Harjoitus 8

Nelli Sviili

nekasvii@student.jyu.fi

TIES436 Langattomat teknologiat

Informaatioteknologian tiedekunta

10.3.2020

Sisällys

1. RFID- ja NFC-teknologioiden uhat ja niiltä suojautuminen

Radiotaajuuden etätunnistusta eli RFID:ta (Radio Frequency Identification) käytetään datan etälukuun RFID-tunnisteiden avulla. Edullinen RFID-teknologialla on monia hyödyntämismahdollisuuksia muun muassa kaupanalalla, arjessa ja julkisella sektorilla. Teknologoalla on kuitenkin merkittäviäkin uhkia. Teknologia on altis viruksille ja monille haavoittuvuuksille. Useissa tapauksissa RFID-haavoittuvuuden hyödyntäminen vaatii sisäpiiritietoja.

Hollantilainen Vrijen yliopisto on havainnut tutkimuksissaan, että RFID-teknologia on altis viruksille, madoille ja haittaohjelmille. RFID-tunniste voidaan saastuttaa tarkoituksella viruksella ja skannatessa tunnistetta virus saastuttaa RFID-ohjelmiston käyttämän taustatietokannan. Taustatietokannasta virus voidaan levittää helposti muihin RFID-tunnisteisiin. RFID-haittaohjelmia vastana voi suojautua pääkäyttäjätasolla tarkistamalla ohjelmakoodit, lukitsemalla käyttäjätilit ja poistamalla kaikki ne ominaisuudet, joita ei tarvita. Mitä enemmän on rajapintoja ohjelmiston ja käyttäjän välillä, sitä enemmän myös hyökkääjällä on mahdollisuuksia päästä käsiksi ohjelman koodiin ja tietokantoihin.

Tietoturva-alan yritykset ovat osoittaneet huolensa yritysten kulunvalvontajärjestelmien tietoturvatason vajavuudesta. Kulunvalvontajärjestelmät on yleensä toteutettu RFID-teknologian avulla, jolloin avainkortit ja lukija keskustelevat radiotaajuudella. Tätä liikennettä voidaan yrittää manipuloida ja huijata päästäkseen yrityksen tiloihin tai heidän tietoihinsa käsiksi esimerkiksi yritysvakoiluun liittyen. Avainkortti voidaan lukea lähietäisyydeltä ja kopioida sen sisältö tyhjälle kortille, jolloin entistä tyhjää korttia voidaan käyttää alkuperäisen avainkortin tavoin. Keskeistä suojautua edellä mainitun kaltaiselta tilanteelta on säilyttää aina avainkortit huolella tallessa eikä lainaa niitä kenellekään. Yritys voi myös toteuttaa lukosto suojatulla avainprofiililla, jolloin lisäavainten teettäminen on mahdollista vain tunnuksilla. Lisäksi kulkuun kriittisiin paikkoihin voidaan vaatia avainkortin lisäksi PIN-koodi.

RFID-tunnisteisiin on mahdollista lisätä salaussuojaus, mikäli halutaan, että vain valtuutettu lukija voi lukea tai kirjoittaa laitteelle. Suojausta hyödynnetään esimerkiksi sähköavainten, lukkojen ja käynnistyksenestolaitteiden kohdalla. Suojauksen taso on kuitenkin suhteessa muuhun tietotekniikkaan heikko. Esimerkiksi maaliskuussa 2020 on paljastunut vakavia haavoittuvuuksia Kian, Hyundain ja Toyotan ajonestolaitteissa. Näiden autonvalmistajien ajonestolaitteissa hyödynnetään Texas Instrumentsin DTS80-piiriä, joka mahdollistaa myös salauksen. Autonvalmistajat eivät ole

kiinnittäneet riittävästi huomiota laitteiston tietoturvaan. Edullisella Proxmark RFID-lukijalla saa luettua autosta tai avaimesta riittävästi tietoa purkaakseen laitteen kryptauksen, jolloin samaisella RFID-lukijalla voisi matkia auton avainta, sulkea käynnistyksenestolaite ja käynnistää moottori. Toimenpide vaatii kuitenkin varkaalta murtautumista autoon.

Uudemman teknologian omaavia autoja on onnistuttu varastamaan aiemminkin. Perinteisesti niin sanotuilla relay-hyökkäyksillä on pystytty varastamaan luksusautoja. Relay-hyökkäykset vaativat sen, että auton avainnippu on suhteellisen lähellä autoa. Varkaat vahvistavat radioverkkoa muutamalla radiolla, jolloin auto tunnistaa sähköavainten läheisyyden ja kykenee avaamaan ovien lukituksen ja käynnistämään auton. Autoon kohdistuvat uhat voidaan torjua autonvalmistajatasolla kiinnittämällä enemmän huomiota autojen eri laitteiden tietoturvaan ja omistajatasolla hankkimalla lisäturvalaitteita autoon, kuten ohjauspyörän lukituslaitteita, tai säilyttämällä autoa lukitussa tilassa.

Tietosuojaongelmat ovat yksi merkittävistä RFID-teknologian uhista. Yksityisyys on perusoikeus, jota suojataan monin perustavanlaatuisin asetuksin ja laein, kuten esimerkiksi EU:n perusoikeuskirjassa ja Euroopan ihmisoikeussopimuksessa. RFID-tekniikan avulla voidaan kerätä tietoja, jotka ovat yhdistettävissä yksilön henkilötietoihin. Tekniikka mahdollistaa esimerkiksi kaupan kanta-asiakaskorttiin yhdistetyn RFID-tarran avulla asiakkaan tarkan seuraamisen kaupan tiloissa ja sitä kautta muun muassa kauppa kykenee kohdentamaan entistä voimakkaammin mainontaansa.

RFID-teknologiaa voi hyödyntää myös matkakorttien yhteydessä osana etäluettavaa rahastusjärjestelmää. Tällöin kuljetusfirma voisi tallentaa RFID-tunnisteeseen asiakkaansa henkilötiedot, jolloin yritys tietäisi koko ajan, missä asiakas liikkuu matkustaessaan heidän liikennevälineissään. Tämä toiminta jo rikkoisi henkilötietolakeja. Lisäksi mahdolliset hyökkääjät voisivat etälukea tietoja täysin huomaamatta. Tietosuojaongelmiin keskeisin ratkaisu, on ettei RFID-tunnisteille tallenneta mitään ihmisten yksityisyyteen liittyviä tietoja eikä RFID-tekniikkaa käytetä ihmisten seuraamiseen. Tietosuojan määrittää lait. Liike-elämälle jää kuitenkin merkittävä vastuu itsesäätelystään.

Lähteet:

Greenberg, A. (2020). Hackers can clone millions of Toyota, Hundai and Kia keys. Ars technical. Viitattu: 10.3.2020. https://arstechnica.com/cars/2020/03/hackers-can-clone-millions-of-toyota-hyundai-and-kia-keys/

Kankaanpää, T. (2006). Radiotaajuustunnistusteknologiaan (RFID) liittyvät tietosuojaongelmat. Lapin yliopisto, Oikeustieteiden tiedekunta.

Rieback, M.R., Simpson, P.N.D., Crispo, B., Tanenbaum, A.S. (2006). RFID viruses and worms. Vrije Universiteit, Faculty of sciences. Viitattu: 10.3.2020. http://www.rfidvirus.org/

Salmela, S. (2017). Kulunvalvontajärjestelmän haavoittuvuudet -10 vinkkiä kulunvalvontajärjestelmien turvallisuuteen. Accesspoint. Viitattu: 10.3.2020. https://accesspoint.fi/blog_post/kulunvalvontajarjestelmien-haavoittuvuudet/