Tiivistelmä

Langattomien tietoverkkojen tietoturva

Tässä LUOTI-ohjelman yhteydessä tuotetussa raportissa tarkastellaan keskeisten langattomien tietoverkkojen tietoturvan nykytilaa, tietoturvauhkia ja niiden ratkaisuja. Nykypäivän keskeisiksi ja merkittäviksi teknologioiksi tarkasteluun valittiin WLAN, WiMax, Bluetooth, 3G, RFID ja Flash-OFDM. Teknologiat ovat hyvinkin erilaisia ja niiden keskinäinen vertailu ei ole mielekästä. Niillä on kuitenkin sekä yhteisiä että teknologiakohtaisia tietoturvauhkia. Esimerkiksi Bluetoothin käyttö saattaa sisältää viestien lähettämisiä ennalta tuntemattomien laitteiden kanssa, jolloin tietoturvan arviointi jää paljolti käyttäjän tehtäväksi.

Langattomia tietoverkkoja koskevat myös yleiset tietoturvauhkat, joskin toiset uhkat nousevat muita merkittävämmiksi. Palveluntarjoajan näkökulmasta palveluiden väärentäminen, haitta-ohjelmat, tietoturvaongelmien julkisuusvaikutukset ja asiakkaiden yksityisyyden suojan menetys ovat päähuolenaiheet. Loppukäyttäjän tietoturvauhkia ovat mm. yhteyden tai tunnuksien kaappaaminen, päätelaitteen sisällön muutokset ja salakuuntelu.

Langattomilla verkoilla ei ole kiinteiden verkkojen luonnollista fyysistä pääsynhallintaa. Vihamielisten käyttäjien heikko jäljitettävyys ja radiotaajuushäiriöt ovat myös langattomille verkoille ominaisia. On teknisesti mahdollista paikantaa radiohäiriöiden aiheuttaja, mutta ei ilman erikoislaitteita ja valvontaa.

WLAN

WLAN on langaton lähiverkkoteknologia, jolla yleisesti tarkoitetaan IEEE:n 802.11-standardiperheen mukaisia laitteita. WLAN-teknologiat ovat laajassa käytössä niin kotona kuin toimistoissakin; käytännössä kaikkialla. Kaikilla eri käyttötarkoituksilla on erilaiset tietoturva-vaatimukset. Lisäksi, jotkin WLAN-verkot ovat tarkoituksella avoimia, kuten kaupunkiverkot. WLAN-teknologioiden tietoturvaominaisuuksiin kuuluu Wired Equivalent Privacy (WEP, vanhentunut) ja uudemmat Wi-Fi Protected Access versiot 1 ja 2 (WPA ja WPA2). WPA on osajoukko 802.11i-standardista ja WPA2 802.11i-standardin täyttävä toteutus tietoturva-mekanismeista.

Koska WLAN:ia käytetään yleisesti Internet-yhteyksissä, koskevat kaikki Internetiä koskevat uhkat myös WLAN-käyttäjiä. WLAN-verkoissa tietoturvauhkia ovat mm. Rogue Access Point eli valetukiasema, joka kaappaa WLAN-käyttäjän liikenteen itselleen. Yritysten WLAN-verkot saattavat tarjota vapaan pääsyn esimerkiksi yritysten omiin sisäverkkoihin.

Suljetuissa yksityisissä WLAN-verkoissa hyvänä tietoturvaratkaisuna voidaan pitää CCMP-protokollaa ja AES-algoritmia. Autentikointimenetelmistä kaikki Extensible Authentication Protocol (EAP) -pohjaiset menetelmät eivät sovellu langattomaan käyttöön. TLS-protokollaan perustuva EAP on turvallinen. Suurissa WLAN-verkoissa voidaan käyttää myös IEEE 802.1X -autentikointipalvelinta ja Julkisen avaimen (PKI) järjestelmiä skaalautuvan ja turvallisen ylläpidon mahdollistamiseksi, jos linkkikerroksen tietoturvaa halutaan. WPA2-sertifioitujen tuotteiden käyttö on suositeltavaa näissä WLAN-verkoissa. Jos WPA2 ei ole käytettävissä, tulee käyttää WPA:ta. Jos laitteet ovat vanhoja ja edelliset eivät käy, pitää käyttää WEP:n

lisänä esimerkiksi VPN-tunnelointia. Julkisissa avoimissa verkoissa kuka tahansa voi liittyä verkkoon ja seurata sen liikennettä; näissä verkoissa yrityskäyttäjän on käytettävä VPN-tunneleita ja kaikkien käyttäjien on syytä varmistua sovellustason salauksen, kuten SSL tai TLS, käytöstä, mikäli tarpeellista.

WiMAX

WiMAX (Worldwide Interoperability for Microwave Access) on esitelty IEEE:n 802.16-standardissa ja virallinen nimi on WirelessMAN. WiMAX tarjoaa joko laajan kaistan (70Mbit/s) tai vaihtoehtoisesti jopa yli 100 km:n kantaman. WiMax käyttää autentikaatioon DOCSIS BPI+ mukaista tietoturvaprotokollaa ja PKM-EAP-menetelmää, joka perustuu TLS-standardiin. WiMAX käyttää moniliityntämenetelmää (TDMA), joka vaikeuttaa valetukiasemahyökkäystä ja salakuuntelua.

Vanhassa 2004 standardissa tukiasemia ei autentikoida, joten teoriassa mikä tahansa tukiasema voi esittää olevansa oikea tukiasema. WiMaxin hallintaviestejä ei nykyversioissa salata, joten niitä voidaan helposti salakuunnella. Hyökkääjä voi myös toistaa tallettamiaan salattuja paketteja. Hyökkääjä voi myös saada käyttäjän päätelaitteen jumiin MAC-viestejä modifioimalla.

WiMax-verkoissa tulisi pitäytyä uudemman IEEE 802.16-2005 mukaisissa tuotteissa, joissa käytettävä PKMv2 sisältää molemminpuolisen sertifikaattipohjaisen autentikoinnin. Uusi standardi sisältää myös EAP-pohjaisen autentikoinnin. Koska 2005-versio on taaksepäin yhteensopiva 2004-version kanssa, tulisi 2004-toiminnallisuus kytkeä pois käytöstä!

Bluetooth

Bluetooth on radiostandardi ja kommunikaatioprotokolla (IEEE 802.15.1) langattomille henkilökohtaisille verkoille (PAN), jotka yhdistävät erilaisia, yleensä mobiileja, laitteita toisiinsa. Bluetooth tarjoaa kolme eri tietoturvamoodia: 1) suojaton, 2) palvelukerroksen pakotettu tietoturva ja 3) linkkikerroksen pakotettu tietoturva. Autentikaatioon ja avainten luontiin käytetään SAFER+ -algoritmia. Salaamiseen käytetään E_0-virtasalainta.

Car Whisperer -projekti osoitti, että lukuisissa Bluetooth-laitteissa ympäri maailman on käytössä laitevalmistajan asettamat PIN-koodit (mm. 0000 tai 1234). Mobiilit haittaohjelmat, kuten Cabit, voivat käyttää Bluetooth-verkkoja leviämiseen. Pääuhkat Bluetooth-käyttäjille ovat tietovarkaudet, luvaton käyttö ja laitteiden vahingoittaminen. Eräs merkittävä tietoturva-uhka on kirjava laitevalmistajajoukko ja vanhat huonolaatuiset toteutukset.

Useimmat Bluetoothin tietoturvaongelmat johtuvat ohjelmistotason toteutusvirheistä, joita on paljon etenkin vanhoissa laitteissa. Bluetoothin sovelluskenttä ei yleensä vaadi kovin vahvaa salausta (vrt. hf-korvanappi, keskustelun toinen osapuoli kuultavissa akustisesti). Toisaalta, kannettavat tietokoneet ja älypuhelimet, joissa myös tyypillisesti on Bluetooth, usein sisältävät merkittävää tietoa. Yleensä ottaen Bluetooth on hyvä pitää poissa päältä, ellei se ole käytössä. Samoin on syytä asettaa oma laite tilaan, jossa se ei ole radioteitse löydettävissä (non-discoverable mode). Yleensä ottaen on suositeltavaa noudattaa tietoturvallista lähestymistapaa Bluetooth-laitteiden kanssa.

3G ja 4G

3G:llä tarkoitetaan kolmannen sukupolven matkapuhelinverkkoja. Euroopassa käytetään UMTS-verkkoja. Loppukäyttäjän näkökulmasta ja datapohjaisten palveluiden kannalta UMTS näyttää IP-pohjaiselta verkolta, joten niiltä osin 3G-verkon tietoturva on IP-verkon kaltainen. UMTS ei kuitenkaan ole yhtä avoin kuin Internet. UMTS-verkon tietoturvan takaaminen ja mekanismien luonti on ennen kaikkea laitevalmistajien ja verkko-operaattorien hallussa. Tästä syystä 3G on käytännössä rajattu tässä dokumentissa tarkastelun ulkopuolelle.

3G-laitteet on yhdistettävissä Internetiin, joten ne ovat – käyttöjärjestelmästä riippuen – alttiita erilaisille haittaohjelmille. 3G-kenttä on niin laaja, että tietoturvauhkia on mahdoton käsitellä kattavasti tämän selvityksen piirissä. Huiman kehityksen ja uusien ominaisuuksien myötä päätelaitteet alkavat muistuttaa tietokoneita, jolloin myös tietoturvauhkat ja haavoittuvuudet tulevat vastaavasti tietoverkkoihin kytketyn tietokoneen tietoturvaongelmien kaltaisiksi.

3G-verkkoja reguloi pääsääntöisesti valtiolliset ja kansainväliset organisaatiot. Käyttäjän on hyvä varmistaa, että PIN-kysely on aktivoitu puhelimessa. Operaattoreiden erilaiset rajoitus- ja turvapalvelut on hyvä ottaa käyttöön. Itse puhelimen IMEI-koodi on säilytettävä hyvin ja eri paikassa kuin itse puhelin, puhelimen katoamisen varalta. Puhelimen muisti on syytä varmuuskopioida säännöllisesti tietokoneelle tai erilliselle muistikortille (älä säilytä puhelimessa!). Puhelimeen tuleva soitto tai viesti voi olla tietoturvahyökkäys.

4G:llä tarkoitetaan 3G:tä seuraavaa sukupolvea. Tällä ei tarkoiteta yhtä yksittäistä uutta teknologiaa, vaan useita erilaisia, mutta osittain päällekkäisiä ideoita. 4G on kokoelma erilaisia langattomia teknologioita, jolloin tietoturvauhkat ovat kullekin teknologialle ominaiset ja tietysti osittain samat kuin tämän raportin muiden teknologioiden kohdalla esitetyt. Tämänhetkisten 4G:lle tyypillisten tietoturvauhkien analysointi ei ole tämän selvityksen piirissä mielekästä.

RFID

RFID on tunnistusmetodi, jossa kohteet tunnistetaan niihin kiinnitettyjen RFID-tagien avulla. Näihin voidaan usein myös tallentaa tietoa, joka voidaan noutaa etälukijalla. Tagit voivat olla passiivisia, semiaktiivisia tai aktiivisia. Edulliset RFID-tagit eivät sisällä minkäänlaisia tietoturvaominaisuuksia, sillä niissä ei ole edes peruskryptografiaan kykenevää laskentatehoa. Tageissa voi silti olla staattisia avaimia, PIN-koodeja, joita käytetään esimerkiksi tagin kytkemiseksi pois käytöstä. Kalliimmat tagit kykenevät esimerkiksi symmetriseen kryptografiaan ja haaste–vaste-autentikointiin. Julkisen avaimen kryptografia on käytettävissä todella kalliissa RFID-tageissa, joiden käyttö on kuitenkin vielä vähäistä.

RFID:n kohdalla usein luotetaan lyhyen kantaman tuomaan fyysiseen suojaan, vaikka sopivilla antenneilla voidaan kasvattaa lukuetäisyyttä merkittävästi. RFID:lle ei myöskään ole yleisiä tietoturvastandardeja, vaan jokaisella toteutuksella on tyypillisesti omansa, jolloin kaikilla on myös omat tietoturva-aukkonsa. RFID voi olla myös uhka loppukäyttäjän yksityisyydelle, jos jossakin tuotteessa tuotantoketjun logistiikkaa varten tarkoitettu uniikki RFID-tag jää toimintakykyiseksi tuotteen asiakkaalle luovuttamisen jälkeen.

RFID-tietoturvaratkaisut ovat valmistajakohtaisia. RFID-tageja ja järjestelmiä suunniteltaessa on syytä selvittää valmistajalta erilaiset ratkaisut ja menetelmät, joita järjestelmässä voidaan

käyttää. Tietoturvaa on hyvä kokeilla myös käytännössä. Itse RFID-standardit eivät juurikaan määrittele tietoturvaominaisuuksia. Joissakin tageissa voi olla mahdollisuus lukita muisti etälukijalla estäen tiedon lukemisen ja muuttamisen. Jotkut tagit voidaan kill-komennolla kytkeä pysyvästi pois toiminnasta, mikä pitäisi tehdä kaikille logistiikkaketjun edellyttämille tageille tuotetta asiakkaalle luovutettaessa. Huolimatta näistäkin toiminnoista, lähes poikkeuksetta tagit voidaan tuhota, irrottaa ja vaihtaa tai jopa kopioida. Nämä tosiasiat pitää ottaa huomioon jo järjestelmää suunniteltaessa.

Flash-OFDM

Flash-OFDM on Qualcomm Flarion technologiesin tuote. Se on mobiili WAN-soluverkko-teknologia IP-pohjaisille verkoille. Suomessa 450MHz:n (vanha NMT-taajuus) taajuus on lisensoitu Flash-OFDM-verkon rakentavalle Digita Oy:lle. Verkko tulee palvelemaan erityisesti haja-asutusalueiden asukkaita. Yhteys molempiin suuntiin päätelaitteen ja tukiaseman välissä on salattu.

Flash-OFDM käyttää valmistajan omia tietoturvamekanismeja. Kryptografisten algoritmien yksityiskohdat, protokollat ja fyysisen sekä linkkikerroksen toimintojen spesifikaatiot on saatavissa ainoastaan salassapitosopimuksen solmimisen jälkeen. Tästä syystä niitä ei ole julkisesti analysoitu eikä valitettavasti niin voida tehdä nytkään. Järjestelmän salassapito ei lisää sen turvallisuutta, vaan voi pikemminkin päinvastoin heikentää sitä, sillä muut asian-tuntijat eivät pääse arvioimaan tai analysoimaan järjestelmän turvamekanismeja ja ehdottamaan parannuksia.

Tässä selvityksessä ei ole mahdollista antaa spesifisiä ratkaisuja haavoittuvuuksiin, koska niitä ei tunneta. Flash-OFDM:n spesifikaatioiden saamiseksi pitäisi solmia salassapitosopimus, mikä tarkoittaisi sitä, että analyysin tuloksia ei voitaisi kuitenkaan julkaista. Toisaalta, kaikkiin epävarmoihin tilanteisiin voidaan soveltaa puolustuksen syvyyden lisäämistä eli käytetään VPN-ratkaisuja ja sovelluskerroksen salausta (SSL/TLS).

Yhteenveto

Useimmat langattomat tietoverkot sisältävät tietoturvaominaisuuksia, jotka on syytä ottaa käyttöön. Joskus tämä voi edellyttää uudempien tuotteiden hankkimista, vaikka vanhakin muuten olisi toimintakuntoinen. Samoin useimpien verkkoteknologioiden kohdalla on silti syytä ottaa käyttöön ylemmän kerroksen salaustekniikoita; VPN-tunnelit yrityskäyttäjillä ja SSL/TLS-sovelluskerroksen salaus, jos mahdollista. Loppukäyttäjän on syytä varmistaa lähettäessään yksityistä tietoa Internetin yli, että salaus on päällä.