Luottamus. Tietoturva. Sähköiset palvelut.

LUOTI-julkaisuja 1/2005

Mobiilimaailman tietoturvauhkat ja ratkaisut

Palvelunkehittäjän näkökulma

Luottamus ja tietoturva sähköisissä palveluissa – kehittämisohjelma

Mobiilimaailman tietoturvauhkat ja ratkaisut
Palvelunkehittäjän näkökulma

ISBN 952-201-286-6, 952-201-287-4 (verkkojulkaisu)
LUOTI-julkaisuja 1/2005
Helsinki 2005

Julkaisija

KUVAILULEHTI

Julkaisun päivämäärä

2.6.2005

Tekijät	Julkaisun laji
VTT: Pasi Ahonen, Jarkko Holappa, Kaarina Karppinen, Mikko Rapeli, Anni Sademies, Reijo Savola, Ilkka Uusitalo ja Timo Wiander Oulun yliopisto: Juhani Eronen, Jorma Kajava, Tiina Kaksonen, Kati Karjalainen ja Juha Röning	Raportti
	Toimeksiantaja Liikenne- ja viestintäministeriö

Julkaisun nimi

Mobiilimaailman tietoturvauhkat ja ratkaisut. Palvelunkehittäjän näkökulma.

Tiivistelmä

Tässä selvityksessä kartoitetaan mobiilimaailman tärkeimmät tietoturvauhkat ja niiden ratkaisut palvelunkehittäjien näkökulmasta. Kartoituksen tutkimusmenetelminä olivat yrityshaastattelut, kirjallisuushaut, asiantuntijoiden näkemykset ja laaja-alaiset kommentointikierrokset. Raportti on osa liikenne- ja viestintäministeriön Luottamus ja tietoturva sähköisissä palveluissa (LUOTI) -ohjelmaa, jonka tarkoituksena on monikanavaisten sähköisten palveluiden tietoturvan kehittäminen.

Selvityksen tärkein havainto on, että mobiilipalveluiden tietoturvauhkia on olemassa ja niihin pitää suhtautua vakavasti. Tämä ei kuitenkaan tarkoita, että tietoturvaongelmat olisivat este palvelujen kehittämiselle tai käyttöönotolle. Heti palvelunkehitysprosessin alkuvaiheessa on selvitettävä tärkeimmät palveluun liittyvät tietoturvauhkat ja ratkaistava ne. Hyviä, jo olemassa olevia menetelmiä ja teknisiä ratkaisuja, jotka soveltuvat myös mobiiliympäristöön on jo olemassa. Mobiiliin ympäristöön sovellettuja ohjeistoja, joiden avulla huolehditaan mm. ihmisten toiminnan ja prosessien turvallisuudesta on vähemmän saatavilla.

Tärkeimpiä mobiilipalvelujen kehittäjiä koskevia tietoturvauhkia ovat teknisten toteutusten monimutkaisuus, sisältöjen ja ohjelmien laiton kopiointi, Internetin uhkat, eritasoiset toimijat palvelunkehitysprosessissa ja palvelun käyttäjien ja palvelinten tunnistukseen sekä tietojen luottamuksellisuuteen liittyvät uhkat. Mobiilipalveluihin liittyy myös muita uhkia, mutta niiden merkitys palvelunkehittäjälle riippuu voimakkaasti kulloinkin kehitettävästä palvelusta, joten niistä aiheutuvaa riskiä on vaikea arvioida yleisesti.

Selvityksessä kuvataan erilaisia ratkaisumahdollisuuksia havaittuihin tietoturvauhkiin. Kukin kehitettävä palvelu vaatii kuitenkin tietoturvan erityistarkastelua, koska yleispäteviä ratkaisuja tietoturvaan ei ole olemassa. Palvelunkehitysprosessia käsitellään selvityksessä erikseen, tarkentaen tietoturvan merkitystä prosessin kussakin vaiheessa palvelun ideoinnista palvelun lopetukseen asti.

Avainsanat (asiasanat)

Tietoturva, matkapuhelimet, mobiililaitteet, sähköiset palvelut, palvelunkehitys, tietoturvauhkat

Muut tiedot

Selvityksen katselmointiin ovat osallistuneet Simo Niklander ja Göran Schultz (Oy L M Ericsson Ab), Jari Råman (Lapin yliopisto), Erno Kuusela ja Marko Laakso (Oulun yliopisto), Marko Helenius (Tampereen yliopisto), Heikki Ailisto ja Ritva Poikolainen (VTT).

Sarjan nimi ja numero		ISBN	
LUOTI-julkaisuja 1/2005		952-201-286-6, 952-201-287-4 (verkkojulkaisu)	
Kokonaissivumäärä	Kieli suomi	Hinta	Luottamuksellisuus julkinen
Jakaja Liikenne- ja viestintäministeriö		Kustantaja Liikenne- ja viestintäministeriö	

Utgivare

PRESENTATIONSBLAD

Utgivningsdatum

2.6.2005

Författare	Typ av publikation
VTT: Pasi Ahonen, Jarkko Holappa, Kaarina Karppinen, Mikko Rapeli, Anni Sademies, Reijo Savola, Ilkka Uusitalo och Timo Wiander Uleåborgs Universitet: Juhani Eronen, Jorma Kajava, Tiina Kaksonen, Kati Karjalainen och Juha Röning	Rapport
	Uppdragsgivare Kommunikationsministeriet

Publikation

Hot och lösningar beträffande mobilvärldens informationssäkerhet. Serviceutvecklarens perspektiv.

Referat

I utredningen beskrivs de viktigaste hoten mot informationssäkerheten i mobilvärlden och lösningar på hoten ur serviceutvecklarens perspektiv. Som forskningsmetoder användes företagsintervjuer, litteratursökningar, expertutlåtanden och en omfattande insamling av kommentarer. Rapporten utgör en del av kommunikationsministeriets LUOTI-program (Förtroende och informationssäkerhet i elektroniska tjänster), vars syfte är att utveckla informationssäkerheten i fråga om elektroniska tjänster som fungerar via många olika kanaler.

Utredningens viktigaste observation är att det förekommer hot mot informationssäkerheten gällande de mobila tjänsterna och att hoten bör tas på allvar. Detta betyder dock inte att problemen med informationssäkerheten skulle utgöra ett hinder för att utveckla tjänsterna och ta dem i bruk. Det är viktigt att genast i den inledande utvecklingsfasen identifiera de viktigaste hoten mot tjänstens informationssäkerhet och lösa dem. Det finns redan i dag goda metoder och tekniska lösningar som lämpar sig även för den mobila miljön. Däremot finns det inte speciellt många anvisningar som tillämpats på den mobila miljön i avsikt att sörja för bl.a. den mänskliga verksamhetens och processernas säkerhet.

De viktigaste informationssäkerhetshoten som gäller utvecklarna av mobila tjänster är teknikens komplexitet, illegal kopiering av innehåll och program, Internethot, aktörer på olika nivåer i serviceutvecklingsprocessen och hot som har att göra med identifieringen av tjänstens användare och servrarna samt hot mot uppgifternas konfidentialitet. Det finns även andra hot mot de mobila tjänsterna, men deras betydelse för serviceutvecklaren beror i hög grad på den service som utvecklas, och därför är den risk de medför svår att bedöma på ett allmänt plan.

I utredningen beskrivs olika möjligheter att skydda sig mot de observerade hoten mot informationssäkerheten. En särskild granskning av informationssäkerheten krävs dock för varje tjänst som utvecklas, eftersom det inte finns några allmängiltiga lösningar för att trygga informationssäkerheten. Serviceutvecklingsprocessen behandlas skilt i utredningen med fokus på informationssäkerhetens betydelse i varje skede av processen allt från idéstadiet till dess tjänsten läggs ned.

Nyckelord

Informationssäkerhet, mobiltelefoner, mobilutrustning, elektroniska tjänster, serviceutveckling, hot mot informationssäkerheten

Övriga uppgifter

Raporten har utvärderats av Simo Niklander och Göran Schultz (Oy L M Ericsson Ab), Jari Råman (Laplands Universitet), Erno Kuusela och Marko Laakso (Uleåborgs Universitet), Marko Helenius (Tammerfors Universitet), Heikki Ailisto och Ritva Poikolainen (VTT).

Seriens namn och nummer		ISBN	
LUOTI publikationer 1/2005		952-201-286-6, 952-201-287-4 (nätpublikation)	
Sidoantal	Språk finska	Pris	Sekretessgrad offentlig
Distribution Kommunikationsministeriet		Förlag Kommunikationsministeriet	

The publisher

DESCRIPTION

Date of publication

2.6.2005

Authors	Type of publication
VTT: Pasi Ahonen, Jarkko Holappa, Kaarina Karppinen, Mikko Rapeli, Anni Sademies, Reijo Savola, Ilkka Uusitalo and Timo Wiander University of Oulu: Juhani Eronen, Jorma Kajava, Tiina Kaksonen, Kati Karjalainen and Juha Röning	Report
	Assigned by Ministry of Transport and Communications

Name of the publication

Information security threats and solutions in the mobile world; the service developer's perspective

Abstract

This study examines the major information security threats relating to mobile services and solutions to these threats from the service developer's perspective. Research methods employed include interviews with enterprises, literature searches, expert opinions and extensive rounds of commentary. The report is part of LUOTI, a Development Programme on Trust and Information Security in Electronic Services, which aims to promote information security in new multi-channel electronic services.

The fact that information security threats also concern mobile services and should be given serious consideration is the most important finding of the study. However, this does not mean information security issues would pose an obstacle to the development or introduction of mobile services. All information security issues need to be addressed at the very outset of the service development process. Methods and technological solutions that may also be utilized in mobile services have already been developed. Sets of instructions safeguarding e.g. the security of actions and processes are less readily available.

The major information security threats facing developers of mobile services include the complexity of technological solutions, the illegal copying of content and programs, threats posed by the Internet, the different levels of various players in the service development process, and threats involving the identification of service users and servers and the confidentiality of information. Mobile services also involve other threats; however, since their significance to the service developer greatly depends on the nature of the service under development, it is difficult to assess the risks arising therefrom on a general level.

The study describes alternative solutions to information security threats observed. Nevertheless, information security issues need to be examined individually for each service to be developed, as there are no universal solutions for information security. The service development process is addressed separately in the study and the significance of information security is expanded upon at each stage of the process from idea generation to service termination.

Keywords

Information security, mobile phones, mobile devices, electronic services, service development, information security threats

Miscellaneous

Following persons participated in the survey of this report: Simo Niklander and Göran Schultz (Oy L M Ericsson Ab), Jari Råman (University of Lapland), Erno Kuusela and Marko Laakso (University of Oulu), Marko Helenius (University of Tampere), Heikki Ailisto and Ritva Poikolainen (VTT).

Serial name and number		ISBN	
LUOTI publications 1/2005		952-201-286-6, 952-201-287-4 (www publication)	
Pages, total	Language Finnish	Price	Confidence status Public
Distributed by Ministry of Transport and Communications		Published by Ministry of Transport and Communications	

Esipuhe

Tämä mobiilimaailman tietoturvauhkia ja niiden ratkaisumahdollisuuksia käsittelevä selvitys on toteutettu taustoittamaan liikenne- ja viestintäministeriön Luottamus ja tietoturva sähköisissä palveluissa (LUOTI) -kehittämisohjelmassa tehtävää työtä. Selvitys on laadittu palvelunkehittäjän näkökulmasta.

Selvityksen tavoitteena on lisätä tietoisuutta mobiilipalveluihin liittyvistä tietoturvauhkista sekä niiden ratkaisumahdollisuuksista palvelunkehitysprosessin eri vaiheissa. Selityksessä pyritään myös luomaan näkemyksellisyyttä tietoturvan roolista digitaaliseksi konvergenssiksi kutsutussa tilanteessa, jossa useat digitaaliset palvelut lähestyvät toisiaan ja liittyvät toisiinsa teknisellä tasolla.

Kaikki selvityksessä esitetyt mielipiteet ja johtopäätökset ovat tekijöiden omia, eivätkä edusta liikenne- ja viestintäministeriön virallista kantaa.

Selvityksen ovat toteuttaneet VTT ja Oulun yliopisto VTT:n erikoistutkija Pasi Ahosen projektijohdolla. Selvityksen tutkimusmetodeina on käytetty yrityshaastatteluja, kirjallisuushakuja, asiantuntijoiden näkemyksiä sekä kommentointikierroksia. Työtä ovat ohjanneet ohjelmapäällikkö Kimmo Lehtosalo Eera Finland Oy:stä ja neuvotteleva virkamies Päivi Antikainen liikenne- ja viestintäministeriöstä. Selvitystä ovat matkan varrella ansiokkaasti kommentoineet Juha Perttula liikenne- ja viestintäministeriöstä, Janne Uusilehto Nokia Oyj:stä, Kari Oksanen Nordea Pankki Suomi Oyj:stä sekä Marko Koukka TeliaSonera Finland Oyj:stä.

Liikenne- ja viestintäministeriö kiittää kaikkia niitä, jotka omalla panoksellaan tekivät selvityksen laatimisen mahdolliseksi.

Helsingissä 2. kesäkuuta 2005

Päivi Antikainen
Neuvotteleva virkamies

Tiivistelmä

Viime vuosien kuluessa on syntynyt uudenlaisia sähköisen viestinnän muotoja. Matkapuhelimella tai PDA-laitteella voi käyttää palveluja, joihin on liitetty uusia toiminnallisuuksia, kuten Bluetooth, WLAN, paikannus, musiikki, kamera, videot, jne. Erityisesti datapalveluja, joista on yhteys eri verkkoihin, kuten Internetiin, on saatavilla runsaasti. Tämä kehitys avaa uusia liiketoimintamahdollisuuksia alan suomalaisille yrityksille, mutta aiheuttaa samalla uusia haasteita tietoturvan hoitamiseen.

Tässä liikenne- ja viestintäministeriölle (LVM) maalis–huhtikuun 2005 kuluessa tehdyssä selvityksessä on kartoitettu mobiilimaailman tärkeimpiä tietoturvauhkia ja -ratkaisuja palvelukehittäjän näkökulmasta. Selvitys toimii taustaselvityksenä ministeriön Luottamus ja tietoturva sähköisissä palveluissa (LUOTI) -kehittämisohjelmaan.

Selvityksen tärkein havainto on, että mobiilipalvelujen tietoturvauhkia on olemassa ja niihin pitää suhtautua vakavasti. Tämä ei kuitenkaan tarkoita, että tietoturvaongelmat olisivat este palvelujen kehittämiselle tai käyttöönotolle. Heti palvelunkehitysprosessin alkuvaiheessa on selvitettävä tärkeimmät palveluun liittyvät tietoturvauhkat ja ratkaistava ne. Hyviä, jo olemassa olevia menetelmiä ja teknisiä ratkaisuja, jotka soveltuvat myös mobiiliympäristöön, on jo olemassa. Mobiiliympäristöön sovellettuja ohjeistoja, joiden avulla huolehditaan mm. ihmisten toiminnan ja prosessien turvallisuudesta, on vähemmän saatavilla.

Tässä selvityksessä löydetyt tietoturvauhkat luokiteltiin mobiiliverkon, päätelaitteen, konvergenssin, tunnistuksen ja maksuliikenteen uhkiin sekä palvelun kehitykseen liittyviin uhkiin. Selvityksessä ei käsitellä kaikkia mobiilipalveluja koskevia tietoturvauhkia, vaan keskitytään vain tärkeimpiin palvelunkehittäjiä koskeviin uhkiin. Keskeisimmät mobiilipalvelujen kehittämiseen liittyvät tietoturvauhkat ovat:

- Palvelussa käytettyjen palvelualustojen ja tuotteiden suuri määrä ja monimutkaisuus.
- Palvelusisältöjen ja ohjelmien laiton kopiointi.
- Palvelunkehityksessä mukana olevien toimijoiden tietoturvanhallinnan eritasoisuus.
- Internetin uhkat, kuten palvelunestohyökkäykset, jotka kohdistuvat tulevaisuudessa paljolti myös päätelaitteisiin.
- Käyttäjän ja palvelun tunnistukseen sekä käyttäjän tietojen luottamuksellisuuteen liittyvät uhkat.

Myös seuraavat asiat todettiin selvityksen kuluessa mahdollisiksi uhkiksi:

- Kuluttajien ongelmat palvelujen ja laitteiden asetusten hallinnassa sekä niiden luotettavuuden varmistamisessa.
- Kuluttajien ja palvelunkehittäjien osaamistason puutteet ja alan nopea muuttuminen.
- Uudet teknologiat sekä tuotteiden ja palvelujen uudet käyttötavat, jotka osoittautuvat käytössä tietoturvattomiksi, koska niitä ei ole testattu mobiiliympäristössä.
- Palvelujen luvaton käyttö asiakkaan kustannuksella, mm. tahallinen puhelinlaskun kasvattaminen.
- Haittaohjelmat, kuten virukset ja madot, voivat yleistyä myös mobiililaitteissa.
- Mobiilimaksamisen käytettävyysongelmat ja suurten ostosten turvattomuus.

Selvityksen tehtävänä oli löytää ja kuvata ratkaisut edellä selostettuihin tietoturvauhkiin. Nämä ratkaisut listattiin, taulukoitiin ja jaettiin kolmeen ryhmään: sisällönsuojaukseen, hyökkäyksiltä suojautumiseen ja palvelunkehittäjän tietoturvaprosessiin. Kunkin ratkaisun suhde tietoturvaan ja erilaisiin uhkaluokkiin kirjattiin ylös taulukon muodossa.

Tärkeimpiä *sisällönsuojaukseen* liittyviä teknologisia ratkaisuja ovat:

- median edelleenlevityksen rajoittaminen laittoman kopioinnin estämiseksi ja tallennetun datan salakirjoitus,
- ohjelmien digitaalinen allekirjoittaminen ja kelpoisuuden toteaminen ohjelmien alkuperän ja eheyden varmistamiseksi.

Hyökkäyksiltä suojautumisen tärkeimmät teknologiset ratkaisut liittyvät:

- käyttäjän tunnistukseen ja liittymiseen elektroniseen maksujärjestelmään väärinkäytön estämiseksi,
- käyttäjän yksityisyyden suojaamiseen eri keinoin,
- resurssien suojaamiseen, kuten palvelimien suojaamiseen, hyökkäysten havaitsemiseen, haittaohjelmilta suojautumiseen ja asetusten hallintaan.

Palvelunkehittäjän tietoturvaprosessiin havaittiin liittyvän seuraavia asioita:

- riskienhallinta ja kolmannen osapuolen arviointimenetelmät,
- fyysiset turvaratkaisut sekä vikatilanteista toipuminen ja suunnittelu,

- CERT-toiminta, versionhallintajärjestelmät, tietoturva liiketoiminnan johtamisessa sekä
- teknisen prosessin seuranta, parantaminen ja koulutus.

Kuvattuihin ratkaisuihin on suhtauduttava varauksella, sillä kukin palvelu vaatii tietoturvan erityistarkastelua ja tässä selvityksessä esitetyt ratkaisut ovat vain esimerkkiratkaisuja löydettyihin uhkiin. Alla on kuvattu tarkemmin keskeisimpiä mobiilipalvelujen tietoturvauhkien ratkaisuja.

Monikanavajakelussa *sisällön laittoman edelleenlevittämisen rajoittamiselle* ei ole kaikkien yhteisesti hyväksymiä standardiratkaisuja, joita voisi hyödyntää. Tämä estää tehokasta liiketoimintaa, koska ei ole olemassa ”tehojakelijaa”, joka mahdollistaisi ongelmitta erityyppisten sisältöjen suojauksen eri jakeluverkoissa. Esimerkiksi pelien kopioinnin suojaus on työlästä, koska usein pelit täytyy toteuttaa erikseen jokaiselle mobiililaitteen teknologia-alustalle (erilaiset PDA-laitteet, Java-puhelimet, Symbian-puhelimet, operaattorikohtaiset puhelimet, jne.).

Käyttäjän identiteetin ja yksityisyyden suojaaminen. Verkkoyhteyden kannalta käyttäjän identiteetin ja yksityisyyden suoja ei ole merkittävä ongelma SSL/TLS-salauksen ja PKI:n ansiosta. Tosin aivan halvimmissa matkapuhelimissa suojauksen (SSL/TLS ja PKI) toteuttaminen on vaikeaa kapasiteetin puutteen takia. Palvelinten tunnistamisessa on edelleen ongelmia, jotka liittyvät mm. DNS-palvelinten ja niiden tietoliikenteen luotettavuuteen. Tosin näihinkin ollaan kehittämässä ratkaisuja, kuten DNSSEC. Mobiililaitteeseen voi päästä virus tai jokin muu haittaohjelma, jolla käyttäjän identiteettiä voidaan käyttää väärin. Haittaohjelmia vastaan on kuitenkin olemassa torjuntaohjelmia. Käyttäjän identiteettiä ja yksityisyyttä pitää suojella myös silloin, kun palvelu lopetetaan tai siirretään toiselle alustalle. Tämä voidaan tehdä hävittämällä asiakastietokannat tai käsittelemällä niitä asianmukaisella tavalla siirron aikana.

Palvelimeen kohdistuvilta hyökkäyksiltä, varsinkin turhilla palvelupyynnöillä ylikuormittamiselta, on edelleen vaikea suojautua. Suojautuminen on erityisen vaikeaa, mikäli kyseessä on ennalta suunniteltu, hajautettu palvelunestohyökkäys. Tämän vuoksi tarvitaan entistä parempilaatuisia palvelinohjelmistoja, turvallisempia kehitysprosesseja, osaavia ihmisiä ja hyökkäyksen havaitsemis- ja torjuntajärjestelmiä. Käyttäjille olisi hyvä tiedottaa etukäteen, miten salasanoja tullaan palveluntarjoajan tai operaattorin puolelta käsittelemään. Käyttäjille on tärkeää tiedottaa etukäteen, että tunnuksia ja salasanoja ei saa missään tilanteessa luovuttaa puhelimitse tai sähköpostitse, ei edes kyseisen palveluntarjoajan edustajaksi esittäytyvälle henkilölle.

Helppokäyttöisyys lisää tietoturvaa. Palvelu tulee suunnitella siten, että käyttäjä ymmärtää kaikki toimenpiteet, joita häneltä vaaditaan palvelun käytön aikana. Palveluun sisäänrakennettu intuitiivinen logiikka auttaa käyttäjää huomaamaan, jos jotain poikkeuksellista on tapahtumassa (esim. poikkeuksellinen viive tai epämääräinen palaute). Tällöin käyttäjällä on paremmat mahdollisuudet havaita palveluun kohdistuva hyökkäys tai toimintahäiriö.

Helppokäyttöistä tietoturvaa tulisi integroida kaikkialle tietoverkkoihin, laitteisiin ja koko toimijoiden verkostoon. Teknologisten ratkaisujen tulisi olla sopeutettavissa monenlaisiin liiketoimintaprosesseihin, jolloin niitä voidaan uusiokäyttää, eikä koko järjestelmää tarvitse korvata uudella liiketoiminnan muuttuessa.

Palvelunkehitysprosessi

Tietoturvan huomioiminen palvelunkehitysprosessin eri vaiheissa on tärkeää. Palvelun-kehitysprosessia käsitellään selvityksessä erikseen tarkentaen tietoturvan merkitystä prosessin kussakin vaiheessa palvelun ideoinnista palvelun lopetukseen asti. Selvityksessä kaikille tietoturvaa koskeville teknisille ja prosessityyppisille ratkaisuille esitettiin palvelunkehityksen eri vaiheita koskeva vaikutusalue taulukon muodossa. Useimmat tietoturvauhkat ja niiden ratkaisut vaativat aktiviteetteja useimmissa palvelunkehityksen vaiheissa.

Tietoturvatietoisuuden ja -osaamisen puute on yleinen ongelma palvelunkehityksessä. Tämä johtuu osittain siitä, että todelliset uhkat ovat riippuvaisia kehitettävästä palvelusta. Tietoturvan kokonaisvaltaisen hoitamisen edellytyksenä on, että pystytään ajoissa suuntautumaan juuri kehitettävään palveluun kohdistuviin uhkiin ja ratkaisuihin. On mm. kiinnitettävä huomiota siihen, millaisia suunnittelusääntöjä ohjelmistojen kehittämiseen on sovellettu (ja tullaan soveltamaan), ja miten kehitysympäristön suojauksesta huolehditaan.

Tietoturvan hoitamisessa tulisi olla kyse tuote- ja palvelunkehitysympäristön riskienhallinnasta ja elinkaariajattelusta. On tärkeää ymmärtää, millä ajanjaksolla ja missä vaiheessa riski voi realisoitua. Jotta tietoturva kattaisi palvelukehityksen koko arvoverkon ja sen kaikki vaiheet, on ennen palvelun käyttöönottoa tärkeää selvittää myös alihankkijoiden prosessit sekä testata palvelun laatu ja sitkeys.

Lyhenteet ja terminologia

2G	GSM (Euroopassa).
2,5G	GPRS (Euroopassa).
3G	Matkaviestinnän kolmas sukupolvi (tärkeimpänä UMTS).
3GPP	3rd Generation Partnership Project. Standardointijärjestö.
802.11	IEEE:n standardoima WLAN-standardiperhe, kehittyy edelleen.
A3	Päätelaitteen tunnistusalgoritmi (GSM).
A5	Ilmatien jonosalausalgoritmi (GSM).
A8	Ilmatien salausavaimen luontialgoritmi (GSM).
A-GPS	Assisted Global Positioning System. Verkkoavusteinen GPS-paikannus.
AAC	Advanced Audio Coding. Musiikinpakkausstandardi.
AES	Advanced Encryption Standard. Uusi salausstandardi.
AKA	Authentication and Key Agreement. Protokolla, jonka avulla matkapuhelimen USIM-kortti ja matkapuhelinverkko todentavat toisensa (UMTS).
AMR	Adaptive Multi-Rate. Puheenpakkausstandardi.
ATM	Asynchronous Transfer Mode. Eräs kytkentäverkko.
AuC	Authentication Center (GSM). Matkapuheliverkon solmu, joka hoitaa todentamiseen liittyvät toiminnot.
BG	Border Gateway (GPRS).
BS	Base Station. UMTS:n tukiasema.
BSC	Base Station Controller (GSM). Tukiasemaa ohjaava solmu matkapuhelinverkossa.
BT	Bluetooth. Langaton radioteknologia lyhyille etäisyyksille (10 m).
BTS	Base Transceiver Station. GSM:n tukiasema.
CA	Certification Authority. Varmentajaviranomainen.
CDM	Contract Design Manufacturer.

CERT	Computer Emergency Response Team. CERT-FI on Viestintävirastossa toimiva kansallinen CERT-ryhmä, jonka tehtävänä on tietoturvaloukkausten ennaltaehkäisy, havainnointi, ratkaisu sekä tietoturvauhkista tiedottaminen.
CG	Charging Gateway (GPRS).
CN	Core Network. UMTS:iin liittyvä runkoverkko.
COMP128	Salaisesti GSM:ään kehitetty tunnistusalgoritmi, jota voidaan käyttää päätelaitteen tunnistusalgoritminä ja ilmatien salausavaimen luontialgoritminä.
CPU	Central Processing Unit. Keskusyksikkö.
CRL	Certificate Revocation List. Varmenteiden sulkulista.
CUE	Consistent User Experience.
DB	Database. Tietokanta.
DM	Device Management (OMA). Laitehallintastandardi.
DNS	Domain Name System (UMTS, IP). Nimipalvelin.
DNSSEC	DNS Security Extensions. DNS:n tietoturvalaajennus.
DRM	Digital Rights Management. Sähköisten oikeuksien hallinta. Menetelmä, jolla pyritään kontrolloimaan sähköisen sisällön jakelua.
DSCP	Differentiated Services Code Point.
EAP	Extensible Authentication Protocol. Tunnistusjärjestelmien yhteentoimivuutta edistävä standardi.
EDGE	Enhanced Data GSM Environment (GPRS).
EEPROM	Electrically Erasable Programmable Read Only Memory.
EIR	Equipment Identitty Register (GSM). Mobiililaitteiden IMEI-koodit tallennetaan kansallisella tasolla EIR-laitetunnisterekistereihin.
FTP	File Transfer Protocol. Tiedostonsiirtoprotokolla.
FW	Firewall. Palomuuriohjelmisto tai laitteisto, joka valvoo laitteeseen tulevaa ja siitä lähtevää tietoliikennettä.

GAP	Generic Access Profile (Bluetooth). Määrittelee yleiset toimintatavat, jotka liittyvät Bluetooth-laitteiden hakemiseen ja linkin hallintaan.
GEA	GPRS:n ilmatien salauksen uudempi algoritmi, joka on GSM-verkon A5:n kaltainen.
GGSN	Gateway GPRS Support Node. GPRS-verkon ja ulkoisen verkon (esim. Internet) välinen yhdyskäytävä.
GIS	Geographic Information System. Paikkatietojärjestelmä.
GPRS	General Packet Radio Service. GSM-verkossa toimiva pakettikytkentäinen tiedonsiirtopalvelu.
GPS	Global Positioning System. Satelliittipaikannusjärjestelmä.
GSM	Global System for Mobile communication. Matkapuhelinverkko-standardi.
GSMA	GSM Association.
GTP	GPRS Tunneling Protocol.
H.263	ITU-T:n videopakkausstandardi.
H.264	ITU-T:n ja ISO/IEC MPEG -ryhmän yhteisesti standardoima videopakkaus.
HIP	Host Identity Protocol.
HLR	Home Location Register (GSM). Kotirekisteri.
HST	Henkilön Sähköinen Tunnistaminen. Suomalainen sirupohjainen henkilövarmenne.
HTML	HyperText Markup Language. Hypertekstin merkintäkieli.
HTTP	HyperText Transfer Protocol. Hypertekstin kuljetusprotokolla.
HW	Hardware. Fyysinen laite.
I/O	Input/Output.
ICAO	International Civil Aviation Organization.
ICT	Information and Communications Technology.
ID	Identiteetti.
IDS	Intrusion-detection System. Tunkeutumisen tunnistusjärjestelmä.

IEC	International Electrotechnical Commission.
IEEE	Institute of Electrical and Electronics Engineers.
IKE	Internet Key Exchange. IPSec-tietoturvaprotollien yhteydessä käytettävä avaintenvaihtoprotokolla.
IMAP4	Internet Message Access Protocol version 4. Sähköpostiprotokolla.
IMEI	International Mobile Equipment Identity (GSM). Mobiililaitteen yksilöintitunnus.
IMS	IP Multimedia Subsystem (UMTS).
IMSI	International Mobile Subscriber Identity (GSM). Käyttäjän tunniste SIM-kortilla.
IP	Internet Protocol. Vastaa päätelaitteiden osoitteista ja pakettien reitittämisestä verkossa. IPv4 ja IPv6 ovat IP:n eri versioita.
IPSec	IP security. Kokoelma tietoturvaprotokollia IP:n liittyen.
IRT	Incident Response Team.
ISDN	Integrated Services Digital Network. Piirikytkentäinen digitaalinen puhelinverkkojärjestelmä.
ISIM	IMS Subscriber Identity Module.
ISM	Industrial, scientific, and medical -radiotaajuudet.
ISO	International Organization for Standardization.
IST	EU:n Information Society Technologies -ohjelma.
ITU	International Telecommunications Union.
LAN	Local Area Network. Lähiverkko.
LIG	Lawful Interception Gateway. GPRS-verkon viranomaiskuuntelun mahdollistava solmu.
LUOTI	Luottamus ja tietoturva sähköisissä palveluissa -ohjelma.
LVM	Liikenne- ja viestintäministeriö.
MD5	Message Digest 5. Tiivistealgoritmi, joka tuottaa syötteestä 128-bitin mittaisen tiivisteen. Tiivisteestä ei pysty päättelemään syötettä.
MeT	Mobile electronic Transactions.

MMC	MultiMediaCard. Matkapuhelimissa yleinen muistikortti.
MMS	Multimedia Messaging System. Multimediaviestijärjestelmä.
MP3	MPEG-1 Audio Layer-3. Musiikinpakkausstandardi.
MPEG-4	ISO/IEC Moving Picture Experts Group:n videostandardikokoelma.
MPLS	Multiprotocol Label Switching.
MS	Mobile Station. GSM:n langaton päätelaite.
MSC	Mobile services Switching Center. GSM:n matkapuhelinkeskus.
NAT	Network Address Translation. Yhdessä verkossa tunnetun IP-osoitteen muuttaminen toisessa verkossa tunnetuksi IP-osoitteeksi.
NIST	National Institute of Standards and Technology. USA:n standardiviranomainen.
NNTP	Network News Transfer Protocol. Protokolla uutisartikkeleiden levitykseen, kyselyyn, noutoon ja lähettämiseen luotettavan verkkoyhteyden läpi.
ODM	Original Design Manufacturer. Sopimusvalmistaja.
ODRL	Open Digital Rights Language. Avoin digitaalisten oikeuksien kuvauskieli.
OMA	Open Mobile Alliance. Mobiilitoiminnallisuuksien standardointiorganisaatio.
P-TMSI	Packet-Temporary Mobile Subscriber Identity. Käyttäjän tilapäistunniste GPRS-verkossa.
PAN	Personal Area Network. Lyhyen kantaman lähiverkko, esim. Bluetooth.
PCMCIA	Personal Computer Memory Card International Association.
PDA	Personal Digital Assistant. Esimerkiksi kämmentietokone.
PGP	Pretty Good Privacy. Suosittu sähköpostien salausohjelma.
PIN	Personal Identification Number (GSM). Käyttäjäntunnistuskoodi.
PKI	Public Key Infrastructure. Julkisen avaimen infrastruktuuri.
PLMN	Public Land Mobile Network. Matkapuhelinverkko.

POP3	Post Office Protocol version 3. Sähköpostiprotokolla.
PSTN	Public Switched Telephone Network. Lankapuhelinverkko.
PUK	Personal Unblocking Key (GSM). Avaa lukkiutuneen SIM-kortin.
RA	Registration Authority. Rekisteröijä, joka todentaa varmenteen hakijan henkilöllisyyden varmennepolitiikan mukaisesti.
RAM	Random Access Memory. Luku- ja kirjoitusmuisti.
RAN	Radio Access Network (UMTS). Radioliityntäverkko.
RFID	Radio Frequency Identification. Radiotaajuinen tunnistusteknologia.
RNC	Radio Network Controller (UMTS). Radioverkko-ohjain.
ROM	Read Only Memory.
RPC	Remote Procedure Call. Protokolla, jota käytetään kahden prosessin väliseen tiedonvälitykseen kahden kohdejärjestelmän välillä.
RTP	Real-time Transport Protocol. Protokolla tosiaikaisen datan (ääni, video, musiikki) siirtoon pakettiverkoissa
S/MIME	Secure Multi-Purpose Internet Mail Extensions. Sähköpostin suojaamiseen tarkoitettu protokolla.
SAML	Security Assertion Markup Language. Protokolla käyttäjätietojen välittämiseen.
SANS	SysAdmin Audit Network Security Institute.
SATU	Sähköinen henkilöllisyyden tunnus HST:ssä.
SC	Smart Card. Toimikortti.
SD	Secure Digital.
SGSN	Serving GPRS Support Node. Reitittää datapaketit mobiileilta päätelaitteilta GGSN:lle ja päinvastoin.
SHA	Secure Hash Algorithm. Tiivistealgoritmi, joka tuottaa syötteestä kiinteän mittaisen tiivisteen. Tiivisteestä ei pysty päättelemään syötettä.
SIM	Subscriber Identity Module (GSM). Käyttäjän tunnistamiseen käytettävä toimikortti.

SIMPLE	SIP for Instant Messaging and Presence Leveraging Extensions.
SIP	Session Initiation Protocol. Signalointiprotokolla multimediaistuntojen käynnistämiseen ja lopettamiseen.
SMB	Server Message Block. Microsoftin kehittämä verkkotiedostojärjestelmä.
SMS	Short Message Service (GSM). Tekstiviestipalvelu.
SMTP	Simple Mail Transfer Protocol. Sähköpostiprotokolla.
SSH	Secure Shell. Protokolla etäyhteyksien ja tiedonsiirron suojaamiseksi.
SSID	Service Side Identifier. Tunnus, jonka perusteella kytkeydytään langattoman lähiverkon tukiasemaan.
SSL	Secure Sockets Layer. Tietoliikenteen salausprotokolla.
SW	Software. Ohjelmisto.
SWIM	WIM-moduuli integroituna SIM-korttiin.
SyncML	Synchronization Markup Language. Kieli tietojen synkronointiin laitteiden, tietoverkkojen ja alustojen välillä.
TCP	Transmission Control Protocol. Vastaa kahden päätelaitteen välisestä tiedonsiirtoyhteydestä, pakettien järjestämisestä ja hävinneiden pakettien uudelleenlähetyksestä.
TELNET	Internet-protokolla etäyhteyksiin.
TETRA	Terrestrial Trunked Radio. Ammattikäyttöön tarkoitettu radioverkkostandardi.
TLS	Transport Layer Security. Tietoliikenteen salausprotokolla.
TMSI	Temporary Mobile Subscriber Identity. Tilaajan väliaikainen tunnus, jolla käyttäjän identiteetti suojataan, kun siirretään tätä koskevia tietoja.
UDP	User Datagram Protocol. Vastaa kahden päätelaitteen välisestä tiedonsiirtoyhteydestä. Kevyempi kuin TCP, ei järjestä eikä uudelleenlähetä hävinneitä paketteja.
UE	User Equipment. UMTS-päätelaite.
UMTS	Universal Mobile Telecommunications Service. Kolmannen sukupolven (3G) matkapuhelinteknologia.

USB	Universal Serial Bus. Sarjaväyläarkkitehtuuri oheislaitteiden liittämiseksi laitteeseen.
USIM	User Services Identity Module (UMTS). “SIM-kortti” UMTS:ssä.
VAHTI	Valtionhallinnon tietoturvallisuuden johtoryhmä.
VIRVE	Suomen viranomaisverkko.
VLR	Visitor Location Register (GSM). Vierailijarekisteri.
VoIP	Voice over IP. Puheen välittämistä IP-protokollan avulla dataverkossa.
VPN	Virtual Private Network. Virtuaalinen sisäverkko. Ratkaisu, jolla organisaation sisäverkko voidaan ulottaa turvallisesti turvattoman julkisen verkon, kuten Internetin yli.
Vrk	Väestörekisterikeskus.
WAP	Wireless Application Protocol.
WCDMA	Wideband Code-Division Multiple-Access. Yksi pääteknologia 3G-järjestelmien toteuttamiseksi.
WEP	Wired Equivalent Privacy. Vanhentunut salausjärjestelmä WLAN-verkoissa.
WiFi	Wireless Fidelity. 802.11:n mukainen WLAN.
WIM	WAP Identity Module. Tunnistusmoduuli WAP:ssa.
WLAN	Wireless Local Area Network. Langaton lähiverkko.
WPA	WiFi Protected Access. Salausjärjestelmä WLAN-verkoissa. Kehitettiin korvaamaan WEP:n tietoturva-aukkoja.
WWW	World Wide Web.
X.509	ITU:n suositukset sähköisille varmenteille ja sulkulistoille.
XHTML	Extensible Hypertext Markup Language.
XML	eXtensible Markup Language.

Sisällysluettelo

1. Tutkimuksen taustaa

1.1 Selvityksen tavoitteet

Matkaviestimillä käytetään yhä enemmän palveluja, jotka hyödyntävät yhteyksiä Internet-verkkoon ja siellä oleviin palveluihin. Tämä ja muut digitaaliseen konvergenssiin liittyvät kehityssuuntaukset lisäävät monimutkaisuutta ja mobiilikäyttäjiin ja palveluihin kohdistuvia tietoturvauhkia. Liikenne- ja viestintäministeriössä on nähty tärkeäksi tutkia tätä ongelmakenttää kartoittamalla mobiilimaailman tärkeimmät tietoturvauhkat ja ratkaisut, jotta voitaisiin paremmin keskittyä uusia liiketoimintamahdollisuuksia avaavaan palvelunkehitykseen.

Tämä dokumentti on taustaselvitys liikenne- ja viestintäministeriön LUOTI-ohjelmaan [LUOTI], jonka yksi perusajatus on, että tietoturva on otettava sähköisiin palveluihin mukaan jo niiden kehittämisen alkuvaiheessa. Lisäksi ohjelman tavoitteena on lisätä tietoturvatietoisuutta koko palvelunkehitysverkostossa. Taustaselvitysten yleisiksi tavoitteiksi on annettu:

- Keskitytään sähköisiin palveluihin.
- Käsitellään palvelukehitysprosessin vaiheita.
- Tunnistetaan realistisia tietoturvariskejä ja uhkia.
- Löydetään tunnistettuihin tietoturvauhkiin realistisia ratkaisumahdollisuuksia.
- Luodaan näkemyksellisyyttä monikanavajakeluun liittyvistä tietoturvakysymyksistä: digi-tv, Internet ja mobiiliverkko.
- Selvitetään, kuinka tietoturvan helppokäyttöisyys voitaisiin toteuttaa palvelunkehittäjän toimesta.

1.2 Tietoturva

Tietoturvallisuuden kehittämisen päätavoite on hyvän ja tehokkaan tietojenkäsittelytavan ja asianmukaisen perusturvallisuustason luominen. Sitä tarvitaan laitteisto- ja ohjelmistovikojen, luonnontapahtumien sekä tahallisten, tuottamuksellisten tai tapaturmaisten tekojen aiheuttamilta uhkilta ja vahingoilta. Tietoturvallisuus perustuu tiedon kolmeen eri peruskäsitteeseen:

- *Luottamuksellisuus* – tiedot ovat vain niiden käyttöön oikeutettujen saatavissa, eikä niitä paljasteta tai muutoin saateta sivullisten käyttöön.
- *Eheys* – tiedot ja järjestelmät ovat luotettavia, oikeita ja ajantasaisia, eivätkä ne ole laitteisto- ja ohjelmistovikojen, luonnontapahtumien tai oikeudettoman inhimillisen toiminnan seurauksena muuttuneet tai tuhoutuneet.
- *Saatavuus* – järjestelmien tiedot ja niiden muodostamat palvelut ovat tarvittaessa niihin oikeutettujen käytössä.

Keskeisesti tietoturvan piiriin kuuluvat myös turvafunktiot, joilla tietojenkäsittelyn turvaamisen tehtävät jaetaan seuraavasti:

- väärinkäytösten havaitseminen, ehkäiseminen ja välttäminen,
- korjaustoimenpiteet, elpyminen ja pelotteet.

Turvafunktioiden toteuttamiseksi tietojärjestelmään luodaan kontrolleja: politiikka, menetelmä, käytäntö, laite, tai ohjelmoitu mekanismi.

Määritelmiä:

Tietoturvalla tarkoitetaan hallinnollisia ja teknisiä toimia, joilla varmistetaan se, että tiedot ovat vain niiden käyttöön oikeutettujen saatavilla, ettei tietoja voida muuttaa muiden kuin siihen oikeutettujen toimesta ja että tiedot ja tietojärjestelmät ovat niiden käyttöön oikeutettujen hyödynnettävissä. *(Sähköisen viestinnän tietosuojalaki, 16.6.2004/516).*

Tietoturvallisuudella tarkoitetaan eri muodossa olevien tietojen, palvelujen, järjestelmien ja tietoliikenteen suojaamista niihin kohdistuvien riskien hallitsemiseksi soveltuvilla toimenpiteillä. Tietoturvallisuus on laajempi käsite kuin vain tieto- ja viestintäteknologioiden tekninen turvallisuus. *(Kansalliseen tietoturvallisuusstrategiaan liittyvä yritysten tietoturvatietoisuus-työryhmä [YRTI])*

Tietosuojalla tarkoitetaan henkilön yksityisyyden suojaamista henkilötietojen käsittelyssä. Tätä tarkoitusta varten henkilötiedot on suojattava oikeudettomalta tai henkilöä vahingoittavalta käytöltä. *(Viestintävirasto).*

1.3 Yrityshaastatteluista

Tämän selvityksen valmistelun yhteydessä haastateltiin (maalis–huhtikuu 2005) useita sähköisten palvelujen alueella Suomessa toimivia yrityksiä liitteen A kysymysten pohjalta. Kysymysten tarkoituksena oli toimia pohjana vapaamuotoisemmalle keskustelulle. Tärkein yksittäinen kysymys yrityksille oli: ”Mitä tietoturvauhkia näette sähköiselle liiketoiminnalle mobiilipalveluihin liittyen?”

Haastattelut suoritettiin anonyymisti. Näin tehtiin sen vuoksi, että haastatteluissa pystyttäisiin olemaan mahdollisimman avoimia, mitään ongelmia salaamatta tai peittelemättä.

Yrityshaastatteluiden selvitykseen antamat tärkeimmät suuntaviivat olivat:

- Uhkat kohdistuvat tulevaisuudessa enemmän päätelaitteisiin kuin palveluihin, koska päätelaitteiden suojauksesta ei voida huolehtia niin hyvin kuin verkkojen ja palvelinten. Palveluntarjoajan ja verkko-operaattorin säännelty vastuu ei yksin turvaa päätelaitteita, vaan kuluttaja vastaa viimekädessä itse laitteensa turvallisesta käytöstä. Vastuut tosin riippuvat liiketoimintamallista.
- Palveluiden teknologinen kompleksisuus aiheuttaa suuria ongelmia laadulle ja tietoturvalle, koska tuote- ja palvelukehitysaikaa ei ole tarpeeksi. Tietoturvaa ei useinkaan ole otettu huomioon riittävän varhaisessa vaiheessa.

- Palveluun liittyvien tiedostojen ja ohjelmien oikeudeton kopiointi sekä levittäminen ovat suuria ja vaikeita ongelmia palveluntarjoajan näkökulmasta.
- Monet Internetin uhkat kohdistuvat tulevaisuudessa myös mobiilipalveluihin.
- Uudet toimijat avaavat liiketoiminnallisesti mielenkiintoisia mahdollisuuksia palvelunkehitykselle.

2. Lyhyt teknologiakatsaus

2.1 Lyhyt IP-maailman kuvaus

Internet-protokolliin (IP) pohjautuvat järjestelmäratkaisut ovat olleet vallalla tietoliikenteessä jo 90-luvun alusta lähtien, sillä sen suurimpia etuja ovat laajennettavuus, riippumattomuus fyysisestä verkosta, sekä reititysmallin toimintavarmuus. Internet muodostuu yhteenliitetyistä IP-verkoista ja laitteen liittäminen Internetiin tarkoittaa sen yhdistämistä verkkoon käyttäen tiedonsiirron verkkokerroksena IP-protokollaa. Internetiin liitettävä laite saa IP-osoitteen, jonka ei tarvitse olla globaalisti toimiva, vaan paikallisen verkon osoite. Fyysisenä siirtotienä voi toimia mikä tahansa yhteys, kuten esimerkiksi ISDN, ATM, GPRS tai UMTS. Nykyisin puhutaan usein jo ns. all-IP-verkoista, sillä puhelinverkoissakin siirrytään käyttämään IP-pohjaisia ratkaisuja.

IP-verkoissa tiedonsiirtoon käytetään TCP- tai UDP-protokollia, jotka muodostavat yhdessä muiden protokollien kanssa ns. TCP/IP-protokollaperheen. Näin voidaan rakentaa hyvinkin erilaisia palveluja toteuttavia protokollia. Näihin palveluihin kuuluvat: reititystekniikat, verkonhallinta, verkkopakettien kuljetus, hakemistopalvelut, autentikointi, verkkolaitteiden hallinta, tiedostojen siirto, sähköpostin välitys, WWW-sivujen välitys, äänen ja liikkuvan kuvan välitys, palvelunlaadun hallinta, IP-puhelujen hallinta ja niin edelleen. Nämä protokollat ovat harvemmin palvelujen näkyviä osia, useimmin ne toimivat niiden tukiresursseina.

Käyttäjien näkökulmasta tärkeimmät nykypäivän Internetin palvelut ovat useimmiten WWW-selaus ja kommunikaatiopalvelut kuten sähköposti, uutisryhmät sekä pikaviestintä. Selauksen osuus Internet-palveluista on selvästi ylikorostunut: Selaimilla käsitellään monenlaista passiivista sekä aktiivista sisältöä ja mm. pankki-, kauppa- ja virastopalveluita siirretään verkkoon. Internetin merkitys vain kasvaa tulevaisuudessa yhä useampien toimintojen siirtyessä verkkoon, esimerkiksi verkon välityksellä äänestämisestä on jo tehty pilottiprojekteja. Suosiotaan Internet-palveluina ovat myös lisäämässä IP-puhelut ja erilaiset yksisuuntaiset sekä vuorovaikutteiset video- ja audiopalvelut.

2.1.1 Internet-maailman uhkat

Eduistaan huolimatta TCP/IP-protokollaperhe ei kuitenkaan ole suunnittelultaan kovin sitkeä. Se on suunniteltu mm. kestämään laitevikoja, mutta ei toimimaan verkon sisällä tapahtuvia hyökkäyksiä vastaan. TCP/IP:n suunnitteluvaiheessa ajateltiin, että kaikki verkossa olevat laitteet ovat luotettavissa käsissä, joten turvallisuus jätettiin aluksi pois. Joitakin yleisiä Internet-maailmaan liittyviä uhkia on eritelty seuraavassa taulukossa.

Taulukko 1. Internetin uhkia. Lähteitä mm. [Garfinkel03] ja [wwwfaq].

Syy	Internet-uhka
Käyttäjän turvaton toiminta	Palvelujen **käyttäjätunnus-salasanaparien** arvaaminen esimerkiksi sanakirjoihin perustuvilla menetelmillä.
	Suojaamattomien yhteyksien **salakuuntelu** käyttäjätunnusten, salasanojen tai muiden arkaluontoisten tietojen saamiseksi.
	”S**ocial engineering”-hyökkäykset** arkaluontoisten tietojen selvittämiseksi (esim. salasanojen kysely puhelimitse).
	WWW-selaimissa aktiivinen sisältö ja laajennusohjelmat voivat aiheuttaa kaatumisia, tietomurtoja, virusten tai haittaohjelmien levitystä, soitto-ohjelmia (esim. ulkomainen kallis puhelinnumero) ja yksityisyysrikkomuksia.
Verkon tai järjestelmän puutteet, (myös käyttäjä voi olla osallinen)	**Verkko-osoitteen väärennökset**, jotta päästäisiin käsiksi arkaluontoisiin tietoihin tai vältettäisiin tunnistusmenetelmiä.
	Jotain protokollaa hyödyntävän **yhteyden kaappaaminen** arkaluontoisten tietojen saamista tai murtautumista varten.
	Toisen lähettämän **verkkoliikenteen väärentäminen** esimerkiksi mustamaalaamista tai murtautumista varten.
	Verkko-ohjelmistojen haavoittuvuuksien hyödyntäminen **järjestelmiin murtautumisessa**.
	Palvelunestohyökkäykset, erityisesti useammalla koneella suoritetut hajautetut hyökkäykset.
	Hyökkäykset nimipalvelua kohtaan, esimerkiksi väärien tietojen syöttäminen palvelinten välimuisteihin, kyselijän hukuttaminen virheellisiin vastausviesteihin tai kokonaan vihamieliset nimipalvelimet.
	Resursseja syövä roskaposti, järjestelmien suoranainen tukkiminen suureen määrään käsiteltävää liikennettä, **viestien väärentäminen** tai muut väärennetyt otsikkotiedot ja **haittaohjelmien levittäminen**.

IP-standardeja kehitetään edelleen, mutta valitettavasti tämäkin voi aiheuttaa turvaongelmia. Useita kokeellisia tekniikoita on otettu tuotantokäyttöön ja niitä käytetään tavoilla, joihin niitä ei ole koskaan tarkoitettu. Hajautetut hallinta- ja reititystekniikat voivat toimintavarmuuden kasvattamisen lisäksi siirtää myös vikoja laajemmalle alueelle. Historian painolastina on, että IP-verkko suunniteltiin alussa täysin avonaiseksi.

Sittemmin IP:n riskejä torjumaan kehitettiin useita tekniikoita, joista vallalle jäivät erityisesti palomuurit ja NAT-tekniikat. NAT eli Network Access Translation piilottaa paikallisen verkon siten, että ulkopuolisten silmissä kaikki liikenne näyttää tulevan ja menevän vain yhteen osoitteeseen. NAT lieventää myös IPv4-osoiteavaruuden loppumisen ongelmaa. Muita protokollien puutteiden paikkaamiseen käytettyjä välineitä ovat erilaiset suodattimet, kuten sisältöherkät palomuurit ja roskapostisuodattimet. Tällaisilla tekniikoilla on kuitenkin varjopuolensa, ne rikkovat IP-verkon perusajatusta asettaen esteitä ohjelmisto- ja palvelukehitykselle. Protokollaperheen vikoja paikataan uusissa standardeissa kuten IPv6 ja IPSec, jotka ovatkin jo UMTS-verkoissa käytössä. IPv6 on jo leviämässä voimakkaasti Kiinassa, Japanissa, Etelä-Koreassa ja Taiwanissa.

Internetin tyyppiset uhkat ovat mahdollisia yhä useammin myös mobiilissa maailmassa, joten tietoturvatilanteen kehittymistä pitää koko ajan seurata myös mobiiliverkoissa ja -palveluissa.

2.2 Nykyisistä mobiiliverkoista

Tärkeimmät nykyiset mobiilipalvelut koostuvat seuraavista ryhmistä:

- puhe, tekstiviestit,
- viihdepalvelut (video, musiikki ja ääni, soittoäänet, kuvat, seurustelu, pelit, jne.),
- hyötypalvelut (uutiset, sää, pankkiyhteydet, tapahtumakalenterit, pysäköintimaksut, yrityssovellukset, jne.),
- julkiset palvelut (mm. viranomaistiedottaminen ja -asiointi),
- perinteisen teollisuuden mobiiliratkaisut (etäohjaus, tiedonkeruu, valvonta, jne.).

Katso myös esim. [Alahuhta2005]. Mobiilipuhelinten käyttöikä on nykyisin melko lyhyt. Tämä antaa laitevalmistajille ja palvelukehittäjille oivat mahdollisuudet saada uusia palveluja mahdollistavaa uutta teknologiaa loppuasiakkaiden käyttöön. Mainittakoon esim. värinäytöt, kamerat ja musiikinkuunteluominaisuudet, joita voidaan helposti hyödyntää useammissakin palveluissa tai sovelluksissa. Yhä useammin matkapuhelinta ja PDA-laitetta käytetään ainakin Internet-terminaalina.

Suomessa nykyiset mobiiliverkot sisältävät mm.:

- GSM (äänipuhelut, tekstiviestit, GSM-data)
- GPRS (datapalvelut, sis. EDGE-modulointi)
- TETRA (VIRVE-viranomaisverkko)
- UMTS (äänipuhelut sekä musiikki, kuva, video eli data yleensä)

Esimerkiksi WLAN-verkkoja ei voida ainakaan vielä pitää Suomessa pohjana uusille mobiiliverkoille, mm. hyvin puutteellisen verkkopeiton vuoksi.

2.2.1 GSM- ja GPRS-verkko

GSM-verkko:

GSM-verkko on erittäin hyvin tunnettu verkkotyyppi, koska sitä on implementoitu lähes kaikkialla maailmassa. Näin ollen myös GSM:n tietoturvasta on paljon tietoa, joten sitä ei tyhjentävästi toisteta tässä. Alla kuitenkin GSM:n tärkeimmät tietoturvaan liittyvät komponentit selitettynä hyvin lyhyesti. Yleistä tietoa GSM:stä löytyy esim. [3GPP] ja [GSMA].

Langaton päätelaite on käyttäjän hallussa ja koostuu puhelimesta ja älykortista (SIM). SIM mahdollistaa käyttäjän sähköisen tunnistamisen riippumatta käytettävästä puhelimesta, koska SIM:llä on käyttäjän tunniste IMSI (International Mobile Subscriber Identity). SIM-kortti voidaan suojata PIN- ja PUK-koodeilla. Jos PIN syötetään kolme kertaa väärin, kortti lukittuu ja se voidaan avata ainoastaan PUK-koodilla.

Tukiasema-alijärjestelmä ohjaa radioyhteyttä päätelaitteeseen.

Kytkentäalijärjestelmän pääkomponentti matkapuhelinkeskus MSC huolehtii mm. puhelunvälityksestä. Kotirekisteri HLR sisältää tiedot kaikista tämän GSM-verkon tilaajista, samoin kuin käyttäjän kulloisenkin sijainnin, joka annetaan yleensä sijaintiverkon VLR:n osoitteena. Vierailijarekisteri VLR sisältää tarpeelliset tiedot kaikista GSM-verkossa olevista käyttäjistä, jonka perusteella reititetään puhelut käyttäjälle. Laiterekisteri EIR on tietokanta, johon on saatettu listata verkon kaikki asianmukaiset puhelimet IMEI-koodin perusteella. Todennuskeskus AuC sisältää käyttäjän salaisen avaimen tiedot IMSI-tunnisteen perusteella. Näitä tietoja käytetään käyttäjän tunnistamisessa ja ilmatien salauksessa.

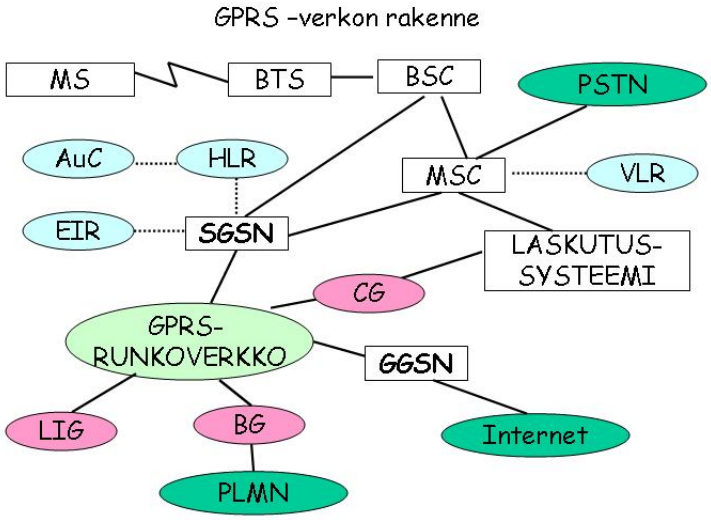
GSM-verkossa on rakenteellisesti useita tietoturvaongelmia. Seuraavalla sivulla on esitetty näistä yleisimpiä [Vesanen].

Taulukko 2. GSM verkon yleisimpiä tietoturvaongelmia (yksinkertaistus), joista muutamia voidaan korjailla jälkikäteen [Vesanen].

Tyyppi	GSM-tietoturvaongelmia
Identiteetti, tunnistus	Käyttäjä ei erota väärää tukiasemaa, joten häntä voidaan periaatteessa huijata käyttämään hyökkääjän valetukiasemaa.
	IMEI-koodin käyttö lisäämään turvallisuutta on ongelmallista (käytännössä useisiin puhelimiin voi olla jäänyt sama IMEI-koodi valmistuksen yhteydessä).
	COMP128-algoritmin heikkous mahdollistaa salaisen avaimen paljastumisen SIM-kortilta hyökkäyksen yhteydessä.
Salaus	Salausavaimet ja tunnistukseen käytettävä data lähetetään salaamattomana verkkojen sisällä ja välillä, jolloin operaattorin tietoturvaan joudutaan luottamaan paljon.
	Ilmatien salauksen heikkoudet. Data salataan ainoastaan tukiasemalle saakka. A5-algoritmi on vahvimmillaankin varsin heikko ja monissa verkoissa käytetään heikennettyä versiota tai ei salata lainkaan.
Eheys	Datan eheyttä ei tarkisteta (ellei tätä ole toteutettu ylemmällä tasolla).
Informaation saatavuus	Näkyvyyden puute: Käyttäjä ei voi nähdä, käytetäänkö salausta. Kotiverkkoon ei tule vahvistusta siitä, käyttääkö palveleva verkko oikein tunnistusparametreja käyttäjän liikkuessa.
Ylläpito	Joustamattomuus. Turvatoimintojen päivityksiä on vaikea toteuttaa, vaikka haavoittuvuuksista tiedettäisiinkin.

GPRS-verkko:

Koska datan siirtäminen ei ole GSM-verkossa tehokasta, on suunniteltu pakettikytkentäinen ratkaisu GPRS, jolla kytkeytyminen pakettikytkentäisiin IP-verkkoihin kuten Internetiin helpottuu ja tiedonsiirtonopeus paranee. GPRS pohjautuu GSM-teknologiaan, joten verkon perusarkkitehtuuri on sama kuin GSM-verkossakin, mutta keskeisimpiä uusia komponentteja ovat SGSN ja GGSN. Puhe kulkee edelleen samaa reittiä kuin GSM-verkossakin, mutta GPRS-data lähetetään SGSN:lle, joka on liitetty GPRS:n runkoverkon kautta GGSN:ään.



Kuva 1. GPRS-verkon rakenne [Vesanen].

SGSN – mm. tunnistaa käyttäjän, pitää yllä sijaintitietoja ja tuottaa laskutusdataa.

GGSN – hoitaa liitynnän ulkoisiin pakettiverkkoihin, kuten Internetiin. BG toimii rajapintana ulkoisiin verkkoihin, loogisesti osa GGSN:ää ja päätarkoituksena on sallia vaeltaminen verkkojen välillä.

CG – kerää laskutusdatan GPRS-verkosta ja ohjaa sen laskutussysteemille.

LIG – esim. tietyltä laitteelta tuleva GPRS-data voidaan oikeuden päätöksellä ohjata arkistoon, jota poliisi sitten voi lukea LIG:n kautta.

GPRS-verkoissa ilmenee paljon uusia uhkia johtuen pakettikytkentäisestä runkoverkosta, joka voi kytkeytyä ulkoisiin pakettiverkkoihin.

Taulukko 3. GPRS-verkon yleisimpiä tietoturvaongelmia.

Tyyppi	**GPRS-tietoturvaongelmia**
GSM-uhkat	**Lähes kaikki samat uhkat kuin GSM verkossa**. Parannuksina ilmatien salaus SGSN:lle saakka ja salauksen uusi algoritmi GEA.
Järjestelmään murtautuminen	Hyökkäys GGNS:ä suojelevaan palomuuriin tai käytettävään NAT:iin.
Internet-roskadata, palvelunesto	Roskadatan lähetys selvittämällä, mihin porttiin laitteita on kommunikoimassa ja IP-pakettien väärentäminen. Ilkeämielinen Internet-palvelin voi lähettää roskapaketteja asiakkaalle tiettyyn TCP- tai UDP-porttiin.

Paketin reititykseen käytettävä GTP-protokolla (GPRS Tunneling Protocol) voi siirtää erilaisia pakettiverkkojen protokollia. Lisäksi GGSN ei välttämättä suodata käyttäjäkerroksen runkoverkon suuntaista liikennettä. Kaikki kytkennät ulkopuolisiin verkkoihin onkin varustettava vähintään palomuureilla.

2.2.2 TETRA

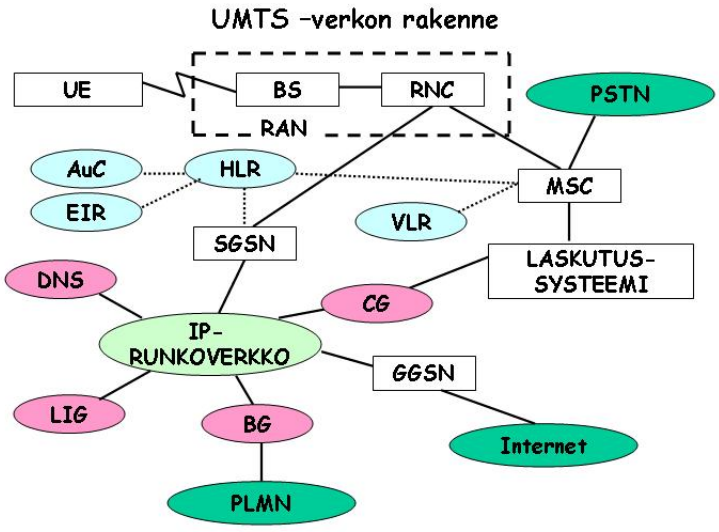
TETRA (Terrestrial Trunked Radio) on ammattikäyttöön tarkoitettu avoin digitaalisen radioverkon standardi, jolla voidaan toteuttaa erilaisten organisaatioiden viestiliikenteessään tarvitsemat erityisominaisuudet, kuten tehokkaat ja nopeat ryhmäpuhelut, puheluiden priorisointi ja hätäpuhelut. TETRA-verkko pystyy välittämään puhetta ja dataa (esimerkiksi lyhytsanomia ja pakettidataa).

TETRA-verkot sopivat vaativaan ammattikäyttöön, kuten viranomaisille, joukkoliikennelaitoksille ja tuotantolaitoksille. TETRAAN perustuvan Suomen viranomaisverkon VIRVE ensisijaisia käyttäjiä ovat valtion ja kuntien turvallisuusviranomaiset. VIRVE-verkosta saa lisätietoja [VIRVE].

2.2.3 UMTS-verkko

UMTS-verkkoja oli vuoden 2005 alussa kaupallisesti saatavissa 33 maassa ja verkkojen lukumäärä oli 64 [3GCO]. UMTS-tilaajia tulee lisää noin 2 miljoonaa kuukaudessa, kokonaismäärän ollessa noin 20 miljoonaa. Voimakkaimmin UMTS-verkkoja on rakennettu Aasiaan, mm. Japaniin, Suomessa UMTS-peitto on vasta suurimpien kaupunkien alueella.

Kuva 2. UMTS-radioverkko (RAN) ja sen liityntä SGSN kautta operaattorin runkoverkkoon sekä liityntä matkapuhelinkeskukseen MSC (yksinkertaistus) [Vesanen].



UMTS-verkon kehittäminen perustuu avoimeen standardointiin, jonka dokumentit on saatavilla 3GPP-yhteistyöjärjestön sivuilta [3GPP]. Tämän 3G-radioverkon käytännön siirtonopeudet ovat muutamia satoja kbit/s, mutta se tarjoaa GPRS-verkon palvelujen lisäksi uusia palveluja: tyypillisiä ovat paikkaan liittyvät, yhtäaikaiset puhelut ja datayhteydet sekä muokattavat palvelut.

Verkon komponentit ovat pääsääntöisesti samankaltaiset kuin GPRS:ssä, mutta 3G:ssä päätelaite on (UE), radioverkko (RAN) ja runkoverkko (CN). SIM:in lisäksi puhutaan nyt USIM:sta, jossa on turvallisemmat algoritmit.

UMTS:n tietoturvan hallinta on rakennettu käytännön syistä GSM-verkon turvamallin päälle, mutta tunnettuja heikkouksia korjaten. UMTS-verkon turva-arkkitehtuuri jakaantuu kolmeen kerrokseen: *sovelluskerros*, *koti/palvelukerros* ja *siirtokerros*. Lisäksi UMTS-turva-ominaisuudet jaetaan luokkiin, ks. ao. taulukko.

Taulukko 4. Yksinkertaistus UMTS:n tietoturvaominaisuuksista. Viides luokka, eli turvallisuuden näkyvyys ja muokattavuus on jätetty pois taulukosta yksinkertaistuksen vuoksi.

Tyyppi	**UMTS-tietoturvaominaisuus**
Verkon pääsyturvallisuus **radiolinkin** tasolla	Tunnistus – sekä verkon että käyttäjän on todennettava toisensa.
	Luottamuksellisuus – sekä signalointidata että käyttäjädata ilmatiellä salataan ja näiden salaukseen käytettävät algoritmit ja avaimet neuvotellaan luottamuksellisesti. Käyttäjän identiteetin ja sijainnin luottamuksellisuus suojataan.
	Signalointidatan eheys – varmistetaan osapuolten välillä neuvoteltavalla algoritmeilla ja avaimilla.
Verkkoturvallisuus – verkon komponenttien signalointidatan turvallisuus	Laitteiden tunnistus – varmistaa, ettei verkkoon voi liittää vihamielisiä komponentteja.
	Verkon signalointidatan luottamuksellisuus ja eheys suojataan.
	Hyökkäystietojen keräysjärjestelmä.
Käyttäjäturvallisuus	USIM:lle pääsyyn vaaditaan käyttäjän tunnistus. Pääsy päätelaitteelle voidaan rajoittaa ainoastaan luvanvaraisille USIM:eille.
Sovellusturvallisuus	USIM:n ja verkon välinen liikenne turvataan, USIM Application Toolkit -palvelut turvataan. Antaa palvelujen tarjoajille mahdollisuuden tuottaa USIM:lla sijaitsevia palveluja, jotka vaativat muokattavissa olevaa salaustasoa.

UMTS-verkoissa on onnistuttu ratkaisemaan useimmat GSM-verkon tietoturvaongelmat. Verkko on kuitenkin altis tietynlaisille palvelunestohyökkäyksille, jotka ovat langattomissa ympäristöissä yleensä erittäin hankalasti kokonaan estettävissä.

2.3 Tulevaisuuden näkymiä

3G on tuomassa laajemman palveluvalikoiman mobiilien päätelaitteiden ulottuville. Lähes rajaton MP3-musiikin kuuntelu ja megapikseliluokan kamerat videonauhoituksineen ja tarkkoine värinäyttöineen ovat jo nykypäivää. Kaavaillut 3G:n hittipalvelut videopuhelut ja -neuvottelut eivät ole ainakaan vielä saaneet laajaa jalansijaa Suomessa. Nokia on kehittämässä digitaalisen konvergenssin hengessä mobiileja massamarkkinapalveluita, kuten television katselu (Mobile TV), ”näköradio” (Visual radio) ja kehittyneet mobiilipelit.

Alla on esitetty yhteenveto keskeisimmistä matkapuhelimissa ja PDA-laitteissa tulevaisuudessa esiin nousevista lähi- tai paikallisverkkoteknologioista. Tiedonsiirtoyhteydet muiden käyttäjien laitteisiin on nimenomaan se tekijä, joka antaa lisäarvoa, mutta samalla aiheuttaa paljon uusia uhkia.

2.3.1 WLAN-yhteydet matkapuhelimissa ja PDA-laitteissa

Langaton lähiverkko (WLAN) voidaan toteuttaa useallakin teknologialla matkapuhelimessa tai PDA-laitteessa, mutta varsinkin matkapuhelimissa tämän toiminnallisuuden toteutus on ollut vielä vähäistä. Aiemmin mm. WLAN:n virrankulutuksen ja muiden teknisten tekijöiden arveltiin olevan ongelma. Kuitenkin tutkimusyhtiö In-Statin [INSTAT] mukaan matka-puhelin-WLAN tilaajien määrä nousee maailmanlaajuisesti yli 256 miljoonaan vuonna 2009, käsittäen noin 12 % kaikista maailman matkapuhelimen käyttäjistä. Tämän vuoksi WLAN-teknologiaa on käsiteltävä hieman tässäkin selvityksessä. WLAN-tekniikoiden nopeus on noussut jo 54 Mbit/s ja valmisteilla on jo yli 100 Mbit/s nopeudella toimiva standardi. Suomessakin on jo tarjolla edullisia WLAN-puhelimia ja markkinoille on tulossa joukko malleja, joissa on yhdistetty WLAN/VoIP sekä GSM samaan puhelimeen [Karila].

IEEE 802.11 on WLAN:n perusstandardi. Verkkotopologia voi olla ad hoc -(tukiasematon) tai infrastruktuuriverkko (vaatii tukiaseman käyttöä). Kukin tukiasema käyttää omaa kanavaa, ts. taajuusaluetta, jotta eri tukiasemien liikenteet eivät haittaisi toisiaan. Tukiasemat kytketään yleensä samaan runkoverkkoon.

WLAN:n kohdistuvia uhkia ovat mm. [Vesanen]:

- salakuuntelu, liikenteen analysointi (voidaan toteuttaa passiivisesti – vaikea havaita),
- siirtomedian häirintä tai katkaisu (WLAN käyttää vapaata taajuusaluetta),
- siirrettävän datan muokkaaminen,
- organisaation järjestelmään tunkeutuminen (WLAN:n kautta).

WLAN-protokollaperhe määrittelee fyysisen ja siirtoyhteyskerroksen toiminnan sekä niissä toimivat todennuspalvelut ja siirtotien suojauksen.

On kuitenkin osoittautunut selvióksi, että WLAN:n perustietoturvamekanismit SSID (Service Set Identifier) eli verkon ID ja vanhahtava WEP (Wired Equivalent Privacy) eivät ole riittäviä. Niinpä WEP-salauksen aukkoja korvaamaan kehitettiin WPA (WiFi Protected Access) -salausstandardi, jonka tietoturva on jo paljon paremmalla tasolla ja tukee monia erilaisia tunnistusmenetelmiä. WPA:n versioista alla:

- **WPA:**ta voidaan käyttää kahdessa muodossa – tunnistus manuaalisesti (jaetulla salaisuudella) tai erillistä palvelinta käyttämällä. WPA käyttää 128-bittisiä salausavaimia ja dynaamisia sessioavaimia.
- Uusi **WPA2** perustuu IEEE 802.11i standardiin ja toteuttaa AES-salausalgoritmin. Tunnistus manuaalisesti (jaetulla salaisuudella) tai erillistä palvelinta käyttäen. Alaspäin yhteensopiva WPA:n kanssa.

Monissa laitteissa on vanhoja WLAN-versioita, jolloin muodostetun WLAN-verkon muutkin laitteet voivat tulla sitä vastaan siirtymällä WEP-salaukseen. Tämän tai mm. päästä-päähän-salaustarpeiden takia WLAN:ssä on useimmiten lisäksi käytettävä samoja tietoturva-mekanismeja kuin Internetissäkin. Näitä ovat mm. IPSec, SSL/TLS ja avaintenhallinta sekä julkisen avaimen infrastruktuuri (PKI), joilla voidaan toteuttaa päästäpäähän-salaus myös mobiililaitteisiin. Esim. SSL/TLS ja PKI onkin jo toteutettu useimmissa kännyköiden WAP- ja WWW-selaimissa ja myös IPSec on vakiona ainakin 3G-puhelimissa (IPv6:n takia).

WLAN:n tietoturvaa (ja sen puutteita) käsitteleviä dokumentteja on paljon, mm. NIST:n “Wireless Network Security 802.11, Bluetooth and Handheld Devices” [NIST800-48].

Mobiililaitteessa käytettävän WLAN-yhteyden suurimmat ongelmat liittyvät kuitenkin käyttäjän epätietoisuuteen mm. seuraavista asioista:

- Mitkä WLAN-verkot ovat turvallisia käyttää? Kuka niitä hallinnoi?
- Mihin verkkoon parhaillaan itse asiassa olen kytkeytymässä tai jo olen kytkeytynyt? Miten varmistun asiasta? Onko verkko suojattu ja miten?
- Millaisia tietoturva-asetuksia minun tulisi käyttää?

Näitä tarpeita tyydyttämään onkin jo olemassa pienikokoisia WLAN-verkkotutkia [Canary], joilla voidaan missä tahansa etsiä WLAN-verkkoja ja yksityiskohtia niiden liikenteestä; kuten signaali (802.11b- ja 802.11g-verkot), signaalivoimakkuus, verkko ID (SSID), salauksen käyttö (WEP ja WPA) ja päällekkäiset verkot.

Lisäksi on määritelty SIM-kortin käyttö WLAN-tunnistukseen (EAP-SIM ja 802.1x), jolla teleoperaattorit voivat tarjota pääsyn WLAN-palveluihin SIM-kortin identiteetin avulla tunnistautumalla [WLANSC]. Teleoperaattorit voivat tarjota ratkaisuja, jotka hyödyntävät esim. USB-muistitikussa olevaa SIM-korttia tai itse puhelimessa olevaa SIM-korttia WLAN-verkkonsa pääsynvalvontaan (WLAN-SIM -rajapinta toteutettu erillisenä SIM-kortin sovelluksena).

Näin voidaan hyödyntää olemassa olevat roaming-, tietoturva- ja laskutusinfrastruktuurit. WLAN Smart Card konsortion standardi EAP-SC kelpaa rajapinnaksi useaan eri tunnistus-tarpeeseen; EAP-TLS (WWW), EAP-SIM (2G, 2,5G) and EAP-AKA (3G).

2.3.2 Bluetoothista ja spontaaneista (ad hoc) verkoista

Spontaanilla verkolla tarkoitetaan langatonta tietoliikenneverkkoa, joka ei tarvitse toimiakseen mitään tukiasemia tai vastaavaa infrastruktuuria, vaan laitteet (kannettavat tieto-koneet, matkapuhelimet, PDA-laitteet, yms.) tunnistavat itse toinen toisensa ja kykenevät muodostamaan verkon keskenään automaattisesti. Spontaanin verkon perusominaisuuksiin kuuluu myös se, että laitteet välittävät dataa toisten laitteiden kautta määränpäähän eli jokainen verkossa oleva laite on tasa-arvoinen ja palvelee muita verkon laitteita reitittimenä. Spontaanien verkkojen käyttö on levinnyt viime vuosina räjähdysmäisesti, ja niiden tulevaisuusnäkymät ovat erittäin suotuisat. Suurimpia etuja ovat verkon helppo ja nopea pystytys sekä käyttö minkälaisessa ympäristössä tahansa.

Spontaaneissa verkoissa on kuitenkin piirteitä, jotka aiheuttavat monia muita verkkoja suuremman tietoturvariskin. Keskitetyn hallinnon puuttuessa pelkästään rajoitetun kirjautumisen järjestäminen voi olla hankalaa. Samoin viestiliikenne oletuksellisesti kulkee minkä tahansa verkon laitteen kautta, jolloin signaaliin kiinnipääsy on helppoa, kuten mahdollisesti myös liikenteen salakuuntelu, reittien muuttaminen tai muu häirintä. Verkko itsessään voi liikkua, ja verkossa olevat laitteet ovat luonnostaan liikkuvia, joten verkon rakenne ja sijainti voi vaihdella lyhyessä ajassa paljon. Tämä asettaa suuria haasteita verkon katkottomalle toimivuudelle ja aiheuttaa sen, että normaalin ja epänormaalin verkkotoiminnan raja hämärtyy. Lisäksi joidenkin verkossa toimivien laitteiden resurssit ovat rajalliset, joten monimutkaisten suojausten toiminta saattaa olla epävarmaa. Osalla laitteista voi olla hyvinkin pieni akkukapasiteetti, jolloin yksi mahdollinen hyökkäys verkon toimintaa vastaan on jo pelkästään turhien viestien lähettäminen verkkoon. Näitä haasteita pyritään tällä hetkellä ratkaisemaan mm. kehittämällä turvallisia reititysprotokollia, soveltuvia tunnistusmenetelmiä ja itsenäistä tapahtumahavainnointia [SAVOLA].

Bluetooth

Monissa älypuhelimissa on jo nykyään Bluetooth (BT), joka on langaton, radiotaajuinen, lyhyen kantaman kommunikointiteknologia. Bluetoothilla muodostettu laiteverkko järjestyy automaattisesti, kun laitteet tuodaan toistensa läheisyyteen (kunhan laitteen Bluetooth-toiminnallisuus on päällä). Käytettävä radiotaajuusalue on vapaa ISM, joka kuitenkin altistaa verkon myös häiriöille. Bluetooth-laitteet muodostavat verkon, joka tapahtuu vaiheittain:

- Valmiustilassa laitteet kuuntelevat toisiinsa tahdistumattomina kyselyitä.
- Joku laite lähettää kyselyn kaikille taajuuksille. Lähistöllä olevat laitteet vastaan-ottavat kyselyn ja vastaavat siihen omalla osoitteellaan ja kellonsa siirtymällä.

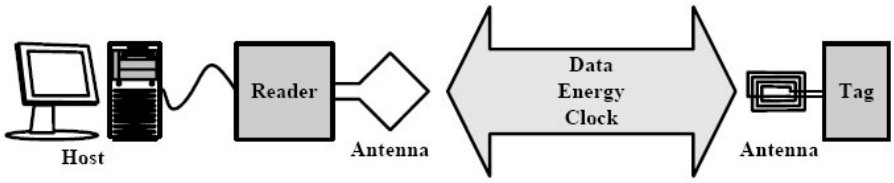
Laite voi olla kuitenkin näkymätön (ei vastaa kyselyihin), mutta näkymättömään laitteeseenkin saadaan yhteys sen yksikäsitteisellä laiteosoitteella.

- Haussa muodostetaan varsinainen yhteys (pikoverkko) isännän ja orjan välillä levittämällä haku-sanoma (sis. kohteen osoite), johon vastaanottaja vastaa, ja vaihtamalla mm. kanavaparametreja, jonka jälkeen laitteet ovat valmiina kommunikoimaan. Isäntä voi liittyä peräkkäisillä hauilla maksimissaan seitsemään orjaan.

GAP (Generic Access Profile) määrittelee yleiset toimintatavat, jotka liittyvät Bluetooth-laitteiden hakemiseen ja linkin hallintaan. Muut profiilit tukeutuvat GAP:iin, joka on tietoturvan kannalta tärkein profiili. Sen mukaan on olemassa kolme turvatilaa: palvelutason turvallisuus, linkkitason turvallisuus ja ei turvallisuutta.

2.3.3 RFID

RFID (Radio Frequency Identification) on halpa radioteknologia, jolla voidaan tunnistaa jokin kohde, kuten kulutustavara. RFID:llä voidaan sähköisesti tunnistaa henkilöitä tai tavaroita nopeasti ilman kontaktia tai näköyhteyttä ja sen käyttö on nopeasti lisääntymässä teollisuudessa.



Kuva 3. RFID:n periaate [ECRFID].

RFID-lukijassa (Reader) on antenni ja lähetinvastaanotin sekä objektissa on (usein passiivinen) RFID-tunniste (microchip Tag), joka ilmoittaa tunniste- ja muut tietonsa lukijalle, kun lukija niitä pyytää. Taajuus 13,56 MHz on alue, jolla tunniste ja lukija yleisimmin signaloivat keskenään, ollen myös kansainvälisesti vapaa taajuus. Tälle taajuudelle on kehitetty kaksi tärkeää RFID-standardia, ISO 14443 ja ISO 15693. Näistä ISO 14443 ei alaluokkineen ja kryptausavaimineen ole valmistajariippumaton ja sen tunnetuin sovellus on Philips Mifare, jota käytetään erilaisissa maksusovelluksissa ja sen lukuetäisyys on rajattu 3–4 senttimetriin. ISO 15693 -standardi on aidosti valmistajariippumaton [VILANT]. Suomessa on RFID:stä tehty paljon esiselvityksiä ja pilotteja sekä mm. RFID-lukija Symbian puhelimeen.

Tärkeimmät halvimpien RFID-järjestelmien tietoturvaongelmat ovat:

- Kommunikointia ei ole salattu tai sen eheyttä tarkastettu. Standardoimatonta salausta käytetään paljon lisenssimaksusäästöjen takia.
- RFID-tunnisteen muisti voidaan lukea, ellei pääsynvalvontaa ole toteutettu. RFID-lukija voidaan jumiuttaa lähistölle tuodulla taajuuslähettimellä.

- Yksityisyys – käyttäjän kulutusprofiili ja paikkatieto on vaarassa levitä väärille osapuolille tulevaisuudessa?

Lisätietoa RFID:n turvallisuudesta on paljon saatavilla, katso esim. [LASEC]. Myös tuore Euroopan komission työasiakirja RFID:n tietosuojasta on löydettävissä [ECRFID], mutta ”RFID-direktiivejä” ei ole vielä olemassa. Soveltajille hyödyllinen on etätunnistus-sovelluksiin keskittyvä sovelluskeskus RFID Lab Finland, joka on avattu kevättalvella 2005 Technopolis Helsinki-Vantaan teknologiakeskukseen [RFIDLAB].

2.3.4 Yhteenveto yleistyvistä matkapuhelinteknologioista

Seuraavassa taulukossa on tiivis yhteenveto joistakin tulossa olevista matkapuhelinten tai PDA-laitteiden teknologioista ja niiden tietoturvasta.

Taulukko 5. Yhteenveto muutamien uusien matkapuhelinteknologioiden tietoturvasta.

Sovellus/ tekniikka	**Teknologia**	**Tietoturva**		
		Uhkat	**Vaikutukset**	**Ratkaisut**
Musiikki ja ääni	MP3, AAC, AACplus, AMR, jne.	kompleksisuus, laiton kopiointi	sisällön tarjonta hidastuu?	uudet standardit, laitteiden kyvykkyyden kasvu
Bluetooth	BT-profiilit, siru-teknologia	käyttäjän ymmärtämättö-myys	turvattomia tai tahattomia yhteyksiä	salaus, asetukset, käyttäjän valveutuneisuus
Paikannus	GPS, A-GPS, solupohjaiset	paikkatieto leviää	yksityisyys rapautuu	asetusten hallinta
Presence	SIMPLE, SIP	läsnätieto leviää	yksityisyys rapautuu	asetusten hallinta
Push-to-talk	RTP, SIP	palvelun hitaus, vahinkosoitot	luottamus palveluun?	palvelun luonteen ymmärtäminen
RFID	RFID lähilukija	yksityisyyden suoja	uusia käyttötilanteita	sovelluskohtainen tietoturva, protokollakehitys
Sähkö-posti	POP3, IMAP4, SMTP	haittaohjelmien leviäminen, roskaposti	laitteen puhtautta ja eheyttä suojeltava	suodattimet, haittaohjelmien torjunta
Video	MPEG-4, H.263, H.264	kompleksisuus, laiton kopiointi	sisällön tarjonta hidastuu?	uudet standardit, laitteiden kyvykkyyden kasvu
WLAN	IEEE 802.11	käyttäjän ymmärtämättö-myys, toteutusten vaihteleva laatu	turvattomia tai tahattomia yhteyksiä	salaus, WPA, SIM, asetukset, käyttäjän valveutuneisuus
VoIP	RTP, SIP	mainospuhelut, salakuuntelu	ajanhukka	salaus, vahva käytt. tunnistus
WWW	XHTML, HTTP	haittaohjelmat, hyökkäykset	suojautumisen ja ylläpidon tarve	SSL/TLS, PKI, torjunta, päivitykset

2.4 Lyhyt digitaalisen konvergenssin kuvaus

Digitaaliseksi konvergenssiksi kutsutaan tilannetta, jossa useat digitaaliset palvelut lähestyvät toisiaan ja liittyvät toisiinsa teknisellä tasolla. Samoja palveluja tarjotaan eri verkkoja käyttäville asiakkaille yhdenmukaistuvaa välitysjärjestelmää pitkin. Tietoturvan kannalta konvergenssin pääongelmana voidaan pitää integroituvien verkkojen erilaista peruslaatua: Internet on avoin ja hallitsematon järjestelmä, kun taas monet siihen liittyvät järjestelmät, kuten televisio- ja (matka)puhelinverkot sekä tuotannonohjausjärjestelmät, ovat olleet keskitetymmin hallinnoituja.

Suljettuihinkin verkkoympäristöihin kohdistuu kuitenkin jo erilaisia paineita. Suuri osa organisaatioista ulkoistaa toimintojaan voimakkaasti, jolloin verkko voi siirtyä toisen tahon hallintaan. Yleisesti verkkoinfrastruktuurit muuttuvat kohti all-IP -ratkaisuja kustannussäästöjen vuoksi, jolloin esimerkiksi puhelinliikennettä voidaan ohjata IP-verkon päällä MPLS-reitityksellä ja muilla vastaavilla tekniikoilla. Verkkojen yhdistyessä kontrolli ja vastuu hallinnasta pirstaloituu.

Yhtenä suljettujen ympäristöjen ongelmana on yleisesti ollut turvallisuusajattelun puutteellisuus. Kun koko verkko on yhden organisaation käsissä, eikä verkossa oleteta olevan vihamielisiä tahoja, syntyy helposti vaikutelma turvallisuudesta. Konvergenssiuhkan tärkeimpinä peruspiirteinä voidaan siis pitää järjestelmien siirtymistä suljetuista verkoista avoimiin ympäristöihin ja siten myös verkkoliikenteen leviämistä uusiin ympäristöihin suunnittelemattomilla ja testaamattomilla tavoilla. Konvergoituneissa järjestelmissä tiedot kulkeutuvat erilaisten verkkoympäristöjen välillä ja virheellinen sanoma voi aiheuttaa joissain verkoissa ongelmia systeemiolettamusten tai vikojen vuoksi.

Internetissä konvergenssin kaltaiset tilanteet eivät ole mitään uutta. Kun verkko alkoi laajeta, siihen liitettiin paljon suljettuja, usein myös yhden käyttäjän järjestelmiä. Eristetyiksi ajateltuihin järjestelmiin päästään nyt verkon kautta käsiksi uusilla tavoilla. Joskus tietoturvan murtamiseen ei tarvittu edes toteutusvirheitä hyödyntäviä hyökkäyksiä tai tunnistusmenetelmien ohittamista – joissakin järjestelmissä ei ollut alkeellisimpiakaan turvamekanismeja. Nykyisin turvallisuus- ja toimintavarmuuskulttuuri on levinnyt ja leviämässä IP-maailman ohjelmistokehitykseen, mutta verkottumisen aikaansaamien haasteiden merkkejä on nähtävissä monissa teknologioissa, joita ollaan liittämässä IP-verkkoon. Nämä teknologiat voivat kärsiä samoista uhkista, jotka ovat Internetissä arkipäivää.

3. Mobiilimaailman tietoturvauhkat

Olemassa olevissa suomalaisissa verkoissa ja päätelaitteissa käytetään GSM-, SMS-, GPRS- ja Bluetooth-teknologioita (ja jopa UMTS jossain määrin). Näiden aiheuttamat uhkat ja ratkaisumallit ovat melko hyvin tunnettuja, mutta vielä uudemmat teknologiat voivat aiheuttaa arvaamattomampia uhkia.

Uusia teknologioita ovat mm. UMTS, mobiiliverkkoihin yhdistetyt IP-pohjaiset yleiset- ja palveluverkot ja niissä tarjottavat palvelut kuten video, audio, digikuvat, push-to-talk, paikannuspalvelut, IP-puhelut, maksupalvelut sekä kontakti- ja tukipalvelut. Lisäksi uhkia tulee uudentyyppisistä verkkoyhteyksistä kuten WLAN ja PAN sekä niiden mahdollisesta vaikutuksesta mobiiliverkkoihin ja niissä tarjottaviin palveluihin. Palvelunkehittäjän näkökulmasta tietoturvauhkat liittyvät mm. seuraavantyyppisiin asioihin:

- toimijoiden ja käyttäjien tietoturvatoiminnan eritasoisuus,
- toimijoiden (henkilöiden) osaamistasojen erot ja alan nopea muuttuminen,
- palveluun tai laitteeseen kohdistuvat hyökkäykset ja virheet, palvelunesto, monimutkaisuus ja väärät asetukset,
- käyttäjän ja palvelun tunnistus ja tietojen luottamuksellisuus,
- palvelusisältöjen ja ohjelmien käyttöoikeudet ja laiton kopiointi,
- uudenlaiset käyttötavat ja teknologiat,
- palvelujen luvaton käyttö,
- haittaohjelmat kuten virukset ja madot,
- mobiili sähköinen maksaminen.

Mobiilipalveluihin kohdistuvat erityyppiset uhkat liittyvät mm. digitaaliseen konvergenssiin. Päätavoitteena on ollut riskien ja uhkien tunnistaminen mobiiliverkoissa, jakelussa, päätelaitteissa, palveluissa, jne. Toisaalta on muistettava, että vielä tänään esim. älypuhelimia ei ole vielä kovin paljon käytössä (niiden kehitys on kesken) ja että tämän hetken mobiiliverkot ovat melko hyvin eristettyjä, joten uhkia ei pidä myöskään liioitella. Maailma muuttuu nopeasti ja uhkien painotus voi pian olla erilainen.

3.1 Yleistä

Mobiilimaailman uhkat voidaan karkeasti jakaa kolmeen osa-alueeseen: mobiiliverkkoihin, mobiililaitteisiin ja mobiililaitteiden käyttäjiin kohdistuvat uhkat. Toki myös palvelujen tuottajiin kohdistuu uhkia, mutta niitä käsitellään jäljempänä.

Mobiiliverkkoihin kohdistuvat uhkat ovat vaikutusalueiltaan laajimmat, mutta useimmiten kuitenkin epätodennäköisimpiä, ainakin radiorajapinnan osalta. Operaattoriverkon uhkaaminen ilmateitse vaatii laitteistoa ja osaamista. Mobiiliverkon kriittisimpien uhkien voidaankin katsoa seuraavan enimmäkseen konvergenssistä. Verkon uhkista on käytettävissä aikaisempaakin tutkimusta, esimerkiksi 3GPP on listannut julkaisussaan ”Security Threats and Requirements” [3GPP] 3G-mobiiliverkon uhkia.

Konvergenssi uhkaa myös mobiililaitteiden tietoturvaa. Päätelaitteiden monipuolistuminen ja monimutkaistuminen lisää uhkia enenevässä määrin. Mobiililaitteisiin kohdistuu jo nyt suuri osa tavallisten tietokoneiden uhista. Samalla käyttäjän harteille on kasattu laitteestaan lisää vastuuta, joka voi olla hankala hahmottaa.

Käyttäjään kohdistuvat uhkat ovat kasvaneet mobiililaitteiden käytön kasvamisen ja monimuotoistumisen myötä. Käyttäjän tarpeet ja luottamus mobiililaitteisiin lisäävät häneen kohdistuvia uhkia. Esimerkiksi mobiililaitteiden käyttö työvälineinä, henkilökohtaisten tietojen säilyttäjänä sekä palveluiden hankintakanavana ovat nostaneet monet Internet-maailmassa tutuiksi tulleet huolet muun muassa varmenteista, salasanoista ja oikeista konfiguraatioista myös mobiilikäyttäjien päänvaivaksi. Käyttäjän on erittäin tärkeä havaita erot laitteen työkäytön ja henkilökohtaisen käytön välillä, johtuen näiden tilanteiden erilaisista tietoturvatarpeista. PC-maailmassahan on jo pitkään tarvittu erillinen laite työkäyttöön tarkoitettujen tietojen suojaamiseksi.

Digitaalisen konvergenssin aiheuttamia uhkia voivat osaltaan pienentää Internet-maailman puolella jo kerätyt kokemukset toteutusten ja verkkojen tietoturvasta. Mikäli nämä opit saadaan hyödynnettyä uusia ohjelmistoja, rajapintoja ja verkkoja luotaessa, säästytään paljolta harmilta.

Tämä selvitys ei esitä kaikenkattavaa listaa uhista, vain keskeisimmät uhkat. Koska tulevaisuuteen ei voi nähdä, kaikkia uhkakuvia ei ole mahdollista listata etukäteen.

3.2 Mobiiliverkon uhkat

Mobiiliverkon uhkista konkreettisin lienee puhelujen tai dataliikenteen sisällön salakuuntelu. Tähän on standardoinnissa tartuttu lähetettävän tiedon salauksella, joka vähentää uhkan merkitystä. Uhka perustuu siis salauksessa käytetyn algoritmin laatuun, mikä on GSM-järjestelmässä jo osoittautunut kyseenalaiseksi [GSMsec]. Joissain tapauksissa GSM-liikenteen kuunteleminen on mahdollista, koska tilaajilla on edelleen vanhoja (COMP128-1 A3/A8-toteutuksena) SIM kortteja, jolloin vahvemmista salausalgoritmi (A5)-varianteista ei ole hyötyä. Kuluttajille suunnatut ohjelmistoradiot ovat tuoneet salakuuntelun tekniset edellytykset harrastelijahintaluokkaan. Potentiaalisena esimerkkinä voidaan pitää teollisuusvakoilua, jolloin uhka koskettaa, tosin ohuesti, myös palvelukehityksen eri vaiheita.

Vielä edellistäkin kriittisempi, mutta myös hypoteettisempi uhka on alkuperäisen mobiililiikenteen muuttaminen, jossa tunkeilija korvaa puhetta tai dataa omalla informaatiollaan.

Mobiililiikenteen analyysi on suhteellisen helposti teknisesti toteutettavissa, mutta se vaatii kuitenkin yhä laitteistoa, asiantuntemusta ja hyvää ajoitusta. Mobiililaitteen ja tukiaseman välistä liikennettä seuraamalla voidaan selvittää valitun kohteen mobiililaitteen paikkaa, nopeutta, liikenteen aikaa, kestoa, kohdetta ja niin edelleen. Uhkaan liittyvät hyötyskenaariot tunkeilijan näkökulmasta ovat kuitenkin rajatut, eniten hyötyä eri tahoille olisi paikkatiedoista ja käyttäjämassoja profiloivista tiedoista.

Mobiililaitteen tai -verkon liikenteen estäminen on hyvin vakava uhka, esimerkiksi hätätilanteissa. Liikenteen estämisellä on myös hyödyllisiä (esim. suojelevia) käyttötarkoituksia ja siihen on kehitetty kaupallisia ratkaisuja. Estämisen aikaansaamiseen vaaditaan jonkin verran resursseja, mutta siinä voidaan nähdä sabotaasin ja kiusanteon lisäksi myös kaupallisia hyötyjä. Todennäköisin liikenteenestouhka verkolle kuitenkin lienee sähkökatkokset ja verkkolaitteisiin kohdistuva ilkivalta.

Mobiiliverkossa käyttäjän täytyy luottaa siihen verkkopalvelutarjoajaan, jonka alueella hänen päätelaitteensa sijaitsee. Tämä asetelma voi olla ongelmallinen erityisesti roaming-tilanteissa, sillä ei voida olettaa, että kaikki operaattorit olisivat täysin luotettavia. Käyttäjä on melko turvaton myös tukiaseman väärennöstä kohtaan.

3.3 Päätelaitteisiin liittyvät uhkat

Mobiileihin päätelaitteisiin liittyy monenlaisia uhkia. Suurin uhka on laitevarkaus, johtuen laitteen pienestä koosta ja liikuteltavuudesta. Laitteita käytetään nykypäivänä paljon myös työasioiden hoitoon, joka luo haasteita tietoturvalle ja laajentaa riskien vaikutusaluetta.

Mobiilipäätelaitteiden käyttäjille ongelmia aiheuttavat myös saastuneet SMS- ja MMS-viestit, roskaposti, WAP-sivut, Internet-sivut ja nopeasti leviävät haittaohjelmat. Uusien matkapuhelinmallien Java-standardien mukaiset ohjelmistot lisäävät myös virusten määrää yleiskäyttöisen ohjelmointikielen ansiosta. Uudeksi uhaksi ovat muodostuneet Internet-maailmasta jo tutut troijan hevoset, näppäinpainallusten tallentajat, keyloggerit, ja Spyware-haittaohjelmat, jotka tutkivat tiedostoja ja lähettävät ne vakoilutarkoituksessa eteenpäin ohjelmassa määriteltyyn osoitteeseen.

Mobiililaitteissa yleisesti käytettävän Java-kielen uhkia voi jakaa itse kielen suunnitteluun liittyviin uhkiin [javafaq] [javavul] [javasec], sekä Java-virtuaalikoneeseen liittyviin uhkiin. Securityfocus.comin arkistoista löytyy 33 Java-haavoittuvuutta yksinomaan hakusanalla virtual machine [secfocus], joten virtuaalikoneet ovat tietoturvavirheille alttiita samalla tavoin kuin kaikki muutkin ohjelmistot. Uhkia liittyy myös Javan native interfacen käyttöön, jolloin osa koodista onkin tehty alhaisen tason ohjelmointikielellä, johon liittyy enemmän uhkia kuin

itse Javaan. Sulautetuista laitteista osa kääntää Javaa natiivikoodiksi, kun taas toiset suorittavat suoraan Javan bytekoodia, ja tällä on vastaavasti vaikutusta ohjelmistoihin liittyviin uhkakuviin. Kuitenkaan edellä mainittujen uhkien vaikutusalue ei ole erityisen laaja.

Bluetoothin turvallisuudesta on puhuttu jo pitkään ja sen on todettu olevan ainakin vanhemmissa toteutuksissa puutteellinen. Bluesnarfing-hyökkäyksessä hyökkääjä voi esimerkiksi lukea hyökkäyksen kohteena olevasta kännykästä kalenteri- ja muistiotietoja, soittaa haluamaansa numeroon tai lähettää SMS-viestejä käyttäjän laskuun. Pääasiassa ongelmat kuitenkin johtuvat Bluetooth-spesifikaation huolimattomasta toteutuksesta ja ohjelmiston tuotantoon liittyvistä virheistä. WLAN:iin ja Bluetooth:iin liittyvät uhkat ovat hyvin paljon samantyyppisiä.

Laitteiden yhteensopimattomuus aiheuttaa myös omat uhkansa. Palvelunkehittäjäosapuolten kannalta tilanne on liiketoiminnan kannalta ikävä – heidän luomansa koodi tulee toimimaan vain tietyssä osassa puhelimia ja saavuttamaan vain osan käyttäjistä. Eri puhelinmalleille julkaistaviin versioihin ei tällöin tule löytymään kovinkaan paljon resursseja, mikä tulee näkymään toteutusten laadussa ja siten myös tietoturvassa.

Muita uhkia puhelimissa ovat mm. ohjelmistoversioiden suuri määrä, ohjelmien heikko ylläpitäminen (esim. virusohjelmien päivitys ja tietojen varmuuskopiointi) ja uusien puhelinkäyttöjärjestelmien avoin ohjelmointirajapinta, joka lisää uhkia. Palvelunkehittäjä voi vaikuttaa päätelaitteisiin kohdistuviin uhkiin parantamalla oman palvelunsa toimintavarmuutta.

RFID-tekniikoiden käyttöä mobiilipalveluihin liittyen on pilotoitu. Turvallisuutensa puolesta tekniikka on kuitenkin epävarmalla pohjalla ja kaipaa kehitystä ja uudelleenarviointia. Tärkeiden tietojen säilyttämistä RFID-tunnisteissa tulisi välttää, vaikka niiden käyttöä on suunniteltukin, mm. passeissa.

Päätelaitteiden tietoturvasta on kirjoitettu muun muassa FiCom ry:n artikkelissa ”Katsaus mobiilitietoturvaan” [FICOM].

3.4 Digitaaliseen konvergenssiin liittyvät uhkat

Digitaalisen konvergenssin myötä laitteen monimutkaisuus ja rajapintojen lukumäärä kasvaa, jolloin järjestelmäkokonaisuuden hallinnan tarve lisääntyy. Mobiililaitteiden suojausohjelmien tehokkuus ja yhteensopivuus on vielä puutteellista ja tietoturvan kokonaistilanteen hahmottaminen tärkeää. Voidaankin ajatella, että mobiililaitetta alkavat koskea samat lainalaisuudet kuin tietokoneita yleensäkin. Ei voida olettaa, että päätelaitteille tulevat syötteet ovat hyvin muodostettuja, oikeanlaisia ja harmittomia. Ohjelmiston toimintavarmuus muuttuu entistä kriittisemmäksi tekijäksi, samoin kuin sen kyky suodattaa ympäristöstä saatavaa dataa.

Erilaisten ryhmälevitystekniikoiden käyttäminen tulevien palvelujen tuottamisessa lisää myös palvelujen uhkakuvia, esimerkiksi palvelunestoon ja lähteen varmennukseen liittyen.

Mobiililaitteet ovat varmasti haluttuja kohteita Internetistä lähtöisin oleville hyökkäyksille siinä missä muutkin verkon järjestelmät. Eräs konvergenssin päätelaitteisiin luoma uhka onkin verkon kautta suoritettavat hyökkäykset mobiililaitteen ohjelmistoja vastaan. Näiden hyökkäysten onnistuessa toteutuvat päätelaiteuhkien lisäksi erilaiset Internet- ja maksupalveluihin liittyvät uhkat, yleisemmällä tasolla Internet-laitteisiin liittyvät uhkat.

Samalla tavoin operaattoriverkko alkaa saada enemmän avoimen Internet-verkon piirteitä, vertautuen ehkä lähinnä yrityksen sisäverkoksi, jonka täytyy tarkoin hyväksyä vain halutunkaltainen liikenne. Operaattoriverkot perivät tällöin myös Internet-verkkojen uhkia. Niiden palvelimia uhkaa epäkelpo ja pahantahtoinen verkkoliikenne niin Internetin kuin mobiilikäyttäjienkin taholta.

3.5 Tunnistukseen liittyvät uhkat

Tunnistukseen liittyvät uhkat jakautuvat karkeasti ottaen kahteen kategoriaan. Yleisesti tunnistukseksi ajatellaan verkon suorittama käyttäjän ja mobiililaitteen tunnistus, mutta toisaalta myös käyttäjän ja mobiililaitteen tulisi tunnistaa verkko halutuksi. Tällä tavoin käyttäjä voi suojautua huijaushyökkäyksiltä. Palveluntarjoajien uhkista tärkeimpiä ovat kopioidut tai muutoin laittomasti haltuun otetut mobiililaitteet.

Tunnistukseen käytetään kryptografista todennusta, jonka vahvuus riippuu valitun kryptografisen algoritmin valinnasta. Huono algoritmi aiheuttaa uhan, koska se voi mahdollistaa SIM-kortille säilötyn salaisuuden paljastumisen, kopioinnin ja esimerkiksi mobiili- ja mobiilivarmennettujen palveluiden käytön ilman SIM-korttia. Hyökkäys voidaan toteuttaa esimerkiksi puhelimen varastamisen tai katoamisen yhteydessä erittäin nopeasti. Ilmateitse uhka lienee epätodennäköinen, sillä se vaatii tarvittavat laitteistot palveluntarjoajaksi tekeytymistä varten ja pidemmän aikavälin. Tälläkin hetkellä laajalti todennuksessa käytettävässä Comp-128-1-algoritmissä uhka on todellinen [comp128] ja osoitettu jo vuonna 1998. Sen sijalle kehitettyjen algoritmien vahvuus on tällä hetkellä epäselvä.

Algoritmin heikkouden lisäksi tunnistamisen uhkana ovat erilaiset *man in the middle*-hyökkäykset, missä käyttäjän aloittama istunto kaapataan vihamieliseen käyttöön. Internet-maailmassa tällaiset hyökkäykset ovat arkipäivää, mobiilimaailman radiorajapinnassa niiden toteutus on hankalampaa.

Tunnistuksessa käyttäjän osa on heikoin. Paitsi teknisille uhille, käyttäjät ovat alttiita konkreettisemmille uhille, kuten erilaisille huijauksille ja muille social engineering-hyökkäyksille, laitteen anastamiseen ja muilla keinoin tapahtuvaan käyttäjäksi tekeytymiseen.

Tärkeä uhka tulee kahden em. yhdistelmästä, esim. huijausohjelma saadaan ensin syötettyä käyttäjän puhelimeen, myöhemmin käyttäjälle soitetaan ylläpitäjäksi tekeytyen ja annetaan epäilyttäviä ohjeita ”vian korjaamiseksi”. Viranomaisten ja palveluntarjoajien roolit ovat tärkeitä tietoturvan perusteiden opastamisessa ja hyvän tietoturvakulttuurin kannustajina.

3.6 Maksuliikenteen uhkat

Maksuliikenne on toteutuksellisesti lähellä tunnistamista, täytyyhän maksaja ja maksun saaja tunnistaa tapahtuman mahdollistamiseksi. Osa tunnistuksen uhkista soveltuukin maksuliikenteeseen. Lisäuhkia maksuliikenteeseen palveluntarjoajan kannalta tuo maksutapahtumien kiistämättömyyden tutkinta, joka voi olla vaivalloista, pitkällistä ja tuoda tulonmenetyksiä. On syytä määritellä ja tiedottaa etukäteen millä tavoin palvelun käyttäjä on vastuussa niistä kuluista, joita rikollinen toiminta, kuten mobiililaitteen varastaminen tai huijaaminen, voivat palvelun käytön kautta aiheuttaa. Käyttäjän velvollisuus on olla tietoinen siitä kuka hänen laitettaan käyttää ja millä tavoin, sekä ilmoittaa vastuullisille tahoille mikäli laite ei ole hänen hallinnassaan.

Digitaalinen konvergenssi tuo mobiililaitteiden käyttäjien uhiksi myös erilaiset Internetistä tutut phishing-hyökkäykset, joissa käyttäjää yritetään huijata käyttämään oikeannäköistä, mutta väärennettyä maksupalvelusivustoa. Yhtä lailla, niin palvelun kehittäjän kuin käyttäjänkin kannalta yksi tärkeimmistä uhkista on luottamuksellisten tietojen, kuten tiliotteiden tai luottokorttitietojen, vuotaminen. Maksuliikenteen palvelimille kohdistuu näin ollen vastaavankaltaisia uhkia kuin tärkeitä Internet-palvelimia kohtaan. Samalla tavalla luottamuksellisia tietoja käsittelevien ja ehkä säilyttävien päätelaitteiden uhkia voi verrata Internet-päätelaitteiden vastaaviin.

3.7 Palvelun kehitykseen liittyvät uhkat

Sisällöntuotannon näkökulmasta peliteollisuuden tärkein uhka on piratismi. Sähköinen sisällönsuojaus on nuorta, eikä siihen ole nähtävissä yhtä oikeaa tai erityisen hyvää ratkaisua. Sisällön suojaukseen liittyvät kysymykset jopa rajoittavat ja estävät tiettyjen palveluiden tarjonnan. DRM:ään (Digital Rights Management) itseensä liittyy joskus uhkia varmenneketjujen epämääräisyyden yms. muodossa, mutta luotettu alusta minimoisi yleisesti uhkia.

Uhkia ja ongelmia voi liittyä järjestelmien ja palveluiden kehityksen jokaiseen vaiheeseen. Konseptivaiheeseen liittyviä riskejä ovat esimerkiksi tilanteet, joissa käytetään teknistä ratkaisua, vaikka riskit ovat liian suuret, tai vaihtoehtoisesti jätetään hyödyntämättä automaation mukanaan tuomia etuja. Vaatimusmäärittely ja järjestelmäsuunnittelu ovat niin ikään keskeisiä vaiheita. Toteutukseen voi liittyä lukuisia ongelmakohtia, joita ovat mm. ohjelmointivirheet ja vääränlaiset kytkökset osien välillä. Myös tukijärjestelmät muodostavat omia uhkiaan, jotka liittyvät esimerkiksi heikkoihin ohjelmointikieliin ja huonoihin kehitys-

työkaluihin; niihin voidaan luottaa liikaa. Järjestelmäsuunnittelun analyysiin liittyviä ongelmia ovat väärät oletukset järjestelmän ympäristöstä ja ihmisten käyttäytymisestä sekä vialliset mallit ja simulaatiot. Toteutuksen analyysiin liittyvät mahdollisuudet vääränlaiseen testaukseen ja virheisiin ohjelmiston debuggauksessa. Kehitykseen liittyviä yleisiä ongelmia ovat osaajien puute (mm. hitaat uusien ylläpitotapojen omaksumiskeinot), kiire, sekä puutteellinen dokumentointi.

Tietoturvan taso monesti muuttuu päivitysten tai komponenttien liittämisen yhteydessä. Myös järjestelmien käytöstä poistamiseen liittyy uhkia, kuten tarpeellisten osien liian aikainen alasajo tai piilossa oleva riippuvuus vanhasta versiosta, jota ei olekaan enää olemassa. (Neumann 1995: 8). Kehittäjien tietoturvatietoisuuden puute on suuri uhka. Muita ongelmia voivat olla toimijan lyhytaikainen toiminta, resursointiongelmat tai turvaton palvelunkehitysprosessi.

4. Ratkaisut tietoturvauhkiin

Tärkeimmät ratkaisut ja arkkitehtuurit edellä mainittuihin palvelunkehittäjän tietoturvauhkiin kuvataan tässä luvussa. Vain tärkeimpiä suuntaviivoja kirjattiin ylös, sillä täydellisiä, pysyviä ratkaisuja tietoturvaan ei ole olemassa.

Tietoturvasta huolehtiminen asettaa monenlaisia vaatimuksia verkoille, palvelimille, laitteille, ohjelmistoille, järjestelmille ja menettelyille. Näiden kaikkien yhtäaikainen käsittely ja täydellinen hallinta on hankalaa ja sovellusalueesta riippuvaa, joskus jopa mahdotonta. Tämä tarkoittaa, että toiminnan järjestämiseksi riskejä täytyy tunnistaa, hallita ja minimoida kulloisessakin tilanteessa. Riskianalyysi on ehkä tärkein yksittäinen menetelmä, jolla tietoturvaa voidaan selkeästi parantaa. Riskiä ei yleensä voida kokonaan välttää, ellei kyseisistä toimista pidättäydytä kokonaan. Vastaavasti riskiä voidaan pienentää vaikuttamalla siihen, että riski toteutuisi mahdollisimman harvoin ja toteutumisen seuraukset olisivat minimoidut. Riskiä voidaan myös siirtää toiselle taholle sopimusteitse. Tyypillisiä sopimuksia ovat mm. kuljetus- ja alihankintasopimukset.

Osa riskeistä on sellaisia, että ne joudutaan tai kannattaa pitää omalla vastuulla. Tällaisia ovat esimerkiksi sähköisessä liiketoiminnassa tarpeellisten Internetiin kytkettyjen palvelimien muodostamat riskit. Esimerkiksi tietoturvaohjelmiston toimittaja ei korvaa välillisiä vahinkoja, jos tuote ei huomaa virusta tai uhkaa. Riskienhallintaa on myös varautuminen etukäteen, suunnitella miten edetään kun palvelinta vastaan on hyökätty ja miten vahingosta toivutaan mahdollisimman nopeasti ja pienin vaikutusaluein.

Uudet ja yhdistelmätyyppiset tekniset ratkaisut muodostavat erittäin moninaisen kirjon mm. Internetin käytön yhdistyessä mobiiliverkon käyttöön. Tämä aiheuttaa monimutkaisuutta ja ongelmallisuutta palvelunkehittäjien ratkaisuvalintoihin (esim. teknologia-alustojen valinnassa).

Palvelunkehittäjän tärkeimmät tietoturvaa koskevat ratkaisut eri uhkaluokkiin on yhdistetty toisiinsa taulukossa 6.

Taulukko 6. Tietoturvaratkaisujen suhde kohteisiin (uhkaluokkiin) ja tietoturvamääritelmiin.

	Teknologia/Prosessi	Kohde (luvun 3. luokittelun mukaan)							Tietoturva (kohdan 1.2 määritelmien mukaan)						
									Turvafunktiot				Turvakäsite		
		Palvelukehityksen uhkat	Maksuliikenteen uhkat	Tunnistuksen uhkat	Konvergenssin uhkat	Päätelaitteen uhkat	Mobiiliverkon uhkat		Korjaus	Suojaus	Havainnointi		Saatavuus	Eheys	Luottamuksellisuus
Sisällönsuojaus palvelussa	Median edelleen levityksen rajoittaminen	X		X	X	X	X			X	X		X	X	X
	Tallennetun datan salakirjoitus	X	X		X	X				X			X		X
	Ohjelmien digitaalinen allekirjoittaminen ja verifiointi	X		X		X				X	X		X	X	
Hyökkäyksiltä suojautuminen palvelussa	Liityntä elektroniseen maksujärjestelmään	X	X	X	X	X				X	X		X	X	X
	Yksityisyyden suojaaminen	X	X	X	X	X	X			X	X			X	X
	Palvelimien suojaaminen	X	X		X		X		X	X	X		X	X	X
	Hyökkäysten havaitseminen	X	X		X	X	X			X	X		X	X	
	Haittaohjelmilta suojautuminen	X	X	X	X	X	X		X	X	X		X	X	X
Palvelunkehittäjän tietoturvaprosessi	Kolmannen osapuolen arviointimenetelmät	X	X			X			X		X		X	X	X
	Riskienhallinta	X	X	X	X	X	X		X	X	X		X	X	X
	Fyysiset turvaratkaisut, esim. varmuuskopiointi, tamper-resistant HW	X		X		X			X	X	X		X	X	X
	Vikatilanteista toipuminen, suunn.	X	X		X		X		X		X		X		
	CERT-toiminta	X			X	X			X	X	X		X	X	X
	Versionhallintajärj.	X							X	X	X		X	X	X
	Tietoturva liiketoiminnan johtamisessa	X							X	X	X		X	X	X
	Tekn. prosessin seur. parant. ja koulutus	X							X	X	X		X	X	X

Edellä olevaan taulukkoon on suhtauduttava tietyin varauksin, sillä tietoturvaan liittyvät ratkaisut on räätälöitävä kunkin sovellusalueen mukaan. Esimerkiksi *videoleikkeiden* jakelussa tulee teknisin ratkaisuin ja prosessein varmistaa:

- kapasiteetiltaan sopivien päätelaitteiden tunnistus ja tiedottaminen,
- palvelun saatavuuden varmistaminen, palvelinkapasiteetti, yhteyden kaistanleveys (esim. DSCP), muistinkäyttö, hyökkäyksentorjunta, ym.,
- MPEG-4- ja audiokoodekkien ja levitystiedostojen yhteensopivuus,
- kaksisuuntainen tunnistus, maksutapojen integrointi, ym.,
- salaus,
- helppokäyttöisyys,
- edelleenlevityksen rajoitukset (esim. DRM), tekijänoikeudet, lähioikeudet.

Edelleen voidaan todeta, että *mobiilipeleissä* ratkaisut sisältävät samoja elementtejä kuin videon ja musiikin jakelu, mutta erityishuomiota vaativat esim. digitaalinen allekirjoittaminen, haittaohjelmilta suojautuminen, ryhmäpelit ja niihin liittyvät tekniset ratkaisut, kuten ryhmäpelaamisen maksaminen. Päätelaitteissa myös grafiikkaan liittyvät HW- ja SW-moduulit vaativat tietoturvan erityistarkastelua, jotta dataa ei pääse ”vuotamaan” moduulista ulos.

4.1 Riskienhallinta

4.1.1 Teknologiariippuvuuden hallinta

Tietoinfrastruktuurin heikkoudet ovat tehneet yhteiskunnasta uudella tavalla haavoittuvaisen. Tietoverkkoympäristöt ovat nyt monimutkaisempia kuin koskaan aiemmin ja niiden kompleksisuus tulee nykyisestä tilanteesta vain kasvamaan. Eräs tärkeä monimutkaistumiseen vaikuttava tekijä on erilaisten tietoverkkojen yhdistyminen, lisäksi sovellustason ymmärrys verkoissa on välttämätöntä käytettävyyden varmistamiseksi. Niinpä verkkokokonaisuuden ymmärtäminen voi jäädä vajavaiseksi, mikä itse verkonhallinnan vaikeutumisen lisäksi hankaloittaa muun muassa riskienhallintaa ja haavoittuvuusanalyysiä. Riskienhallinta-päätökset edellyttävät teknologiariippuvuuden hahmottamista ja tähän voidaan hyödyntää protokollalähtöistä tarkastelua.

Laajastakin näkökulmasta katsottuna kokonaiskuvan epäselvyys on huomattava puute protokollaympäristöjen tutkimisessa. Yksittäisten protokollaperheiden hahmottamista on kyllä tutkittu, mutta eri protokollia ei voi käsitellä toisistaan eristettyinä yksittäistapauksina. Nämä eri protokollat kuitenkin esiintyvät samoissa verkoissa ja sisältävät standardointiprosessin tuloksena usein samoja tai toisiinsa vaikuttavia aliprotokollia tai rakenteita. Näin protokollien välillä esiintyy riippuvuuksia ja yhteyksiä, jotka ovat usein piileviä.

Näiden yhteyksien hahmottaminen on kuitenkin ensiarvoisen tärkeää muun muassa haavoittuvuusanalyysin, haavoittuvaisuusprosessin koordinoinnin ja infrastruktuurin riskienhallinnan kannalta. Yksittäinen haavoittuvaisuus voi protokollariippuvuuden kautta uhata verkkoa tavoilla, jotka eivät löydy normaalilla haavoittuvaisuusanalyysillä.

Oulun yliopistossa Tietoturvallisen ohjelmoinnin tutkimusryhmässä on kehitetty visuaalinen ratkaisumalli teknologia- ja protokollariippuvuuksien hahmottamiseen. Mallin mukaan protokollista kerätään niiden teknisiin ominaisuuksiin ja levinneisyyteen liittyvää tietoa. Myös tieto protokollaan kohdistuvasta julkisesta huomiosta on tärkeä tutkimuksen kannalta. Aiheen laajuuden vuoksi asiantuntijahaastattelut ovat kartoitusta tehtäessä erittäin tärkeällä sijalla. Alustavan protokollaselvityksen jälkeen haastattelemalla oman organisaation asiantuntijoita saadaan laajempaa ja tarkempaa näkymää ”protokollaviidakkoon”. Mediaseuranta auttaa löytämään uusia kotimaisia asiantuntijoita ja antaa joitakin viitteitä kriittiseen infrastruktuurin eri osa-alueisiin liittyvistä protokollista. Asiantuntijoita haastattelemalla saattaa löytyä protokollia ja protokollarykelmiä, jotka eivät ole olleet perinpohjaisen tutkimuksen kohteena ja muodostavat tämän vuoksi suuria, todennäköisiä tietoturvariskejä. Eri protokollatoteutusten levinneisyydet ja käyttöympäristöt ovat analyysin kannalta erityisen tärkeitä.

Ratkaisumallilla saadaan parempi tekninen ja hallinnollinen ymmärrys ja kokonaiskuva kriittisen infrastruktuurin protokollien kentästä sekä nähdään ongelmakohdat, kuten piilevät kytkökset, riippuvuudet ja periytyvyydet. Visualisointi tarjoaa informatiivisen kommunikaatiotavan kentän toimijoiden välille. Mallia hyödyntäen voidaan tutkia erilaisia käytännön skenaarioita ja niihin vaikuttavia tekijöitä. Eräs tällainen skenaario on jonkin tietyn tietoverkon komponentit ja niiden toteuttamat protokollat. Lisäksi voidaan ottaa huomioon verkkoa ylläpitävän organisaation omat haavoittuvuusanalyysit, riskienhallintasuunnitelmat ja uhkaskenaariot. Malli toimii lähdemateriaalina riskienhallinnassa, haavoittuvuusanalyysissä, strategisessa suunnittelussa ja myös tietoturvatutkimuksen tulevan suunnan viitoittamisessa.

4.1.2 Muutostenhallinta

Tietotekniikan kehitys perustuu abstraktioihin: tietotekniset järjestelmät luottavat alemman tason järjestelmien toimintaan. Abstraktiot pyritään pitämään hallinnassa erilaisilla modulaarisilla rakenteilla ja tarkasti määritellyillä rajapinnoilla. Periaatteessa alla oleva järjestelmä voitaisiin vaihtaa toiseen, joka noudattaa samoja rakenteita ja sääntöjä kuin sen edeltäjä. Abstraktiota on käytetty menestyksekkäästi verkkoteknologiassa, esimerkiksi TCP/IP-pinossa, mutta ohjelmistomaailmassa se on osoittautunut hankalaksi.

Palvelunkehityksen toteutusosio sitoo ideoidun ja määritellyn ohjelmiston tiettyyn ympäristöön ja siten sen toimivuus on myös riippuvainen ympäristöstään. Monimutkaisissa järjestelmissä nämä riippuvuussuhteet muuttuvat nopeasti kompleksisiksi: ohjelmisto on riippuvainen tietystä käyttöjärjestelmäversiosta, laiteajureista, ohjelmointikieliympäristöstä ja muista ohjelmistoista.

Normaalit ylläpitotoimet voivat rikkoa tämän useasti herkänkin tasapainon. Palvelun kehityksessä ja erityisesti ylläpidossa siinä käytettävien järjestelmien muutosten hallinta onkin keskeisellä sijalla.

Dokumentointi on tärkeä osa muutosten hallintaa: palvelun käyttämät resurssit täytyy määritellä tarkasti. Tällöin voidaan tunnistaa sellaiset kohteet, joiden muuttaminen täytyy tehdä erityistä varovaisuutta noudattaen. Alustava selvitys voidaan tehdä jo konseptivaiheessa. Alihankinta tuo lisää kompleksisuutta muutosten hallintaan, ja se tulee ottaa huomioon käytännöistä sovittaessa. Muutoksen hallinnassa ja muissakin ylläpito-prosessissa yhteinen dokumentoitu malli on välttämätön, etenkin verkostoituneessa ympäristössä.

Kaikki muutokset tulisi testata testijärjestelmissä ennen tuotantokäyttöön siirtämistä. Mikäli tehtävä muutos on palvelun kannalta haitallinen, mutta itse järjestelmän kannalta välttämätön, täytyy ohjelmistoa itseään päivittää. Hankaluudeksi voi nousta kuluttajille jo jaettu ohjelmisto, joka lakkaakin toimimasta laitteen päivityksen yhteydessä. Ohjelmistojen päivittäminen onkin tehtävä kuluttajille helpoksi ja siitä täytyy asianmukaisesti tiedottaa.

4.1.3 Tietoturvariskienhallinta

Yleisesti tiedon käsittelyriskit voidaan jakaa vahinkoihin (esim. ylläpitovirhe ja lörpöttely) ja tahallisiin tekoihin. Tietoteknisiä riskejä ovat mm. virukset ja luvaton tunkeutuminen järjestelmään. Vaikeasti hallittavia riskejä ovat valmisohjelmistojen virheet. Huomioitavia ovat myös hallinnolliseen tietoturvaan kohdistuvat riskit, kuten

- tietoaineiston puutteellinen luokittelu,
- puuttuva strategiasuunnittelu,
- osaamisen puute ja
- tietoturvatehtäviin liittyvä vastuumäärittely.

Riskienhallinnan vaiheita ovat karkeasti jakaen riskien tunnistaminen, niiden arviointi ja niihin varautuminen. Nämä vaiheet voivat mennä osaksi päällekkäin. Riskienhallinnan eri vaiheissa sitä toteuttava organisaatio erottelee toimintojaan ja pyrkii näkemään niiden edellytykset ja liitokset, jolloin riskienhallinnalla voi olla myös yleisesti toimintaa tehostava vaikutus. Suunnitelmallisuus ja säännöllinen arviointi on tärkeää. Myös johdon sitoutuminen on oleellista, koska johto määrittelee siedettävän riskitason ja allokoi resurssit suojaus-toimenpiteille. Riskeiltä suojautumisen onnistumista tulee mitata jatkuvasti. Arvokasta tietoa potentiaalisista riskeistä kertoo myös ns. ”läheltä piti” -tilanteiden tarkkailu ja raportointi. Tärkeää on muodostaa yhteys alihankkijaketjun toimijoiden riskienhallintaprosessien välille läpi koko ketjun.

Tunnistusvaiheessa luetellaan toimintojen edellytyksiä ja pyritään löytämään niihin liittyviä uhkia. Tunnistetut uhkat voivat tässä vaiheessa olla kuinka epätodennäköisiä tahansa; niiden tärkeyttä arvotetaan myöhemmissä vaiheissa. Samalla voidaan arvioida uhkien realisoitumisesta kieliviä merkkejä, joita seuraamalla uhkaan liittyvä riski voidaan välttää ennen kuin se toteutuu. Välttämissuunnitelma voidaan luoda tässä vaiheessa tai viimeisessä vaiheessa yhdessä varasuunnitelman kanssa.

Arviointivaiheessa pohditaan toimintoon kohdistuvan uhkan toteutumisen vakavuutta ja itse uhan todennäköisyyttä. Yksi tapa arvottaa riskien vakavuutta toisiinsa nähden on esittää arvioinnit numeroarvoina ja vertailla näiden arvojen tuloa keskenään. Lisäksi täytyy muistaa, ettei joitakin uhkia voi liennyttää millään.

Varautumisvaiheessa tehdään riskien välttämis- ja varautumissuunnitelmia. Itse riskienhallinta koostuukin tilanteen aktiivisesta seuraamisesta, eri riskeihin liittyvien oireiden tunnistamisesta ja seuraamisesta, suunnitelmien toteuttamisesta ja itse riskienhallinnan arvioinnista ja kehittämisestä eri tilanteiden mukaan.

Riskit voidaan jakaa teknologiaan, käyttäjiin ja toimintatapoihin kohdistuviin riskeihin. Käyttäjiin kohdistuvat riskit ovat merkittävämmässä osassa; teknisiä riskejä käsitellään kuitenkin usein enemmän ehkä niiden helpomman hallittavuuden vuoksi. Käyttäjät voivat kuitenkin toimillaan tehdä tekniset ratkaisut tyhjiksi.

Käyttäjistä aiheutuvat riskit liittyvät koulutuksen puutteeseen tai toisaalta tahalliseen toimintaan. Tietoisuuden puute tietoturva-asioista voi aikaansaada tahattomia tietovuotoja ja vaarallisia työvälineiden käyttö- ja konfiguraatiotapoja. Koulutuksen tarve korostuu, mikäli voidaan olettaa käyttäjiä vastaan esiintyvän urkintaa tai muuta social engineering -toimintaa vihamielisten tahojen taholta. Toisaalta merkittävä osa tietorikoksista suoritetaan organisaation sisältäpäin. Riskiä voi pienentää organisaation toiminnan jakaminen useisiin eri käyttöalueisiin ja niiden sisällä käyttöoikeuksiin. Ylläpitäjät ja heidän osaamisensa ovat tietysti avainasemassa.

Teknisten riskien hallintaan on olemassa useita perusmenetelmiä. Tärkeistä järjestelmistä täytyy olla olemassa varajärjestelmät, jotka käynnistyvät alkuperäisen pettäessä. Tällöin käytetään vain sellaisia ohjelmistoja ja laitteistoja, jotka ovat testeissä täyttäneet ainakin jotkin laatukriteerit. Niitä täytyy hankkia useammalta eri tuottajalta: riippuvuus yksittäisestä valmistajasta voi aiheuttaa ongelmia esimerkiksi tuotelinjan lopettamisen tai konkurssin yhteydessä. Ei haittaa, jos samoja komponentteja valmistetaan useammassa eri valtiossa, jolloin minimoidaan erilaisia poliittisia riskejä.

Laitteisiin täytyy olla nopeasti saatavilla varaosia, jotta rikkoutumisista koituvat haitat voidaan minimoida. Hallintajärjestelmään on löydyttävä asiantuntijaosaamista: hyödyllisyys muuttuu kyseenalaiseksi, mikäli kukaan ei osaa ylläpitää ja tarvittaessa muokata sitä. Järjestelmiä säilytetään turvallisessa paikassa lukkojen takana. Niiden toimintalämpötila, energiansaanti ja muut tarvittavat toimintaolosuhteet varmistetaan. Tietoaineistoa ovat myös paperitulosteet ja puhuttu tieto, jne.

4.2 Teknologiakeskeiset ratkaisut

Teknologiset ratkaisut mobiilimaailman uhkakuviin ovat moninaiset. On mahdotonta kuvata niitä tyhjentävästi ja samalla lyhyesti. Seuraavassa taulukossa on luetteloitu tutkimuksemme havaitsemat tärkeimmät teknologiset ratkaisut:

Taulukko 7. Teknologiakeskeisiä ratkaisuja mobiilimaailman uhkiin.

Ratkaisu	Nykyinen teknologia	Uusia teknologioita
Käyttäjän ja palvelun tunnistus	SIM, USIM, WIM, SWIM, IKE, salasanat, SMS, ym.	HST, biometriikka, HIP, DNSSEC
Digitaalinen allekirjoitus ja kelpoisuuden toteaminen	Selainten allekirjoitukset	Sovelluskohtaiset tai universaalit älykortti allekirjoitukset
Median levityksen rajoitus	OMA-DRM, valmistajakohtainen DRM, suojatut muistikortit, vertaisverkkojen skannaus	Luotetut alustat
Tallennetun datan salakirjoitus	Muistinsalausohjelmat	Kaikkien muistivälineiden vahva krytografinen suoj.
Liityntä elektroniseen maksujärjestelmään	ssl/tls salattu wap tai web, pankin kertakäyttösalasanat (Tupas)	Luotetut HW/SW alustat, HST-SIM
Yksityisyyden suojaaminen	ssl/tls, PKI, VPN, SIM auth, NAT, anon. palvelut, rekisterien suojaus, SAML, Liberty	Esim. spontaanit- ja vertaisverkot, onion routing
Palvelimien suojaaminen	FW, SW-autopäivitykset, ym.	Autom. laadunvarmistus työkalut
Hyökkäyksen havaitseminen	Paikalliset DB IDS -järjestelmissä, mustien listojen levitys (hosts)	Globaalit, jaetut DBt IDS järjestelmissä
Haittaohjelmien torjunta	Tunnistepohj. virustor-juntaohjelmat	Uutena mm. heuristiset analyysit, muistialueet
Turvalliset asetukset	Manuaalisesti tai SMS-viestinä	Etäkonfiguroinnin standardit, OMA SyncML DM

Tärkeimpiä teknologiakeskeisiä käytäntöjä tiedon ja järjestelmien suojaamiseen palvelunkehitysympäristössä on lueteltu alla olevassa esimerkissä (lähteinä käytetty mm. [CERT]):

Esimerkki: Teknologiakeskeisiä tietoturvakäytäntöjä palvelunkehitysympäristössä.

- Suunnittele kokonaisarkkitehtuuri.
- Valitse palvelinlaitteet, joiden tietoturvan perusominaisuudet vastaavat sovellusten mukaista vaatimustasoa. Varmista laajennettavuusominaisuudet. Halpaa ja tietoturvaominaisuuksiltaan suppeaa palvelinta ei yleensä voi käyttää vaativiin sovelluksiin.
- Päivitä käyttöjärjestelmät ja sovellukset riittävän nopeasti vikojen löydyttyä. Nykyään päivityksiä täytyy seurata jopa päivittäin. Tee tukisopimukset ja varmista tarvittavien korjauspäivitysten saatavuus.
- Aseta pakollinen käyttäjäntunnistus kaikille järjestelmän käyttäjille. Perusta käyttäjältä vaadittavat tunnistuksen menetelmät sovelluksen ja käyttöoikeuksien mukaisiksi – esim. vahvempi tunnistus (kuten SecurID kortti + salasanat) jos etäkäyttäjätunnuksella ylläpitäjän oikeudet. Opeta oikea salasanojen käyttö. Suunnittele ja toteuta erillinen pääsynvalvontahierarkia käyttöjärjestelmän hakemistoihin, tiedostoihin ja laitteisiin. Varmista toiminta huolellisesti erityisesti päivitysten ja ylläpitotoimenpiteiden jälkeen.
- Järjestä laadukas, riittävän pitkäaikainen ja turvallinen varmuuskopioiden säilytys kaikille järjestelmän tiedostoille mukaan lukien käyttäjätiedot ja järjestelmän konfiguraatiot. Selvitä lainsäädäntö ja mahdolliset toimialavelvoitteet.
- Suojaa laitteet tietokoneviruksilta ja haittaohjelmilta. Nykypäivänä tämän suojauksen toimivuus (virustorjunnan päivitysten latautuminen) on erittäin tärkeää varmistaa. Jopa järjestelmän tai sen osien (esim. sähköposti) hallittu sulkeminen virusuhkan ollessa pahimmillaan voi olla tarpeen tietyissä tapauksissa.
- Suojaa tarvittavat yhteydet VPN:llä.
- Käytä järjestelmän kahdennusta palvelun saatavuuden varmistamiseksi. Testaa ennakolta turvallisiksi todettuja replikointimenetelmiä.
- Estä suorat yhteydet web-palvelimiin julkisista verkoista samoin kuin organisaation sisäisestä verkosta käyttämällä palomuureja. Jo tämä estää suuren osan tavallisista hyökkäyksistä. Valitse sopivantasoisten lokitietojen keruu ja seuraa niitä järkevillä menetelmillä (hälytykset, ym.). Minimoi web-palvelimen toiminnallisuus vain olennaisiin, sovellukseen liittyviin ohjelmiin.
- Ota käyttöön järjestelmiä, joilla voidaan havaita järjestelmässä esiintyvä käyttöoikeuksien vastainen tai muuten odottamaton ja epäilyttävä toiminta. Käytä hyökkäyksen tunnistus- ja estojärjestelmiä (IDS).
- Käytä jotain käytännönläheistä järjestelmää, johon tallennetaan aiemmista virheistä (tai toteutuneista tietoisista riskeistä) opittu tieto ja jota on helppo käyttää myös aktiivisesti suojauksen suunnittelussa ja toteutuksessa.
- Jos aiot esim. ostaa järjestelmään kuuluvat tietoturvan hallinnoinnin ja palvelun, tee se huolella suunnitellen ja erilaiset vastuut sopimusteitse nauliten. Vakavimmat seuraukset ongelmatilanteessa eivät useinkaan kohdistu siihen osapuoleen, joka on vastuussa suojaavista toimenpiteistä.

4.2.1 Käyttäjien, laitteiden ja palveluiden tunnistaminen

Matkapuhelimiin on valmistajan taholta upotettu IMEI-koodi, mutta tätä koodia ei paljoakaan käytetä. Periaatteessa varastetun puhelimen käytön voisi estää panemalla IMEI-koodi estolistalle, mutta käytännössä kansallisrajoja ylittäviä IMEI-estolistoja ei käytetä. Sen sijaan mobiililiittymän tilaaja tunnistetaan puhelimeen asetetulla SIM-kortilla.

Tunnistamiseen voidaan käyttää varmenteita. Kryptografinen varmennejärjestelmä voidaan perustaa joko kahdenväliseen luottamukseen tai luotetun kolmannen osapuolen varaan. Maailmanlaajuinen julkisen avaimen infrastruktuuri on törmännyt luottamuspulaan. Tilalla on ”tilkkutäkki”, jossa käyttäjä joutuu vastaamaan kyseenalaisiin luottamuskysymyksiin reaaliajassa. ”Hyväksytkö N:n antaman sertifikaatin palvelun X varmennukseksi?” Kuitenkin internet-osoitteen ja sitä vastaavan julkisen avaimen yhteys pitää tärkeissä yhteyksissä varmentaa. Suojattuun verkkoselaukseen yleisesti käytössä oleva keino on ”https:”-sertifikaattivahvistus turvatulla TLS/SSL-kanavalla. Sähköpostissa on käytössä sertifikaatti-pohjainen S/MIME-varmistus. Tunnusten ja identiteetin jakelu on oma haasteensa, mutta etenkin liittymän tilaajan kryptografisen identiteetin jakelu on helppo toteuttaa perinteisellä välineellä, eli SIM-kortilla.

Suomalainen sirupohjainen henkilövarmenne, (HST), samoin kuin pankkien käyttämät tunnistusmenetelmät, perustuvat siihen, että rekisteröintihetkellä käyttäjä on henkilö-kohtaisesti tunnistettu. Toinen yleisesti käytetty malli perustuu välittömään aloitukseen, jonka tuloksena yhteyden kummassakin päässä tallennetaan kryptografista varmennetietoa. Tämä tieto on käytössä vain yhteyden kestäessä ja tallennettu turvallisesti siten, että seuraavalla kerralla tiedetään toisen osapuolen olevan sama kuin edellisellä kerralla. Tästä hyvänä esimerkkinä ovat SSH-suojaukset. Harrastajien keskuudessa on käytössä tästä kehitellyt luottamusrenkaat (PGP-malli), jossa säilytetään omalla koneella varmistettujen luotettavien tahojen julkiset avaimet. Jos uutta yhteyttä muodostettaessa löytyy yhteinen tuttu, voi luottamus nimen ja identiteetin välille perustua tällaiseen kolmioon.

Yleisesti nimen ja osoitteen välinen yhteys on hankala. Nimen ja identiteetin yhteys voi olla huonosti määritelty, ja identiteetin esitys voi olla ympäristöriippuvainen. Osoitteella tarkoitetaan tietomäärää, joka tarvitaan verkossa olevan olion löytämiseksi, oli se sitten puhelinnumero tai IP-osoite. Nimiresoluutio on perusfunktio, jolla identiteetin esitys muutetaan esimerkiksi IP-osoitteeksi. Sähköpostiosoite voi siten olla verkon kannalta identiteetin esitys, mutta sovelluksen kannalta osoite.

Perusjako on puhelinnumeroiden ja internet-avaruusosioiden välillä. Puhelinnumerot ovat globaalisia vain jos käytetään niiden kansainvälistä etuliite-esitystä. Internet-osoitteet ovat osa universaalista hierarkkista nimiavaruutta, jossa pohjalla on juurihakemisto, josta kaikki muu on johdettavissa.

GSM- ja UMTS-verkoissa käyttäjä tunnistetaan IMSI-koodilla, joka löytyy SIM-kortista. Turvallisuussyistä sitä pyritään käyttämään harvoin, ja siksi siitä luodaan kertakäyttökoodi TMSI (GPRS-käyttöön vielä erikseen P-TMSI), joka vaihdetaan joka käytön jälkeen ja lähetetään käyttäjälle salatulla kanavalla. SIM-kortista voi löytyä USIM (jossa osana IMSI) ja multimediakäyttöön ISIM. UMTS-verkkojen USIM-kortti voi sisältää IMSI:n lisäksi todennuksessa tarvittavan salaisen avaimen sekä yksityiset identiteetit, jotka tarvitaan, jos halutaan samanaikaisesti monesta terminaalista yhteys samalla julkisella identiteetillä. Yhteenvetona voidaan todeta, että SIM sisältää jaetun salaisuuden (salaisen avaimen) oman kotiverkon kanssa.

Esimerkki uudesta tunnistusteknologiasta: Uusin ja vielä kokeilu/standardointivaiheessa oleva HIP (Host Identity Protocol) -teknologia perustuu tunnistuksen ja sijainnin erillisyyteen. Siinä erotetaan identiteetti ja osoite toisistaan, jolloin laite voi luontevalla tavalla hyödyntää vaihtuvia kuljetuskerroksia (WLAN, UMTS, …) ja käyttäjän sovellus tuntee vain kryptografisen identiteetin. Loppu hoituu kuljetus-kerroksessa, jossa voi olla käytössä monenlaisia osoitteita samanaikaisesti. Katso [HIP].

Nykyisten puhelinnumeroiden korvaaminen muilla käyttäjätunnisteilla on lähinnä poliittinen päätös. Numerosiirrettävyyden tultua mahdolliseksi puhelinnumeroilla tunnistetaan nykyisin liittymän tilaajat eikä puhelinlankoja. Kaikki osoiteavaruudet eivät kuitenkaan hallinnallisesti ole samanarvoisia; hierarkkisesti rakennetulla järjestelmällä on parempi skaalautuvuus kuin tasomaisella. Välttämätöntä on tarkastella myös haavoittuvuuksia hyökkäyksiä vastaan. Keskeistä on suojata nimipalvelimet, johon on olemassa jo uusi standardi DNSSEC, joka ei vielä ole laajalti käytössä.

Suuri vedenjakaja tällä hetkellä on piirikytkentäinen tai pakettikytkentäinen ajattelutapa. SIP-protokollaa käytetään eri tarkoituksiin kummallakin puolella, ja uudet XML-pohjaiset web-palvelut tulevat hämärtämään osoitteen merkitystä kokonaisuudessa. Lisäksi nykyisissä käyttäjähakemistojen ratkaisuissa käyttäjäidentiteetin, tunnisteiden ja profiilitietojen hallinta on suuri haaste. Varsinkin verkostoituneessa ympäristössä tulee hallinnollisia haasteita muun muassa valtuutusten kanssa. Hakemistojen hallintatyökalujen merkitys korostuu.

Esimerkki: Tunnistus.fi-palvelu tarjoaa pääsyn viranomaisten verkkopalveluihin, jonka kautta tehdään kuukaudessa noin 20 000 tunnistusta. Ylivoimaisesti suurin osa tehdään pankkitunnuksilla. Palvelu toimii yleisillä Internet-selaimilla, joissa on käytössä SSL/TLS-protokolla. Tunnistautuminen vaatii joko sirullisen henkilökortin tai pankin henkilö- tai yrityskohtaiset verkkopankkitunnukset. Kertakir-jautumisella pääsee kaikkiin listan palveluihin.

Lisäesimerkki: Biometrinen tunnistus. Henkilön tunnistaminen matkaviestintään liittyen saatetaan tulevaisuudessa tehdä myös fyysisen ominaisuuden tai käyttäytymisen perusteella. Tyypillisiä *biometrisen henkilöntunnistuksen* tuotteita ja palveluita ovat tällä hetkellä mm. laitteen pääsynvalvonta, biometriset lukot ja kulunvalvonta, puolustusvoimien sovellukset, passintarkastus, viranomaistoiminta ja asiapaperit. Nykyisin markkinoilla on puheen-, kasvojen-, iiris-, verkkokalvon-, käden- ja sormenjäljen-tunnistus sekä allekirjoituksen tarkastus (sormenjälkitunnistus on kaikkein kypsin tekniikka). On kuitenkin muistettava että sormenjäljen käyttö (ja muu biometrinen tunnistus) liittyy myös yksityisyyden suojaan, jolloin tarpeettomasti ei saa käyttää dataa joka esim. erikoistilanteissa (varkaus, laitevika) saattaa joutua vääriin käsiin. Tulevaisuudessa biometrian sovellusalue todennäköisesti laajenee esim. seuraaville alueille:

- Sähköinen kauppa, mobiilit päätelaitteet, tulevaisuuden Internet-matkapuhelimet.
- Laitteiden ja palveluiden personointi käyttäjälle. Ikääntyneiden turvallisuus.

Rajoituksia ja tietoturvauhkia voi tulla biometristen anturien liittämisestä matkapuhelimeen (esim. USB:n kautta) ja yleensä integrointiin matkapuhelimen ohjelmistoihin. Sormenjälki- ja äänentunnistus ovat lupaavimpia tekniikoita matkapuhelimeen. Katso esim. EU IST:ssä BioSec (Biometrics & Security) -projekti [BIOSEC]. Kattavia kansainvälisiä standardeja biometriikan alueella on heikonlaisesti, mutta esim. BioAPI konsortio [BIOAPI] on standardoinut biometriikka-API:n ja ICAO standardoi matkustusasiakirjojen biometriaa, myös ISO on aktiivinen.

4.2.2 Ohjelmien digitaalinen allekirjoittaminen ja kelpoisuuden toteaminen

Sähköisellä allekirjoituksella voidaan yksilöidä allekirjoittaja ja allekirjoitettu tieto. Allekirjoitus on luotava avaimella, jota vain allekirjoittaja pitää omassa hallinnassaan. Tällä saavutetaan tapahtuman kiistämättömyys, mikä vahvistaa allekirjoitetun tiedon ja allekirjoittajan alkuperän ja tiedon eheyden. Sähköisen allekirjoituksen asemaa on selkeyttänyt Euroopan parlamentin hyväksymä direktiivi 1999/93. Tämä on mahdollistanut sen, että yritykset voivat nyt suorittaa laillisesti sitovia liiketapahtumia verkossa entistä suuremmalla luottamuksella.

Allekirjoituksessa on käytössä useita tiivistealgoritmeja, esimerkiksi MD5 (128-bittinen tarkistussumma) ja SHA (Secure Hash Algorithm, 160-bittinen). Sähköisellä allekirjoituksella varmistetaan tiedon alkuperä, kun allekirjoittaja salaa tiivisteen tuloksen omalla yksityisellä avaimellaan. Syntynyt allekirjoitus lisätään allekirjoitettavaan viestiin, joka lähetetään vastaanottajalle. Tarkistaakseen viestin, vastaanottajan on avattava allekirjoituksen salaus lähettäjän julkisella avaimella ja talletettava se. Jos vastaanotetusta viestistä laskettu tiiviste vastaa alkuperäistä tiivistettä, vastaanottaja voi olla varma viestin alkuperästä ja eheydestä.

Myös julkisen avaimen kryptografiaan liittyviä avaimia voidaan suojata sähköisellä allekirjoituksella. Lisätietoineen allekirjoitettua avainta kutsutaan varmenteeksi (sertifikaatti). Tämä prosessi vähentää avainten väärinkäyttöä, kun osapuolten identiteetti on varmistettu kolmannen osapuolen toimesta. Varmentajaviranomaisen myöntämällä varmenteella voidaan tunnistaa avaimen haltija, ja tällaisella varmenteella on rajallinen voimassaoloaika.

Sähköisissä palveluissa varmenteita käytetään palvelun alkuperän, ts. palveluntarjoajan tai ohjelmiston tunnistamisessa. Loppukäyttäjän hankkiman sovelluksen tapauksessa vaikkapa Java-kielisestä sovelluksesta lasketaan tiiviste, joka allekirjoitetaan palveluntarjoajan salaisella avaimella, jonka kolmas osapuoli on varmentanut. Mukana tulevalla varmenteella loppukäyttäjä voi tarkistaa sovelluksen alkuperän ja muuttumattomuuden. Yleisimmin varmenteet pohjautuvat X.509-standardiin, joka määrittelee varmenteen muodon ja sisällön sekä varmenteiden sulkulistan (CRL), jota käytetään varmenteen mitätöimiseen ennen sen varsinaisen voimassaoloajan päättymistä, esimerkiksi yksityisen avaimen vuotaessa julkisuuteen.

Sähköinen allekirjoitus on mobiilissa laitteessa turvallisimmillaan, kun siihen liittyvät algoritmit ja avaimet sijaitsevat kajoamiselta suojatussa laitteessa, kuten SIM-kortilla. Tällainen tilanne on WAP-identiteetti moduulissa (WIM) ja HST-SIM:ssä, joten ne ovat varsin turvallisia teknologioita (jos itse SIM ja matkapuhelin on toteutettu turvallisesti). SIM-korttihan alun perin tarkoitettiin GSM-tilaajien haaste/vastaus-todennukseen, mutta se sisältää nykyisin mikroprosessorin, ROM-, EEPROM- ja RAM-muistia, I/O-portin, käyttö-järjestelmän, tiedostojärjestelmän. Näin ollen SIM:lle voidaan toteuttaa vaativia, luotettuja sovellusohjelmia. Luotettu alusta voi tarkoittaa standardista riippuen eri asioita. Alla on yksi esimerkki luotetusta matkapuhelinalustasta.

Esimerkki luotetusta mobiilialustasta: Trusted Mobile Platform [TMP] on yksi tapa varmistaa osaltaan vahvojen kryptografisten menetelmien turvallisuuden matkapuhelinlaitteessa, sillä siinä määritellään mm. laitteistoarkkitehtuurin kolme eri tietoturvatasoa (levels). Esim. korkeimmalla turvatasolla käyttäjän tunnistus pitää suorittaa HW-salausmoduulissa ja CPU pitää olla erillisessä HW-alueessa käyttäen luotettua muistiväylää.

4.2.3 Median edelleen levityksen rajoittamisesta ja tallennetun datan salakirjoittamisesta

Yleisesti *tekijänoikeudet* antavat teoskynnyksen ylittävän teoksen tekijälle joukon yksin-oikeuksia, jotka on ajallisesti rajattu julkaistulle teokselle 70 vuoteen tekijän kuoleman jälkeen. Vastaavasti *lähioikeudet* suojaavat mm. esittäviä taiteilijoita, tuottajia ja valokuvaajia esim. teosten kopioinnilta, levittämiseltä ja välittämiseltä, suoja-ajan ollessa 50 vuotta tallentamisesta. Digitaalisessa maailmassa tiedostojen täydellinen ja häviötön kopiointi on helppoa. Aina, kun oikeuksien omistajat ovat keksineet tavan turvata sisältönsä liian laajalta kopioinnilta, käyttäjät ovat löytäneet tavan kiertää sen. Teoksen siirto digitaalisesta muodosta analogiseen eli ihmisen ymmärtämään muotoon on viimeistään se kohta, jossa suojauksen voi rikkoa. Digitaalisen ympäristön kopiosuojaus ei siis estä kopiointia. Tästä johtuen kopiosuojauksilla ei näytä olleen vaikutusta ammattimaiseen kopioiden jälleenmyyntiin eli piratismiin. Lisäksi kannattaa huomata, että ns. ”verkostoefektistä” johtuen rikkomuksilla voi olla myös myönteisiä vaikutuksia laillisten teoskappaleiden myyntiin.

Esimerkiksi Applen Itunes-musiikkipalvelun kopiosuojaus murrettiin (Pymusiquen toimesta) vain siksi, että iTunes-musiikkia voitaisiin kuunnella myös Linux-koneissa, jolloin potentiaalinen käyttäjäkunta laajeni.

Kopiosuojaukseen käytettävän panostuksen suuruuteen vaikuttaa sisällön arvon kehitys ajan suhteen. Esimerkiksi huomisen säätiedon myyntiaika keskittyy yhteen päivään, jonka jälkeen tuote sisältöineen on kuluttajille arvoton. Toisaalta mobiilipelin tai -ohjelman myyntiaika voi olla jopa muutaman vuoden mittainen, jonka jälkeen kilpailevat tuotteet, uudet ominaisuudet tai jopa vaihtunut kännykkäsukupolvi, voivat viedä sen arvon lähelle nollaa. Pitkällä aikavälillä kopiosuojauksesta voi olla enemmän haittaa kuin hyötyä, vaikka sisällöntuottajat vaativatkin useimmiten sen käyttöä. Uusi tekijänoikeuslaki on eduskunnan käsittelyssä, joten uusia säädöksiä on tulossa asiaan liittyen.

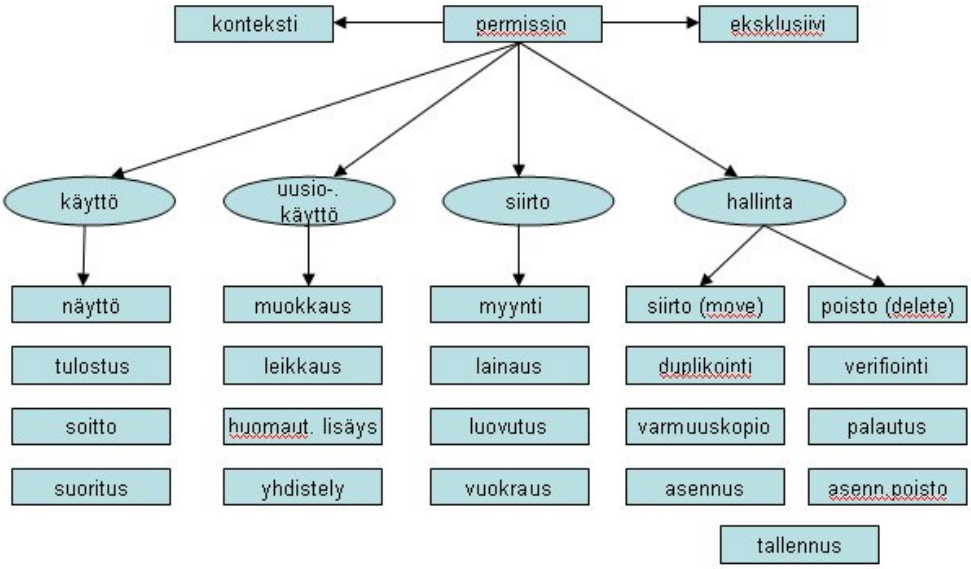
Teknisesti tekijänoikeuksia voi yrittää valvoa mobiileissa päätelaitteissa aivan samoin kuin kotitietokoneissakin. Tosin suojausmekanismin ohittaminen voi olla hivenen hankalampaa (fyysiseltä- ja ohjelmistorakenteeltaan suljetussa) matkapuhelimessa kuin kotitietokoneissa, vaikka avoimet käyttöjärjestelmät, kuten Symbian, tuovatkin älypuhelimet hyvin lähelle kotitietokoneiden ominaisuuksia myös tekijänoikeuksien suojelemisen kannalta.

Laite- ja alustavalmistajilla on ollut hyvin erilaisia ja yhteen sopimattomia ratkaisuja, joita on pyritty sovittelemaan yhteisten standardien alle. Standardointiyhteisöistä tärkeimmältä vaikuttaa Open Mobile Alliance (OMA), joka on määritellyt tekijänoikeuksien suojeluun tähtääviä OMA DRM (Digital Rights Management) -standardeja. OMA DRM:n ensimmäisen vaiheen toteutuksia löytyy jo usean valmistajan puhelinmallistoista.

OMA DRM versio 1.0 määrittää edelleenlähetyksen eston (forward-lock) sekä yhdistetyn ja erillisen jakelun (combined and separate delivery) laitteistoriippumattomat mekanismit. Yhdistetyssä jakelussa materiaalin käytölle voi asettaa lisärajoituksia, kuten ”saa käyttää vain kerran” tai ”saa käyttää viikon ajan”. Erillisessä jakelussa käyttöoikeudet ja sisältö toimitetaan toisistaan riippumattomin tiedonsiirroin, jolloin kokonaan erilliset tahot voivat helpommin kontrolloida sisällön jakelun ja käyttöoikeudet. Myös OMA DRM 2.0 standardiluonnos on jo olemassa.

Miten käyttöoikeuksia kuvataan? Tärkein standardi on ehkä Open Digital Rights Language (ODRL), joka on suhteellisen kevyt ja yksinkertainen oikeuksia kuvaava kieli ja lisäksi riippumaton sisällön tyypistä ja siirtotiestä. ODRL on itsessään avoin ja lisenssimaksuton standardi, mutta OMA on ottanut sen käyttöön DRM standardissaan määrittelemällä OMA ODRL -profiilin. Viimeisin ODRL:n versio 1.1 [W3ORG] ja myös seuraavan version vaatimukset [ODRL] ovat saatavana.

ODRL:n permissiot mahdollistavat käyttöoikeuksien monipuolisen määrittelyn (katso kuva 4):



Kuva 4. ODRL v1.1:n käyttöoikeusmalli.

Nämä sisällön jatkokäsittelyn permissioihin liittyvät toiminnot on tietenkin toteutettu tapauskohtaisesti käytettävässä laitteessa, kuten matkapuhelimessa. Esim. jos sisältöön kohdistettu DRM-permissio antaisikin käyttäjälle oikeuden vaikka *muokata* sisältöä, käyttäjän laitteeseen ei välttämättä sisälly muokkaustoimintoa, jolloin muista oikeuksista (esim. *siirto*) riippuu voiko käyttäjä todellisuudessa muokata kyseenä olevaa sisältöä laillisesti vai ei.

Esimerkki multimedian levityksen kopiosuojauksesta. MPEG-patentteja hallinnoiva järjestö MPEG LA [MPEGLA] on ehdottanut tammikuussa 2005 OMA:lle, että OMA DRM 1.0 -standardia hyödyntävien verkko-operaattoreiden tulisi maksaa 0,01 dollaria jokaisesta transaktiosta ja 1 dollari jokaisesta puhelimesta patenttien haltijoille. GSM Association [GSMA] on kuitenkin operaattoreilta saadun palautteen perusteella kieltäytynyt jyrkästi hyväksymästä tällaisia ehtoja sanoen niiden olevan sekä epäkäytännöllisiä, kohtuuttomia että lyhytnäköisiä. Operaattorit ovatkin nyt etsimässä kuumeisesti korvaavia (standardoimattomia?) DRM-ratkaisuja, joiden lisensiointi olisi yksinkertaisempaa ja edullisempaa. GSMA onkin pyytänyt kaikkia vaihtoehtoisten DRM-ratkaisujen tarjoajia antamaan ehdotuksensa GSMA:lle, joka voisi sitten suositella jotain DRM-ratkaisua jäsenoperaattoreilleen. Valitettavasti tämä voi johtaa käyttäjän kannalta tilanteeseen, jossa mm. sisältöpalvelut eivät toimi verkkovierailujen aikana, sisällön siirrettävyys laitteesta toiseen edelleen heikkenee, jne.

4.2.3.1 Esimerkkejä datan tallennuksesta ja salakirjoituksesta

Nykyään on jo olemassa useita eri ”lisäteknologioita” ja välineitä, joilla matkapuhelimen tai PDA-laitteen käyttäjä voi tallettaa itselleen hyödyllistä informaatiota massoittain. Matkapuhelimen keskusmuistin määrä (joissain puhelimissa jopa kymmeniä megatavuja) kasvaa tietysti jatkuvasti, mutta sekään ei ole enää rajoittava tekijä, sillä uusia tallennusvälineitä, kuten USB-muistitikun käyttö, on räjähdysmäisesti tulossa käyttöön myös matkapuhelimiin mm. ääni- ja kuvadatan tallennuksen tarpeisiin. Alla on esimerkkejä matkapuhelinten tallennusvälineistä.

Taulukko 8. Matkapuhelimien fyysisiä tallennusvälineitä.

Muistityyppi	**Esimerkkejä**
Keskusmuisti, lisämuisti	Sisäinen ROM ja RAM ja niiden erilaiset ratkaisut, yhteiskäyttöiset muistit, välimuistit, rekisterit, flash.
Muistikortti	CompactFlash (CF)-kortti. PCMCIA-standardiin perustuva (43x36 mm) flash-muisti. Esim. 1 GB saatavilla.
	MultiMediaCard (MMC)-kortti. Sisältää ROM ja Flash (read/write) teknologiaa. Lisäksi MMCplus 24x32x1.4 mm, ja MMCmobile 24x18 x1.4 mm kortit.
	Secure Digital (SD)-kortti kooltaan 24x32x2.1 mm.
	MiniSD-kortti. Kuten SD-kortti, mutta kooltaan 20x21.5x1.4 mm.
Muistitikku käyttäjädatalle	USB-muistitikku. Esim. SanDisk esitellyt sormenjälkitunnistuksella ja datan salauksella suojatun 512 megatavun USB 2.0 -muistitikun.
Kovalevy	Matkapuhelimeen yhdistetty pienikokoinen kovalevy kuten MP3-soittimissa.

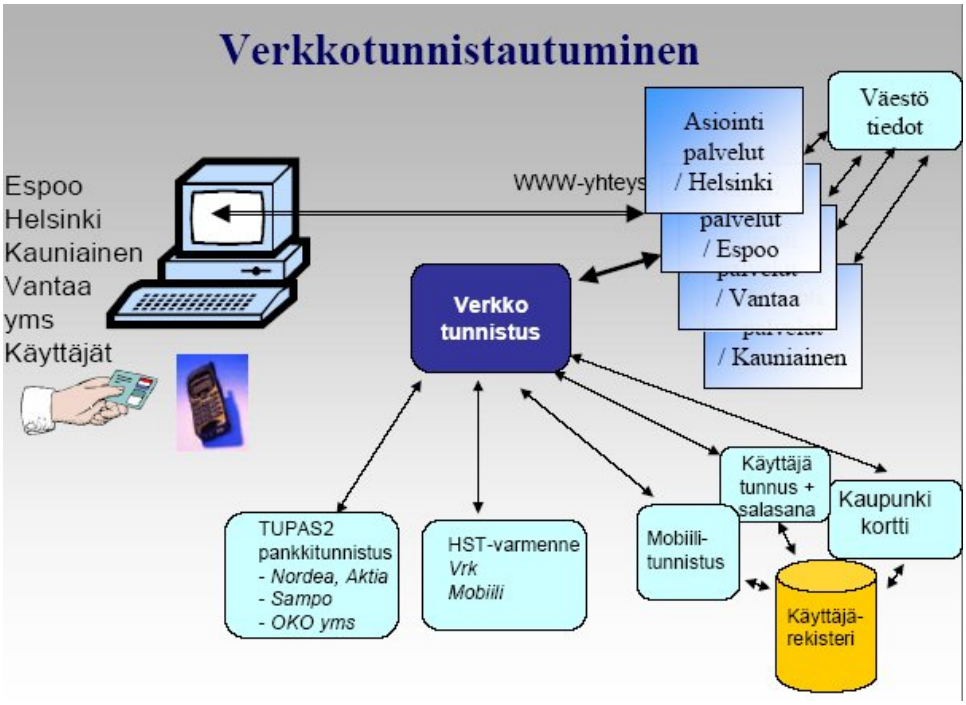
Joihinkin älypuhelimiin (Series 80) ja PDA-laitteisiin onkin jo saatavissa yleiskäyttöisiä tiedostojen salausohjelmistoja, joilla voidaan salakirjoittaa niin puhelimen sisäiseen muistiin kuin ulkoisiin muisteihinkin tallennetut tiedot. Ohjelmat käyttävät esim. salasanalla suojattua pääsynvalvontaa ja 128-bittistä datan salakirjoitusta (esim. Psiloc Secure Storage). Tosin niiden automatisoinnissa (esim. kaikkien tiedostojen automaattinen suojaus) voi vielä olla ongelmia, esim. laitteen rajoittuneesta laskentakapasiteetista johtuen. Tulevaisuudessa matkapuhelimen muistikorttiliityntään voidaan liittää enemmän lisälaitteita, kuten kamera, Bluetooth, GPS, ja WLAN. Alla olevalla esimerkillä havainnollistetaan talletettavan datan salausratkaisujen divergenssiä.

Esimerkki massamuistista: SD-muistikortti käyttää suljetun 4C-konsortion (IBM, Intel, Matsushita ja Toshiba) määrittelemää CPRM (Content Protection for Recordable Media) teknologiaa laittoman kopioinnin estämiseksi. Ominaisuuksia:

- Laitteiden keskinäinen tunnistus vaaditaan ennen pääsyä SD-kortille, jonka jälkeen generoidaan uusi satunnaisluku. Kopiointi PC:ltä SD-kortille on rajoitettu kolmeen kopioon. Ilman avainta salakirjoitettua dataa ei voida purkaa.
- SDIO (Input/Output) -määritelmän mukaisella SD-kortilla korttipaikkaan voidaan liittää lisälaitteita, kuten kamera, Bluetooth, GPS, ja WLAN.

4.2.4 Liityntä elektroniseen maksujärjestelmään

Maksullisten sähköisten palveluiden suurin ongelma on asiakkaan tunnistaminen, sillä asiakkaat eivät mielellään hanki esim. satunnaisesti ostamiinsa palveluihin erillisiä tunnuksia. Hyvänä asiana voidaan kuitenkin pitää viimeaikaista kehitystä julkisella sektorilla, esim. pääkaupunkiseudun kaupunkien yhteistyöhanke viranomaisasiointiin**,** jossa rakennetaan valtionhallinnon kanssa yhdessä yhteinen verkkotunnistautumis- ja maksamispalvelu. Tässä palvelussa Tupas-pankkitunnistus ja HST-varmenne ovat rinnakkaisia ”tunnistus-teknologioita”:



Kuva 5. Tunnistaminen pääkaupunkiseudun yhteistyöhankkeessa [HEL].

Valtionvarainministeriö suosittelee julkisten palveluiden tunnistamisiin:

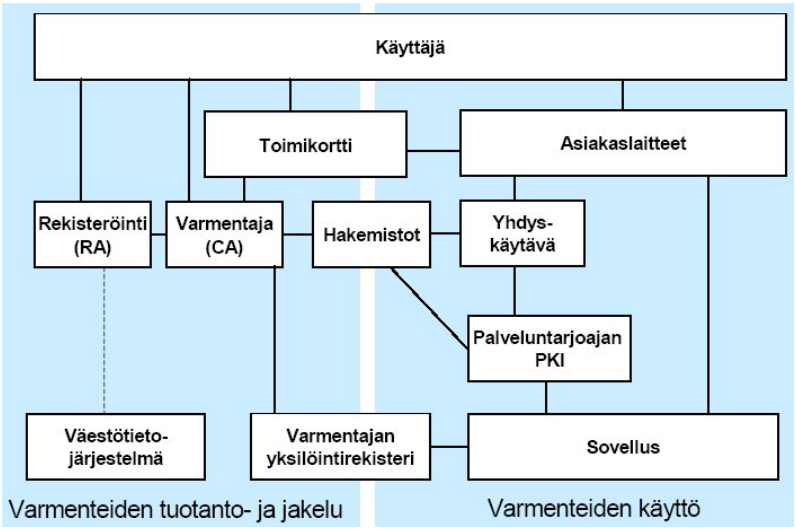
- pankkien Tupas-standardin pankkitunnuksia tai
- kansalaisvarmenteeseen perustuvaa tunnistusta **(**HST**)**.

Taulukko 9. Lyhyesti Tupas- ja HST-ratkaisuista.

Maksajan tunnistus-ratkaisu	**Kuvaus**	**Yleisyys**
Tupas	Suomalaisten pankkien Tupas-palvelu (lisätietoja mm [PANKKIYHD]: • Pankki tunnistaa asiakkaan palveluntarjoajan puolesta. Perustuu samojen pankkitunnusten käyttöön, joita asiakas käyttää pankkipalveluissaan. • Tunnistusvaiheessa asiakas valitsee sivustolta löytyvän pankkinsa logon, joka ohjaa tunnistustapahtuman pankkiin. Käyttäjä syöttää esim. kertakäyttösalasanan tunnistusta varten. • Tunnistusvaiheen jälkeen asiakas hyväksyy itsestään palveluntarjoajalle välitettävän tiedon ja palaa palvelun sivustolle.	Käytetään noin 100 sähköisessä palvelussa. Pankkitunnukset miljoonilla kansalaisilla. Nordea, Osuuspankit, Sampo, Säästöpankit, Tapiola, Ålands-banken.
HST	Kansalaisvarmenne (HST) perustuu Väestörekisterin kansalaisille luomaan sähköiseen PKI-henkilöllisyyteen. Sähköisen henkilöllisyyden tunnuksena turvallisessa verkkoasioinnissa toimii sähköinen asiointitunnus (SATU). HST-varmenne on jo käytössä: • sirullisella henkilökortilla, • OP-ryhmän sirullisella VISA Electron -maksukortilla, • matkapuhelimen SIM-kortilla TeliaSoneralla ja Elisalla (kevään 2005 aikana). HST-tunnistusta käytettäessä saadaan vain henkilön SATU tiedoksi. Vahvuuksia ovat tietoturvataso ja sähköinen allekirjoitus.	Käytetään yli 50 sähköisessä palvelussa. HST-kortteja on käytössä yli 60 000. Luottokunta, DNA, Elisa, OPK, Handels-banken, Säästöpankit,Paikallis osuuspankit, TeliaSonera, Vrk

Voitaneen arvella, että samoja maksajan tunnistusperiaatteita siirtyy myös kaupallisiin sähköisiin palveluihin (sis. mobiilimaksamisen), sillä käyttäjien tottumukset siirtyvät helposti eteenpäin käyttöalueesta (julkinen / yksityinen maksaminen) tai tilanteesta (langallinen verkkoyhteys / langaton yhteys) riippumatta. Ratkaisuja on siis olemassa, mutta niiden tulisi olla helposti kaikkien toimijoiden käyttöönotettavissa, toimittava kaikissa teknologia-alustoissa, jne. Sirupohjaisuuden vuoksi HST:llä on suuremmat vaatimukset teknologia-alustalle, sillä se vaatii perinteisen SIM-kortin vaihtoa sellaiseksi, jolle HST-varmenne on lisäksi toteutettu.

Alla on kuvattu esimerkkinä tarkempi käyttäjän liityntä HST-infrastruktuuriin:



Kuva 6. Esimerkki: HST-arkkitehtuurin yleiskuva [HST].

Luottokorttiko matkapuhelimeen? Kilpailijoiden välisen yhteistyön puutetta on ollut pitkään eri toimijoiden keskittyessä omien luottokorttiratkaisujensa kehittämiseen. Luottokortti-maksaminen on kohtalaisesti toimiva järjestelmä (PC:n kautta) Internetissä, mutta varsinkin silloin päätelaite on suojattava esimerkiksi vakoiluohjelmilta (haittaohjelmahan voi kopioida käyttäjän luottokorttitietoja, tms.). Nykyisin on käytössä Wallet-sovelluksia mm. älypuhelimiin, joissa käyttäjän puhelimelle tallettamat luottokorttiensa tiedot pidetään sovelluksen suojissa ja voidaan kätevästi kopioida palvelun myyjän sivustolle. Se ei kuitenkaan poista tarvetta käyttäjän tarkkaavaisuudelle luottokorttitietojen antamisessa. Nykyään muutkin palveluntarjoajat kuin verkko-operaattori saa tallentaa SIM-kortille omia sovelluksiaan. Tämä johtaa jatkokysymyksiin: Hyödyttävätkö kilpailevien toimijoiden (esim. pankkien ja luottolaitosten) yhteensopimattomat sovellukset SIM-kortilla lopulta kuluttajaa? Tuleeko pankkisuhteen vaihtamisesta helpompaa vai vaikeampaa?

Digiraha on tapa maksaa verkossa *pieniä* ostoksia tai siirtää toisen henkilön kukkaroon rahaa, myös matkapuhelimella. Se otetaan käyttöön avaamalla Internetissä kukkaro (www.digiraha.net) ja siirtämällä kukkaroon rahaa oman pankin pankkitililtä. Tekstiviestillä voi siirtää rahaa oman kukkaron ja vastatilin välillä, tai siirtää rahaa toisen henkilön kukkaroon. (Käytössä Soneran, Elisan, Saunalahden ja DNA:n asiakkaille.)

Mobiilin maksamisen perustavat ongelmat liittyvät paljolti *käytettävyyteen*. Esimerkiksi MeT [MET] pyrkii vahvistamaan mobiilin maksamisen turvallisia käytäntöjä mm. laitevalmistajien implementoinnin yhtenevyyttä tukemaan. Käytettävyyteen liittyen MeT on määritellyt “Consistent User Experience” (CUE):n, joka ottaa huomioon käyttäjän ymmärtämän tilannekuvan, varsinkin maksupalveluja käytettäessä.

Käyttäjän tulisi kokea mahdollisimman samantyyppinen maksulogiikka eri palveluita maksaessaan, jolloin luottamus mobiilia maksamista kohtaan kasvaa. MeT CUE:n määrittelemät yhtenevät käyttäjien kokemat vaiheet ovat pääpiirteissään:

- laitteen alustus, sertifikaatin lataus, rekisteröityminen,
- transaktion vaiheet (yhteyden avaus, käyttäjän tunnistus, digitaalinen allekirjoitus, erikoistilanteiden käsittely),
- PIN-koodin, sertifikaattien ja tikettien hallinta.

4.2.5 Yksityisyys

Yksityisyys on loppukäyttäjän oikeutta määrätä itseään koskevista tiedoista, ja vaikuttaa näiden tietojen käsittelyyn sekä tarvittaessa saada tietoja niitä hallinnoivilta osapuolilta. Yksityisyyden suhteen on muistettava, että mobiilipalvelut ovat palveluympäristönä lainsäädännöllisesti kuin mikä tahansa sähköisiä palveluita tarjoava alusta ja sitä koskevat samat säädökset. Palvelunkehittäjä on velvollinen suunnittelemaan yksityisyyteen ja tietoturvaan liittyvät ominaisuudet niin helppokäyttöisiksi, että käyttäjä ymmärtää tekemiensä toimintojen merkityksen ja siihen mahdollisesti liittyvät vastuukysymykset. Käyttöympäristönä mobiililaite on verrattain rajoittunut, joten palvelunkehittäjällä on suuri vaikutus siihen miten loppukäyttäjä voi hallita omaan yksityisyyteensä vaikuttavaa informaatiota. Yksityisyyden suoja taataan Suomen perustuslaissa.

Esimerkki: Palvelujen osalta keskeisimpiä yksityisyyden säädöksiä ovat:

- Kuluttajasuojalaki
- Laki tietoyhteiskunnan palvelujen tarjoamisesta
- Henkilötietolaki
- Sähköisen viestinnän tietosuojalaki

Suomessa lainsäädännöllä on kielletty asiakastietojen myynti, mutta uhka on olemassa, jos palvelu tarjotaan maasta, jonka lainsäädäntö ei tätä kiellä. Pääsääntöisesti voidaan todeta, että henkilötietojen kerääminen on oltava aina perusteltua, eikä mitään tietoa loppukäyttäjästä saa kerätä eikä säilyttää tarpeettomasti.

Palvelujen käytön kasvun myötä lisääntyy mahdollisuus kerätä käyttäjistä profilointitietoa, vaikkapa tilastoa musiikin kuuntelun tottumuksista. Lähtökohtaisesti tällaiseen tiedonkeruuseen täytyy aina olla lupa käyttäjiltä. Profilointitietoja ei saa missään vaiheessa siirtää mobiililaitteesta muualle ilman käyttäjän hyväksyntää.

Yksityisyydellä tarkoitetaan myös anonymiteettiä, jota mobiilimaailmassa turvataan yhteyskohtaisilla avaimilla. Oikeata tunnistetta joudutaan kyllä käyttämään, kun puhelin kytketään päälle, mutta sen jälkeen yhteyksiä hoidetaan ja siirretään pseudotunnisteilla, jotka ovat kertakäyttöluonteisia. Kun mobiilikäyttöön lisätään Internet-ulottuvuus, yksityisyyden

suojauksella on eri ratkaisut nykyisissä IPv4-verkoissa ja uusissa (mm. UMTS) IPv6-verkoissa. Näköpiirissä on myös ratkaisuja, joissa käyttäjän identiteetti on hoidettu ns. julkisilla kryptoavaimilla. Anonymiteetin eräs ulottuvuus tulee etukäteen maksetuista liittymistä (prepaid-liittymät). Kun Suomessa useimmat käyttäjät ovat identifioitavissa SIM-korttinsa kautta (ja laskutus tapahtuu sitä käyttäen), niin maailmalla on yleisesti käytössä esimaksettu SIM-kortti, johon liittyy puhelinnumero, jota ei suoraan voida yhdistää henkilöön.

Mobiliteettiyksityisyyden mielenkiintoinen ulottuvuus liittyy paikkatietoon. Paikantamista varten viranomaisilla on tietyin edellytyksin oikeus saada operaattorilta tietoa puhelimen sijainnista. Jos puhelin on monen tukiaseman kuuloalueella, tämä paikannus voi olla hyvinkin tarkka. Tämä tieto olisi toki muutenkin hyödynnettävissä, Suomessa käyttäjän luvalla, esimerkiksi perhe- tai ystäväpiirin käyttöön, mutta mahdollisesti myös mainostarkoitukseen. Väärinkäytösmahdollisuuksia on runsaasti. Paikkatiedon erityisluonteeseen yksityisyyden suojan kannalta onkin herätty lainsäätäjän puolelta. Paikkatiedon käyttöä säännellään erikseen sähköisen viestinnän tietosuojalaissa.

Yksityisyyden säädöksiä on määritelty EU-direktiivein 95/46/EY (henkilötieto), 2002/58/EY (sähköisen viestinnän tietosuoja). Tällöin yksityisyydellä tarkoitetaan yksilön oikeutta päättää itse milloin, miten, missä laajuudessa ja mihin tarkoitukseen häntä koskevat tiedot annetaan toisille. Hyvä esimerkki yksityisyyttä vaativasta tiedonsiirrosta on terveyteen liittyvä informaatio. Jotkin ehdotetut liiketoimintamallit saattavat jopa olla ristiriidassa kansalaisten yksityisyyden suojan kanssa.

4.2.6 Resurssien suojaaminen

Mobiilipalvelun tuottava järjestelmä kokonaisuudessaan koostuu erilaisista verkoista ja verkkoihin liitetyistä laitteista. Laitteet tai laitteiden muodostamat alijärjestelmät tarjoavat kokonaisuuteen toiminnallisuuksia resursseilla, joiden tahallinen tai tahaton väärinkäyttö on uhka laitteen tai alijärjestelmän omistajalle tai muille osapuolille. Resurssin väärinkäyttöä estetään valvomalla ja rajaamalla sen käyttöä. Esimerkkejä väärinkäyttöä estävistä mekanismeista ovat käyttäjä- ja tiedosto-oikeudet, palomuurit sekä virustentorjunta-ohjelmistot.

Tietokoneet kännykästä ja PDA-laitteista kotitietokoneisiin, palvelimiin ja supertietokoneisiin perustuvat yleensä muutamaan peruskomponenttiin ja niiden tarjoamaan toiminnallisuuteen. Prosessori on laskennan ydin ja se tarjoaa sovelluksille suoritusaikaa, jonka käyttöä esimerkiksi käyttöjärjestelmä säätelee. RAM-muisti on lyhytaikaista muistia, jota lähes kaikki sovellukset tarvitsevat toimiakseen ja jonka käyttöä säätelee yleensä käyttöjärjestelmä. Massamuisti on pitempiaikaisen tiedon varastointiin erikoistunutta muistia, jonka käytön rajoittaminen on yleensä käyttöjärjestelmän asetuksilla mahdollista.

Tietokoneen oheislaiteväylät ja -liitynnät mahdollistavat tiedonsiirron eri tietokoneiden, verkkojen ja käyttäjien välillä. Tiedonsiirtoa on yleensä mahdollista rajoittaa käyttöjärjestelmien ja laitteiden verkkoasetuksilla ja oheislaitteiden käyttöoikeuksilla.

Koska tiedonsiirrossa käytettävien protokollien suoritukseen tarvittavat resurssit kuten prosessoriaika ja muistin määrä, kasvavat abstraktiotason kasvaessa, tulee näiden resurssien puute korkeamman tason protokollien tiedonsiirtonopeuden esteeksi. Tästä johtuen esimerkiksi prosessoriajan ja muistin käytön rajoituksilla on vaikutus tiedonsiirtonopeuteen. Yksittäisen resurssin käytön rajoittamisen lisäksi on siis tarkasteltava myös kokonaisuutta, jotta haluttu suorituskyky saadaan laitteista ja alijärjestelmistä irti.

Palvelua tuottavissa laitteissa on kaikkien näiden resurssien käyttöä syytä rajata siten, että yksi huonosti käyttäytyvä palvelin ei saa kokonaisuutta polvilleen. Samoin yhden laitteen sisällä ei yksi prosessi saisi saada koko laitetta toimimattomaksi käyttämällä kohtuuttomasti prosessoriaikaa tai RAM-muistia. Se, kuinka paljon palvelimen prosessi tai alijärjestelmän tietokone voi käyttää yhteistä jaettua resurssia, kuten tiedonsiirtokapasiteettia, prosessoriaikaa tai muistia, on mitoituskysymys. Palvelimen prosessien prosessoriajan ja muistin käyttö voidaan rajata siten, että resurssit riittävät tietylle lukumäärälle palveluprosesseja, ja alijärjestelmän tietoliikenneyhteydet voidaan mitoittaa siten, että siirtokapasiteetti riittää tietylle lukumäärälle yhtäaikaisia palvelupyyntöjä.

Resurssien käytön valvonnalla voidaan havaita järjestelmän virhetilanteita, jotka voivat olla tahattomia, esimerkiksi ylläpidon vahinkoja tai tahallisia hyökkäyksiä tai järjestelmän väärinkäyttöä. Turvallisuuden kannalta resurssin käytön rajat olisi syytä asettaa siten, että oikean toiminnan aiheuttamat rajan ylitykset (ns. false positive) olisivat mahdollisimman harvinaisia. Myös järjestelmän väärän toiminnan jääminen rajojen sisäpuolelle (ns. false negative) tulisi olla mahdollisimman harvinaista. Järjestelmän toimintaympäristön muutokset ja käyttöasteen kasvu aiheuttavat muutoksia resurssien käyttöön, joten myös resurssien käytön rajoituksia on syytä tarkistaa ja säätää riittävän usein.

Tietokoneiden laskentateho ja muistien koot kasvavat niin sanotun Mooren lain mukaan. Tästä johtuen myös ohjelmistojen määrä on voinut kasvaa siten, että olemassa olevien toiminnallisuuksien ja toteutusten päälle on rakennettu uutta ja entistä helppokäyttöisempää toiminnallisuutta. Tämän abstraktiotason kohoamisen seurauksena myös hyökkäykset kohdistuvat ja käyttävät hyväkseen yhä korkeamman tason elementtejä. Esimerkiksi perinteinen verkkoliikennettä suodattava palomuuri ei estä nykyisin yleisiä HTTP-, HTML- tai sähköpostiprotokollia vastaan tehtyjä hyökkäyksiä, sillä lähes kaikki TCP/IP-palomuurit sallivat näiden protokollien käytön. Siksi on odotettavissa, että kun uutta helppokäyttöistä tekniikkaa (XML ja HTTP:n päällä kulkevat RPC-etäkutsut) otetaan käyttöön, sitä vastaan myös hyökätään. Tätä täytyy pyrkiä estämään uusilla mekanismeilla. Myös matkapuhelin ja PDA-laite tarvitsevat tulevaisuudessa kehittyneen palomuurin.

WLAN-älypuhelimiin (Nokia Series 80) onkin jo saatavilla ainakin Symantec:n palomuuri- ja virustorjuntaohjelmisto, joka estää tunkeutumisen yritysverkkoihin puhelimen kautta, ominaisuuksina mm. etähallinnointi sekä tietoturvakäytäntöjen määrittäminen ja konfigurointi.

Abstraktiotason nopea kasvu ja entistä vihamielisemmät sovellusympäristöt ovat paljastaneet lisäksi sen, että kaikki olemassa olevat ohjelmat ovat sisältäneet sellaisia ohjelmointivirheitä, joiden kautta hyökkääjä on voinut suorittaa kohteessa haittaohjelmia. Näiden ohjelmointi-virheiden korjaus ja sovellusten päivitys on yleiskäyttöisissä järjestelmissä nykyisin helppoa, mutta suljetuissa ja sulautetuissa järjestelmissä, kuten matkapuhelimissa, se voi olla mahdollista vain kolmannen osapuolten ohjelmistoille. Resurssien käytön rajaamisella: RAM-muistin luku-, kirjoitus- ja suoritusoikeuksien valvonnalla tai ohjelma-tiedostojen digitaalisilla allekirjoituksilla, haavoittuvaisuuksien hyödyntämistä on saatu hankalammaksi. Näitäkin rajoituksia on onnistuttu kiertämään korkeamman tason protokollia (HTML) ja ohjelmointikieliä (JavaScript) käyttämällä. Lisäksi protokollien ja ohjelmistojen päältä löytyy vielä käyttäjän tai ylläpitäjän roolissa ihminen, joka on erilaisin keinoin harhautettavissa – varsinkin, jos hän ei erota järjestelmän oikeaa toimintaa virhetilanteesta.

Koska nykyiset yleiskäyttöiset tietokonearkkitehtuurit ovat osoittautuneet pohjimmiltaan epäluotettaviksi, tietokone- ja erityisesti sisältöteollisuus on suunnittelemassa kryptografisesti suojattua turvallista tietokonearkkitehtuuria (Trusted Computing Group), jossa ohjelmien suoritusta ja muita oikeuksia voisi tarkemmin rajata. Tämä valta suorituksen rajoittamiseen on kuitenkin kyseenalaistettu, sillä sitä on liian helppo käyttää väärin pelkästään taloudellisten etujen ajamiseen, joten sen tulevaisuus avoimissa järjestelmissä ei ole mitenkään varmaa. Sen sijaan suljetuissa järjestelmissä, kuten matkapuhelimissa tai mediapäätelaitteissa (maksu-TV) tällainen arkkitehtuuri on mahdollisesti toimivampi. Suljetuissa järjestelmissä uhkat, kuten maksukorttien väärentäminen, voivat olla hyvin erilaisia kuin avoimissa järjestelmissä.

4.2.6.1 Palvelimien suojaamisesta käytännössä

Palvelimella tarkoitetaan ohjelmistoa tai tietokonetta ohjelmistoineen, joka tuottaa palveluita muille (asiakas-) ohjelmistoille, tietokoneille ja käyttäjille. Palvelut sisältävät yleensä tiedon hakua, muokkaamista ja jakelua. Palvelun tuottaminen turvallisesti vaatii aktiivisia ylläpitotoimia, jotka ovat osittain toteutuskohtaisia ja jotka muuttuvat sitä mukaa, kun uusia hyökkäyksiä ja haavoittuvaisuuksia löydetään. Erilaisten palvelualustojen ylläpitotoimet ovat erilaisia, parhaat käyttö- ja ylläpitotavat kehittyvät myös ajan mukaan jne.

CERT-FI on Viestintävirastossa toimiva kansallinen CERT (Computer Emergency Response Team) -ryhmä, jonka tehtävänä on tietoturvaloukkausten ennaltaehkäisy, havainnointi, ratkaisu sekä tietoturvauhkista tiedottaminen [FICORA]. Palvelinten ylläpitäjien on syytä seurata tällaista ajankohtaista ja yleiseen tietoturvallisuuteen liittyvää tietoa. Esimerkiksi CERT-FI:n ”vuosikatsaus 2004” mukaan mm. matkapuhelimiin kohdistetut haittaohjelmat

kehittyvät käytännöllisempään suuntaan, joten matkapuhelimiin pääseviä ohjelmia on syytä huolellisesti kontrolloida useilla tahoilla, kuten mobiilipalveluiden palvelimissa. Yleensäkin organisaatioiden varautumistoimet Internetin uhkia vastaan korostuvat jatkossa ja varautumistoimet vaativat yhä enemmän aktiivisia toimia ja tilanteiden harjoittelua. IRT (Incident Response Team) -ryhmien käyttö korostuu.

Palvelun tuottavan palvelimen suojaaminen on jatkuva prosessi. Suunnitteluvaiheessa palvelun tuottavien protokollien, verkkoarkkitehtuurin, palvelinalustan jne. valinnassa on kiinnitettävä huomiota palvelun turvallisuustekijöihin. Palveluiden arvo yrityksen toiminnalle on myös syytä arvioida, jotta kriittisimmät toiminnot osataan suojata niiden arvoa vastaavalla tavalla. Yleisiä protokollia SMTP, POP, IMAP, HTTP, TELNET tai SMB ei ole syytä käyttää selkokielisinä verkkoliikenteessä, mikäli siirrettävä informaatio voi olla luottamuksellista ja verkko epäluotettava.

Palvelun tuottamiseen tarvittavan ja palvelun yhteydessä syntyvän tiedon varmuuskopiointi ja pääsynvalvonta toteutetaan, jotta palvelun saatavuus varmistuu halutulle tasolle ja jotta lakisääteiset velvollisuudet tulee hoidettua. Palvelinalustan eli tietokonearkkitehtuurin, käyttöjärjestelmän ja itse palvelinohjelmiston valintaa tehdessä on hyvä ymmärtää oma osaamisen ja tietämyksen taso ja käyttää julkisesti saatavilla olevaa tietoa alustan turvallisuusominaisuuksista. Turvallinenkin ympäristö rapautuu ajan kuluessa, jos sitä ei osata ylläpitää. Palvelun kokonaisuuden suunnittelussa on myös syytä kiinnittää huomiota siihen, että mahdollisimman moni palvelun osa voidaan tuottaa jonkun standardin mukaisilla laitteilla ja ohjelmistoilla, jolloin yksittäisen komponentin vaihto toiseen, kenties turvallisempaan, on mahdollista myös palvelun käytön aikana. Verkkoon kytketyille palvelimille on yleensä olemassa toteutuskohtaisia sääntöjä ja hyvän ylläpitotavan ohjeita, joita on syytä noudattaa.

Palvelun tuottavan järjestelmän monimutkaisuus on nykyisin muodostunut ongelmaksi, joten suunnitelmien ja toteutusten yksinkertaistamiseen on syytä panostaa. Palvelualustan laitteista, käyttöjärjestelmästä ja ohjelmistoista on syytä karsia kaikki halutun palvelun kannalta ylimääräiset ominaisuudet pois. Valitettavasti kuitenkin monet turvallisuutta lisäävät ominaisuudet: varmuuskopiointi, salaus-protokollat, VPN-laitteet ja -ohjelmistot, palomuurit ja virustentorjuntaohjelmistot, tekevät järjestelmästä monimutkaisemman ja siten myös mahdollisesti haavoittuvaisemman. Mitä enemmän järjestelmässä on tartuntapintoja, sitä herkemmin sitä vastaan voidaan hyökätä. Ylläpitäjän on kuitenkin osattava toimia myös virhetilanteissa, joten kokonaisuuden ja yksittäisten komponenttien toiminnan ymmärtäminen on tärkeää. Mitään sellaista komponenttia, jonka toimintaa ei ymmärretä, ei ole syytä ottaa käyttöön palvelimissa. Erillisen testijärjestelmän käyttämistä suositellaan, koska siellä sekä palvelun kehittäjät että ylläpitäjät voivat kokeilla muutoksia vaarantamatta tuotannossa olevaa järjestelmää.

Kun palvelin on toiminnassa, ylläpitäjän täytyy tarkkailla sen toimintaa säännöllisesti**,** ainakin lokitietoja tutkimalla. Lisäksi palvelimen komponenttien toimintavirheitä ja turvallisuus-puutteita on syytä seurata valmistajan ja viranomaisten tiedotteista ja käyttäjäyhteisöjen keskustelupalstoilta. Ohjelmistojen ja käyttöjärjestelmien päivityksistä on tehtävä rutiininomaisia erityisesti julkiseen verkkoon liitetyille palvelimille.

Palvelutuotannossa yritysten väliset riippuvuudet monimutkaistavat kokonaisuuden hallintaa, samoin kuin palvelimenkin hallintaa. Mikäli palvelun tuotannossa joudutaan luottamaan kolmansien osapuolten palveluihin, on näiden pettämiseen syystä tai toisesta hyvä varautua.

Esimerkiksi Internet-yhteyden tarjoajan tietoliikenne-, sähköposti- tai nimipalvelussa voi esiintyä yllättäviä häiriöitä, joiden vaikutus liiketoimintaan on tarkastettava etukäteen. Ylläpidon toimintaa häiriötilanteissa on myös syytä suunnitella ja harjoitella etukäteen.

Koska myös yritysten sisäisiin uhkiin tulee varautua, palvelimen ja järjestelmän laillisten käyttäjien (ja ylläpitäjien) sallitut ja kielletyt toimenpiteet on hyvä olla yrityksen sisällä yleisesti tiedossa. Myös mahdolliset lakien asettamat vaatimukset esimerkiksi henkilötietojen ja henkilökohtaisten viestien käsittelylle on oltava järjestelmän ja palvelun parissa työskentelevien tiedossa. Mikäli työntekijät ymmärtävät oman vastuualueensa ja tehtävänsä, he todennäköisimmin myös havaitsevat, jos joku taho yrittää käyttää niitä väärin. Sama pätee myös palvelimen toimintoihin. Kun palvelimen oikeasta toiminnasta ymmärretään riittävästi, myös virhetilanteita voidaan havaita.

Esimerkki suojauksesta: Mobiilipalvelinten suojaukseen liittyviä toimia:

- Palvelun tuottavien protokollien ja mobiilialustojen valinta oman tietämyksen, standardien ja muiden suositusten mukaan. Palvelujen (tarttumarajapintojen) karsinta vain oleelliseen..
- Estä mobiilikäyttäjän erehtyminen palvelimen identiteetin suhteen. Käytä palvelin-varmenteita, joissa palvelimen verkkotunnus kuvattu. Varmista että mobiilikäyttäjä huomaa selvästi minkä verkkotunnuksen palveluun hän on pyrkimässä.
- Keskitetty käyttöoikeuksien hallinta ja valvonta. Varmista kaksisuuntaisen tunnistuksen toteutuminen mobiililla päätelaitteella.
- Ohjelmistojen päivitykset turvallisin väliajoin. Turvallisuusohjelmistojen, kuten palomuurin ja virustentorjuntaohjelmiston käyttö. Palvelintietojen varmuuskopiointi, lokitietojen keräys.
- Mahdollisten mobiiliuhkien jatkuva havainnointi ja ideointi. Riippuvuuksien ja kompleksi-suuden hallinta jakamalla toiminnallisuuksien toteutus eri laitteiden kesken.

4.2.6.2 Hyökkäyksen havaitsemiskäytännöistä

Yleinen lähestymistapa järjestelmää kohtaavien hyökkäysten havaitsemiseksi on:

- Seuraa automatisoidusti ja systemaattisesti järjestelmää kohtaavia yllättäviä tai epäilyttäviä tapahtumia ja verkon liikennettä. Älä unohda fyysistä suojausta ja sen murtamisen havaitsemista. Käytä muiden ihmisten havaintoja koko ajan täydentämässä omia havaintojasi ja vertaa niitä.
- Tutki tarkemmin, jos jotain epätavallista on sattunut järjestelmässä.
- Käynnistä valmiiksi testatut suojausmekanismit, jos epäilet, että järjestelmään on tunkeuduttu.
- Muuta käytäntöäsi, jos uhkat, järjestelmäsi tai sen vaatimukset muuttuvat.

Hyökkäysten havaitsemisjärjestelmät perustuvat verkkoa, palvelinta tai työasemaa kuuntelevasta analysointilaitteesta (sensori) tai sovelluksesta sekä hallintajärjestelmästä. Yleensä sensori tutkii kaiken liikenteen ja tekee päätelmiä valmiiden hyökkäystunnisteiden tai verkon käyttäytymistä tutkivan keinoälyn pohjalta. Tunnisteisiin perustuvat hyökkäykset ovat melko selkeitä ja niihin löytyy valmiit toimintasuunnitelmat. Verkkosensoritkin ovat melko yleisiä. Tietoturvaohjelmistojen toimittajat tuovat IDS-ominaisuudet mukaan omiin paketteihinsa. On huomattava, että salatut yhteydet voivat estää IDS-laitteita löytämästä kielletyn verkkoliikenteen viestit.

Hallintajärjestelmässä ylläpidetään hyökkäystunnisteita sekä sensoreiden säännöstöjä. Toimittajat päivittävät tunnisteita vaihtelevalla reagointinopeudella, mutta pääosin päivitys-nopeus on riittävä. Koko ICT-arkkitehtuurin IDS-analyysi ja raportointi ovat kuitenkin edelleen haasteellisia ja vaikeita toteuttaa.

Järjestelmien omat hallintasovelluksetkin tekevät (pääosin) hyvin alustavan analyysin verkkotapahtumien poikkeavuuksista. Useissa tapauksissa lopullisessa analyysissä tarvitaan kuitenkin vahvaa osaamista, jolla tulkitaan ongelman vaikutus käytössä olevaan ympäristöön. Väärinkäytöstapauksissa tulkitseminen vaatii aina työntekijöiden vahvaa osaamista. Haasteena on kuitenkin edelleen verkon poikkeavuuksista havaitut hyökkäykset. Tietyt ominaisuudet voidaan tutkia useassa eri pisteessä. Esim. vertaisverkkoliikenne voidaan napata IDS-, proxy-, virustorjunta-, palomuurilaitteessa tai jossain älykkäässä kytkimessä. Tällöin kokonaisuuden hallinnan osaaminen korostuu.

Useita pienimuotoisia hyökkäystietokantoja on perinteisesti käytetty yrityksissä ja organisaatioissa saamaan ulkoiset tietoturvauhkat hallintaan. Tällainen työ on kuitenkin turhauttavaa aina uusien hyökkäysten ilmaantuessa ilman ennakkovaroitusta. Maaliskuun 2005 lopussa suuret tietoliikenneyhtiöt ovat päättäneet jakaa keskenään tietoa tietoturva-hyökkäyksistä Fingerprint Sharing Alliance:ssa [ARBOR]. Tämä yhteenliittymä kerää ja analysoi tiedot kaikista potentiaalisista hyökkäysyrityksistä ja automaattinen järjestelmä

varoittaa kaikkia tahoja mahdollisimman varhaisessa vaiheessa, esimerkiksi palvelun-estohyökkäyksistä (Tietoviikko). Järjestelmässä erityinen ohjelmisto valvoo verkkoja ja pyrkii tunnistamaan liikenteessä ilmenevät piikit tms., jotka viestivät epänormaalista toiminnasta ja tällainen aktiviteetti kirjataan niin sanotuksi sormenjälkitiedostoksi, jota voidaan vertailla muihin hyökkäyksiin.

Olisi hyödyllistä, jos tulevaisuudessa esim. verkko-operaattorien havaitsemista aktiivisista hyökkäyksistä tulisi reaaliaikainen tieto myös muille palveluntarjoajille ja mahdollisesti loppukäyttäjän laitteelle (esim. tekstiviestinä).

4.2.6.3 Virustorjunta ja haittaohjelmat käytännössä

Taulukko 10. Haittaohjelmat alatyyppeineen. Lähteenä [VAHTI3/2004] ja [Korhonen].

Haitta-ohjelma	**Alatyypit/leviäminen**	**Merkitys langattomassa päätelaitteessa**	**Perustorjunta**
Virukset – kopioituu ja levittää itseään uusiin kohteisiin	Tiedostovirukset – tarttuvat ohjelmatiedostoihin ja leviävät kaikilla tavoilla, joissa siirretään ohjelmatiedostoja.	Ei ongelmaa vielä Suomessa. Ongelmat lisääntyvät mobiilivirusten ja ladattavien ohjelmien yleistyessä. **Lasco**-virus/mato.	**Virusskannauksella** ja **hävityksellä**.
	Makrovirukset – tarttuvat sovellusten dokumenttitiedostoihin. Leviää dokumenttien mukana käyttö-järjestelmästä riippumatta.	Ei ongelmaa vielä ainakaan Suomessa. Haitat voivat lisääntyä toimistosovellusten lisääntyessä langattomissa päätelaitteissa.	**Estämällä** makrojen suoritus, käyttämällä tiedostomuotoja, joissa ei makroja
Madot (virusten osajoukko) – leviävät käyttämällä tarkoituksellisesti verkkoyhteyttä	Komentojonovirukset – hyödyntää kohdejärjestelmän komentokieliä (scripts).	Ei ongelmaa vielä ainakaan Suomessa.	Mm. **asetuksilla**.
	Viestimadot – leviää MMS-viestissä, sähköpostissa tai liitteessä.	**CommWarrior** löydetty Suomesta (lähettää MMS viestejä ilman lupaa). **Mabir** lähettää MMS viestejä. Ei varsinaista ongelmaa vielä Suomessa.	Palomuurit, autopäivittyvät virusskannaukset, verkon segmentointi ja yhdyskäytävien virussuojaus, järjestelmien valinta, tietoturvapäivitykset
	Verkkomadot – käyttävät itsenäisesti hyväkseen verkkoyhteyttä.	Bluetoothia hyödyntäviä matoja ovat **Lasco** (saastuttaa ohjelmatiedostoja), **Cabir**, **CabirDropper** (tuhoaa muita ohjelmia) ja **CommWarrior**. Cabir löydetty Suomesta, mutta ei vielä varsinaista ongelmaa.	
Troijan hevoset – tekevät salassa jotain arvaamatonta	Voivat avata kohdekoneelle takaportin. Voivat lähettää eteenpäin tietoa koneesta tai käyttäjän toimista. Voivat tuhota tietoa. Tulevat mm. toisen ohjelman mukana.	Aiheeton laskutus ja palvelujen käyttö. **Brador** avaa takaoven. **Dampig** tuhoaa järjestelmätiedostoja. **Drever** estää virustorjuntaohjelmistojen toiminnan. **Fontal** estää puhelimen käynnistyksen. **Locnut** tuhoaa käyttöjärjestelmän. **MGDropper** aiheuttaa ohjelmiin häiriöitä. **Mquito** lähettää SMS viestejä.	Mm. käyttäjän **valveutuneisuus** ohjelmistoasennuksissa.
Vakoilu- ja mainos-ohjelmat	Vakoilukomponentteja sisältävät ohjelmat. Vakoiluominaisuudesta saatetaan kertoa, mutta jotkut asentuvat salaa.	Ei merkittäviä ongelmia havaittu mobiililaitteissa.	**Torjuntaohjelmistot**, turvallinen **tiedostojärjestelmä** ja käyttäjän **valveutuneisuus**
Huijaus-viestit (Hoax), ketjukirjeet ja pilailuohjelmat	Huijausviestit mm. tuhlaavat aikaa, pyytävät poistamaan tiedostoja. Pilailuohjelmat antavat virheellisiä ilmoituksia. Leviävät hyväuskoisten käyttäjien lähettäminä.	Huijausviestejä voi paikoin olla liikkeellä paljonkin.	Mm. käyttäjän **valveutuneisuus**.

Älypuhelimessa haittaohjelmat voivat levitä esimerkiksi pelien ja musiikkiohjelmien välityksellä mm. Internet-yhteyden, oheislaiteyhteyden, tai työasemasynkronoinnin kautta. Näihin riskeihin on varauduttava suunnittelulla ja hallitulla käyttöpolitiikalla.

Haittaohjelmilla tarkoitetaan vahingollisia tietokoneohjelmia. Älypuhelimen ja PDA-laitteen lähitulevaisuudessa relevantit haittaohjelmat luokitellaan taulukossa 10.

Virukset aiheuttavat ainakin epäsuoraa vahinkoa kuluttamalla levytilaa, aiheuttamalla yhteensopivuusongelmia ja hidastamalla laitteen toimintaa. Ne sisältävät usein ohjelmointivirheitä, jotka saattavat aiheuttaa vahinkoa viruskirjoittajan tahtomattakin. Jos laite-järjestelmätoimittajat ottaisivat tietoturvallisuuden merkityksen jo suunnitteluvaiheessa (mm. arkkitehtuureissa) mahdollisimman hyvin huomioon, asiakastyytyväisyys kasvaisi väärinkäytösten ja jälkikäteen toteutettavan suojaustarpeen vähentyessä.

Suomessa käyttäjien matkapuhelimista on jo löytynyt virus/mato nimeltään CommWarrior, joka toimii Symbian Series 60 -puhelimissa ja leviää MMS-viestien ja Bluetoothin välityksellä. Myös Cabir-mato on löydetty Suomesta. Roskaviestit ja virukset on huomioitava matkapuhelinten hyödyllisen käytön turvaamisessa mm. matkapuhelinverkon yhdyskäytävissä ja sähköpostipalvelimissa käytettävin suodattimin.

Verkko-operaattorin on suojattava verkkonsa reunat sekä laitteet virustorjuntajärjestelmin. Tämäkään ei yksin riitä, vaikka kyseessä onkin erillisverkko, josta on Internetiin pääsy vain tietyistä kohdista. Yksittäinen toimija ei yleensäkään pysty ottamaan koko vastuuta tietoturvasta, vaan hyvä suojaus vaatii myös operaattorien välistä päivittäistä ja kansainvälistä yhteistyötä. Verkoissa on suojauduttu mm. monitoroimalla seuraavien protokollien avulla siirrettävää data – SMTP, POP3, HTTP, FTP, IMAP4, NNTP ja SOCKS.

Jo nyt on saatavilla virustorjunta-, haittaohjelmatorjunta- ja palomuuriohjelmistoja älypuhelimiin (mm. joihinkin Symbian puhelimiin). Virustorjuntaohjelmistoja älypuhelimiin myyvät jo ainakin F-Secure, Symantec, Trend Micro ja McAfee (Tietokone 4/2005). Valitettavasti näiden täydellinen käyttö tausta-ajona voi hidastaa puhelimen muuta toimintaa huomattavasti rajallisen laskenta- ym. kapasiteetin vuoksi. Tulevaisuudessa torjuntaohjelmistojen käytön tarve kannettavissa päätelaitteissa on huomattavasti lisääntymässä. Erittäin tärkeä teknologinen suojaus on laitteen muistien ominaisuudet, mm. suljetut muistialueet, joilta ei voi viitata ulos, ohjelmia suorittamattomat alueet, ROM-alueet, jne. Sekä laite- että SW-toteutuksia näihin on olemassa. Ohjelmien toimintaa on syytä tarkkailla menetelmillä, joilla myös toistaiseksi tuntemattomia viruksia pystytään tehokkaasti havaitsemaan (esim. Norman). Uudet haittaohjelmat leviävät todella nopeasti, joten pelkkä virustunnisteen etsintä ei riitä.

Esimerkki haittaohjelmien torjunnasta: Seuraavat toimet auttavat hallitsemaan haittaohjelmien torjuntaa palvelunkehitys- ja tuotanto-organisaatioissa:

- Työasemia ja palvelimia ylläpitämään on erikoistunut tukiorganisaatio joka tuntee ”kaikki” haavoittuvuudet. Laitteet varustetaan haittaohjelman torjuntaohjelmalla. Tietoturvapäivityksien automatisointi ja seurantaprosessit erittäin tärkeitä. Koulutus myös käyttäjille.
- IDS-järjestelmä LAN:ssa. Lisäksi LAN:n kriittiset palvelimet, testi- ja tuotantojärjestelmät sekä työasemat tulee erottaa omiin segmentteihinsä. Haittaohjelmien mahdollisuuksien rajaus laite- ja verkkoarkkitehtuurin keinoin.
- LAN eristettävä verkon liittymäpisteissä haittaohjelmatorjunnalla, palomuurilla ja reitittimen turvaominaisuuksilla. Etäyhteydet on turvattava erikseen. Matkapuhelinverkon yhdyskäytäviin voidaan asentaa torjuntaohjelmistot, jotka poistavat käyttäjäviesteistä haittaohjelmat.
- Älypuhelimiin ja PDA-laitteisiin samat torjunnat kuin kannettaviin työasemiin. Huolehditaan päätelaitteen ohjelmien ja torjunnan turvallisista asetuksista ja automaattisista päivityksistä (esim. tehtaalla esiasennetut torjuntaohjelmat, organisaation toimet). Käyttäjiä kielletään asentamasta tuntemattomia ohjelmia älypuhelimiin ja PDA-laitteisiin.

5. Mobiilipalvelun kehitystyöhön liittyvät erityispiirteet

Edellä mainittujen uhkien ja ratkaisujen monimutkaisuuden vuoksi mobiileihin päätelaitteisiin suunnattujen palveluiden kehittäminen on vaikeaa. Tämä on tietenkin osaltaan hidastamassa kunnollisten palveluiden syntymistä ja käyttöönottoa. Tämän vuoksi tässä luvussa pyritään keskittymään (erityisesti palvelinpään) palvelunkehittäjän erityisongelmiin ja esittämään hyviksi havaittuja tai hyviksi arvioituja tietoturvan ratkaisumalleja ja prosesseja. Myös tärkeimmiksi katsotut päätelaitteisiin liittyvät ongelmat ja ratkaisut käydään läpi.

Luvussa tutkitaan myös tietoturvan integroituvuutta ja helppokäyttöisyyttä. Miten nämä voitaisiin parhaiten toteuttaa palvelunkehittäjän näkökulmasta? Luvussa käsitellään yksityiskohtaisemmin kaikkia palvelunkehitysprosessin vaiheita, mm. ideointi, suunnittelu, testaus, toteutus, käyttöönotto ja ylläpito.

5.1 Luottamusmallit

Tässä selvityksessä tavoitteena oli selvittää miten arvoketjussa tai pikemminkin arvoverkossa vastuu siirtyy toimijalta toiselle arvoketjun loppupäästä (kuluttajapää) siirryttäessä kohti alkupäätä. Tähän kysymykseen vastaaminen on osoittautunut erityisen vaikeaksi, sillä jokaisessa palvelussa arvoverkko on erilainen ja lisäksi jopa kilpailevissa palveluissa (samanlainen palvelu) toteutukseen voi olla valittu täysin erityyppinen liiketoimintamalli ja erilaisia toimijoita. Yrityshaastatteluissa ei päästy pureutumaan tähän, sillä sellaista case-esimerkkiä ei voitu osoittaa, josta olisi voitu avoimesti puhua tai jonka edes kaikki haastateltavat olisivat jotakuinkin tunteneet.

Uuden tyyppisiä luottamusmalleja tulee rakentumaan jatkossa uusien palvelujen ympärille. Esim. Nokian esittämässä Visual Radio -palvelussa toimijoita voivat olla mm. radioasema, palvelukehittäjä, verkko-operaattori ja laitetoimittaja, joilla on siis oltava luottamussuhde keskenään. Mobiili TV:ssä vastaavasti mm. TV-yhtiö, TV-verkko-operaattori ja mobiiliverkko-operaattori voivat saada lisäarvoa toisiltaan. Voisiko luottamuksen varmistamista varten käyttää riippumatonta toimijatyyppiä, ns. luotettua kolmatta osapuolta?

5.2 Luottamuksen rakentaminen

Luottamuksen rakentaminen vaatii yhteistyötä eri toimijoiden kesken, sen lisäksi, että eri toimijat omilla sisäisillä prosesseillaan pyrkivät näihin päämääriin. Esim. tietohävikistä 80 % aiheutuu käyttäjien toiminnasta (johtuen mahdollisesti heidän puutteellisesta informoinnistaan) ja vain 20 % tietoteknologiasta [YRTI]. On selvää, että luottamuksen kehittämiseksi

yrityksissä on kiinnitettävä huomiota siihen, miten yritykselle ja asiakkaille tärkeitä tietoja säilytetään ja toisaalta miten niitä jaetaan. Epäselvät tiedon käsittelytavat saattavat aiheuttaa sopimusrikkomuksia tai jopa lakien vastaista toimintaa.

Järjestelmien ja verkkojen toimintahäiriöt vaikeuttavat niiden hyödyntämistä ja estävät tehokkaan työskentelyn. Käytettävyyden heikkeneminen laskee palvelutasoa ja voi huonontaa yrityksen mainetta. Häiriötilanteissakin yrityksen on tarpeen varautua säilyttämään toiminnan kannalta riittävä palvelutaso.

Kuluttajien luottamus uusiin *sähköisiin pankkipalveluihin* perustuu [FIBA] mm.:

- luottamukseen pankkeihin instituutiona,
- kokemuksiin aiemmista pankkipalveluista,
- pankkipalveluiden toiminnallisuuteen ja mahdollisiin vakaviin ongelmiin,
- muiden käyttäjien mielipiteisiin.

Suomessa pankkeihin luotetaan sähköisten pankkiasiointipalvelujen tarjoajana kansainvälisessä vertailussa erittäin hyvin. Asiakkaiden luottamusta sähköisiin pankkipalveluihin on rakennettu luomalla käyttäjille tiettyjä tapoja toimia (esim. maksupalvelut, puhelinpankki), sekä kehittämällä palveluiden tietoturvaa ja luotettavuutta sekä tiedottamalla niistä kuluttajille.

Monet pienet yritykset toimivat nykyään suurempien yritysten alihankkijoina tai ovat muutoin osa useamman yrityksen muodostamaa palvelukokonaisuutta. Tällaisessa verkostoituneessa toimintamallissa tärkeimmän yrityksen tieto-turvavaatimukset määrittävät kaikkien toimintaketjun yritysten tietoturvallisuuden minimitason [YRTI]. Usein tämä ”veturiyritys” myös tarkastaa muiden toimijoiden turvallisuusmenettelyt. Myös lainsäädäntö, viranomaisten ohjeet, mahdolliset sopimukset sekä alakohtaiset vaatimukset edellyttävät, että yrityksen henkilöstö on tietoinen yrityksen tietoturvavastuista ja käytännön menettelytavoista. Tietoturvan kehittäminen tulee olla osana yrityksen strategista suunnittelua ja tavoitteiden asettamista. Yrityksellä tulee olla tietoturvapolitiikka määriteltynä ja käytännönläheinen ohjeistus.

Käyttäjän sekä muiden palvelukehitykseen osallistuvien toimijoiden luottamusta valittuun palvelukonseptiin voidaan nostaa käyttämällä tunnettuja referenssitoteutuksia, parhaita työkaluja, soveltuvia menetelmiä ja standardeja tuotteen pohjana. Hyvin suunnitellut ja kommunikoidut pilottiprojektit sekä tunnettujen testausalustojen käyttö lisäävät luottamusta.

Arvoverkosto ja kunkin toimijan ansaitsemislogiikka tulisi olla alusta lähtien selvillä palvelunkehityksen aikana, samoin kuin loppukäyttäjän tulisi palvelua käyttäessään tietää, ketkä toimijat saavat rahaa, kun palvelua käytetään, ja kuinka suurin osuuksin. On huomattava, että lisäarvoksi jollekin verkoston toimijalle voi riittää tunnettuuden

lisääntyminen tai palvelun/pilotin avulla toteutettu markkinointi. On hyvä muistaa, että mobiilipalveluissa arvoverkostot ja ansaitsemislogiikat ovat usein edelleenkin kypsymättömiä, jolloin niiden selventämiseen on panostettava koko prosessin ajan.

Esimerkki teknologisista tekijöistä luottamuksen kasvattamisessa:

- käyttäjän ja palvelun tunnistaminen luotettavasti,
- tunnetun palvelualustan käyttö, levitettävien sisältöjen puhtauden varmistaminen,
- verkkoteknologian ja päätelaitteiden luotettavuus ja turvallisuusominaisuudet,
- testattujen teknologioiden (esim. OMA:n standardoimat) käyttö on suositeltavaa.

Koko palvelu voi romahtaa, jos valittu teknologia ei ole kypsä kaupalliseen hyödyntämiseen tai jos se rajoittaa toiminnallisuutta tulevaisuudessa. Kuluttajat voivat myös hyljeksiä palvelua, jos siihen liittyy roskaposti-tyyppisiä haittoja tai tekniikan epäluotettavaa toimintaa (sisältäen tietojärjestelmät ja verkot).

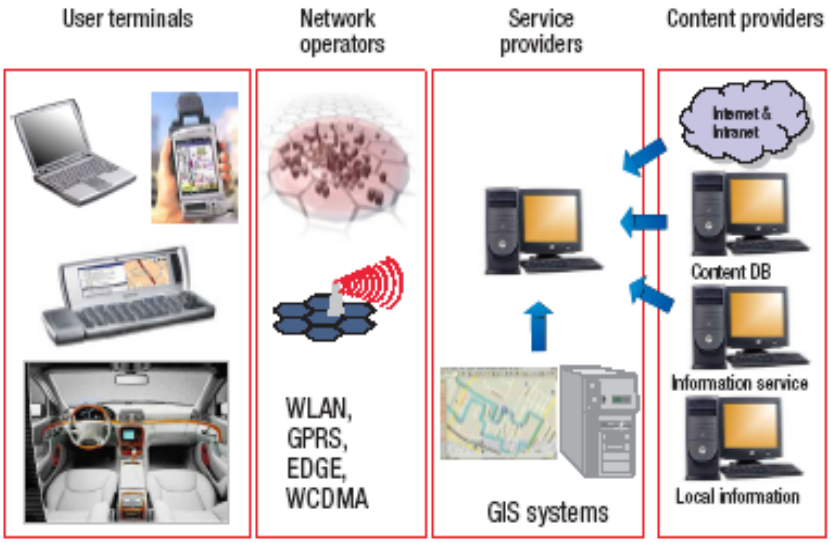
Muita luottamuksen kasvattajia ovat:

- sertifioitujen tuotteiden ja ammattilaisten käyttäminen,
- yrityksen olemassa olevat palvelut, aiempi hyvä imago ja maine, tietosuojan hoito,
- luotettavat toimijat, alihankkijat, luotetun kolmannen osapuolen käyttö, esim. lausunnot tietoturva auditoinneista,
- muiden käyttäjien positiiviset mielikuvat.

5.3 Yleistä pohdintaa palvelunkehityksestä

5.3.1.1 Toimijat – arvoverkko

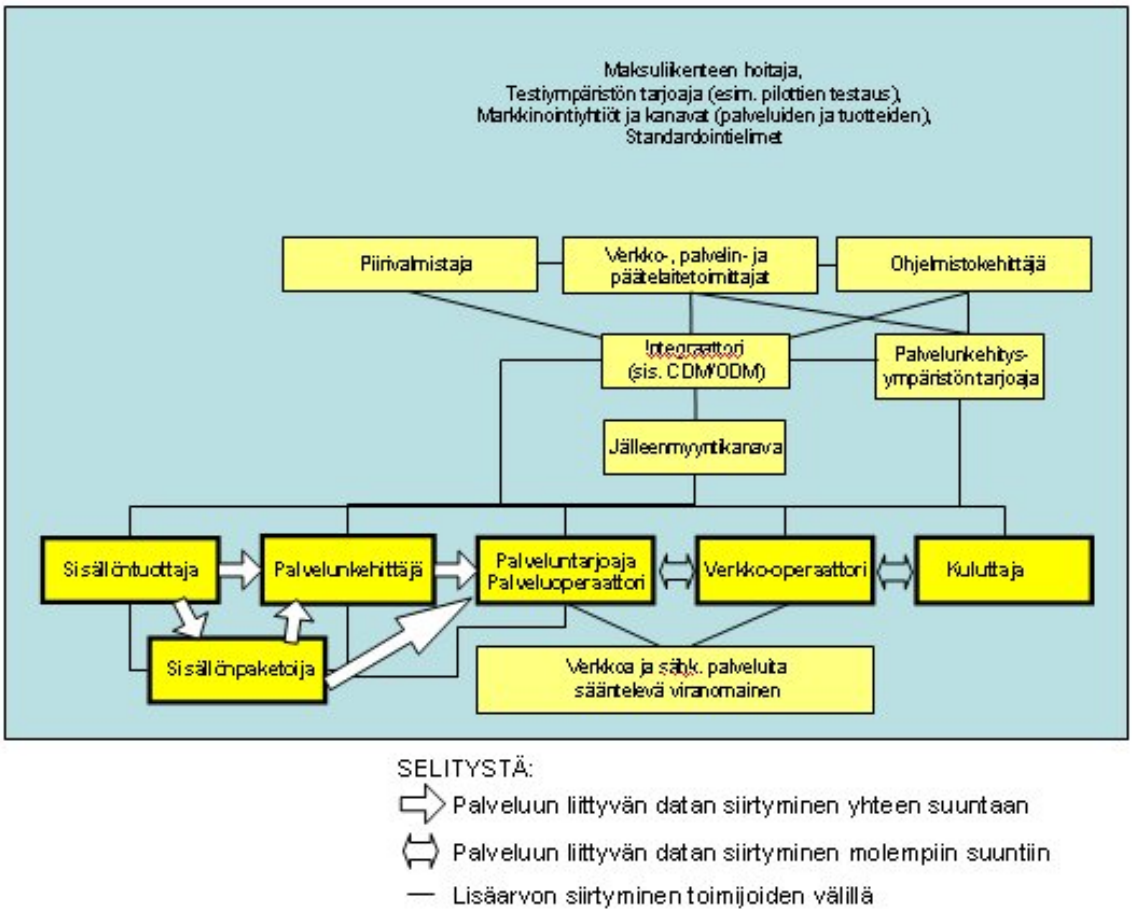
Arvoketjua mobiilipalvelun tarjoamiseksi on perinteisesti kuvattu esim. seuraavalla tavalla:



Kuva 7. Mobiilipalveluiden arvoketju. (Ote dokumentista [Alahuhta2005]).

Arvoketju alkaa olla jo hieman vanhentunut käsite. Kysymys on yhä enemmän liiketoiminta-ympäristöstä, jossa verkostoidutaan ja liittoudutaan yhä laajemmin markkinoille pääsemiseksi. Internetissä ansaintalogiikka käynnistyy usein suosittujen ilmaispalveluiden ympäriltä ja sama logiikka saattaa tarttua mobiilikäyttäjiin. Näin ollen kyseessä on oikeastaan arvoverkko, jossa kukin toimija voi hyötyä verkostosta eri tavoin.

Jäljempänä on kuvattu tätä esimerkillä, jossa mobiilipalvelussa tyypillisesti mukana olevat toimijat ja niiden väliset yhteydet näyttävät seuraavanlaiselta:



Kuva 8: Yksinkertaistettu geneerinen malli mobiilipalvelun arvoverkosta.

Esimerkki toimijoista: Yllä olevassa kuvassa tekijänoikeusjärjestöt (kuten Teosto) voivat sisältyä vasemmalla olevaan sisällöntuottaja-laatikkoon. Kuluttajat voivat tarvita palvelunkehitysympäristöä suoraan (oikealla), sillä älypuhelimille on jo saatavana PC-ohjelmistoja, joilla jopa tavallinen käyttäjä onnistuu muokkaamaan älypuhelimensa käyttöliittymän mahdollisimman yksilölliseksi kirjasintyylejä, grafiikkaa ja äänimaailmaa myöten.

Erittäin keskeinen toimija palvelu- ja tuotekehitysprosessissa on integraattori, joka kokoaa yhteen eri valmistajien ja kehittäjien toimittamat tuotteet yhdeksi toimivaksi palvelukokonaisuudeksi (ks. kuva yllä). Palvelunkehittäjä voi itsekin toimia integroijana ainakin jossain määrin, mutta yleensä tämän tyyppinen toiminta vaatii erikoistuneen tahon, joka on jo kerryttänyt tarpeellisen osaamisen ja teknisen ympäristön integroinnin toteutukseen ja testaukseen. Integraattori toimii palvelinpään kehitykseen liittyen usein suoraan palvelunkehittäjän tai palveluntarjoajan kanssa, jolloin erillistä jälleenmyyntikanavaa ei tarvitse käyttää. Lisäksi integraattorin käyttämien toimijoiden tuotteet ovat tyypillisesti muodostuneet hieman varhempien arvoketjujen tuloksena, kuten teknologia-alustat (HW ja SW) palvelin ja terminaali puolella, ja yleiskäyttöiset työkalu- ja sovellusohjelmistot ja piirit.

Palvelunkehittäjä on itse hyvin keskeisessä roolissa, koska sen täytyy koordinoida toimintansa mm. sisällöntuottajien edustajien organisaatioihin, sisällönpaketoijiin, integraattoriin, kehitys-ympäristön- ja palveluntarjoajiin. Palvelua ideoitaessa sekä suunnitteluvaiheessa arvoverkon aktiivisen osan tulisi muodostua mahdollisimman selkeäksi ja kestäväksi pitkällä tähtäimellä.

Esimerkki arvoverkosta: Toimivaksi todettu arvoverkko on matkapuhelinten soittoäänipalveluissa, joille Teosto r.y. on määritellyt lupaehdoiksi [TEOSTO] (yksinkertaistus):

- Teoksen kesto enintään 30 s, kattaen monofoniset, polyfoniset ja ääniteperäiset soittoäänet.
- Maksu on 12 % arvonlisäverottomasta kuluttajahinnasta, vähintään 0,10 euroa/lataus.

LUOTI-ohjelman käynnistystilaisuudessa tuli esille, että kuluttajapalaute tulisi käydä koko arvoketjun ylitse. Tämä edellyttää luonnollisesti hyvää yhteistyötä kyseisen palvelun kaikkien toimijoiden kesken. Samoin käytettyjen tietoturvaelementtien hinnan täytyy olla sopusoinnussa palveluhintojen kanssa, muutoin palvelu ei tule kannattamaan.

Palvelunkehittäjä ja -tarjoaja ovat keskeisessä roolissa uhkien torjujana. Alalle tulleet uudet toimijat saattavat kuitenkin olla pieniä suhteessa heille lankeamaan vastuuseen. Toisaalta monet innovaatiot (myös palveluissa) syntyvät pienissä yrityksissä, jotka haluaisivat ehkä itse toteuttaa omat keksintönsä. Siksi onkin syytä varmistaa viranomaisten taholta, että toimijoilla on riittävät edellytykset hoitaa toimintansa myös tietoturvallisesti. Käytännössä kysymys on resursseista. Kompleksisessa ympäristössä on yleensä aina suuremmat riskit ja enemmän tietoturva-aukkoja. Kaikkien on varmistettava, että käytössä on oikean skaalan tietoturva-palvelut ja käytännöt.

5.3.1.2 Tietoturvalähtöisyys

Tietoturvalähtöisyys voi organisaatiossa muodostua mm. riskinhallinnasta, strategisesta suunnittelusta ja resursoinnista.

Esimerkki: Yksi sovellus tietoturvalähtöisestä toiminnasta palvelun kehittämiseksi:

- Suojaa oma verkko.
- Perusta kehitysympäristö ja/tai testiverkko sekä eristä se (ainakin osittain).
- Etsi hyvät toimijat – tarkasta eri toimijoiden tietoturvan taso.
- Tutki toimitusketju (keneltä mikäkin osa hankittu, miten, jne.).
- Muista että tietoturva on mukana palvelukehityksen kaikissa vaiheissa.

5.4 Palvelunkehitysprosessista

Sähköisiä palveluita kehitettäessä toimitaan usein jonkun ennalta määritellyn prosessin mukaisesti. Palvelunkehitys koostuu eri vaiheista, joille kullekin on määritelty omat tavoitteensa ja toimintatapansa. Käytännössä palvelun kehittäminen tuottaa kuitenkin yleensä aina jonkinlaisia hallintaongelmia. Mikä olisi sopiva prosessikuvaus juuri tällaisen palvelun kehittämiseksi? Miten eri toimijat kommunikoivat ja mitä tietoja välittävät toisilleen? Käytännössä monet asiat saattavat edetä suunnittelematonta reittiä, jolloin prosessi on vain apuväline joka auttaa hahmottamaan tekemistä kokonaisuutena.

Erittäin tärkeä on muistaa, että vaikka palvelunkehitysprosessi olisikin hyvin määritelty, se ei koskaan ota huomioon kaikkia tietoturvaan liittyviä tekijöitä (jotka ovat ajan myötä muuttuvia). Ei voida tuudittautua toteamaan, että tietoturvasta on jo huolehdittu, vaan uusia uhkia ja keinoja on aina pysähdyttävä ajattelemaan uudelleen prosessin eri vaiheissa. Prosessi ei suojaa kaikilta uhkilta.

Kuva 9. Esimerkki palvelunkehitysprosessin vaiheista [LUOTI].

Tässä dokumentissa palvelunkehitysprosessin vaiheiksi on määritelty:

- Palveluidean/konseptin kehittely
- Palvelun suunnittelu
- Palvelun toteutus
- Palvelun testaus
- Palvelun käyttöönotto
- Palvelun ylläpito
- Palvelun edelleen kehittäminen
- Palvelun lopettaminen.

5.4.1 Tietoturvaratkaisujen sijoittuminen kehitysprosessin vaiheisiin

Seuraavassa taulukossa on sijoitettu tärkeimmät ratkaisut palvelukehitysprosessin eri vaiheisiin.

Taulukko 11. Tärkeimmät ratkaisut palvelukehitysprosessin eri vaiheissa.
Selitys: ”X”= yleisesti, ”x”= mahdollisesti.

	Ratkaisut	Pääuhkatyyppi	Soveltamisvaihe							
			Palvelun lopettaminen	Palvelun edelleenkehitt.	Palvelun ylläpito	Palvelun käyttöönotto	Palvelun testaus	Palvelun toteutus	Palvelun suunnittelu	Idean/konseptin kehittely
Sisällönsuojaus palvelussa	Median edelleen levityksen rajoittaminen	Tekijänoikeuksien loukkaukset		X	X	X		X		x
	Tallennetun datan salakirjoitus	Laitteisiin ja käyttäjään liittyvät uhkat	X	X	X	X	X	X	x	x
	Ohjelmien digitaalinen allekirjoittaminen ja verifiointi	Alkuperään ja eheyteen liittyvät uhkat			X	X	X	x		X
Hyökkäyksiltä suojautuminen palvelussa	Liityntä elektroniseen maksujärjestelmään	Maksuliikenteen uhkat	X	X	X	X	X	X	X	X
	Yksityisyyden suojaaminen	Identifiointiin ja datan luottamuksellisuuteen liittyvät uhkat	X	X	X	X	X		X	
	Palvelimien suojaaminen	Verkkoon ja palvelimiin liittyvät uhkat	X	X	X	X				
	Hyökkäysten havaitseminen	Verkkoon ja palvelimiin liittyvät uhkat		X	X	X	X			
	Haittaohjelmilta suojautuminen	Laitteisiin liittyvät uhkat		X	X	X	X	X	X	
Palvelunkehittäjän tietoturvaprosessi	Kolmannen osapuolen arviointimenetelmät	Palvelunkehitysprosessin uhkat		X			X	X		X
	Riskienhallinta	Palvelunkehitysprosessin uhkat	X	X	X	X	X	X	X	X
	Fyysiset turvaratkaisut, esim. varmuuskopiointi, tamper-resistant HW	Palvelunkehitysprosessin uhkat	X	X	X	X	X	X	X	
	Vikatilanteista toipuminen, suunnitelma	Palvelunkehitysprosessin uhkat		X	X	X	X	X	X	
	CERT-toiminta	Palvelunkehitysprosessin uhkat	x	x	X	x	X	X	x	
	Versionhallintajärj.	Palvelunkehitysprosessin uhkat		X	X	X	X	X	X	
	Tietoturva liiketoiminnan johtamisessa	Palvelunkehitysprosessin uhkat		X	X	X				X
	Tekn. pros. seuranta, parantaminen ja koulutus	Palvelunkehitysprosessin uhkat		x	x	x	X	X	x	

Lisäksi liitteessä B (Löydetyt uhkat kussakin kehitysvaiheessa) on vielä yksityiskohtaisempi taulukko, jossa myös toimijoiden vaikutusta on pyritty arvioimaan palvelunkehityksen eri vaiheisiin liittyviin uhkiin.

5.4.2 Palveluidean/konseptin kehittely

Palvelun idea saattaa usein tulla sisällöntuottajalta, palveluntarjoajalta tai palvelunkehittäjältä itseltään. Näillä toimijoilla on tietenkin vastuu omista tuotteistaan ja niiden laadusta.

Palvelua ideoitaessa täytyy miettiä, keitä toimijoita tarvitaan palvelun toteuttamiseksi parhaalla tavalla. Tähän voi saada ideoita muilta toimijoilta kuten integraattoreilta, verkko-operaattoreilta sekä erilaisista viranomaistahoilta ja tutkimuslaitoksista. Usein on hyödyllistä, että jo ideointi vaiheessa selvitetään mitä standardeja toimialaan ja palveluun liittyy, ja miten ne voisivat olla hyödynnettävissä. Jos käytetään standardien ulkopuolisia ratkaisuja, ajaudutaan usein umpikujaan ennemmin tai myöhemmin palvelun laajetessa. Lähes aina myös tietoturvan kannalta useimpien toimijoiden tuntemat standardiratkaisut ovat parhaita luotettavuuden ja toteutuksen (esim. alihankinnan) kannalta.

Tietoturva-asiantuntijan esim. konsulttitoimiston käyttö on erittäin hyödyllistä jo palvelunkehityksen alkuvaiheessa: pääuhkien tunnistaminen uudessa palvelussa (järjestelmä-näkökulma) sekä tärkeimmät tietoturvaratkaisut ja niiden realistisuuden arviointi voisivat kuulua konsultin tehtäviin.

Käytännössä kysymys on pääasiassa tuote- ja palvelukehitysympäristön riskienhallinnasta ja elinkaariajattelusta, esim. minkä ajanjakson tai vaiheen riski voi realisoitua.

Esimerkki ideointivaiheen toimista: Tee uhka-analyysi ideointivaiheessa, määrittele kohderyhmä sekä palvelu hyvin:

- Selvitä rajapinnat mitkä asiat voivat muodostua uhkiksi (ja miten).
- Luo uhkapuu (root causes). Käytä tietoturva-asiantuntijoita uhkien ja ratkaisujen arviointiin.
- Mitkä uhkista ovat realisoituvia käytännössä, onko meillä resursseja suojautua?
- Hallitse riskejä.
- Tee alustavat suunnitelmat kehittelyyn liittyville prosesseille. Etsi hyödynnettävät standardit.

5.4.3 Palvelun suunnittelu

Palvelun suunnitteluprosessi on tietysti hyvin riippuvainen siitä palvelusta, jota ollaan kehittämässä. Jos kyseessä on palvelu, jonka toteuttaminen edellyttää teknologia-enableria, kuten Bluetooth, tärkeää on teknologia-alustatoimittajien, piirivalmistajien ja ohjelmisto-ajurien kehittäjien valinta ja arviointi. Monesti ollaan riippuvaisia ohjelmistokehittäjien ja laitevalmistajien kyvystä ylläpitää hyvää tietoturvaa ja laatua omassa ympäristössään ja teknologia-alustoissaan. Valittuun teknologiaan liittyvien kunnollisten työkalujen hankinta, käytön suunnittelu ja koulutus on tärkeää integroinnin onnistumiselle.

Jos palvelun kehittäminen ei edellytä varsinaisesti teknologian (esim. protokollan) suunnittelua tai implementointia, voidaan paremmin keskittyä varsinaisen palvelun kartoittamiseen, kuten esitutkimuksiin siitä millaisia pilotteja aiemmin on tehty, keitä ollut mukana, ja millaisia kokemuksia on saatu. Tällä tavoin voidaan palvella kehitysympäristön kuntoon saattamista ja nähdä esimerkiksi tiettyjen työkalujen aiheuttamia rajoituksia palvelun toteutukseen. Jotkut työkalut tarjoavat riittämättömiä tietoturvaominaisuuksia, kuten päivittämättömän protokollan tai algoritmin. Tärkeää on myös selvittää edeltä käsin, millaiset käyttäjäryhmät palvelua tulisivat käyttämään, jolloin helppokäyttöisyys (esim. tietoturva-ominaisuuksien parametrit ja asetusvaihtoehdot) kriteerit selkiytyvät. Tämä koskee erityisesti kohdennettuja palveluja. Joissain tapauksissa taas palvelun käyttäjät voivat olla erittäin vaativia, jolloin heille on annettava mahdollisuus esimerkiksi muuttaa tietoturva-asetuksia tarpeen mukaan. Tällöin on kuitenkin varmistuttava siitä, että käyttäjää informoidaan tällaisten asetusmuutosten vaikutuksista.

Palvelun toteuttaminen vaatii usein ohjelmointia ja erilaisten ohjelmakirjastojen käyttöä, joita tyypillisesti kutsutaan yleisnimellä Software Development Kit (SDK). Ennen ohjelmointityön aloittamista työ pitää suunnitella ja vaiheistaa mm. palveluun liittyvään liiketoiminta-suunnitteluun, vaatimusmäärittelyyn, toteutussuunnitteluun, sekä testauksen ja käyttöönoton suunnitteluun. Kaikki tämä voi olla hyvin palvelukohtaista, mutta tietoturva tulisi olla eräs näkökulma, joka on aina mukana kaikissa suunnittelun vaiheissa. Lisäksi esim. kehitysympäristöjen ja dokumenttien tietoturvatestaus tai auditointi täytyisi suunnitella jollain tavalla.

Esimerkki palvelun suunnitteluun liittyvistä toimista:

- Tutki mitä teknologia-enablereita tarvitaan. Valitse parhaat teknologiatoimittajat, kysy esim. missä heidän teknologiansa on jo käytössä.
- Perehdy teknologiassa tarvittaviin työkaluihin ja suunnittele niiden hankintaa tarvttaessa.
- Tee esitutkimuksia, esim. mitä pilotteja on aiemmin tehty.
- Suunnittele helppokäyttöisyyden vaatimukset suunnitellulle käyttäjäryhmälle. Millä keinoin ne voidaan toteuttaa?
- Varmista liiketoimintasuunnittelun, vaatimusmäärittelyn, toteutussuunnittelun, testauksen ja käyttöönoton suunnittelun laatu.
- Suunnittele kehitysympäristöjen ja dokumenttien auditointi.

5.4.4 Palvelun toteutus

Tärkeä osa palvelun toteutusta on toteutusvaihtoehtojen tutkiminen ja parhaan valinta. Erittäin tärkeää on valita oikeat henkilöt, eli tekijöiden valinta. Tietoturva on suhteellisen uusi asia mobiilipalvelujen toteutuspuolella, koska mobiiliverkot ja laitteet ovat olleet aiemmin erillään esimerkiksi Internetistä. Täten mobiilipalvelun tietoturvan toteuttamiseen ei useinkaan liity kunnollista kehityshistoriaa, joka antaisi pohjan uusien palvelujen toteuttamiseen.

Palvelun toteutuksessa on käytettävä selkeää prosessia, joka voi olla toteuttajan oma tai tilaajan (esimerkiksi laitevalmistajan) prosessi sovellettuna tähän palveluun. On varmistuttava etukäteen, että prosessi on tietoturvallinen kaikissa suhteissa. Käytettävän toteutuskielen mukaiset tietoturvalliset ja toimintavarmat toteutustavat tulisi ottaa käytännöksi palvelua toteutettaessa, erityisesti päätelaitteissa.

Käytettävien työkalujen (esim. kryptokirjastot, protokollatoteutukset, käyttöliittymän kehitysympäristöt) valintaan kannattaa kiinnittää erityistä huomiota. Palvelinpäässä valmiita ratkaisuja on olemassa. Toisaalta työkalut päätelaitteen tietoturvan toteuttamiseksi ovat hajanaisia ja on vaikea löytää toimivaa kokonaisuutta tuotekehitystä varten. Niinpä palvelut joudutaankin toteuttamaan erikseen kullekin puhelinalustalle. Älypuhelimet ovat tuoneet hieman helpotusta asiaan, esimerkiksi Symbianin käyttöliittymäversioista Nokian Series-60 parhaana esimerkkinä, joka sisältää mm. IPSec ja SSL/TLS toteutukset. Älypuhelimet eivät vielä ole kovin yleisiä ja näin ollen palvelun kehittäjä ja tarjoaja ovat riippuvaisia useista eri puhelinvalmistajista, joilla on omia ratkaisujaan tietoturvaan. Käytännössä useissa tapauksissa palveluun liittyvän palvelimen ja puhelimen tietoturvaominaisuuksien päästä-päähän -yhteensopivuutta ei ole kunnolla testattu.

Yksi keskeinen vastuuriski mobiiliviestinnässä koskee sähköisen viestinnän tietosuojalain mukaisia velvollisuuksia tietoturvasta ja tiukkoja säännöksiä henkilötietojen käsittelystä tietoturvatarkoituksessa. Säännösten soveltuminen riippuu siitä liitetäänkö palvelussa mobiili-laite yleiseen viestintäverkkoon vai vain lokaaliin verkkoon (esim. Bluetooth), onko kyse

viestinnästä vai puhtaasti laitteiden välisestä tiedon siirrosta (kuten RFID tapauksessa monesti on) ja välitetäänkö verkossa luottamuksellisia viestejä. Näiden vastuiden ja velvollisuuksien selvittäminen sekä oman roolin ymmärtäminen on yksi keskeisiä vaatimuksia tietoturvasta huolehtimisessa. Mikäli säännökset tulevat sovellettaviksi, viestinnän tunnistamistietoja käsittelevällä on velvollisuus tallentaa yksityiskohtaiset tapahtumatiedot siitä, kuka käsitteli, milloin ja kuinka kauan. Kyse on henkilötietojen käsittelyn lokitiedoista (esim. kuka yrityksessä on käsitellyt tietoja), eikä viesteihin liittyvien tunnistamistietojen tallentamisesta.

Esimerkki toteutuksen aikana muistettavista asioista:

- Eri toteutusvaihtoehtojen tutkiminen ja parhaan valinta. Tekijöiden valinta.
- Luo lukkoon käytettävä, turvallinen prosessi. Muista varmistaa myös alihankkijan prosessi.
- Lyö lukkoon käytettävät kryptokirjastot, protokollapinot, käyttöliittymän kehitysympäristöt. Jätä suunnitelmaan varaa vielä vaihtaa joku niistä tarpeen tullen.
- Tarkista että henkilö- ja tunnistetietojen käsittely tullaan toteuttamaan asianmukaisella tavalla.

5.4.5 Palvelun testaus

Tärkeimpiä asioita testauksessa ovat sen monipuolisuus ja kattavuus. Testauksen hahmottaminen useammasta eri näkökulmasta auttaa ohjelmistojen ja järjestelmien toimintavarmuutta. Tulisi käyttää ohjelmiston staattista ja dynaamista analyysiä, käsitellä ohjelmistoa sekä avoimena että suljettuna järjestelmänä keskittyen ohjelmistokoodin rakenteeseen ja käännetyn ohjelmiston toimintaan ympäristöönsä nähden. Hyväksymis-testauksessa tulee testata ohjelmiston oikeellinen toiminta ja ettei ohjelmisto toimi epähalutuilla tavoilla.

Testauksen kattavuutta ohjelmiston tilajoukosta ja koodipohjasta tulisi mahdollisuuksien mukaan arvioida. Järjestelmän kuormittuessa ohjelmiston toimintaa tulee arvioida. Kuorma voi aiheuttaa palveluneston tai mahdollistaa hyökkäyksiä operaatioiden epäatomisuuksien vuoksi. Fail-over -testauksella nähdään mitä tapahtuu palvelun ylikuormittuessa.

Rajapintatestauksen tärkeys korostuu verkkoympäristössä. Ympäristöstä saatavien syötteiden käsittely ohjelmistossa on testattava monipuolisesti. Ohjelmiston kaikkien rajapintojen oikeellista syntaksia on testattava kattavin osin, sekä täysin virheellisillä, pahantahtoisilla syötteillä (hakkerointitestaus). Ympäristörajapinnat testataan siis integraatio- ja toiminta-varmuustestauksella. Eräs tapa on käyttää ulkopuolisia penetraatiotestauspalveluita, jotka yrittävät löytää ohjelmistosta murtautumisessa yleisesti käytettyjä virheitä. Ohjelmiston muuttuessa regressiotestaus on erittäin tärkeää, jotta vanhat viat eivät ilmaannu uudelleen koodin uudistumisen myötä.

5.4.6 Palvelun käyttöönotto

Käyttöönoton alussa on hyvä varautua erikoistuneiden asiantuntijoiden ja työkalujen käyttöön. Tietoturva-auditointi tulisi tehdä ennen käyttöönottoa, jolloin varmistutaan, että kaikki tarvittava on tehty tietoturvan toteutumiseksi. Ohjelmistojen paikat ja korjaukset on asennettava ennen käyttöönottoa (patch management).

Palvelun käyttäjän näkökulmasta palvelun käyttöönotto on kriittinen vaihe. Käyttäjän täytyy mahdollisesti ladata jokin ohjelma matkapuhelimeensa, tai hänen täytyy saada esim. verkkoasetuksia muutetuksi palvelulle sopiviksi. Jatkossa joudutaankin rakentamaan lisää käytäntöjä ja sovelluksia, joiden avulla käyttäjä pystyy muuttamaan ja päivittämään laitteensa asetuksia automaattisesti. Tämä on erittäin vaativa ongelma tietoturvanäkökulmasta, sillä jonkin yksittäisen toimijan määräämät asetukset saattavat estää käyttäjää käyttämästä joitain toisia palveluita.

Verkko-operaattori on perinteisesti keskeinen toimija palveluasetuksiin liittyen, mutta rajapinta verkkopalveluiden ja muiden palveluiden välillä on hämärtynyt ja tämä voi tuottaa ongelmia esim. palveluntarjoajan, verkko-operaattorin ja käyttäjän välisiin suhteisiin.

Asiakkaan toiminta yksinkertaistuisi, jos hänelle myytäisiin puhelin ja liittymä (SIM) palveluineen integroituna pakettina, jossa puhelimen ja SIM-kortin asetukset olisi esiasetettu. Tällöin vaarana on kuitenkin asiakkaan tietämättömyydestä johtuva tahaton sitoutuminen operaattorin tarjoamiin palveluihin. Lähtökohtaisesti myös markkinointimateriaali muodostaa sopimuksen osan. Jos markkinointimateriaalissa luvataan tietoturvallisuutta, käyttäjällä on myös oikeus sitä vaatia. Lisäksi hänellä on oikeus vaatia korvausta, mikäli hän on luottanut luvattuun turvallisuuteen ja kuitenkin kärsinyt vahinkoa esim. palvelussa säilytettyjen kontaktitietojen menetyksen muodossa.

5.4.7 Palvelun ylläpito

Mikäli tuotteissa ja palveluissa on puutteita ja virheitä, ne ovat haavoittuvaisia asiattomalle hyväksikäytölle palvelun ylläpitovaiheen aikana. Ohjelmistojen päivittäminen on erittäin tärkeä suojautumiskeino löytyneitä virheitä vastaan. Tiedonlähteitä haavoittuvuuksien torjuntaan löytyy esim. SANS:n (SysAdmin Audit Network Security Institute) [SANS] kautta.

Palvelun ylläpitovaiheessa haavoittuvuuksien käsittelyprosessi on keskeinen. Sillä tarkoitetaan ohjelmistojen ja laitteiden kehittämiseen liittyvää toimintojen kokonaisuutta, joka kattaa (ohjelmiston tai laitteiston) haavoittuvuuden koko elinkaaren, löytämisestä korjaukseen saakka.

Haavoittuvuuksien käsittelyyn osallistuu ensisijaisesti kolme päätoimijaa [Laakso1999]:

- haavoittuvuuden löytänyt taho,
- haavoittuvuuden korjaamisesta vastaava, esim. valmistaja, ja
- käsittelyprosessia koordinoiva tai ohjaava taho.

Ylläpitovaiheessa tietoturvaan liittyvä toiminta on valitettavasti usein reaktiivista. Palvelun haavoittuvuus voi johtua palvelun tai ohjelman asetuksista, mikä hidastaa korjauksen aloittamista. Ylläpitovaiheen ohjelmistohaavoittuvuuksia vähennetään proaktiivisesti tekemällä järjestelmästä mahdollisimman yksinkertainen. Lisäksi järjestelmän komponenttien tulisi olla helposti päivitettäviä ja ylläpitäjän tulisi huomioida, että myös erilliset tietoturvatuotteet ja -ominaisuudet lisäävät järjestelmän monimutkaisuutta. Parhaillaan ne onnistuvat takaamaan tiedon eheyden ja luotettavuuden, mutta usein hintana on kuitenkin palvelun saatavuuden hienoinen heikkeneminen. Monimutkaisuuden välttäminen sen sijaan vaikuttaa positiivisesti kaikilla osa-alueilla.

Haavoittuvuusprosessia koordinoivat viranomaistahot, (Suomessa Viestintäviraston CERT-FI) helpottavat haavoittuvuuksien raportointi- ja korjausprosessia omalla panostuksellaan. Heillä on valmiina viestintäkanavia oikeisiin tahoihin ja he voivat puolueettomana organisaationa tukea prosessin sujuvaa onnistumista.

Esimerkki palvelun ylläpitovaiheen toimista:

- Etsi haavoittuvuuksien käsittelyyn osallistuvat toimijat. Käytä prosesseja haavoittuvuuksien havaitsemiseksi ja suunnittele uusia havaitsemiskeinoja. Sovi prosessista, joilla löydetyt haavoittuvuudet käsitellään ja korjataan talon sisällä ja ulkopuolisten toimijoiden taholla.
- Havainnoi hyökkäyksiä. Suunnittele, miten havaitun hyökkäyksen aikana toimitaan.
- Käytä prosessia kaikkien ohjelmistojen päivitykseen (patch management). Määrittele vastuut.
- Järjestä lokitietojen keräys ja poikkeavuuksien etsintä.

5.4.8 Palvelun edelleen kehittäminen

Palvelun edelleen kehittäminen voi tapahtua useammastakin syystä. Voi olla, että palvelua varten kehitetty järjestelmä ei pystykään palvelemaan uusia käyttäjiä, joita tulee ”liian paljon” tai heidän toiveensa palvelusta voivat olla erilaisia kuin niiden käyttäjien, joille palvelu alun perin suunniteltiin. Voi myös olla, että palvelua on vasta pilotoitu ja positiivisten kokemusten perusteella on tarkoitus kehittää palvelu täysimittaiseen käyttöön.

Nämä syyt aiheuttavat usein tarpeen puuttua palveluarkkitehtuuriin. Käytännössä tämä voi tarkoittaa, että palvelua pitää pystyä käyttämään uuden tyyppisestä verkosta, esim. mobiiliverkon GPRS:n tai EDGE:n kautta aiemman GSM-datan lisäksi. Tällöin on käytävä uudelleen läpi arkkitehtuurin suunnitteluvaihe ja katsottava mitkä oletukset ovat muuttuneet

uuden tyyppisen verkon käytön myötä. Samalla pitää ottaa huomioon tulevaisuuden kapasiteettitarve tms. asiat. Palvelinten tai ohjelmistojen kapasiteetti voi muodostua ongelmaksi vanhassa arkkitehtuurissa, samoin kuin tietoturvapalveluiden riittävyys. Käyttäjän tunnistamismenettelyyn saattaa tulla muutoksia, jolloin palvelun käyttö uuden verkon kautta vaatii erilaisen käyttäjätunnistuksen. Tätä on syytä välttää ja suunnitella arkkitehtuuri siten, että kaikista verkoista tulevat käyttäjät tulisivat käyttämään yhtenäistä menettelyä käyttäjän tunnistamiseksi. Muutoinkin käyttäjänhallinnan tulisi olla yhtenäistä.

Muutosten hallinta on keskeistä palvelua edelleen kehitettäessä. On selvitettävä, esimerkiksi matriisin avulla, mihin kaikkeen muutoksen vaikutukset kohdistuvat, ja suunniteltava miten vaikutus huomioidaan toteutuksessa. Palvelun testaus on tietenkin syytä suorittaa mahdollisimman laajasti muutosten jälkeen.

Vaikka pilottivaiheessa ongelmia ei havaittu, käyttäjämäärän kasvu ja esim. joidenkin uusien käyttäjien erilainen asenne palvelun seuraavassa vaiheessa voi muodostua tekijäksi, johon täytyy palvelun kehittämisessä ennalta varautua. Kehittäjäverkosto tai muut toimijat, kuten verkko-operaattorin ja palveluoperaattorin, pitäisi pystyä auttamaan näissä tilanteissa. Esimerkiksi laajempia tekijänoikeuksien loukkauksia saattaa tulla ilmi vasta, kun palvelu on ollut jo jonkin aikaa toiminnassa, jolloin palvelua saatetaan joutua edelleen kehittämään tämänkin vuoksi. Tämä ei välttämättä tule ilmi, ellei hyödynnetä koko verkoston tiedonkeruu ja valvontakapasiteettia. Eri toimintojen tukemiseen tulisi kehittää yhtenäiset käytännöt.

Esimerkki palvelun edelleen kehittämiseen liittyvistä toimista:

- Käy palvelun suunnitteluvaihe uudelleen läpi ja katso mitkä ympäristötekijät tai oletukset palvelun suhteen ovat muuttuneet.
- Suunnittele muutokset arkkitehtuuriin ja tietoturvapalveluihin.
- Yhtenäistä samalla toimintoja, esim. käyttäjänhallinnan osalta.
- Hallitse muutoksia tekemällä ne asteittain, kunkin muutoksen vaikutukset testaten.
- Suunnittele tiedonkeruu järjestelmän toimivuudesta ja hyödynnä palaute.

5.4.9 Palvelun lopettaminen

Palvelun lopettamisessa korostuvat asiakkaiden tietosuojaan liittyvät kysymykset. Esimerkkejä ovat:

- Onko asiakasrekisterin tiedot asianmukaisesti tuhottava vai siirrettävä?
- Miten asiakastietojen siirto toteutetaan tietoturvallisesti?
- Ovatko käyttäjät riippuvaisia jostain palvelun ylläpitämästä tiedosta tai järjestelmästä suoraan tai välillisesti?

Muita palvelun lopettamisessa huomioitavia seikkoja tietoturvan kannalta ovat mm.:

- Onko palvelun aikana saatu tieto hyökkäyksistä tai niiden yrityksistä tallentuneena johonkin ja hyödynnettävissä?
- Ovatko salasanat ja muut tietoturvan hallintaan liittyvät tiedot tuhottu asianmukaisesti?

Palvelun lopettamiseen on olemassa viranomaissäännöksiä, joiden noudattaminen varmistaa oikeat toimet palvelua lopetettaessa. Uusilla ja pienemmillä toimijoilla ei aina ole palvelujen lopettamiseen liittyvää toimintakulttuuria, jolloin siihen liittyvät menettelytavat täytyy luoda ja kirjata ylös, jotta ne ovat kaikkien saatavilla. Palvelun lopettamiseen liittyvä tietoturva-politiikka täytyy olla oikeassa suhteessa tarjottaviin palveluihin, vastuisiin ja riskitekijöihin.

Lähdeluettelo

[3GCO] http://www.3g.co.uk/PR/March2005/1117.htm

[3GPP] http://www.3gpp.org/; http://www.3gpp.org/ftp/Specs/html-info/21133.htm

[Alahuhta2005] Alahuhta P., Ahola J., Hakala H. ”Mobilizing Business Applications”, TEKES Technology Review 167/2005. http://www.tekes.fi/julkaisut/Mobilizing.pdf

[ARBOR] http://www.arbor.net/

[BIOAPI] www.bioapi.org/

[BIOSEC] http://www.vtt.fi/ele/research/tel/projects/biosec.html

[Canary] https://www.canarywireless.com, The Digital Hotspotter Wi-Fi detector

[CERT] http://www.cert.org/security-improvement/#Harden

[comp128] http://www.gsm-security.net/faq/gsm-a3-a8-comp128-broken-security.shtml

[ECRFID] http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2005/wp105_en.pdf

[FIBA] ”Trust in the New Economy – The Case of Finnish Banks”, p.22, Ministry of transport and communications, Finland, Publication 17/2004

[FICOM] http://www.ficom.fi/fi/t_tekniikka_r.html?Id=1109941358.html

[FICORA] http://www.ficora.fi/suomi/tietoturva/cert.htm

[Garfinkel03] Simson Garfinkel, Gene Spafford and Alan Schwartz: Practical Unix and Internet Security, third edition

[GSMA] www.gsmworld.com

[GSMsec] http://www.gsm-security.net/faq/gsm-a5-broken-security.shtml

[HEL] http://www.hel.fi/hank/tp/45/Liite3TarpeetVaatimukset.pdf

[HIP] http://www.ietf.org/html.charters/hip-charter.html

[HST] HST Arkkitehtuurit ja liiketoimintamallit määrittely, Versio 1.0 12.5.2003

[INSTAT] www.instat.com

[javafaq] http://www.cs.princeton.edu/sip/faq/java-faq.php3

[javavul] http://www.dtic.mil/ieb_cctwg/contrib-docs/JAVA/JAVA-VUL/

[javasec] http://www.cs.princeton.edu/sip/pub/secure96.html

[Karila] Internet-puhelut (VoIP) –Selvitys, LIIKENNE- JA VIESTINTÄMINISTERIÖN JULKAISUJA 16/2005

[KORHONEN] Korhonen H. Haitalliset ohjelmat mobiilipäätelaitteissa, harjoitustyö toukokuu 2005. Tampereen Yliopisto, tietojenkäsittelytieteiden laitos.

[Laakso1999] Laakso, M, Takanen, A. & Röning, J. 1999. The Vulnerability Process: A Tiger Team Approach to Resolving Vulnerability Cases. In the proceedings of the 11th FIRST Conference on Computer Security Incident Handling and Response. Brisbane. 13.–18.6.1999. Saatavilla www-muodossa: http://www.ee.oulu.fi/research/ouspg/protos/sotaFIRST1999-process

[LASEC] http://lasecwww.epfl.ch/~gavoine/rfid/

[LUOTI] www.luoti.fi

[MET] http://www.mobiletransaction.org/

[MPEGLA] http://www.mpegla.com/

[NIST800-48] http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf

[ODRL] http://odrl.net

[PANKKIYHD] http://www.pankkiyhdistys.fi/

[Radiol] http://www.cs.helsinki.fi/u/rnikifor/nyt/kalvot/20030402_Valtari.pdf

[RFIDLAB] http://www.rfidlab.fi/

[SANS] http://www.sans.org/resources/

[SAVOLA] Savola R., Holappa J. 2005, Towards estimation of the security level in mobile and ad hoc networks. In the proceedings of the IWWST'05, London, April 4-5.

[secfocus] http://www.securityfocus.com/bid/keyword/

[TEOSTO] http://www.teosto.fi

[TMP] www.trusted-mobile.org/

[VAHTI3/2004] VAHTI – HAITTAOHJELMILTA SUOJAUTUMISEN YLEISOHJE

[Vesanen] http://www.tol.oulu.fi/~avesanen/Langaton_TT/

[VILANT] http://www.vilant.com/

[VIRVE] www.virve.com

[W3ORG] www.w3.org/TR/odrl/

[WLANSC] http://www.wlansmartcard.org/specifications.html

[wwwfaq] WWW security FAQ: http://www.w3.org/Security/Faq/www-security-faq.html

[YRTI] ”Tietoturvalliseen tietoyhteiskuntaan”, Yritysten tietoturvatietoisuus – työryhmän raportti, 21.2.2005. http://www.mintc.fi/oliver/upl263-Työryhmän%20raportti%2021.pdf

Liite A: Yrityshaastatteluiden kysymyksiä

Yleiset kysymykset

Miten yritys näkee uhkat ja ongelmat?

Mitä uhkia näette sähköiselle liiketoiminnalle mobiili/digi-tv palveluihin liittyen palvelunkehittäjän näkökulmasta?

Tietoturvan integroituvuus, helppokäyttöisyys.
Mitä yleisiä tavoitteita näette tietoturvan helppokäyttöisyydelle? Miten voitaisiin toteuttaa palvelunkehittäjän näkökulmasta? Mitä ongelmia tähän liittyy?

Ratkaisuista

Miten vähennätte uhkia ”välttämällä” tiettyjä toimintoja? Mitä toimintoja joudutte välttämään?

Uhkan pienentäminen.
Mitä olette tehnyt että tietty riski toteutuisi mahdollisimman harvoin ja jos se toteutuu, seuraukset olisivat mahdollisimman pienet.

Uhkan siirtäminen tai jakaminen sopimuksia tehden – Tyypillisiä sopimuksia ovat esimerkiksi alihankintasopimukset.
Mitä uhkakuvia on vältetty esim. vakuuttamalla?

Tiettyjen strategisten uhkien hyväksyminen, riskin pitäminen omalla vastuulla.
Mitä uhkia olette hyväksyneet liiketoiminnan kannalta välttämättömiksi pitää omalla vastuulla, sillä teillä on esim. jotain erityisosaamista jonka avulla onnistutte?

Miten on suunniteltu toimittavan vahingon sattuessa? Miten vahingosta on mahdollista toipua nopeasti ja mahdollistaa liiketoiminnan mahdollisimman hyvä jatkuvuus?

Kysymyksiä pidemmän aikavälin ratkaisusta:

Miten yo. toimenpiteitä seurataan?

Vastuuhenkilöt? Oletteko miettineet kenen vastuualueelle uhkat kuuluvat? Onko allokoitu resurssi riittävä (esim. yleensä tietoturvateknologiasta vastaava henkilö ei ehdi vastaamaan koko operatiivisen toiminnan uhkakuvista)?

Miten uusia uhkia identifioidaan?

Miten uhkista ja toimenpiteistä tiedotetaan?

Onko saatavilla tietoa, jonka avulla uhkat kyetään tunnistamaan ja arvioimaan?

Ymmärrämmekö hallinnan ulottumattomiin jäävän riskitason, jonka toiminnasta vastuussa olevat hyväksyvät?

Onko teillä (käytännössä hallittavissa olevat) turvatavoitteet?

Arvioitteko säännöllisesti tavoitteita ja uhkia?

Palvelunkehitykseen liittyvät osapuolet ja prosessi

Seuraavanlaisia kysymyksiä arvoverkoista käytettiin.

Käsitellään palvelunkehitysprosessin vaiheita (ideointi, suunnittelu, testaus, toteutus, käyttöönotto, ylläpito).

Mitkä osapuolet osallistuvat palveluidean/konseptin kehittelyyn? Prosessi?

Mitkä toimijat osallistuvat palvelun suunnitteluun? Prosessi?

Mitkä toimijat osallistuvat palvelun toteutukseen? Prosessi?

Mitkä toimijat osallistuvat palvelun testaukseen? Prosessi?

Mitkä toimijat osallistuvat palvelun käyttöönottoon? Prosessi?

Mitkä toimijat osallistuvat palvelun ylläpitoon? Prosessi?

Mitkä toimijat osallistuvat palvelun edelleen kehittelyyn? Prosessi?

Mitkä toimijat osallistuvat palvelun lopettamiseen? Prosessi?

Teknologiset sovellusalueet

Mistä teknisistä laitteista/järjestelmistä koette olevanne riippuvaisia? (Mitä ilman ette pärjäisi?) Miksi?

Mitkä ovat mielestäsi kriittisimmät mobiiliin tietoliikenteeseen liittyvät protokollat? Miksi?

> Tässä yhteydessä haastateltavalle näytetään kaavio joukosta protokollia, joista hän voi arvioida mielestään kriittisimmät ja ehdottaa mahdollisesti jotain, jotka eivät kaaviossa ole.

Mitkä käsityksesi mukaan käytössä olevista protokollat toimivat selkeimmin liitekohtina IP- ja GSM-maailman välillä?

Mitkä ovat mielestäsi tärkeimmät IP-pohjaiset protokollat, joita käytetään mobiililaitteissa ja -verkoissa?

Mitä kautta saatte yleensä tiedon tietoturvahaavoittuvuuksista?

Miten toimitte, kun jostain löytyy jokin haavoittuvuus? Millainen haavoittuvuusprosessi teillä on käytössä? Kuvaile.

> Haastateltavalle esitellään hahmottelemamme yleisellä tasolla oleva kaavio haavoittuvuusprosessiin osallistuvista tahoista ja häntä pyydetään konkretisoimaan, ketkä käytännössä toimivat heidän kannaltaan kussakin roolissa.

Mihin suuntaan olemme käsityksesi mukaan seuraavaksi menossa? Esimerkiksi: millaisia toiminnallisuuksia/applikaatioita otetaan lähitulevaisuudessa käyttöön?

Mitkä protokollat tulevat olemaan tulevaisuudessa merkityksellisimpiä? Miksi?

Vähentyykö joidenkin protokollien merkitys tulevaisuudessa? Miksi?

Liite B. Löydetyt uhkat kussakin kehitysvaiheessa

Taulukko 12. Identifioidut uhkat ja kriittiset toimijat palvelukehitysprosessin eri vaiheissa. Lisäksi tietoturvauhkana on **toimijoiden riittämätön osaamistaso ja alan nopea muuttuminen**, mutta nämä uhkat vaikuttavat lähes kaikkiin prosessin vaiheisiin ja toimijoihin, joten yksinkertaisuuden vuoksi ne jätettiin pois ao. taulukosta.

Kehitys-vaihe	Uhkat	Lailliset toimijat, jotka toiminnallaan saattavat aiheuttaa kyseisen uhkan
Palveluidean/ -konseptin kehittely	liian suppea toimijaverkosto	palveluntarjoaja
	datan salakuuntelu, datan oikeudeton käyttö tai muokkaus	uudet palvelunkehittäjät
Palvelun suunnittelu	datan salakuuntelu, datan oikeudeton käyttö tai muokkaus	uudet palvelunkehittäjät, integraattori
	virukset, haittaohjelmat	uudet palvelunkehittäjät
Palvelun toteutus	toimijoiden eritasoisuus	ohjelmistokehittäjä, integraattori, uudet palvelunkehittäjät, palvelunkehitys-ympäristöntarjoaja
	datan salakuuntelu, datan oikeudeton käyttö tai muokkaus	sisällöntuottaja, ohjelmistokehittäjä, integraattori, uudet palvelunkehittäjät
	palvelukehitysympäristön eheys (integriteetti, stabiilisuus)	palvelunkehittäjät ja kehitysympäristöjen tarjoajat
	palveluun tai laitteeseen kohdistuvat hyökkäykset, ohjelmointivirheet, väärät tekniset ratkaisut tai kehitystyökalut, kompleksisuus, väärät asetukset	ohjelmistokehittäjä, integraattori, palvelunkehittäjät ja kehitysympäristöjen tarjoajat
	sisältöjen (kuten video, audio) käyttöoikeudet ja kopiointi	sisällönpaketoija, integraattori, palvelunkehittäjä, palveluntarjoaja
	virukset, haittaohjelmat	uudet palvelunkehittäjät, kehitysympäristöjen tarjoajat
Palvelun testaus	toimijoiden eritasoisuus	integraattori, uudet palvelunkehittäjät ja palveluntarjoajat
	testiympäristön eheys	testiympäristön tarjoaja
	virukset, haittaohjelmat	integraattori, testiympäristön tarjoaja
Palvelun käyttöönotto	datan salakuuntelu, datan oikeudeton käyttö tai muokkaus	palveluoperaattori, verkko-operaattori
	palveluun tai laitteeseen kohdistuvat hyökkäykset, ohjelmointivirheet, väärät tekniset ratkaisut tai kehitystyökalut, kompleksisuus, väärät asetukset	palveluntarjoaja, palvelunkehittäjä, palveluoperaattori, verkko-operaattori, markkinointiyhtiöt
	tunnistus, käyttäjän identiteetin luottamuksellisuus	palveluntarjoaja, palvelunkehittäjä, palveluoperaattori, verkko-operaattori
	käyttäjän luottamuksellisen tiedon jakaminen	palveluoperaattori, verkko-operaattori
	käyttäjän paikkatiedon luottamuksellisuus	palveluoperaattori, verkko-operaattori
	sisältöjen (kuten video, audio) käyttöoikeudet ja kopiointi	palveluntarjoaja, palvelunkehittäjä, palveluoperaattori, markkinointiyhtiöt
	virukset, haittaohjelmat	palveluntarjoaja, palvelunkehittäjä, palveluoperaattori, verkko-operaattori
Palvelun ylläpito	datan salakuuntelu, datan oikeudeton käyttö tai muokkaus	kuluttaja, palveluoperaattori, verkko-operaattori
	tuotantoympäristön eheys	palveluoperaattori, palvelunkehittäjä

Kehitys-vaihe	Uhkat	Lailliset toimijat, jotka toiminnallaan saattavat aiheuttaa kyseisen uhkan
	palveluun tai laitteeseen kohdistuvat hyökkäykset, ohjelmointivirheet, väärät tekniset ratkaisut tai kehitystyökalut, kompleksisuus, väärät asetukset	kuluttaja, palveluntarjoaja, palvelunkehittäjä, palveluoperaattori, verkko-operaattori
	tunnistus, käyttäjän identiteetin luottamuksellisuus	kuluttaja, palveluntarjoaja, palvelunkehittäjä, palveluoperaattori, verkko-operaattori
	käyttäjän luottamuksellisen tiedon jakaminen	kuluttaja, palveluntarjoaja, palveluoperaattori, verkko-operaattori
	käyttäjän paikkatiedon luottamuksellisuus	kuluttaja, palveluntarjoaja, palveluoperaattori, verkko-operaattori
	sisältöjen (kuten video, audio) käyttöoikeudet ja kopiointi	kuluttaja, sisällönpaketoija, palveluntarjoaja, palveluoperaattori
	uudenlaiset käyttötavat- ja tilanteet (sis. esim. WLAN, Bluetooth, RFID)	kuluttaja, palveluntarjoaja, palvelunkehittäjä, palveluoperaattori, verkko-operaattori, markkinointiyhtiöt
	palvelujen luvaton käyttö toisen asiakkaan kustannuksella (fraud), laitevarkaus	kuluttaja, palveluntarjoaja, palveluoperaattori, verkko-operaattori
	palvelunesto esimerkiksi ylitarjonnalla, liikenteen estäminen, roskaposti	kuluttaja, palveluntarjoaja, palveluoperaattori, verkko-operaattori
	hätäpuheluiden läpipääsy (esim. laitteiden ja ohjelmistojen yhteensopimattomuus)	kuluttaja, palveluntarjoaja, palvelunkehittäjä, palveluoperaattori, verkko-operaattori
	virukset, haittaohjelmat	kuluttaja, palveluntarjoaja, palvelunkehittäjä, palveluoperaattori, verkko-operaattori
	mobiilin sähköisen maksamisen riskit, kiistettävyys, väärennetty palvelusivusto	kuluttaja, palveluntarjoaja, palvelunkehittäjä, palveluoperaattori, verkko-operaattori, maksuliikenteen hoitaja
Palvelun edelleen kehittäminen	datan salakuuntelu, datan oikeudeton käyttö tai muokkaus	ohjelmistokehittäjä, integraattori, uudet palvelunkehittäjät
	palvelukehitysympäristön eheys (integriteetti, stabiilisuus)	palvelunkehittäjät ja kehitysympäristöjen tarjoajat
	palveluun tai laitteeseen kohdistuvat hyökkäykset, ohjelmointivirheet, väärät tekniset ratkaisut tai kehitystyökalut, kompleksisuus, väärät asetukset	ohjelmistokehittäjä, integraattori, palvelunkehittäjät ja kehitysympäristöjen tarjoajat
	käyttäjän luottamuksellisen tiedon jakaminen	palveluntarjoaja, palveluoperaattori
	sisältöjen (kuten video, audio) käyttöoikeudet ja kopiointi	sisällönpaketoija, integraattori, palvelunkehittäjä, palveluntarjoaja
	virukset, haittaohjelmat	uudet palvelunkehittäjät, kehitysympäristöjen tarjoajat
Palvelun lopettaminen	toimijoiden eritasoisuus	palveluntarjoaja, palveluoperaattori
	palveluun tai laitteeseen kohdistuvat hyökkäykset, ohjelmointivirheet, väärät tekniset ratkaisut tai kehitystyökalut, kompleksisuus, väärät asetukset	kuluttaja, palveluntarjoaja, palveluoperaattori
	tunnistus, käyttäjän identiteetin luottamuksellisuus	kuluttaja
	käyttäjän luottamuksellisen tiedon jakaminen	palveluntarjoaja, palveluoperaattori

Lisätietoja:

LUOTI-ohjelman internet-sivut
www.luoti.fi

Liikenne- ja viestintäministeriön internet-sivut
www.mintc.fi