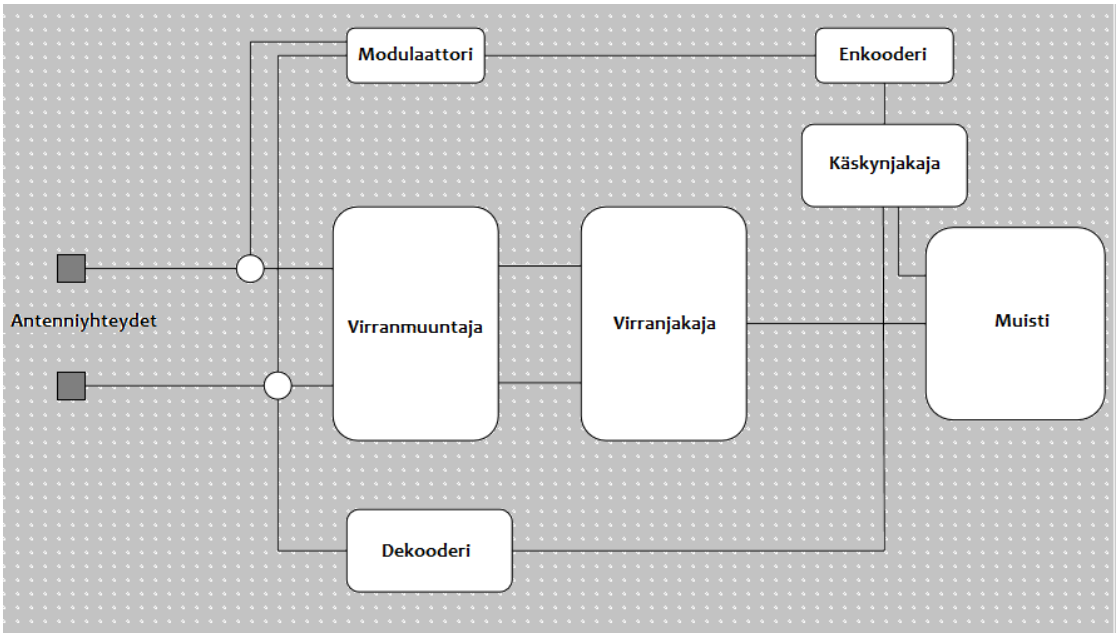
Smart cardeilla tarkoitetaan perinteisen luottokortin kokoluokkaa olevia kortteja, joihin on implementoitu dataprosessoinnin mahdollistavia ominaisuuksia. RFID:n yhteydessä puhutaan kontaktittomista smart cardeista. Nämä ovat muovisia kortteja, jotka sisältävät passiivisen RFID-tagin, ja joiden lukuetäisyydet vaihtelevat välillä 0-100cm. Korttien toimintataajuus on 13,56MHz (HF) ja ne sisältävät yleensä tiedonsalauksen. [5]

NXP Semiconductorsin omistama MIFARE on markkinajohtaja ja yksi yleisimmistä käytetyistä kontaktittomista smart cardeista Euroopassa ja USA:ssa. MIFARE:n markkinaosuus automatisoiduissa lippujärjestelmissä on 77%. Lisäksi korttia käytetään monissa kulunvalvontaratkaisuissa, joissa valvotaan kulkua rakennuksiin. [6] Esimerkiksi HSL eli Helsingin Seudun Liikenne käyttää lippuratkaisussaan MIFARE DESFire EV1 tagia. Salauksena kyseisessä tagissa toimii 3DES, eli kolminkertainen DES-algoritmi, jolloin avaimen pituudeksi tulee 3 * 56bittiä eli 168 bittiä.

Kuva 3. HSL:n käyttämä MIFARE DESFire EV1 - Smartcard

2.4 Erilaiset RFID-tagityypit

RFID-tagit koostuvat antennista, mikrosirusta, radiovastaanottimesta, radiolähettimestä, sekä voimanlähteestä tai itse antennin muodostamasta induktiosilmukasta josta tagi saa virtansa. Tagit voidaan karkeasti jaotella kahteen eri ryhmään: passiivisiin ja aktiivisiin, perustuen siihen miten ne saavat käyttövirtansa. [2] Seuraava kuva esittelee tyypillisen RFID tagin sisältämän mikrosirun rakenteen:



Kuvaaja 2.4 s.34 [1]

Kyseinen siru on osa passiivista tagia, eli siinä ei ole erillistä virtalähdettä. Jos voimanlähde, kuten esimerkiksi paristo lisättäisi tagiin, kytkeytyisi se piirin virranmuuntajaan.

Aktiivisessa tagissa käytetään voimanlähteenä esimerkiksi paristoa. Aktiiviset tagit käyttävät usein hyödykseen korkeita kommunikaatiotaajuuksia. Korkeataajuuksisuus ei ole kuitenkaan aktiivitagien yksinoikeus: myös passiiviset tagit voidaan rakentaa käyttämään korkeita taajuuksia, jos tarve vaatii. Aktiivitagin käyttökantama on kytköksissä virtalähteen tehoon. Periaatteessa mitä tehokkaampi virtalähde, sitä suurempi lähetysteho. Aktiiviset tagit ovat virtalähteensä takia huomattavasti suurikokoisempia kuin passiiviset vastinkappaleensa. Erillinen voimanlähde mahdollistaa myös monimutkaisempien laskutoimitusten suorittamisen tagin sirulla.

Passivisessa tagissa piirin tarvitsema sähkövirta indusoidaan suoraan lukijan lähettämästä radiosignaalista, tai magneettikentästä. Passiivisten tagien antennit ovat yleensä pieniä, sillä lähetystehot ja tagin tarvitsema virta ovat pieniä. Koska erillinen voimanlähde puuttuu, ja antenni on pienikokoinen, passiivisten tagien fyysinen koko on huomattavasti pienempi, kuin aktiivisten tagien. Indusoimalla voidaan periaatteessa saada aikaan suuriakin sähkövirtoja ja lähetystehoja, mutta lakisääteisten lähetystehorajojen takia näin ei toimita. Kun siru tarvitsee enemmän käyttövirtaa, esimerkiksi laskutoimitusten suorittamiseen, on käännyttävä aktiivisten tagien puoleen. Seuraavassa kuvassa on

Lappeenrannan teknillisessä yliopistossa käytetyn kulunvalvontaratkaisun keskeinen komponentti: Passiivinen RFID-tagi.

Kuva 4. Passiivinen RFID-tagi

Tagi voi olla myös semi-passiivinen. Tällöin sirua ja muistia varten on varattu voimanlähde, kuten paristo, mutta lukijan kanssa kommunikoimiseen käytetään yhä lukijan lähettämästä signaalista indusoitua sähköä. Kuten aktiivinen tagi, myös semi-passiivinen tagi pystyy monimutkaisemppin toimintoihin kuin passiivinen vastinkappaleensa. [2] Esimerkkinä tästä ovat kylmäketjuissa käytettävät tagit. Tässä tagilla on paristolla toimivia antureita, jotka mittaavat jatkuvasti kuljetuksen lämpötilaa. Jatkuvaa antennin käyttöä ei tarvita; vain lämpötilan seurannalla on väliä. Luettaessa tagi indusoi kommunikaatioon tarvittavan sähkövirran antenninsa kautta, ja välittää anturin muistiin tallentamat lämpötilatiedot lukijalle. Näin saadaan tietää onko kuljetus pysynyt tarvittavan kylmänä koko kylmäketjun ajan.

2.5 Tagien toimintataajuudet ja lukuetäisyydet

Toimintataajuudella takoitetaan taajuutta, jota tagi käyttää kommunikaatioon ja sähköntuottoon. Tagien käyttämät taajuusalueet voidaan jaotella seuraavasti: low frequency (LF), high frequency (HF), ultra high frequency (UHF) ja mikroaalto. ISM-

taajuusalue (Industrial, Scientific, Medical) määrittelee rajat tagien ja lukijoiden käyttämille taajuuksille. Koska RFID luokitellaan radiotekniikaksi, ei se siksi saa aiheuttaa interferenssiä tai haittaa muille järjestelmille. ISM-standardia käytetään kaikkialla maailmassa ja sen tarkoitus on toimia vapaana kanavana muulle kuin telekommunikaatioon käytetylle radioliikenteelle. ISM ei reguloi alle 135kHz taajuuksia, ja tämän takia LF RFID-toteutukset toimivat usein juurin tämän taajuuden alapuolella. [2] Internal Telecommunication Union (ITU) jakaa mailman kolmeen alueeseen radiotaajuuksien määrittelemiseksi. Alue 1: Eurooppa Afrikka ja Lähi-Itä. Alue 2: Amerikka, Grönlanti ja osa Tyynenmeren saarista. Alue 3: Aasia ja Oseania. Seuraavassa taulukossa esitellään eri tagikategorieoiden käyttämät taajuudet, sekä niitä vastaavat ISM-taajuudet. Jos taajuuden jälkeen ei ole eritelty aluetta, se on kansainvälinen.

Lyhenne	Taajuusalue	ISM taajuus
LF	30-300kHz	< 135kHz
HF	3 – 30MHz	6,78MHz; 13,56MHz; 27,125MHz; 40,680MHz
UHF	300MHz – 3GHz	433,920MHZ(Alue1), 869MHz, 915MHz(Alue2)
Mikroaalto	> 3GHz	2,45GHz; 5,8GHz; 24,125GHz

Table 3.1 RFID frequency ranges s59 [2]

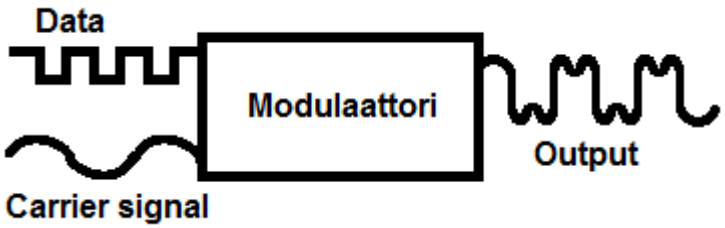
RFID tagin lukuetäisyys perustuu antennin kokoon, tagin lähetystehoon, sekä käyttötaajuuteen. Seuraavassa taulukossa on kuvattu tyypilliset lukuetäisyydet jaettuna taajuusalueittain. Luvut perustuvat mittauksiin todellisista aplikaatioista ja kuvaavat yleisesti käytössä olevia tageja. Teoreettiset maksimaaliset lukuetäisyydet riippuvat virtalähteen tehosta, sekä ulkoisista olosuhteista, kuten esteistä ja niiden materiaalikoostumuksesta. Yleisesti ottaen kuitenkin aaltoluonteensa takia radiosignaali on sitä helpompi lukea pitkältä matkalta, mitä suurempitaajuuksinen se on.

Taajuusalue	Lukuetäisyys
LF	50cm
HF	3m
UHF	9m
Mikroaalto	>10m

Table 3.2 Read range by frequency s60 [2]

2.6 Tagien koodaus

Fyysisesti kommunikaatio tapahtuu moduloimalla radioaaltoa, eli muodostamalla aallon, jonka eri ominaisuudet edustavat ykköstä, ja toiset nollaa. Tämä saavutetaan vaihtelemalla esimerkiksi aallonpituutta, tai taajuutta. Lähetettäessä dataa, tasaista kantosignaalia muokataan modulaatiosignaalilla, joka sisältää lähetettävän datan. Kun vastaanotetaan moduloitu signaali, prosessi suoritetaan päinvastaiseen suuntaan, eli data erotetaan kantosignaalista. Tätä kutsutaan demodulaatioksi. [5] Kuva 3 esittää, minkä muotoinen moduloitu aalto voisi olla:



Kuva 5. Radiosignaalin modulointi

Tagien koodauksella tarkoitetaan tapaa, jolla tagi, ja lukija keskustelevat. Toisin sanoen se on käytäntö, jonka mukaan analogiset radiosignaalit tulkataan kummankin laitteen ymmärtämään muotoon. Käytännössä tämä tarkoittaa binäärimuotoa, eli jonoa ykkösiä ja nollia. Termi ”serial communication” tarkoittaa kommunikaatiota jossa tietoa lähetetään yksi bitti kerrallaan. Lähes kaikki tagit ja lukijät käyttävät tätä yksittäisten bittien jonoa kommunikoinnissaan. Bittisolulla tarkoitetaan koodauksen yhteydessä osaa aallosta, joka edustaa joko arvoa 1 tai 0. Esimerkkinä tästä on NRZ koodaus, jossa 1 esitetään aallonharjana ja 0 vastaavasti aallonpohjana [5]. Seuraavaksi esitellään yleisimmin käytetyt tagien ja lukijoiden koodaukset. [2]

2.6.1 Biphase Manchester encoding

Tässä koodauksessa positiivinen transitio kellojakson bittisolussa tarkoittaa arvoa 1. Negatiivinen transitio on arvo 0. Käytössä on kaksi signaalia: Kellosignaali jota käytetään synkronoimiseen, sekä itse dataa sisältävä signaali. Koska koodaus perustuu transitioihin, käytettävällä modulaatiolla ei ole väliä. Kellosignaalin takia signaali on helpo palauttaa häiriön jälkeen ja siksi se sopii suurien tietomäärien välittämiseen. [2]

2.6.2 Pulse interval encoding

Koodauksessa käytetään pulssien välistä taukoa, tai intervallia. Tietynpituinen tauko tai välimatka tarkoittaa arvoa 1 ja kaksi kertaa tämän pituinen tauko tai intervalli on arvo 0. Yksinkertaisuutensa takia signaali vie vähemmän virtaa, mutta on herkkä desynkronoitumiselle, sillä se ei sisällä kellosignaalia. [2]

2.6.3 DBP encoding

Binääriarvo 0 esitetään transitiona jompaankumpaan suuntaan, puolikkaan bittisolun sisällä. Arvo 1 saavutetaan, kun transitiota ei tapahdu. Jokaisen bittisolun lopussa signaalin taso käännetään. Tietyissä tapauksissa tämä helpottaa signaalin lukemista. [5]

2.6.4 Biphase space encoding

Transitio tapahtuu jokaisessa kellojaksossa, bittisolun reunalla. Jos datasignaalin transitio tapahtuu kellosignaalin transition välissä, kyseessä on arvo 0. Jos ylimääräistä transitiota ei tapahdu, kyseessä on arvo 1. [2]

2.6.5 Pulsed RZ encoding

Neljä lyhyttä pulssia bittisolun alussa tarkoittaa arvoa 1. Jos pulssit tapahtuvat bittisolun lopussa, kyseessä on arvo 0. Signaali palaa nollatilaan joka bittisolun keskivaiheessa. [2]

2.6.6 Differential encoding

Tässä koodaustavassa jokainen binääriarvo 1 aiheuttaa signaalissa tason muutoksen. Arvo 0 ei vaikuta signaalin tasoon lainkaan. Differential koodattu signaali voidaan generoida muokkaamalla NRZ koodausta lisäämällä piiriin XOR-portti ja D-kiikku. [5]

2.6.7 EPC Miller encoding

Millerin koodauksen perustana on transitio jompaan kumpaan suuntaan bittisolun puolivälissä. Uudempi variaatio tästä koodauksesta on käyttää ajoituspulsseja, tällöin ”transitio” on ajoituspulssien lukumäärä per bittisolu. Esimerkiksi 4 pulssia on arvo 0, ja 3 pulssia arvo 1. [2]

2.7 Tagien tietoturva

Ennen erilaisten tietoturvaratkaisujen katselmusta on tärkeää tunnistaa erilaiset vaarat ja hyökkäystavat, jotka uhkaavat RFID-teknologiaa eniten. Järjestelmät ovat usein varsin laajoja, ja erilaisia hyökkäystapoja on paljon. Kulunvalvonnan näkökulmasta tärkein uhkakuva on kuitenkin autentikoimattoman henkilön pääsy suojauksen alla olevalle alueelle, tai järjestelmiin. RFID-järjestelmiin sovellettavat hyökkäystavat voidaan jakaa neljään pääkategoriaan: Denial of service (DOS), insert, spoofing ja replay [7]. Näiden lisäksi omiksi metodeikseen voidaan laskea ”skimming”, ”eavesdropping” ja ”buffer overflow”. [8]

Salakuuntelu, eli ”eavesdropping” tarkoittaa nimensä mukaan lukijan ja tagin välisen kommunikaation kuuntelua ja tallentamista. Kommunikaatio tapahtuu siis autentikoidun lukijan ja tagin välillä ja viestit napataan ”lennosta”. Kuorinta, eli ”skimming tarkoittaa yksinkertaisesti tagien luvatonta lukemista vieraalla lukijalla. Usein tagit eivät vaaadi autentikaatiota, eli ne lähettävät muistinsa sisällön lukijan alkuperään katsomatta. [8] Molemmat edellä mainitut hyökkäystavat pyrkivät saamaan tagin sisällön selville, jonka jälkeen dataa voidaan käyttää miten parhaaksi nähdään, esimerkiksi tagin kloonaamiseen. Tämänkaltaiset hyökkäykset ovat ongelmallisia jos tagi pitää sisällään esimerkiksi henkilötietoja, kuten elektronisen passin sisältö.

Denial of service- hyökkäyksessä järjestelmään syötetään niin paljon dataa, että sen toiminta estyy kapasiteetin ylittymisen takia. RFID yhteydessä Kyseessä on monesti RF-jamming, eli tilanne, jossa tietty radiotaajuus tukitaan voimakkaalla häiriösignaalilla. [7]

Replay- hyökkäys on nimensä mukaan toistohyökkäys. Siinä aito RFID signaali napataan

lennosta, ja sen sisältö tallennetaan. Kopioitu data lähetetään lukijalle myöhemmin alkuperäisen sijasta, ja koska data vaikuttaa aidota, järjestelmä hyväksyy sen. [7]

Muistivuoto, eli ”buffer overflow” tarkoitaa muistipuskurin ylivuotoa. Tämä on yleinen ohjelmistopohjainen haavoittuvuus. Monet ohjelmointikielet eivät suojaa muistin käyttöä optimointisyistä, eli syötteen pituutta ei välttämättä rajoiteta. Puskuri voi sijaita fyysisessä muistissa ohjelman toiminnan kannalta kriittisen datan vieressä. Muistivuodon tapahtuessa puskuri voi vuotaa ohejlmakoodia sisältävään muistiin, jolloin ohjelma voi potentiaalisesti suorittaa haitallista koodia. Tagit ovat usein varsin resurssirajoittuneita. Tämänkaltaisen hyökkäyksen suorittamiseen tehokkaasti tarvitsisi siis laitteen, joka osaa simuloida tageja mutta toimii ilman oikeiden tagien tuomia rajoitteita. [8]

Insert-hyökkäyksessä komento syötetään kohtaan, johon järjestelmä odottaa syötettävän dataa. Web maailmassa tämän kaltaiset hyökkäykset ovat yleisiä (SQL injektiot, jossa käyttäjä antaa tietokantakomentoja, esimerkiksi web-käyttöliittymän kautta.) Samaa voidaan periaatteessa soveltaa tagiin syöttämällä systeemikomento tilaan joka on varattu datan tallentamista varten. [7]

Spoofing- hyökkäyksessä lähetetään väärää dataa, joka kuitenkin näyttää validilta. RFID-tagi voi esimerkiksi lähettää väärää tunnistekoodia. Koska koodi näyttää oikealta, järjestelmä hyväksyy sen. [7]

Hyökkäyksen ei tarvitse tapahtua radioteitse. Se voi tapahtua myös väliohjelmiston kautta. Tällöin kyseessä on middleware- hyökkäys ja se kohdistuu johonkin kohtaan lukijan ja itse hallintaohjelmiston väliin. Hyökkääjä voi esimerkiksi tarkkailla verkkoliikennettä, jota lukija käyttää hyväkseen ottaeessaan yhteyttä ohjelmistopalvelimeen. Kalastettua dataa hyväksikäyttäen voi hyökkääjä myöhemmin tehdä esimerkiksi replay-hyökkäyksen. Samaa verkkoliikennettä on myös mahdollista häiritä ja estää palvelun toiminta esimerkiksi DOS-hyökkäyksen muodossa. Hyökkäyksen kohteena voi olla myös itse backend, eli esimerkiksi tietokantapalvelin. Hyökkääjä siis pyrkii muokkaamaan järjestelmän tietoja, esimerksi lisäämällä tietokantaan uusia tietueita. [7] Kulunvalvontajärjestelmässä tämä voisi tarkoittaa sitä, että alimman turvatason tagilla onkin yhtäkkiä pääsy kaikkialle.

Järjestelmäkokonaisuutta suunniteltaessa, riskianalyysissa on otettava nämä lähestymistavat huomioon, ja pyrittävä minimoimaan niihin kohdistuvat haavoittuvuudet.

Pääasiassa tageja voi suojata kolmella eri tavalla. Tagi voidaan lukita, ja näin estää kaikken sen sisältämän datan muokkaaminen. Tämä tapahtuu yleensä salasanaa hyväksikäyttäen. Toinen yleisesti käytössä oleva suojaustapa on tagin sisältämän tiedon salaus. Viimeinen keino on tagin sulkeminen, eli kill-komento. [1] Kill-komento voi tagista riippuen tuhota tagin fyysisesti, tai muistiin voidaan yksinkertaisesti asettaa arvo”kuollut”. Vaikka sirulle olisi muuten mahdollista kirjoittaa dataa, standardien mukaan kill-komennon käyttöön tarvittavaa salasanaa ei pidä voida ylikirjoitaa, tai edes lukea millään komennolla. [2]

Yksinkertaisin tapa suojata tagi autentikoimattomilta luvuilta on estää radiosignaalien pääsy tagille. Tämä saavutetaan pitämällä tagi esimerkiksi metallilla suojatussa pussissa. Tämä on kuitenkin sangen epäkäytännöllistä, ja sen takia tämänkaltaisiin turvakeinoihin ei yleensä turvauduta. Tietyissä tapauksissa, kuten esimerkiksi passien kanssa toimittaessa tämä on kuitenkin hyvä suojakeino tiedon arkaluonteisuuden ja arvon takia. [9] Lompakossa olevia kulkukortteja voi suojata erikoiskortilla, jossa on ”antiskimming” – ominaisuus. Kyseinen kortti luo käänteisen magneettikentän, joka estää lompakossa olevien korttien luvun. [8] Seuraavissa kappaleissa esitetään muutamia suojautumistapoja, sekä esimerkki koskien MIFARE Classic- smart cardeissa käytettyä salausta.

2.7.1 Blocker Tagit

Blocker tagi on teknologialtaan tavallinen passiivinen tagi. Toiminnaltaan se kuitenkin eroaa muista tageista. Kun sen läheisyydessä olevia tageja luetaan, blocker tagin tehtävä on estää autentikoimattomat luvut, jotka kohdistuvat suojattuun ryhmään. Tagit on voitu esimerkiksi jakaa kahteen ryhmään: Julkiset ja suojatut. Blocker tagin ainoa tehtävä olisi tässä tilanteessa estää luvut, jotka kohdistuvat suojattuihin tageihin. [10]

Blocker-tagin toiminta perustuu protokollaan, jolla tageja luetaan. Monesti kyseinen protokolla toimii puun tavalla: Lukija suorittaa syvyyshaun kartoittaakseen lähettyvillä olevat tagit. Lukija pyytää tageja lähettämään sarjanumeronsa ensimmäisen bitin. Jos tämä bitti on 0, lukija siirtyy puussa vasemmalle. Vastaavasti jos arvo on 1, siirtyy lukija puussa

oikealle. Jos vastauksena tagit lähettävät molempia arvoja, siirrytään puussa molempiin suuntiin. Tämän jälkeen lukija pyytää tageja lähettämään seuraavan bitin sarjanumerostaan, ja niin edespäin. Tällä lailla lukija saa tietoonsa tagien yksilölliset sarjanumerot, ja voi aloittaa tagikohtaisen kommunikoinnin. Blocker tagi hyödyntää tätä protokollaa lähettämällä aina arvot 0 ja 1. Tämä johtaa siihen, että puun koko kasvaa valtavaksi, ja yksittäisten tagien löytäminen mahdottomaksi. [10] 32 bittisen sarjanumeron kohdalla tämä tarkoittaisi, että lukijan näkökulmasta tageja olisi 2^32, eli 4 294 967 296.

Tämänkaltaisen suojauksen implemetoimiseksi tagit on jaettava luokkiin sarjanumeronsa perusteella. Jako voi toimia esimerkiksi siten, että tagit joiden sarjanumero alkaa arvolla 0 ovat private-luokka ja tagit joiden sarjanumeron ensimmäinen arvo on 1, ovat vastaavasti julkiset-luokka. Tällöin blocker-tagi estäisi vain puun vasemmalle olevien, 0-alkuisten tagien hakemisen ja sitä kautta lukemisen. [10]

2.7.2 Selective RFID Jamming

Kuten Blocker tagitkin, RFID jamming kuuluu myös off-tag- tietoturvan piiriin. Off- tag tarkoittaa nimensä mukaisesti sitä, että turvamekanismi ei sijaite suojattavalla tagilla. Selective RFID jamming tarkoittaa valikoivaa signaalin häirintää. Kyseessä on tekniikka, joka estää autentikoimattomat lukuyritykset suojataville tageille: Lukijan lähetettyä kyselyn tagille, turvalaite elvittää reaaliajasa onko kysely oikeutettu. Jos näin ei ole, turvalaite lähettää lyhyen jumitussignaalin, joka estää luettavan tagin ja lukijan välisen kommunikaation. Signaali yksitaajuuksinen ja se on satunnaisesti moduloitu, jotta sen pois suodattaminen olisi vaikeaa. [11]

Turvalaitteeksi kelpaa paristoilla toimiva mobiililaite, kuten moderni puhelin tai kämmentietokone. Tämä sen takia, että laitteen on kyettävä monimutkaisiin laskuoperaatioihin, eikä passiiviivinen ratkaisu tarjoaisi tarvittavaa laskentatehoa eikä tallennustilaa. RFID jamming käyttää hyväkseen ACL-listoja (Access controll list) samaan tapaan kuin tietokoneissa käytettävät palomuurit. ACL määrittää, mitkä tageihin kohdistuvat kyselyt ovat sallittuja ja mitkä estettyjä. Säännöt perustuvat kolmeen asiaan: lähteeseen eli lukijaan, kohteisiin eli luettaviin tageihin, sekä käytettyyn komentoon. Jotta tekniikka toimisi, on hyvä olla lukijoita, jotka tunnistautuvat jollakin tavalla ennen

kyselyjen esittämistä. Tällä tavalla ACL voi määrittää erikoisoikeuksia lukijakohtaisesti. Koska lukijat eivät yleensä yksinkertaisesti suorittavat kyselynsä ilman tunnitautumista, ACL:n täytyy sisältää tietueet, miten toimitaan näiden tuntemattomien lukijoiden kanssa. Yleensä näiden lukijoiden oikeudet ovat varsin rajatut. Sääntöjen avulla turvalaite voi siis esimerkiksi estää kaikkia tuntemattomia lukijoita lukemasta ainuttakaan tagia, tai sallia vain yhden tietyn lukijan muokata jotakin tagiryhmää. [11]

Selective RFID jamming on siis keskitetty turvaratkaisu suuren tagimäärän suojaamiseksi. ACL on helppo muuttaa ja päivittää tarpeen mukaan, ja tekniikka on varsin yksinkertainen. Muutama ongelma on kuitenkin otettava huomioon: Turvalaite on kriittisessä roolissa: jos se hajoaa, koko järjestelmä lakkaa toimimasta. Tekniikka on myös haavoittuvainen DoS-hyökkäyksille: Suuren kyselymäärän yhteydessä jumitussignaali tukkii radioaallot, ja estää pahimmassa tapauksessa muiden järjestelmien toiminnan. [11]

2.7.3 MIFARE Classic Crypto 1

Seuraava esimerkki käsittelee Nicolas T. Cortouis:n pitämää seminaaria, joka pidettiin vuoden 2009 RFIDsec messuilla. Siinä esitetään Card-only hyökkäys, joka kohdistuu MIFARE Classic- kortin käyttämään salaukseen. Card-only viittaa siihen, että hyökkäykseen ei tarvita muuta kuin osaa järjestelmästä, kuin kortti. Crypto-1 on *stream cipher*, eli salaustapa, jossa blokkien sijaan sanoma salataan käyttäen pseudorandomia avainvirtaa, *keystreamia*. Jokainen merkki salataan käyttäen vastaavaa merkkiä avainvirrassa. [12]

MIFARE Classic kortia on myyty yli 200 miljoonaa kappaletta, ja kyseistä korttia käytetään mm Englannin metrojärjestelmässä, ja monissa korkean turvatason kulunvalvontaratkaisuissa ympäri maailman. Noin 70% tutkituista kohteista käytti MIFARE Classic- versiota, tai jotakin LF-ratkaisua. [12]

Cortouis esittää, että hyväksikäyttämällä bugia MIFARE Classic-kortissa, Cipher-1-salaus voidaan helposti murtaa. Bugissa kortti lähettää tietyt 4 bittiä, jos olosuhteet ovat oikeat. Nämä 4 bittiä ovat itse asiassa komento avainvirtaa luodessa. Olosuhteita muokkaamalla

siis voidaan näin testata milloin kortti vastaa ja milloin ei. Kun salaus on purettu, on kortin kopioiminen helppoa. Courtois:n esittämässä hyökkäyksessä kortille tarvitsee tehdä vain 300 kyselyä. Tämän jälkeen kortti voidaan kopioida. Kyselyihin tarvittava aika on noin 10 sekuntia Proxmark3-työkalulla. Tämän ohjelmoitavan lukija-emulaattorin voi tilata netin kautta kuka vain. Edellämainittua työkalua käyttämällä tunkeutuja voi siis periaatteessa ”varastaa” kortin , ja käyttää työkalua emuloimaan eli esittämään korttia. Tunkeutujalla menee siis pahimmassa tapauksessa 10 sekuntia kortin varastamiseen, ja hän voi tämän jälkeen välittömästi astua esimerkiksi suojattuun rakennukseen. [12]

2.8 NFC-teknologia

NFC, eli Near Field Communication on teknologia joka perustuu RFID-standardeihin. NFC mahdollistaa kaksisuuntaisen kommunikaation teknologiaa käyttävien laitteiden välillä. Vaihtoehtoisesti kommunikaatio voi olla myös yksisuuntaista, jolloin kyseessä on lukija ja passiivinen NFC-tagi. NFC:llä on kaksi kommunikointilaa: passiivinen ja aktiivinen. Passiivisessa tilassa kommunikaation aloittaja initialisoi radiokentän, ja kohde saa tarvittavan virran magneettisen induktion avulla. Aktiivisessa tilassa kumpikin laite muodostaa oman radiokenttänsä. NFC toimii 13,56 MHz taajuudella, ja datansiirtonopeuksia on kolme: 106, 212 ja 424 kbps. Periaatteessa suuremmatkin siirtonopeudet ovat mahdollisia jos käytetään vain aktiivista tilaa. Tätä ei kuitenkaan ole määritelty standardeissa. [13]

NFC laitteeella on kolme toimintatapaa: Korttiemulaatio, p2p (peer to peer) sekä lukija/kirjoittaja. Korttiemulaatiossa laite nimensa mukaan voi emuloida smart cardeja. Tämä mahdollistaa toiminnot kuten kaupanteon ja kulunvalvonnan. P2P mahdollistaa kaksi NFC laitetta keskustelemaan toistensa kanssa. Tässä tilassa voidaan lähettää dataa suuntaan tai toiseen. Tämä mahdollistaa esimerkiksi valokuvien jakamisen kahden puhelimen välillä. Lukija/kirjoittaja tilassa NFC-laite voi lukea halpoja ja yksinkertaisia passiivisia NFC-yhteensopivia tageja. Näitä tageja voi olla esimerkiksi juna-aseman aikataulussa, tai mainosjulisteessa. [14]

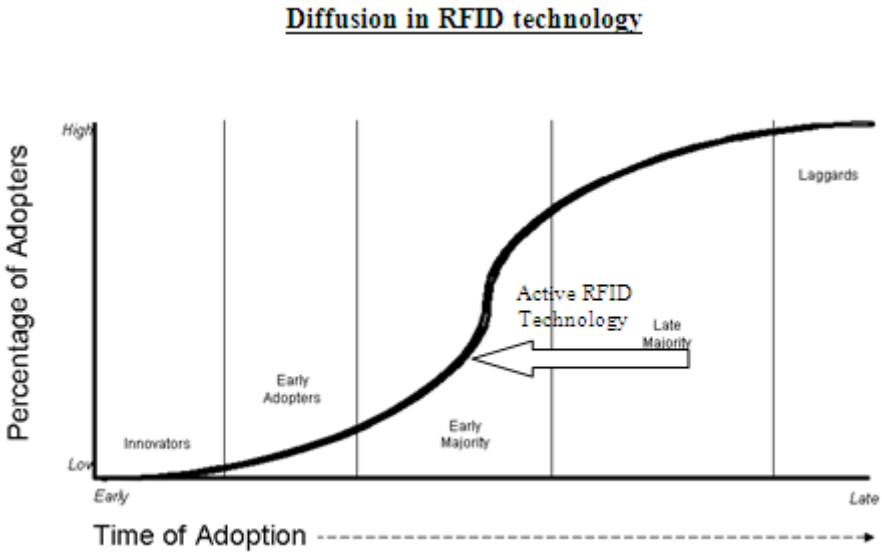
NFC on yleistyvä ominaisuus matkapuhelimissa. Tämän takia on hyvä tarkastella, onko NFC parempi kuin Bluetooth. NFC:n suurin etu Bluetoothiin nähden on yhteyden

avaamisen nopeus. Bluetoothissa puhelinten pitää tunnistaa toisensa, ja tähän monesti tarvitaan manuaalista asetusten säätöä. NFC:n kanssa yhteyden muodostus on välitöntä. Bluetoothin ongelmana on myös pidempi toimintaetäisyys, jolloin se on alttiimpi uhille, kuten kuuntelulle. NFC:n toimintaetäisyys on alle 10cm. Bluetoothin version 1.2 siirtonopeus on nopeampi kuin NFC:n (721 kbps vs. 424 kbps). Tässä on kuitenki otettava huomiooon se, että yleensä näitä teknologioita käytetään siltana muodostamaan nopeampi yhteys, kuten WLAN. Tällöin 300 kbps nopeuserolla ei juuri ole merkitystä, vaan suurempi painoarvo on käytettävyydellä, jossa NFC on Bluetoothia parempi. [15]

Kulunvalvonnan näkökulmasta NFC on mielenkiintoinen teknologia sen takia, että se voi emuloida smart cardien toimintaa. Smart cardein toimivia kulunvalvontatoteutuksia on paljon, ja periaatteessa siirros NFC:n käyttöön on mahdollinen ilman suuria infrastruktuurin muutoksia. NFC omaa myös etuja smart cardeihin nähden. Kulku- ja käyttöoikeuksia voidaan myöntää helposti ilman fyysisen kulkukortin toimittamista. Tämä mahdollistaa esimerkiksi vierailuiden järjestämisen lähettämällä tarvittavat tiedot vierailijan matkapuhelimeen. Lippujärjestelmiä on myös mahdollista korvata NFC:llä: Ennen käyttäjä latasi esimerkiksi viivakoodillisen lipun netistä, mutta nyt hän lataakin kulkukortin jota matkapuhelin emuloi.

2.9 Teknologian Diffuusio

Diffuusiolla tarkoitetaan tässä yhteydessä uusien teknologioiden adoptoimista, ja niiden yhtymistä osaksi valtavirtaa. Diffuusion mittaamiseen käytetään yleisesti S-käyrää. Pystyakseli esittää teknologiaa käyttävien tahojen määrää ja vaaka-akseli esittää käyttöönoton ajankohtaa tuotteen elinkaaren aikana. Seuraava kuva esittää, mihin kohtaan käyrää aktiivisen RFID-teknologian uskotaan sijoittuvan nykypäivänä. Kuvaajan mukaan käyttäjien määrän kasvunopeus on suurimillaan juuri nyt. [16] Passiivinen teknologia sijoittuisi pidemmälle käyrällä, sillä se on ollut yleisessä käytössä pidempään.



Kuva 6. Diffusion in RFID technology [16]

Tulevaisuutta ajatellen voidaan vertailukohteena voidaan käyttää viivakoodeja: kesti useita vuosikymmeniä ennen kuin teknologia saavutti globaalisti dominoivan aseman. RFID ei ole vielä kokoaan syrjäyttänyt kilpailevia teknologioita, vaikka passiivisten tagien kohdalla ollaan jo varsin pitkällä. Sulautumisessa ollaan kuitenkin jo pitkällä ja kasvun voidaan mallin mukaan nousevan vielä hyvän aikaa. Tähän pisteeseen pääsy on vienyt useita vuosia. [16] Kuvaajan mukaan voidaan siis olettaa, että teknologiassa piilee vielä paljon potentiaalia.

3 ESIMERKIT

Tässä kappalessa esitellään kolme erilaista esimerkkiä kulunvalvontaratkaisuista, joissa on hyödynnetty RFID:tä. Ensin implemetaatiot ja tutkimukset esitellään, ja tämän jälkeen jokaisesta tehdään SWOT- nelikenttäanalyysi.

SWOT-analyysi (Strengths, Weaknesses, Opportunities, Threats) on yleinen nelikenttäpohjainen arviointimenetelmä, joka soveltuu moneen tarkoitukseen, kuten esimerkiksi yrityksen strategiseen suunniteluun tai ideoiden ja tuotteiden arviointiin. Ajatuksena on arvioida tarkasteltavan kohteen sisäiset vahvuudet ja heikkoudet sekä ulkoiset mahdollisuudet ja uhkat. Analyysin pohjalta voidaan edelleen luoda päätelmät vahvuuksien vahvistamiseksi, heikkouksien muuttamiseksi vahvuuksiksi, mahdollisuuksien hyödyntämiseksi ja uhkien välttämiseksi.

3.1 Kulunvalvontaa älypuhelinten avulla

Darmstadin yliopiston suorittamassa tutkimuksessa, tutkimusryhmä (Dmitrienko A, Sagedi A-R, Tamrakar S ja Wachsmann C) esittävät suunnitelman ja implementaation kulunvalvontaratkaisusta, joka käyttää hyväkseen NFC-ominaisuudella varustettuja matkapuhelimia. Malli on geneerinen ja sitä voidaan soveltaa useaan eri käyttökohteeseen, mutta työryhmä on valinnut esimerkikseen elektroniset ovilukot. Keskeinen ominaisuus, joka erottaa mallin muista jo olemassa olevista ratkaisuista on käyttöoikeuksien delegointi: käyttäjä voi rajoitetusti jakaa omaa käyttöoikeuttaan muiden laitteiden ja käyttäjien kanssa. Tutkimusryhmän esittämä tietoturvamalli on kerrostettu maksimaalisen turvatason saavuttamiseksi käyttämällä suojattuja suoritusympäristöjä. [17]

Yksinkertaisesti malli toimii siten, että alunperin valtuuksia on vain rekisteröidyillä laitteilla. Nämä rekisteröidyt laitteet voivat jakaa omaa valtuuttaan muiden laitteiden kanssa, jolloin ne saavat samat kulkuoikeudet kuin rekisteröity käyttäjä. Näitä kutsutaan delegoiduiksi käyttäjiksi. Tämä mahdollistaa esimerkiksi oman hotellihuoneen avaimen antamisen kutsuvieraalle. Adminstraattori voi poistaa valtuuksia verkon kautta, ja jos rekisteröity käyttäjä poistetaan, poistuvat myös kaikki hänen delegoimansa käyttäjät. [17]

Suunnittelussa on tehty seuraavanlaisia oletuksia järjestelmämallista:

1. Samalla alustalla ajetaan epäluotettavaa koodia (käyttäjän lataamat sovellukset)
2. Alustalle tallennetaan arkaluontoista tietoa (käyttäjätiedot, autentikointi)
3. Alustalla ajetaan turvallisuuden kannalta kriittistä koodia (kryptograafiset avaimet jne.)

Virtuaaliset kulunvalvonta-valtuudet mahdollistavat moninaisia asioita: niitä voidaan jakaa tai tehdä toimimattomiksi verkon ylitse, ja nykyisten puhelinten ansiosta ne voivat tukea kulunvalvontakäytäntöjä jotka ottavat huomioon esimerkiksi ajan, sijainnin tai ympäristön. Nykyisin on jo olemassa toteutuksia puhelimiin lähetettävistä hotelliavaimista, jotka raukeavat oleskelun päättyessä. Työryhmän mukaan nykyisiin toteutuksiin kuitenkin liittyy riskitekijänä se, että hyökkäyksen kannalta arkaluonteista dataa säilötään matkapuhelimiin joiden käyttöjärjestelmissä on tietoturva-aukkoja. Ongelmana on myös osaksi se, että nykyisten ohjelmien implementaatiot eivät ole julkisia, joten niiden tietoturvatasoa on vaikea arvioida. [17]

Esitetyssä mallissa hyödynnetään suojattua suoritusympäristöä. Tällä tarkoitetaan sitä, että kaikki turvallisuuden kannalta kriittinen koodi (esimerkiksi autentikointi) suoritetaan eristyksissä muusta järjestelmästä ja ohjelmakomponenteista. Samaan piiriin kuuluu myös koodin valvonta, jossa vain luotetut lähteet voivat kutsua turvallisuuden kannalta kriittisiä ohjelman osia.Työryhmä päätyi käyttämään hybridiä ohjelmisto- ja laitteistopohjaisista ratkaisuista. Tämä on parempi kuin kumpikaan yksin, sillä näin voidaan kiertää laitteistopohjaisten ratkaisuiden resurssirajoituksia, ja toisaalta ohjelmistopohjaisten ratkaisuiden tietoturvariskiä. Suunniteltu malli on joustava: suojatun suoritusympäristön voi rakentaa esimerkiksi ARM Trustzone (laitteistopohjainen) ja virtualisaation (ohjelmistopohjainen) avulla. [17]

Kokoonpanoon kuului Android-käyttöjärjestelmällä varustettuja Samsung Nexus S –älupuhelimia ja geneerinen NFC-lukija. Lukija oli yhdistetty Ubuntu Linux-tietokoneeseen. [17]

Sisäiset vahvuudet	*Sisäiset heikkoudet*
1. Turvaominaisuudet 2. Valtuuksien delegointi 3. Siirrettävä arkkitehtuuri 4. Nopeus	5. Arkaluontoinen data 6. Laajempi testaus puuttuu
Ulkoiset mahdollisuudet	***Ulkoiset uhkat***
7. Potentiaalia standardiksi 8. Ohjelmistokyvykkyyden lisääminen	9. Keskitetyn järjestelmän suojaus 10. Matkapuhelimen varastaminen

1. Kerrostettu tietoturvamalli jossa käytetään hyväksi niin laitteistopohjaista eristystä, kuin ohjelmistopohjaistakin.
2. Vastaavista ratkaisuista poiketen valtuuksia voidaan jakaa käyttäjien kesken ilman yhteydenottoa järjestelmänvalvojaan, tai vastaavaan auktoriteettiin.
3. Mallia voidaan soveltaa moniin eri älypuhelimiin ja alustoihin.
4. Tunnistautuminen on nopeaa (testilaitteella tähän meni ~500ms)
5. Arkaluontoista dataa (avaimet ja tunnisteet) säilytetään lähtökohtaisesti vaarallisella alustalla, älypuhelimella.
6. Koska toteutus on kokeellinen ja vielä kehityksessä, laajempi testaus puuttuu. Tätä tarvitaan myöhemmin, jos halutaan edetä standardiksi.
7. Järjestelmällä on periaatteessa potentiaalia kehittyä standardiksi asti (iempia standardeja kyseisille toteutuksille ei ole)
8. Ohjelmiston ominaisuuksien laajentamisen mahdollistaminen.
9. Järjestelmän, joka hallitsee valtuuksia tulee olla hyvin suojattu. (yhteydessä verkkoon, johon ei voi luottaa)
10. Matkapuhelin voidaan varastaa, tai se voi hävitä. Tätä varten käyttäjien olisi hyvä voida itse deletoida valtuutensa esimerkiksi selainpohjaisen sovelluksen kautta. (Yhteyden ottaminen järjestelmänvalvojaan voi olla liian hidasta.)

3.2 RFID:llä varustetut implantit

Enstablishment Lab on kosmeettisten implanttien, kuten rintaimplanttien valmistaja. Yhtiö on nyt uutena ominaisuutena sisällyttänyt osaan tuotteistaan RFID sirun. Kyseessä on LF tyyppinen passiivinen tagi, joka pitää sisällään tunnistetietoja. Tagin toimintataajuus on 134khz. Tunnistetietojen avulla voidaan selvittää yksityiskohtaista dataa implantista. Tagi voidaan lukea ihokudoksen lävitse, kannettavalla lukijalla. [18]

Tunnistetiedot voivat osoittautua tärkeiksi implanttiin liittyvien ongelmien noustessa esille. Implantin tietoja voidaan tarvita vuosien jälkeen, ja tällöin tagi osoittaa hyödyllisyytensä: Paperilla olevat tiedot ovat voineet hävitä kauan sitten, mutta tagi pysyy lukukelpoisena koko implantin elinajan ja pidenpäänkin. Tagi mahdollistaa myös autentikoinnin: Potilas ei voi aina olla täysin varma mikä implantti hänelle on asennettu (malli, materiaalit, aitous etc.) Tagin avulla potilas tietää tarkalleen, mitä hänen kehonsa sisällä on. Tämä siirtää valtaa potilaalle, sillä hän voi tällöin myös itse tutkia implantin tietoja ja muuta siihen liittyvää dataa. Implanttia poistettaessa lääkäri lukee tagin, ja saa tietokannan kautta tarvitsemansa tiedot implantista, ja kuinka se kuuluu poistaa. [18]

Enstablisment Labin toteutus on kattava. Jokainen rintaimplantti sisältää tagin, joka on sijoitettu implantin sisäiseen geeliin. Yritys myy myös tagien lukemiseen tarkoitettuja lukijoita. Tagien ja lukijoiden lisäksi tarjotaan viellä kolmannen osapuolen ylläpitämä tietokanta, josta lääkärit voivat hakea tietoa tagin tunnisteen mukaan. [18]

Samaa teknologiaa voidaan periaatteessa käyttää muissakin implanteissa. Ominaisuus olisi mielenkiintoinen erityisesti terveyden kannalta kriittisissä sovelluksissa, kuten sydämentahdistimissa. Tällöin hätätapauksissa ensihoitajat saisivat kaikki tarpeelliset tiedot potilaan käyttämistä implanteista.

Sisäiset vahvuudet	*Sisäiset heikkoudet*
1. Hoitoon liittyvä tieto saatavilla 2. Hallittava ratkaisu	3. Tiedon arkaluontoisuus 4. Standardien muuttuminen
Ulkoiset mahdollisuudet	***Ulkoiset uhkat***
5. Laajennettava ratkaisu muillenkin implanteille	6. Standardointi 7. Tietojen urkinta

1. Lääkärit ja potilas itse saavat helposti jatkohoitoon tarvittavat esitiedot tietokannasta
2. Ratkaisu on helposti hallittavissa.
3. Potilastiedot ovat aina arkaluontoisia. Ihmiset eivät halua muiden tietävän, mitä implantteja he käyttävät.
4. Standardit voivat muuttua, jolloin arkkitehtuuria voidaan joutua muuttamaan ja tämä voi käydä kalliiksi.
5. Samanlaista ratkaisua voidaan periaatteessa käyttää muissakin implanteissa.
6. Standardit voidaan laskea myös ulkoiseksi uhaksi, sillä niihin ei välttämättä voida vaikuttaa. Kilpaileva ratkaisu voi muodostua standardiksi, jolloin kyseinen ratkaisu syrjäyttää muut implementaatiot.
7. Tietojen urkinta voi muodostua ongelmaksi, jos urkkijalla on myös pääsy tietokantaan, jossa on listattu implanttien tarkemmat tiedot.

3.3 Disney MyMagic+: RFID kulunvalvontaratkaisu

Disneyn MyMagic+ on kokonaisvaltainen lippu, - ja varausjärjestelmä, jota käytetään Disneyn teemapuistoissa. Tässä tarkastelussa keskitytään osaan tästä järjestelmästä: MagicBand-lippujärjestelmään. FastPass+ on osa MyMagic+ järjestelmää. Sen avulla asiakkaat voivat varata tiettyjä viihdykkeitä (laitteita, näytöksiä etc.) etukäteen ja välttää tällä tavalla ruuhkan. Faspass+ -varauksia on rajattu määrä per asiakas. [19]

MagicBand koostuu nimensä mukaan RFID-tagilla varustetusta vedenpitävästä rannekkeesta. Ranneke jaetaan asiakkaille hotelli-checkinin yhteydessä. Jos asiakas ei ole hotellivieras, hän saa smartcard-kortin, joka on toiminnaltaan ranneketta vastaava. Asiakas voi myöhemmin ostaa rannekkeen puistosta. MyBandilla on useita käyttötarkoituksia, joista tärkeimmät ovat: [19]

- Disney Resort- hotellihuoneen avain
- Pääsylippu vesi-, ja huvipuistoihin
- Fastpass+ pääsylippu (varaus/lyhyempi jono)
- Maksuväline virvokkeiden ostoon teemapuistoissa ja hotelleissa

Ranneke koostuu passiivisesta tagista (MIFARE DESFire EV1), sekä paristolla toimivasta piirisarjasta. Rannekkeessa on myös korkeatehoinen radiolähetin, (2,4gHz) joka on yhteydessä langattomaan verkkoon Disney-kohteissa. Rannekkeella on siis kaksi pääasiallista ominaisuutta: RFID:n kautta toimiva tunnistus, sekä langattoman verkkoyhteyden avulla toteutettu valvonta. Korkeataajuuksinen radiolähetin toimii majakkana, (beacon) jonka avulla rannekkeen sijaintia voidaan seurata kun se on yhteydessä puistossa oleviin vastaanottimiin. [19]

Toteutukseen kuuluu keskeisenä osana älypuhelinsovellus. Ranneke on yhteydessä sovellukseen ja sovellus on yhteydessä asiakkaan luomaan Disney-tiliin. Sovellus mahdollistaa FastPass+ varausten tekemisen asiakkaan tilille. Varaus lunastetaan kohteeseen saavuttaessa MagicBandin avulla. Asiakkaalla ei tarvitse olla älypuhelinta, eikä sovelluksen käyttö ole pakollista. Tällöin asiakkaan on tehtävä FastPass+-varauksensta

joko tietokoneella, tai asiakaspalvelupisteessä. [19]

Sovellus mahdollistaa myös jonotilanteen tarkastamisen: sovellus seuraa jonoja, sekä esimerkiksi maskottien liikkeitä puistossa. Tämän mahdollistaa rannekkeen korkeatehoinen radiolähetin, joka on yhteydessä puiston langattomaan verkkoon. Tällä tavoin järjestelmä voi pitää kirjaa kaikista puistossa olevista rannekkeista, sekä niiden liikkeistä. Viimeisenä tärkeänä ominaisuutena ranneketta voi käyttää maksamiseen puistossa, tai hotellissa. Ranneketta näytetään lukijalle, joka kirjaa maksuusuoritukset asiakkaan huonetilille, johon on sidottu luottokortti. Maksuominaisuutta voi siis vain käyttää, jos on hotellivieras. [19]

Sisäiset vahvuudet	***Sisäiset heikkoudet***
1. Asiakasystävällisyys 2. Massojen seuraaminen 3. Asiakaskäyttäytymisen seuraaminen 4. Kollektiivinen järjestelmä	5. Hinta 6. Yksityisyys
Ulkoiset mahdollisuudet	***Ulkoiset uhkat***
7. Kilpailuvaltti 8. Patentit	9. Varkaus 10. Rannekkeen kopioiminen [20]

1. Teknologia on läpinäkyvää, ja ranneketta on hellpo käyttää. Sen käyttö nopeuttaa puiston sisäisiä prosesseja huomattavasti.
2. Älypuhelinsovelluksen avulla voidaan ohjata ihmismassoja puiston sisällä, uutisoimalla esimerkiksi jonotilanteista puiston sisällä.
3. Ratkaisu mahdollistaa asiakasryhmien analysoimisen esimerkiksi iän ja sukupuolen mukaan. Tällöin eri kohteita voidaan datan avulla suositella esimerki FastPass+-kohteiksi.
4. Järjestelmä kasaa yhteen ennen erillisinä toimineet järjestelmät.
5. Ratkaisu on hintava niin puistolle, kuin asiakkaallekin.

6. Ihmiset haluavat tietää missä ja miten heidän liikkeitään seurataan. Järjestelmän toiminta täytyy olla hyvin dokemntoitu ja avoin yleisölle. Jos näin ei toimita, tulee olemaan asiakkaita, jotka eivät käytä järjestelmää yksityisyydensuojan takia.
7. Teknologia on kilpailuvaltti, sillä se on tällä hetkellä kehittynein kulunvalvontaratkaisu huvipuistojen saralla.
8. Patentit ovat mahdollisuuksia: Ne voivat olla tuottoisia Disneylle tulevaisuudessa kun muutkin huvipuistot alkavat uusia kulunvalvontaansa.
9. Ranneke toimii maksuvälineenä ja hotellihuoneen avaimena, joten väärinkäytön mahdollisuus on olemassa.
10. MIFARE DESFire EV1 on luultavasti lähitulevaisuudessa mahdollista kopioida samalla tavalla kuin MIFARE Classic- tagi, sillä korttien kopioimiseen käytetyt työkalut kehittyvät koko ajan. [20]

4 RFID JA KULUNVALVONTA TULEVAISUUDESSA

RFID-kulunvalvontajärjestelmä tarvitsee ainakin vielä tukijärjestelmiä, kuten kameravalvontaa, pin-koodia tai kosketusnäyttöjä jos turvallisuus halutaan maksimoida. Niin kauan kun tagi voidaan varastaa tai väärentää, tukijärjestelmille on tarvetta. Kännyköiden kehitys, sekä kehon sisälle asennettavat tagit voivat muuttaa tämän. Antenni-, paristo- ja akkuteknologian kehittyessä aktiivisen tagin koko pienenee lähelle nykyisiä passivisia toteutuksia, ja niiden käyttöikä myös kasvaa reippaasti. Aktiivinen tagi antaa paljon laajemmat mahdollisuudet mille tahansa implementaatiolle, mukaanlukien kulunvalvonnalle, mm. tagin vahvan salauksen muodossa.

Kulunvalvonnan kannalta myös kännyköiden kehitys on mielenkiintoinen alue. Kun puhelinten NFC-teknologia tulevaisuudessa kehittyy, puhelimiin voidaan potentiaalisesti tehdä aplikaatioita, jotka emuloivat lähes mitä tahansa tagia. Tällöin itse puhelin voisi toimia kulkukorttina, eikä erillisiä tägejä tarvitsisi. Koska kyseessä on aplikaatio, voidaan sitä muokata helposti, esimerkiksi vaihtaa salauksen tyyppiä, tai jopa toimintataajuutta. Tämä vähentäisi tagin etälukemisen ja väärentämisen riskiä huomattavasti, sillä kun rikollinen yrittäisi valvotulle alueelle, olisi hänen käyttämä taginsa jo vanhentunut. Tämän lisäksi tunkeilijan olisi toki päästävä myös mahdollisten tukijärjestelmien, kuten pin-koodin syötön ohi. Riski on todellinen, joskin pienempi kuin erillisen tagin kohdalla. Puhelin on niin integroitunut ihmisten jokapäiväiseen elämään, että sen puuttumisen huomaisi lähes heti. Tämän jälkeen kyseinen puhelin voitaisiin poistaa sallittujen laitteiden listalta.

Biometriset tunnisteet tulevat luultavasti yleistymään tulevaisuudessa entisestään. Tulevaisuudessa tämä tunniste olisi kehon sisäinen RFID-implantti, joka sisältäisi esimerkiksi henkilötiedot ja sairashistorian. Kyseinen tagi voidaan asentaa tulevaisuudessa ehkä jo vastasyntyneen ensimmäisten rokotteiden kanssa, rutiinitoimenpiteenä. Kulunvalvonan näkökulmasta tämä tarkoittaisi, että ihmisten liikkumista voitaisiin valvoa massiivisella skaalalla. Monista tukijärjestelmistä voitaisiin myös luopua, sillä kehonsisäistä tagia olisi hankala varastaa. Salauksen tulisi tämän kaltaisessa tagissa olla vahva, ja tagia luultavasti jouduttaisiin päivittämään teknologian kehittyessä.

5 KESKUSTELU JA YHTEENVETO

RFID-teknologia on tunkeutunut jo lähes joka teollisuudenalalle, ja nyt sama tapahtuu kuluttajapuolella: uusia implementaatioita kehitetään koko ajan. RFID:tä hyväkseen käyttäviä kulunvalvontaratkaisuja on ollut jo varsin kauan, mutta ne ovat alkaneet yleistyä vahvasti vasta viime aikoina: Vanhoja kulunvalvontajärjestelmiä päivitetään käyttämään uudempaa teknologiaa, ja täysin uusia käyttökohteita kehitetään kaiken aikaa.

Kulunvalvonnan näkökulmasta RFID on monin tavoin parempi, kuin kilpailevat vanhemmat teknologiat, kuten viivakoodit ja magneettiraidat. RFID on halvempi ja yleisesti ottaen myös turvallisempi, kuin kilpailijansa. Monia järjestelmiä ei voitaisi edes toteuttaa vanhemmilla teknologioilla (esim rintaimplanttien sisältämät RFID-tagit).

RFID:llä on myös omat heikkoutensa. Riskejä ei voi unohtaa, sillä tällöin voi muodostua vakavia turva-aukkoja. On kuitenkin osoitettu, että huolellisella suunnittelulla näitä heikkouksia voidaan paikata monin eri tavoin. Tapoihin kuuluvat niin ulkoiset järjestelmät, kuin sisäinen arkkitehtuurikin.

RFID tulee luultavasti syrjäyttämään suuren osan vielä nykyisin markkinoilla olevista teknologioista. RFID-teknologian kehitykseen sijoitetaan nykyisin myös paljon rahaa, ja tulevaisuuden näkymät ovat siksi varsin hyvät.

LÄHTEET

1. Kleist, R., Chapman, T., Sakai, D., Jarvis, B., *RFID Labeling, Smart Labeling Concepts & Applications for the Consumer Packaged Goods Supply Chain,* 2nd Edition, Printronix, USA, 2005.
2. Bill Glover, Himanshu Bhatt, *RFID Essentials*, O'Reilly Media, 2006.
3. Vuorinen, A.,Vironen, V., Leskinen, M., *Kulunvalvonta ja Rikosilmoitinjärjestelmät*, 2002.
4. http://www.hightechaid.com/tech/card/what_ms.htm (What's With This Magnetic Stripe Stuff?)
5. Klaus Finkelzeller, RFID Handbook: *Fundamentals and Applications in Contactless Smart Cards and Identification*, 2nd Edition, John Wiley & Sons, 2006.
6. http://www.mifare.net/en/aboutmifare/ (Yleistä tietoa MIFARE:sta)
7. Thornton, F., Haines, B., M. Das, A., Bhargava, H., Campbell, A., Kleinschmidt, J., *RFID Security*, Syngress Publishing, Inc., Kanada, 2005.
8. Paris Kitsos (Ed.), Yan Zhang (Ed.), *Security in RFID and Sensor* Networks. Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan M. Estevez-Tapiador, Arturo Ribagorda, *Attacking RFID Systems*, Auerbach Publications, USA, 2009.
9. http://www.rfidjournal.com/articles/view?1218 (U.S. Tests E-Passports)
10. Garfinkel, Simon, Beth Rosenberg, *RFID: Applications, security, and privacy, Pearson Education*, Intia, 2006.
11. Melanie R. Rieback, Bruno Crispo, Andrew S. Tanenbaum, *Keep on Blockin' in the Free World: Personal Access Control for Low-Cost RFID Tags*, Computer Systems Group, Vrije Universiteit, Amsterdam, The Netherlands.
12. Card-Only Attacks on MiFare Classic, Nicolas T. Courtois, RFIDsec09, 2009.
13. Ecma International: Standard ECMA-340, Near Field Communication Interface and Protocol(NFCIP-1),3rd edition, 2013
14. http://nfc-forum.org/
15. Rachana Wardekar, Rasika Ingole, *Wireless Communication Technology NFC in Mobile Computing – A Review Article*, G. H. Raisoni College of Engineering, Department Of Master in Computer Application,Nagpur, India

16. http://icow313.wordpress.com/diffusion/ (RFID-teknologian diffuusio)
17. Alexandra Dmitrienko, Ahmad-Reza Sadeghi, Sandeep Tamrakar, Christian Wachsmann, SmartTokens: *Delegable Access Control with NFC-enabled Smartphones*, Fraunhofer SIT Darmstadt, Germany, Technische Universität Darmstadt, Germany, Aalto University School of Science, Finland, 2012
18. http://www.rfidjournal.com/articles/view?11093/3 (RFID & implantit)
19. https://disneyworld.disney.go.com/plan/my-disney-experience/my-magic-plus/ (Disney MyMagic+)
20. Adrian McGabe, *Disney's MagicBand, a Security Assessment*, George Mason University, Department of Computer Science, Fairfax VA, 2013 (http://mousechat.net/index.php/2013/12/15/disney-magic-bands-security/)