SECURITY THREATS TO DIGITAL TELEVISION PLATFORM AND SERVICE DEVELOPMENT

Jarkko Holappa, Reijo Savola
VTT Technical Research Centre of Finland, Kaitoväylä 1, FIN-90570 Oulu, Finland

Keywords: Digital television, MHP, security threats, digital convergence.

Abstract: Digital convergence is introducing more diverse digital television services. The return channel, which enables interactive television, is a 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. Multimedia Home Platform (MHP) 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. Threat analysis presented in this paper is carried out in Finnish companies that include digital-TV broadcasters, MHP-platform developers, service developers and telecom operators.

1 INTRODUCTION

As a service environment, digital television places very high requirements on the usability and information security solutions. 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, the consumers' trust in the new media is not increased by inconsistent practices in software updates of terminal devices, carried out other than within the program stream.

The trend for digital convergence is also present in digital television solutions – 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.

The goal of this study is to increase awareness of information security threats connected with digital television in different phases of the service development cycle. Focus is on security solutions with the Multimedia Home Platform (MHP) and a return channel. The research methods employed in this study include interviews with Finnish and European industrial companies, literature searches and extensive rounds of commentary among experts of the domain area. A more complete discussion of the interview results is presented in (Holappa *et al*. 2005).

2 DIGITAL TELEVISION TECHNOLOGIES

Digital television in Finland and most of the Europe is based on the DVB (Digital Video Broadcasting) standards (DVB 2005). 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. Audio and video is encoded in the broadcast system and combined into one MPEG2-bitstream in a multiplexer (ISO/IEC IS 13818-1, 2000).. One bit stream is known as multiplex. In addition to audio, video and signaling information, it is possible to transfer data using Internet Protocol based services (Södergård 1999), (FICORA).

Holappa J. and Savola R. (2006).
SECURITY THREATS TO DIGITAL TELEVISION PLATFORM AND SERVICE DEVELOPMENT.
In *Proceedings of the Eighth International Conference on Enterprise Information Systems - ISAS*, pages 508-515
DOI: 10.5220/0002493505080515

2.1 Multimedia Home Platform

At the moment, MHP (Multimedia Home Platform) (ETSI 2002) based services are broadcast in Germany, Italy and Spain, of which Italy is considered the frontrunner in the introduction of MHP services. MHP pilot projects and declarations of supporting MHP are being made in almost every European country.

MHP is an open standard and defines a general purpose interface between interactive applications and digital television 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 (ETSI 2002).

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 Table 2.

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

Table 2: MHP Profiles.

MHP Profile	Description
Enhanced broadcast	The profile was made to comply with many existing middleware systems and receivers without a return channel.
Interactive services	This profile includes receivers that have return channel capabilities. It is possible to download applications from the DVB stream. Interactive behaviour is also supported in the application programming interfaces.
Internet access	The most advanced profile in the MHP standard. 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.

2.2 Digital Television Receivers

The most important factor in interactive service popularization is that terminals, in other words set-top boxes, become more general. 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.

2.2.1 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. 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 only a maintenance company or the equipment

manufacturer can restore it. Distributing erroneous software updates on purpose can also be considered a threat if the attacker is able to falsify the broadcast with another transmitter.

3 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 (ArviD).

3.1 Programme Guide

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 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.

3.2 Super Teletext

Super teletext is a renewed version of the old teletext. The user interface is super teletext browser, 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.

3.3 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.

3.4 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.

3.5 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. In the future, 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.

4 INFORMATION SECURITY THREATS TO DIGITAL TELEVISION

In this section, we present a threat analysis concentrating on security threats to digital television world based on previous studies and industrial interviews. These threats 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. Table 3 depicts this division along with simple examples in each category and affected technologies.

Table 3: Examples of the threats against different targets.

Threat target	Example	Related technologies
Transmission network/ terminal device	Downloaded faulty software update (containing e.g. software bugs or being damaged during transportation).	DVB, MPEG-2
Transmission network/ terminal device	A program signal contains errors that the set-top box is not able to handle or fix.	DVB, MPEG-2
Return channel	Downloaded malware to terminal device and its execution in full access privileges because of the lack of certificate checks.	MHP, IP, content formats
Service development process	Inadequate testing of software components Interopearability problems between different versions of software	Development tools

4.1 Threats to Transmission Network and Terminal Devices

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 almost 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 (Coded Orthogonal Frequency Division Multiplexing) 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 sending flawed data during an update of system programs. Using device protection mitigates this threat – 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 devices 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, digital television environment will become closer to the Internet environment 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 and adding potential security threats due to false interpretations.

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

4.2 Management of Return Channel and Threats due to Digital Convergence

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 HTTPS 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. 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 web 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.

5 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 (Holappa *et al.* 2005) 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

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 or European legislation concerning information security in the world of digital television. 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 and the regulations concerning electronic commerce.

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.

6 CONCLUSIONS

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.

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.

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.

ACKNOWLEDGEMENTS

The authors acknowledge a debt of gratitude to the LUOTI programme (Development Programme on Trust and Information Security in Electronic Services) of Finnish Ministry of Transport and Communications (MINTC) for funding. Ms. Päivi Antikainen of MINTC and Mr. Kimmo Lehtosalo of Eera Finland are acknowledged for helpful comments and fruitful discussions, as well as all the co-authors and interviewees of the study behind this article – Their contribution to this work has been essential.

REFERENCES

A Guide for Digital TV Service Producers. ArviD-publication 02/2004.

Digital Video Broadcasting (DVB) Project (2005). At: http://www.dvb.org.

ETSI TS 101 812 (2002): Digital Video Broadcasting – Multimedia Home Platform (MHP) Specification,, 757 p.

Holappa J., Ahonen P., Eronen J., Kajava J., Kaksonen T., Karjalainen K., Koivisto J.-P., Kuusela E., Ollikainen V., Rapeli M., Sademies A. and Savola R. (2005): Information Security Threats and Solutions in Digital Television – the Service Developer's Perspective. VTT Research Notes 2306, Espoo 2005. 81 p. + app. 4 p.
http://www.vtt.fi/inf/pdf/tiedotteet/2005/T2306.pdf

ISO/IEC IS 13818-1 (2000): Information Technology – Generic Coding of Moving Pictures and Associated Audio Information – Part 1: Systems. International Standards Organisation (ISO).

Södergård, C., Ollikainen, V., Mäkipää, R. (1999). Digitaalisten televisiolähetysten käyttö datajakelussa. Espoo: VTT. VTT Tiedotteita – Meddelanden – Research Notes 1971. 69 p. + app. 3 p.. http://www.inf.vtt.fi/pdf/tiedotteet/1999/T1971.pdf (in Finnish).

The Finnish Communications Regulatory Authority (FICORA).
http://www.ficora.fi/englanti/radio/digitv.htm Tietoviikko 2004.http://www.tietoviikko.fi/doc.ot?d_id=124100 (in Finnish).