Luottamus. Tietoturva. Sähköiset palvelut.

LUOTI-julkaisuja 2/2005

Digi-tv:n tietoturvauhkat ja ratkaisut

Palvelunkehittäjän näkökulma

Digi-tv:n tietoturvauhkat ja ratkaisut
Palvelunkehittäjän näkökulma

ISBN 952-201-288-2, 952-201-289-0 (verkkojulkaisu)
LUOTI-julkaisuja 2/2005
Helsinki 2005

Julkaisija

LUOTI

KUVAILULEHTI

Julkaisun päivämäärä

2.6.2005

Tekijät	Julkaisun laji
VTT: Jarkko Holappa, Pasi Ahonen, Mikko Rapeli, Ville Ollikainen, Juha-Pekka Koivisto, Anni Sademies ja Reijo Savola Oulun yliopisto: Tiina Kaksonen, Juhani Eronen, Kati Karjalainen, Erno Kuusela, Jorma Kajava ja Juha Röning	Raportti
	Toimeksiantaja Liikenne- ja viestintäministeriö

Julkaisun nimi

Digi-tv:n tietoturvauhkat ja ratkaisut. Palvelunkehittäjän näkökulma.

Tiivistelmä

Tässä raportissa tarkastellaan digitaalisen television mukanaan tuomia tietoturvauhkia ja ratkaisu-vaihtoehtoja palvelunkehittäjän näkökulmasta. Teknisten ratkaisujen lisäksi raportissa kiinnitetään huomiota palvelunkehitysprosessiin – siihen liittyvään arvoverkkoon sekä palvelunkehityksen eri vaiheisiin ja niihin liittyviin uhkiin.

Raportti on osa liikenne- ja viestintäministeriön Luottamus ja tietoturva sähköisissä palveluissa (LUOTI) -ohjelmaa, jonka tarkoituksena on monikanavaisten sähköisten palveluiden tietoturvan kehittäminen. Raportin tutkimusmenetelminä on ollut kirjallisuushaut, asiantuntijoiden näkemykset, yrityshaastattelut sekä laaja-alaiset kommentointikierrokset.

Digitaalinen konvergenssi tuo monipuolistuvia palveluita digi-tv-maailmaan. Vuorovaikutteiset palvelut mahdollistava paluukanava on tässä kehityksessä avainasemassa. Sen voidaan nähdä olevan päätelaitteen haavoittuvin osa tietoturvamielessä, joten sen suojaaminen Internet-käytön tuomilta uhkilta, kuten haittaohjelmilta, on ensiarvoisen tärkeää. Tuotekehitysprosessien on otettava huomioon digitaalisen konvergenssin erityispiirteet – arvoverkot ja erilaisten infrastruktuurien turvallinen yhdistäminen.

Koska Multimedia Home Platform (MHP) on paluukanavan ohella tärkeimpiä interaktiivisen television mahdollistavia teknologioita, saa se tässä raportissa erityishuomion. Sen mukanaan tuomia uhkia tarkastellaan palvelunkehittäjän näkökulmasta. MHP:n tietoturvaratkaisuja käsitellään ja niiden kypsyyttä ja soveltuvuutta arvioidaan muun muassa rakentumassa olevien allekirjoituskäytäntöjen osalta.

Avainsanat (asiasanat)

Digi-tv, MHP, tietoturva, tietoturvauhkat, sähköiset palvelut, palvelunkehitys

Muut tiedot

Selvityksen katselmointiin ovat osallistuneet Tommi Riikonen (Ortikon Interactive Ltd.), Jari Råman (Lapin yliopisto), Marko Helenius (Tampereen yliopisto) ja Ritva Poikolainen (VTT)

Sarjan nimi ja numero		ISBN	
LUOTI-julkaisuja 2/2005		952-201-288-2, 952-201-289-0 (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: Jarkko Holappa, Pasi Ahonen, Mikko Rapeli, Ville Ollikainen, Juha-Pekka Koivisto, Anni Sademies och Reijo Savola Uleåborgs Universitet: Tiina Kaksonen, Juhani Eronen, Kati Karjalainen, Erno Kuusela, Jorma Kajava och Juha Röning	Rapport
	Uppdragsgivare Kommunikationsministeriet

Publikation

Hot och lösningar beträffande informationssäkerheten i digital-tv. Serviceutvecklarens perspektiv.

Referat

I rapporten granskas de hot mot informationssäkerheten som den digitala televisionen för med sig och alternativa lösningar ur serviceutvecklarens perspektiv. Förutom de tekniska lösningarna undersöks även serviceutvecklingsprocessen och värdenätet som har att göra med den samt de olika faserna inom serviceutvecklingen och hot som är förknippade med dem.

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. Som forskningsmetoder för rapporten användes litteratursökningar, expertutlåtanden, företagsintervjuer och en omfattande insamling av kommentarer.

Den digitala konvergensen öppnar möjligheter för ett bredare sortiment av tjänster inom digital-tv-världen. Returkanalen är ett nyckelord i denna utveckling. Med returkanal avses teknik som möjliggör interaktiva mertjänster. Returkanalen kan anses vara terminalutrustningens sårbaraste del i fråga om informationssäkerheten och därför är det mycket viktigt att skydda den mot hot som användningen av Internet medför, till exempel skadliga program. I produktutvecklingsprocesserna måste man beakta särdragen i den digitala konvergensen – värdenäten och en trygg sammanlänkning av olika infrastrukturer.

Eftersom Multimedia Home Platform (MHP) vid sidan av returkanalen är en av de viktigaste tekniker som gör den interaktiva televisionen möjlig, uppmärksammas den särskilt i rapporten. De hot som MHP medför granskas ur serviceutvecklarens perspektiv. Dessutom behandlas lösningar för att trygga informationssäkerheten i fråga om MHP och man bedömer hur färdiga och tillämpbara de är, bland annat när det gäller den signaturpraxis som håller på att ta form.

Nyckelord

Digital-tv, MHP, informationssäkerhet, hot mot informationssäkerheten, elektroniska tjänster, serviceutveckling

Övriga uppgifter

Raporten har utvärderats av Tommi Riikonen (Ortikon Interactive Ltd.), Jari Råman (Laplands Universitet), Marko Helenius (Tammerfors Universitet) och Ritva Poikolainen (VTT)

Seriens namn och nummer		ISBN	
LUOTI publikationer 2/2005		952-201-288-2, 952-201-289-0 (nätpublikation)	
Sidoantal	Språk finska	Pris	Sekretessgrad offentlig
Distribution Kommunikationsministeriet		Förlag Kommunikationsministeriet	

The publisher

DESCRIPTION

Date of publication

2.6.2005

Authors

VTT: Jarkko Holappa, Pasi Ahonen, Mikko Rapeli, Ville Ollikainen, Juha-Pekka Koivisto, Anni Sademies and Reijo Savola

University of Oulu: Tiina Kaksonen, Juhani Eronen, Kati Karjalainen, Erno Kuusela, Jorma Kajava and Juha Röning

Type of publication

Report

Assigned by

Ministry of Transport and Communications

Name of the publication

Information security threats and solutions in digital television; the service developer's perspective

Abstract

This report examines the information security challenges brought about by digital television and their potential solutions from the service developer's perspective. Emphasis in the report is not only on technological solutions but also the service development process, the related network of values and the various stages of service development and threats related thereto.

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. Research methods employed include literature searches, expert opinions, interviews with enterprises and extensive rounds of commentary.

Digital convergence is introducing more diverse services to the world of digital television. The return channel, which enables interactive television, is key to this development and may be considered the most vulnerable element of the terminal device in terms of information security. Accordingly, its protection from threats brought about by Internet use, such as malicious programs, is of the essence. The special characteristics of digital convergence – value networks and the secure linking of different infrastructures – need to be taken into consideration in service development processes.

Special emphasis in this report is given to Multimedia Home Platform (MHP), as alongside the return channel it is one of the most important technologies enabling interactive television. The information security threats related to it are examined from the viewpoint of the service developer. MHP information security solutions are discussed and their maturity and suitability assessed with regard e.g. to signature practices currently being developed.

Keywords

Digital TV, MHP, information security, information security threats, electronic services, service development

Miscellaneous

Following persons participated in the survey of this report: Tommi Riikonen (Ortikon Interactive Ltd.), Jari Råman (University of Lapland), Marko Helenius (University of Tampere) and Ritva Poikolainen (VTT).

Serial name and number

LUOTI publications 2/2005

ISBN

952-201-288-2, 952-201-289-0 (www publication)

Pages, total	Language	Price	Confidence status
	Finnish		Public

Distributed by

Ministry of Transport and Communications

Published by

Ministry of Transport and Communications

Esipuhe

Tämä digi-tv:n 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 digi-tv:hen liittyvistä tietoturvauhkista sekä niiden ratkaisumahdollisuuksista palvelunkehitysprosessin eri vaiheissa. Multimedia Home Platformin (MHP) sekä paluukanavan tietoturvaratkaisut ovat selvityksessä tarkastelun keskipisteessä. Selityksessä pyritään luomaan myös 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 tutkija Jarkko Holapan projektijohdolla. Selvityksen tutkimusmetodeina on käytetty yrityshaastatteluja, kirjallisuushakuja, asiantuntijoiden näkemyksiä sekä laaja-alaisia kommentointi-kierroksia. Työtä ovat ohjanneet ohjelmapäällikkö Kimmo Lehtosalo Eera Finland Oy:stä ja neuvotteleva virkamies Päivi Antikainen liikenne- ja viestintäministeriöstä. Selvitystä ovat matkan varrella ansiokkaasti kommentoineet Esko Junnila, Petri Luoma, Tarja Rautio ja Mika Sorsa Digita Oy:stä, Pekka Nykänen ja Arto Saikanmäki JP-Epstar Oy:stä, Juha Perttula liikenne- ja viestintäministeriöstä, Kimmo Pöntiskoski ja Carina Stenvall MTV Oy:stä, Seppo Kalli Ortikon Interactive Oy:stä sekä Mika Kanerva Sofia Digital Oy:stä.

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

Helsingissä 2. kesäkuuta 2005

Päivi Antikainen
Neuvotteleva virkamies

Tiivistelmä

Digitaalinen televisio asettaa palveluympäristönä erittäin korkeat vaatimukset palvelujen käytettävyydelle ja tietoturvaratkaisuille. Käyttäjäryhmä on hyvin heterogeeninen lapsista vanhuksiin, eikä heidän tietoteknisestä osaamistasostaan voi tehdä mitään oletuksia. Tämänhetkisten päätelaitteiden käytettävyys ei kaikilta osin vastaa näitä vaatimuksia. Esimerkiksi vaihtelevat käytännöt päätelaitteiden ohjelmistopäivityksissä, mikäli niitä ei tehdä ohjelmavirran mukana tulevilla päivityksillä, eivät nosta kuluttajien luottamusta uuteen mediaan.

Digi-tv-palvelujen odotukset, edut ja hyödyt saavutetaan, kun kuluttaja uskaltaa, osaa ja haluaa käyttää palveluja. Tärkeimpänä tekijänä on käyttäjän luottamus palveluun ja sen toimittajaan. Yrityksen maine luotettavana palveluntoimittajana on loppukäyttäjän näkökulmasta kustannusten ohella yksi tärkeimmistä tekijöistä palveluntarjoajan valinnassa.

Digi-tv:n tietoturvan teknisistä uhkatekijöistä suurimmaksi nousee päätelaitteen eli digisovittimen turvallisuus erityisesti, kun interaktiiviset palvelut yleistyvät. Digisovittimen toimintavarmuuteen liittyvät uhkat on tiedostettu ja esimerkkejä virhetilanteiden aiheuttamista päätelaitteiden vioittumisista on jo Suomessa nähty. Laitteiden käyttäytyminen virheellistä signaalia vastaanotettaessa on monen päätelaitteen kohdalla arvaamatonta ja tämän voidaan todeta johtuvan suurelta osin puutteellisesta toimintavarmuustestauksesta. Tähän liittyvät palvelunkehittäjän näkökulmasta myös suurimmat digi-tv-verkon aiheuttamat uhkat.

MHP-standardin mahdollistama vuorovaikutteisuus sen määrittelemissä profiileissa 2 (Interactive Services) ja 3 (Internet access) tuovat joitakin jo tämän päivän Internet-maailmasta tuttuja uhkia digi-tv-ympäristöön. Toistaiseksi sovellusympäristö on rajoittunut ja digitaalisen jakeluverkon kannalta tiukasti digi-tv-verkko-operaattoreiden sekä televisiokanavien hallittavissa, sillä sovellukset tulevat ohjelmasignaalin mukana. Tämä tulee muuttumaan MHP1.1:n myötä, kun sovelluksia voi ladata myös paluukanavan kautta. Silloin palvelujen jakelukanavat monimutkaistuvat ja tulevat entistä haavoittuvaisemmiksi. MHP:n Java-pohjaisuus tuo Javan vahvuudet verkotetussa ympäristössä myös digisovittimeen, mutta samalla myös sen heikkoudet, jotka palvelunkehittäjän on syytä tuntea. Palvelunkehittäjän on osattava hyödyntää Javan tarjoamia tietoturvaominaisuuksia, kuten sovellusten digitaalista allekirjoitusta ja ohjelmointirajapintojen tarjoamaa tukea salakirjoitusmenetelmille, mutta samalla on tiedostettava eri Java-toteutuksiin liittyvät haavoittuvuudet.

Kovalevylliset päätelaitteet ja MHP-standardin 1.1-versio tuovat esiin uhkan myös vastaanotetun sisällön turvallisuudesta: sovelluksia ja siihen liittyvää dataa on mahdollista tallentaa digisovittimen massamuistiin. Lisääntyneen toiminnallisuuden kääntöpuolena on uhka pc-maailmasta tuttujen haittaohjelmien, virusten ja erilaisten vakoiluohjelmien pesiytymisestä päätelaitteeseen. Sisältöformaattien (kuva ja ääni) haavoittuvaisuudet muodostavat myös uhkan digisovittimen toiminnalle; väärin muotoillulla kuvatiedostolla on mahdollista estää vastaanottimen normaali toiminta. Kuva- tai äänitiedosto voi sisältää myös haitallista koodia, jonka päätelaite suorittaa virhetilanteessa, mikäli tällaisia käyttötapauksia ei ole riittävästi testattu palvelun kehitysvaiheessa. Palvelunkehittäjän näkökulmasta katsojalle toimitettu sisältö on tekijänoikeuslain alaista materiaalia, joka on suojattava kopiointia ja väärinkäytöksiä vastaan. Sisällön laiton käyttö, esim. tilanteessa kun palvelun maksettu käyttöaika on loppunut, on uhka palvelunkehittäjän liiketoiminnan näkökulmasta.

Paluukanavan kautta digitaalisessa televisiossakin voidaan puhua konvergenssista muiden digitaalisten sisältöjen levityskanavien kanssa. Kun palvelut integroituvat muihin kokonaisuuksiin ja verkkoihin, edessä on erityyppisillä käytännöillä ja laatustandardeilla kehitettyjä ympäristöjä. Näiden yhteensovittaminen tietoturvallisesti on erittäin suuri haaste, jota ei ole vielä kyetty kaikilta osin ratkaisemaan.

Sähköisten palveluiden tilaus- ja maksamisprosessien tulisi olla mahdollisimman helppokäyttöisiä ja käyttäjille entuudestaan tuttuja. Interaktiivisen television yleistyessä passiivisesta katsojasta tulee palvelujen myötä aktiivinen kuluttaja ja tuottajasta elinkeinonharjoittaja, jolloin kaupanteon pelisäännöt on oltava osapuolten kesken sovittuina välineestä riippumatta.

Palvelujen turvallisuuteen on pyritty vaikuttamaan olemassa olevien uhkakuvien vuoksi jo teknologioiden standardointivaiheessa. MHP tarjoaa alustana monia, osittain Javasta peräisin olevia, tietoturvaratkaisuja. Ohjelmien alkuperä voidaan tunnistaa digitaalisilla varmenteilla, joilla voidaan vaikuttaa myös siihen, minkälaisia oikeuksia sovellus saa päätelaitteessa – allekirjoittamatonta sovellusta käsitellään epäluotettavana, eikä se voi esimerkiksi avata paluukanavaa. Avoimia kysymyksiä ovat varmennekäytännöt. MHP-standardi määrittelee julkisen avaimen järjestelmän juurivarmenteineen, mutta suurimmasta osasta tällä hetkellä myynnissä olevista päätelaitteista ei tukea sille löydy. Lisäksi maakohtaiset varmennekäytännöt ovat vasta muotoutumassa, vaikkakin joitakin kokeiluja on jo tehty.

Kuten muussakin ohjelmisto- ja tuotekehityksessä, palveluntekijän sisäiset prosessit ovat avainasemassa laadukasta tuotetta kehitettäessä. Tietoturva on otettava suunnittelussa huomioon alusta lähtien. On tarkasteltava palvelukonseptin tavoitteita

tietoturvamielessä ja tutkittava, mitä vaatimuksia esimerkiksi luottamuksellisuudelle on asetettava, jotta loppukäyttäjän luottamus palveluun on oikeutettua. Tietoturvasta on huolehdittava kehitettävän tuotteen lisäksi myös yrityksen käytännöissä ja prosesseissa mukaan lukien alihankkijoiden prosessit. Palveluun liittyvä arvoverkko ja sen eri osapuolten roolit ja vastuut on tunnistettava. Henkilöstöä on koulutettava, jotta se tuntisi tietoturvalliset toimintatavat ja työskentelisi niiden mukaisesti tietäen oman vastuualueensa. Tuote on testattava kattavasti ennen sen toimittamista asiakkaalle. MHP-sovellusten yhdenmukaisuustestaus, jota tehdään MHP-laitteille, parantaisi loppukäyttäjän kokemaa palvelunlaatua.

Tietoturva tarkoittaa eri toimijoiden näkökulmasta erilaisia asioita – painotukset uhkien vakavuudessa ja ratkaisuissa vaihtelevat arvoverkon eri osissa. Sisällöntuottajalle suurimpia uhkia ovat ohjelman tai muun sisällön laiton käyttö ja levitys, verkko-operaattorille esimerkiksi viallinen ohjelmasisältö, joka haittaa katsojien päätelaitteiden toimintaa. Katsojalle uhkakuvia muodostavat yksityisyyden suoja tai vaikka sähköiseen kaupankäyntiin liittyvät riskit, kuten esimerkiksi luottokorttitietojen varastaminen. Loppukäyttäjän yksityisyyteen liittyvät uhkat tietyn palveluntarjoajan tuotteissa heikentävät tämän toimijan luotettavuutta ja näin ollen puutteellisesta yksityisyydensuojasta on tullut riski palveluntarjoajan liiketoiminnan jatkuvuudelle. Tietoturva on monitahoinen asia, johon liittyy aina teknisten ratkaisujen lisäksi lainsäädäntökysymykset ja ihmisten toimintatavat; kaikki ulottuvuudet tulisi ottaa huomioon palvelunkehitysprosessissa.

Lyhenteet ja terminologia

802.11	IEEE:n standardoima WLAN standardiperhe
API	Application Programming Interface. Sovellusohjelmointirajapinta.
Arvoverkko	Tapa kuvata monimutkainen liiketoimintakenttä perinteistä arvoketjua monipuolisemmalla tavalla, jossa on horisontaalisen ulottuvuuden lisäksi myös vertikaalinen ulottuvuus. Arvoketjuista poiketen arvoketjuissa voi olla useita samalla toimialalla olevia toimijoita.
BT	Bluetooth. Langaton tiedonsiirtoteknologia lyhyille etäisyyksille (10 m).
CA	Certification Authority. Varmentajaviranomainen.
CERT	Computer Emergency Response Team. CERT-FI on Viestintävirastossa toimiva kansallinen CERT-ryhmä, jonka tehtävänä on tietoturvaloukkausten ennaltaehkäisy, havainnointi, ratkaisu sekä tietoturvauhkista tiedottaminen.
CPU	Central Processing Unit. Keskusyksikkö.
CRL	Certificate Revocation List. Varmenteiden mitätöintilista.
DNS	Domain Name System.
DRM	Digital Rights Management. Sähköisten oikeuksien hallinta. Menetelmä, jolla pyritään kontrolloimaan sähköisen sisällön jakelua.
DSM-CC	Digital Storage Media – Command and Control. Tekniikka, joka mahdollistaa sovellusten lähettämisen osana DVB-ohjelmavirtaa.
DVB(-T/C/S/H)	Digital Video Broadcasting. Eurooppalainen digi-tv-standardi, joka käsittää mm. eri siirtoverkkoteknologiat: – C: Cable – kaapeli, – S: Satellite – satelliitti, – T: Terrestrial – maanpäällinen, – H: Handheld – mobiili-tv.

EPG	Electronic Program Guide. Ohjelmaopas. Yleensä lähetysvirran kautta ladattava sovellus, joka näyttää tietoja tulevista ohjelmista. Päätelaitteissa on myös tyypillisesti laitevalmistajan tekemä ohjelmaopas.
FTP	File Transfer Protocol. Tiedostonsiirtoprotokolla.
FW	Firewall. Palomuuri. Ohjelmisto tai laitteisto, joka valvoo tietokoneeseen tulevaa ja siitä lähtevää tietoliikennettä.
H.263	ITU-T:n standardoima videokompressio.
H.264	ITU-T:n ja ISO/IEC MPEG -ryhmän yhteisesti standardoima videokompressio.
HST	Henkilön Sähköinen Tunnistaminen.
html	HyperText Markup Language. Sivunkuvauskieli.
http	HyperText Transfer Protocol. html:llä kuvattujen sisältöjen siirtoprotokolla.
HW	Hardware. Laitteisto.
ICT	Information and Communications Technology.
ID	Identiteetti.
IDS	Intrusion-detection System. Tunkeutumisen tunnistusjärjestelmä (Tietojärjestelmät).
IP	Internet Protocol. Vastaa päätelaitteiden osoitteistamisesta ja pakettien reitittämisestä verkossa. IPv4 ja IPv6 ovat IP:n eri versioita.
IPSec	IP security. Kokoelma tietoturvaprotokollia IP:hen liittyen.
IRT	Incident Response Team.
ISDN	Integrated Services Digital Network. Piirikytkentäinen digitaalinen puhelinverkkojärjestelmä.
ISO	International Organization for Standardization.
ITU	International Telecommunications Union.

LAN	Local Area Network. Lähiverkko.
LUOTI	Luottamus ja tietoturva sähköisissä palveluissa -ohjelma.
LVM	Liikenne- ja viestintäministeriö.
MHP	Multimedia Home Platform. Avoin sovellusohjelmointirajapinta digi-tv:n vuorovaikutteisille sovelluksille.
MPEG	ISO/IEC: Moving Pictures Expert Group. Joukko liikkuvan kuvan pakkausstandardeja. Digi-tv-maailmassa on käytössä MPEG2. Äänen pakkaukselle käytössä ovat MPEG1 audio layer 1 ja 2.
MPLS	Multiprotocol Label Switching.
NAT	Network Address Translation. Yhdessä verkossa tunnetun IP-osoitteen muuttaminen toisessa verkossa tunnetuksi IP-osoitteeksi.
NNTP	Network News Transfer Protocol. Protokolla uutisartikkeleiden levitykseen, kyselyyn, noutoon ja lähettämiseen luotettavan verkkoyhteyden läpi.
Objektikaruselli	Järjestelmä, joka mahdollistaa sovellusten ja niiden tarvitsemien tiedostojen sekä päätelaitteen ohjelmistopäivitysten lähettämisen digi-tv:n ohjelmasignaalin mukana.
Paluukanava	Tekninen ratkaisu, jolla katsoja voi lähettää palveluntarjoajalle tietoja, hakea sovelluksia tai muuta sisältöä. Tällä hetkellä Suomessa tyypillisesti toteutettu modeemiyhteydellä. Tulevaisuudessa paluukanava on laajakaistainen Internet-yhteys sitä tukevien päätelaitteiden tullessa markkinoille.
PAN	Personal Area Network. Lyhyen kantaman lähiverkko, esim. Bluetooth.
PDA	Personal Digital Assistant.
PKI	Public Key Infrastructure. Julkisen avaimen infrastruktuuri.
POP3	Post Office Protocol version 3. Sähköpostiprotokolla.
PSTN	Public Switched Telephone Network. Kiinteä lankapuhelinverkko.

PVR	Personal Video Recorder. Päätelaitteen ohjelmavirran tallennustoiminto, joka on toteutettu esimerkiksi kovalevyllä.
RA	Registration Authority. Rekisteröijä. Taho, joka todentaa varmenteen hakijan henkilöllisyyden varmennepolitiikan mukaisesti.
RAM	Random Access Memory. Luku- ja kirjoitusmuisti.
ROM	Read Only Memory. Lukumuisti.
S/MIME	Secure Multi-Purpose Internet Mail Extensions. Sähköpostin suojaamiseen tarkoitettu protokolla.
SANS	SysAdmin Audit Network Security Institute.
SATU	Sähköinen asiointitunnus.
SHA	Secure Hash Algorithm. Tiivistealgoritmi, jota käytetään mm. kryptografiassa. Tiivistää syötteen kiinteän pituiseksi tiivisteeksi. Yksisuuntainen eli tiivisteestä ei pysty päättelemään syötettä.
SSID	Service Side Identifier. Tunnus, jonka perusteella kytkeydytään langattoman lähiverkon tukiasemaan.
SSL	Secure Sockets Layer. Tietoliikenteen salausprotokolla.
TCP	Transmission Control Protocol. Vastaa kahden päätelaitteen välisestä tiedonsiirtoyhteydestä, pakettien järjestämisestä ja hukkuneiden pakettien uudelleenlähetyksestä.
TLS	Transport Layer Security. Ks. SSL.
UDP	User Datagram Protocol. Vastaa kahden päätelaitteen välisestä tiedonsiirtoyhteydestä. Kevyempi kuin TCP. Ei järjestä eikä uudelleen lähetä hukkuneita paketteja.
USB	Universal Serial Bus. Sarjaväyläarkkitehtuuri oheislaitteiden liittämiseksi laitteeseen.
VAHTI	Valtionhallinnon tietoturvallisuuden johtoryhmä.
WEP	Wired Equivalent Privacy. Salausjärjestelmä WLAN-verkoissa.
WiFi	Wireless Fidelity. 802.11:n mukainen WLAN.

WLAN	Wireless Local Area Network. Langaton lähiverkko.
VRK	Väestörekisterikeskus.
www	World Wide Web.
X.509	ITU:n suositukset sähköisille varmenteille ja mitätöintilistoille.
xhtml	Extensible Hypertext Markup Language.
xml	eXtensible Markup Language.

Sisällysluettelo

1. Tutkimuksen taustaa

1.1 Selvityksen tavoitteet

Televisioverkon digitalisointi etenee Suomessa verrattain nopealla tahdilla. Digitalisoinnin taustalla on hallituksen 4.3.2004 tekemä periaatepäätös, jonka mukaan televisiolähetykset muuttuvat kokonaan digitaalisiksi 31.8.2007 alkaen. Maanpäällisen digitaalisen tv-jakelun piirissä on laskennallisesti jo noin 94 % väestöstä ja vuoden 2005 loppuun mennessä sen on tarkoitus kattaa 99,9 % väestöstä, kun digitalisoinnin kolmas vaihe on toteutettu [Digi-tv]. Finnpanelin tekemän tutkimuksen mukaan tammikuussa 2005 digisovittimia oli jo yli puolessa miljoonassa kodissa eli 22 % kotitalouksista on varustettu joko antenni-, kaapeli- tai satelliittivastaanottoon tarkoitetulla digisovittimella tai -televisiolla. Näistä kuitenkin vain noin viisi prosenttia oli vuorovaikutteiset palvelut mahdollistavan Multimedia Home Platform (MHP)-standardin mukaisia.

Uusien palvelujen ja teknologioiden tietoturvakysymykset ovat hyvin monimutkainen ongelmakenttä. Tämän hetken digi-tv-verkko on palvelunkehittäjän näkökulmasta turvallinen, koska aidosti vuorovaikutteisia palveluja (ts. palveluja, jotka vaativat paluukanavan) ei ole kovin paljon johtuen mm. niiden vaatimien päätelaitteiden huonosta saatavuudesta. Tilanne tulee lähitulevaisuudessa muuttumaan, kun MHP-standardin mukaiset päätelaitteiden hinnat laskevat ja valikoima kasvaa.

Digi-tv-toimialan arvoverkko on hyvin laaja ja sisältää paljon toimijoita eri rooleissa. Vastuukysymykset esimerkiksi tietoturvaloukkaustapauksissa ovat erittäin ongelmallisia, eikä niihin ole kaikilta osin selviä toimintaohjeita. Televisiolähetys-toiminta on verrattain tarkasti säädeltyä sekä Suomessa että koko EU:n tasolla, mutta arvoverkon riippuvuussuhteet ja uusien palvelujen luonne luovat tilanteita, joissa kaikki tarjottuun palveluun ja sisältöön liittyvät säädökset ja direktiivit eivät ole aina kaikkien arvoverkon toimijoiden tiedossa.

Tulevaisuudessa mobiililaitteet (kännykkä, PDA), digi-tv ja tietokone voivat olla palvelun näkökulmasta vain eri päätelaitteita, joilla voidaan käyttää yhtä ja samaa palvelua. Digitaalisen television näkökulmasta tämä tarkoittaa sitä, että joitakin osia on avattava Internetille ja Internet-protokollan rooli tulee merkittävästi kasvamaan. Kääntöpuolena on nähtävissä turvallisuusriskien kasvaminen; Internet-maailmasta tutut uhkakuvat ovat siirtymässä digi-tv-maailmaan, mikäli uhkia ei tunnisteta ja turvallisuusnäkökulmaa ei oteta riittävästi huomioon palvelunkehitysvaiheessa.

Tämän selvityksen tarkoituksena on tarkastella digitaalisen television ja erityisesti MHP-sovellusten mukanaan tuomia tietoturvauhkia. Selvityksessä pyrittiin löytämään ratkaisuja (sekä teknisiä että palvelunkehitysprosessiin liittyviä), joilla uhkakuviin voidaan vastata. Selvitys antaa kuvan digi-tv-maailmaan liittyvistä teknologioista, uhkista ja MHP-palvelunkehitysprosessin erityispiirteistä.

1.2 Tietoturvan määritelmä

Tietoturvallisuuden kehittämisen päätavoite on hyvän tietojenkäsittelytavan ja asianmukaisen perusturvallisuustason luominen. Tietojen luottamuksellisuutta, eheyttä ja saatavuutta turvataan laitteisto- ja ohjelmistovikojen, luonnontapahtumien sekä tahallisten, tuottamuksellisten tai tapaturmaisten tekojen aiheuttamilta uhkilta ja vahingoilta. Tietoturvallisuus perustuu tiedon kolmeen eri peruskäsitteeseen eli luottamuksellisuuteen, eheyteen ja saatavuuteen:

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

Turvafunktiot kuuluvat myös keskeisesti tietoturvan piiriin. Niiden avulla tietojen-käsittelyn turvaamisen tehtävät voidaan jakaa seuraavasti:

- Väärinkäytösten havaitseminen, ehkäiseminen ja välttäminen
- Korjaustoimenpiteet, elpyminen ja pelotteet.

Turvafunktioiden toteuttamiseksi tietojärjestelmään luodaan kontrolleja, jotka voivat olla esim. politiikka, menetelmä, käytäntö, laite, tai ohjelmoitu mekanismi.

Määritelmät:

Tietoturva: 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).*

Tietoturvallisuus: eri muodossa olevien tietojen ja palvelujen, järjestelmien ja tietoliikenteen suojaamista niihin kohdistuvien riskien hallitsemiseksi soveltuvilla toimenpiteillä. Tietoturvallisuus on laajempi käsite kuin vain tieto- ja viestintä-teknologioiden tekninen turvallisuus. *(Yritysten tietoturva-tietoisuustyöryhmä, [YRTI]).*

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

1.3 Yrityshaastattelujen antamat suuntaviivat

Selvityksessä pyrittiin kartoittamaan digi-tv-palvelujen nykytilaa ja palvelunkehittäjän näkökulmaa haastattelemalla alan toimijoita Suomessa ja muualla. Haastattelun tavoitteena oli lisäksi selvittää digi-tv-alan arvoverkkoa ja sen eri osiin kohdistuvia uhkia eri toimijoiden mielestä ja pyrkiä tunnistamaan palvelunkehitysprosessiin liittyviä erityispiirteitä. Haastatteluissa selvitettiin digitaaliseen televisiotoimintaan vaikuttavaa arvoverkostoa. Digitaalisen television ohjelmien tuotanto voidaan jakaa viiteen päävaiheeseen. Nämä ovat ohjelmien tuotanto, palvelujen tuotanto, paketointi, jakelu ja kuluttaminen. Haastattelussa käytettiin keskustelun pohjana kysymysrunkoa, joka on esitetty liitteessä A. Arvoverkkoa ja palvelunkehitysprosessia on käsitelty tarkemmin kappaleessa 5. Tässä kappaleessa esitetään yhteenvetona yrityshaastattelun esiin tuomia näkökulmia.

Haastatteluissa todettiin, että tämän selvityksen kannalta on keskeistä pohtia kuhunkin näihin vaiheisiin liittyviä tietoturvakysymyksiä, mahdollisia ongelmia, uhkia ja niiden ratkaisuja.

Tämän hetken suurimmaksi uhkatekijäksi digitaalisen television kentässä nähdään päätelaitteen ja digisovittimen turvallisuus. Päätelaite on verrattain haavoittuva virheelliselle datavirralle, mistä nähtiin esimerkki, kun keväällä 2004 virheellinen ohjelmavirta vioitti päätelaitteita Suomessa (Tietoviikko 15.4.2004). MHP-sovellusten yleistyessä päätelaitteiden tietoturva tulee entistä tärkeämpään asemaan ja ratkaistaviksi kysymyksiksi nousevat esimerkiksi sovelluksen alkuperän tunnistaminen, päätelaitteen suojaaminen (virustarkistus, palomuurit) ja katsojan yksityisyyteen liittyvät kysymykset. Yleinen näkemys oli, että tietoturvan suhteen päätelaitteen hankkija on hyvin pitkälti laitevalmistajan armoilla, koska tekniset ratkaisut ovat lähes poikkeuksetta laitekohtaisia siitä huolimatta, että laitteiden teknisille ratkaisuille on olemassa standardoidut määritykset. Nämä määritykset ovat kuitenkin verrattain väljiä ja se mahdollistaa saman toiminnallisuuden toteuttamisen usealla, toisistaan poikkeavalla tavalla. Eksoottisempiin ratkaisuihin joudutaan varsinkin, kun on tarvetta tehdä kompromisseja muistinkulutuksen tai laskentatehon rajoitusten vuoksi.

Yleisesti uhkat voivat kohdistua erityisesti ohjelmasisältöihin, päätelaitteisiin ja kuluttajan tietosuojaan. Näistä erityisen vahingollisia tv-toiminnan luotettavuudelle olisivat sisältöön kohdistuvat väärinkäytökset, esimerkiksi tilanteet, joissa ohitetaan todellinen sisältö väärennetyllä sisällöllä tai vahingoitetaan päätelaitetta ohjelmallisesti.

Päätelaitteisiin kohdistuvat hyökkäykset joutuisivat useissa tapauksissa käyttämään hyväkseen toteutustason yksityiskohtia, joten sama hyökkäys ei usein toimisi kaikkia päätelaitteita vastaan. Toisaalta eri valmistajien päätelaitteet käyttävät paljon samoja ohjelmistokomponentteja. Esimerkiksi MHP:n Java-alusta ja digisovittimen käyttöjärjestelmä ovat niin suuria ohjelmistokokonaisuuksia, että päätelaitevalmistajien kannattaa usein lisensoida ne kolmansilta osapuolilta, tai valmistuttaa tai lisensoida koko laitteisto- ja ohjelmistokokonaisuus ulkopuolelta. Java-toteutuksissa on ollut historiallisesti paljon haavoittuvuuksia, joiden avulla Java-ohjelma voi saada kohdejärjestelmässä laajemmat oikeudet kuin mitä sille kuuluisi ja päästä käsiksi alla olevaan käyttöjärjestelmään ja laitteistoon.

Todennäköisimpinä voidaan pitää hyökkäyksiä, joilla pyritään murtamaan tietyn valmistajan Java-toteutus. Tällaiset hyökkäykset aiheuttavat merkittävän taloudellisen riskin. Yksittäisten päätelaitteiden tuhoaminen on marginaalisempi ongelma ja päätelaitteiden kirjavuudesta johtuen kaikkiin laitteisiin kohdistuvat hyökkäykset ovat suhteellisen epätodennäköisiä. Todennäköisempänä voidaan pitää hyökkäyksiä, joilla yritetään kaataa jonkin tietyn laitevalmistajan tietyntyyppisiä laitteita. Tällaiset hyökkäykset ovat ikäviä loppukäyttäjän kannalta, mutta eivät sinällään aiheuta merkittävää taloudellista tai poliittista riskiä. Kuluttajan tietoturvaan kohdistuvat uhkat, kuten roskaposti ja yksityisyyden suojaan liittyvät ongelmat, ovat luonnollisesti kriittisiä.

Nykymuodossaan järjestelmään kohdistuvat uhkat eivät kosketa laajoja kuluttajaryhmiä, koska todellisten interaktiivisten palvelujen määrä on vielä suhteellisen pieni. Kun interaktiivisuus digitaalisessa televisiossa lisääntyy, tietoturvakysymykset kiteytyvät erityisesti päätelaitteeseen ja paluukanavaan liittyviin asioihin. Erityisesti loppukäyttäjän asema interaktiivisuuden lisääntyessä on tietoturvan kannalta asia, johon tulisi kiinnittää huomiota. Digitaaliseen televisioon liittyvistä standardeista erityisesti MHP on tietoturvaselvityksen näkökulmasta keskeinen. Tarkemmin MHP:hen liittyviä kysymyksiä on selvitetty kappaleessa 3.

Digitaalisen televisiotoiminnan todettiin haastatteluissa olevan vielä varsin tiivistä yhteistyötä muutamien keskeisten toimijoiden välillä, mutta tarve yhteistyön koordinoinnille ja organisoinnille toimijakentän laajetessa tulee lisääntymään. Toimijakenttä tulee varsin todennäköisesti muuttumaan lähitulevaisuudessa palvelujen määrän kasvaessa ja digitaalisen televisiotoiminnan kehittyessä interaktiivisempaan suuntaan. Toistaiseksi markkinat ovat vielä varsin pienet ja siitä johtuen tuotekehityspanos, joka tietoturvaan on mahdollista laittaa, on suhteellisen pieni.

Riskianalyysi on palvelunkehityksessä erityisen keskeisessä asemassa. On tarkkaan pohdittava, mitä riskejä on olemassa ja mitkä niistä todella vaativat toimenpiteitä. Kaikkia riskejä vastaan suojautuminen ei ole mahdollista, eikä taloudellisesti järkevää.

Tietoturva-asiantuntijan osallistuminen palvelunkehitykseen heti suunnitteluvaiheesta lähtien on järkevää riskien hallintaa.

Haastatteluissa todettiin, että tällä hetkellä huomattavia puutteita lainsäädännössä ei ole olemassa. Tästä syystä lainsäädännöllisten kysymysten pohtiminen rajataan tämän selvityksen ulkopuolelle. Voidaan kuitenkin todeta, että sähköisen viestinnän tietosuoja-direktiivi kieltää digitaalisessa televisiovastaanotossa tallennetun tilaajaan tai käyttäjään liittyvän viestinnän tiedon, kuten kanavavalintojen, kellonaikojen, katsottujen mainosten tai pelattujen pelien, kuuntelun ja siirron palvelun tarjoajalle. Lisäksi sähköisten palvelujen kehittäjän on otettava huomioon erityisesti yksityisyyteen vaikuttava lainsäädäntö, jota on käsitelty kappaleessa 4.2.4, sekä sähköiseen kaupankäyntiin liittyvät säännökset.

2. Lyhyt teknologiakatsaus

2.1 Lyhyt internet-verkon ja protokollien kuvaus

IP-protokollan suurimpia etuja ovat sen joustavuus, yksinkertaisuus ja mahdollisuus eri fyysisten siirtoteiden käyttöön sekä sen reititysmallin tuoma toimintavarmuus. IP-pohjainen arkkitehtuuri on ollut vallalla tietoliikenteessä 90-luvulta lähtien.

Internet on nippu yhteensovitettuja IP-verkkoja. Laitteen liittäminen Internetiin tarkoittaa siis vain sen yhdistämistä verkkoon muiden verkon laitteiden kanssa käyttäen tiedonsiirron verkkokerroksena IP-protokollaa. Fyysisenä siirtotienä voi tällöin toimia mikä tahansa yhteys, kuten esimerkiksi ISDN, ATM, UMTS tai GPRS. Internetiin liitettävä laite saa IP-osoitteen, jonka ei välttämättä tarvitse edes olla globaali, vaikka se protokollaperheen alkuperäiseen filosofiaan kuuluukin.

IP-verkoissa tiedonsiirtoon käytetään TCP- ja UDP-protokollia, ja näin muodostuvan TCP/IP-protokollaperheen päälle voidaan rakentaa hyvin erilaisia sovelluksia. IP toimii siis monenlaisten verkkojen päällä ja sen päälle voidaan rakentaa melkein mitä tahansa. Tämä onkin ollut tärkeänä syynä tekniikan suosioon: IP-tekniikoita voidaan hyödyntää olemassa olevaa infrastruktuuria käyttäen, ja toisaalta uusiin siirtotekniikoihin siirtyminen onnistuu ilman muutostarpeita verkkoihin ja sovelluksiin. Nykyisin puhutaan usein ns. all-IP-verkoista, joissa perinteisistä tekniikoista, kuten puhelin-verkoista, siirrytään käyttämään IP-pohjaisia ratkaisuja.

Teknisesti katsottuna TCP/IP-protokollaperheeseen kuuluu mitä moninaisimpia eri palveluja toteuttavia protokollia. Näihin palveluihin kuuluvat eri reititystekniikat, verkonhallinta, verkkopakettien kuljetus eri tavoin, hakemistopalvelut, autentikointi, verkkolaitteiden hallinta, tiedostojen siirto, sähköpostin välitys eri tavoilla, www-sivujen välitys, äänen ja liikkuvan kuvan välitys, palvelunlaadun hallinta, IP-pohjaisten puhelujen hallinta ja niin edelleen. Nämä protokollat ovat harvemmin palvelujen näkyvinä osina, mutta toimivat niiden tärkeinä tukiresursseina.

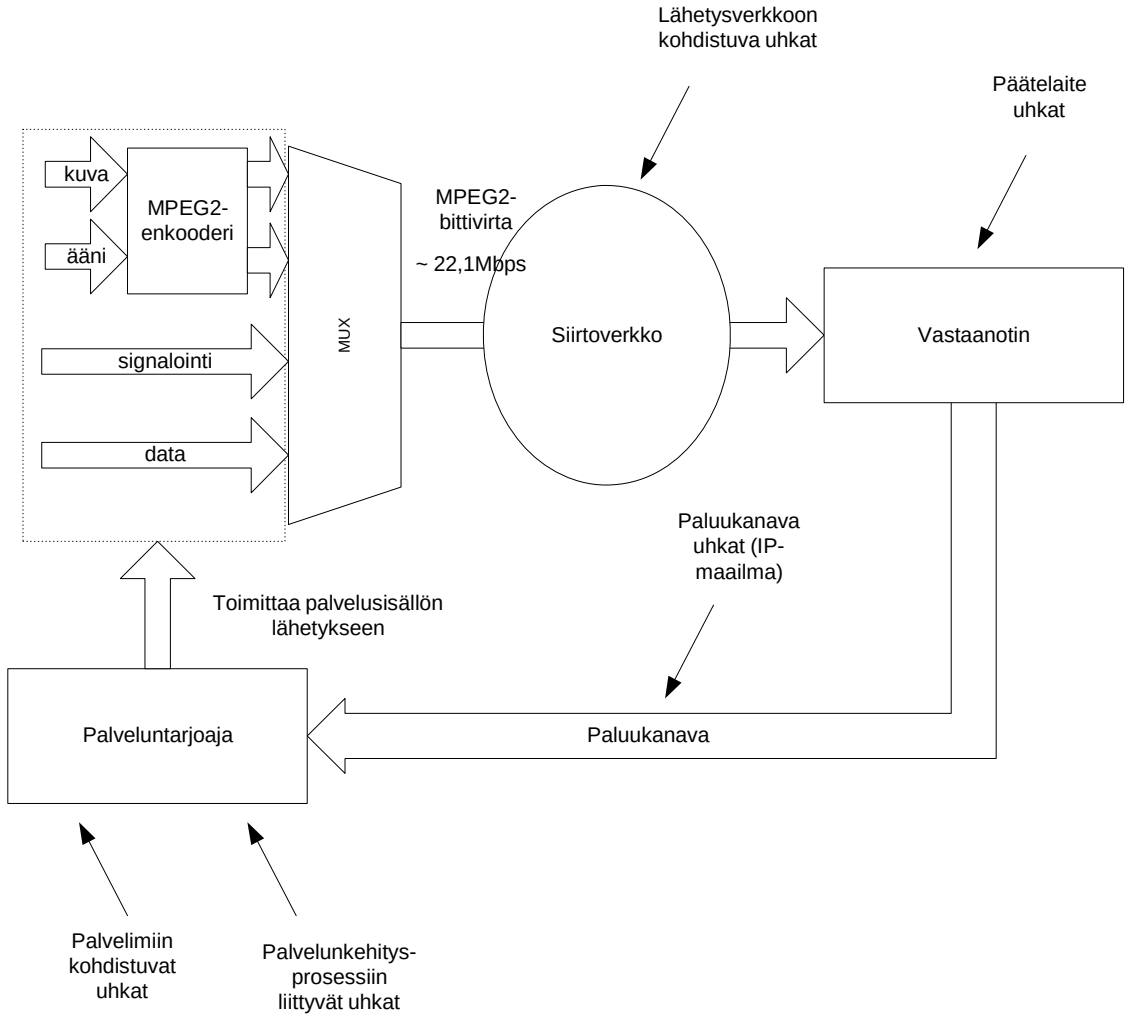
Käyttäjien näkökulmasta tärkeimmät Internetin palvelut ovat www-selaus ja kommunikaatiopalvelut, kuten sähköposti, uutisryhmät sekä pikaviestintä. Selauksen osuus Internet-palveluista on selvästi ylikorostunut, usein käyttäjien ja mediankin mielestä Internet käsitetään synonyymiksi www:lle. Selaimilla käsitellään monenlaista passiivista ja aktiivista sisältöä ja eri pankki-, kauppa- ja virastopalveluja siirretään verkkoon voimakkaasti. Internetin merkityksen voi nähdä tulevaisuudessa vain kasvavan yhä useampien toimintojen siirtyessä verkkoon, esimerkiksi verkon välityksellä äänestämisestä on jo tehty pilottiprojekteja.

Suosiotaan Internet-palveluina ovat myös lisäämässä IP-puhelut ja erilaiset yksi-suuntaiset ja vuorovaikutteiset video- ja äänipalvelut monilähetys- ja palvelunlaatu-tekniikoineen.

2.2 Lyhyt digi-tv-järjestelmien kuvaus

2.2.1 Lähetysverkko ja -teknologiat

Digitaalinen televisio Suomessa perustuu DVB-standardeihin [DVB]. Maanpäälliset verkot käyttävät DVB-T-standardia, kaapeliverkoissa on käytössä DVB-C ja satelliitti-lähetykset pohjautuvat DVB-S-standardiin. Liikkuvissa päätelaitteissa voidaan hyödyntää DVB-H-standardia, joka pohjautuu DVB-T:hen. Standardit eroavat toisistaan lähinnä eri siirtoteille optimoitujen modulointimenetelmien osalta. Päätelaitteet eroavat toisistaan vastaavasti. Tietovirta digitaalisessa televisioverkossa on toistaiseksi pääasiassa DVB:n avulla tapahtuvaa äänen ja kuvan siirtoa suljettua verkkoa pitkin lähettäjältä vastaanottajalle. Kuvan ja äänen lisäksi digi-tv:n kautta voidaan lähettää myös dataa ja tuottaa datapalveluja. Kuvassa 1 on esitetty digitaalisen jakeluverkon yleisen tason lohkokaavio, joka ei ota kantaa siirtotien tyyppiin (maanpäällinen, kaapeli tai satelliitti). Kuvassa on myös esitetty eri osiin kohdistuvat uhkat. Palvelunkehittäjä voidaan tässä käsittää sisällöntuottajaksi, kehittäjäksi ja paketoijaksi. Järjestelmässä kuva ja ääni koodataan MPEG2-standardin [MPEG2] mukaisesti enkooderissa ja samalla tavalla koodatut palvelut yhdistetään yhteen MPEG2-kuljetusbittivirtaan multiplekserin (MUX) toimesta. Yhdestä kuljetusbittivirrasta käytetään myös nimitystä kanavanippu. Kuvan ja äänen sekä palvelujen vaatiman merkinantotiedon lisäksi jakeluverkossa voidaan välittää myös dataa käyttäen IP-protokollan mukaisia palveluja [Södergård 1999], [FICORA].



Kuva 1. Digitaalinen jakeluverkko ja sen eri osiin kohdistuvat uhkat.

Seuraavassa lyhyt yhteenveto DVB-standardeista ja niiden tärkeimmistä eroista. Kaikkia DVB-muotoihin liittyy lukuisia eri parametreja. Nämä parametrit asetetaan lähetteelle suunniteltujen vastaanotto-olosuhteiden mukaan siten, että saadaan aikaan mahdollisimman tarkoituksenmukainen kompromissi lähetteen kaistanleveyden ja näkyvyyden välille.

DVB-S

DVB-S-järjestelmä on suunniteltu toimimaan kaikilla satelliittiviestinnän kaistanleveyksillä. Se on DVB-standardeista vanhin ja yleisimmin käytetty. Kaikki data on vakiokokoisina DVB-TS-paketteina. DVB-S käyttää QPSK-modulointia.

DVB-T

DVB-T:ssä perustana ovat MPEG2-paketit ja lähetykset perustuvat COFDM-modulaatioon. DVB-T:ssä on optimoitu kyky toimia erilaisissa lähetysympäristöissä, mikä tekee siitä monikäyttöisen.

DVB-C

DVB-C perustuu DVB-S:ään, siinä käytetään QAM-modulointia. Lisäksi paketin sisäistä virheenkorjausta ei tarvita.

DVB-H

DVB-H on maanpäällinen digi-tv-standardi, joka pohjautuu DVB-T-standardiin ollen taaksepäin yhteensopiva sen kanssa. Merkittävämpänä erona on pienempi virrankulutus ja parempi tuki liikkuvalle vastaanottimelle. DVB-H-standardissa käytetään DVB-T-verkkoa IP-liikenteen välittämiseen. Tämä tunnetaan yleisnimikkeellä IP-Datacasting. DVB-H-standardin mukaiset päätelaitteet, kuten kännykät ja PDA-laitteet, voivat siis vastaanottaa digi-tv-lähetyksiä käyttäen maanpäällistä digi-tv-verkkoa (DVB-T), jolloin signaalin siirtämiseen ei käytetä lainkaan matkapuhelinverkkoja. DVB-H ei ota kantaa videon pakkaukseen; tyypillisesti käytetään H.263- ja H.264-koodekkeja (MPEG4). DVB-H:ssa kanavanipun parametrit asetetaan siten, että mobiilivastaanotto helpottuu (mm. virransäästön vuoksi). Kanavanipun koko on 10 Mbit/s, yhden kanavan vaatima datavirta on noin 256 kbit/s.

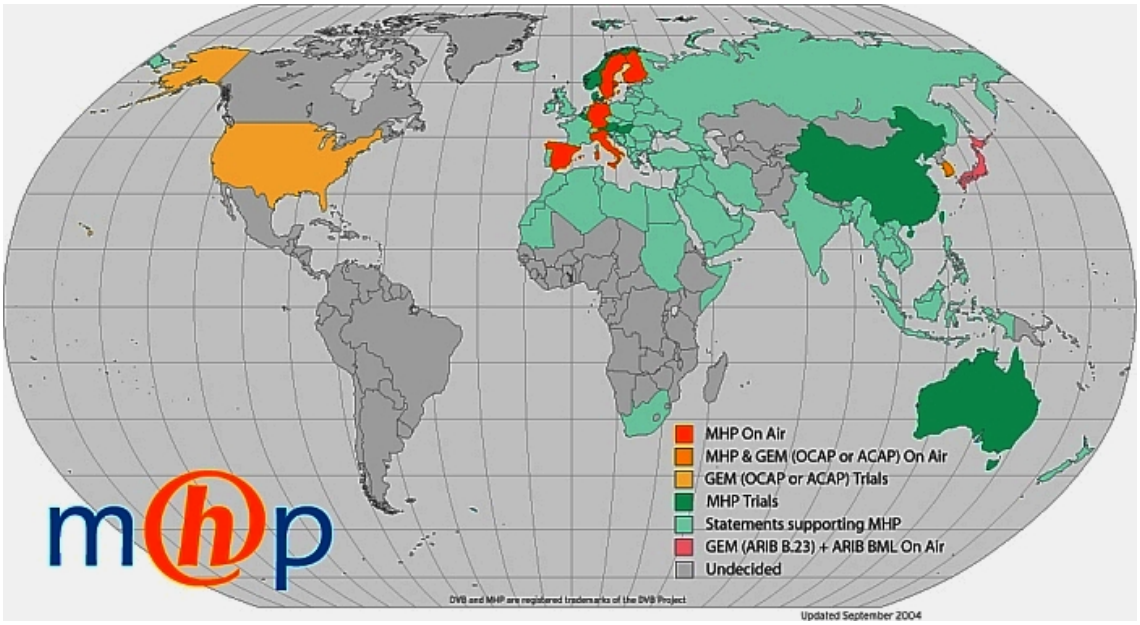
Sovellusympäristönä DVB-H muistuttaa MHP:ta. Päätelaitteen rajoitukset esimerkiksi ruutukoon ja resoluution suhteen tuovat palvelunkehitykseen kuitenkin omat erityispiirteensä. PDA-laitteiden kosketusnäytöt tarjoavat myös uusia mahdollisuuksia esimerkiksi käyttöliittymien teossa. Kännykkä on päätelaitteena televisiota henkilökohtaisempi ja käyttötottumukset hyvin erilaisia perinteiseen television katsomiseen verrattuna. DVB-H-vastaanotto voidaan toteuttaa päätelaitteessa mediakännyköistä tyypillisillä tekniikoilla.

DVB-IP (IPTV)

IPTV-teknologia perustuu Internet-protokollan käyttöön sekä ohjelmanjakelussa että paluukanavassa. Kotipäätteeksi vaaditaan DVB-IP-määrityksen mukainen laite. Yhden ohjelman välittäminen vaatii siirtonopeudeksi 2–5 Mbit/s, mikä tarkoittaa käytännössä vaatimusta vähintään 8 megabitin laajakaistaliittymän käytöstä. Liiketoimintamalliltaan IPTV rinnastetaan kaapelijakeluun eli sillä on must carry -velvoite, jonka mukaan korvauksettoman jakeluvelvoitteen alaiset digi-tv-lähetykset on jaettava verkossa salaamattomina niin, että ne voidaan vastaanottaa ilman lisämaksuja ja ylimääräisiä, esimerkiksi salauksenpurkujärjestelmistä aiheutuvia kustannuksia. Laajakaistainen paluukanava mahdollistaa tilaajakohtaiset palvelut, kuten esimerkiksi tilausvideo-palvelun (Video-on-Demand).

2.2.2 Multimedia Home Platform (MHP)

DVB-organisaatio alkoi vuonna 1998 kehittää standardia lisäarvopalvelujen kehittämistä varten. Tämän työn tuloksena syntyi Multimedia Home Platform (MHP), jonka myös Suomi on valinnut vuorovaikutteisten lisäarvopalvelujen toteutus-teknologiaksi. Tällä hetkellä MHP-standardien mukaisia palveluja lähetään Suomen lisäksi Ruotsissa, Saksassa, Italiassa ja Espanjassa, joista varsinkin Italiaa pidetään edelläkävijänä Euroopassa MHP:n käyttöönotossa. MHP-kokeiluija ja MHP:ta tukevia julkilausumia on tehty lähes kaikissa Euroopan maissa.



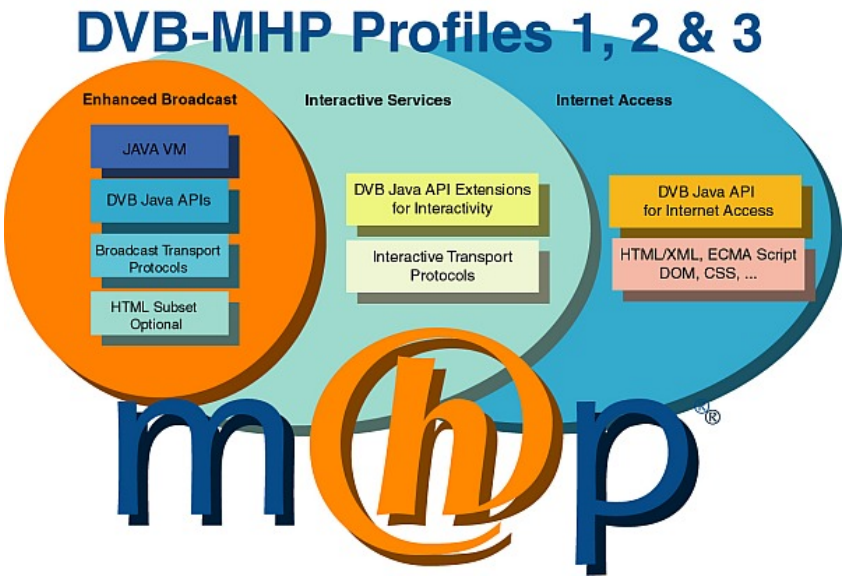
Kuva 2. MHP:n levinneisyys (www.mhp.org).

MHP on avoin standardi ja se määrittelee yleiskäyttöisen rajapinnan vuorovaikutteisten sovellusten ja päätelaitteen (digisovitin) välille. Sovellukset kirjoitetaan Java-ohjelmointikielellä ja Xhtml-sivunkuvauskielellä, jolloin ohjelmavirran mukana lähetetään myös Java-pohjainen selain. Tällä varmistetaan sovellusten alusta-riippumattomuus laitteisto- ja käyttöjärjestelmätasolla. MHP-arkkitehtuuri voidaan kuvata kolmen kerroksen avulla, jotka on esitetty taulukossa 1 [MHP].

Taulukko 1. MHP:n arkkitehtuurin osat.

Kerros	**Tehtävä**
Resurssit	MPEG-muotoisen signaalin demultipleksointi, audio- ja videosignaalin käsittely, I/O-laitteet, suoritin (CPU), muisti- ja grafiikkaresurssit.
Järjestelmäohjelmisto	Käyttää resursseja tarjotakseen korkeamman tason näkymän alustasta sovelluksille.
Sovellukset	MHP-toteutukset sisältävät sovellushallinnan (”navigator”), joka ohjaa MHP-alustaa ja sovelluksia joita siinä ajetaan.

MHP-standardi sisältää kolme erilaista profiilia, jotka on esitetty kuvassa 3.



Kuva 3. MHP:n profiilit (www.mhp.org).

Ne on kehitetty helpottamaan standardien käytännön toteutusten tekemistä. Profiili viittaa sovellusalueeseen ja myös päätelaitteen ominaisuuksiin. MHP:n kolme profiilia ovat:

1. Enhanced broadcast (Parannettu lähetys)
   Profiili tehtiin vastaamaan toiminnaltaan monia olemassa olevia välitason järjestelmiä ja niissä ajettavia sovelluksia. Tämä profiili edustaa suorituskyvyltään alimman tason päätelaitteita, joissa ei ole lainkaan paluukanavaa.

2. Interactive services (Vuorovaikutteiset palvelut)
   Tämä profiili sisältää päätelaitteet, joissa on kehittyneemmät paluukanava-ominaisuudet. Merkittävin ero profiiliin 1 on, että tässä profiilissa on mahdollisuus ladata sovelluksia ohjelmavirran mukana, kun profiilissa 1 sovellusten lataaminen ei onnistu. Vuorovaikutteisuus on tuettu myös ohjelmointirajapinnan osalta.

Internet Access Profile määrittää päätelaitteeseen paikallisen selainsovelluksen sekä rajapinnan, jolla tätä selainta voidaan hallita.

3. Internet access (Internet-käyttö)
   MHP-standardin kehittynein profiili. Päätelaite on edellisten profiilien määrittelemiä päätelaitteita tehokkaampi ja siinä on enemmän muistia. Profiili keskittyy Internet-sisällön käyttöön digi-tv-vastaanottimella.

   MHP-laitteen Internet-käyttö tuskin koskaan korvaa henkilökohtaista tietokonetta. Resurssien rajallisuus, käyttöliittymän rajoitukset ja mahdolliset paluukanavaan liittyvät rajoitukset, esimerkiksi käytettävissä olevien protokollien suhteen, rajaavat Internet-sisällön verrattain yksinkertaisiin sähköposti- ja nettisurffailu-tyyppisiin (esim. pankkien tarjoamat verkkopalvelut) sovelluksiin.

   MHP:n ydin perustuu DVB-J-alustaan, joka sisältää Sun Microsystemsin tekemän Java Virtual Machine Specification -määrityksen mukaisen virtuaalikoneen ja ohjelmointirajapinnan (API), jonka kautta MHP-sovellukset käyttävät alustan tarjoamia resursseja ja järjestelmätason ohjelmiston palveluja.

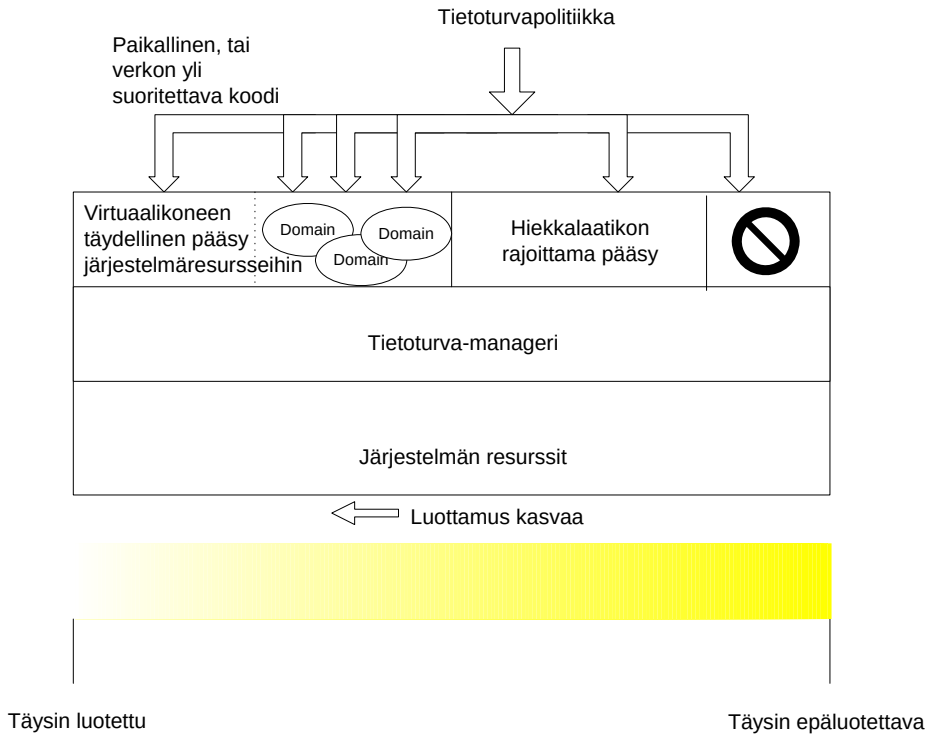
Tavallisen tv-katselijan näkökulmasta digi-tv:n interaktiivisuus perustuu tällä hetkellä lähinnä MHP1.0.2-standardiin. MHP1.1 on uusi standardi, jonka käyttöönoton myötä digisovittimiin voidaan ladata sovelluksia paluukanavan kautta, kun MHP1.0.2 mahdollistaa sovellusten lataamisen ainoastaan ohjelmavirran mukana. Tulossa oleva MHP1.1-standardi tuo mukanaan uusia tietoturvariskejä, jotka liittyvät suurimmaksi osaksi paluukanavan käyttöön, mutta toistaiseksi MHP1.1:n mukaisia päätelaitteita ei ole myynnissä.

Koska MHP-alusta ja sen ohjelmointirajapinnat perustuvat Javaan, kehittäjän on otettava huomioon Javan tietoturvaominaisuudet; sen tarjoamat edut ja rajoitukset.

Java on oliopohjainen ohjelmointikieli ja se on alusta asti suunniteltu verkotettujen ohjelmistojen kehittämiseen ja tarjoamaan turvallisen tavan ladata sovelluksia verkon yli. Tämä ei ole kuitenkaan toteutunut täysin aukottomasti Java-toteutuksissa; haavoittuvaisuuksia, joissa sovellus voi rikkoa sille asetettuja käyttöoikeusrajoituksia, esiintyy aika ajoin. Javan pääkomponentteja ovat tavukoodi ja virtuaalikone, jossa koodi ajetaan. Javan virtuaalikone piilottaa sovellukselta käyttöjärjestelmän ja laitteiston, joten Javasta voinee puhua pelkän ohjelmointikielen sijaan ohjelmistoalustana. Java on verkotettujen ohjelmistojen kannalta parempi alusta kuin perinteiset C-pohjaiset alustat, koska siihen sisäänrakennettua tietoturvamallia on kehitetty eteenpäin aina Javan ensimmäisistä versioista lähtien. Javan sovellusohjelmointirajapinnat tarjoavat tuen salakirjoitustekniikoille ja julkisen avaimen menetelmille, mukaan lukien varmenteisiin pohjautuva X.509 käyttäjäntunnistuskehys, jota myös MHP-määritykset hyödyntävät sovelluksen alkuperän tarkistamisessa.

Muiden sovellusten X.509-toteutuksissa on ollut jonkin verran sellaisia tietoturva-haavoittuvuuksia, jotka mahdollistavat X.509-toteutukseen murtautumisen sekä sellaisia, jotka mahdollistavat X.509-pohjaisen varmennuksen ohittamisen.

Kuvassa 4. on esitetty Javan tietoturvamalli. Se tarjoaa eri tavoin rajoitetun pääsyn järjestelmäresursseihin riippuen suoritettavan koodin tietoturvapolitiikasta ja alku-perästä. Näiden perusteella määräytyy ohjelman luotettavuus ja se, kuinka paljon ohjelma saa oikeuksia kohdejärjestelmässä. Toisessa päässä on täysin luotettava sovellus, jonka toimintaa ei rajoiteta ollenkaan; vastakohtana täysin epäluotettava sovellus, jonka käynnistämistä ei sallita ollenkaan. Java käyttää käyttöoikeuksien rajoittamisesta termiä hiekkalaatikko, joita voidaan määritellä esimerkiksi erityyppisille palvelunkehittäjille omansa (laitevalmistaja, operaattori, kolmas osapuoli).



Kuva 4. Javan tietoturvamalli.

Javan tietoturvapolitiikka on käytännössä sovelluksen mukana tuleva ”oikeuksien pyyntö” -tiedosto (permission request). Kuvassa 5. on esitetty esimerkin omaisesti tällainen tiedosto [MHP]. MHP:ssä on käytössä Javan oma tietoturvapolitiikka sekä MHP:n määrittelemä politiikka. Tämän käytännön toteutus vaihtelee eri päätelaitteiden välillä. MHP-standardissa on jätetty tarkoituksellisesti avoimeksi, mitkä käyttöoikeus-pyynnöt jäävät käyttäjän hyväksyttäväksi. Näin ollen tietoturvapolitiikka tämän osalta on jätetty markkinoiden, kuluttajien ja valvovien viranomaisten tehtäväksi.

Toukokuussa 2005 Suomessa ei ole käytössä MHP:hen oikeuksien pyyntötiedostoa, vaan sovellus saa Javan virtuaalikoneen puitteissa kaikki oikeudet, joskin digisovittimissa voi olla laitevalmistajakohtaisia rajoituksia, jotka ovat tiukempia kuin Javan tietoturvamalli.

```
<?xml version="1.0"?>
<!DOCTYPE permissionrequestfile
  PUBLIC "-//DVB//DTD Permission Request File 1.0//EN"
  "http://www.dvb.org/mhp/dtd/permissionrequestfile-1-0.dtd">

<permissionrequestfile orgid="0x000023d2" appid="0x0020">

  <file value="true"></file>

  <capermission>
    <casystemid
      id="0x1111" messagepassing="true"
      entitlementquery="true" mmi="false">
    </casystemid>
  </capermission>

  <applifecyclecontrol value="true"></applifecyclecontrol>

  <returnchannel>
    <defaultisp></defaultisp>
    <phonenumber>+3583111111</phonenumber>
    <phonenumber>+3583111112</phonenumber>
    <phonenumber></phonenumber>
  </returnchannel>

  <tuning value="false"></tuning>
  <servicesel value="true"></servicesel>
  <userpreferences read="true" write="false"></userpreferences>

  <network>
    <host action="connect">hostname</host>
  </network>

  <persistentfilecredential>
    <grantoridentifier id="0x0202030"></grantoridentifier>
    <expirationdate date="24/12/2032"></expirationdate>
    <filename read="true" write="false">
      5/15/dir1/scores
        </filename>
    <filename read="true" write="false">
      5/15/dir1/names
    </filename>
    <signature>
      02320329329293293292149314392942394329423943
    </signature>
    <certchainfileid>3</certchainfileid>
  </persistentfilecredential>


</permissionrequestfile>
```

Kuva 5. Javan Permission Request -tiedosto.

Palvelunkehittäjän näkökulmasta Java tarjoaa samat tietoturvatyökalut ja -ratkaisut laitteistosta riippumatta, jos vain virtuaalikone on toteutettu standardin mukaisesti. Taulukossa 2. on esitetty Suomessa tähän mennessä tehtyjä MHP-palveluja, joita tarjotaan maanpäällisessä tai kaapeliverkossa.

Taulukko 2. MHP-Palveluita Suomessa *2.5.2005* (*lähteet: Yleisradio, Mtv3, Ortikon Interactive, Sofia Digital ja Digita, www.digitv.fi*).

Uutispalvelut	**Uutiset (kotimaa, ulkomaa, urheilu)**	• Ylen supertekstitelevisio • Uutisrulla (Yle) • MTV3 Tekstikanava (MTV3, MTV3+, Subtv) • FST:n uutiset (Yle) • Savon Sanomat • Netlari • Kaleva • Olet.info • Radio 957
	Säätiedot	• Ylen supertekstitelevisio • MTV3 Tekstikanava (MTV3, MTV3+, Subtv)
	Talousuutiset	• Kauppalehti/MTV3 Tekstikanava (MTV3, MTV3 + Subtv)
Ohjelmaoppaat	**Tulevat elokuvat ja sarjat**	• MTV3 Tekstikanava (MTV3, MTV3 + Subtv) • Nelosen supertekstitelevisio (Nelonen, Nelonen+)
	Lähiajan ohjelmatiedot	• Ohjelmaopas (kaikki digi-tv-kanavat, suomen- ja ruotsinkielinen)
Viihde	**Pelit**	• Muistipeli (Yle) • NE-spelet (Yle) • Lotto (koekäytössä) (MTV3, MTV3 + Subtv) • OBlox • Klondike
	Ohjelmakohtaiset palvelut	• G5, Käenpesä, Joka kodin asuntomarkkinat, T.i.l.a., Ruokala.tv, SM-liiga Hockey Night (MTV3) • Food: Impossible, Anarkistit, SubLeffat (Subtv)
Muut	**Yhteiskuntapalvelut**	• Eduskuntafakta (Yle) • Postin digi-tv-palvelu (lähetä sähköinen joulukortti Postin digi-tv-palvelulla)
	Pankkipalvelut	• Osuuspankin Digi-tv-palvelu (MTV3, MTV3 + Subtv)
	Viestintä	• Sähköposti ja chat-palveluja • Lupiini Deitti • Sooda-Portal

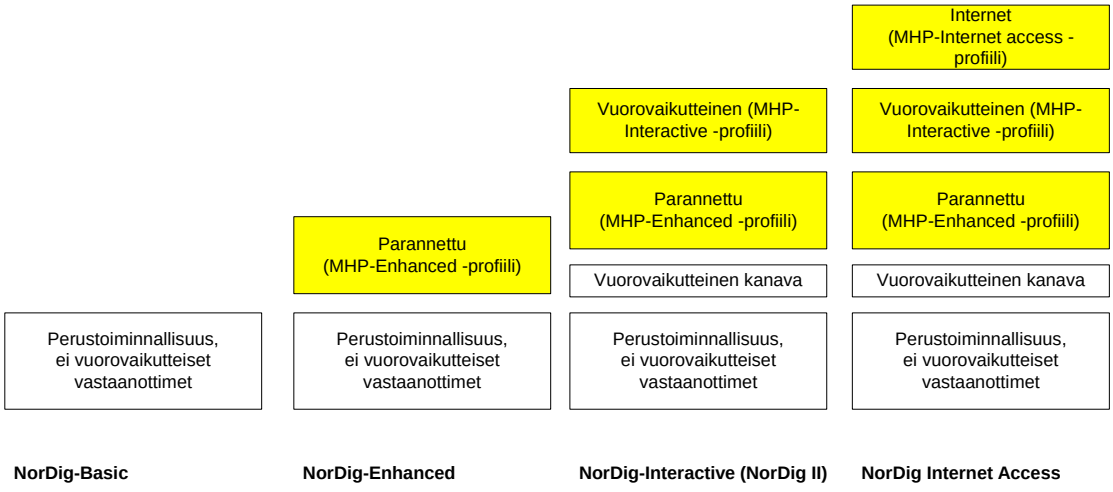
2.2.3 Päätelaitteet

Päätelaitteiden eli digisovittimien yleistyminen on tällä hetkellä tärkein tekijä interaktiivisten palvelujen yleistymisessä. Tällä hetkellä on nähtävissä muna-kana-ongelma interaktiivisten MHP1.1.-palvelujen kohdalla; MHP1.1-yhteensopivat päätelaitteet eivät yleisty, koska palveluja ei vielä ole ja toisaalta uusia palveluja ei voimallisesti kehitetä, koska päätelaitteita ei ole vielä markkinoilla. Ensimmäiset sovittimet tarjosivat perusominaisuudet digitaalisen televisionlähetyksen vastaanottamiseen ja kortinlukijalla varustetut mallit mahdollistivat myös maksullisten tv-kanavien vastaanottoon. Toisen kehitysvaiheen päätelaitteiksi voidaan lukea kovalevylliset digisovittimet, jotka mahdollistavat ohjelmien tallennuksen (PVR, Personal Video Recorder) ja nk. ajansiirron (time-shifting), jossa katsoja keskeyttää televisiosta tulevan ohjelman katsomisen esimerkiksi puhelun takia ja jatkaa puhelun jälkeen

katsomista siitä mihin jäi. Tällä hetkellä myynnissä olevissa MHP-standardia tukevissa päätelaitteissa ei ole kovalevyä. Kolmas kehityssukupolvi tuo tullessaan aidosti interaktiivisen digisovittimen eli siis MHP1.1-standardin mukaisen laitteen. Tämä monipuolistaa palvelutarjontaa ja maksullista sisältöä. Konvergenssi nykyisen Internet-maailman kanssa lähenee vuorovaikutteisen kanavan myötä. Tässä kappaleessa esitellään Suomen markkinoiden kannalta tärkein päätelaitemääritys, NorDig, sekä Italian DGtvi D-Book -määritys.

NorDig

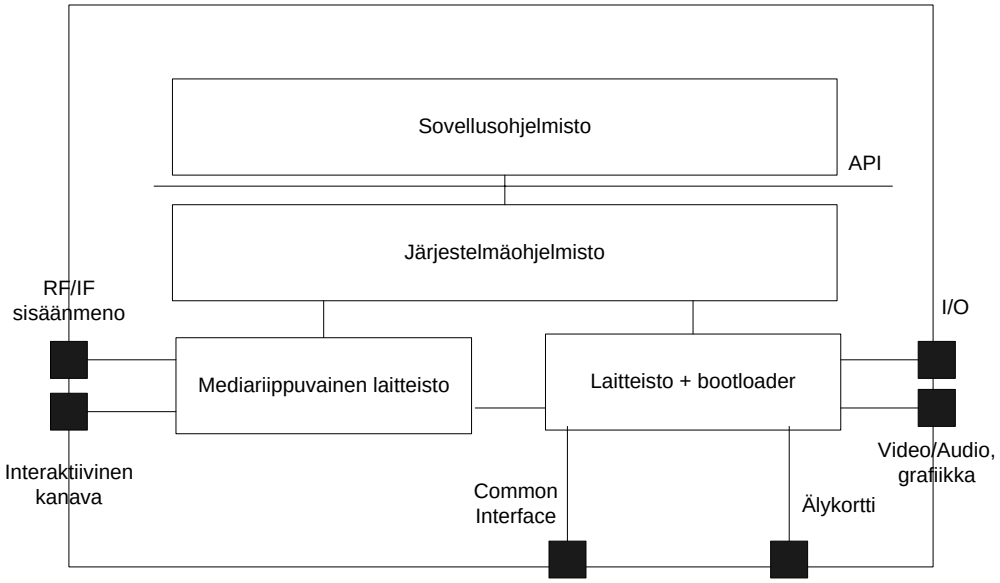
NorDig-yhteenliittymä perustettiin luomaan yhteispohjoismainen digitaalitelevision vastaanotinmäärittely käyttäen pohjana DVB-standardeja. Tällä haluttiin helpottaa kuluttajien siirtymistä digi-tv:seen ja mahdollistaa DVB-lähetyksien vastaanotto samalla vastaanottimella maasta tai mediasta riippumatta. Sisällöntuottajille NorDig-määrittely tuo tiedon siitä, minkälaista signaalia vastaanottimet pystyvät vastaanottamaan, ja miten heidän tuottamansa palvelut ja sisältö näkyvät niissä. Nordig-Unified-määritys esittelee neljä profiilia (Kuva 6). Perustoiminnallisuuden lisäksi määrityksessä on kolme profiilia, jotka vastaavat MHP-standardin profiileja.



Kuva 6. NorDig-määrityksen profiilit.

Kuvassa 7. on esitetty NorDig-päätelaitteen arkkitehtuuri. NorDig-vastaanottimessa on ainakin yksi sisäänrakennettu kaapeli-, satelliitti- tai maanpäällisen järjestelmän viritin. NorDig:ssa on lisäksi Common Interface -liitäntä, jonka avulla vastaanottimeen on mahdollista kytkeä erillinen satelliitti- tai kaapeliviritin sisäänrakennetun maanpäällisen virittimen rinnalle. Common Interfacen kautta voidaan kytkeä myös erillinen CA-moduuli (Conditional Access), joka mahdollistaa useamman erilaista salausjärjestelmää käyttävän palveluntarjoajan ohjelman seuraamisen.

Kaikissa NorDig-vastaanottimissa on älykortin lukija, jolla päästään sekä salattuihin että mahdollisiin muihin palveluihin, kuten vedonlyönti- ja pankkipalveluihin, jotka vaativat tunnistautumista. NorDig-määrityksessä luetellut paluukanavatekniikat on esitelty kappaleesa 2.2.4.1 [YLE TK-lehti], [NorDig].



Kuva 7. NorDig-päätelaitteen arkkitehtuuri.

Italian DGtvi D-Book

Italia on tehnyt määrityksen maansa markkinoille sopivasta digi-tv-vastaanottimesta [D-Book]. Italian valtion tuella on tehostettu MHP-yhteensopivien päätelaitteiden kehitystä ja hankintaa, minkä vuoksi vastaanottimia on käytössä siellä jo noin 1,5 miljoonaa (Tammikuu 2005, www.mhp.org). Suuren penetraation vuoksi Italian digi-tv-vastaanotin määritys on suuren mielenkiinnon kohteena muuallakin Euroopassa. DGtvi-määritys kuvaa teknologiat ja toiminnalliset edellytykset päätelaitteelle sekä laitteiston että ohjelmiston osalta. Se perustuu kansainvälisiin standardeihin (MHP, DVB). Yhtenä päätavoitteena on ollut myös yhteen toimivuuden säilyttäminen muiden vastaavien määritysten (NorDig) kanssa.

2.2.4 Lisäarvopalvelut

Lisäarvopalvelut ovat sovelluksia, joita käytetään päätelaitteen kaukosäätimellä ja esimerkiksi näppäimistöllä. Useimmat lisäarvopalvelut toteutetaan MHP-sovelluksina. Sovellukset voivat olla joko valmiiksi laitteeseen asennettuja tai ne välitetään ohjelmavirran mukana (MHP1.0) tai ladataan paluukanavan kautta (MHP1.1). Tässä kappaleessa esitellään lyhyesti yleisimmät lisäarvopalvelut, joita tällä hetkellä on käytössä [ArviD3].

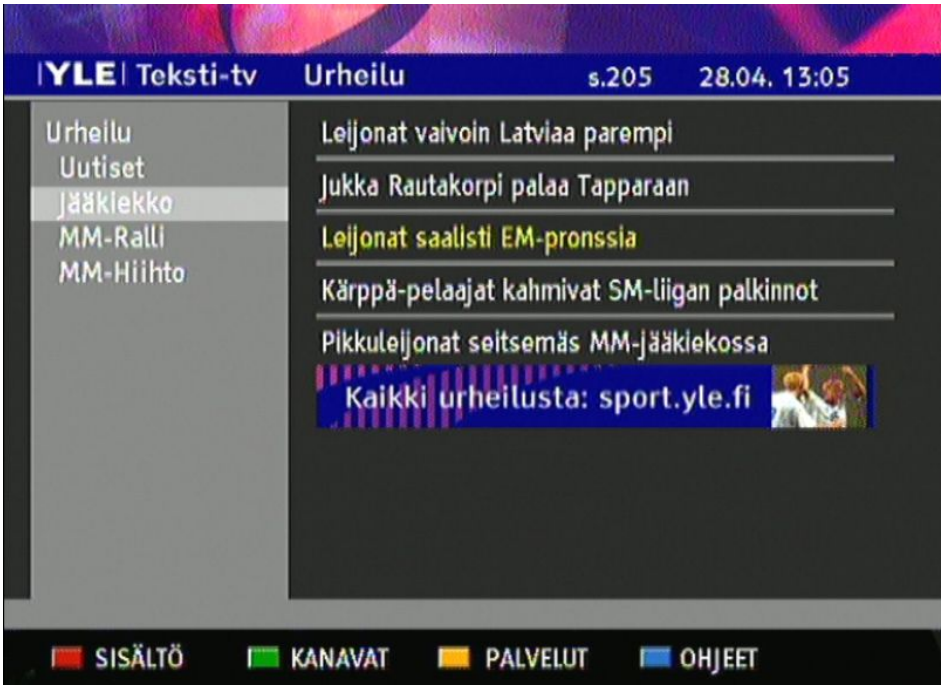
Ohjelmaopas

Kuva 8. Esimerkki ohjelmaoppaan käyttöliittymästä.

Ohjelmaopas (EPG, Electronic Program Guide) on käytetyin ja tärkein lisäarvopalvelu. Oppaan avulla katsoja voi selata ohjelmatietoja ja valinnaisesti seurata yhtä aikaa tv-ohjelmaa. Käyttöliittymä on yksinkertainen; sitä käytetään kaukosäätimen väri- ja nuolinäppäimillä. Oppaan toiminta perustuu lähetysvirran mukana lähetettävään SI-dataan (service information). Ohjelmaopas voidaan toteuttaa vastaanottimeen sisäänrakennettuna tai MHP-sovelluksena. Ohjelmia koskevat tiedot päivittyvät jatkuvasti, joten vastaanotin pystyy mm. virittymään oikealle kanavalle.

Superteksti-tv

Superteksti-tv on vanhan teksti-tv:n uudistettu versio. Siinä vanhan teksti-tv:n teksti ja kömpelö grafiikka ovat vaihtuneet värigrafiikkaan ja linkkejä sisältävään hypertekstiin. Käyttöliittymänä on supertekstiselain, johon sopivaa sisältöä digi-tv-operaattorit ja sisällöntuottajat tekevät käyttäen siihen soveltuvia työkaluja; sivujen määritykset tehdään xhtml:n ja CSS:n avulla. Sivuilla voidaan perinteisten sivunumeroiden lisäksi navigoida käyttämällä tekstiin upotettuja linkkejä, jolloin selailu muistuttaa hyvin paljon www-sivujen lukemista. Superteksti-tv vaatii MHP-yhteensopivan päätelaitteen.



Kuva 9. Esimerkki Superteksti-tv:n käyttöliittymästä.

Ohjelmakohtaiset palvelut

Tyypillisesti ohjelmakohtaisia palveluja voidaan käyttää vain ohjelman lähetyksen aikana tai saatavuutta on muuten rajoitettu esimerkiksi tietyn tyyppisiin lähetyksiin, kuten vaikkapa Olympialaisten ajaksi. Tällaisia palveluja ovat esimerkiksi ohjelmaan liittyvät tietokilpailut, pelit ja äänestykset, urheiluohjelmien sekä vaalien tulokset tai ohjelmiin liittyvät sivut superteksti-tv:ssä.

Kanavakohtaiset palvelut

Kanavakohtaiset palvelut eivät liity mihinkään ohjelmaan, vaan ne ovat aina saatavilla, kun vastaanotin on viritetty oikealle kanavalle. Tällaisia palveluja voivat olla uutis- ja pörssikurssipalvelut tai palautteen antaminen kanavalle. Kanavakohtaisiin palveluihin luetaan myös ohjelmaopas ja superteksti-tv.

Paluukanavan vaativat palvelut

Kun vastaanottajalla on tarve viestiä palveluntarjoajan kanssa, tarvitaan paluukanava. Tällaisia palveluja ovat esim. edellä mainitut äänestys- ja palautepalvelut. Paluukanava-tekniikoita on käsitelty tarkemmin seuraavassa kappaleessa. Tulevaisuudessa paluu-kanavan vaatimat palvelut monipuolistuvat. Internetistä tutut palvelut, kuten sähköposti, pankkipalvelut ja sähköinen kaupankäynti, nähdään mielenkiintoisimpina kuluttajan näkökulmasta. Tämän tyyppisissä palveluissa tietoturvavaatimukset korostuvat.

Päätelaitteen suojaaminen viallisilta sovelluksilta sekä luottamuksellisen tiedon käsittely ja siirto vaativat turvallisia toteutuksia, ennen kuin loppukäyttäjän luottamus palveluihin voidaan ansaita. Kuten kaikissa muissakin lisäarvopalveluissa, käyttöliittymän helppouden lisäksi on korostettava tietoturvan helppoutta ja läpinäkyvyyttä katsojalle.

2.2.4.1 Paluukanava ja päätelaitteiden ohjelmistopäivitykset

Paluukanavatoteutukseen on standardoitu useita vaihtoehtoja. Taulukossa 3. esitetään yhteenvetona yleisimmät mahdolliset paluukanavatekniikat. Taulukon yhdeksän ensimmäistä tekniikkaa on määritelty NorDig-spesifikaatiossa, jonka mukaan päätelaitteen tulee tukea ainakin yhtä niistä. Muut taulukossa esitetyt tekniikat edustavat mm. erityyppisiä kotiverkkoteknologioita, jotka mahdollistavat päätelaitteen liittämisen kodin muuhun tietoverkkoinfrastruktuuriin. Näiden paluukanavatoteutusten kohdalla nopeus tarkoittaa suurinta liitäntätekniikan mahdollistamaa tiedonsiirtonopeutta digisovittimen ja Internet-liitännän tarjoavan laitteen välillä; ei siis välttämättä paluukanavan siirtonopeutta. Italian digivastaanotinmäärityksessä paluukanavatekniikaksi on määritetty modeemiliitäntä (56 kbit/s), linkkitason protokollaksi on määritetty PPP. Vaihtoehtoisina tekniikkoina DGtvi-D-Book määrittelee Ethernet-liitännän DHCP-tuella varustettuna tai GSM/GPRS-liitännän matkapuhelinverkkoon. Tämän lisäksi on olemassa teollisuusyhteenliittymiä, jotka pyrkivät yhdenmukaistamaan kotiverkon laitteiden tiedonsiirtoprotokollia ja liitettävyyttä, esimerkkinä Universal Plug and Play (UPnP) ja Digital Living Network Alliance (DLNA) [ArviD], [FICORA2].

Ohjelmistopäivitykset

Päätelaitteeseen voidaan päivittää ohjelmallisesti uusia ominaisuuksia tai korjata aikaisemman ohjelmistoversion virheitä. Ohjelmistopäivitys voidaan toimittaa lähetysvirran mukana. Tämä toiminto mahdollistaa esimerkiksi MHP-standardin kehittyessä sen uusien ominaisuuksien käyttöönoton (laitteiston toiminnallisuuden rajoissa). Verkko-operaattori (esim. Digita) testaa ohjelmistopäivitykset ennen kuin se laittaa ne lähetykseen. Ohjelmistopäivityksiä ei lähetetä jatkuvasti, vaan ne ovat saatavilla rajoitetun ajan. Tämän vuoksi laitevalmistajat ovat tehneet erilaisia ratkaisuja, joilla päivityksiä voi asentaa vaikkapa huoltoliikkeessä. Katsoja voi myös itse siirtää päivityksen päätelaitteeseen esimerkiksi kotitietokoneelta käyttäen RS232C-sarjakaapelia. Asennusohjeet ja -käytännöt vaihtelevat laitevalmistajalta toiselle, ja ne vaativat tietoteknistä perusosaamista, jota ei voida olettaa olevan jokaisella televisionkatsojalla. Tietoturvan kannalta ohjelmistopäivitykset ovat uhka lähinnä toimivuudelle; virheellinen päivitys voi sotkea päätelaitteen toiminnan niin, että se on palautettavissa vain huoltoliikkeessä tai laitevalmistajalla. Uhkana voidaan nähdä myös viallisen ohjelmistopäivityksen tahallinen levittäminen, mikäli hyökkääjä kykenee väärentämään lähetyksen toisella lähettimellä.

Taulukko 3. Paluukanavatekniikoita.

Tekniikka	Nopeus	erityispiirteitä
V.32bis	14,4 kbit/s	Puhelinverkko on kaikkialla käytettävissä, mutta verkoissa on maakohtaisia eroavaisuuksia, jotka rajoittavat kansainvälistä yhteiskäyttöisyyttä.
V.90	56 kbit/s	
Ethernet (IEEE 802.3 tai nopeampi)	10 Mbit/s - 10 Gbit/s	Ethernet-teknologia kehittyy nopeammaksi ja alueellisesti laajempiin verkkoihin. Uusissa asunnoissa on usein kaapelointi valmiina Ethernet-verkkoa varten.
EURO-ISDN (ETS 300 012)	128 kbit/s	ISDN ei ole yleistynyt yhtä paljon kuin Saksassa ja Norjassa.
DECT (ETS 300 175)	32 kbit/s	DECT ei ole laajassa käytössä, eikä todennäköisesti yleisty paluukanavan toteutusteknologiana.
GSM/GPRS (EN 301 195 /ES 202 218)	GSM: 9,6 kbit/s HSCSD: 43,2 kbit/s GPRS: 171,2 kbit/s	GSM/GPRS-päätelaiteen liityntä digisovittimeeen on tyypillisesti joko IrDA tai Bluetooth.
DVB-paluukanavaliitäntä (ETS 300 800)	3,088 Mbit/s	EURODOCSIS-tekniikan kilpailija.
Euro DOCSIS (ES 201 488)	38 – 51 Mbit/s (jaetaan samassa solussa olevien kesken) Päätelaitteen enimmäissiirtonopeus tyypillisesti 512 kbit/s	Suomen Kaapelitelevisioliiton määritys [REF!!] vaatii sisäänrakennetun EuroDocsis-kaapelimodeemin.
IEEE 1394 (Firewire)	400 Mbit/s	Reaaliaikaisen kuvan ja äänen siirtämiseen kehitetty teknologia.
IrDA	4 Mbit/s	Laitteella on oltava näköyhteys toiseen laitteeseen ja etäisyys lyhyt. Ei yleistyne digi-tv –päätelaitteissa.
xDSL	8 Mbit/s (ADSL, tilaajalle) 1,5 Mbit/s (verkkoon päin) 54 Mbit/s (VDSL)	Laajakaistainen datayhteys, joka käyttää puhelinkaapelointia. Levinnein laajakaistatekniikka Suomessa.
Bluetooth	721 kbit/s/57 kbit/s (asymmetrinen) 433,9 kbit/s (symmetrinen)	Etäisyys laitteiden välillä n. 10m.
IEEE 802.11 (WLAN)	54 Mbit/s	Langaton lähiverkkoteknologia.
IEEE 802.15 (WPAN)	TG3: 11..55 Mbit/s TG4: 20..250 kbit/s	Pohjautuu Bluetooth-teknologiaan.
HomePNA	1 Mbit/s	Puhelinkaapelointia hyödyntävä lähiverkkoratkaisu
Datasähkö	2 – 4 Mbit/s (jaetaan saman muuntopiirin alueella olevien kesken)	Hyödyntää olemassa olevaa sähkökaapelointia. Ongelmana häiriönpoisto.
IEEE 802.16 (WiMAX)	70 Mbit/s	Langaton MAN–verkkoteknologia (Metropolitan Area Network). Ulottuvuus noin 50 km.

2.3 Lyhyt digitaalisen konvergenssin kuvaus

Konvergenssiksi kutsutaan tilannetta, jossa useat 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 konvergoitumisen myötä kaikki siihen liittyvät, perinteisesti suljetut järjestelmät, kuten televisio- ja (matka)puhelinverkot sekä tuotannonohjausjärjestelmät, ovat olleet yksittäisen organisaation hallussa.

Suljettuihin verkkoympäristöihin kohdistuu kuitenkin nyt ja tulevaisuudessa erilaisia paineita. Suuri osa organisaatioista ulkoistaa toimintojaan voimakkaasti, jolloin verkko voi siirtyä toisen tahon hallintaan. Verkkoinfrastruktuurien muutokset ajavat kohti all-

IP-ratkaisuja kustannussäästöjen vuoksi, jolloin esimerkiksi puhelinliikennettä voidaan ohjata IP-verkon päällä, MPLS-reititystä ja muita vastaavia tekniikoita käyttäen. Verkkojen yhdistyessä kontrolli ja vastuu niistä pirstaloituu.

Yhtenä suljettujen ympäristöjen ongelmana on ollut turvallisuusajattelun puutteellisuus: kun koko verkko on yhden organisaation käsissä, eikä verkossa ole vihamielisiä tahoja, syntyy helposti vaikutelma turvallisuudesta, vaikka verkon tietoturva olisi millä tahansa tasolla. 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 uusissa verkkoympäristöissä ongelmia niissä tehtyjen oletusten tai virheiden vuoksi.

Internetissä konvergenssin kaltaiset tilanteet eivät ole mitään uutta. Kun verkko alkoi laajentua, siihen liitettiin paljon suljettuja, usein myös yhden käyttäjän järjestelmiä. Näihin eristetyiksi ajateltuihin järjestelmiin alkoi verkon kautta päästä käsiksi tavoilla, joita ei otettu tai ehkä voitukaan ottaa lukuun aiemmin. Tietoturvan murtamiseen ei aina tarvittu edes toteutusvirheitä hyödyntäviä murtautumisia tai tunnistusmenetelmien ohittamista – joissakin järjestelmissä ei ollut alkeellisimpiakaan turvamekanismeja. 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. Digi-tv:n tietoturvauhkat

Tämä uhkakartoitus pohjautuu olemassa oleviin tutkimuksiin sekä projektin yhteydessä toteutettuihin yrityshaastatteluihin.

Digitaaliseen televisiotoimintaan liittyvät uhkat voidaan karkeasti jakaa digi-tv:n lähetysverkkoon ja päätelaitteeseen kohdistuviin uhkiin, paluukanavan hallintaan ja digitaaliseen konvergenssiin liittyviin uhkiin sekä palvelunkehityksen uhkiin.

3.1 Lähetysverkkoon ja päätelaitteisiin kohdistuvat uhkat

Esimerkki 1: Käyttäjä asentaa digisovittimelle tarkoitetun ohjelmistopäivityksen, joka on viallinen (sisältää esimerkiksi ohjelmistovirheitä tai on vioittunut siirron aikana). Ohjelmiston toiminta varmistetaan yleensä sovittimessa ennen sen käyttöönottoa. Varmistamisen epäonnistuminen saattaa vahingoittaa laitetta, kun ohjelmistoa yritetään käynnistää.

Esimerkki 2: Ohjelmasignaali sisältää virheitä, joita digisovitin ei pysty käsittelemään/korjaamaan Tämä aiheuttaa digisovittimessa ei-toivottuja toimintoja tai jopa vahingoittaa sitä.

DVB:hen liittyvät tietoturvauhkat ovat pienehköjä. Tämä johtuu siitä, että DVB:llä tapahtuva tiedon (pääasiassa äänen ja kuvan) siirto on operaattorin kontrollin alaista. Operaattorin itsensä mukaan uhkia ei esiinny ohjelmien paketointi- tai jakeluvaiheessa, koska näitä vaiheita operaattorilla on mahdollisuus valvoa ja niihin voidaan tarvittaessa puuttua. Todennäköisimmin operaattorin näkökulmasta uhkat liittyvät siis ohjelmien tuotantovaiheeseen tai kuluttamiseen ja laitteistoihin. Toimijakenttä on kuitenkin laajenemassa ja tämän myötä myös siirron hallinta muuttuu entistä haastavammaksi.

Käytännössä DVB-pohjaiseen liikenteeseen puuttuminen on ulkopuoliselle toistaiseksi verrattain vaikeaa, mutta ei mahdotonta. Lähetystä on mahdollista yrittää väärentää toisella lähettimellä. DVB-T-lähetykset perustuvat COFDM-modulaatioon, jonka tunnusomaisena piirteenä on monitie-etenemisen eliminointi siten, että vastaanotin lukittuu siihen hetkeen, jolloin signaali on ”puhdas” eli monitie-eteneminen on ehtinyt vaientua ja kaikki lähetteet näkyvät samana symbolina. Tämä mahdollistaa kaapeli-tv-verkossa väärän lähetteen syöttämisen vastaanottopisteeseen jo pienilläkin (muutama watti) teholla, mutta etäisyys vastaanottopisteeseen ei saa olla suuri. Muita uhka-esimerkkejä DVB:hen liittyen on virheellisen datan lähettäminen systeemiohjelmistojen päivittämisen yhteydessä. Laitteistopäässä tähän riskiin on varauduttu suojauksilla. Esimerkiksi päätelaitteessa oleva flash-muisti tyhjennetään vasta, kun on varmistettu, että uusi ohjelma on verifioitu.

Digi-tv:ssä käytettyä maksu-tv-järjestelmää, Conaxia, kohtaavat älykorttien ja maksu-tv:n yleiset uhkat. Satelliittitelevisiokäytössä älykortit pitävät piratismin ja luvattoman käytön kohtuullisissa rajoissa, vaikka järjestelmä ei ajoittain tarvittavien korttipäivitysten kalleuden vuoksi ole optimaalinen. Suuremmat tietoturvauhkat liittyvät MHP:n käyttöön. MHP1.0.2 asettaa tällä hetkellä useita rajoituksia digi-tv:n interaktiiviselle käytölle. MHP1.1:n käyttöönoton myötä digi-tv lähenee entistä enemmän Internetiä. Toistaiseksi MHP1.1:n mukaisia päätelaitteita tai palveluja ei ole saatavilla, mutta sitä mukaa kun teknologiaa otetaan käyttöön, vaaditaan entistä tarkempaa tähän standardiin liittyvien uhkien tarkastelua. MHP:n yleistyessä on mahdollista, että kolmansien osapuolten tekemät komponentit niissä yleistyvät. Tällöin on ainakin teoriassa mahdollista, että jokin ulkopuolinen taho voi näiden komponenttien kautta soluttaa haittaohjelman lähetyksessä olevaan MHP-sovellukseen sovelluksen tekijän tietämättä.

Tällä hetkellä MHP-sovelluksia on mahdollista ladata omalle laitteelle vain lähetysvirran kautta, jolloin siitä ja siinä lähetettävien sovellusten turvallisuudesta vastaa operaattori. Niin sanottuun objektikaruselliin ladattavat sovellukset lisätään tyypillisesti käsin, vaikka automatisoituja järjestelmiä on kehitetty. Tämä takaa sen, että joku ihminen vastaa, miten sovellukset saatetaan ihmisten ulottuville. Toisaalta se voi altistaa inhimillisille erehdyksille. Vaikka karuselliin lisätäänkin ladattavat sovellukset käsin, ne on yleensä liitetty paikallisverkkoon. Mikäli joku ulkopuolinen taho pääsee tunkeutumaan tähän verkkoon, hänellä on ainakin teoriassa mahdollisuus karusellin ohjaamiseen ja kenties myös luvattoman aineiston lähettämiseen.

Itse MHP-standardiin liittyy lukuisa joukko tulkinnanvaraisuuksia. MHP-sovellusten toimivuus ristiin eri laitemalleissa on vielä tästä syystä kehitysvaiheessa, varsinkin MHP-standardin 1.1-version kohdalla. Myös tämä osaltaan hidastaa sovellusten kehittämistä.

MHP:n tietoturvaa voidaan varmistaa sähköisillä allekirjoituksilla, mutta ne ovat MHP:n osalta Suomessa vasta tulossa käyttöön. Allekirjoitusprosessi koostuu kolmesta osasta: tiivistetiedostoista, allekirjoitustiedostoista ja todistustiedostoista. Allekirjoitukset ovat tällä hetkellä olemassa olevista keinoista paras tapa varmistua, ettei sovellusten sisältöä ole muutettu. Juurivarmenneviranomaisen allekirjoittamaan sovellukseen liitetään ns. lupatiedosto (esimerkki tällaisesta tiedostosta on esitetty kappaleessa 2.2.2), joka kertoo, mitä resursseja kyseinen sovellus saa käyttää. MHP:n juurivarmentaja on tällä hetkellä WiseKey SA, joka on suuri ulkomainen toimija. Suomessa allekirjoituskäytäntö on vasta muotoutumassa. Todennäköinen vaihtoehto on, että allekirjoitusvarmenne annetaan yhdelle suurelle toimijalle, jolloin pienemmät toimijat eivät tarvitse omaa varmennetta, vaan voivat toimia esimerkiksi verkonhaltijan varmenteen alla. Tällöin kaikilla varmenteen haltijoista on kuitenkin vastuu omasta osastaan.

Tämän hetken suurin haaste varmenteiden osalta on päätelaitteiden kehittymättömyys tältä osin; valtaosassa digi-tv-vastaanottimia ei ole mitään juurivarmenteita, mistä johtuen allekirjoituksen tarkistaminen ja sovellusten käyttöoikeuksien määrittäminen on laitevalmistajan toimesta kytketty pois toiminnasta. MHP-määritysten vastaisesti on siten mahdollista, että allekirjoittamaton sovellus voi avata paluukanavan vaikkapa modeemikaappausta varten tai vaihtaa kanavaa.

Digitaalisen varmennuksen kanssa täytyy olla erityisen tarkkana silloin, kun käyttäjän pitää varmistaa jotain toimintoja varmennustietoihin liittyen. Laitteessa täytyy olla tällainen mekanismi esimerkiksi sellaisia tilanteita varten, joissa jokin varmenteista vaarantuu ja laitteet täytyy päivittää uutta varmennetta varten – muutoinhan ohjelmiston koko ketju vaarantuisi. Tällöin voidaan kuitenkin olettaa, ettei suurin osa käyttäjistä ole tällöin tehtävän tasalla, vaan voi suorittaa satunnaisen, yleensä sallivan, toiminnon. Tällöin koko käyttäjän väliintuloa vaativa mekanismi muodostaa uhan käyttäjän kannalta ja sen toteutusta palveluntarjoajan ja päätelaitevalmistajan täytyy tarkoin pohtia. Toisaalta liiallinen luottaminen varmenteihin voi mahdollistaa vanhojen sertifikaattien käytön vahingoittaviin tarkoituksiin, kuten ActiveX-tapauksessa[1].

Muita tärkeitä MHP:n turvallisuusominaisuuksia ovat varmenteet, resurssien käyttöluvat sekä kanavakohtaiset turvallisuusominaisuudet. Mikäli näitä osataan käyttää oikein, teknologian käyttö on tällä hetkellä suhteellisen turvallista.

3.2 Paluukanavan hallinta ja konvergenssin uhkat

Esimerkki: Katsoja lataa palveluntarjoajalta haluamansa MHP-sovelluksen, joka on palveluntarjoajan digitaalisesti allekirjoittama. Allekirjoitusta ei tarkisteta päätelaitteessa, joten sovellus saa laajimmat mahdolliset oikeudet käyttää laitteen resursseja. Sovellus lataa paluukanavan kautta JPEG-muotoisen kuvan. Kuva on koodattu virheellisesti niin, että osaa sen sisältämästä datasta käsitellään käynnistettävänä koodina, kun kuvaa luetaan. Tämä koodiksi tulkittava osuus sisältää haittaohjelman, joka kaataa digisovittimen.

Paluukanava ja siihen liittyvät uhkat kiteytyvät suurimmaksi osaksi Internet-protokollien käyttöön. Konvergenssin myötä digisovitin monipuolistuu. Jossain määrin se lähestyy kotitietokonetta; kovalevylliset mallit tarjoavat tallennustilaa, paluukanava-tyypit monipuolistuvat tulevaisuudessa ja prosessointiteho kasvaa. Kuitenkin ero kotitietokoneeseen tulee aina säilymään johtuen erilaisesta käyttötarkoituksesta. Resurssien suhteen digisovitin ei liene koskaan kotitietokoneen rinnalla, vaan kehitys kulkee jäljessä.

[1] http://www.dataworldindia.com/html/activex.html

Tietoturvan kannalta paluukanava on digi-tv:n riskialttein kohta. Paluukanavan turvallisuuden varmistamiseen käytetään TLS-protokollaa (transport layer security), jonka myötä liikenne on salattua. Tyypillisestä www-selaimesta poiketen, TLS-yhteyden avaava MHP-sovellus ei tarkista palvelimen varmenteen oikeellisuutta (esimerkiksi voimassaoloaikaa), koska päätelaitteissa ei tällä hetkellä välttämättä ole tallennettuna juurivarmennetta, jota vastaan tarkistus voitaisiin tehdä. Sovelluksen mukana on mahdollista lähettää juurivarmenne, mutta se ei ole pakollista ja haitta-ohjelmien kohdalla tämä sisältää väärinkäyttömahdollisuuden vaikkapa itsegeneroitujen varmenneketjujen muodossa. Digisovittimien yksinkertaisuus lisää niiden turvallisuutta. Esimerkiksi porttiskannaukset yksinkertaisiin laitteisiin eivät ole järkeviä: bokseissa ei ole käynnissä sovelluksia, joihin porttiskannauksilla kannattaisi yrittää ottaa yhteyttä.

Käytännössä tärkeimmät digi-tv:n paluukanavan toimintaan liittyvät tekniset ratkaisut ovat tällä hetkellä http- ja https-protokolla sekä sivunkuvauskieli xhtml, joka on xml-kieleen pohjautuva html:n parannus. Xhtml on ulkoasultaan tiukemmin määritelty kuin html. Http on kohtuullisen yksinkertainen protokolla, jonka toteutukset Internet-maailmassa ovat kohtuullisen toimintavarmoja. Eniten hankaluuksia ovat perinteisesti aiheuttaneet http:n laajennukset ja http:n päällä siirrettävien protokollien ja tiedosto-formaattien käsittely. Näiden toteutukseen voi liittää uhkia myös digi-tv:n kehitykseen liittyen. Http:n laajennuksista lähinnä evästeet voivat aiheuttaa käyttäjälle uhkan heidän yksityisyytensä kannalta, jos evästeitä käytetään käyttäjätottumusten ja profiilien muodostamiseen. Kun http toimii TLS:n/SSL:n päällä, uhkat liittyvät TLS:n toteutustason haavoittuvuuksien lisäksi digitaaliseen allekirjoitusjärjestelmään ja sen toteutukseen, joita on käsitelty laajemmin kappaleessa 3.1. Digi-tv:n paluukanavassa käytetään paljon http:n päällä siirrettävää sisältöä, esimerkiksi Xhtml, kuvaformaatit (GIF, JPEG, PNG), MPEG ja fonttiformaatti PFR [MHP].

Ainakin em. kuvaformaatit ovat melko monimutkaisia tiedostomuotoja, joiden käsittelyssä muissa sovelluksissa on esiintynyt haavoittuvaisuuksia, joilla formaattia tulkitseva sovellus voidaan ottaa haltuun vihamielisesti rakennetulla syötteellä.

Html:n uhkat liittyvät html-koodin parsintatoteutuksen toimintavarmuuteen, joka on joutunut viimeaikoina tarkasteluun, ja jonka toteutuksista www-selaimissa on vastikään löytynyt jonkin verran haavoittuvuuksia. Xhtml:n ja xml:n tapauksessa vastaavia haavoittuvaisuuksia on myös löytynyt.

Html:n päälle luotujen laajennusten tietoturva on vaihtelevan tasoista. Html:n itsensä lisäksi selaimet ovat monimutkaisia ohjelmia, joista tyypillisesti löytyy erilaisia haavoittuvuuksia. Uhkia ovat aiheuttaneet erilaiset aktiivista sisältöä tuovat laajennukset, kuten Java, Javascript, ActiveX sekä Macromedia Flash.

Toinen kriittinen piirre laajennusten kannalta on niiden toteutusten toimintavarmuus ja erityisesti helppo hallittavuus, jotta niiden toiminnat voidaan tarkasti rajoittaa. Tällä hetkellä MHP-standardissa ei käytetä tämän tyyppisiä laajennuksia.

Palvelunkehittäjillä ja päätelaitetoimittajilla on halukkuutta lisätä digi-tv-laitteisiin paluukanavaa käyttäviä toimintoja, erityisesti erilaisia maksupalveluja kuten ostos- ja videontilauspalveluja. Tällaisten palvelujen uhkat ovat samankaltaisia kuin Internetissä toimivien pankki- ja kauppapalvelujen ja niiden kehityksessä tulisi seurata samankaltaisia ohjeita.

Tietoturvauhkien voidaan todeta olevan siirtymässä loppukäyttäjäpäähän päätelaitteiden kehittymisen ja yleistymisen myötä. Kun laitteet muistuttavat entistä enemmän tavallista tietokonetta, ja ne ovat lisäksi suoraan internetyhteyden päässä, voidaan pitää varsin todennäköisenä, että tavalliset tietokoneiden uhkat ilmestyvät myös digi-tv-laitteiden riesaksi.

MHP1.1:n käyttöönoton myötä riskit mahdollisille digisovittimissa esiintyville viruksille kasvavat. Digisovittimien yleistyminen lisää niiden kiinnostavuutta virusten kirjoittajien silmissä. Tyypillisiä haittaohjelmien tekijöiden tavoitteita voivat olla esimerkiksi laitteiden valjastaminen palvelunestohyökkäysten välikappaleeksi tai digisovitinroskapostin automaattiseksi lähetyspisteeksi. Digisovittimet ja niissä toimivat sovellukset toimivat tällä hetkellä Javan päällä, joten myös digisovittimia koskevat yleisesti Javan tietoturvaominaisuudet. MHP:ssa käytettävät Java-ohjelmat toimivat toistaiseksi omassa suojatussa ympäristössään, nk. hiekkalaatikossa. Tällä tavoitellaan sitä, että mikään haittasovellus ei pysty käyttämään luvallisia sovelluksia hyväkseen. Digisovittimien MHP-osuuden (Java-virtuaalikoneen) kaataminen esimerkiksi yksinkertaisella silmukkarakenteella on mahdollista.

Koska vielä ei ole käytössä MHP-sovelluksen itsenäistä leviämistä digisovittimien välillä mahdollistavaa toimintoa, eivät itsenäisesti leviävät madot ole relevantti uhka. Mikäli digisovittimiin toteutetaan sähköpostimahdollisuus, tästä uhkasta tulee myös digi-tv-maailmassa konkreettinen.

Kanavavaihdon yhteydessä digisovittimen ohjelmamuisti tyhjennetään, mikä ehkäisee haittaohjelmien pesiytymistä niihin. MHP1.0-standardissa on kuitenkin määritetty ns. persistent storage -rajapinta (pysyväismuistirajapinta), joka mahdollistaa allekirjoitetun sovelluksen kirjoittavan tiedostoja päätelaitteen pitkäkestoiseen muistiin, vaikka se joudutaankin lataamaan uudelleen päätelaitteeseen joka kerta, kun sovellus käynnistetään. Lisäksi MHP:n interapplication comminication -rajapinta (sovellusten välinen kommunikointirajapinta) mahdollistaa verkon yli välitettävät metodi-kutsut hyväksikäyttäen Javan RMI:tä. Tämä helpottaa sovelluskehittäjän työtä, koska toisessa virtuaalikoneessa ja tietokoneessa pyörivän Java-sovelluksen metodeja voidaan kutsua

samoin kuin paikallista, eikä kehittäjän tarvitse miettiä sovelluskohtaisen protokollien määrittelyä. Ilmeinen tietoturvauhka on kuitenkin olemassa, mikäli metodikutsujen välitystä verkon yli ei ole suojattu millään tavalla. Palvelinpään Java-sovelluksen täytyy kuitenkin RMI:tä käytettäessä luoda ja ottaa käyttöön Javan SecurityManager, muuten RMI-luokkien lataaminen ei ole sallittua.

IP-datacasting

PC-käyttäjille ja yrityskäyttöön soveltuvaan tiedonsiirtoon on yleistymässä Internet-protokollan käyttö DVB-verkon tiedonsiirrossa (ns. IP datacasting). Internetissä liikkuva sisältö voidaan paketoida televisioverkon lähetyspäässä osaksi DVB-T-lähetettä ja sisältö puretaan edelleen DVB-T-lähetteestä PC-vastaanotinkortissa. IP:n käyttö tiedonsiirrossa mahdollistaa esimerkiksi laajakaistaiset video streaming -lähetteet sekä suurien tiedostojen siirrot.

Vastaanottimena IP-datacastingissa käytetään tällä hetkellä PCI- ja USB-väyläisiä tietokonekortteja. IP-datacastingin standardointityö on vielä kesken, mikä aiheuttaa omat haasteensa myös tietoturvalle.

3.3 Palvelunkehitysprosessi

Esimerkki: Palveluntarjoaja koostaa palvelun käyttämällä monen eri valmistajan ohjelmisto-komponentteja. Näiden yhteentoimivuutta ei ole riittävästi testattu. Loppukäyttäjälle tämä näkyy aika-ajoin tapahtuvina päätelaitteen virhetilanteina ja sen epäluotettavana toimintana. Kun palvelusta tehdään uusi versio ja osa komponenteista korvataan uudemmilla versioilla, yhteensopivuusongelmat kasvavat entisestään, mikäli uutta versiota ei testata kattavasti.

Järjestelmien ja palvelujen kehityksen jokaiseen vaiheeseen voi liittyä uhkia ja ongelmia. Systeemin konseptualisaatiovaiheeseen liittyviä riskejä ovat esimerkiksi tilanteet, joissa käytetään riskialtista kypsymätöntä teknistä ratkaisua tai vaihtoehtoisesti haetaan turvallisin mahdollisin ratkaisu ja tingitään uudempien teknologioiden tuomasta lisätoiminnallisuudesta. Vaatimusmäärittely ja systeemisuunnittelu ovat niin ikään keskeisiä vaiheita. Impelementointiin voi liittyä lukuisia ongelmakohtia, joita ovat mm. ohjelmointivirheet ja vääränlaiset kytkennät. Myös tukijärjestelmät muodostavat omia uhkiaan, jotka liittyvät heikkoihin ohjelmointikieliin ja huonoihin kehitystyökaluihin. Myös kolmansien osapuolten tekemien ohjelmakomponenttien käyttö voi aiheuttaa riskejä tietoturvan kannalta, jos niiden tietoturvatasoa ei tunneta. Systeeminsuunnittelun analyysiin liittyviä ongelmia ovat mm. väärät oletukset järjestelmän ympäristöstä ja ihmisten käyttäytymisestä sekä vialliset mallit ja simulaatiot. Toteutuksen analyysissä uhkan muodostavat lähinnä vääränlaiset testausmenetelmät.

Kehitykseen liittyviä ongelmakohtia ovat esimerkiksi hitaat uusien ylläpitotapojen omaksumiskeinot ja uusien virheiden omaksuminen vanhoja korjatessa. Myös järjestelmien käytöstä poistamiseen liittyy uhkia, kuten tarpeellisten osien liian aikainen alasajo tai piilossa oleva riippuvuus vanhasta versiosta, jota ei enää ole olemassa.

4. Ratkaisut digi-tv:n tietoturvauhkiin

Tämä kappale käsittelee tärkeimpiä ratkaisuja ja arkkitehtuureita edellä esiin tulleisiin palvelunkehittäjän tietoturvaongelmiin. Koska täydellistä tietoturvaa on mahdoton saavuttaa, eivätkä mitkään ratkaisut voi olla pysyviä, voidaan esitettyjä ratkaisuja pitää vain hyvinä suuntaviivoina tietoturvan suunnittelussa.

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 kulloisessakin tilanteessa esiintyviä riskejä täytyy identifioida, hallita ja minimoida. 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. Tyypillisimpiä sopimuksia ovat esimerkiksi kuljetus- ja alihankintasopimukset.

Osa riskeistä on sellaisia, että ne joudutaan tai kannattaa pitää omalla vastuulla. Tällaisia ovat sähköisessä liiketoiminnassa tarpeellisten, Internetiin kytkettyjen palvelimien muodostamat riskit. Riskienhallintaa on myös varautuminen etukäteen – esimerkiksi työstää suunnitelma, 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. paluukanavan käyttöön. Tämä aiheuttaa kompleksisuutta ja ongelmallisuutta palvelunkehittäjien ratkaisuvalintoihin (esim. teknologia-alustojen valinnassa).

Digitaalisen television luonne joukkoviestimenä nostaa sisällönsuojaukseen ja ohjelmalähteen tunnistamiseen liittyvät ratkaisut tärkeään rooliin. Palveluntarjoaja haluaa estää sisällön laittoman käytön ja toisaalta katsoja haluaa tietää, mistä kulloinenkin sovellus on peräisin sekä varmistaa päätelaitteensa häiriöttömän toiminnan estämällä tuntemattomien sovellusten lataamisen. DRM-tekniikoiden (Digital Rights Management) kehittymättömyys ja ennen kaikkea niiden huono yhteentoimivuus ovat rajoittaneet sellaisten palvelujen yleistymistä, joissa levitetään laillisesti tekijänoikeus-lain alaista materiaalia, esimerkiksi musiikkia digitaalisessa muodossa. Digitaalisen sisällön levitykseen liittyvät palvelut ovat hyvin houkuttelevia digi-tv:n katsojan näkökulmasta, koska digi-tv-verkko soveltuu erinomaisesti tämäntyyppisten palvelujen levityskanavaksi.

Palvelunkehittäjän tärkeimmät ratkaisut eri uhkaluokkiin on pyritty yhdistelemään seuraavissa taulukoissa, joista ensimmäinen on teknologialähtöinen ja toinen keskittyy palvelunkehittäjän tietoturvaprosessiin.

Taulukko 4. Teknologialähtöiset ratkaisut ja uhkat digi-tv:ssä.

	Teknologia /Prosessi	Vaikutus tietoturvaan	Toteutustavat	Kohde				Tietoturva					
								Turvafunktiot			Turvakäsite		
				Päätelaite/Loppukäyttäjä	Paluukanava	Jakeluverkko	Palvelunkehitysprosessi	Korjaus	Suojaus	Havainnointi	Saatavuus	Eheys	Luottamuksellisuus
Sisällönsuojaus	Digitaalinen käyttöoikeuksien hallinta.	• Kontrolloi sisällön laillista käyttämistä ja kopiointia. • Maksullisten sisältöjen levittäminen.	DVB-CMCP,DRM, Conax.	X	X		X		X	X	X	X	X
	Ohjelmien digitaalinen allekirjoittaminen ja verifiointi.	• Ohjelmien alkuperän ja eheyden varmentaminen. • Ohjelman saamien oikeuksien rajoittaminen päätelaitteessa.	MHP-PKI.	X	X				X	X	X	X	
	Tallennetun datan salakirjoitus.	• Tietoturvapolitiikan mukainen tiedon suojaus. • Yksityisyyden vaatimusten täyttäminen.	Muistivälineiden salakirjoitus.	X	X		X		X		X		X
Hyökkäyksiltä suojautuminen	Liityntä elektroniseen maksujärjestelmään.	• Palvelun turvallinen liittyminen ulkopuolisiin maksujärjestelmiin. • Käyttäjän tunnistaminen.	Tupas, HST.	X	X				X	X	X	X	X
	Haittaohjelmilta suojautuminen.	Virusten ja haitallisen sisällön kohdejärjestelmään pääsyn estäminen .	Antivirus-ohjelmistot, sisällönsuodatus.	X	X	X	X	X	X	X	X	X	
	Yksityisyyden suojaaminen.	Henkilötietolain ym. alaisten yksityistietojen suojaaminen.	Käyttöoikeuksien hallinta, muistivälineiden salakirjoitus, tietoturvapolitiikat.	X	X	X	X		X	X		X	X
	Palvelimien ja lähetyslaitteiston suojaaminen.	Verkosta tulevilta hyökkäyksiltä suojautuminen. Luottamuksellisen tiedon suojaus.	Palomuurilla voidaan parantaa lähiverkossa olevan palvelimen tai muun laitteen suojausta.		X	X	X	X	X	X	X	X	X
	COFDM-lähetysten suojaaminen.	Suurin riski päätelaitteen varusohjelmiston muokkaminen väärennetyllä lähetteellä.		X		X				X		X	X
	Hyökkäysten havaitseminen.	Verkkoliikenteen havainnointi hyökkäystilanteiden varalta.	IDS/IPS-järjestelmät.	X	X	X	X		X	X	X	X	

Taulukko 5. Palvelunkehittäjän tietoturvaprosessi.

	Teknologia/Prosessi	Vaikutus tietoturvaan	Kohde				Tietoturva					
							Turvafunktiot			Turvakäsite		
			Päätelaite/Loppukäyttäjä	Paluukanava	Jakeluverkko	Palvelunkehitysprosessi	Korjaus	Suojaus	Havainnointi	Saatavuus	Eheys	Luottamuksellisuus
Palvelunkehittäjän tietoturvaprosessi	Kolmannen osapuolen arviointimenetelmät. (esim. laatu- tai tietoturva-auditoinnit).	• Palvelunkehittäjän tietoturvaprosessit ja tuotekehitysprosessit sekä laatujärjestelmä. • Suosituksia antava ennakoiva toimenpide puolueettoman tahon suorittamana. • Kohdennetut toimenpide- ja parannusehdotukset. • Tekninen tai hallinnollinen auditointi.	X			X	X		X	X	X	X
	Riskienhallinta.	Riskien tunnistaminen, arviointi ja vähentäminen. Jatkuva prosessi.	X	X	X	X	X	X	X	X	X	X
	Fyysiset turvaratkaisut.	Kulunvalvonta, paloturvallisuus, varmennettu virransyöttö palvelimille.	X		X	X	X	X	X	X	X	X
	Vikatilanteista toipuminen, suunnitelma.	Varautuminen vikatilanteisiin: • Tiedon menettäminen. • Laitteisto-ongelmat. • Tietoturvaloukkaukset. • Asioista tiedottaminen.			X	X	X		X	X		
	Tuotteen versionhallintajärjestelmät.	Tuotekehitysprosessi. Eri kehitysaikaisten versioiden hallitseminen.				X	X	X	X	X	X	X
	Tietoturva liiketoiminnan johtamisessa.	• Tietoturvaprosessit johtamisessa. • Tiedottaminen. • Kouluttaminen. • Vastuuhenkilöt organisaatiossa.			X	X	X	X	X	X	X	X
	CERT-Toiminta.	• Tietoturvaloukkauksien ennaltaehkäisy, havainnointi ja ratkaisu. • Tietoturvauhkista tiedottaminen. • Suomessa Viestintäviraston CERT-FI.	X	X		X	X	X	X	X	X	X
	Tuotekehitys prosessin seuranta, parantaminen ja koulutus.	Laadun parantaminen				X	X	X	X	X	X	X

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. Tärkeä monimutkaistumiseen vaikuttava tekijä on erilaisten tietoverkkojen yhdistyminen. Verkkokokonaisuuden ymmärtäminen voi jäädä vajavaiseksi, mikä itse verkonhallinnan vaikeuttamisen lisäksi hankaloittaa mm. riskienhallintaa ja haavoittuvuusanalyysiä. Riskienhallintapäätökset edellyttävät teknologiariippuvuuden hahmottamista ja tähän voidaan hyödyntää protokollalähtöistä tarkastelua.

Laajemmastakin 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 esiintyvät kuitenkin 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 mm. haavoittuvuusanalyysin, haavoittuvaisuusprosessin koordinoinnin ja infrastruktuurin riskienhallinnan kannalta. Yksittäinen haavoittuvaisuus voi protokollariippuvuuden kautta uhata verkkoa tavoilla, jotka eivät löydy normaalilla haavoittuvaisuusanalyysillä. Televisiolähetyksen tyypillinen piirre on, että sama sisältö jaetaan jopa miljoonille vastaanottajille samanaikaisesti, jolloin viallisen lähetteen kyseessä ollessa ongelmatilanteet kasvavat nopeasti todella suuriksi. Suurin osa katsojista on kuitenkin tekniikkaa syvemmin tuntemattomia, joiden valmiudet reagoida teknisiin ongelmiin ovat verrattain vähäiset.

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. Laajempaa ymmärrystä vallitsevaan tilanteeseen antavat asiantuntijahaastattelut.

Aiheen laajuuden vuoksi asiantuntijahaastattelut ovat kartoitusta tehtäessä erittäin tärkeällä sijalla. Alustavan protokollaselvityksen jälkeen haastattelemalla oman organisaation asiantuntijoita saadaan laajempaa ja tarkempaa näkymää protokolla-

viidakkoon. 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.

Ratkaisumallin tarkoituksena on saada parempi tekninen ja hallinnollinen ymmärrys, jolla saadaan kokonaiskuva protokollien kentästä sekä nähdään selkeästi ongelmakohdat, kuten piilevät kytkökset, riippuvuudet ja periytyvyydet. Visuaalinen ajattelu mahdollistaa mielikuvien, muotokielen ja värimaailman käyttöön valjastamisen ja tarjoaa informatiivisen kommunikaatiotavan kentän toimijoiden välille. Mallin tarkoituksena on tuoda esille kriittiseen infrastruktuuriin vaikuttavia protokolla-riippuvuuksia.

Mallilla voidaan tutkia erilaisia käytännön skenaarioita ja niihin vaikuttavia tekijöitä. Eräs tällainen skenaario on jonkin tietyn tietoverkon komponentit ja niiden toteuttamat protokollat. Tässä skenaariossa voidaan verkon ongelmakohtien tutkimiseksi ottaa protokollista kerätyn tiedon lisäksi 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 Muutosten hallinta

Tietotekniikan kehitys perustuu abstraktioihin: kaikki tietotekniset järjestelmät luottavat alemman tason järjestelmien toimintaan. Abstraktioita hallitaan 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. Vähänkään monimutkaisemmissa 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.

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

Alihankinta tuo lisää kompleksisuutta muutosten hallintaan, ja tämä tulee ottaa huomioon käytännöistä sovittaessa.

4.1.3 Tietoturvariskien hallinta

Riskien hallinnan vaiheita ovat karkeasti jakaen riskien identifioiminen, niiden arviointi ja niihin varautuminen. Nämä vaiheet voivat mennä osaksi päällekkäin. Riskien hallinnan eri vaiheissa sitä toteuttava organisaatio erottelee toimintojaan sekä pyrkii näkemään niiden edellytykset ja liitokset, jolloin riskien hallinnalla voi olla myös yleisesti toimintaa tehostava vaikutus.

Identifiointivaiheessa toimintojen edellytyksiä luetellaan 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 uhkiin liittyvä riski voidaan välttää ennen kuin se toteutuu. Välttämissuunnitelma voidaan luoda tässä vaiheessa tai viimeisessä vaiheessa yhdessä varasuunnitelman kanssa.

Arviointivaiheessa pohditaan toimintoon kohdistuvan uhan toteutumisen vakavuutta ja itse uhan todennäköisyyttä. Eräs 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 varautumissuunnitelmat. Itse riskienhallinta koostuukin tilanteen aktiivisesta seuraamisesta, eri riskeihin liittyvien oireiden tunnistamisesta ja seuraamisesta, suunnitelmien toteuttamisesta ja itse riskien hallinnan arvioinnista sekä kehittämisestä eri tilanteiden mukaan.

Riskit voidaan jakaa teknologiaan ja käyttäjiin 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.

Käyttäjiin liittyvät riskit liittyvät koulutuksen puutteeseen tai toisaalta tahalliseen toimintaan. Tietoisuuden puute tietoturva-asioista voi aikaansaada tahattomia tietovuotoja, vaarantavia 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, mikäli tämä ei aiheuta toiminnalle esteitä.

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

Laitteisiin täytyy olla nopeasti saatavilla varaosia, jotta rikkoutumisista koituvat haitat voidaan minimoida. Järjestelmän hallintaan on löydyttävä asiantuntijaosaamista: niiden hyödyllisyys muuttuu kyseenalaiseksi, mikäli kukaan ei osaa ylläpitää ja tarvittaessa muokata niitä. Järjestelmiä on säilytettävä turvallisessa paikassa lukkojen takana. Niiden toimintalämpötila, energiansaanti ja muut tarvittavat toimintaolosuhteet on varmistettava. Televisiotoiminnan riskienhallinnassa keskeistä on saatavuuden varmistaminen kahdentamalla kriittiset järjestelmät ja nopeasti käyttöönotettavissa olevat varajärjestelmät. Häiriötilanteissa toimimista, harjoittelua, koulutusta ja hyvien menettelytapojen suunnittelua ei voida liikaa korostaa.

4.2 Teknologiakeskeiset ratkaisut

Tärkeimmät teknologiakeskeiset käytännöt tiedon ja järjestelmien suojaamiseen palvelinpäässä ovat mm. (lähteinä käytetty mm. [CERT]):

- Valitse palvelinlaitteet, joiden tietoturvan perusominaisuudet vastaavat sovellusten mukaista vaatimustasoa. Halpaa ja tietoturvan perusominaisuuksiltaan suppeaa palvelinta ei yleensä voi käyttää vaativiin sovelluksiin.
- Päivitä käyttöjärjestelmät ja sovellukset riittävän nopeasti vikojen löydyttyä. Päivityksiä täytyy seurata jopa päivittäin.

- Aseta pakollinen käyttäjäntunnistus kaikille järjestelmän käyttäjille. Perusta käyttäjältä vaadittavat tunnistuksen metodit sovelluksen ja käyttöoikeuksien mukaisiksi – esim. vahvempi tunnistus (kuten SecurID kortti + salasanat), jos etäkäyttäjätunnuksella on järjestelmän ylläpitäjän oikeudet. Päätä, onko etäkäyttönä tapahtuva järjestelmän hallinnointi tarpeen vai ei. Arvioi, onko tietoturvan kannalta enemmän hyötyä vai haittaa etähallinnasta aiheutuviin riskeihin nähden. Usein järjestelmän etähallinta on hyödyllistä.
- 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.
- 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.
- Käytä järjestelmän kahdennusta palvelun saatavuuden varmistamiseksi. Tämä on kuitenkin tehtävä asiantuntevasti ja ennalta testaten käyttämällä turvallisia replikointimenetelmiä.
- Eristä/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. Pyri aina suojautumaan tavallisimmilta hyökkäyksiltä olemassa olevia suojamenetelmiä hyödyntäen.
- Ota käyttöön järjestelmiä, joilla voidaan havaita järjestelmässä esiintyvä oletettujen käyttöoikeuksien vastainen tai muuten odottamaton ja epäilyttävä toiminta.
- 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.
- Suunnittele ja toteuta huolella mahdollinen järjestelmään kuuluva tietoturvan hallinnoinnin ulkoistaminen, erilaiset vastuut sopimusteitse nauliten. Useinkaan vakavimmat eivät seuraukset kohdistu siihen osapuoleen, joka on vastuussa suojaavista toimenpiteistä, riippumatta siitä mitä sopimuksissa lukee.

4.2.1 Käyttäjien ja laitteiden tunnistaminen

Didi-tv:ssä toteutetun sähköisen kaupankäynnin kannalta loppukäyttäjän tunnistaminen voidaan jakaa kahteen tapaukseen: katsojan henkilökohtaiseen tunnistamiseen ja tilaajan tunnistamiseen, jossa katsojan identiteettitiedolla ei ole merkitystä, vaan palvelun tilaajan tietoja tarvitaan vain maksullisesta sisällöstä laskuttamiseen. Käyttäjän henkilökohtainen tunnistaminen voidaan tehdä paluukanavan yli. Digi-tv-palvelujen tunnistamismenetelmissä päätavoitteena on ollut jo olemassa olevien ratkaisujen hyödyntäminen (esim. web), jolloin kuluttajalle voidaan tarjota samanlainen käyttökokemus palvelusta riippumatta. Tässä on hyödynnetty esimerkiksi pankkien käyttämiä tunnistautumismekanismeja ja erityyppisiä älykorttiratkaisuja. Maksamis-menetelmänä kuluttaja voi käyttää älykorteille ladattavaa rahaa, mobiilimaksamista tai paluukanavan kautta erilaisia turvallisia maksumenetelmiä [TIEKE], [ArviD2].

4.2.1.1 Käyttäjien tunnistaminen

Suomen valtionvarainministeriö suosittelee julkisiin palveluihin:

- Pankkien Tupas-standardin pankkitunnuksia tai
- Kansalaisvarmenteisiin perustuvaa tunnistusta (HST).

Voidaan olettaa, että samoja maksamisperiaatteita siirtyy myös kaupallisiin sähköisiin palveluihin, sillä käyttäjien tottumukset siirtyvät helposti eteenpäin käyttöalueesta (julkinen/yksityinen maksaminen) tai tilanteesta (langallinen verkkoyhteys/langaton yhteys) riippumatta.

Taulukko 5. Tupas ja HST ratkaisuista.

Maksajan tunnistus-ratkaisu	Kuvaus	Yleisyys
Tupas	Suomalaisten pankkien **Tupas-palvelu** (lisätietoja mm. http://www.pankkiyhdistys.fi/): • 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 n. 4 milj. kansalaisella. Nordea, Osuuspankit, Sampo, Säästöpankit, Tapiola, Ålandsbanken.
HST	Kansalaisvarmenne (Hst-) perustuu Väestörekisterin kansalaisille luomaan sähköiseen PKI henkilöllisyyteen. Sähköisen henkilöllisyyden tunnuksena turvallisessa verkkoasioinnissa toimii sähköinen asiointitunnus (SATU). HST-varmenne 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, Handelsbanken, Säästöpankit,Paikallis-osuuspankit, TeliaSonera, VRK.

4.2.1.2 Päätelaitteiden tunnistaminen

Päätelaitteita ei ole tarpeen tunnistaa tai muuten yksilöidä, mikäli käytetään maksutonta ja/tai salaamatonta sisältöä. Maksullisen sisällön käyttö rajoitetaan salauksella, jonka purkamiseksi täytyy hankkia salauksenpurkukortti. Tätä varten päätelaitteessa on oltava kortinlukija, joka tukee Conditional Access (CA) -toimintoa. Kortissa on tyypillisesti salausavaimen lisäksi yksilöivä numero, johon liittyvät asiakastiedot ovat palvelun-tarjoajan tiedossa laskutusta varten. Suomessa käytössä olevien päätelaitteiden CA-järjestelmät perustuvat Conax-salauksenpurkujärjestelmään.

4.2.2 Palvelujen tunnistaminen

Sähköisellä allekirjoituksella voidaan yksilöidä allekirjoittaja ja allekirjoitettu tieto. Jotta allekirjoitus olisi pätevä, sen tulee liittyä yksiselitteisesti allekirjoittajaan. Allekirjoitus on luotava välineellä, jota allekirjoittaja voi pitää omassa hallinnassaan. Tällä saavutetaan tapahtuman kiistämättömyys, mikä vahvistaa allekirjoitetun tiedon ja allekirjoittajan alkuperän ja tiedon eheyden [MINTC].

Sähköisen allekirjoituksen asemaa on selkeyttänyt Euroopan parlamentin hyväksymä direktiivi 1999/93, jonka monet Euroopan maat ovat ottaneet osaksi lainsäädäntöään.

Jotta sähköisessä muodossa oleva tieto voidaan allekirjoittaa, sen sisältämistä tiedoista täytyy ensin laskea tiivistetty muoto. Tämän tehdään tiivistealgoritmeillä. Alkuperäinen ja tiivistetty versio liittyvät toisiinsa matemaattisten kaavojen välityksellä siten, että samasta tiedosta voidaan laskea aina sama tiiviste, mutta siitä ei voida palauttaa alkuperäistä tietoa. Kun alkuperäistä asiakirjaa muutetaan, on siitä laskettava uusi tiiviste. Viestiin liitetyllä tiivisteellä voidaan todistaa tarvittaessa asiakirjan muuttumattomuus. Mikäli tiivistetty versio ei vastaa alkuperäistä, jotain on muutettu. Sähköisessä allekirjoituksessa on käytössä useita tiivistealgoritmeja, esimerkiksi MD5 (128-bittinen tarkistussumma) ja SHA (Secure Hash Algorithm, 160-bittinen).

Sähköisellä allekirjoituksella varmistetaan myös tiedon alkuperä, kun allekirjoittaja salaa tiivisteen yksityisellä avaimellaan. Näin saadaan ns. sinetti, joka lähetetään vastaanottajalle. Lukeakseen viestin, vastaanottajan on purettava salaus lähettäjän julkisella avaimella. Viestin vastaanottaja laskee viestin tiivisteen, ja jos se vastaa lähetettyä tiivistettä, käyttäjä voi olla varma tiedon alkuperästä. Myös salausavaimet voidaan suojata sähköisellä allekirjoituksella. Allekirjoitettua avainta kutsutaan varmenteeksi. 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 tunnistamisessa. Sovelluksena loppukäyttäjälle toimitettavan palvelun 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 (Cerfiticate Revocation List), jota käytetään varmenteen mitätöimiseen ennen sen varsinaisen voimassaoloajan päättymistä, esimerkiksi yksityisen avaimen vuotaessa julkisuuteen.

MHP-palveluissa allekirjoituksilla ja varmenteilla säädellään myös sovelluksen päätelaitteessa saamia oikeuksia sen mukaan onko sovellus allekirjoitettu vai ei. DVB-organisaatio on määritellyt julkisen avaimen järjestelmän, MHP-PKI:n, joka koostuu kolmesta juurivarmenteesta:

1. Aktiivinen MHP PKI juurivarmenne.
2. Korvaava MHP PKI juurivarmenne.
3. Juurivarmenne-hallintaviestin allekirjoitusvarmenne. Root Certificate Management Message, RCMM-viestillä voidaan vaihtaa juurivarmenteet päätelaitteeseen .

Ensimmäiset kaksi ovat MHP-PKI:n päätason varmenteita, kolmatta käytetään vain RCMM-viestien allekirjoitukseen. MHP-määrityksen mukaisesti päätelaitevalmistaja asentaa kaikki nämä varmenteet vastaanottimeen, joiden avulla varmenteista muodostuvat varmenneketjut voidaan todentaa [MHP-PKI].

4.2.3 Sisällönsuojaus

Yleisesti tekijänoikeudet antavat teoskynnyksen ylittävän teoksen tekijälle joukon yksinoikeuksia, jotka on ajallisesti rajattu esimerkiksi julkaistulle teokselle 70 vuoteen tekijän kuoleman jälkeen. Teoskappaleiden levitys on aina ollut hankalaa, koska oikeuksien omistajien asettamat rajoitukset ja materiaalin käyttäjien käytännöt ovat olleet kaukana toisistaan. Tämä asetelma tuskin tulee muuttumaan digitaalisessa maailmassa, jossa avoimista järjestelmistä johtuen 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 paikka, jossa tekijänoikeuksia voi suojauskeinoista riippumatta rikkoa, vaikka digitaalinen ympäristö olisikin suojattu kyseisen teoksen osalta esimerkiksi kryptografisesti. Tästä johtuen kopiosuojauksilla ei näytä olleen vaikutusta ammattimaiseen kopioiden jälleenmyyntiin eli piratismiin. Kannattaa huomata, että ns. ”verkostoefektistä” johtuen jopa tekijänoikeusrikkomuksilla voi olla myös myönteinen vaikutus laillisten teoskappaleiden myyntiin, mikä on mainittu esimerkiksi Microsoftin yhtenä menestyksen osatekijänä.

Koska kuluttajien tottumuksiin vaikuttavat tekijänoikeuksien lisäksi teoskappaleiden saatavuus, oston ja käytön helppous, hinta sekä muut kysynnän ja tarjonnan lait, ei keskimääräinen kuluttaja anna suurta arvoa pelkille tekijänoikeuksille. Monikanava-jakelua käytettäessä sama sisältö on käyttäjien saatavilla useissa eri päätelaitteissa ja useita eri kanavia pitkin. Mikäli yhden kanavan ja päätelaitteen sisällönsuojauksia nostetaan ja käyttäjän toimintaa kuten sisällön kopioimista toiseen päätelaitteeseen hankaloitetaan, käyttäjä voi siirtyä hakemaan saman sisällön jonkun toisen kanavan kautta, olkoonpa lähde laillinen tai laiton, ja mahdollisesti siirtää sen toisiin laitteisiinsa.

Sisältöä suojattaessa panostuksen suuruuteen vaikuttaa myös sisällön arvon kehitys ajan suhteen. Esimerkiksi huomisen säätiedon myyntiaika keskittyy yhteen päivään, jonka jälkeen tuote sisältöineen on varsinkin kuluttajille arvoton. Toisaalta MHP-palvelun myyntiaika voi olla jopa muutaman vuoden mittainen, jonka jälkeen kilpailevat tuotteet tai uuden version kehittyneemmät ominaisuudet voivat viedä sen arvon lähelle nollaa.

Digitaalisen television kehitys tuo mukanaan erilaisia palveluja, tilausvideojärjestelmiä (Video-on-Demand) ja paluukanavan mahdollistamia interaktiivisia palveluja, kuten

pelejä. Sisällön suojauksen rooli kasvaa palvelujen monipuolistuessa. DRM:n toteutus on tärkeää siksi, että tekijänoikeuksin suojattu sisältö ei vuoda, esimerkiksi Internetiin levitykseen. Jos järjestelmässä ei ole toimivaa sisällönsuojausta, uhkana on että televisio-ohjelmista on olemassa korkealaatuisia kopioita Internet-levityksessä, ja maksullisia MHP-sovelluksia vaihdellaan erilaisissa vertaisverkkojärjestelmissä.

DVB-Organisaatio alkoi vuonna 1999 kehittää Sisällön suojaus ja kopionnin hallinta -järjestelmää (CPCM, Copy Protection and Copy Management) digitaaliseen televisioon. Vaikka DVB on kehittänyt aiemmin maksulliseen sisältöön liittyviä suojausmekanismeja (Conditional Access, CA), joita on laajasti toteutettu päätelaitteissa, DVB CPCM -järjestelmän määritys on vielä kesken. Käsitteellinen malli on saatu valmiiksi, ja se sisältää DRM-ratkaisujen tyypilliset komponentit:

- Oikeuksien määritys, jossa kuvataan sisältöön liittyvät käyttöehdot.
- Pääsynvalvonta: Tekninen ratkaisu, jolla varmistetaan että vain oikeutetut katsojat pääset käyttämään sisältöä.
- Tunnistaminen, joka mahdollistaa sisällön seuraamisen tekijänoikeuksien omistajan taholta.
- Laskutus- ja maksujärjestelmät.

Käsitteellisen mallin tavoitteena on säilyttää yhteensopivuus muihin DRM- ja kopioinninestojärjestelmiin myös toteutustasolla. Mahdollisia toteutusteknologioita ovat sisällön salaus jakelijan ja loppukäyttäjän välillä, vesileimaus- ja sormenjälkitekniikat sekä tunnistamisjärjestelmät.

4.2.4 Yksityisyys

Yksityisyys tarkoitetaan loppukäyttäjän oikeutta määrätä itseään koskevista tiedoista, ja vaikuttaa näiden tietojen käsittelyyn sekä tarvittaessa saada tietoja niitä hallinnoivilta osapuolilta. Yksityisyyden suhteen on muistettava, että digitaalinen televisio palveluympäristönä on lainsäädännöllisesti kuin mikä tahansa sähköisiä palveluja 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 digitaalinen televisio on verrattain rajoittunut, joten palvelunkehittäjällä on suuri vaikutus siihen, miten loppukäyttäjä voi hallita omaan yksityisyyteensä vaikuttavaa informaatiota. Digitaalisen television tapauksessa merkittävimmät haasteet liittyvät sähköisten palvelujen käsittelemän tiedon suojaukseen, varsinkin interaktiivisten palvelujen tapauksessa, sekä televisiokanavien keräämän profilointitiedon rajoittamiseen [MINTC2].

4.2.4.1 Yksityisyys sähköisissä palveluissa

Yksityisyyden suoja taataan perustuslaissa. Palvelujen osalta keskeisimpiä säädöksiä ovat:

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

Suomessa lainsäädännöillä on kielletty esimerkiksi asiakastietojen myynti, mutta tällainen uhka on olemassa kun käytetään kanavia (siirtotienä esimerkiksi satelliitti), joiden lähetys tapahtuu maasta, jonka lainsäädäntö ei tätä kiellä.

Pääsääntöisesti voidaan todeta, että henkilötietojen kerääminen on oltava aina perusteltua, eikä loppukäyttäjästä saa kerätä mitään tietoa eikä säilyttää tarpeettomasti.

4.2.4.2 Katsojien profilointi

Kun massamuistilla varustetut päätelaitteet yleistyvät, kasvaa myös mahdollisuus kerätä katsojista ns. profilointitietoa, vaikkapa katsomistottumuksista. Lähtökohtaisesti tällaisen tiedonkeruuseen täytyy aina olla lupa käyttäjältä. Toisaalta profilointi mahdollistaa käyttäjän kannalta uusia sovelluksia, kuten vaikkapa automaattisesti käyttäjän todennäköisesti katsomat ohjelmat tallentava sovellus, mutta tällaisessa tapauksessakin on varmistuttava siitä, että profilointitietoja ei missään vaiheessa siirretä päätelaitteesta paluukanavaa pitkin muualle ilman käyttäjän hyväksyntää.

4.2.5 Digi-tv:n perusrakenteiden suojaaminen

Sähköinen palvelu koostuu sitä käyttävän päätelaitteen lisäksi myös palvelinympäristöstä, joka on yleensä Internetiin kytketty palvelin. Internet-yhteys mahdollistaa paluukanavaa hyödyntävät palvelut. Palvelimen suojaaminen on ensiarvoisen tärkeää, koska palvelun tyypistä riippuen palvelimelle voi olla talletettuna vaikkapa käyttäjän maksuyhteyksiin liittyvää tietoa. Myös palvelujen toimivuus ja saatavuus riippuvat palvelinten toimivuudesta ja niiden suojaamisesta palvelunestohyökkäyksiltä.

MHP-palvelun tuottava järjestelmä kokonaisuudessaan koostuu erilaisista verkoista ja verkkoihin liitetyistä laitteista. Laitteet tai niiden 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 antivirus-ohjelmistot.

Tietokoneet kännykästä ja PDA-laitteista kotitietokoneisiin, palvelimiin ja super-tietokoneisiin, perustuvat yleensä muutamaan peruskomponenttiin ja niiden tarjoamaan toiminnallisuuteen. Prosessori on laskennan ydin ja se tarjoaa sovelluksille suoritus-aikaa, jonka käyttöä esimerkiksi käyttöjärjestelmä säätelee. RAM-muisti on lyhyt-aikaista 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 ja verkkojen sekä 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.

Palvelun tuottavissa laitteissa on kaikkien näiden resurssien käyttöä syytä rajata siten, että esimerkiksi yksi huonosti käyttäytyvä palvelin ei saa kokonaisuutta tilaan, jossa se ei pysty tarjoamaan palvelua käyttäjille. Samoin yhden laitteen sisällä ei esimerkiksi yksi virheellisesti toimiva prosessi saisi saada koko laitetta toimimattomaksi käyttämällä kohtuuttomasti prosessoriaikaa tai RAM-muistia. Se, kuinka paljon yksi palvelimen prosessi tai alijärjestelmän tietokone voi käyttää yhteistä jaettua resurssia, kuten tiedonsiirtokapasiteettia, prosessoriaikaa tai muistia, on mitoituskysymys. Esimerkiksi 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, 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. Samoin myös järjestelmän väärän toiminnan jääminen rajojen sisäpuolelle (ns. false negative) tulisi olla mahdollisimman harvinaista.

Järjestelmän toimintaympäristön muutokset, kuten esimerkiksi 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, helppokäyttöisempää tekniikkaa, kuten XML tai http:n päällä kulkevat etäkutsut (RPC) otetaan käyttöön, niitä vastaan löytyy myös hyökkäyksiä, joita täytyy pyrkiä estämään joillakin uusilla mekanismeilla.

Abstraktiotason nopea nousu ja entistä vihamielisemmät sovellusympäristöt ovat paljastaneet lisäksi sen, että kaikki olemassa olevat ohjelmat ovat sisältäneet sellaisia ohjelmointivirheitä, joiden kautta hyökkääjä on voinut suorittaa kohteessa haitta-ohjelmia. Näiden ohjelmointivirheiden 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, kuten esimerkiksi RAM-muistin luku-, kirjoitus- ja suoritusoikeuksien valvonnalla tai ohjelmatiedostojen digitaalisilla allekirjoituksilla on haavoittuvaisuuksien hyödyntämistä saatu hankalammaksi. Näitä rajoituksia on kuitenkin myös onnistuttu kiertämään esimerkiksi korkeamman tason protokollia, kuten html, ja ohjelmointikieliä kuten JavaScript käyttämällä. Lisäksi protokollien ja ohjelmistojen päältä löytyy vielä käyttäjänä tai ylläpitäjänä 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 mediapäätelaitteissa (maksu-tv) tällainen arkkitehtuuri on mahdollisesti toimivampi, vaikka niissä uhkat (esim. järjestäytynyt rikollisuus, vrt. maksukorttien väärentäminen) voivat olla hyvin erilaiset kuin avoimissa järjestelmissä.

4.2.5.1 Palvelimien suojaamisesta käytännössä

Palvelimella tarkoitetaan ohjelmistoa tai tietokonetta ohjelmistoineen, joka tuottaa palveluja 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 palvelu-alustojen ylläpitotoimet ovat erilaisia, parhaat käyttö- ja ylläpitotavat kehittyvät myös ajan mukaan jne.

CERT-FI on Viestintävirastossa toimiva kansallinen CERT -ryhmä (Computer Emergency Response Team), jonka tehtävänä on tietoturvaloukkausten ennaltaehkäisy, havainnointi, ratkaisu sekä tietoturvauhkista tiedottaminen http://www.ficora.fi/suomi/tietoturva/cert.htm. Palvelinten ylläpitäjien on syytä seurata tällaista ajankohtaista ja yleiseen tietoturvallisuuteen liittyvää tietoa. Esimerkiksi CERT-FI:n ”vuosikatsaus 2004” mukaan mm. matkapuhelimiin kohdistetut haitta-ohjelmat kehittyvät käytännöllisempään suuntaan, joten matkapuhelimiin pääseviä ohjelmia on syytä huolellisesti kontrolloida useilla tahoilla, kuten MPH-palvelujen palvelimissa. Yleensäkin organisaatioiden varautumistoimet Internetin uhkia vastaan korostuvat jatkossa ja varautumistoimet vaativat yhä enemmän aktiivisia toimia ja tilanteiden harjoittelua. IRT -ryhmien (Incident Response Team) käyttö korostuu.

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

Palvelun tuottamiseen tarvittavan ja sen yhteydessä syntyvän tiedon varmuuskopiointi ja pääsynvalvonta on syytä varmistaa, 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 kompleksisuus 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 kuten varmuuskopiointi, kryptografiset protokollat, VPN-laitteet ja -ohjelmistot, palomuurit ja antivirusohjelmistot 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 virhe-tilanteissa, 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 temmeltää vaarantamatta tuotannossa olevaa järjestelmää.

Kun palvelin on toiminnassa, ylläpitäjän täytyy tarkkailla sen toimintaa säännöllisesti esimerkiksi lokitietoja tutkimalla. Lisäksi palvelimen komponenttien toiminta- ja turvallisuusvirheistä on syytä pysytellä tietoisena valmistajan ja viranomaisten tiedotteita ja käyttäjäyhteisöjen keskusteluja seuraamalla. Ohjelmistojen ja käyttöjärjestelmien päivityksistä on syytä tehdä rutiininomaisia erityisesti julkiseen verkkoon liitetyille palvelimille.

Palvelutuotannossa yritysten väliset riippuvuudet monimutkaistavat kokonaisuuden hallintaa aivan samoin kuin itse palvelimenkin hallintaa. Mikäli palvelun tuotannossa joudutaan luottamaan kolmansien osapuolten palveluihin, näiden pettämiseen on syystä tai toisesta hyvä varautua. Esimerkiksi Internet-yhteyden tarjoajan tietoliikenne-, sähköposti- tai nimipalvelussa voi esiintyä yllättäviä häiriöitä, joiden vaikutus liiketoimintaan on syytä etukäteen tarkastaa. Ylläpidon toimintaa häiriötilanteissa on myös syytä suunnitella ja harjoitella etukäteen.

Koska myös yritysten sisäisiin uhkiin tulee varautua, palvelimen ja järjestelmän laillisten käyttäjien sekä 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, voidaan myös virhetilanteita havaita.

Yhteenvetona palvelinten suojaukseen liittyvistä toimista:

- Palvelun tuottavien protokollien ja alustan valinta oman tietämyksen ja muiden suositusten mukaan. Palvelujen karsinta.
- DNS palvelinten suojaus: Internet-yhteydentarjoajan DNS-palvelun suojauksen tarkistaminen.
- Pyrkimys estää käyttäjän erehtyminen palvelimen identiteetin suhteen. Sellaisten palvelinvarmenteiden käyttäminen, joissa palvelimen domain kuvattu. Varmistaminen, että käyttäjä huomaa selvästi, minkä domainin palveluun hän on pyrkimässä.
- Tietojen varmuuskopiointi. Lokitietojen keräys.
- Käyttöoikeuksien hallinta ja valvonta. Kaksisuuntaisen autentikoinnin toteutumisen varmistaminen, ssl/tls, salasanat.
- Ohjelmistojen päivitykset turvallisin väliajoin.
- Turvallisuusohjelmistojen, kuten palomuurin ja antivirusohjelmiston käyttö.
- Mahdollisten uhkien jatkuva havainnointi ja ideointi.
- Riippuvuuksien ja kompleksisuuden hallinta.

4.2.5.2 Hyökkäyksen havaitsemiskäytännöistä

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 toiminta-suunnitelmat. Verkkosensoritkin alkavat olla melko yleisiä. Tietoturvaohjelmistojen toimittajat tuovat IDS-ominaisuudet mukaan omiin paketteihinsa.

Hallintajärjestelmässä ylläpidetään hyökkäystunnisteita sekä sensoreiden säännöstöjä. Toimittajat päivittävät tunnisteita vaihtelevalla reagointinopeudella, mutta pääosin päivitysnopeus on riittävä. Koko tietotekniikka- ja tietoliikennealan 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 tulkita ongelman vaikutus käytössä olevaan ympäristöön. Väärinkäytöstapauksissa tulkitseminen vaatii aina työntekijöiden vahvaa osaamista, mutta hyökkäystunnisteisiin perustuvien hyökkäysten hallinta on helppoa. 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.

Yrityksissä ja organisaatioissa on perinteisesti käytetty useita pienimuotoisia hyökkäystietokantoja tietoturvauhkien hallintaan. Tämä työ on kuitenkin ollut ehkä turhauttavaakin aina uusien hyökkäysten ilmaantuessa ilman ennakkovaroitusta. Maaliskuun 2005 lopussa suuret tietoliikenneyhtiöt ovat päättäneet alkaa jakaa keskenään tietoa tietoturvahyökkäyksistä Fingerprint Sharing Alliance:ssa (http://www.arbor.net/). Tämä yhteenliittymä kerää ja analysoi tiedot kaikista potentiaalisista hyökkäysyrityksistä ja automaattinen järjestelmä varoittaa kaikkia tahoja mahdollisimman varhaisessa vaiheessa, esimerkiksi palvelunestohyökkäyksistä (Tietoviikko). Järjestelmässä erityinen ohjelmisto valvoo verkkoja ja pyrkii tunnistamaan liikenteessä ilmenevät piikit tms., jotka viestivät epänormaalista toiminnasta ja epänormaali aktiviteetti kirjataan niin sanotuksi sormenjälkitiedostoksi, jota voidaan vertailla muihin hyökkäyksiin.

Yleiset lähestymistavat järjestelmää kohtaavien hyökkäysten havaitsemiseksi ovat:

- 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 muuttuvat tai järjestelmäsi tai sen vaatimukset muuttuvat.

4.2.5.3 Virustorjunnasta ja haittaohjelmista käytännössä

Haittaohjelmilla tarkoitetaan vahingollisia tietokoneohjelmia. Haittaohjelmat voidaan luokitella seuraavasti:

Taulukko 6. Haittaohjelmat alatyyppeineen. Lähteenä käytetty mm. [VAHTI 3/2004].

Haittaohjelma	Alatyypit/leviäminen	Perustorjunta	Merkityksellisyys digi-tv-maailmassa
Virukset – kopioituvat ja levittävät itseään uusiin kohteisiin. **Madot** – (virusten osajoukko) – leviävät käyttämällä tarkoituksellisesti verkkoyhteyttä.	Tiedostovirukset - leviävät kaikilla tavoilla, joissa siirretään ohjelmatiedostoja.	**Virusskannauksella** ja **hävityksellä**.	MHP-ympäristössä uhka (plugin).
	Makrovirukset – tarttuvat sovellusten dokumenttitiedostoihin. Leviää dokumenttien mukana käyttöjärjestelmästä riippumatta.	Mm. makrotjen toiminta **estämällä.**	Ei todennäköinen. Vaatii makroja käyttävän sovelluksen, kuten esim. toimisto-ohjelmat.
	Komentojonovirukset – hyödyntää kohdejärjestelmän komentokieliä (scripts).	Mm. **asetuksilla**.	Vialliset laitepäivitykset tai asetustiedostot.
	Sähköpostimadot – leviävät sähköpostissa tai sen liitteessä.	Sähköpostin **skannauksilla**.	Sähköpostisovelluksia käytettäessä uhka.
	Verkkomadot - käyttävät itsenäisesti hyväkseen verkkoyhteyttä.	Mm. **palomuurein**.	Paluukanavan yhteydessä uhka.
Troijan hevoset – tekevät salassa jotain arvaamatonta.	Voivat avata kohdekoneelle takaportin. Voivat lähettää eteenpäin tietoa koneesta tai käyttäjän toimista. Leviävät toisen ohjelman mukana.	Mm. käyttäjän **valveutuneisuus** ohjelmistoasennuksissa.	Paluukanavan yhteydessä uhka, mikäli käyttäjä hyväksyy tällaisen sisällön ajamisen.
Vakoilu- ja mainosohjelmat	Vakoilukomponentteja sisältävät ohjelmat. Vakoiluominaisuudesta saatetaan kertoa, mutta jotkut asentuvat salaa. Esim. tekstitiedostoon piilotettu ADS (Alternate Data Stream).	**Torjuntaohjelmistot**, turvallinen **tiedostojärjestelmä** ja käyttäjän **valveutuneisuus.**	Mahdollinen Internet-sisältöjä käytettäessä. MHP:ssä turvamekanismeja, jotka vaikeuttavat tällaisten asentamista.
Huijausviestit (Hoax), ketjukirjeet ja pilailuohjelmat	Huijausviestit tuhlaavat aikaa, pyytävät poistamaan tiedostoja. Pilailuohjelmat antavat virheellisiä ilmoituksia. Leviävät hyväuskoisten käyttäjien lähettäminä.	Mm. käyttäjän **valveutuneisuus**.	Mahdollinen Internet-sisältöjä käytettäessä.

Digisovittimen rajoittuneet ominaisuudet pienentävät osaltaan haittaohjelmien uhkaa. Toistaiseksi esimerkiksi ei ole mahdollista ottaa yhteyttä suoraan toiseen päätelaitteeseen, mikä estää tehokkaasti verkkomatojen leviämisen. Tyypillisestä koti-pc:stä eroten digisovittimessa ei yleensä ole käyttäjän tietämättä lukuisia verkkoyhteydessä olevia sovelluksia käynnissä, joihin haittaohjelmien kannattaisi yrittää ottaa yhteyttä. Digisovittimen rajallisten resurssien vuoksi virustorjunta tulisi tapahtua verkkopalvelimella, eikä päätelaitteessa jo virustietokantojen päivitysten sujuvuuden varmistamiseksi.

Virukset aiheuttavat ainakin epäsuoraa vahinkoa – ne kuluttavat levytilaa, aiheuttavat yhteensopivuusongelmia ja hidastavat laitteen toimintaa. Ne sisältävät usein ohjelmointivirheitä, jotka saattavat aiheuttaa vahinkoa viruskirjoittajan tahtomattakin.

Verkko-operaattorin on suojattava verkkonsa reunat sekä laitteet virustorjunta-järjestelmin, mutta tämäkään ei yksin riitä, vaikka televisioverkko onkin erillinen verkko, josta on Internetiin pääsy vain tietyistä kohdista. Yksittäinen toimija ei yleensäkään pysty ottamaan koko vastuuta tietoturvasta, vaan hyvä suojaus vaatisi myös operaattorien välistä (päivittäistä) yhteistyötä kansainvälisestikin. Verkoissa voidaan suojautua mm. monitoroimalla seuraavien protokollien avulla siirrettävää data: SMTP, POP3, http, TFP, IMAP4, NNTP ja SOCKS.

Erittäin tärkeä teknologinen suojaus on myös laitteen muistien ominaisuudet – mm. suljetut muistialueet, joilta ei voi viitata ulos, read/write -alueet (ei suoritusta), vain ROM alueet, jne. Näihin tarvitaan sekä fyysisiä että ohjelmallisia toteutuksia. Ohjelman haitallista toimintaa on syytä valvoa ohjelmabinäärejä heuristisesti tutkivilla antivirus-ohjelmistoilla pelkän virustunnisteen etsinnän lisäksi, sillä uudet haittaohjelmat leviävät todella nopeasti. Jos hiekkalaatikkoon laitettu ohjelma yrittää jotain asiatonta, se paljastuu haittaohjelmaksi ja tuhotaan.

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

- Työasemia ja palvelimia ylläpitämään 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 tuotanto-järjestelmät sekä työasemat tulee erottaa omiin segmentteihinsä.
- LAN eristettävä verkon liittymäpisteissä haittaohjelmatorjunnalla, palomuurilla ja reitittimen turvaominaisuuksilla. Etäyhteydet on turvattava erikseen.

5. MHP-palvelun kehitystyöhön liittyvät erityispiirteet

Palvelunkehitystyöhön liittyviä erityispiirteitä on hyvä lähteä tarkastelemaan mukana olevien toimijoiden näkökulmasta, ja siitä, minkälaisia arvoverkkoja ne muodostavat. Toimijoiden väliset luottamussuhteet vaikuttavat osaltaan siihen, minkälaisia palveluja loppukäyttäjä saa. Tästä on esimerkkinä sopimuksellinen luottamus, vaikkapa maksujärjestelmän toimittajan ja operaattorin välillä. Luottamussuhteet syntyvät osittain normaalin liiketoiminnan kautta, mutta myös esimerkiksi sääntely ohjaa digi-tv-maailman toimijoiden roolia hyvin merkittävästi, vaikka tämä ei välttämättä näykään suoraan palvelunkehittäjälle tai loppukäyttäjälle kovin merkittävänä luottamussuhteiden muodostajana.

Luvussa tutkitaan myös tietoturvan integroituvuutta ja helppokäyttöisyyttä. Miten nämä voitaisiin parhaiten toteuttaa palvelunkehittäjän näkökulmasta. Tässä luvussa käsitellään yksityiskohtaisemmin kaikkia palvelunkehitysprosessin vaiheita, mm. ideointia, suunnittelua, testausta, toteutusta, käyttöönottoa ja ylläpitoa.

5.1 Luottamusmallit

Tämän selvityksen yhtenä 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. Myöskään yrityshaastatteluissa ei päästy pureutumaan tähän riittävällä tasolla, sillä sellaista case-esimerkkiä ei voitu osoittaa, josta olisi voitu avoimesti puhua tai jonka edes kaikki haastateltavat olisivat jotakuinkin tunteneet.

5.2 Luottamuksen rakentaminen

Luottamuksen rakentaminen vaatii yhteistyötä eri toimijoiden kesken sen lisäksi, että eri toimijat omilla sisäisillä prosesseillaan pyrkivät näihin päämääriin. Esimerkiksi tietohävikistä 80 % johtuu käyttäjien toiminnasta (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 useisiin asioihin [FIBA], mm:

- Luottamus pankkeihin instituutiona,
- Kokemuksiin aiemmista pankkipalveluista,
- Pankkipalvelujen toiminnallisuudesta ja mahdollisista vakavista ongelmista,
- Muiden käyttäjien mielipiteistä.

Suomessa pankkeihin luotetaan sähköisten pankkiasiointipalvelujen tarjoajana kansainvälisessä vertailussa erittäin hyvin. Asiakkaiden luottamusta on rakennettu sähköisiin pankkipalveluihin mm: luomalla käyttäjille tiettyjä tapoja toimia (esim. maksupalvelut, puhelinpankki) sekä kehittämällä palvelujen 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 kokonaisuuden merkittävimmän yrityksen tietoturvavaatimukset määrittävät kaikkien toimintaketjun yritysten tietoturvallisuuden tason [YRTI]. Usein tämä ”veturiyritys” tarkastaa myös muiden toimijoiden turvallisuusmenettelyt. Myös lainsäädäntö, viranomaisten ohjeet sekä mahdolliset sopimukset sekä alakohtaiset vaatimukset edellyttävät, että yrityksen henkilöstö on tietoinen yrityksen tietoturvavastuista sekä menettelytavoista, joilla vastuut käytännössä toteutetaan. Tietoturvan kehittäminen tulee olla osana yrityksen strategista suunnittelua ja tavoitteiden asettamista. Yrityksellä tulee olla tietoturvapolitiikka määriteltynä ja käytännönläheinen ohjeistus tietoturvapolitiikan toteuttamiseksi.

Käyttäjän sekä muiden palvelukehitykseen osallistuvien toimijoiden luottamusta valittuun palvelukonseptiin voidaan nostaa käyttämällä tunnettuja referenssitoteutuksia, parhaita työkaluja, soveltuvia menetelmiä ja standardeja tuotteen pohjana. Samoin 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 digi-tv-palveluissa arvoverkostot ja ansaitsemislogiikat ovat usein edelleenkin kypsymättömiä, jolloin niiden selventämiseen on panostettava koko prosessin ajan.

Teknologisia tekijöitä luottamuksen kasvattajana:

- Käyttäjän ja palvelun tunnistaminen luotettavasti.
- Tunnetun palvelualustan käyttö, levitettävien sisältöjen puhtauden varmistaminen.
- Verkkoteknologian ja päätelaitteiden luotettavuus ja turvallisuusominaisuudet.
- Testattujen teknologioiden käyttö on suositeltavaa.

Muita luottamukseen liittyviä tekijöitä:

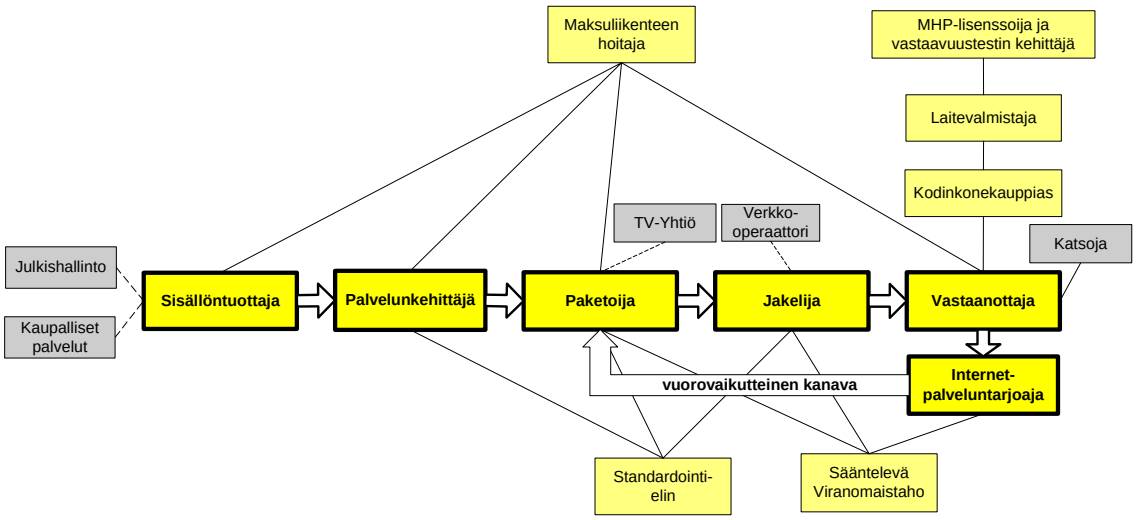
- Sertifioitujen tuotteiden ja ammattilaisten käyttäminen.
- Yrityksen olemassa olevat palvelut, aiempi hyvä imago ja maine, tietosuojan hoito.
- Luotettavat toimijat, alihankkijat, luotettavan kolmannen osapuolen käyttö, esim. lausunnot tietoturva auditoinneista.
- Muiden käyttäjien positiiviset mielikuvat.

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 vaikkapa uhkia haittaohjelmista tai tekniikan epäluotettavaa toimintaa (sisältäen tietojärjestelmät ja verkot).

5.3 Yleistä pohdintaa palvelunkehityksestä

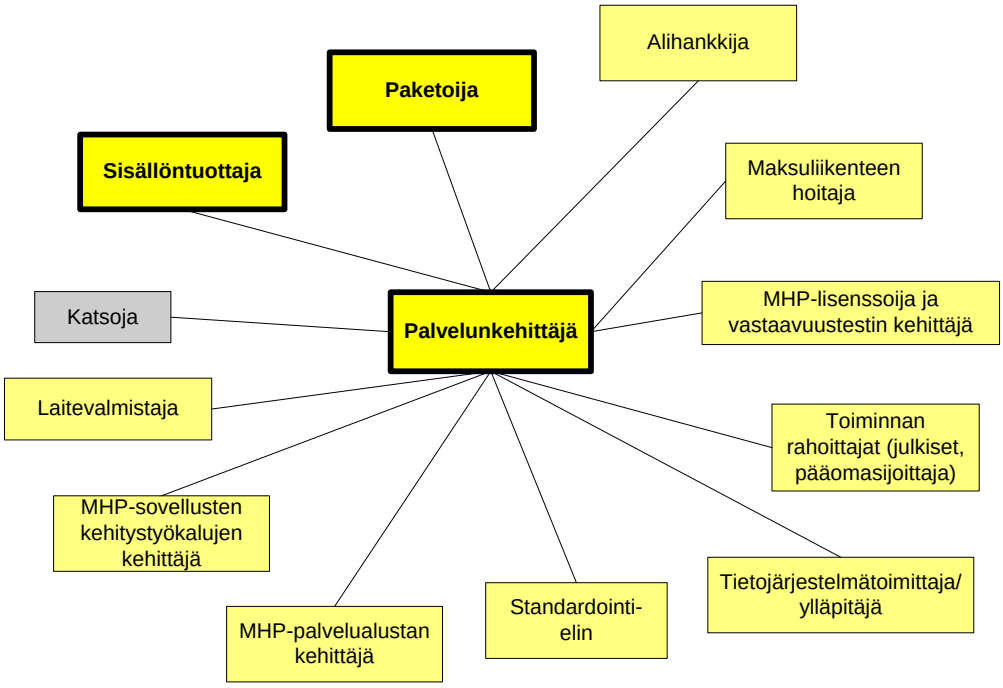
5.3.1 Toimijat – arvoverkko

Arvoverkko digitaalisen television maailmasta MHP-palvelunkehittäjän näkökulmasta on esitetty kuvassa 10. Toimijoiden määrä ja riippuvuussuhteet sekä liiketoimintamallien monimutkaisuus vaikuttavat luottamusmallien kautta sovelluskehittäjän toimintatapoihin ja jopa itse palvelunkehitysprosessiin. MHP-sovellukset ovat tyypillisesti kytköksissä muihin lähetyspalveluihin, kuten peleihin, tapahtumiin ja muihin sovelluksiin, joita yhdistelemällä kuluttajalle tarjottu palvelu on koottu. Toimijoiden roolit eivät ole yksiselitteisiä; esimerkiksi Suomessa paketoijan roolissa toimivat televisiokanavat ovat hyvin useasti myös palvelunkehittäjiä ja sisällöntuottajia. Tästä syystä arvoverkkokuvaus on aina palvelu- ja näkökulmasidonnainen.



Kuva 10. Digitaalisen television arvoverkko.

Kuvassa 11 arvoverkkoa on tarkasteltu MHP-palvelunkehittäjän näkökulmasta ja lisätty siihen toimijoita, jotka ovat merkityksellisiä itse palvelunkehitysprosessin näkökulmasta. Palvelunkehittäjän prosessiin suoranaisesti liittyvien sisällöntuottajan ja paketoijan lisäksi siinä ovat osallisena mm. alihankkija, joka on tietoturvan kannalta erittäin tärkeä komponentti. Palvelunkehittäjän on tunnettava heidän tuotekehitysprosessinsa ja tapansa toimia esimerkiksi tietoturvanloukkaustilanteissa. Standardointiorganisaatiot, laitevalmistajat ja palveluun liittyvien muiden komponenttien kehittäjät asettavat kukin tiettyjä vaatimuksia palvelunkehitysprosessille ja itse kehitettävälle palvelulle.



Kuva 11. MHP-palvelunkehittäjän arvoverkko.

5.3.2 Asiakaslähtöisyys

Interaktiivisen television tapauksessa asiakaslähtöisyys tarkoittaa mahdollisimman helppokäyttöisiä ja standardilla tavalla rakennettuja käyttöliittymiä. Käyttöliittymän alla olevat tekniset ratkaisut ja tietoturvamekanismit eivät ole katsojan mielenkiinnon kohteena, ennen kuin joku menee vikaan. Loppukäyttäjän teknisestä osaamistasosta ei voida käytännössä olettaa mitään, johtuen television katsojien heterogeenisuudesta. Loppukäyttäjän mielenkiinnon kohteena eivät siis ole tekniset ratkaisut, vaan se, onko sijoitetulla rahalla saatu luvattu hyödyke. Katsojan on saatava maksamansa palvelu niin että se tekee mitä palveluntoimittaja on luvannut, eikä aiheuta häiriöitä muille samassa laitteessa toimiville palveluille. Palvelun myyjällä on tässä suuri vastuu jo säädöstenkin kautta. Kuluttajansuojalaki ja tietosuojalaki ovat tiukkoja ja kuluttajaa suojelevia. Digitaalisen television maailmasta on pääsy myös sähköiseen kaupankäyntiin interaktiivisten sovellusten kautta. Tällöin kuluttaja on samassa tilanteessa kuin tänä päivänä Internetin kautta hyödykkeitä tilaava asiakas. Myös loppukäyttäjän kuluttajan roolissa on tiedostettava riskit esimerkiksi luottokorttimaksuissa. Kuluttajan käyttäytymistä voidaan palvelun käyttöliittymän hyvällä suunnittelulla kuitenkin opastaa turvallisempiin toimintatapoihin esimerkiksi varmenteiden hyväksynnässä ja maksutapahtumissa.

5.3.3 Tietoturvalähtöisyys

Tietoturvalähtöisyys voi organisaatiossa muodostua mm. riskinhallinnasta, strategisesta suunnittelusta, ja resursoinnista. Käytännössä tämä voi tarkoittaa mm.:

- Suojaa oma verkko.
- Sulje kehitysympäristö ja/tai testiverkko joko osittain tai kokonaan.
- Etsi hyvät toimijat - tarkasta eri toimijoiden tietoturvan taso.
- Tutki toimitusketju (keneltä mikäkin komponentti hankittu, miten, jne.).

5.4 Palvelunkehitysprosessista

Sähköisiä palveluja 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 jonkun tyyppisiä 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 tärkeää on muistaa, että vaikka palvelunkehitysprosessi olisikin hyvin määritelty, se ei koskaan ota huomioon kaikkia tietoturvaan liittyviä tekijöitä, jotka ovat ajan myötä muuttuvia. Toisin sanoen, 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 12. 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 Palvelunkehitysprosessin vaiheiden suhde ratkaisuihin

Taulukossa 7 on sijoitettu tärkeimmät ratkaisut palvelukehitysprosessin eri vaiheisiin.

Taulukko 7. 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
	Teknisten prosessien seuranta, parantaminen ja koulutus.	Palvelunkehitysprosessin uhkat.		x	x	x	X	X	x	

Liitteessä B (Yksityiskohtaiset uhkat kussakin kehitysvaiheessa) on yksityiskohtaisempi taulukko.

5.4.2 Palveluidean/konseptin kehittely

Palvelun idea saattaa usein tulla sisällöntuottajalta, palveluntarjoajalta tai tietenkin palvelunkehittäjältä itseltään. Näillä toimijoilla on 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, sisällön paketoijalta (esimerkiksi televisiokanava) sekä erilaisilta viranomaistahoilta ja tutkimuslaitoksilta. On hyödyllistä, että jo ideointi vaiheessa selvitetään, mitä standardeja toimialaan ja palveluun liittyy, ja miten ne voisivat olla hyödynnettävissä. Standardien ulkopuoliset ratkaisut johtavat usein umpikujaan palvelun laajetessa. Tietoturvan kannalta useimpien toimijoiden tuntemat standardiratkaisut ovat parhaita luotettavuuden ja toteutuksen (esim. alihankinnan) kannalta.

Tietoturva-asiantuntijan, esim. konsulttitoimiston, käyttö on usein erittäin hyödyllistä jo palvelunkehitysprosessin alkuvaiheessa: pääuhkien identifiointi uudessa palvelussa (systeeminäkökulma), tärkeimmät kyseeseen tulevat tietoturvaratkaisut ja niiden realistisuuden arviointi voisivat kuulua konsultin tehtäviin.

Käytännössä kysymys on pääasiassa tuote/palvelukehitysympäristön riskienhallinnasta ja elinkaariajattelusta, esim. minkä ajanjakson tai vaiheen riski voi realisoitua. Lopussa testataan palvelun laatu ja sitkeys (robustness).

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).
- Selvitä, mitkä uhkista ovat realisoituvia käytännössä, onko meillä resursseja suojautua.
- Hallitse riskejä.
- Arvioi suojaukseen käytettäviä kustannuksia verrattuna suojattavan omaisuuden/tiedon arvoon.
- Tee alustavat suunnitelmat kaikille kehittelyyn liittyville prosesseille.

5.4.3 Palvelun suunnittelu

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 mm. tiettyjen työkalujen aiheuttamia rajoituksia palvelun toteutukseen. Jotkin työkalut voivat tarjota esimerkiksi riittämättömiä tietoturvaominaisuuksia kuten päivittämättömän protokollan tai algoritmin. Tärkeää on myös edeltä käsin selvittää, millaiset käyttäjäryhmät palvelua tulisivat käyttämään, jolloin helppokäyttöisyys (esim. tietoturvaominaisuuksien parametrit ja asetusvaihtoehdot) kriteerit selkiytyvät. Tämä koskee erityisesti kohdennettuja palveluja.

MHP-palvelu voidaan toteuttaa monella tavalla. Kyseessä voi olla selainpohjainen paluuyhteydetön tai paluukanavaa käyttävä palvelu, jolloin palvelu toteutetaan käyttäen markkinoilla olevia Xhtml-editoreita. Tyypillisesti päätelaitteen selain ja kehitysympäristö ovat saman valmistajan tekemiä. Tällaisen palvelun tekeminen ei vaadi varsinaista ohjelmointia, vaan suurin osa työstä on käyttöliittymän suunnittelua. Palvelun toteuttaminen voi vaatia myös Java-ohjelmointia ja erilaisten MHP:ssa standardoitujen ohjelmakirjastojen käyttöä. Markkinoilla on myös työkaluja Java-pohjaisten MHP-palvelujen kehittämiseen. Ennen ohjelmointityön aloittamista se on vaiheistettava jollakin tavoin sisältäen palveluun liittyvän liiketoimintasuunnittelun, vaatimusmäärittelyn, toteutussuunnitelmat, suunnitelmia käyttöönotosta ja testauksesta. Kaikki tämä voi olla hyvin palvelukohtaista, mutta tietoturva tulisi olla eräs näkökulma, joka on aina mukana kaikissa suunnittelun vaiheissa. Lisäksi esim. kehitysympäristöjen ja dokumenttien tietoturva testaus tai auditointi täytyisi suunnitella jollain tavalla.

Tietoturva tulisi ottaa huomioon heti palvelun suunnitteluvaiheessa, kun ideointivaihe on tuottanut palvelukonseptin. Tässä vaiheessa tulee kiinnittää huomiota tietoturvavaatimuksiin – esim. minkälaisia tunnistusjärjestelmiä tarvitaan, onko tarvetta salatuille yhteyksille, miten käyttöoikeuksia hallitaan ja miten tallennettava tieto suojataan. Tässä vaiheessa on tiedettävä, minkälaista tietoa palvelu käsittelee, ja mitä vaatimuksia sen suojaukseen on esim. lainsäädännön näkökulmasta. Tietoturvaan liittyvät komponentit tunnistetaan ja suunnitellaan tässä vaiheessa muun järjestelmän kanssa.

5.4.4 Palvelun toteutus

Palvelun toteutusvaiheessa tutkitaan eri toteutusvaihtoehdot ja valitaan niistä paras. Lisäksi valitaan oikeat tekijät käytettävien teknologioiden mukaan. Tietoturva on melko uusi asia digitaalisen television palvelujen toteutuksessa, koska interaktiivisia palveluja ei ole kovinkaan laajamittaisesti vielä kehitetty. Näin esimerkiksi MHP-palvelun 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 siitä, että prosessi on tietoturvallinen kaikissa olosuhteissa.

5.4.5 Palvelun testaus

Tärkeimpiä asioita testauksessa ovat sen monipuolisuus ja kattavuus. Testauksen hahmottaminen useammasta eri näkökulmasta auttaa ohjelmistojen ja järjestelmien toimintavarmuutta. Tämä tarkoittaa esimerkiksi sitä, että tulisi käyttää sekä ohjelmiston staattista että dynaamista analyysia. Ohjelmistoa tulisi käsitellä sekä avoimena että suljettuna järjestelmänä keskittyen sekä ohjelmistokoodin rakenteeseen että käännetyn ohjelmiston toimintaan ympäristöönsä nähden. Hyväksymistestauksessa tulisi keskittyä ohjelmiston oikeellisen toiminnan varmistamisen lisäksi testaamaan, ettei ohjelmisto toimi ei-toivotuilla tavoilla.

Testauksen kattavuutta ohjelmiston tilajoukosta ja koodipohjasta tulisi mahdollisuuksien mukaan arvioida. Ohjelmiston toimintaa järjestelmän kuormittuessa tulisi arvioida, kuorma voi aiheuttaa palveluneston tai mahdollistaa hyökkäyksiä operaatioiden epäatomisuuksien vuoksi.

Rajapintatestauksen tärkeys verkkoympäristössä korostuu. Ympäristöstä saatavien syötteiden oikeellisuuden varmistamista ohjelmistossa testataan sekä laillisilla syötteillä, että täysin virheellisillä, pahantahtoisilla syötteillä. Ympäristörajapinnat testataan siis integraatiotestauksen lisäksi toimintavarmuustestauksella. Ohjelmiston muuttuessa erityisen tärkeää on suorittaa regressiotestausta, etteivät vanhat viat ilmaannu uudelleen koodin uudistumisen myötä.

MHP-sovellusten kohdalla erityispiirteenä on syytä mainita nk. yhdenmukaisuustestaus, jolle MHP:n standardoinnista vastaava organisaatio on määritellyt yksityiskohtaiset testitapaukset. Tällä hetkellä testausprosessi on hyvin yksinkertainen: MHP-yhteen sopivan laitteen kehittäjä hankkii testikirjaston ja vaadittavat dokumentit ETSI:ltä ja

suorittaa testit itse. Onnistuneiden testien jälkeen kehittäjä voi lunastaa oikeuden käyttää MHP-logoa tuotteessaan. On huomattava, että sovellusten kohdalta tällainen yhdenmukainen testausprosessi puuttuu.

Palvelun toteutus- ja testausvaiheessa suunnitellut tietoturvaratkaisut koodataan hyvien ja turvallisten koodausperiaatteiden mukaisesti ja koodi katselmoidaan ja testataan kattavasti. Testausvaiheessa on syytä tehdä myös haavoittuvuustestausta ja analysoida sen tuloksia.

5.4.6 Palvelun käyttöönotto

Palvelun käyttäjän näkökulmasta palvelun käyttöönotto on kriittinen vaihe. Käyttäjän täytyy mahdollisesti ladata jokin ohjelma päätelaitteeseensa, tai hänen täytyy saada joitakin laiteasetuksia muutetuksi palvelulle sopiviksi. Jatkossa joudutaankin enenevässä määrin rakentamaan käytäntöjä ja sovelluksia, joilla käyttäjä pystyy muuttamaan ja päivittämään laitteensa asetuksia automaattisesti. Tämä on vaativa ongelma tietoturvanäkökulmasta, sillä jonkin yksittäisen toimijan määräämät asetukset saattavat estää käyttäjää käyttämästä joitain toisia palveluja. Verkko-operaattori onkin keskeinen toimija palveluasetuksiin liittyen. Rajapinta verkkopalvelujen ja muiden palvelujen välillä on kuitenkin hämärtynyt ja tämä voi tuottaa ongelmia esim. palveluntarjoajan, verkko-operaattorin ja käyttäjän välisiin suhteisiin.

Palvelun markkinoinnin merkitys kasvaa monipuolisemmaksi, koska sen avulla annettu viesti palvelun sisällöstä tai käyttötavoista saattaa vaikuttaa myös tietoturvaan kuluttajan omaksuman asenteen johdosta. Kuluttajan kokemaan tietoturvaan vaikuttaa voimakkaasti myös palveluntarjoajan sitoutuminen palveluun. Jos palvelut jäävät lyhytikäisiksi kokeiluiksi tai niiden operointi ei ole ammattimaisesti toteutettu, saattaa kuluttaja pettyä odotuksissaan ja menettää hänelle palveluun kertynyttä hyödyllistä informaatiota, jonka säilymiseen hän on luottanut.

5.4.7 Palvelun ylläpito

Teknisten ratkaisujen kehittämistyö on monimutkaistunut, samalla kun kehitystahti on kiihtynyt. Tämä yhtälö on vaikeasti hallittavissa. Seurauksena onkin voinut olla, että tuotteissa ja palveluissa on puutteita ja virheitä, jotka aiheuttavat niiden haavoittuvuutta. Haavoittuvuudella tarkoitetaan ohjelmistossa tai laitteistossa esiintyvää virhettä, joka voi olla syntynyt suunnittelu-, toteutus-, käyttö-, tai ylläpitovaiheessa, ja joka voi mahdollistaa sen asiattoman hyväksikäytön. Hyväksikäyttö voi tarkoittaa esimerkiksi luvatonta tiedon käyttöä tai keskeisten prosessien häirintää. Haavoittuvuudet syntyvät inhimillisten erehdysten, väärien tuotantoprosessien tai vastaavien hallintaongelmien seurauksena [Arbaugh 2000]. Tiedonlähteitä haavoittuvuuksien torjuntaan löytyy esim. SANS:n (SysAdmin Audit Network Security Institute), http://www.sans.org kautta.

Haavoittuvuuksien käsittelyprosessilla 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 [Laakso 1999]:

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

Käsittely alkaa, kun haavoittuvuus havaitaan. Löytynyt virhe arvioidaan, ja mikäli se todetaan todelliseksi, virhe raportoidaan koordinoijalle ja valmistajalle. Molemmat suorittavat oman arviointinsa löydöksen oikeellisuudesta ja tekevät siitä yhteenvedon. Mikäli haavoittuvuus todetaan todelliseksi uhaksi, käynnistyvät varsinaiseen korjauksen julkistamiseen johtavat valmistelut. Näkökulmaa on myöhemmin laajennettu [Havana 2003], jolloin otetaan huomioon, että haavoittuvuuksien käsittelyssä on huomioitava myös laaja joukko toissijaisesti siihen vaikuttavia toimijoita. Näitä ovat esimerkiksi valmistajien alihankkijat, jälleenmyyjät, omistajat, vakuutusyhtiöt, media, koulutus-organisaatiot, lainsäädäntöelimet ja standardoinnista vastaavat toimijat.

Tähän mennessä tehdyissä digi-tv-toimijoiden haastatteluissa on käynyt ilmi, että haavoittuvuusprosessiin osallistuvien toimijoiden määritteleminen on ollut vaikea tehtävä. Toistaiseksi selvästi yhtenevää käsitystä ei ole syntynyt. Asian selvittäminen vaatisi lisää tiedonkeruuta. Ylläpitovaiheessa tietoturvaan liittyvä toiminta onkin yleensä reaktiivista: palvelun haavoittuvuus voi johtua myös palvelun tai ohjelman asetuksista mikä hidastaa korjauksen aloittamista. Ennakoiva tapa välttää ylläpitovaiheen ohjelmistohaavoittuvuuksia on tehdä järjestelmästä mahdollisimman yksinkertainen. Lisäksi järjestelmän komponenttien täytyy olla helposti päivitettäviä ja ylläpitäjän pitää huomioida, että myös erilliset tietoturvatuotteet ja -ominaisuudet lisäävät järjestelmän monimutkaisuutta.

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

5.4.8 Palvelun edelleen kehittäminen

Palvelun edelleen kehittäminen voi tapahtua useammastakin syystä, yhtenä esimerkkinä palvelun käyttäjämäärien kasvu tai muuttuneet odotukset palvelusta. 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 sitä, että palvelua pitää pystyä käyttämään uuden MHP-standardin mukaisissa laitteissa vanhan MHP1.0.2-mukaisten laitteiden lisäksi. Tällöin on käytävä uudelleen läpi arkkitehtuurin suunnitteluvaihe ja katsottava, mitkä oletukset ovat muuttuneet uuden standardiversion myötä. Samalla pitää ottaa huomioon esimerkiksi tulevaisuuden kapasiteettitarveasiat. Palvelinten tai ohjelmistojen kapasiteetti voi muodostua ongelmaksi vanhassa arkkitehtuurissa, samoin kuin tietoturvapalvelujen riittävyys.

Vaikka pilottivaiheessa ongelmia ei havaittu, voi käyttäjämäärän kasvu ja joidenkin uusien käyttäjien erilainen asenne palvelun seuraavassa vaiheessa muodostua tekijäksi johon palvelun kehittämisessä täytyy ennalta varautua. Kehittäjäverkosto tai muiden toimijoiden, kuten verkko-operaattorin ja palveluoperaattorin, pitäisi pystyä auttamaan näissä tilanteissa. 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.

Jatkokehitysvaiheessa on syytä pitää huoli siitä, että suunnittelu- ja toteutusvaiheessa saavutettua tietoturvan tasoa ei heikennetä esim. valitsemalla palvelun uuteen versioon komponentteja, joita ei ole riittävästi testattu, tai tekemällä muutoksia ilman asianmukaista muutostenhallintaprosessia. Tässä prosessissa muutokset on dokumentoitava, testattava ja hyväksyttävä ennen kuin ne tulevat tuotantoversioon.

5.4.9 Palvelun lopettaminen

Palvelun lopettamisessa korostuvat asiakkaiden tietosuojaan liittyvät kysymykset, joita ovat esimerkiksi:

- 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 sen yrityksistä tallentuneena johonkin ja hyödynnettävissä?
- Ovatko salasanat ja muut tietoturvan hallintaan liittyvät tiedot tuhottu asianmukaisesti?

Palvelun lopettamisvaiheessa on myös tarkasteltava eri viranomaistahojen vaatimuksia tallennetun tiedon hävittämisestä. Nämä vaatimukset on syytä kirjata ylös jo palvelun suunnitteluvaiheessa ja ne on sisällytettävä palvelun ylläpitäjän tietoturvapolitiikkaan.

Lähdeluettelo

[Arbaugh 2000] Arbaugh, W.A., Fitchen, W.L. & McHugh, J. 2000. Window-s of Vulnerability. A Case Analysis. IEEE Computer. Vol. 33, No. 12. Saatavilla www-muodossa: http//www.cs. umd.edu/~waa/pubs/Windows_of_Vulnerability.pdf

[ArviD] Digi-tv:npaluukanava ArviD-julkaisu 01/2005.http://www.arvid.tv/micaj_storage/EB0A30B34658E20BDAFC4AD09BC660C0/29/ArviD-2005-01_Digi-tv_n_paluukanava.pdf

[ArviD2] Digitaalisen television ansaintalogiikat – Palvelujen kustannuksista ja ansainnasta digi-tv:ssa ArviD-julkaisu 03/2004 http://www.arvid.tv/micaj_storage/D9A1CBB1450B87333BD27D6B128EA98A/29/ArviD-2004-03_Digitaalisen_television_ansaintalogiikat.pdf

[ArviD3] Digi-tv:n palveluntekijän opas Vuonna 2001 Tekes-ohjelmassa tehdyn oppaan päivitys. ArviD-julkaisu 01/2004 http://www.arvid.tv/micaj_storage/D9A1CBB1450B87333BD27D6B128EA98A/29/ArviD-2004-01_Digi-tv_n_palveluntekijan_opas.pdf

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

[D-Book] DGtvi D-Book (D-book v.1 (final)(corr) clean.doc) Sept. 2004. Compatible DTtv receivers for the Italian Market. http://www.dgtvi.it/pdf/D_book_v1.pdf

[Digitv] http://www.digitv.fi/

[DVB] http://www.dvb.org/

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

[FICORA] http://www.ficora.fi/suomi/radio/digitv.htm

[FICORA2] Vuorovaikutteisen kanavan toteutusmahdollisuuksista digitaalisessa televisiojärjestelmässä. DVB-MHP-ryhmän paluukanavaraportti4/2005. http://www.ficora.fi/suomi/document/TRaportti042005.pdf

[Havana 2003, Ottawa] Havana, T. & Röning, J. Communication in the Software Vulnerability Reporting Process. In the proceedings of the 15th FIRST Conference on Computer Security Incident Handling. Ottawa, Canada. 22.-27.6.2003.

[Havana 2003] Havana, T., Laakso, M., Kemi, P. & Röning, J. 2003. Checklist for Designing a Vulnerability Disclosure Policy. Esitetty Cybersecurity Reseach and Disclosure Conference-tapahtumassa, Stanford, Palo Alto, USA. 11/2003. Saatavilla http://www.ee.oulu.fi/research/ouspg/protos/sota/Stanford2003/index.html

[Laakso 1999] 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.

[LUOTI] www.luoti.fi

[MHP] http://www.mhp.org/documents//mhp_Ts101812.V1.2.1.pdf.zip

[MHP-PKI] http://www.dvbservices.org/index.php?id=39

[MINTC] Turvalliset sähköisen allekirjoituksen luomisvälineet. Vaatimusten arviointi Julkaisuja 52/2004. http://www.mintc.fi/oliver/upl878-52_2004.pdf

[MINTC2] Digi-tv:n yksityisyys
http://www.mintc.fi/www/sivut/dokumentit/julkaisu/julkaisusarja/2002/a022002.pdf

[MPEG2] ISO/IEC IS 13818-1 "Information technology – Generic coding of moving pictures and associated audio information – Part 1: Systems", International Standards Organisation (ISO), 2000.

[NORDIG] http://www.nordig.org

[Södergård 1999] Digitaalisten televisiolähetysten käyttö datajakelussa Södergård, Caj; Ollikainen, Ville; Mäkipää, Risto1999. VTT, Espoo. 69 s. + liitt. 3 s.
VTT Tiedotteita - Meddelanden - Research Notes : 1971 ISBN 951-38-5458-2; 951-38-5459-0 http://www.inf.vtt.fi/pdf/tiedotteet/1999/T1971.pdf

[TIEKE] Julkisen hallinnon palvelut digi-tv:ssä – selvitys. Valtiovarainministeriön ja liikenne- ja viestintäministeriön Tietoyhteiskunnan kehittämiskeskus ry:ltä. tilaama selvitys suomalaisen julkishallinnon kehitysnäkymistä digitaalisessa televisiossa. TIEKE ry/TIEKEn julkaisusarja
http://www.arvid.tv/micaj_storage/28C400A89D4F6673ED7D42DCC800612A/29/julksarja12.pdf

[YLE TK-Lehti] http://www.yle.fi/tekniikka/tklehti/

[YRTI] ”Tietoturvalliseen tietoyhteiskuntaan”, Yritysten tietoturvatietoisuus – työryhmän raportti, 21.2.2005.
http://www.mintc.fi/oliver/upl263-Ty%C3%B6ryhm%C3%A4n%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, jolla 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 käsiteltäessä 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 mielestänne kriittisimmät mobiiliin tietoliikenteeseen liittyvät protokollat? Miksi?

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

Mitkä käsityksenne mukaan käytössä olevista protokollista toimivat selkeimmin liitekohtina IP- ja GSM-maailman välillä?

Mitkä ovat mielestänne 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 käsityksenne 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 11. 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.

Kehitysvaihe	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
	Katsojan profilointitiedon 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
	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
	Katsoja profilointitiedon luottamuksellisuus.	kuluttaja, palveluntarjoaja, palveluoperaattori, verkko-operaattori
	Sisältöjen (kuten video, audio) käyttöoikeudet ja kopiointi.	kuluttaja, sisällönpaketoija, palveluntarjoaja, palveluoperaattori
	Uudenlaiset käyttötavat- ja tilanteet.	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
	Laitteiden ja ohjelmistojen yhteensopimattomuus.	kuluttaja, palveluntarjoaja, palvelunkehittäjä, palveluoperaattori, verkko-operaattori
	Virukset, haittaohjelmat.	kuluttaja, palveluntarjoaja, palvelunkehittäjä, palveluoperaattori, verkko-operaattori
	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

Liite C. Verkkolähteitä

Sisältöformaatteihin ja web-sisältöön liittyvistä haavoittuvaisuuksista:

http://www.kb.cert.org/vuls/id/388984

http://www.microsoft.com/technet/security/bulletin/MS04-028.mspx

http://secunia.com/advisories/14685/

http://www.eweek.com/article2/0,1759,1681412,00.asp

http://www.securityfocus.com/bid/11439/

http://www.uniras.gov.uk/niscc/docs/al-20030930-00565.html

http://www.cert.org/advisories/CA-2003-26.html

Java-alustan ja X.509 -toteutusten haavoittuvaisuuksista:

http://cellphones.engadget.com/entry/0535421442242743/

http://www.ficora.fi/suomi/tietoturva/varoitukset/varoitus-2004-82.htm

http://xforce.iss.net/xforce/xfdb/8399

http://java.sun.com/sfaq/chronology.html

http://ipsec-tools.sourceforge.net/x509sig.html

http://secunia.com/advisories/11948/

http://www.openssl.org/news/secadv_20030930.txt

Turvallisista ohjelmointikäytännöistä:

http://java.sun.com/security/seccodeguide.html

http://www.faqs.org/docs/Linux-HOWTO/Secure-Programs-HOWTO.html

Lisätietoja:

LUOTI-ohjelman internet-sivut
www.luoti.fi

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