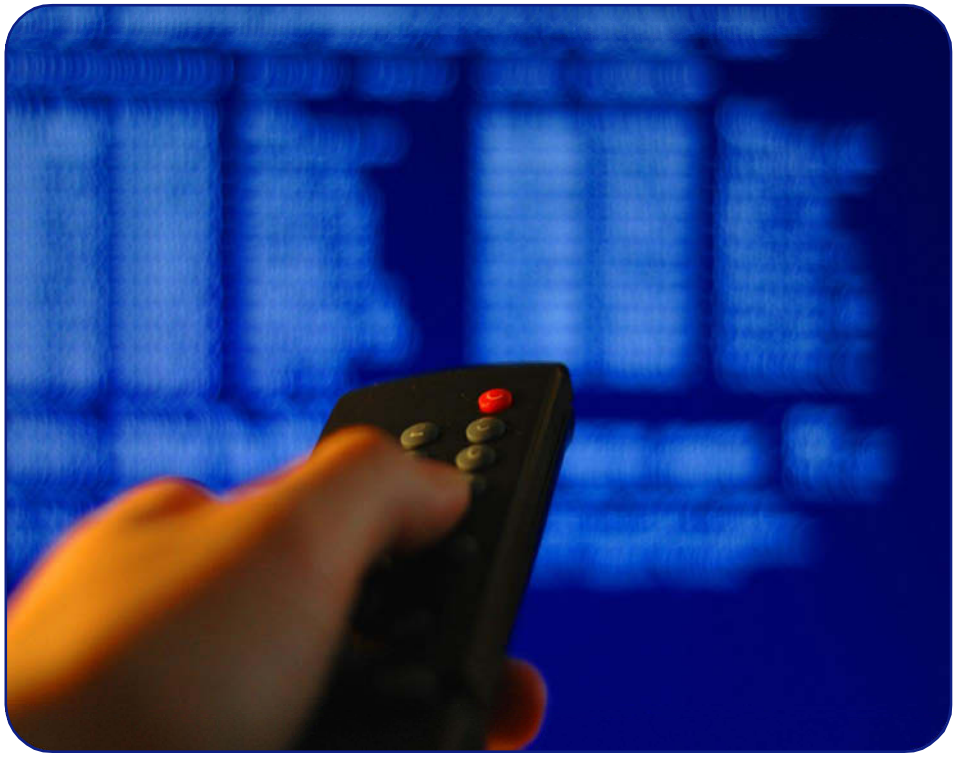
ESPOO 2005 VTT RESEARCH NOTES 2306



Jarkko Holappa, Pasi Ahonen, Juhani Eronen, Jorma Kajava, Tiina Kaksonen, Kati Karjalainen, Juha-Pekka Koivisto, Erno Kuusela, Ville Ollikainen, Mikko Rapeli, Anni Sademies & Reijo Savola

Information security threats and solutions in digital television

The service developer's perspective

VTT TIEDOTTEITA – RESEARCH NOTES 2306

Information security threats and solutions in digital television

The service developer's perspective

Jarkko Holappa, Pasi Ahonen, Juhani Eronen, Jorma Kajava,
Tiina Kaksonen, Kati Karjalainen, Juha-Pekka Koivisto,
Erno Kuusela, Ville Ollikainen, Mikko Rapeli,
Anni Sademies & Reijo Savola

VTT Electronics

ISBN 951–38–6733–1 (soft back ed.)
ISSN 1235–0605 (soft back ed.)

ISBN 951–38–6734–X (URL: http://www.vtt.fi/inf/pdf/)
ISSN 1455–0865 (URL: http://www.vtt.fi/inf/pdf/)

JULKAISIJA – UTGIVARE – PUBLISHER

VTT, Vuorimiehentie 5, PL 2000, 02044 VTT
puh. vaihde 020 722 111, faksi 020 722 4374

VTT, Bergsmansvägen 5, PB 2000, 02044 VTT
tel. växel 020 722 111, fax 020 722 4374

VTT Technical Research Centre of Finland, Vuorimiehentie 5, P.O.Box 2000, FI–02044 VTT, Finland
phone internat. +358 20 722 111, fax +358 20 722 4374

VTT Elektroniikka, Kaitoväylä 1, PL 1100, 90571 OULU
puh. vaihde 020 722 111, faksi 020 722 2320

VTT Elektronik, Kaitoväylä 1, PB 1100, 90571 ULEÅBORG
tel. växel 020 722 111, fax 020 722 2320

VTT Electronics, Kaitoväylä 1, P.O.Box 1100, FI–90571 OULU, Finland
phone internat. +358 20 722 111, fax +358 20 722 2320

Technical editing Anni Kääriäinen

Valopaino Oy, Helsinki 2005

Holappa, Jarkko, Ahonen, Pasi, Eronen, Juhani, Kajava, Jorma, Kaksonen, Tiina, Karjalainen, Kati, Koivisto, Juha-Pekka, Kuusela, Erno, Ollikainen, Ville, Rapeli, Mikko, Sademies, Anni & Savola, Reijo. Information security threats and solutions in digital television. The service developer's perspective [Digi-tv:n tietoturvauhkat ja -ratkaisut. Palvelunkehittäjän näkökulma. Hot och lösningar beträffande informationssäkerheten i digital-tv. Serviceutvecklarens perspektiv]. Espoo 2005. VTT Tiedotteita – Research Notes 2306. 81 p. + app. 4 p.

Keywords digital television, multimedia, data transfer, information security, authentication, user identification, privacy, terminals, intrusion detection, virus protection

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.

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.

Holappa, Jarkko, Ahonen, Pasi, Eronen, Juhani, Kajava, Jorma, Kaksonen, Tiina, Karjalainen, Kati, Koivisto, Juha-Pekka, Kuusela, Erno, Ollikainen, Ville, Rapeli, Mikko, Sademies, Anni & Savola, Reijo. Information security threats and solutions in digital television. The service developer's perspective [Digi-tv:n tietoturvauhkat ja -ratkaisut. Palvelunkehittäjän näkökulma. Hot och lösningar beträffande informationssäkerheten i digital-tv. Serviceutvecklarens perspektiv]. Espoo 2005. VTT Tiedotteita – Research Notes 2306. 81 s. + liitt. 4 s.

Avainsanat digital television, multimedia, data transfer, information security, authentication, user identification, privacy, terminals, intrusion detection, virus protection

Tiivistelmä

Tässä julkaisussa tarkastellaan digitaalisen television mukanaan tuomia tietoturvauhkia ja ratkaisuvaihtoehtoja palvelunkehittäjän näkökulmasta. Teknisten ratkaisujen lisäksi julkaisussa kiinnitetään huomiota palvelunkehitysprosessiin – siihen liittyvään arvo-verkkoon sekä palvelunkehityksen eri vaiheisiin ja niihin liittyviin uhkiin.

Tutkimusmenetelminä ovat olleet kirjallisuushaut, asiantuntijoiden näkemykset, yrityshaastattelut sekä laaja-alaiset kommentointikierrokset.

Digitaalinen konvergenssi tuo monipuolistuvia palveluita digi-tv-maailmaan. Vuoro-vaikutteiset 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, se saa tässä julkaisussa erityis-huomion. Sen mukanaan tuomia uhkia tarkastellaan palvelunkehittäjän näkökulmasta. MHP:n tietoturvaratkaisuja käsitellään ja niiden kypsyyttä ja soveltuvuutta arvioidaan muun muassa rakentumassa olevien allekirjoituskäytäntöjen osalta.

Holappa, Jarkko, Ahonen, Pasi, Eronen, Juhani, Kajava, Jorma, Kaksonen, Tiina, Karjalainen, Kati, Koivisto, Juha-Pekka, Kuusela, Erno, Ollikainen, Ville, Rapeli, Mikko, Sademies, Anni & Savola, Reijo. Information security threats and solutions in digital television. The service developer's perspective [Digi-tv:n tietoturvauhkat ja -ratkaisut. Palvelunkehittäjän näkökulma. Hot och lösningar beträffande informationssäkerheten i digital-tv. Serviceutvecklarens perspektiv]. Espoo 2005. VTT Tiedotteita – Research Notes 2306. 81 s. + app. 4 s.

Nyckelord digital television, multimedia, data transfer, information security, authentication, user identification, privacy, terminals, intrusion detection, virus protection

Abstrakt

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.

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.

Preface

This report, which addresses security threats and solutions in digital television, is based on our study done in the LUOTI programme (a Development Programme on Trust and Information Security in Electronic Services) of the Finnish Ministry of Transport and Communications, published in Finnish in June 2005. The study was conducted from the service developer's perspective.

The goal of the study was to increase awareness of information security threats connected with digital television and their possible solutions in different phases of the service development cycle. We focused on security solutions with the Multimedia Home Platform (MHP) and a return channel. We also aimed at providing a perspective on the role of information security in digital convergence, where several interdependent services are interconnected at the technical level.

The study was done by a group of network and information security researchers at VTT and the University of Oulu, managed by Mr. Jarkko Holappa of VTT. The research methods included industrial company interviews, literature surveys, experts' views and iterative analysis. The work was supervised by Mr. Kimmo Lehtosalo of Eera Finland Oy and Ms. Päivi Antikainen of the Finnish Ministry of Transport and Communication (MINTC). Their supervision and valuable comments have been crucial for the success of this study. The financial support of MINTC in the LUOTI programme is also gratefully acknowledged.

The authors wish to express their thanks for valuable comments by Mr. Esko Junnila, Mr. Petri Junnila, Ms. Tarja Rautio and Mr. Mika Sorsa of Digita Oy, Mr. Pekka Nykänen and Mr. Arto Saikanmäki of JP-Epstar Oy, Mr. Juha Perttula (Finnish Ministry of Transport and Communications), Mr. Kimmo Pöntiskoski and Carina Stenvall of MTV Oy, Mr. Seppo Kalli and Mr. Tommi Riikonen of Ortikon Interactive Oy, Mr. Mika Kanerva of Sofia Digital Oy, Mr. Jari Råman of the University of Lapland, Dr. Marko Helenius of the University of Tampere, Ms. Ritva Poikolainen (VTT) and Prof. Juha Röning (University of Oulu).

Oulu, Finland, September 1st, 2005

Reijo Savola

Network and Information Security Research Coordinator

VTT Technical Research Centre of Finland

Executive summary

As a service environment, digital television places very high requirements on the usability and information security solutions of services. The user group is highly heterogeneous, ranging from children to senior citizens. One cannot make many assumptions regarding the level of information technology know-how this group possesses. Usability of state-of-the-art terminal devices is not fully sufficient. For example, inconsistent practices in software updates of terminal devices, carried out other than within the program stream, do not increase the consumers' trust in the new media.

The expectations, advantages and benefits of digital television are achieved when a consumer has the courage to, is able to and wants to use the services. The most important factor is the customer's trust in the service and its provider. The enterprise's reputation, in addition to the costs, is important from the end user's perspective when selecting the service provider.

The main technical security concern in digital television is the terminal device – i.e. digital transceiver security in general when interactive services become more common. We have already been sensitized to threats connected with the reliability of digital transceivers, and there have even been some examples of terminal devices that have been damaged in Finland due to erroneous situations in the technology. The behaviour of many devices when receiving an erroneous signal is unpredictable – and this can be deemed to be due to insufficient reliability testing. From the service developer's point of view, the major threats to digital television networks are connected with the above-mentioned issues.

Some of the current Internet world threats are brought to the digital television environment because of interactivity enabled by the MHP standard profiles 2 (Interactive Services) and 3 (Internet Access). For the time being, the application environment has been restricted and strictly under the control of the digital television network operators and broadcasting channels because the applications come within the program signal. This is going to change due to the emergence of MHP version 1.1, enabling applications to be loaded via the return channel. In this situation the distribution channels get more complex and become more vulnerable. Because digital transceivers are Java-based, the strengths of Java are present in the networked environment. However, Java also introduces some weaknesses that a service developer should know about. The service developer should be able to exploit the security features of Java, like digital signatures of applications and programming interface support for encryption methods, but the vulnerabilities of Java implementations must still be taken into account.

Terminal devices with hard disks and the MHP standard version 1.1 introduce the security threat of content: one is able to store applications and connected data in the mass memory of the digital transceiver. A drawback to increased functionality is the threat that different kinds of malware, viruses and spyware, familiar from the PC world, establish themselves in the terminal devices. The vulnerabilities of content formats (audio and video) cause a threat to the functionality of a digital transceiver – e.g. a malformed picture file can cause a denial of service situation in the transceiver. A picture or audio file can contain also malicious code, being executed by the terminal device in an erroneous situation. From the service developer's perspective, the content delivered to the viewer is material under copyright, which should be protected from copying and other kinds of malpractices. Unauthorised use of content, e.g. in a situation when the paid usage time of the service has already expired, is a threat to the business of a service developer.

The trend for digital convergence is also present in digital television – mainly as convergence of the return channel with other channels of digital content distribution. The services are integrated with different kinds of systems and networks, resulting in a situation where there are environments that have been developed using different types of practices and quality standards. From the information security management point of view, the interconnection of the different systems and understanding the whole environment are very challenging, and have not yet been solved.

The subscription and payment processes of electronic services should be as easy to use as possible and familiar to the users. At the same time as interactive television is becoming more common, the passive viewer is becoming an active consumer of services, and the producer is becoming an entrepreneur. The rules of commerce should be agreed between the stakeholders, despite the devices involved.

Because of existing threat scenarios, there has been an ambition to influence the security of services during the standardisation phase of the technologies. The MHP platform offers many information security solutions, partly inherent from Java. The applications can be authenticated and authorised using digital certificates – and an application without a signature is treated as unreliable and cannot, for example, open a return channel. Certificate policy issues still remain open. The MHP standard defines a Public Key Infrastructure with root certificates, but most of the terminal devices currently on sale do not support it. Furthermore, national certificate conventions are still about to form, although there have been some experiments.

As in other software and product development the functional processes of the digital television service developer are in focus in order to develop a quality product. Information security should be taken into account in the design right from the

beginning. The goals of service concept should be reviewed from the security point of view and one should investigate what requirements should be set for confidentiality in order to achieve the end users' trust in the service. In addition to the product under development, information security should be managed internally in the company's practices and processes, including subcontractors' processes. The value net of the service, and the different roles and responsibilities of each stakeholder should be identified. The personnel should be trained to achieve security awareness and knowledge of security practices in order to make it possible for them to work in a secure way in their own areas of responsibility. The product should be tested extensively before it is delivered to the customer. Conformance testing of MHP applications carried out for MHP devices would increase the end-user quality of service.

Information security means different kinds of issues for different stakeholders – the emphasis on threats varies in severity and solutions across different parts of the value net. For the content producer, the most important threats include unauthorised use and distribution of programs or other content, and for the network operator, erroneous program content causing trouble in viewers' devices. For the viewer, threat scenarios include privacy problems and risks of electronic commerce like theft of credit card information. End user privacy threats in a service provider's products decrease the trust in this party and actually become a threat to the continuity of the service provider's business. Information security is a multifaceted issue, including legal issues and human behaviour in addition to the technical solutions – all dimensions of information security should be taken into account in the service development process.

Contents

Abbreviations and terminology

802.11	WLAN standard family of IEEE
API	Application Programming Interface
BT	Bluetooth. A wireless short-range telecommunication technology (10 m).
CA	Certification Authority
CERT	Computer Emergency Response Team. CERT-FI is a Finnish national CERT team (part of the Viestintävirasto, Finnish Communications Regulatory Authority) that carries out security incident prevention, detection, solution and dissemination of security threats.
CPU	Central Processing Unit
CRL	Certificate Revocation List
DNS	Domain Name System
DRM	Digital Rights Management. A method for controlling the distribution of electronic content.
DSM-CC	Digital Storage Media – Command and Control. A technology enabling transmission of applications as a part of DVB program stream.
DVB (-T/C/S/H)	Digital Video Broadcasting. A European digital television standard, incorporating different transmission network technologies: - C: Cable - S: Satellite - T: Terrestrial - H: Handheld.
EPG	Electronic Program Guide. An application that is usually loaded via the transmission stream, showing information about programs. Typically, the terminal devices also contain a program guide implemented by the device manufacturer.
FTP	File Transfer Protocol. A file transfer protocol.

FW	Firewall. A firewall is a software or device that controls traffic coming into a device and leaving from it.
H.263	A video compression standard by ITU-T
H.264	A video compression standardised by ITU-T and ISO/IEC MPEG group in co-operation
HST	Electronic Identification of a Person (In Finnish *Henkilön Sähköinen Tunnistaminen*). A Finnish chip-based identity certificate.
html	HyperText Markup Language
http	HyperText Transfer Protocol
HW	Hardware
ICT	Information and Communications Technology
ID	Identity
IDS	Intrusion Detection System
IP	Internet Protocol. IP is responsible for the addresses of mobile devices and packet routing in the network. IPv4 and IPv6 are different versions of IP.
IPSec	IP security. A collection of IP security protocols.
IRT	Incident Response Team
ISDN	Integrated Services Digital Network. A circuit-switched digital phone network system.
ISO	International Organization for Standardization
ITU	International Telecommunications Union
LAN	Local Area Network
LUOTI	Development Programme on Trust and Information Security in Electronic Services (In Finnish *Luottamus ja tietoturva sähköisissä palveluissa*) of Finnish Ministry of Transport and Communication

MHP	Multimedia Home Platform. An open application development interface for interactive applications of digital television.
MINTC	Ministry of Transport and Communications of Finland
MPEG	Moving Pictures Expert Group of ISO/IEC. A group of moving picture standards. MPEG2 is used in the digital television world. MPEG1 audio layer 1 and 2 are used for voice compression.
MPLS	Multiprotocol Label Switching
NAT	Network Address Translation. Translation of an IP address of a network into an IP address of another network.
NNTP	Network News Transfer Protocol. A protocol for distribution, request, fetching and sending of news articles through a secure network connection.
Object carousel	A system that enables the sending of applications, the files they need and software updates within the digital television program signal.
Return channel	A technical solution that enables the viewer to send service provider information and fetch applications and other content. At this moment the return channel in Finland is typically implemented using a modem connection. In the future the return channel will be a broadband Internet connection (after the introduction to the market of terminal devices that support it).
PAN	Personal Area Network, e.g. Bluetooth
PDA	Personal Digital Assistant
PKI	Public Key Infrastructure
POP3	Post Office Protocol version 3. An email protocol.
PSTN	Public Switched Telephone Network
PVR	Personal Video Recorder. A recording functionality of program stream in a terminal device implemented using e.g. a hard disk.
RA	Registration Authority. An authority that authenticates the identity of a person who applies a certificate according to the certification policy.
RAM	Random Access Memory

ROM	Read Only Memory
S/MIME	Secure Multi-Purpose Internet Mail Extensions. A protocol meant for email protection.
SANS	SysAdmin Audit Network Security Institute
SATU	Electronic Identifier in HST (In Finnish *Sähköinen henkilöllisyyden tunnus*)
SHA	Secure Hash Algorithm. A checksum algorithm that generates a fixed-length checksum of input. The input cannot be revealed using the checksum.
SSID	Service Side Identifier. An identifier used for connection to a WLAN server.
SSL	Secure Sockets Layer. An encryption protocol.
TCP	Transmission Control Protocol. TCP is responsible for communication connection between two terminal devices, packet structuring and retransmission of lost packets.
TLS	Transport Layer Security. See SSL.
UDP	User Datagram Protocol. UDP is responsible for communication connection. UDP is lighter than TCP and does not structure or retransmit lost packets.
USB	Universal Serial Bus. A serial bus architecture for connection of peripheral devices.
VAHTI	Finnish Government Information Security Management Board (*Valtionhallinnon tietoturvallisuuden johtoryhmä*)
Value net	A method to describe a complex business field in a more versatile way than using conventional value chains. In addition to a horizontal dimension, a value net has a vertical dimension as well. Deviating from value chains, value nets can incorporate various stakeholders operating in the same business field.
VRK	Finland's Population Register Centre (In Finnish *Väestörekisterikeskus*)
WEP	Wired Equivalent Privacy. An outdated encryption system in WLAN networks.

WiFi	Wireless Fidelity. A WLAN system conformable to 802.11.
WLAN	Wireless Local Area Network
WWW	World Wide Web
X.509	ITU's recommendations for electronic certificates and certificate revocation lists
XHTML	Extensible Hypertext Markup Language
XML	eXtensible Markup Language

1. Background to the research

1.1 Goals of the study

Digitalisation of the television network is rapidly forging ahead in Finland. On March 4th, 2004, the Finnish Council of State made a decision to convert all television channels to digital by August 31st, 2007. Terrestrial digital television distribution computationally covers about 94 % of the Finnish population already, and, by the end of 2005, at the completion of the third phase of digitalisation, it is anticipated that 99.9 % of the population will be covered [Digi-tv]. According to the study by Finnpanel, there were digital transceivers in more than half a million homes in January 2005 – i.e. 22 % of households were equipped with a digital transceiver meant either for antenna, cable or satellite reception. However, only about five per cent of them supported the Multimedia Home Platfrom (MHP) standard that enables the use of interactive services.

Information security issues in new services and technologies are very challenging. From the service developer's perspective, the current digital television network is rather secure because purely interactive services (i.e. services that require a return channel) do not exist very much, partly because of the weak availability of the terminal devices supporting them. The situation is certainly going to change in the future when the prices of terminal devices supporting the MHP standard come down and the selection gets larger.

The value net of the digital television industry is broad and contains a lot of stakeholders in different roles. For example, responsibility issues in the case of information security violations are very problematic, and clear directives concerning them are non-existent. Broadcasting is quite strictly regulated in Finland and in the whole of the European Union. However, interdependencies in the value net and the nature of new services contribute to a situation in which the stakeholders of the value net do not all the regulations and directives connected with the provided services and content.

In the future, mobile devices (mobile phone, PDA), digital televisions and computers could be seen as different terminal devices for the same service. For digital television, this would mean certain parts of the devices should be open to the Internet, and the role of Internet protocols would become more important. Increased security risks are a drawback to this trend – the threat scenarios of the Internet world will move over to the digital television world unless the threats are identified and the service development phase takes the information security requirements into account.

The goal of this study is to analyse information security threats due to digital television and, in particular, MHP applications. The study aims at finding technical and service development process-oriented solutions as countermeasures to the threats. In addition,

the study introduces the digital television technologies, threats and special characteristics of the MHP service development process.

1.2 Definitions of information security

The main objective of information security management is to implement a good and efficient information management way-of-conduct and to create a sufficient basic level of security. Information security management is needed protection from threats and damage caused by hardware and software faults, and natural events, as well as deliberate, negligent and accidental acts. Information security is based on the following three basic concepts:

- *Confidentiality* – information access and disclosure are limited to the set of authorised users, and access by or disclosure to unauthorised users are prevented.
- *Integrity* – information and information resources are trustworthy, correct, and up to date, and are not changed or destroyed by hardware or software faults, natural events or unauthorised acts.
- *Availability* – information and services connected to them are available to authorised users.

In addition, the following security functions are essential for information security management:

- detection, prevention and avoidance of malpractices
- countermeasures, survivability and intimidation.

Controls can be created in order to implement security functions in the information system: policy, method, practice, device or programmed mechanism.

Some definitions:

Information security means administrative and technical actions to ensure that information can be accessed only by authorised persons, information cannot be changed by unauthorised persons and information and information systems are available to authorised persons. (Finnish Act on the Protection of Privacy in Electronic Communications, *Sähköisen viestinnän tietosuojalaki*, 16.6.2004/516.)

Information security management means information, service, system and communications protection against risks targeted at them with applicable actions. Information security management is broader concept than technical security of

information and communication technologies. (Information security awareness working group of industrial companies of Finnish national information security strategy, *Kansalliseen tietoturvallisuusstrategiaan liittyvä yritysten tietoturvatietoisuus-työryhmä* [YRTI].)

Privacy means protection of a person's privacy in the management of personal information. For this purpose personal information should be protected from unauthorised use and use damaging a person. (Finnish Communications Regulatory Authority, *Viestintävirasto.*)

1.3 On industrial interviews

The state of the art of digital television services and the service developer's perspective were analysed in the study by interviewing actors in the field in Finland and elsewhere. In addition, the goals of interviews were to investigate the value net of the field of digital television, and the threats to its different parts seen from the perspective of different actors, and identify the special characteristics of the service development process of digital television services. Digital television programme production can be divided into five main phases: programme production, service production, packaging, distribution and consumption. The questionnaire presented in Appendix A was used as the basis for the interviews. This section summarizes the perspectives brought out in the interviews.

During the interviews it was noticed that it is essential to analyse the information security issues connected with each phase, their potential problems, threats and solutions.

Currently, the main security concern in the digital television field is the security of the terminal devices, the digital transceivers. The terminal devices are quite vulnerable to erroneous data stream. An example of this vulnerability was seen in the spring of 2004 when an erroneous program stream was damaging terminal devices in Finland [Tietoviikko 2004]. As MHP applications become more common, the security of the terminal devices is becoming more important. The issues to be solved include authentication of the application, protection of the terminal device (anti-virus software, firewalls) and viewer privacy issues. A general view is that with regard to information security, the buyer of a terminal device is dependent on the device manufacturer because the technical solutions are, almost without exception, device-oriented, despite the fact that there are standardised specifications for the technical solutions. These specifications are rather loose, enabling the same functionality to be developed in various different ways. The manufacturers end up with more exotic solutions, especially when there is a need to make trade-offs due to the restrictions of memory consumption and computational power.

In general, the threats can be targeted at program content, terminal devices and consumers' privacy. Especially harmful for the trustworthiness of television broadcasting are malpractices connected with the content – e.g. a situation in which the actual content is replaced by forged content or the terminal device is damaged by a program.

In many cases the attacks targeted at terminal devices should be able to deal with implementation details in order to succeed in all terminal devices. On the other hand, different manufacturers' devices often use the same software components. For example, the Java platform of MHP and the operating system of the digital transceiver are such large software entities that a terminal device manufacturer often licenses them from third parties or orders production licensing for the whole device or software architecture from outside. Historically, Java implementations have included many vulnerabilities that enable the Java program to gain broader access privileges in the target system than is authorised, potentially offering access to the underlying operating system and device.

Attacks that aim at breaking a certain manufacturer's Java implementation can be considered more probable than attacks that target all or many devices. For the manufacturer, the possibility of these kinds of attacks contributes to a remarkable financial risk. Breaking certain terminal devices is a marginal problem and an attack targeted at all devices is not so probable due to the diversity of devices. From the end user's perspective, the attacks aimed at certain manufacturer's devices do not cause a remarkable financial or political risk. Threats targeted at consumer security, such as spam and privacy violations are more critical for the consumers.

Nowadays the threats to the system do not address large groups of consumers since the number of true interactive services is still relatively small. However, as interactivity in digital television increases, the information security issues focus especially on the terminal device and return channel. In particular, the end users' position regarding information security should be given more attention as interactivity becomes more common. For the purposes of the security analysis, the most essential standard in the field is MHP. Issues concerning MHP are analysed in Chapter 3.

According to the interviews, digital television broadcasting was considered close co-operation between some central actors, but the need for co-operation co-ordination was seen during the process of the actor net getting larger and larger. In the near future the group of actors is probably going to change due to the number of services getting bigger and the trend for increasing interactivity in the digital television broadcasting field. So far the markets have been rather limited, and, because of that, the R&D effort on information security issues has been minor.

Risk management is a central activity in service development. A thorough analysis of risks is needed in connection with an analysis of which of them needs actions. It is not possible to protect against all risks, neither it is financially reasonable. Reasonable risk management is to involve an information security specialist in the service development at the design phase.

It was discovered in the interviews that at present there are no remarkable deficiencies in the Finnish legislation concerning information security in the world of digital television. Due to this fact, an analysis of legal issues was not included in the scope of this study. However, we can note that in connection with digital television reception the Privacy Directive of Electronic Communications prohibits the listening to and transfer of information about such telecommunications information as channel selection, time information, information about commercials viewed or games played. In addition, the developers of electronic services should take particular account of the privacy legislation, handled in Section 4.2.4, and the regulations concerning electronic commerce.

2. Brief technological overview

2.1 A brief description of the internet and related protocols

Some of the biggest advantages of the Internet Protocol (IP) are flexibility, simplicity and the possibility of using different kinds of physical transport media. Furthermore, the protocol's routing model strengthens robustness. In the telecommunication domain IP-based architecture has been in wide use since beginning of the 1990s.

The Internet is a group of matched protocols, thus connecting devices to the Internet means merely connecting it to a network using the IP protocol in transport layers together with other devices in the same network. As a physical transport media, almost any connection will do, for example ISDN, ATM, UMTS or GPRS. The device that is connected to the Internet receives an IP address, which does not need to be global although it is part of the original philosophy.

TCP and UDP protocols are used for data transmission in IP networks, which is the basis of the TCP/IP protocol family. Various applications can be built on top of the TCP/IP protocol suite and IP works above a variety of networks. This has been an important reason for the popularity of the protocol: IP-based techniques can be utilized using the existing infrastructure while moving to new transport techniques is possible without an extensive need for a change in the networks and applications. It is common to almost all IP networks, where traditional techniques, i.e. PSTN networks, are moving towards IP-based solutions.

From the technical point of view, many kinds of protocols implementing various services belong to the TCP/IP protocol suite. These services include routing techniques, network management, directory services, authentication, management of network devices, file transport, e-mail exchange, delivery of web content, quality of service management, IP telephony management, and so on. These protocols are seldom visible parts of the services but act as important supporting resources for services.

From the user's point of view, the most important services in the Internet are www browsing and communication services, such as e-mail, newsgroups and instant messaging. The proportion of www browsing is clearly over-emphasized; many times, users and the media do not make a difference between the Internet and www. Web browsers handle many kinds of passive and active content, and banking and e-commerce services as well as public services are moving strongly towards the Internet. It can be assumed that the significance of the Internet is still growing. More and more new services are being piloted on the Internet, e.g. elections via the Internet. IP telephony and different kinds of non-interactive video and audio services, along with multicast and quality-of-service techniques, are growing in popularity as well.

2.2 A brief description of digital television systems

2.2.1 Transmission network and related technologies

Digital television in Finland is based on the DVB standards [DVB]. Terrestrial networks use the DVB-T standard, cable networks utilize DVB-C and satellite broadcasts are based on the DVB-S standard. Mobile handheld devices can receive digital television broadcasts using the DVB-H standard, which is based on DVB-T. The above-mentioned standards mainly differ from each other in the modulation techniques that are optimized to the appropriate transport path, and end-user equipment differs correspondingly.

For the time being, data stream in the digital television network is mainly transport of audio and video using DVB techniques in a dedicated network from broadcaster to receivers. In addition to audio and video it is possible to transfer data and produce data services. Figure 1 presents a block diagram of a digital television broadcast network that does not assume any transport path (terrestrial, cable or satellite). The Figure also displays information security threats directed at different parts of the network. The service developer in this context is comprised of the roles of content provider, service developer and **integrator**. Audio and video is encoded in the broadcast system and combined into one MPEG2-bitstream in a multiplexer [MPEG2]. One bit stream is known as **multiplex**. In addition to audio, video and signaling information, it is possible to transfer data using IP-based services [Södergård 1999], [FICORA].

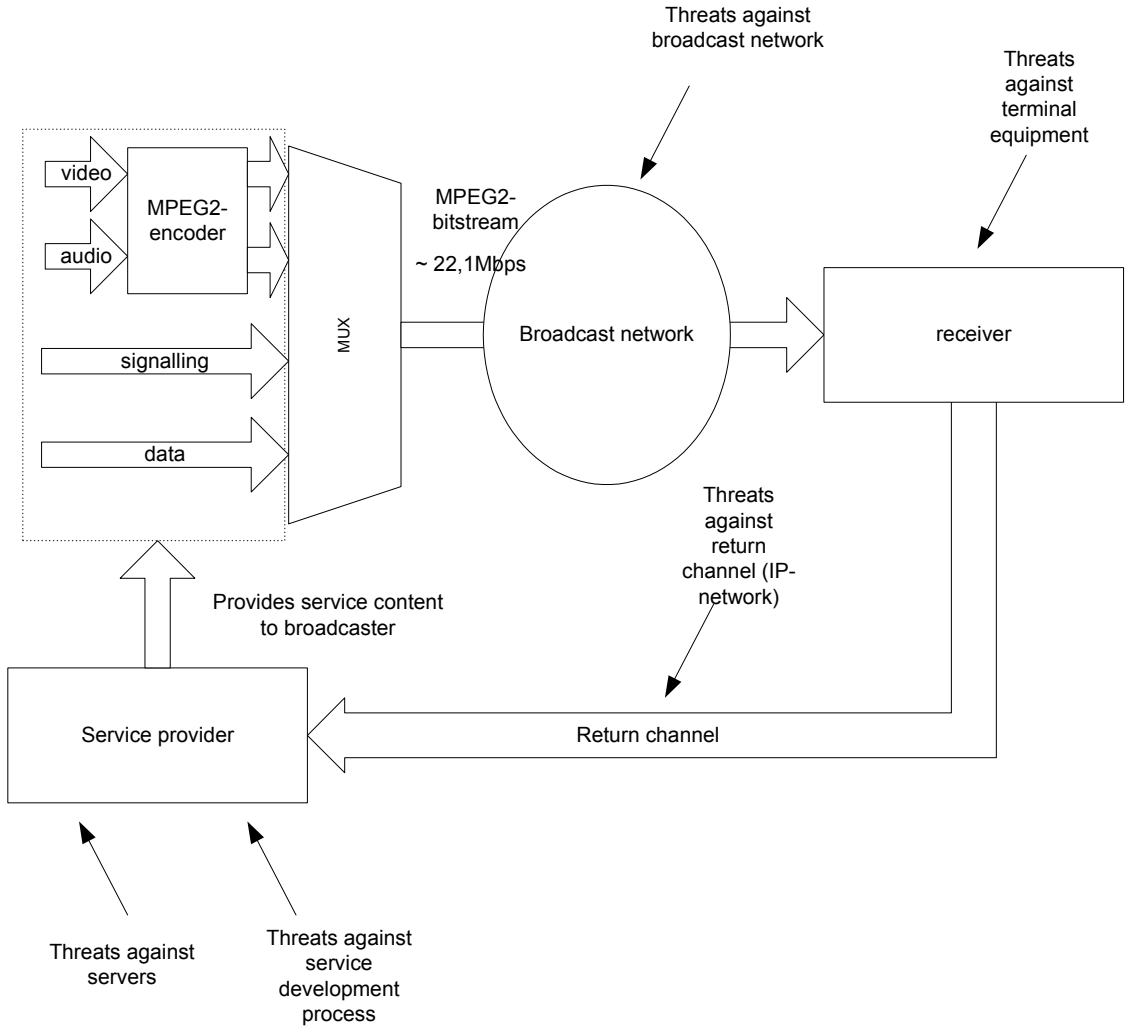


Figure 1. Digital distribution network and threats targeting its different parts.

Next, we present a brief summary of the DVB standards and main differences. Many parameters are associated with all forms of DVB. These parameters are set according to the receiving requirements so that the most suitable compromise between bandwidth and quality of broadcast is achieved.

DVB-S

DVB-S is designed to work in all bandwidths of satellite broadcast. It is the oldest of the DVB standards and the most widely used. All data is in fixed-size DVB-TS packets and DVB-S utilizes the QPSK modulation technique.

DVB-T

DVB-T is based on MPEG2-packets and broadcasts use COFDM modulation. DVB-T is well optimized to be able to broadcast in different kinds of environments, which makes it very versatile.

DVB-C

DVB-C is based on DVB-S and uses QAM modulation. Internal error correction in packets is not needed.

DVB-H

DVB-H is a terrestrial digital television standard that is based on DVB-T, being backward compatible with it. The most notable difference is the lower power consumption and better support for a mobile receiver. DVB-H uses the DVB-T network for IP traffic transmission. This is known as IP Datacasting. DVB-H compatible receivers, such as mobile telephones and PDAs, are able to receive digital television broadcasts using the terrestrial network (DVB-T), so the signal transmission does not use mobile networks at all. DVB-H does not commit to any video compression techniques. Typically, H263 and H.264 codecs (MPEG4) are used. The channel bundle parameters are set so that it is easy to receive a signal on a mobile terminal. The size of the *channel bundle* is 10Mbit/s; one channel requires 256kbit/s bandwidth. As an application environment, DVB-H is similar to MHP, although, the restrictions of the terminal, such as size and resolution of display, bring their own special characteristics to service development. Touch displays in PDAs also provide new possibilities for user interface development. A mobile phone, as end-user equipment, is more personal than television and user experience is very different compared to that of television. DVB-H reception can be implemented using technologies familiar from today's high-end mobile terminals.

DVB-IP (IPTV)

IPTV technology is based on the use of the IP protocol in both broadcast of content and return channel. The receiver must comply with the DVB-IP standard. It requires 2–5Mbit/s bandwidth to broadcast one channel, which basically means a requirement of at least an 8Mbit/s broadband connection. Broadband return channels enable subscriber-based services, such as Video-On-Demand.

2.2.2 Multimedia Home Platform (MHP)

In 1998 the DVB organization started to develop a standard for developing value-added services. This produced a Multimedia Home Platform (MHP), which is also used in Finland as a technology to implement interactive services. At the moment, MHP-based services are broadcast in Sweden, Germany, Italy and Spain, of which Italy is considered the frontrunner in the introduction of MHP services. MHP pilot projects and a declaration of supporting MHP are being made in almost every European country. (See Figure 2.)

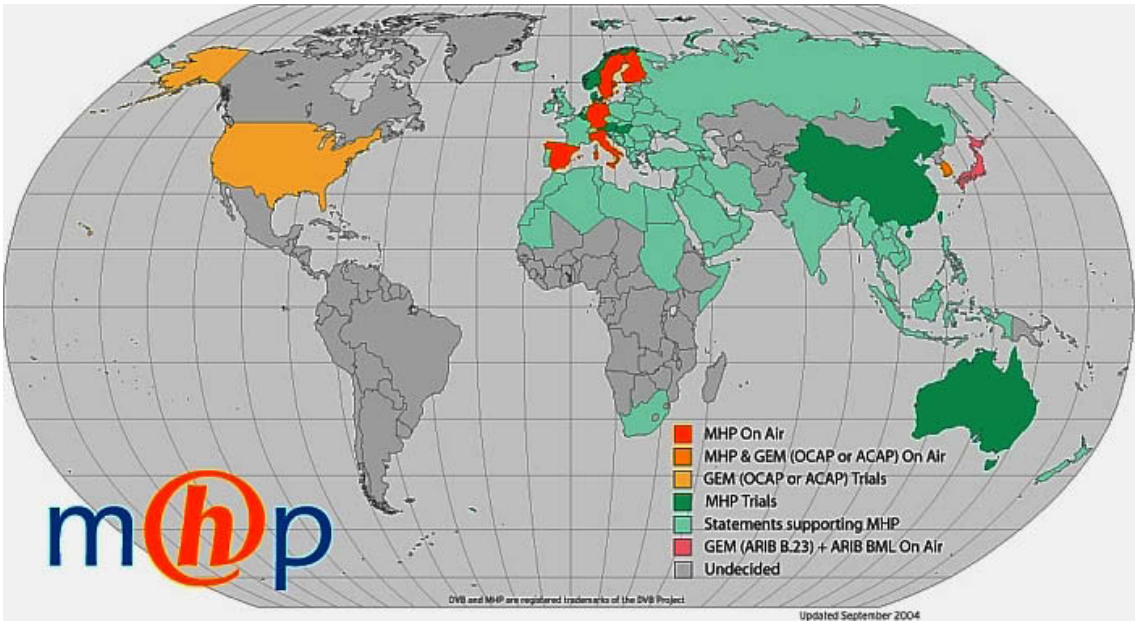


Figure 2. MHP penetration (www.mhp.org).

MHP is an open standard and defines a general purpose interface between interactive applications and receivers. The applications are written in Java programming language and XHTML markup-language, in which case a Java-based browser is transported in the DVB stream. This enables platform independency at both the hardware and operating system level. The MHP architecture is defined on three levels, as described in Table 1. [MHP.]

Table 1. Parts of the MHP architecture.

Layer	**Task**
Resources	Demultiplexing of MPEG-formed signal, processing of audio and video signal, I/O devices, CPU, memory and graphics resources.
System software	Uses resources in order to offer a higher level view from the platform to the applications.
Applications	MHP implementations include application management (“navigator”), which directs the MHP platform and applications run on it.

The MHP standard has three different kinds of profiles, as presented in Figure 3.

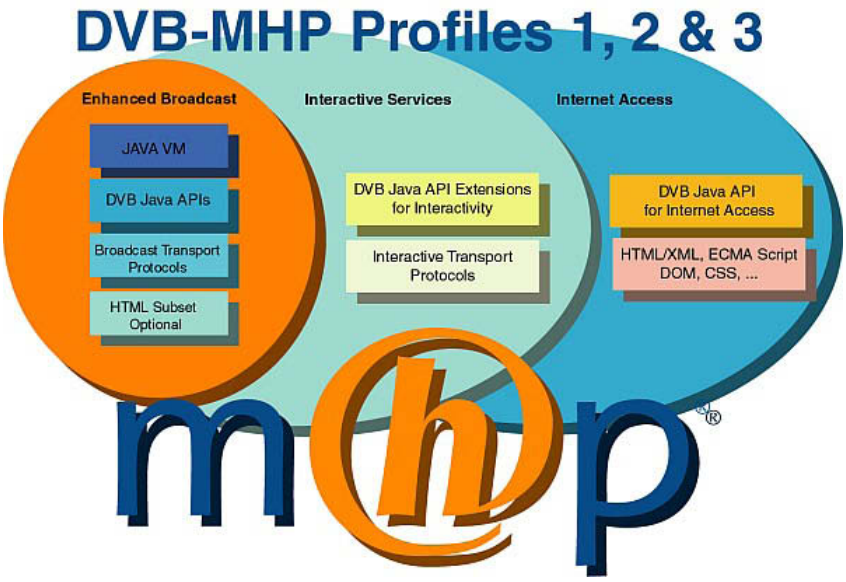


Figure 3. MHP profiles (www.mhp.org).

The profiles are defined to ease implementation of the standard. Each profile denotes the application area and the capabilities of the receiver. The three profiles of the MHP are:

1. **Enhanced broadcast**

   The profile was made to comply with many existing middleware systems and applications. This profile represents the most restricted receivers without a return channel.

2. **Interactive services**

   This profile includes receivers that have return channel capabilities. The most notable difference compared with profile 1 is that in this profile it is possible to download applications from the DVB stream. Interactive behaviour is also supported in the application programming interfaces.

   The Internet Access Profile defines the local browser application to the terminal, as well as the interface with which the browser can be controlled.

3. **Internet access**

   The most advanced profile in the MHP standard. The receiver is more advanced than in the previous profiles, e.g. it has more memory. The profile concentrates on using Internet content with a digital television receiver. The Internet access profile defines a resident browser application to the receiver, as well as the interface for management of the browser.

Internet use of an MHP device hardly ever replaces a PC. Resource limitations, restrictions of user interface and possible restrictions related to the return channel, for example regarding used protocols, delimit the Internet content to rather simple email and net surfing types of applications – e.g. network services offered by banks.

From the end user's point of view, digital television's interactive features are based on the MHP1.0.2 standard. MHP1.1 is a newer standard that enables downloading of the applications via a return channel, whereas MHP1.0.2 enables downloading only via the DVB stream.

The core of MHP is based on the DVB-J-platform, which includes a virtual machine according to the Java Virtual Machine Specification definition made by Sun Microsystems, as well as an application programming interface (API) through which the MHP applications use the resources offered by the platform and the services of the system-level software. Along with MHP1.1 comes new information security threats, which are mostly caused by the use of the return channel, but, so far, there are no MHP1.1-compliant receivers on the market.

The MHP platform and its programming interfaces are based on Java, thus the developer must take Java's security features into account as well as its restrictions. Java is object-oriented programming language and from the beginning was designed for the development of networked applications and to provide a secure way of downloading applications over insecure networks. Nonetheless, this has not fully come true in Java implementations; vulnerabilities that can cause applications to break its security policy come up from time to time. The main components of the Java are byte code and virtual machine, where the code is executed. Java's virtual machine hides the operating system and hardware from the Java application, so it makes sense to talk about Java as a platform rather than a programming language. For networked applications, Java is a better option than the traditional platforms based on C-programming language because Java's inbuilt security model has been developed since the first version of Java. Java's application programming interfaces provide support for cryptographic algorithms and public key infrastructure, including a certificate-based X.509 authentication framework that is also utilized in the MHP platform to ensure the origin of the application.

Other X.509 implementations have had security vulnerabilities that enable breaking the authentication framework.

Figure 4 depicts Java's security model, which provides variable rights depending on the application's security policy and origin. Based on these, trust in the application is evaluated and how much of the application gets rights in the system. At one end is an application with 100 % trust, whose execution is not limited in any way, and at the other end is a fully untrusted application, whose execution is not permitted at all. Java uses

the term ’sandbox’ when speaking of restricting an application’s execution rights in the system. It is possible to define different kinds of sandboxes for different kinds of service developers (device manufacturer, operator, third party).

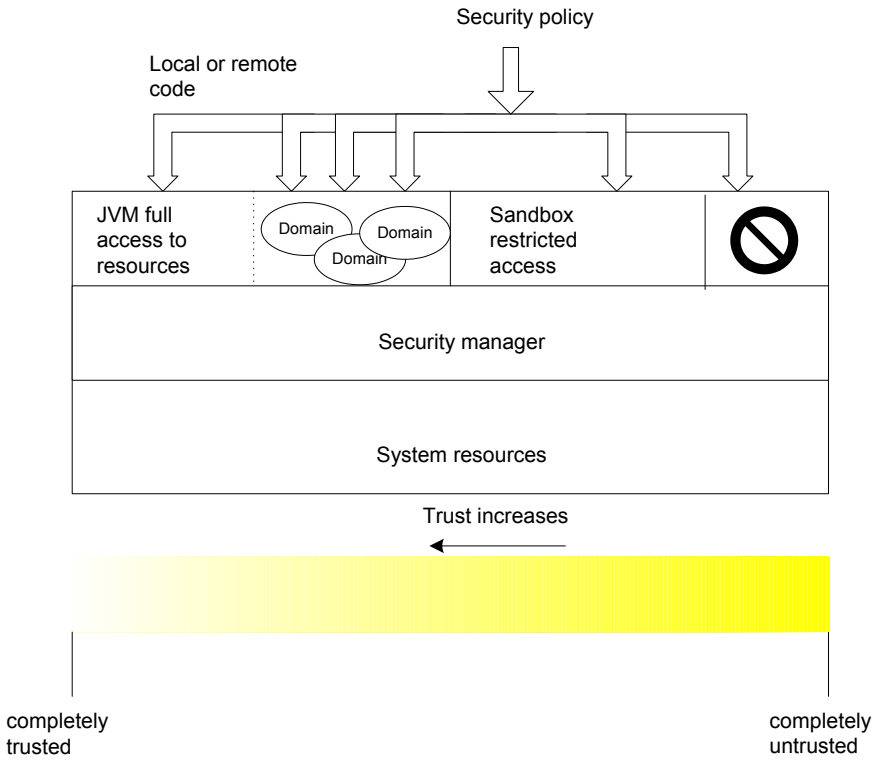


Figure 4. Java information security model.

Java’s security policy is implemented using a permission request file. Figure 5 describes one permission file as an example [MHP]. MHP uses both Java’s own security policies and policies defined by MHP. Implementation of these varies from one receiver to another. The MHP standard has intentionally left which authorization requests are handled by the user undefined. In other words, this leaves the definition of a security policy to the market, the consumers and the regulating authorities.

As at May 2005 there are no permission request files in use in Finland. An application gets all rights inside the virtual machine, although there can be restrictions made by the device manufacturer which may be more restrictive than Java’s security model.

```
<?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 2
    </signature>
    <certchainfileid>3</certchainfileid>
  </persistentfilecredential>

</permissionrequestfile>
```

Figure 5. Java Permission Request file.

From the service developer's point of view, Java provides the same security tools and solutions independent of the target hardware if the virtual machine is compliant with the standard. Table 2 gives examples of MHP services implemented in Finland that are broadcast on a terrestrial or cable network.

Table 2. MHP services in Finland 2.5.2005 (sources: Yleisradio, MTV3, Ortikon Interactive, Sofia Digital and Digita, www.digitv.fi).

News service	**News (domestic, foreign, sports)**	• Yle super teletxt • Uutisrulla (Yle) • MTV3 Text channel (MTV3, MTV3+, Subtv) • FST news (Yle) • Savon Sanomat • Netlari • Kaleva • Olet.info • Radio 957
	Weather reports	• Yle super teletext • MTV3 Text channel (MTV3, MTV3+, Subtv)
	Economy news	• Kauppalehti/MTV3 Text channel (MTV3, MTV3 + Subtv)
Program guides	**Latest movies and series**	• MTV3 Teletext(MTV3, MTV3 + Subtv) • Nelonen super teletext (Nelonen, Nelonen+)
	Near future program information	• Program guide (all digital TV channels, finnish and swedish)
Entertainment	**Games**	• Muistipeli (Yle) • NE-spelet (Yle) • Lotto (in test use) (MTV3, MTV3 + Subtv) • OBlox • Klondike
	Program specific services	• G5, Käenpesä, Joka kodin asuntomarkkinat, T.i.l.a., Ruokala.tv, SM-liiga Hockey Night (MTV3) • Food: Impossible, Anarkistit, SubLeffat (Subtv)
Others	**Community services**	• Eduskuntafakta (Yle) • Post digital TV service (send an electronic Christmas card with Post digital TV service)
	Banking services	• Osuuspankki Digital TV service (MTV3, MTV3 + Subtv)
	Messaging	• Email and chat services • Lupiini Deitti • Sooda-Portal

2.2.3 Terminal devices

The most important factor in interactive service popularization is that terminals, in other words set-top boxes, become more general. At the moment there is a chicken and egg situation concerning interactive MHP1.1.services: MHP1.1-compatible terminals have not become popular because services do not yet exist, and, on the other hand, new services are not being effectively developed because the terminals are not yet on the market. The first set-top boxes offered basic features for receiving digital tv broadcasts, and models equipped with a card reader also enabled receiving pay channels. The terminals of the second development stage can be counted as set-top boxes with hard

drives that enable recording programs (PVR, Personal Video Recorder) and so-called time-shifting, in which the viewer interrupts the tv programme for a phone call, for example, and, after the phone call, continues viewing from where he was interrupted. The current terminals that back up the MHP standard do not include a hard drive. The third development generation brings along a genuine interactive set-top box – in other words, a device according to the MHP1.1 standard. This diversifies the service offering and pay content. Convergence with the current Internet world diminishes with the interactive channel. This chapter presents NorDig, the most important terminal definition for the Finnish market, NorDig, and the Italian DGTVi D-Book definition.

NorDig

The NorDig coalition was founded in order to create a Nordic receiver definition for digital television using the DVB standards as a base. The purpose of this was to ease the transfer of consumers to digital television use and to enable receiving DVB transmissions with the same receiver, independent of country or media. For content producers, the NorDig definition gives knowledge of what kind of signal the receivers can receive and how the services and content they produce shows in them. The Nordig-Unified definition presents four profiles (Figure 6). In addition to the basic functionality, there are three profiles in the definition that correspond to the profiles of the MHP standard.

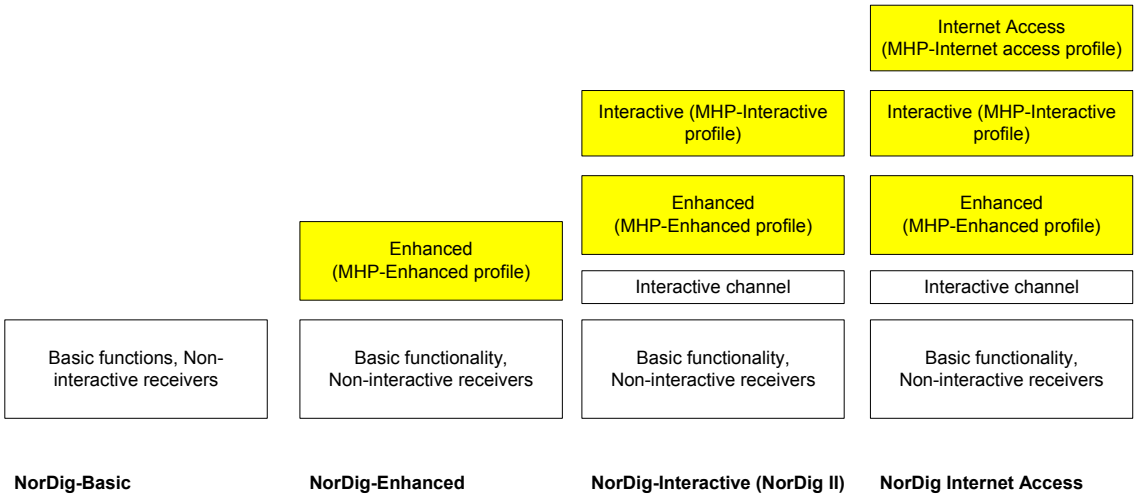


Figure 6. NorDig definition profiles.

Figure 7 presents the architecture of a NorDig terminal. A NorDig receiver has at least one built-in tuner for a cable, satellite or overground system. NorDig also has a Common Interface connection, with which a separate satellite or cable tuner can be coupled with the receiver, beside the overground tuner. With Common Interface a separate CA module (Conditional Access) can be coupled, which enables following several service providers' programs using different encryption systems.

All NorDig receivers include a smart card reader, with which one can access both encrypted and other services, such as betting and banking services that require authentication. The return channel techniques that are enlisted in the NorDig definition have been presented in Chapter 2.2.4.1 [YLE TK-lehti], [NorDig].

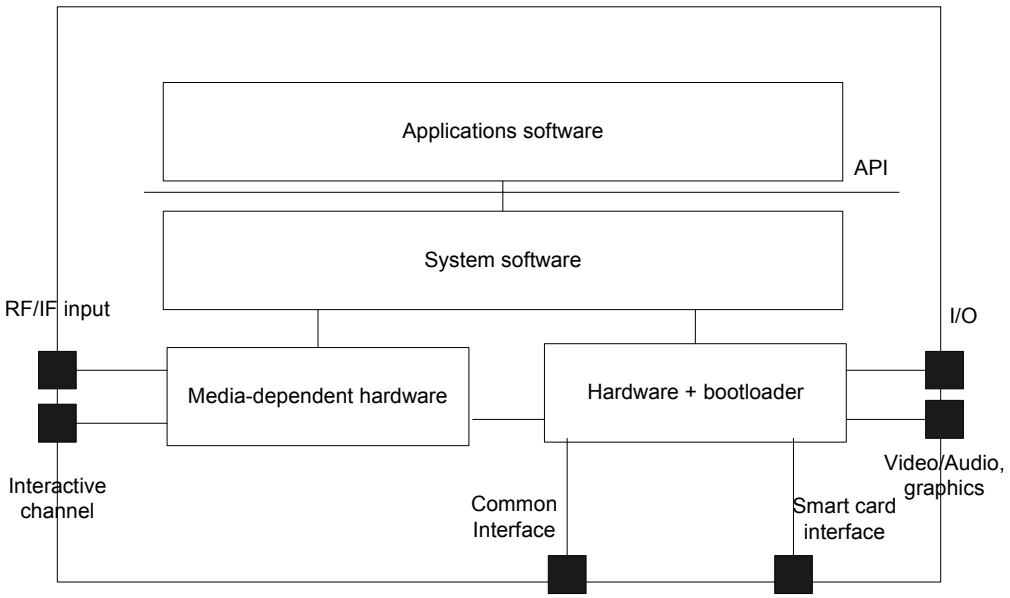


Figure 7. Architecture of NorDig terminal.

Italian DGTVi D-Book

Italy has defined an appropriate digital television receiver for its markets [D-Book]. With support from the Italian government, the development and acquisition of MHP-compatible terminals have been strengthened and the number of receivers in use is already about 1,5 million (January 2005, www.mhp.org). Because of this great penetration, the definition of the Italian digital tv receiver is a target of interest elsewhere in Europe. The DGTVi definition describes technologies and functional premises for the terminal regarding both the device and the software. It is based on the international standards (MHP, DVB). One main goal has been to maintain compatibility with other similar standards (NorDig).

2.2.4 Value-added services

Value-added services are applications that are used with the remote control of the terminal and, for example, with a keyboard. Most of the value-added services are implemented as MHP applications. The applications can either be installed in the device already or they can be transmitted with the program stream (MHP1.0) or downloaded through the return channel (MHP1.1). This chapter briefly presents the most common value-added services that are in use at the moment [ArviD3].

Programme guide

Figure 8. Example of the programme guide's user interface.

EPG, Electronic Programme Guide, is the most used and most important value-added service. With the programme guide the viewer can browse information about programmes and optionally follow a tv programme at the same time. The user interface (see Figure 8) is simple and is used with the colour and arrow keys of the remote control. The functioning of the guide is based on the SI (service information) data sent along the broadcasted stream. The programme guide can be implemented as built into the receiver or as an MHP application. The information on the programmes is updated regularly so the receiver can tune into the right channel.

Super teletext

Super teletext is a renewed version of the old teletext. The text and clumsy graphics from the old teletext have been changed into colour graphics and hypertext containing links. The user interface (see Figure 9) is super teletext browser, for which the digital tv operators and content producers are making appropriate content using applicable tools; page definitions are made with xhtml and CSS. In addition to the traditional page numbers, navigation on the pages can also be done by means of links embedded in the text, so the browsing is very similar to reading www pages. Super teletext requires an MHP-compatible terminal.

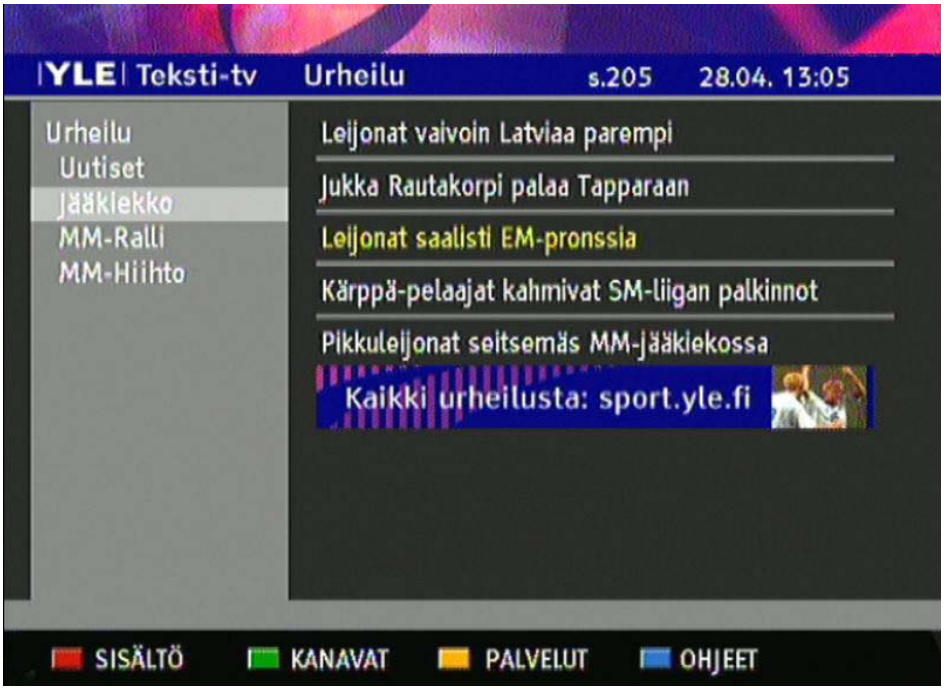


Figure 9. Example of super teletext's user interface.

Programme-specific services

Typically, programme-specific services can be used only during the programme broadcast or the availability is otherwise restricted for certain types of transmissions, such as during the Olympics. These kinds of services are quizzes, games and votes related to the programmes, the results of sports events or elections, and super teletext pages related to the programmes.

Channel-specific services

Channel-specific services do not relate to any programme, but they are always available when the receiver has been tuned to the right channel. These kinds of services can be news and stock rate services or giving feedback to the channel. The programme guide and super teletext are channel-specific services.

Services requiring a return channel

When the receiver has a need to communicate with the service provider, a return channel is required. These kinds of services are the previously mentioned voting and feedback services. Return channel techniques are discussed more closely in the next chapter. In the future, the services required by the return channel will be more diverse. Services familiar from the Internet, such as email, banking services and electronic commerce, will be the most attractive from the consumer point of view. Information security requirements are emphasized when using these kinds of services.

Protecting the terminal from erroneous applications and handling, as well as the transfer of confidential data, requires secure implementations before the end user's trust in the services can be earned. As in other value-added services, in addition to the simplicity of the user interface one has to emphasize ease and transparency of information security for the viewer.

2.2.4.1 Return channel and software updates to terminal devices

There are several standardized alternatives with which to implement the return channel. Table 3 presents as a conclusion the most common possible return channel techniques. The first nine techniques in the Table have been defined in the NorDig specification, according to which the terminal has to back up at least one of these. Other techniques represent different types of home network technologies, which enable connecting the terminal to the other home data network infrastructure. In this context of return channel implementation the speed means the fastest data transfer speed possible between the set-top box and the Internet connection enabled by the connection technique – in other words, not necessarily the actual transfer speed of the return channel. In the Italian digital receiver definition the return channel technique is defined as a modem connection (56 kbit/s); the link level protocol is defined as PPP. As alternative techniques, DGTVi-D-Book defines an Ethernet connection equipped with DHCP backup or a GSM/GPRS connection to mobile phone network. In addition to this, there are industrial coalitions that aim at equalizing the data transfer protocols and connectivity of the home network devices, for example Universal Plug and Play (UPnP) and Digital Living Network Alliance (DLNA) [ArviD], [FICORA2].

Software updates

New features can be updated or errors in earlier versions of the software can be corrected through programs on the terminal. Software updates can be delivered with the broadcast stream. This function enables the utilization of new features (within the limits of the equipment functionality) of the MHP standard as it develops. Software updates are not being sent constantly, but they are available for a limited period of time. Because of this, the device manufacturers have made various solutions with which updates can be carried out by, for example, a maintenance company. The viewer may also transfer the update to the terminal from a PC, for example, using an RS232C serial cable. Installation instructions and practices vary depending on the device manufacturer, and they require basic IT knowledge, which every viewer cannot be assumed to have. Where information security is concerned, the software updates are mainly a threat to the functionality; an erroneous update can mess up the functionality of the terminal so that it can only be restored by a maintenance company or the equipment manufacturer. Distributing erroneous software updates on purpose can also be considered a threat if the attacker is able to falsify the broadcast with another transmitter.

Table 3. Return channel techniques.

Technique	Speed	Special features
V.32bis	14,4 kbit/s	Phone network is available everywhere, but the networks have country-specific differences, which restrict international joint use.
V.90	56 kbit /s	
Ethernet (IEEE 802.3 tai nopeampi)	10 Mbit/s – 10 Gbit/s	Ethernet technology becomes faster and regional, covering more networks. New apartments often have cabling ready for the Ethernet network.
EURO-ISDN (ETS 300 012)	128 kbit/s	ISDN has not become as popular as it is in Germany and Norway.
DECT (ETS 300 175)	32 kbit/s	DECT is not widely used and probably will not become popular as a return channel implementation technique.
GSM/GPRS (EN 301 195 /ES 202 218)	GSM: 9,6 kbit/s HSCSD: 43,2 kbit/s GPRS: 171,2 kbit/s	Connection of a GSM/GPRS terminal to a digital set-top box is typically either IrDA or Bluetooth.
DVB return channel connection (ETS 300 800)	3,088 Mbit/s	Competitor of the EURODOCSIS technique.
Euro DOCSIS (ES 201 488)	38–51 Mbit/s (shared within those in the same cell) Terminal's maximum transfer speed, typically 512 kbit/s	Definition of Finnish Cable Television Association requires built-in EuroDocsis cable modem.
IEEE 1394 (Firewire)	400 Mbit/s	Technology developed for transferring real-time picture and voice.
IrDA	4 Mbit/s	Device has to have a visual communication with another device and the distance has to be short. Not likely to become popular in digital TV terminals.
xDSL	8 Mbit/s (ADSL, for the subscriber) 1,5 Mbit/s (to the network direction) 54 Mbit/s (VDSL)	Broadband data connection, which uses phone cabling. The most distributed broadband technique in Finland.
Bluetooth	721 kbit/s/57 kbit/s (asymmetric) 433,9 kbit/s (symmetric)	Distance between devices about 10 m.
IEEE 802.11 (WLAN)	54 Mbit/s	Wireless local area network technology.
IEEE 802.15 (WPAN)	TG3: 11...55 Mbit/s TG4: 20...250 kbit/s	Based on Bluetooth technology.
HomePNA	1 Mbit/s	Local area network solution exploiting phone cabling.
Data electricity	2–4 Mbit/s (shared within those in the same transforming area)	Exploits existing electricity cabling. Problem with noise removal.
IEEE 802.16 (WiMAX)	70 Mbit/s	Wireless MAN network technology (Metropolitan Area Network). Range about 50 km.

2.3 A brief description of digital convergence

A situation in which several services are getting close to each other and connecting to each other at the technical level is called convergence. The same services are distributed to users using different networks via a converging distribution channel. The main problem with convergence from the information security point of view can be considered to be the different basic qualities of the integrating networks; the Internet is an open and unmanaged system, while the many systems connecting to it, such as television, (mobile) phone networks and production control systems, are owned by separate organizations.

Even closed network environments are facing various kinds of pressure now and in the future. Many organisations are intensively outsourcing their functions, causing the network to be administered by a third party. The changes in network infrastructures are converging towards all-IP solutions due to cost efficiency. This enables phone traffic to be controlled over an IP network using MPLS routing and other similar techniques. As networks are converging, the control and responsibility of the management is becoming fragmented.

One of the problems with closed environments has commonly been the lack of security thinking. Regardless of which level the network security is on, a false sense of security is easily born when the whole network is handled by a single organisation and no hostile parties are located in the network. The main characteristics of the convergence threat can be seen as the switch-over from closed networks to open systems, which causes network traffic to spread in unplanned and untested ways. The data in converged systems is transferred between different network environments, and a false message can cause problems in some networks because of system defaults or errors.

Convergence-like phenomena are nothing new on the Internet. When the network started to expand, many closed, even single-user systems, were added to it. Systems that were planned to be isolated can now be accessed through the network by new means, which were not or could not have been considered before. Attacks using implementation faults or bypassing identification systems were not needed to break security – some systems did not have even the lowest level security mechanisms. Security and reliability cultures have expanded and will expand to the application development in the IP world. Anyhow, signs of challenges caused by networking are visible in many technologies that are being connected to the IP network. These technologies can suffer the same threats as are common on the Internet.

3. Information security threats in digital television

This threat analysis is based on previous studies and industrial interviews. Security threats to digital television broadcasting can be roughly divided into threats to the digital television transmission network and terminal device, threats to the management of the return channel, threats due to digital convergence and threats to service development.

3.1 Threats to the transmission network and terminal devices

Example 1: A user installs a faulty software update for his set-top box (containing e.g. software bugs or being damaged during transportation). Usually, the correct functionality of a program is checked in the set-top box before taking it into use. If this check fails, the device might be harmed when starting the program.

Example 2: A program signal contains errors that the set-top box is not able to handle or fix. This can cause unwanted functions in the set-top box and even damage it.

Security threats to DVB are rather small. This is due to the fact that the data transfer (mainly voice and picture) is done under operator control. There are no threats during the packeting and distribution phases because the operator can monitor and, if needed, interfere with them. From the operator point of view, the most likely threats are connected to the program production phase and consumption phase, as well as to devices. However, the number of stakeholders is increasing in the field and, because of this, transmission management is becoming more challenging.

In practice, interception of DVB-based traffic is still difficult for an outsider, but not impossible. It is possible to try to forge the transmission by another transmitter. DVB-T transmissions are based on COFDM modulation, characterising elimination of multipath fading in a way that the receiver synchronises with the clear signal. In a cable television network this enables transmission of an intrusion signal to the receiving point using small powers (some watts), but the receiving point cannot be too far away. Another threat concerning DVB is the sending of flawed data during an update of system programs. This threat has been covered by using protection in the devices – for example, a flash memory of in a terminal device is only deleted after the new program has been verified.

General threats to smart cards and payment services are targeted to the payment service used by digital television. In satellite television use smart cards keep piracy and unauthorised use moderate, despite the fact that the system is not optimal as card updates are too expensive.

There are more important security threats in the use of MHP. MHP version 1.0.2 currently limits the interactive use of digital television. However, deployment of MHP version 1.1, digital television will become closer to the Internet after the deployment of MHP version 1.1. For the time being, there are no available terminal devices or services that conform to MHP 1.1. An analysis of the threats connected with this standard is needed at the same time as the technology is deployed. It is also likely that as MHP becomes more common, the third-party components used in the MHP devices will also become more common. In this case it is theoretically possible that an intruder could infiltrate a malware program to the MHP application without the service developer knowing about it.

Nowadays it is possible to load MHP applications into a device only from the transmission stream. In this case the operator is responsible for security. Applications loaded into the so-called Object Carousel are typically added manually, although there are some automatic systems. The manual addition of applications guarantees that control over how the services are made available to the users. On the other hand, this can cause human errors. Although the loaded applications are added manually, they are often connected to a local area network. If an intruder can access this network, there is at least a theoretical opportunity to control the Carousel and transmit unauthorised material.

The MHP standard itself is open to many interpretations. The interoperability of MHP applications in different device models is still under development, particularly in the case of MHP standard version 1.1. This is slowing down the process of application development.

MHP security can be strengthened by digital signatures, and they are just about to come into use in Finland. The digital signature process consists of three parts: compression files, signature files and proof files. Signatures are the best that state-of-the-art solutions can offer for ensuring that the contents have not been modified. An application signed by the Root Certificate Authority is attached to the so-called Permission Request File with information on which resources can be used by the application. The Root Certificate Authority for MHP is currently WiseKey SA. In Finland, the practice of using signatures is only just about to start. It is likely that the signature certificate will be given to a big stakeholder. In this event, smaller stakeholders will not need a certificate of their and will be able to operate under a network operator’s certificate. However, all certificate holders will be responsible for their own part.

Currently, the main challenge to the use of certificates is the underdevelopment of the terminal devices – most of the digital television transceivers do not have root certificates. This has resulted in a situation where the signature checking and access control of applications have been disabled by the device manufacturers. Contrary to the MHP standard, it is possible for an unsigned application to open a return channel to implement modem hijacking or change the channel.

Special care and attention is needed and the user must check the functions based on the certificate information. The device should have a mechanism for these kinds of checks – e.g. if a certificate is jeopardized, the equipment should be updated to cope with the changed situation. In another case the whole chain of programs could be jeopardized. It can be assumed that most of the users are not capable of carrying out the task of checking functions. They will carry out a random act that mostly grants permissions. The whole mechanism requiring user intervention is a threat from the user's perspective and the implementation of it should be carefully analysed by the service provider and device manufacturer. Relying too much on certificates can prepare the way to using old certificates for harmful actions, such as an ActiveX incident (http://www.dataworldindia.com/html/activex.html).

Other important security features of MHPs are certificates, resource use permissions and channel-oriented security features. If these features are used in the right way, the current technology is relatively secure.

3.2 Management of return channel and threats due to digital convergence

Example: A viewer loads an MHP application that is digitally signed by the service provider. The certificate is not checked in the terminal device – enabling the application to get the most extensive access permissions to use the resources of the device. The application loads a JPEG picture using the return channel. The picture has been erroneously encoded in such a way that part of its data is handled as an executable code. This code contains a malware program that shuts down the set-top box.

The most of the security threats to the return channel are due to the use of Internet Protocols. Because of the trend for digital convergence, the digital television transceivers are becoming more versatile. To a certain extent, this becomes similar to a PC – the models with hard disks offer storage space, the return channel types are becoming more versatile and the processing power will be increased in the future. However, because of different usage, there will be always differences to PCs. From the point of view of resources, a digital television transceiver will not be similar and will only follow the evolution of PCs.

Most of the information security risks for digital television are connected with the return channel. The TLS (Transport Layer Security) protocol is normally used to protect the return channel, resulting in encrypted traffic. Unlike a www browser, the MHP application opening the TLS connection does not verify the server certificate (e.g. time of validity) because the current terminal devices do not normally have a root certificate, which is needed for the verification; the root certificate can be transmitted along with the application. However, this is not compulsory and there is a chance that the certificate chains are generated by malware.

The simplicity of set-top boxes makes them more secure. For example, it is not reasonable to carry out port scans in simple devices as the devices do not have applications worth connecting.

In practice, the most important technical solutions for the digital television return channel at this moment are the http and http protocols, and xhtml – which is an enhancement of the html language based on xml. The appearance of xhtml is more strictly defined than html. Http is a relatively simple protocol and its implementations in the Internet world are rather robust. Typically, most of the problems are due to extensions of html and the management of protocols and file formats transferred over http. Implementations of these modified versions of http introduce threats to the development of digital television too. Cookies are a privacy threat for the users if they are used to build up user profiles and habits. If http is operating over TLS/SSL, there are security threats in implementation level vulnerabilities and the digital signature system and its implementation, which is presented in more detail in Section 3.1. The return channel of digital television includes a lot of content transferred over http, like xhtml, picture formats (GIF, JPEG, PNG), MPEG and font format PFR [MHP].

At least the picture formats are rather complex. There have been vulnerabilities in the management of picture formats, where the application can be seized with a malicious input.

The threats to html are connected to the reliability of their parsing implementations. Lately, this has been taken into focus. Vulnerabilities have been found in some parsing implementations of www browsers; similar vulnerabilities have not been found in xhtml and xml implementations.

The level of information security solutions in html extensions varies a lot. In addition to the html protocol, there are different vulnerabilities in browsers that are complex programs. The threats are due to different active content-producing extensions, such as Java, Javascript, ActiveX and Macromedia Flash.

Reliability and easy manageability of http extension implementations are critical. The functionality of http extensions should be able to be clearly restricted. Currently, there are no extensions like this in the MHP standard.

Service developers and terminal device manufacturers have an interest in increasing the functions that use the return channel in digital television devices, especially different payment services like shopping and movie subscription services. The security threats to these kinds of services are similar to the threats to Internet banking and shopping services, and similar guidelines should be followed in their development.

It can be noted that the security threats for end users will be more emphasized in connection with the trend for terminal devices becoming more developed and more common. If the devices become more and more like conventional PCs, it is likely that the normal PC threats will also appear in the digital television world.

Along with the deployment of MHP 1.1, the risk of introducing viruses into set-top boxes is increasing. As digital television transceivers become more common, virus writers will be more interested in them. The typical goals of malware developers are, e.g., converting devices to act as vehicles of denial of service attacks or as an automatic transmission point for set-top box spam. State-of-the-art set-top boxes and their applications are based on Java. Consequently, the security issues in Java concern them too. For the present, the Java programs used in MHP operate in their own protected environment, the so-called sandbox. The goal of this arrangement is that malware is not able to use the admissible applications. For example, it is possible to shut down the MHP part (Java virtual machine) of a set-top box using a simple loop structure.

Independently propagating worms are not a relevant threat today because there is no functionality currently in use allowing the MHP applications to be propagated among set-top boxes. If email functionality is integrated into set-top boxes, this threat will become concrete in the digital television world as well.

The program memory of a set-top box is erased during a channel change, preventing malware from gaining a hold. However, MHP standard version 1.0 defines a so-called persistent storage interface that enables a signed application to write files to the long-term memory of the user device, even though it is loaded into the device every time the application is started. In addition, the inter-application communication interface of MHP enables method calls over the network using the Remote Method Invocation (RMI) of Java. This makes the work of an application developer easier because Java methods running in another virtual machine and computer can be called just like local ones, and there is no need to think about application-dependent protocols. An obvious security threat exists if the transmission of method calls over the network is not protected. However, the Java application of the server end must create and employ the Java Security Manager – otherwise the RMI classes cannot be loaded.

IP Datacasting

Use of the Internet protocol in the DVB network data transmission (IP datacasting) is becoming common among PC users and professional communication users. The content transferred on the Internet can be compressed into the DVB-T signal at the transmission end of the television network and decompressed from the DVB-T signal in a PC receiver card. Using IP in the transmission enables broadband video streaming and transfers of large files.

Currently, PC cards with a PCI and USB bus are used as a receiver in IP datacasting. The standardisation work of IP datacasting is still under process, introducing challenges for information security management.

3.3 Service development process

Example: A service provider assembles a service using software components from different manufacturers. The interoperability of these components has not been tested sufficiently. The end user feels this every once in a while as error situations in the user device and as unreliable functionality. When a new version of the service is assembled, interoperability problems grow even bigger if the new version is not tested comprehensively.

There can be threats and problems in each phase of the system and service development. During the design phases threats can be generated by situations where certain immature technology is used, even though the risks are big in that technology, or a security solution is used and a new functionality of newer technology is not utilised. The core phases are the requirement specification and system design phases. The implementation phase can incorporate various problematic issues, e.g. software bugs and wrong kinds of connections between modules. Threats are generated by supporting systems too. These threats are due to weak programming languages and weak development tools – both of which can be trusted too much. In addition, the use of third party components can generate threats, although the information security level of them remains unknown. During the system design threats can be generated by wrong assumptions regarding the system environment and human behaviour, as well as faulty models and simulations. During the implementation analysis phase it is possible to carry out the wrong kind of testing. Some general problems in development are slowness in absorbing new maintenance practices and a low ability to understand new errors during the process of repairing old ones. Moreover, there are threats in the disposal of services, such as premature shutdown of required components and a hidden dependence on a non-existent older version.

4. Solutions to information security threats in digital television

This chapter discusses the most significant solutions to the service provider's information security-related problems, along with the corresponding architectures. Since total information security is impossible to achieve, and no solution can be durable in the long run, the presented solutions can only be considered acceptable guidelines for designing information security.

Taking care of information security places various requirements on networks, servers, hardware, software, systems and procedures. To be able to employ and manage them simultaneously is difficult, sometimes even impossible, and is directly related to the corresponding application area. This means that in order to have a functioning system the risks of the current situation have to be identified, managed and minimized. Risk analysis is, perhaps, the most important individual method that can be used to significantly improve the state of information security. Usually, risks can never be totally avoided unless some related actions are completely ceased. Similarly, risks can be minimized by minimizing the risks' frequency of occurrence and the consequences. A risk can also be transferred to other directions by an agreement. The most typical agreements are, for example, transport agreements and subcontracts.

Part of the risks should, or have to be, kept at one's own risk. These are, for example, risks caused by servers necessary for e-business that are connected to the Internet. Risk management also encompasses proactive actions, such as contingency and recovery plans for server attacks.

There can be a gamut of technical solutions combinations where digital return channels are concerned. This increases the complexity and makes service provider's choice of solution problematic (for instance when choosing an application platform).

The role of digital TV as a mass media emphasizes the importance of solutions related to content protection and program source authentication. The service provider wants to prevent any illicit content use; on the other hand, the viewer wants to know where each application is from and ensure the seamless functioning of the terminal by preventing the download of unknown applications. The infancy of DRM (Digital Rights Management) techniques and, most of all their, low interoperability have restricted the generalization of services that distribute legal copyrighted material, such as digital music. Services related to distributing digital content are very attractive from the digital TV viewer's point of view because a digital TV network is extremely applicable for distributing these kinds of services.

The most important solutions to different threat classes for a service provider have been gathered and combined in the following Tables 4 and 5. Table 4 is from the technology point of view, whereas Table 5 focuses on the information security process of the service provider.

Table 4. Technology-oriented solutions and threats in digital TV.

	Technology /Process	Impact on information security	Implementations	Target				Information security					
								Security functions			Security concept		
				Device/End user	Return channel	Distribution network	Service development process	Recovery	Protection	Observation	Availability	Integrity	Confidentiality
Content protection	Digital rights management.	Controlling the legal use and copying of the content. Distributing chargeable content.	DVB-CMCP, DRM, Conax.	●	●		●		●	●	●	●	●
	Digital signing and verification of the programs.	Certificating the origin and integrity of the programs. Restricting the program rights in the device.	MHP-PKI.	●	●				●	●	●	●	
	Encryption of the saved data.	Data protection according to the information security policy. Fulfilling the requirements for privacy.	Encryption of the data storage medium.	●	●		●		●		●		●
Protection from attacks	Connection to electronic payment system.	Secure connection of the service to external payment systems. User authentication.	Tupas, HST.	●	●				●	●	●	●	●
	Protection from malware.	Preventing viruses and malicious content accessing the target system.	Antivirus software, content filtering.	●	●	●	●	●	●	●	●	●	
	Privacy protection.	Protection of personal data according to the law on personal information, etc.	User rights management, encryption of the data storage medium, information security policies.	●	●	●	●		●	●		●	●
	Server and broadcast equipment protection.	Protection from attacks coming from networks. Protection of confidential data.	Firewall can improve protection of a LAN server or other device.		●	●	●	●	●	●	●	●	●
	COFDM content protection.	Greatest risk is modification of a terminal's utility program with false dispatch.		●		●				●		●	●
	Detection of attacks.	Observation of network traffic in order to detect attacks.	IDS/IPS systems.	●	●	●	●		●	●	●	●	

Table 5. Service developer's information security process.

	Technology /Process	Impact on information security	Target				Information security					
							Security functions			Security concept		
			Device/End user	Return channel	Distribution network	Service development process	Recovery	Protection	Observation	Availability	Integrity	Confidentiality
Service developer's information security process	Third-party assessment methods. (e.g. quality or information security audits).	Service developer's information security processes and product development processes and quality system. Proactive operation that grants recommendations done by neutral party. Allocated operation and improvement proposals. Technical or managerial audit.	●			●	●		●	●	●	●
	Risk management.	Risk identification, assessment and reduction. On-going process.	●	●	●	●	●	●	●	●	●	●
	Physical security solutions.	Access control, fire safety, confirmed power supply to servers.	●		●	●	●	●	●	●	●	●
	Fault situation recovery, contingency plan.	Provision for fault situations: • Data loss. • Hardware problems. • Information security violation. • Communication.			●	●	●		●	●		
	Product version management systems.	Product development process. Managing different versions under development.				●	●	●	●	●	●	●
	Information security in business management.	Information security processes in management. Communication. Education. Responsible people in the organization.			●	●	●	●	●	●	●	●
	CERT activities.	Preventing information security violations, observation and solution. Communication of information security threats. In Finland, CERT-FI of the Communications Regulatory Authority.	●	●		●	●	●	●	●	●	●
	Product development process follow-up, improvement and education.	Quality improvement.				●	●	●	●	●	●	●

4.1 Risk management

4.1.1 Management of technological dependence

Weaknesses in the information infrastructure have induced new kinds of vulnerabilities in the society. Information network environments are now more complicated than ever before and their complexity will increase from the current situation. A significant factor in this increasing complexity is the merging of different networks. Understanding the entirety of networks can be insufficient, which, as well as complicating network management itself, also complicates risk management and vulnerability analysis. Risk management-related decisions presume a perception of the technology dependency, in which protocol-oriented inspection can be used.

From the broader point of view, the lack of clarity in the general view is a notable limitation to the study of protocol environments. Perceiving singular protocol families has been studied, but different protocols cannot be treated as isolated individual cases. These different protocols exist in the same networks, and, as result of the standardization process, often include the same or interrelated sub-protocols or structures. Thus there are dependencies and connections between the protocols that are often hidden. Observing these connections is still of primary importance for the sake of vulnerability analysis, coordination of the vulnerability process and risk management of the infrastructure. A singular vulnerability can, through the protocol dependency, threaten the network in ways that cannot be revealed by normal vulnerability analysis. A typical feature of television broadcast is that the same content is distributed to millions of viewers at the same time, which means that in case of defective dispatch the problem situations will rapidly get really bad. Most of the viewers are still quite unfamiliar with the technique, so the ability to react to the technical problems is rather scarce.

The secure programming group of the University of Oulu has developed a visual solution model for detecting technology and protocol dependencies.

According to the model, data related to the technical features and distribution of the protocol is collected. The information related to the public attention towards the protocol is also crucial from the research point of view. A broader view of the existing situation is achieved by expert interviews.

Because of the extent of the topics, the expert interviews have a significant position in the study. After the primary protocol study, a broader and more detailed view of the protocol jungle is achieved by interviewing the experts in one's own organization. Media follow-up assists in finding new domestic experts and gives some idea of the protocols related to critical infrastructure and its sub areas. By interviewing experts, some new protocols and protocol groups might be found that have not been thoroughly

studied; therefore, they form great and probable information security risks. The distribution and user environments of different protocol implementations are especially important for the analysis.

The purpose of the solution model is to achieve better technical and administrational understanding, with which the general view of the protocol field can be gained and the problems, such as hidden connections, dependencies and inheritances, can be seen. Visual thinking enables harnessing of the images, idioms and colours, as well as offering informative communication means between actors in the field. The purpose of the model is to introduce protocol dependencies that affect critical infrastructure.

The model enables the study of different practical scenarios and the factors that affect them. One of these scenarios includes certain network components and protocols implemented by them. In addition to data gathered from the protocols, this scenario can take account of the network administrating organization's own vulnerability analyses, risk management plans and threat scenarios in order to study problems in the network. The model acts as a source material in risk management, vulnerability analysis and strategic planning, and for paving the way for information security research.

4.1.2 Change management

The development of information technology is based on abstractions: all information technology systems rely on the functioning of the lower level systems. Abstractions are managed by different modular structures and strictly defined interfaces – basically, one underlying system could be interchangeable with another one that follows the same structures and rules as its predecessor. Abstraction has been successfully used in network technology, for example in the TCP/IP stack, but it has proved to be difficult in the software world.

The implementation part of the service development binds the composed and defined software into a certain environment, thus its functionality is dependent on its environment. These interdependencies rapidly become complex when even slightly more complicated systems are concerned: the software is dependent on a certain operating system version, hardware drivers, programming language environment and other programs. Normal administrative duties can break this often very sensitive balance. Managing changes in the used systems is thus fundamental in service development and, especially, in its administration.

Documentation is a vital part of managing changes: the resources used by the service have to be accurately defined. By doing this, the targets that need special caution when changed can be identified. A preliminary study can be done during the concept stage.

All changes should be tested in the test systems before being transferred into production use. In case the change is harmful for the service but necessary for the system, the software itself has to be updated. Difficulties can arise from software already distributed to the consumers that will then cease to function when the update is carried out. The software update has to be made easy for the consumers and it must be appropriately notified.

Subcontracting increases the complexity in change management. This will have to be taken into account when agreeing upon the practices.

4.1.3 Management of information security risks

The risk management stages are roughly divided into risk identification, risk assessment and contingency planning for the risks. These stages can partly overlap. An organization implementing different stages of risk management separates its actions and aims at seeing their conditions and connections, after which risk management can have a generally strengthening affect on the actions.

In the identification stage the conditions for the actions are listed and related threats are sought. Recognized threats can be as unlikely as possible at this stage – their importance is valued in the following stages. At the same time, the signs indicating threat realization can be valued, which, when being followed, can help avoid the risk before its realization. An avoidance plan can be created at this stage or in the last stage together with the contingency plan.

In the assessment stage the severity of the threat realization related to the action and the probability of the threat itself are considered. One way to value risk severities related to each other is to present estimates as numerical values and compare the product of these values. Still, some threats cannot be minimized in any way.

A risk avoidance plan and a contingency plan are made in the contingency planning stage. Risk management itself consists of actively following the situation, recognizing and monitoring symptoms related to different risks, implementing plans and assessing, as well as developing, the risk management itself according to different situations.

Risks can be divided into technology risks and user-related risks. User-related risks are more significant, but technical risks are often handled more – perhaps because of their easier manageability. Still, users can often foil the technical solutions with their actions.

User-related risks have to do with a lack of education or, on the other hand, intentional actions. Lack of awareness of information security matters can cause unintentional

information leaks or hazardous ways to use or configure tools. The need for education is emphasized if prying or other forms of social engineering can be assumed to occur towards the users. On the other hand, a significant part of computer crime takes place inside the organization. The risk can be minimized by dividing the organization's functioning into several use areas and, inside them, into user rights, unless this hinders the functions.

There are several basic methods for managing technical risks. The most important systems must have backup systems that start if the original system fails. Then only such software and hardware that have fulfilled at least some kind of quality criteria in the testing are used. They should be acquired from several producers – the dependency on a single producer can cause problems when the product line is ended or bankruptcy occurs. It does not matter if the component producers are located in several countries, this only minimizes political risks.

The equipment has to have spare parts readily available in order to minimize damage caused by breakdown. Expertise has to be available to manage the system; the benefit is questionable unless someone can administrate and modify it when necessary. Systems have to be kept in a secure place behind locked doors. Their functioning temperature, energy supply and other conditions have to be ensured. One essential detail in the television service risk management is to ensure availability by replicating the critical systems and quickly available backup systems. One can never over-emphasize the functioning of fault situations, training, education and good planning procedures.

4.2 Technology-oriented solutions

The most important technology-oriented practices for securing information and systems on the server side are (sources e.g. [CERT]):

- Choose server equipment with basic information security qualities corresponding to the applications' standard. A cheap server with low basic information security qualities cannot usually be used for demanding applications.
- Update operating systems and applications quickly enough as the faults are detected. Updates have to be followed as often as daily.
- Set obligatory user authentication for every user of the system. Set the authentication methods required for the user according to the application and access rights – for example strong authentication (such as SecurID card + passwords), if the remote user ID has administrator rights. Decide whether system administration occurring remotely is necessary or not. Estimate whether remote control is beneficial for information security when compared with the risks. Often, system remote control is beneficial.

- Plan and implement a separate access monitoring hierarchy for operating system folders, files and equipment. Ensure the functioning carefully, especially after updates and administrative actions.
- Arrange a long-term and secure backup storage of good quality for all system files, including user data and system configurations.
- Protect the equipment from computer viruses and malicious programs. Nowadays it is of the utmost importance to ensure the functionality of this protection (the download of virus protection updates). Even closing the system or its parts (e.g. email) in a controlled manner can be necessary in some cases when a virus threat is at its highest.
- Use system replication to ensure service availability. This has to be done with expertise and with premature testing using secure replication methods.
- Isolate or prevent direct connections to the Web servers from public networks, as well as organization intranets, by using firewalls. Even this prevents most of the regular attacks. Choose an appropriate level of log collecting and monitor them with reasonable methods (alarms, etc.). Minimize the functionality of the Web server to cover only the relevant programs that relate to the application. At all times aim at protection from the most common attacks by using existing protection methods.
- Utilize systems that detect actions against presumed access rights or other kinds of suspicious and unexpected action.
- Use some practical system that stores information learned from previous errors (or realized conscious risks) and is easy to use in protection planning and implementation.
- Carefully plan and implement any possible outsourcing of the system's information security administration and bind different responsibilities by contracts. Often, some of the most serious consequences are not aimed at the party responsible for the protecting actions, regardless of what the contract says.

4.2.1 Authentication and identification of users and devices

End user authentication can be divided into two cases when implementing e-business in digital tv: viewer personal authentication and subscriber authentication, in which viewer identity data is insignificant but service subscriber information is only needed when pay content is charged. Personal user authentication can happen over the return channel. The main goal in digital tv authentication methods has been to utilize already existing solutions (e.g. web), so that the consumer can be offered the same use experience independent of the service. For example, identification mechanisms used by banks and various smart card solutions have been used for this. As a payment method, the user can

use either money loaded into a smart card, or mobile payment, or various secure payment methods through the return channel [TIEKE], [ArviD2].

4.2.1.1 Authentication and identification of users

The Finnish Ministry of Finance recommends the following for public services (see also Table 6):

- bank service ID based on the Tupas standard for the banks or
- authentication based on the civil certificates (HST).

It can be assumed that the same payment principles will be transferred into electronic services because user customs will easily transmit further, regardless of the area of use (public or private payment) or the situation (wired or wireless connection).

Table 6. About Tupas and HST solutions.

Payer authentication solution	Description	Frequency
Tupas	**Tupas service** of the Finnish banks (more information, e.g. http://www.pankkiyhdistys.fi/): • Bank authenticates the customer on behalf of the service provider. Based on the use of same bank service ID that the customer uses within his/her banking services. • During the authentication the customer chooses the bank logo from the web page, which directs the authentication event into the bank. User enters a one-time password for the authentication. • After the authentication the customer accepts the information about himself being transferred to the service provider and returns to the web page.	Used in about 100 electronic services. About 4 million citizens have the bank service IDs. Nordea, Osuuspankit, Sampo, Säästöpankit, Tapiola, Ålandsbanken.
HST	Civil certificate (Hst-) is based on an electronic PKI identity created for the citizens by the population register. The electronic ID used in secure network transactions is called SATU – electronic transaction ID. HST certificate is used in • personal identity chip card • OP-group's VISA Electron payment card with chip • mobile phone SIM card of operators TeliaSonera and Elisa (during spring 2005). Using Hst authentication, only the person's SATU is known. Strengths are security level and digital signature.	Used in over 50 electronic services. Over 60, 000 HST cards are being used. Luottokunta, DNA, Elisa, OPK, Handelsbanken, Säästöpankit, Paikallisosuuspankit, TeliaSonera, VRK.

4.2.1.2 Authentication and identification of terminal devices

It is not necessary to authenticate or otherwise individualize terminals if the used content is free of charge and/or not encrypted. Pay content use is restricted with

encryption that is decrypted with decryption card. For this purpose the terminal has to have a card reader that supports the Conditional Access (CA) function. In addition to the encryption key, the card typically includes a unique number, whose corresponding information is in the customer service's possession for the invoicing. The CA systems of the terminals used in Finland are based on the Conax decryption system.

4.2.2 Authentication and identification of services

Signatory and signed information can be identified with a digital signature. In order for the signature to be valid, it has to be unambiguously connected with the signatory. The signature has to be crated with a tool that the signatory can possess. With this, non-repudiation can be achieved, which verifies the signed information, the origin of the signatory and the integrity of the information [MINTC].

The position of a digital signature has been clarified by the European Parliament's accepted directive 1999/93, which many European countries have adopted as part of their legislation.

In order to be able to sign digital data, a compressed form of the information it includes has to be calculated. This is done by compression algorithms. The original and compressed versions are connected to each other by mathematical formulas so that the same compression of the same data can always be calculated but the original data cannot be restored from it. When the original document is changed, a new compression has to be calculated. The authenticity of the document can be proven by a compression attached with the message, when needed. If the compressed version does not correspond with the original, something has been changed. A digital signature utilizes various compression algorithms, for example MD5 (128 bit check sum) and SHA (Secure Hash Algorithm, with 160 bit).

A digital signature also ensures the origin of the data when the signatory encrypts the compression with his own private key. By doing this, a so-called seal is achieved, which is sent to the receiver. In order to read the message the receiver has to decrypt the encryption with the sender's public key. The receiver of the message calculates the message compression and, if it matches the compression that has been sent, the user can be sure of the origin of the information. The encryption keys can also be secured with a digital signature. A signed key is called a certificate. This process minimizes key misuse as the identities of different parties are confirmed by a third party. A certificate issued by a certificate authority enables the identification of the key owner. This kind of certificate has a limited period of validity.

Certificates are used in digital services to ensure service origin, which means authentication of the service provider. In case of a service delivered to an end user – for example, a Java application – a compression is calculated which then is signed with the service provider's private key that the third party has verified. Using the accompanying certificate, the end user can check the origin and authenticity of the application. The certificates are mostly based on the X.509 standard, which defines the form and content of the certificate as well as the Certificate Revocation List. The Certificate Revocation List is used to cancel a certificate before the expiration of its period of validity, for example when the private key is exposed to publicity.

Signatures and certificates in MHP services also regulate the rights the application has in the terminal, depending on whether the application is signed or not. The DVB organization has defined a public key system, MHP-PKI, which is composed of three root certificates:

1. active MHP PKI root certificate
2. replacing MHP PKI root certificate
3. signature certificate of root certificate management message; the root certificates can be changed in the terminal with an RCMM message.

The first two are certificates of the MHP-PKI main level; the third is only used to sign RCMM messages. The terminal manufacturer installs all these certificates according to the MHP definition for the terminal, with which certificate chains consisting of different certificates can be verified [MHP-PKI].

4.2.3 Content protection

Generally, copyrights give a producer of a copyrighted work some privileges, which are on a time scale limited to, for example, 70 years after the death of the producer in the case of a published work. Distribution of the work has always been difficult because the restrictions set by the rights owners and the practices of the material users have been so far apart from each other. This is not likely to be changed in the digital world, where perfect and loss-free copying of the files is easy because of the open systems. Every time the rights owners have found a way to protect the content from extensive copying, the users have found a way to evade it. Transferring the work from digital form to analogical, i.e. in a form understood by humans, is the ultimate point where copyrights can, regardless of way of protection, be broken, even if the digital environment of the work in question is protected by encryption. Thus the copyright protection seems to have no effect on professional copying for retail, in other words piracy. It is worth mentioning that because of the so-called "network effect", even copyright violations can

have a positive effect on the sale of the original work, which has been mentioned as one of the success factors for Microsoft.

Because, in addition to copyrights, consumer habits are affected by work availability, ease of purchase and use, price, and other laws of supply and demand, the average user does not value copyrights too highly. When using multi-channel distribution the same content is available to several terminals and through different channels to the users. In case the content protection level of one channel and terminal is raised and user actions such as content copy to another terminal is complicated, the user can choose to get the same content using some other channel, be it legal or not, and transfer the content to other terminal.

When protecting content the magnitude of the effort is affected by the development of the content value in relation to time. For example, the sales time of tomorrow's weather is focused on one day, after which the product, with its content, is worthless, especially to the consumer. On the other hand, the sale time of an MHP service can cover several years, after which competitive products or more developed features of a new version can diminish its value close to nothing.

Development of digital tv brings along different services, Video-on-Demand systems and interactive services enabled by the return channel, such as games. The role of the content protection increases when services diversify. Implementation of DRM is important so that copyright-protected content does not leak, for example to Internet distribution. If the system does not have working content protection, the threat is that there will be high-quality copies of tv programs distributed on the Internet and payable MHP applications will be swapped in different peer-to-peer networks.

In 1999 the DVB-Organization began to develop a Copy Protection and Copy Management system (CPCM) for digital tv. Even if DVB has earlier developed pay content related protection mechanisms (Conditional Access, CA), which are broadly implemented on terminals, the definition of the DVB CPCM system is still open. The conceptual model has been finished, including typical components of DRM solutions:

- rights definition, in which the content-related usage terms are described
- access control: a technical solution ensuring that only authorized viewers can use the content
- authentication enabling content follow-up for the copyright owner
- billing and payment systems.

The aim of the conceptual model is to maintain compatibility with other DRM and copy protection systems at the implementation level. Possible implementation methods are

content encryption between distributor and end user, water marking and fingerprint technologies, as well as identification systems.

4.2.4 Privacy

Privacy means end user rights to control the information concerning him, to affect the handling of this information and, when necessary, get information from the parties that manage them. From the privacy point of view, it has to be remembered that, as a service platform, digital tv is legally just like any other platform offering digital services and the same regulations concern it. The service developer is obligated to design features concerning privacy and information security that are so easy to use that the user can understand the meaning of his actions and any possible related responsibility issues. As a use environment, digital tv is rather restricted, so the service developer has great influence on how the end user can manage information related to his privacy. In the case of digital tv, the most significant challenges concern data protection handled by digital services, especially where interactive services are concerned, as well as restriction of profiling information collected by television channels [MINTC2].

4.2.4.1 Privacy in electronic services

Privacy protection is guaranteed in the Constitution. The most essential regulations concerning services are

- law on consumer protection
- law on information society service offering
- law on personal information
- data protection law on electronic communication.

In Finland, for example, customer data merchandise is forbidden by legislation, but this kind of threat exists when such channels are used (transfer link, e.g. a satellite) and the transmission takes place in a country that does not have legislation forbidding it.

Generally speaking, the collection of personal information always has to be justified and no end user information should be collected or stored unnecessarily.

4.2.4.2 Viewer profiling

When terminals equipped with mass memory become more popular the possibility of collecting so-called profiling information about viewers will increase, for example

about viewing habits. By default, there has to be permission from the user for this kind of information collection. On the other hand, profiling enables new kinds of applications for the user, such as application automatically storing programs the user would probably watch, but also in this case there has to be some confirmation that the profiling data is never transferred elsewhere from the terminal through the return channel without user acceptance.

4.2.5 Protection of digital television infrastructure

In addition to the terminal, a digital service also consists of the server environment, which is usually a server connected to the Internet. The Internet connection enables services to utilize the return channel. Protecting the server is ultimately important because, depending on the service type, there can be information such as user payment connections and related data stored in the server. Service functionality and availability also depend on the server functionality and how they are protected from denial of service attacks.

The system producing the MHP service consists, as a whole, of different kinds of networks and devices connected to the networks. The devices, or the subsystems they constitute, offer functionalities for the assembly with resources, whose intentional or unintentional misuse is a threat for the owner of the equipment or a subsystem, or the other parties.

Resource misuse is prevented by monitoring and restricting its use. Examples of mechanisms to restrict misuse are access rights for users or files, firewalls and antivirus programs.

Computers – from mobile phone and PDAs to PCs, servers and supercomputers – are usually based on a couple of basic components and the functionalities offered by them. The processor is the heart of calculation and it offers applications processing time, whose is regulated by the operating system. RAM memory is short-term memory, which almost all applications need to function, and whose usage is usually regulated by the operating system. Mass memory is memory specializing in long-term data storage, and whose usage restriction is usually possible by operating system settings. Computer data busses and bus connections enable data transfer between different computers, networks and users. It is usually possible to restrict data transfer with network settings in the operating systems and equipment, as well as with the access rights of external devices.

Because the resources needed for the processing of protocols used in data transfer, like processor time and memory size, increase as the abstraction level increases, the lack of these resources becomes a hindrance for higher level protocol data transfer speed. Because of this, restrictions on processor time and memory use have an effect on the

data transfer speed. In addition to just monitoring the restriction on a single resource usage, one must also consider the general view in order to gain the desired performance from the equipment and subsystems.

The resource use in all devices that produce services should be restricted in such a way that one disobedient server cannot produce a state where the system cannot offer services to the users. Likewise, one erroneous process inside one device should not jam the whole device by using excessive processor time and RAM memory. How much of common shared resources, like data transfer capacity, processor time or memory, one server process or subsystem computer can spend is a question of design. For example, the processor time and memory usage of server processes can be restricted so that the resources are sufficient for a certain number of service processes, and subsystem data connections can be limited so that the transfer capacity is enough for a certain number of simultaneous service requests.

By monitoring resource use, system error conditions can be detected, which can be unintentional administrator accidents, intentional attacks or system misuse. For security, resource usage limits should be set to minimize false positives. Likewise, false system actions remaining inside limits, so-called false negatives, should also be as rare as possible. Changes in the system usage environment, such as growth in the utilization rate, cause changes to the resource usage, so the restrictions on resource usage should be checked and set often enough.

Computer processing capacity and memory size increases according to the so-called Moore law. Because of this, the number of programs has increased in such a way that new and easier-to-use functionality has been built on top of existing functionalities and implementations. Because of this increase in abstraction level, the attacks are targeted at, and utilize, higher level elements. For example, a traditional network filtering firewall does not nowadays prevent even common attacks against http or html email protocols because almost all TCP/IP firewalls allow the use of these protocols. That is why it can be expected that when a new, easy-to-use technique, such as XML or remote procedure calls (RPC) on top of http, are utilized, there will be attacks against them, which have to be prevented by some new mechanisms.

The rapid growth in the abstraction level and more and more hostile application environments have revealed that all existing programs have included programming errors, which the attacker can use to run malicious programs in the target computer. Correcting these errors and updating the applications is easy in general purpose systems, but in close or embedded systems, such as mobile phones, it is only possible with third-party software. Restricting the resource use, like monitoring the read, write and execute rights of RAM memory, or requiring a digital signature for program files, have made the exploitation vulnerability more and more difficult. These restrictions have been

successfully evaded by using higher level protocols, such as html, and programming languages such as JavaScript. In addition, on top of the protocols and programs there is still a human as a user or administrator, who can be misled by different means – especially, if he cannot separate a system malfunction from a correct one.

Because the current general purpose computer architectures have proven to be fundamentally unreliable, the computer and, most of all, the content industries are planning a computer architecture that is protected by cryptographic means (Trusted Computing Group), in which program execution and other rights could be more accurately restricted. This power to restrict execution is questionable, however, because it is way too easy to misuse it for financial advantage, so its future in the open systems is not certain at all. Instead, in closed systems, such as media terminals (pay-tv), this kind of architecture is possibly more practical, even if the threats to these systems (e.g. organized crime, such as forging pay cards) are very different compared with the open systems.

4.2.5.1 Protection of servers in practice

A server is a software or computer that, together with its software, produces services to other (client) softwares, computers and users. The services usually include information retrieval, modification and distribution. Providing a service securely requires active administrative actions, which are partly implementation-dependent, and which change as new vulnerabilities and methods of attack are found. The ways of administration the various service platforms are different and the best administrative and usage means develop over time, etc.

CERT-FI is a national CERT (Computer Emergency Response Team) group within the Communications Regulatory Authority whose tasks are to prevent information security violation monitoring, find solutions and provide information on security threats http://www.ficora.fi/suomi/tietoturva/cert.htm. The servers' administrators should follow this kind of current, general, security-related information. For example, according to the "annual review 2004" by CERT-FI, malicious programs targeted at mobile phones are developing in a more practical direction, so programs accessing mobile phones should be carefully controlled on many levels, like in the servers of MHP services. Generally, preparing actions against Internet threats are emphasized for the future and will require more and more activity in organizations. The use of IRT (Incident Response Team) groups is emphasized.

Securing a server that is providing services is an on-going process. When choosing service-producing protocols, network architecture, server platform, etc., in the design phase, one has to pay attention to the effect these choices will have on the security

factors of the service. The value of the services for the company is also worth assessing in order to protect the most critical functions at a level they require. For example, protocols using clear text, such as SMTP, POP, IMAP, http, TELNET or SMB, should not be used in network traffic if the transfer of information is confidential and the network is unreliable.

Backup and access control of the data needed to produce the service and the data gained when producing the service should be ensured in order to have the availability of the service at the desired level, and in order to fulfil statutory obligations. When choosing a server platform, i.e. the computer architecture, the operating system and the server program itself, it is good to understand the level of one's own knowledge and skills and to use publicly available knowledge of the platform's security features. The most secure environment will deteriorate in time if it is not appropriately administrated. When designing the entirety of the service, one should pay attention to the fact that as many service parts as possible can be produced with the device and programs according to some standard. Then, a single component is replaceable, perhaps for a more secure component, during the service use. There are implementation-dependent rules and instructions on good administrative manners for servers plugged into a network. These should be followed.

The complexity of the service-producing system is a problem nowadays, so simplifying designs and implementations is worthwhile. Extra features in the devices, operating system and programs of the service platform that are not relevant for the service should be cut down. Unfortunately, many features that increase security, like backup copying, cryptographic protocols, VPN devices and software, and firewalls, as well as antivirus programs, make the system more complicated and thus possibly more vulnerable. The more surfaces attached to the system there are, the easier it is to attack it. An administrator has to know how to act in a fault situation, so understanding the functioning of both the whole assembly and a single component is crucial. Any component whose function is not understood should not be used in the servers. Using a separate test system is to be recommended as the service developers and administrators can there act as they please without jeopardizing the actual system.

When the server is functioning, the administrator has to regularly observe its functioning, for example by detecting log files. In addition, the server component producer's and authorities' announcements, and user community discussions should be followed in order to be aware of the components' manufacturing and security faults. Software and operating system updates should be done routinely, especially concerning servers that are connected to the public network.

The connections between companies in the service production complicate the management of the entirety just like managing the server itself. In case there is a need to

trust the services of a third party, one should be prepared for a failure in these services for one reason or another. For example, there can be sudden disturbances in the Internet provider's data connection, email, or name service, whose effect on business should be inspected in advance. The administrator actions in fault situations should be designed and practiced.

Because a corporation's internal threats should be prepared for as well, the permitted and forbidden actions of a server's and system's legal users and administrators should be in the public domain inside the company. The requirements set by the legislation concerning the handling of personal data and messages, for example, must also be known by the individuals that work with the system and service. If the employees understand their tasks and responsibilities, they are also most likely to notice if someone tries to misuse them. The same goes for the server functions: when the correct functioning of the server is understood well enough, the fault situations can also be detected.

A summary of actions related to protecting servers:

- Choose the protocols providing the service and platform according to one's own knowledge and recommendations by others. Restricting services.
- Protect DNS servers: check the protection of the Internet provider's DNS service.
- Aim to prevent user mistakes concerning server identity. Use server certificates that include a server domain description. Ensure that the user clearly notices which domain's service he is aiming at.
- Data backups. Log file collection.
- Access control and monitoring. Ensure the implementation of a two-way authentication, ssl/tls, passwords.
- Update software regularly.
- Use a security program, like a firewall and an antivirus program.
- Continually monitor and analyse possible threats.
- Manage dependencies and complexity.

4.2.5.2 Intrusion detection practices

Intrusion detection systems are based on a sensor or application listening to a network, server or workstation, and a control system. Usually, the sensor detects all traffic and makes decisions based on known attack patterns or artificial intelligence that studies network behaviour. Attacks based on attack patterns are quite clear and there are action plans for them. Network sensors are becoming more general. Information security software producers integrate IDS features into their own packages.

The control system manages attack patterns and sensor rules. Manufacturers update attack patterns with varying reaction speed, but mostly the update frequency is adequate. IDS analysis and reporting of the whole of computer technology and telecommunications architecture is still challenging and difficult to implement.

In the main, the systems' own management applications only produce very initial analyses of the exceptions to the network events. In most cases the final analysis requires a lot of knowledge in order to interpret the effect the problem has on the environment. Interpreting misuse cases always requires a lot of knowledge on the part of the employees, but managing attacks based on attack patterns is easy. The challenge is still the attacks detected from network deviations. Certain qualities can be analyzed at many points. For example, peer-to-peer connections can be caught in IDS, proxy, antivirus or firewall devices, or some intelligent switch. Then the skill in managing the whole system is emphasized.

Companies and organizations have traditionally used several small-scale attack databases to manage information security threats. This work has perhaps always been frustrating when new attacks have occurred without warning. At the end of March 2005 the large telecommunications companies decided to share information on security attacks in the Fingerprint Sharing Alliance (http://www.arbor.net/). This coalition collects and analyses information on all potential attack attempts and an automatic system warns all the parties as early as possible about denial-of-service attacks, for example (Tietoviikko). A special program in the system monitors the networks and aims at recognizing the peaks, etc., occurring in the traffic that indicates abnormal activity. Abnormal activity is stored as a so-called fingerprint file that can be compared with other attacks.

General approaches for detecting system attacks are:

- Follow unexpected and suspicious events that face the system as well as network traffic in an automatic and systematic manner. Do not forget physical protection and detection if it gets broken. Constantly use other people's observations to complement your own detections and compare them.
- Inspect further if something unusual has occurred in the system. Use previously tested protection mechanisms if you suspect that the system has been broken into. Use your practices if the threats change or your system or its requirements change.

4.2.5.3 Antivirus protection and malware in practice

Malicious software or malware means harmful computer programs. Malicious software can be classified as presented in Table 7 .

Table 7. Malware with related subtypes. Source e.g. [VAHTI 3/2004].

Malware	Sub types/spreading	Basic protection	Significance in digital tv world
Viruses – copy and spread themselves to new targets. **Worms** – (subset of viruses) – spread by deliberately using a network connection.	File viruses – spread in every way that transfers program files.	**Virus scanning** and **deletion**.	Threat in MHP environment (plugin).
	Macro viruses – attach to application documentation files. Spread with the documents regardless of the operating system.	E.g. by **preventing** macros**.**	Not probable. Requires applications utilizing macros, such as office software.
	Command line viruses– utilize scripts in the target system.	E.g. **settings**.	Defective device updates or sets files.
	Email worms – spread in email or its attachments.	Email **scanning**.	Threat to email applications.
	Network worms – independently utilize a network connection.	E.g. **firewalls**.	Threat to return channel.
Trojan horses – secretly perform something unpredicted.	Can open a backdoor on the target computer. Can send information about the computer or user actions forward. Spread with another program.	E.g. user **awareness** in software installations.	Threat to return channel if the user accepts this kind of content.
Spy- and adware	Programs including spy components. The spy feature can be notified, but some are installed secretly – e.g. ADS (Alternate Data Stream) hidden in a txt file.	**Protection programs**, secure **file system** and user **awareness.**	Possible when utilizing Internet contents. MHP includes security mechanisms that make installing these more difficult.
Hoaxes, chain letters and joke programs	Hoaxes waste time, such as having to remove files. Joke programs give false warnings. Spread by unsuspecting users that sent it forward.	E.g. user **awareness**.	Possible when utilizing Internet contents.

The restricted properties of set-top boxes diminish the threat of malicious software on their side. For the time being it is not possible to have a direct connection to another terminal, which effectively prevents the spreading of network worms. Unlike a typical home PC, a set-top box does not usually have several applications running that are connected to the network without the user's knowledge and which malicious programs should contact. Because of the restricted resources of a set-top box, virus protection should occur in the network server, not in the terminal, because of virus update fluency at the very least.

Viruses cause at least indirect damage – they use disk space, cause compatibility problems and slow down devices. They often include programming errors that may cause damage even against the virus programmer's wishes.

A network operator has to protect network interfaces and devices with virus protection programs, but this is not entirely enough, even if a television network is a separate network with access to the Internet in some certain places. A single actor cannot in general take responsibility for the whole information security; effective protection would also require (daily) co-operation between operators, internationally as well.

Network protection can occur by monitoring data transferred by the following protocols: SMTP, POP3, HTTP, TFP, IMAP4, NNTP and SOCKS.

A very important technological protection is the device's memory properties – e.g. closed memory areas from which read/write areas (no execution) cannot be referenced out, only ROM areas, and so on. These require both physical and programming implementations. Because new malware spreads really fast, malicious action in the software should be monitored by antivirus programs that study the program binaries heuristically in addition to just seeking a virus identifier – if a program put in a sandbox tries something irrelevant, it would be revealed as malware and destroyed.

The following actions assist in controlling malicious software protection in service development and production organizations:

- Workstations and servers administration handled by a specialized backup organization that knows all the vulnerabilities. Devices equipped with a malware protection program. Information security update automation and follow-up processes are highly important. Users should have training as well.
- IDS system in a LAN. In addition, critical servers, test and production systems, as well as workstations, of the LAN should be separated into their own segments.
- The LAN has to be separated with malware protection, firewall and router security features at network connection points. Remote connections have to be secured separately.

5. Special characteristics of MHP service development

It is wise to start evaluating the special characteristics of service development from the actors' point of view and the value net they form. The trust relationships between the actors have influence on the services the end user receives. An example of this is contractual trust between the deliverer of a payment system and the operator. Trust relationships are partly formed by doing business as usual; regulation is significantly guiding the actors' role in the digital television world. This is not necessarily visible directly to the service developer or the end user as a very important means of forming trust relationships.

This chapter studies the integration of information security and ease of use, and how they are best implemented from the service developer's point of view. Furthermore, we address all the phases of the service development process, including generation of ideas, design, implementation, testing, deployment and maintenance.

5.1 Trust models

One goal of this document was to clarify how the responsibility in a value net is transferred from one actor to another when moving from the end user's perspective to the beginning of the value net. Finding answers to this question has proved to be significantly difficult as the value net is different in every service, and even in competing (similar) services a totally different business model and actors have been chosen for the implementation. The use of industrial company interviews was not enough to drill into this problem at a satisfactory level because no such industrial case that could have been freely discussed or which all the interviewed persons would have been familiar with at an adequate level could be referred to.

5.2 Building trust

In order to build trust the actors are required to co-operate with each other and to aim at these goals within their own internal processes. For example, 80 % of the information loss is caused by the actions of the users (possibly due to the inadequate amount of information given to them) and only 20 % is caused by information technology [YRTI]. It is clear that to build trust in an organisation attention must be paid to the way in which important data for both the organisation and customers is being stored and how it is distributed. Unclear methods of handling data may cause breaches of contracts or even illegal actions. The malfunctions of systems and networks make their utilization difficult and prevent efficient working. The weakening of usability lowers the service

level and may harm the reputation of the organisation. Even in fault situations the organisation needs to be prepared to maintain the service level necessary for functioning.

The consumers' trust in new electronic banking services is based on several factors [FIBA], for example:

- trust in banks as an institution
- experiences of previous banking services
- functionality of and possible serious problems in banking services
- opinions of other users.

In an international comparison the banks in Finland are highly trusted as a provider of electronic banking services. The consumers' trust in electronic banking services has been built by creating certain ways of actions (payment services, telephone bank), by developing information security and reliability of services, and by informing customers about them.

Many small companies nowadays act as subcontractors to bigger organisations or they are taking part in a service entity formed by several companies. In these kinds of networked business models the information security needs of the most important organisation define the information security level for the whole network [YRTI]. In many cases this so-called leader of the pack audits the security procedures of the other actors. Legislation, authority guidelines and possible agreements, as well as field-specific requirements, also presume that the personnel are aware of the information security responsibilities and procedures how these are carried out in practice. The development of information security must be a part of the organisation's strategic planning and goal setting. Furthermore, the organisation must have a defined information security policy and practical guidelines for implementing it.

The users' and other actors' trust in taking part in the service development for a chosen service concept can be raised by using known reference implementations and the best tools, applicable methods and standards as a basis for the product. Well-designed and communicated pilot projects and the use of known test beds also increase trust.

The value net and revenue logic of each actor should be clear from the beginning of the service development. The end-user should also be aware of which actors profit when the service is used and how this profit is shared. It must be noted that for an actor in the network the added value could be increased fame or marketing put into practice through a service or pilot.

It is good to notice that the value nets and revenue logics are still often immature. In such cases a special effort must be made to clarify them throughout the whole process.

Technological factors for building trust:

- Reliable identification of the user and service.
- Use of a well-known service platform to ensure the purity of the distributed contents.
- Reliability and security features of the network technology and terminal devices.
- It is good practice to use tested technologies.

Other trust-related factors:

- Using certified products and professionals.
- Existing services, previous good image and reputation and privacy/data protection of the organisation
- Reliable actors, subcontractors, use of trustworthy third party – for example information security audit statements.
- Positive images of other users.

The whole service can collapse if the chosen technology is not mature enough for commercial use or if it restricts the functionality in the future. Consumers can reject the service if it involves threats such as malware or unreliable technical function (including information systems and systems).

5.3 General issues in service development

5.3.1 Stakeholders – value net

The number of actors, their interdependencies and the complexity of the business models influence the methods and even the service development process of the application developer. MHP applications are typically linked to other distribution services, such as games, events and other applications, and the service offered to the consumers is aggregated by combining these services. The roles of the actors are ambiguous – for example in Finland the television channels that act in the role of the integrator often have the roles of service developers and content producers as well. This is why the description of a value net is always bound to the service and the point of view. A digital television world value net from the MHP service provider's point of view is presented in Figure 10.

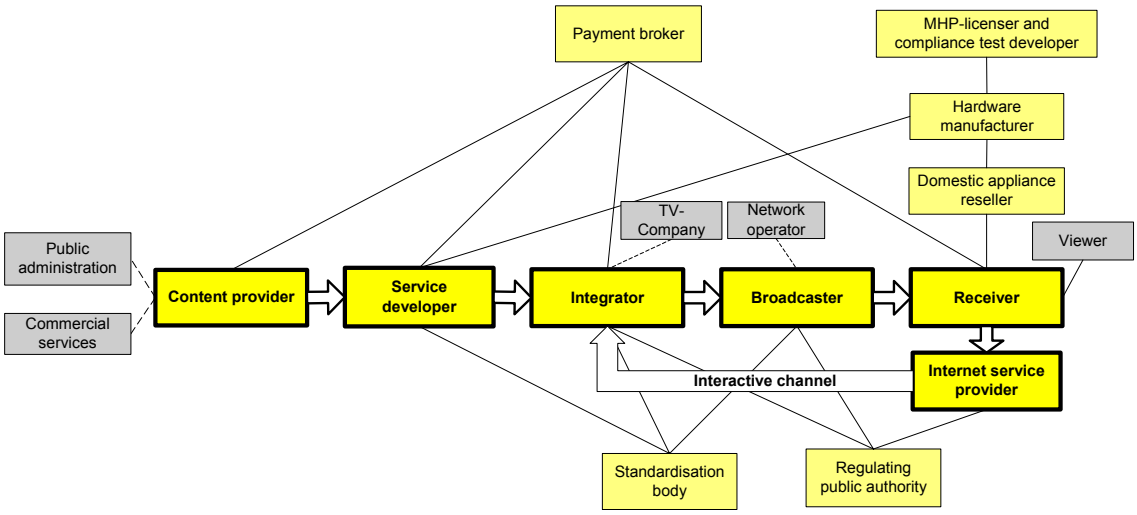


Figure 10. The value net of digital television.

In Figure 11 the value net is examined from the MHP service developer's point of view and some actors relevant to the service development process are added. The service producer and the integrator are directly related to the service developer's process. In addition to them, a highly important component for information security, a subcontractor, is part of the figure. The service developer must know their product development processes and their methods in cases violating information security. Standardisation organisations, device manufacturers and other component developers related to the service are all making certain demands on the service development process and the service being developed.

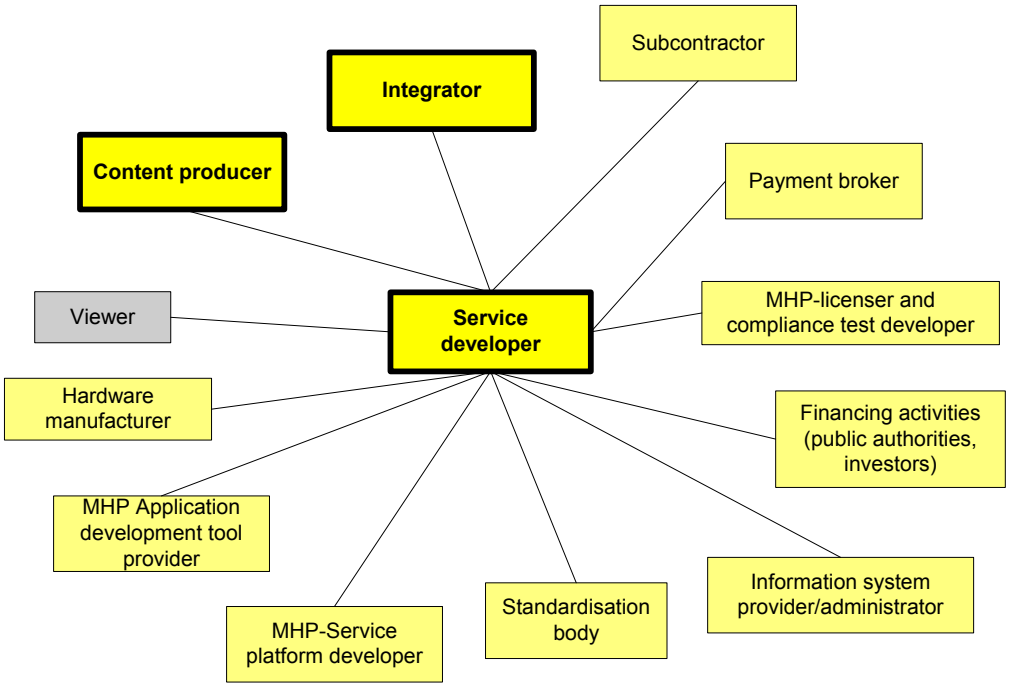


Figure 11. The value net of an MHP service developer.

5.3.2 Customer orientation

In the case of interactive television, customer (viewer) orientation means as usable and standardized interfaces as possible. Underlying technical solutions and information security mechanisms do not concern the customer until something goes wrong. In practice nothing of the end user's technical level can be assumed due to the heterogeneity of the customers. The end user is not interested in the technical solutions but the fact the expected goods have been received. The customer expects he will get the service he has paid for. The service must correspond to what the service provider has promised and it must not disturb other services in the device. In this the service vendor is guided by the regulations and thus has a big responsibility. Consumer Protection Legislation and the Data Protection Act are strict, and they protect the consumer. Interactive applications in the digital television world also give access to electronic commerce. In this case the consumer is in the same situation as the customer ordering goods from the Internet, and the end user must also realize the risks associated with credit card payments. End user behaviour can be guided towards safer actions with a good service interface design. These include, for example, certificate acceptance and payment transactions.

5.3.3 Information security orientation

The information security orientation in an organisation can for example be composed of risk management, strategic planning and resource allocation. In practice this can mean

- protecting your own network
- closing the development environment and/or test network partly or totally
- finding good actors, checking the information security level of different actors
- inspecting the delivery chain (from who and how each component has been acquired, etc.).

5.4 Service development process

A predetermined process is often followed when developing electronic services. Service development consists of different phases, each of which has its own defined goals and methods. In practice this almost always creates some kind of management problems – for example what would be the proper process description for developing just this kind of service and how do different actors communicate and what information do they transfer? In practice various issues may proceed along an unplanned route, so the process is just an aid helping to understand the big picture.

Even if the service development process is very well defined it is crucial to remember that it can never take all the information security factors into account due to change over the course of time. Given this factor, one cannot think that information security has already been taken care of. New threats and means must always be taken into consideration within different phases of the process. The process itself does not protect from all threats. An example of the phases of the service development process according to the LUOTI programme is presented in Figure 12.

Figure 12. An example of the phases of the service development process [LUOTI].

In this document the phases of the service development process are

- generation of service ideas/concept
- service design
- service implementation
- service testing
- service deployment
- service maintenance
- service enhancing
- service terminating.

5.4.1 Information security solutions within the development process

The most important solutions in different phases of the service development process are shown in Table 8.

Table 8. The most important solutions in different phases of the service development process. Explanation: ● = generally, ○ = possibly.

	Solutions	Main threat	Phase							
			Generation of service ideas/concept	Service design	Service implementation	Service testing	Service deployment	Service maintenance	Service enhancing	Service terminating
Content protection in service	Restriction of media redistribution.	Copyright violations.	○		●		●	●	●	
	Encryption of saved data.	Device- and user-related threats.	○	○	●	●	●	●	●	●
	Digital signature and verification of the programs.	Origin and integrity-related threats	●		○	●	●	●		
Attack protection in service	Interface to electronic payment system.	Payment-related threats.	●	●	●	●	●	●	●	●
	Privacy protection.	Identification and data confidentiality-related threats.		●		●	●	●	●	●
	Server protection.	Network and server-related threats.					●	●	●	●
	Intrusion detection.	Network and server-related threats.				●	●	●	●	
	Protection against malware.	Device-related threats.		●	●	●	●	●	●	
Service developer's information security process	Third party evaluation methods.	Service development process-related threats.	●		●	●			●	
	Risk management.	Service development process-related threats.	●	●	●	●	●	●	●	●
	Physical security solutions, e.g. back ups, tamper-resistant HW	Service development process-related threats.		●	●	●	●	●	●	●
	Recovery planning.	Service development process-related threats.		●	●	●	●	●	●	
	CERT activity.	Service development process-related threats.		○	●	●	○	●	○	○
	Version management.	Service development process-related threats.		●	●	●	●	●	●	
	Information security in business management.	Service development process-related threats.	●				●	●	●	
	Technical process follow up, improvement and training.	Service development process-related threats.		○	●	●	○	○	○	

A more detailed Table (threats found in each development phase) is presented in Appendix B.

5.4.2 Generation of a service idea/concept

A service idea can often be generated by the content producer, service distributor or, of course, the service developer itself. These actors have responsibility for their own products and their quality. When generating ideas one has to consider what actors are needed for the best service generation. Other actors, such as integrators (for example, television channel) and various authorities and research institutions, can contribute ideas. It is useful to find out in the generation phase which industry and service standards exist and how they could be used. Solutions outside the standards often result in a dead end while the service expands. From the information security point of view, the standard solutions known by most actors are best. These standard solutions are reliable and feasible for subcontractors.

The use of information security experts, such as consultancies, is often very useful in the early phases of the service development process; identifying the main threats in a new service (system view), the most important security solutions at issue and an assessment of their realisation could be part of the consultancy assignment.

The main issue in practice is the product/service development environment risk management and life cycle – for example in which phase or period of time the risk may become real. The service quality and robustness is tested at the end.

An example of the idea generation phase actions:

- Create a threat analysis, define the target group and service accurately.
- Define interfaces; which issues can become threats (and how).
- Create a threat tree (root causes).
- Define which threats can realize in practice; do we have resources to protect from them?
- Manage risks.
- Assess the protection costs compared with the value of the property/information protected.
- Make preliminary plans for all the processes included in the development.

5.4.3 Design

If the service development does not require the design or implementation of a technology (for example a protocol), the focus be set on the service mapping. This mapping can include preliminary studies on the kinds of pilot projects that have been made, who has been involved and the kinds of experiences that have been gathered.

This serves in setting up the development environment. It also helps to foresee the restrictions of some tools for a particular service implementation. Some tools may provide insufficient information security features, such as an unpatched protocol or algorithm. It is also important to define in advance what user groups will be using service. This clarifies the criteria for the ease of use (for example the parameters and settings for the information security features), which is important, especially for the targeted service.

An MHP service can be implemented in many ways. The service can be a browser-based service without a return connection or one using the return channel. In the latter case the service is implemented by using the available Xhtml editors. Typically, the browser and the development environment of the terminal are made by the same manufacturer. Creating this kind of service does not require programming; most of the work is designing the interface. The service deployment may require Java programming and the use of different MHP standardised computer program libraries. Tools for developing Java-based MHP services are available. The programming must be phased beforehand to include the business planning, the requirement specification, and the implementation plans, as well as the deployment and testing plans concerning the service. All this can be very service-specific, but from the information security point of view should be always included in all the design phases. The information security testing or auditing of the development environments and documents should also be planned in some way.

Information security should be taken into account at the very beginning of the service design when the idea generation phase has produced the service concept. In this phase the information security demands should be noted – for example what kinds of identification systems are needed, is there any need for encrypted connections, how the user rights are managed and how the saved data is protected. In this phase it must be clear what kind of data the service will handle and what protection requirements exist according to the legislation. The components related to information security are identified and planned with the rest of the system.

5.4.4 Implementation

Different implementation alternatives are evaluated and the best of them are selected in the service implementation phase. The actors for the technologies being used are also selected. Information security is a fairly new issue in the implementation of digital television services because the interactive services are not developed on a very large scale. An appropriate development history creates the basis for implementing new services. This is not typically the case in implementing MHP service information security.

A clear process must be used in the service implementation. This process can be owned by either the producer or the customer (for example device manufacturer) and applied to the service in question. The process must be proved to be secure under all circumstances in advance.

5.4.5 Testing

Versatility and comprehension are the most important issues in testing. The testing conceptualization from many different angles supports the reliability of the programs and the systems. This means, for example, that both static and dynamic analyses of the program should be used. The program should be seen as both an open and closed system focusing on the structure of the source code as well as the compiled program's operation in respect of its environment. The acceptance tests should also focus on testing unspecified actions in addition to the correct operation of the program.

The scope of the testing should be evaluated with consideration of the set of states and code base of the program when possible. The evaluation should also include the normal function of the program when the system is strained. Such strain can cause denial of service or enable attacks due to the non-atomicity of the operations.

The importance of interface testing is emphasized in the network environment. To ensure the input correctness from the environment the program is tested with both legal and totally false, malicious inputs. In other words, reliability tests are run in the environment interfaces in addition to integration tests. When iterating the program, regression tests are very important so that old faults will not reappear when the code is renewed.

The so-called conformance test is a special feature of MHP application testing. Detailed test cases for the conformance test have been defined by the MHP standardising organisation. At the moment, this testing process is very simple: the MHP-compatible device's developer acquires the test library and required documents from ETSI and carries out the tests itself. After successful testing, the developer can claim the right to use the MHP logo in its product. It must be noted that this kind of consistent testing process does not exist for applications.

In the implementation and testing phases of the service the planned information security solutions are coded according to good and secure coding principles and the code is reviewed and tested extensively. Vulnerability tests should also be carried out and their results analyzed.

5.4.6 Deployment

Service deployment is a critical phase from the end user's point of view. The end user may have to download a program to his terminal or have to adjust some device settings in order to use the service. In the future, more and more practices and applications must be built to enable the user to change and adjust his device settings automatically. This is a serious problem from the information security point of view because settings defined by a single actor may inhibit the user from using some other services. This is why the

network operator is a centric actor concerning service settings. The interface between network services and other services has blurred. This can cause problems in the relationships between the service provider, the network operator and the end user.

The significance of service marketing will become more versatile. A marketing message about a service content or usage may also affect information security due to the attitude the user has adopted. The service provider's commitment to the service also heavily affects the information security the end user perceives. If the use of services is not continuous or the operations are not run professionally, the user's expectations are not met and he may lose some valuable information accumulated in the service, even though he has relied on its durability.

5.4.7 Maintenance

The development of technical solutions has become more complicated as the development pace has accelerated. This combination is hard to manage. As a consequence, products and services may have shortcomings and faults that cause vulnerabilities in them. By vulnerability is meant a fault in a program or device that may originate from the design, implementation, deployment or maintenance phase and which may enable unjustified use of them. Unjustified use can mean unauthorized use of data or disturbance of centric processes. Human errors, incorrect development processes or similar management problems can cause vulnerabilities [Arbaugh 2000]. Information sources for preventing vulnerabilities can be found through SANS (SysAdmin Audit Network Security Institute), http://www.sans.org.

By vulnerability handling process is meant the entity of actions regarding program and device development. This entity covers the whole (program or device) life cycle from findings to correction. Three main actors are primarily involved in vulnerability handling [Laakso 1999]

- the party who has found the vulnerability
- the party who is responsible for correcting the vulnerability, for example the manufacturer
- the party co-ordinating or steering the handling process.

The handling process starts when the vulnerability is found. The fault is evaluated and if it is found to be real, it is reported to the co-ordinator and manufacturer. Both of them evaluate the finding and summarize it. If the vulnerability is found to be a real threat, preparations for a patch release are started. This point of view has later been expanded [Havana 2003] to take account of the fact that there are a great number of stakeholders

who has impact on it. These include subcontractors, retailers, insurance companies, media, educational institutions, legislative bodies and standardisation parties.

So far the interviews with digital television stakeholders have revealed that it has been difficult to define the actors who participate in the vulnerability process. No clear convergent view has emerged up to now. More information gathering is needed to square this matter. In the maintenance phase the information security actions are usually reactive: the vulnerability in a service may also result from the service or program settings. This slows down the commencement of the patch process. The proactive way to avoid program vulnerabilities in the maintenance phase is to design the system to be as simple as possible. In addition to that, the components of the system must be easily updated. The administrator must also note that separate information security products and features increase complexity in a system.

The authorities co-ordinating the vulnerability process (in Finland CERT-FI of the Finnish Communications Regulatory Authority) make the reporting and patching process of vulnerabilities easier with their own contribution. They have existing communication channels to the right stakeholders and they can support the smooth success of the process as they are independent organisations.

5.4.8 Enhancing a service

Service enhancement can be due to several reasons – for example increasing the number of service users or altering the service expectations. One reason can be that the service has only just been piloted and it is now supposed to be developed to production use due to positive experiences. This may cause a need to alter the service architecture. In practice this can mean that it must be possible to use the service in the devices using the new MHP standard in addition to the old MHP1.0.2 devices. In such a case the architecture design phase must be revised to verify which assumptions have changed compared with the new standardized version. At the same time, the future capacity needs have to be considered. The capacity of servers or applications, as well as the sufficiency of information security services, can cause problems in the old architecture.

Although problems in the pilot phase may not have been detected, an increase in the number of users and a new user's different attitude can become a factor that must be taken into account in advance in the next service phase. The developers or other actors, such as the network operator and the service operator, should be able to help in these cases. The need for further service development may also result from copyright violations that are only noticed when the service has been deployed for some time. These violations are not necessarily noticed unless the full information gathering and monitoring capacity of the network is used.

In the Service enhancement phase one must take care that the information security level achieved in the design and implementation phase is not weakened by choosing new and inadequately tested components for the new version of the service or by making alterations without a proper change management process. In this process the changes must be documented, tested and approved before they are implemented in production.

5.4.9 Terminating a service

When terminating a service the questions related to customer information security are emphasized. These can include:

- Do the customer records have to be destroyed or transferred?
- How is the customer record transfer done securely?
- Are the customers dependent on some information maintained by the service or of the service itself directly or indirectly?

Other issues that have to be taken into account from the information security point of view are:

- Is the data on attacks or attempted attacks during the service recorded somewhere and is it exploitable?
- Are the passwords and other information security management-related data deleted appropriately?

Various authority requirements on the deletion of stored data also have to be taken into account when terminating the service. These requirements should be written down during the design phase of the service. They also should be included in the information security policy of the service administrator.

References

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

[ArviD] Digi-tv:n paluukanava. ArviD publication 01/2005. http://www.arvid.tv/micaj_storage/EB0A30B34658E20BDAFC4AD09BC660C0/29/ArviD-2005-01_Digi-tv_n_paluukanava.pdf. (In Finnish.)

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

[ArviD3] A Guide for Digital TV Service Producers. ArviD publication 02/2004. http://www.arvid.tv/micaj_storage/3BF719B821575D8EBD59497ADE7D55B8/29/ArviD-2004-02_A_Guide_for_Digital_TV_Service_Producers.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/english/

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

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

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

[FICORA2] Vuorovaikutteisen kanavan toteutusmahdollisuuksista digitaalisessa televisiojärjestelmässä. DVB-MHP-ryhmän paluukanavaraportti 4/2005. http://www.ficora.fi/suomi/document/TRaportti042005.pdf. (In Finnish.)

[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. Presented at: Cybersecurity Reseach and Disclosure Conference, Stanford, Palo Alto, USA, November 2003. 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. 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. (In Finnish.)

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

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

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

[Södergård 1999] Södergård, C., Ollikainen, V., Mäkipää, R. 1999. Digitaalisten televisiolähetysten käyttö datajakelussa. Espoo: VTT. VTT Tiedotteita – Meddelanden – Research Notes 1971. 69 s. + liitt. 3 s. ISBN 951-38-5458-2; 951-38-5459-0. http://www.inf.vtt.fi/pdf/tiedotteet/1999/T1971.pdf. (In Finnish.)

[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. (Finnish Information Society Development Centre Publications.) http://www.arvid.tv/micaj_storage/28C400A89D4F6673ED7D42DCC800612A/29/julksarja12.pdf. (In Finnish.)

[Tietoviikko2004] http://www.tietoviikko.fi/doc.ot?d_id=124100. (In Finnish.)

[VAHTI 3/2004] Haittaohjelmilta suojautumisen yleisohje. VAHTI 3/2004. http://www.vm.fi/tiedostot/pdf/fi/88078.pdf. (In Finnish.)

[YLE TK-Lehti] http://www.yle.fi/tekniikka/tklehti/. (In Finnish.)

[YRTI] “Tietoturvalliseen tietoyhteiskuntaan.” Yritysten tietoturvatietoisuus – työryhmän raportti, 21.2.2005.
http://www.mintc.fi/oliver/upl263-Ty%C3%B6ryhm%C3%A4n%20raportti%2021.pdf.
(In Finnish.)

Web references

About vulnerabilities on content formats and web contents:

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

About vulnerabilities on Java platform and X.509 implementations:

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

About safe programming procedures:

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

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

Further information:

LUOTI program:
http://www.luoti.fi

Ministry of Transport and Communications:
http://www.mintc.fi

Appendix A: Questions in industrial interviews

General questions

What is the company's view on threats and problems?

From a service developer's point of view, what kind of mobile/digital television services-related threats to e-trade do you see?

Integratability and ease-of-use of security.

What common objectives do you see for ease-of-use of security? From the viewpoint of a service provider, how could the objectives be reached? What kinds of problems are related to that?

About Solutions

Do you reduce threats by "avoiding" certain functions? How? What functions do you need to avoid?

Minimizing threats. What actions have you taken to ensure that a certain threat is realized as rarely as possible, and to minimize consequences if it is realized?

Transferring or dividing threats via agreements – typical agreements are, for example, subcontracts. Which threats have been avoided by taking out insurances against them?

Accepting certain strategic threats, and keeping the risk as one's own responsibility, are there threats you see as necessary for your business (you may have special knowledge on coping with them), and want to keep the threats as your own responsibility?

What kind of plans do you have in case a threat is realized? How do you recover quickly and ensure as good a continuity of business as possible?

Questions concerning longer term solutions:

How do you keep track of the above actions?

Responsible persons? Have you thought about whose responsibility area the threats belong to? Are the allocated resources adequate (for example, usually the person responsible for security technologies has no time to be responsible for threats regarding operations)?

How do you identify new threats?

How do you inform about threats and respective actions?

Is there enough information to identify and assess threats?

Do we understand the risk level (that the people responsible accept) that remains beyond control?

Do you have (practically controllable) security objectives?

Do you regularly assess objectives and threats?

The parties and processes related to service development

The following questions about value chains were used when discussing steps in the service development process (research, development, testing, implementing, taking into use, maintenance):

Which parties participate in developing the service idea/service concept? Process?

Which parties participate in developing the service? Process?

Which parties participate in implementing the service? Process?

Which parties participate in testing the service? Process?

Which parties participate in taking the service into use? Process?

Which parties participate in maintaining the service? Process?

Which parties participate in developing the service further? Process?

Which parties participate in ending the service? Process?

Technological application areas

What technical appliances/systems do you feel you are dependent on? (What appliances/ systems can you not manage without?) Why?

In your opinion, what are the most critical communication protocols related to mobile telecommunications? Why?

> (A figure with a set of protocols is shown to the interviewee. The interviewee can choose the most critical ones or propose protocols not in the figure.)

In your opinion, which currently used protocols most clearly form a joint between the IP and the GSM worlds?

In your opinion, which are the most important IP-based protocols that are used in mobile devices and mobile networks?

Where do you usually get information regarding security vulnerabilities?

What do you do when a vulnerability is found? What kind of vulnerability process do you have? Describe.

> (The interviewee is presented with a sketch of a general level diagram depicting parties participating in the vulnerability process. The interviewee is asked to concretize which parties he feels work in each role in practice.)

In your opinion, which direction are we heading in? For example: what functionalities/applications are to be taken into use in the near future?

Which protocols will be the most significant? Why?

Will the significance of some protocols decline in the future? Why?

Appendix B: Threats found in each development phase

Table B1. Identified threats in each development phase.

To simplify this table the actors' lack of knowledge and rapid changes in the industry have been excluded as information security threats because they affect almost all process phases and stakeholders.

Development phase	Threats	Legal actors who could cause the threat in question with their operations
Generation of service ideas/concept.	Too small scale net of actors.	service provider
	Data eavesdropping, unauthorised use or manipulation of data.	new service developers
Service design.	Data eavesdropping, unauthorised use or manipulation of data.	new service developers, integrator
	Viruses, malware.	new service developers
Service implementation.	Actors are of a different level.	software developer, integrator, new service developers, service development environment providers
	Data eavesdropping, unauthorised use or manipulation of data.	content provider, software developer, integrator, new service developers
	Integrity of the service development platform (integrity, stability).	service developers, service development environment providers
	Attacks, programming faults, wrong technical choices or development tools, complexity or false settings concerning the service or device.	software developer, integrator, service developers, service development environment providers
	Rights to use and copying contents (such as video and audio).	content wrapper, integrator, service developer, service provider
	Viruses, malware.	new service developers, service development environment providers
Service testing.	Actors are of a different level.	integrator, new service developers and service providers
	Integrity of the test platform.	test environment provider
	Viruses, malware.	integrator, test environment provider
Service deployment.	Data eavesdropping, unauthorised use or manipulation of data.	service operator, network operator
	Attacks, programming faults, wrong technical choices or development tools, complexity or false settings concerning the service or device.	service provider, service developer, service operator, network operator, marketing syndicates
	Identification, confidentiality of the user's identity.	service provider, service developer, service operator, network operator
	Distribution of the confidential data on the user.	service operator, network operator
	Confidentiality of the profiling data on the user.	service operator, network operator
	Rights to use and copy content (such as video and audio).	service provider, service developer, service operator, marketing syndicates
	Viruses, malware.	service provider, service developer, service operator, network operator
Service maintenance.	Data eavesdropping, unauthorised use or manipulation of data.	consumer, service operator, network operator
	Integrity of the production platform.	service operator, service developer
	Attacks, programming faults, wrong technical choices or development tools, complexity or false settings concerning the service or device.	consumer, service provider, service developer, service operator, network operator
	Identification, confidentiality of the user's identity.	consumer, service provider, service developer, service operator, network operator
	Distribution of the confidential data on the user.	consumer, service provider, service operator, network operator

Development phase	Threats	Legal actors who could cause the threat in question with their operations
	Confidentiality of the profiling data on the user.	consumer, service provider, service operator, network operator
	Rights to use and copy content (such as video and audio).	consumer, content wrapper, service provider, service operator
	New kinds of use and operating situations.	consumer, service provider, service developer, service operator, network operator, marketing syndicates
	Unauthorised use of the service at the expense of another customer (fraud), theft of the device.	consumer, service provider, service operator, network operator
	Denial of the service by oversupplying, denying the traffic, spamming.	consumer, service provider, service operator, network operator
	Devices and programs are incompatible.	consumer, service provider, service developer, service operator, network operator
	Viruses, malware.	consumer, service provider, service developer, service operator, network operator
	Risks to electronic payments, non-reputation, forged service pages.	consumer, service provider, service developer, service operator, network operator, payment broker
Service enhancing.	Data eavesdropping, unauthorised use or manipulation of data.	software developer, integrator, new service developers
	Integrity of the service development platform (integrity, stability).	service developers and service development environment providers
	Attacks, programming faults, wrong technical choices or development tools, complexity or false settings concerning the service or device.	software developer, integrator, service developers and service development environment providers
	Distribution of the confidential data on the user.	service provider, service operator
	Rights to use and copy content (such as video and audio).	content wrapper, integrator, service developer, service provider
	Viruses, malware.	new service developers, service development environment providers
Service terminating	Actors are of a different level.	service provider, service operator
	Attacks, programming faults, wrong technical choices or development tools, complexity or false settings concerning the service or device.	consumer, service provider, service operator
	Identification, confidentiality of the user's identity.	consumer
	Distribution of the confidential data on the user.	service provider, service operator

Published by

Series title, number and report code of publication

VTT Research Notes 2306
VTT–TIED–2306

Author(s)
Holappa, Jarkko, Ahonen, Pasi, Eronen, Juhani, Kajava, Jorma, Kaksonen, Tiina, Karjalainen, Kati, Koivisto, Juha-Pekka, Kuusela, Erno, Ollikainen, Ville, Rapeli, Mikko, Sademies, Anni & Savola, Reijo

Title

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.

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 television, multimedia, data transfer, information security, authentication, user identification, privacy, terminals, intrusion detection, virus protection

Activity unit
VTT Electronics, Kaitoväylä 1, P.O.Box 1100, FI–90571 OULU, Finland

ISBN			Project number
951–38–6733–1 (soft back ed.) 951–38–6734–X (URL: http://www.vtt.fi/inf/pdf/)			E5SU00588
Date	Language	Pages	Price
September 2005	English, Finnish abstr., Swedish abstr.	81 p. + app. 4 p.	B
Name of project		Commissioned by	
LUOTI		Ministry of Transport and Communications of Finland	
Series title and ISSN		Sold by	
VTT Tiedotteita – Research Notes 1235–0605 (soft back edition) 1455–0865 (URL: http://www.vtt.fi/inf/pdf/)		VTT Information Service P.O.Box 2000, FI–02044 VTT, Finland Phone internat. +358 20 722 4404 Fax +358 20 722 4374	

Julkaisija

Julkaisun sarja, numero ja raporttikoodi

VTT Tiedotteita 2306
VTT–TIED–2306

Tekijä(t)
Holappa, Jarkko, Ahonen, Pasi, Eronen, Juhani, Kajava, Jorma, Kaksonen, Tiina, Karjalainen, Kati, Koivisto, Juha-Pekka, Kuusela, Erno, Ollikainen, Ville, Rapeli, Mikko, Sademies, Anni & Savola, Reijo

Nimeke

Digi-tv:n tietoturvauhkat ja -ratkaisut
Palvelunkehittäjän näkökulma

Tiivistelmä

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

Tutkimusmenetelminä ovat olleet kirjallisuushaut, asiantuntijoiden näkemykset, yrityshaastattelut sekä laaja-alaiset kommentointikierrokset.

Digitaalinen konvergenssi tuo monipuolistuvia palveluita digi-tv-maailmaan. Vuoro-vaikutteiset 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 erityis-piirteet: arvoverkot ja erilaisten infrastruktuurien turvallinen yhdistäminen.

Koska Multimedia Home Platform (MHP) on paluukanavan ohella tärkeimpiä interaktiivisen television mahdollistavia teknologioita, se saa tässä julkaisussa 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
digital television, multimedia, data transfer, information security, authentication, user identification, privacy, terminals, intrusion detection, virus protection

Toimintayksikkö
VTT Elektroniikka, Kaitoväylä 1, PL 1100, 90571 OULU

ISBN			Projektinumero
951–38–6733–1 (nid.) 951–38–6734–X (URL: http://www.vtt.fi/inf/pdf/)			E5SU00588
Julkaisuaika	Kieli	Sivuja	Hinta
Syyskuu 2005	Englanti, suom. tiiv., ruots. tiiv.	81 s. + liitt. 4 s.	B

Projektin nimi	Toimeksiantaja(t)
LUOTI	Liikenne ja viestintäministeriö
Avainnimeke ja ISSN VTT Tiedotteita – Research Notes 1235–0605 (nid.) 1455–0865 (URL: http://www.vtt.fi/inf/pdf/)	Myynti: VTT Tietopalvelu PL 2000, 02044 VTT Puh. 020 722 4404 Faksi 020 722 4374

Utgivare

Seriens namn, nummer och rapportkod

VTT Meddelanden 2306
VTT–TIED–2306

Författarna
Holappa, Jarkko, Ahonen, Pasi, Eronen, Juhani, Kajava, Jorma, Kaksonen, Tiina, Karjalainen, Kati, Koivisto, Juha-Pekka, Kuusela, Erno, Ollikainen, Ville, Rapeli, Mikko, Sademies, Anni & Savola, Reijo

Namn

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.

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 terminal-utrustningens 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 television, multimedia, data transfer, information security, authentication, user identification, privacy, terminals, intrusion detection, virus protection

Verksamhetsenhet
VTT Elektronik, Kaitoväylä 1, PB 1100, 90571 ULEÅBORG

ISBN			Projekt nummer
951–38–6733–1 (häftad) 951–38–6734–X (URL: http://www.vtt.fi/inf/pdf/)			E5SU00588
Datum September 2005	Språk Engelska, finsk ref., svensk ref.	Sidor 81 s. + app. 4 s.	Prisgrupp B
Projektets namn LUOTI		Uppdragsgivare Kommunikationsministeriet	
Series namn och ISSN VTT Tiedotteita – Research Notes 1235–0605 (häftad) 1455–0865 (URL: http://www.vtt.fi/inf/pdf/)		Försäljning VTT Informationstjänst PB 2000, 02044 VTT Tel. växel 020 722 111 Fax 020 722 4374	

As a service environment, digital television places very high requirements on the usability and information security solutions of services.

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.

Special emphasis in this publication 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. 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.

Tätä julkaisua myy

VTT TIETOPALVELU
PL 2000
02044 VTT
Puh. 020 722 4404
Faksi 020 722 4374

Denna publikation säljs av

VTT INFORMATIONSTJÄNST
PB 2000
02044 VTT
Tel. 020 722 4404
Fax 020 722 4374

This publication is available from

VTT INFORMATION SERVICE
P.O.Box 2000
FI–02044 VTT, Finland
Phone internat. + 358 20 722 4404
Fax + 358 20 7226 4374

ISBN 951-38-6733-1 (soft back ed.)
ISSN 1235-0605 (soft back ed.)

ISBN 951-38-6734-X (URL: http://www.vtt.fi/inf/pdf/)
ISSN 1455-0865 (URL: http://www.vtt.fi/inf/pdf/)