ESPOO 2005 VTT RESEARCH NOTES 2308

Pasi Ahonen, Juhani Eronen, Jarkko Holappa, Jorma Kajava, Tiina Kaksonen, Kati Karjalainen, Kaarina Karppinen, Mikko Rapeli, Juha Röning, Anni Sademies, Reijo Savola, Ilkka Uusitalo & Timo Wiander

Information security threats and solutions in the mobile world

The service developer's perspective

VTT TIEDOTTEITA – RESEARCH NOTES 2308

Information security threats and solutions in the mobile world

The service developer's perspective

Pasi Ahonen, Juhani Eronen, Jarkko Holappa, Jorma Kajava,
Tiina Kaksonen, Kati Karjalainen, Kaarina Karppinen, Mikko Rapeli,
Juha Röning, Anni Sademies, Reijo Savola,
Ilkka Uusitalo & Timo Wiander

VTT Electronics

ISBN 951–38–6737–4 (soft back ed.)
ISSN 1235–0605 (soft back ed.)

ISBN 951–38–6738–2 (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

Ahonen, Pasi, Eronen, Juhani, Holappa, Jarkko, Kajava, Jorma, Kaksonen, Tiina, Karjalainen, Kati, Karppinen, Kaarina, Rapeli, Mikko, Röning, Juha, Sademies, Anni, Savola, Reijo, Uusitalo, Ilkka & Wiander, Timo. Information security threats and solutions in the mobile world. The service developer's perspective [Mobiilimaailman tietoturvauhkat ja -ratkaisut. Palvelunkehittäjän näkökulma. Hot och lösningar beträffande mobilvärldens informationssäkerhet. Serviceutvecklarens perspektiv]. Espoo 2005. VTT Tiedotteita – Research Notes 2308. 95 p. + app. 4 p.

Keywords information security, threats, wireless telecommunication, mobile services, mobile networks, mobile devices, authentication, identification, privacy

Abstract

This study examines the major information security threats relating to mobile services and solutions to these threats from the service developer's perspective. Research methods employed include interviews with enterprises, literature searches, expert opinions and extensive rounds of commentary.

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

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

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

Ahonen, Pasi, Eronen, Juhani, Holappa, Jarkko, Kajava, Jorma, Kaksonen, Tiina, Karjalainen, Kati, Karppinen, Kaarina, Rapeli, Mikko, Röning, Juha, Sademies, Anni, Savola, Reijo, Uusitalo, Ilkka & Wiander, Timo. Information security threats and solutions in the mobile world. The service developer's perspective [Mobiilimaailman tietoturvauhkat ja -ratkaisut. Palvelunkehittäjän näkökulma. Hot och lösningar beträffande mobilvärldens informationssäkerhet. Serviceutvecklarens perspektiv]. Espoo 2005. VTT Tiedotteita – Research Notes 2308. 95 s. + liitt. 4 s.

Avainsanat information security, threats, wireless telecommunication, mobile services, mobile networks, mobile devices, authentication, identification, privacy

Tiivistelmä

Tässä julkaisussa kartoitetaan mobiilimaailman tärkeimmät tietoturvauhkat ja niiden ratkaisut palvelunkehittäjien näkökulmasta. Kartoituksen tutkimusmenetelminä olivat yrityshaastattelut, kirjallisuushaut, asiantuntijoiden näkemykset ja laaja-alaiset kommentointikierrokset.

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

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

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

Ahonen, Pasi, Eronen, Juhani, Holappa, Jarkko, Kajava, Jorma, Kaksonen, Tiina, Karjalainen, Kati, Karppinen, Kaarina, Rapeli, Mikko, Röning, Juha, Sademies, Anni, Savola, Reijo, Uusitalo, Ilkka & Wiander, Timo. Information security threats and solutions in the mobile world. The service developer's perspective [Mobiilimaailman tietoturvauhkat ja -ratkaisut. Palvelunkehittäjän näkökulma. Hot och lösningar beträffande mobilvärldens informationssäkerhet. Serviceutvecklarens perspektiv]. Espoo 2005. VTT Tiedotteita – Research Notes 2308. 95 s. + app. 4 s.

Nyckelord information security, threats, wireless telecommunication, mobile services, mobile networks, mobile devices, authentication, identification, privacy

Abstrakt

I utredningen beskrivs de viktigaste hoten mot informationssäkerheten i mobilvärlden och lösningar på hoten ur serviceutvecklarens perspektiv. Som forskningsmetoder användes företagsintervjuer, litteratursökningar, expertutlåtanden och en omfattande insamling av kommentarer.

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

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

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

Preface

This report, which addresses security threats and solutions in the mobile world, 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 Transportation and Communications published in Finnish in June 2005. The report has been made from the service developer's perspective.

The goal of the study is to increase awareness of information security threats connected with mobile services and their possible solutions in different phases of the service development cycle. We also aim 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 has been done by a group of network and information security researchers at VTT and the University of Oulu, managed by Mr. Pasi Ahonen of VTT. The research methods include industrial company interviews, literature surveys, experts' views and iterative analysis. The work has been supervised by Mr. Kimmo Lehtosalo of Eera Finland Oy and Ms. Päivi Antikainen of Finnish Ministry of Transportation 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 the valuable comments from Mr. Juha Perttula (Ministry of Transportation and Communication), Mr. Janne Uusilehto (Nokia Plc.), Mr. Kari Oksanen (Nordea Bank Finland Plc.), Mr. Marko Koukka (TeliaSonera Finland Plc.), Mr. Simo Niklander and Mr. Göran Schultz (Oy L M Ericsson Ab), Mr. Jari Råman (University of Lapland), Mr. Erno Kuusela, Prof. Juha Röning and Mr. Marko Laakso (University of Oulu), Dr. Marko Helenius (University of Tampere), Prof. Heikki Ailisto and Ms. Ritva Poikolainen (VTT).

Oulu, Finland, September 1st, 2005

Reijo Savola

Network and Information Security Research Coordinator

VTT Technical Research Centre of Finland

Executive summary

New forms of electrical communications have emerged in recent years. Services with new functionalities such as Bluetooth, WLAN, localization, music, camera, and video can be used with mobile phones and PDA devices. Data services with a connection to networks such as the Internet are especially plentiful. This trend is opening up new business opportunities for the industry. However, it is also bringing new challenges for information security management.

This report, ordered by the Finnish Ministry of Transportation and Communications (MINTC) in early 2005, includes an analysis of the most important information security threats and solutions from the service developer's perspective. The report is part of MINTC's LUOTI programme. LUOTI is a development programme on Trust and Information Security in Electronic Services, which aims to promote information security in new multi-channel electronic services.

The main observation from this report is to realise that mobile services include security threats and they should be taken seriously. However, security threats should not be considered a barrier to the development and deployment of new services. The security threats should be analysed and solutions found in the early stages of the service development process. Good state-of-the-art methods and solutions applicable to the mobile environment are already in existence. However, guidelines concentrating on human interaction and security management processes are almost non-existent.

The threats found in this research were categorised as mobile network, mobile device, convergence, authentication and payment threats, and service development threats. We do not address all security threats to mobile services, but concentrate on the most important ones concerning service developers. The major threats from this perspective are

- the large number and complexity of service platforms and products
- unauthorised copying of service content and programs
- the variety and insufficient level of information security management practices of the stakeholders that are part of the service development
- Internet security threats, such as denial of service attacks, that are more and more being directed towards mobile devices
- threats connected to user and service authentication and users' privacy.

In addition, the following are seen as potential threats:

- low end users' (consumers') ability to manage service and device configuration settings, and validate the trustworthiness of these settings

- low end user and service developer know-how and ability to track the evolution of the field
- new technologies and ways of using of products and services that turn out to be insecure because they have not been tested in the mobile environment
- unauthorised use of services causing expense for a customer – e.g. deliberate unauthorised use of mobile phone services resulting in an increase in phone bills
- malware, such as viruses and worms, are likely to become common in mobile devices too
- usability problems of mobile payments and uncertainty in making big purchases.

Our goal was to identify and analyse solutions to the above-mentioned security threats. These solutions were divided into three groups: content protection, protection against attacks, and the service developer's information security management process. The relationship of each solution to the information security and threat classifications was analysed.

The most important technological solutions in *content protection* include

- restriction of media distribution in order to prevent unauthorised copying and encryption of saved data
- digital signing of content and verification of certificates in order to ensure origin and integrity.

The major technological solutions for *protection against attacks* address the following:

- user authentication and identification in electronic payment systems
- protection of user privacy in many ways
- resource protection (like server protection), intrusion prevention and detection, anti-virus protection and configuration management.

The following issues were connected to the *service developers' information security management process*:

- risk management and third-party assurance
- physical security solutions and resilience, and its planning
- CERT activity, version control systems, information security in business management
- monitoring, improvement of processes and training.

When investigating these solutions one must be aware that each service requires a separate security analysis and the solutions mentioned in this report are only meant to be

examples of solutions to threats. In the following we delineate key solutions for mobile service security in more detail.

There are no widely approved standards on *restriction of unauthorised content distribution* in multi-channel distribution. This fact prevents effective business because there is no "Power Distributor" that could realise the protection of different kinds of content in the distribution net. For example, the protection of games is laborious because games are often implemented separately to each platform (such as PDA devices, Java mobile phones, Symbian mobile phones and operator-dedicated mobile phones).

Protection of user identity and privacy. User identity and privacy protection are not often considerable problems in network connections due to SSL/TLS encryption and PKI methods. However, implementation of encryption might be difficult in the cheaper mobile phones due to capacity restrictions. There are still problems in server identification that are connected to the trustworthiness of DNS servers and their communication. Fortunately, new solutions like DNSSEC are emerging. It is possible that a mobile device can receive a virus or another kind of malware that can cause the user identity to be used in an incorrect way. Anti-virus software can be used to protect mobile devices from these kinds of attacks. User identity and privacy should also be protected when a service is discontinued or moved to another platform. This can be done by destroying customer databases or by processing them in an appropriate manner during the transfer.

Nowadays it is still difficult to protect against *attacks targeted at servers* and, especially, excess load due to unnecessary service requests. It is especially difficult to protect against a planned and Distributed Denial of Service (DDoS) attack. Consequently there is need for better server programs, more secure development processes, intrusion detection and prevention systems, and capable people. The users should be informed beforehand how passwords are going to be managed by the service providers and operators. Moreover, the users should be informed beforehand that passwords are not to be disclosed by phone or email under any circumstances, not even to a person who introduces himself or herself as representative of the service provider.

Ease of use increases the level of security. The service should be planned in such a way that the user is able to understand all actions that are required from him or her during the use of the service. Use of built-in intuitive logic helps the user to notice if something unusual is going on (e.g. extraordinary delay or indefinite response). In this case the user has a better chance of detecting an attack targeted at the service or a malfunction.

Easy-to-use security should be integrated everywhere in networks, devices and the net of stakeholders. Technological solutions should be adaptable to different kinds of business processes, so that they can be reused and the whole system does not need to be replaced by a new one during a change of business.

Service development process

It is highly important to take information security into account in all phases of the service development process. In this report we deal with the service development process by focusing on the role of information security at each stage of the process. All technical and process-oriented information security solutions handled in the report are mapped to different phases of service development. Most of the security threats and their solutions require actions in most of the phases of the service development process.

A common problem in service development is the lack of security awareness and know-how. This is partly due to the fact that real threats are dependent on the service to be developed. A requirement for comprehensive information security management is that the threats and solutions connected to the service under development are addressed in time. This includes, e.g., the software development practices used and to be applied, and how the development environment is protected.

Risk management and life cycle management are essential in the information security management of a product and service development environment. It is important to realise when risks can come true. In order to include the whole value net of service development in the security management, it is important to analyse subcontractors' processes and test the quality and robustness of the service well in advance of the introduction of the service.

Contents

Abbreviations and terminology

2G	GSM (in Europe)
2,5G	GPRS (in Europe)
3G	3rd Generation of Mobile Communication (especially UMTS)
3GPP	3rd Generation Partnership Project. A standardisation body.
802.11	IEEE's WLAN standard family, evolving
A3	An authentication algorithm for mobile device (GSM)
A5	An encryption algorithm for air interface (GMS)
A8	A key generation algorithm for air interface (GSM)
A-GPS	Assisted Global Positioning System. A network-assisted GPS positioning system.
AAC	Advanced Audio Coding. An audio compression standard.
AES	Advanced Encryption Standard. A novel standard for encryption.
AKA	Authentication and Key Agreement. A protocol that is used for mutual identification of the network and USIM card of mobile phone.
AMR	Adaptive Multi Rate. A standard for voice compression.
ATM	Asynchronous Transfer Mode. A switching network.
AuC	Authentication Center (GSM). A mobile network node that carries out authentication activities.
BG	Border Gateway (GPRS)
BS	Base Station (UMTS)
BSC	Base Station Controller (GSM)

BT	Bluetooth. A wireless short-range radio technology (10 m).
BTS	Base Transceiver Station. A base station for GSM.
CA	Certification Authority
CDM	Contract Design Manufacturer
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.
CG	Charging Gateway (GPRS)
CN	Core Network (UMTS)
COMP128	A secretly developed algorithm that can be used as an identification algorithm for a mobile device and a key generation algorithm for air interface.
CPU	Central Processing Unit
CRL	Certificate Revocation List
CUE	Consistent User Experience
DB	Database
DM	Device Management (OMA). A device management standard.
DNS	Domain Name System (UMTS, IP). A name server.
DNSSEC	DNS Security Extensions
DRM	Digital Rights Management. A method for controlling the distribution of electronic content.
DSCP	Differentiated Services Code Point

EAP	Extensible Authentication Protocol. A standard for enhancing the interoperability of authentication methods.
EDGE	Enhanced Data GSM Environment (GPRS)
EEPROM	Electrically Erasable Programmable Read Only Memory
EIR	Equipment Identity Register (GSM). IMEI codes of mobile phones are stored in EIRs at the national level.
FTP	File Transfer Protocol
FW	Firewall. A firewall is a software or device that controls traffic coming into a device and leaving from it.
GAP	Generic Access Profile (Bluetooth). GAP defines the general functions for Bluetooth device discovery and link management.
GEA	An algorithm for GPRS air interface encryption that is similar to the A5 algorithm of GSM.
GGSN	Gateway GPRS Support Node. A gateway between a GPRS network and an outside network (e.g. the Internet).
GIS	Geographic Information System
GPRS	General Packet Radio Service. A packet-switched information transfer service in a GSM network.
GPS	Global Positioning System. A satellite positioning system.
GSMA	SGM Association
GTP	GPRS Tunnelling Protocol
H.263	A video compression standard by ITU-T
H.264	A video compression standardised by the ITU-T and ISO/IEC MPEG groups in co-operation
HIP	Host Identity Protocol

HLR	Home Location Register (GSM)
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
I/O	Input/Output
ICAO	International Civil Aviation Organization
ICT	Information and Communications Technology
ID	Identity
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IKE	Internet Key Exchange. A key exchange protocol that is used for the IPSec security protocol.
IMAP4	Internet Message Access Protocol version 4. An email protocol.
IMEI	International Mobile Equipment Identity (GSM)
IMS	IP Multimedia Subsystem (UMTS)
IMSI	International Mobile Subscriber Identity (GSM)
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.
ISIM	IMS Subscriber Identity Module
ISM	Industrial, scientific and medical radio frequencies
ISO	International Organization for Standardization
IST	European Commission's Information Society Technologies programme
ITU	International Telecommunications Union
LAN	Local Area Network
LIG	Lawful Interception Gateway (GPRS)
LUOTI	Development Programme on Trust and Information Security in Electronic Services (in Finnish *Luottamus ja tietoturva sähköisissä palveluissa*) of the Finnish Ministry of Transportation and Communication
MD5	Message Digest 5. A checksum algorithm that generates a 128-bit checksum of the input. The input cannot be unveiled from the checksum.
MeT	Mobile electronic Transactions
MINTC	Ministry of Transportation and Communications of Finland
MMC	MultiMediaCard. A common memory used in mobile phones.
MMS	Multimedia Messaging System. A multimedia messaging system.
MP3	MPEG-1 Audio Layer-3. An audio compression standard.
MPEG-4	A video standard collection by ISO/IEC Moving Picture Experts Group
MPLS	Multiprotocol Label Switching
MS	Mobile Station. A wireless mobile device of GSM.

MSC	Mobile services Switching Centre (GSM)
NAT	Network Address Translation. Translation of an IP address of a network into an IP address of another network.
NIST	National Institute of Standards and Technology. An American standardization body.
NNTP	Network News Transfer Protocol. A protocol for the distribution, request, fetching and sending of news articles through a secure network connection.
ODM	Original Design Manufacturer
ODRL	Open Digital Rights Language
OMA	Open Mobile Alliance. A standardization body for mobile applications.
P-TMSI	Packet-Temporary Mobile Subscriber Identity (GSM)
PAN	Personal Area Network, e.g. Bluetooth
PCMCIA	Personal Computer Memory Card International Association
PDA	Personal Digital Assistant
PGP	Pretty Good Privacy. A common encryption program for email.
PIN	Personal Identification Number (GSM)
PKI	Public Key Infrastructure
PLMN	Public Land Mobile Network
POP3	Post Office Protocol version 3. An email protocol.
PSTN	Public Switched Telephone Network
PUK	Personal Unblocking Key (GSM). PUK is used in opening a locked SIM card.

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. RAM is read and write memory.
RAN	Radio Access Network (UMTS)
RFID	Radio Frequency Identification. An identification method using radio frequencies.
RNC	Radio Network Controller (UMTS)
ROM	Read Only Memory
RPC	Remote Procedure Call. A protocol that is used for inter-process communication between two target systems.
RTP	Real-time Transport Protocol. A protocol for real-time data (audio, video, music) transfer in packet switched networks.
S/MIME	Secure Multi-Purpose Internet Mail Extensions. A protocol meant for email protection.
SAML	Security Assertion Markup Language. A protocol for the transfer of user information.
SANS	SysAdmin Audt Network Security Institute
SATU	Electronic Identifier in HST (in Finnish *Sähköinen henkilöllisyyden tunnus*)
SC	Smart card
SD	Secure Digital
SGSN	Serving GPRS Support Node. SGSN routes data packets from mobile devices from GGSN and vice versa.
SHA	Secure Hash Algorithm. A checksum algorithm that generates a fixed-length checksum of input. The input cannot be revealed using the checksum.

SIM	Subscriber Identity Module (GSM). A smart card for user identification.
SIMPLE	SIP for Instant Messaging and Presence Leveraging Extensions
SIP	Session Initiation Protocol. A signalling protocol for starting and ending multimedia sessions.
SMB	Server Message Block. A network file system developed by Microsoft.
SMS	Short Message Service (GSM)
SMTP	Simple Mail Transfer Protocol. An email transfer protocol.
SSH	Secure Shell. A protocol for securing remote connections and data transfer.
SSID	Service Side Identifier. An identifier used for connection to a WLAN server.
SSL	Secure Sockets Layer. An encryption protocol.
SW	Software
SWIM	WIM module integrated into a SIM card
SyncML	Synchronization Markup Language. A language for data synchronization between devices, information networks and platforms.
TCP	Transmission Control Protocol. TCP is responsible for communication connection between two user devices, packet structuring and retransmission of lost packets.
TELNET	An Internet protocol for remote connections
TETRA	Terrestrial Trunked Radio. A radio communication standard for professional use.
TLS	Transport Layer Security. An encryption protocol.

TMSI	Temporary Mobile Subscriber Identity. A temporary subscriber identifier used for identity protection during the transfer of subscriber information.
UDP	User Datagram Protocol. UDP is responsible for communication connection. UDP is lighter than TCP and does not structure or retransmit lost packets.
UE	User Equipment
UMTS	Universal Mobile Telecommunications Service. 3rd generation mobile communications technology.
USB	Universal Serial Bus. A serial bus architecture for connection of peripheral devices.
USIM	User Services Identity Module (UMTS). "SIM card" in UMTS.
VAHTI	Finnish Government Information Security Management Board (*Valtionhallinnon tietoturvallisuuden johtoryhmä*)
VIRVE	Finland's public authority network
VLR	Visitor Location Register (GSM)
VoIP	Voice over IP. VoIP refers to voice transmission in data networks using Internet protocol.
VPN	Virtual Private Network. A solution that allows the organisation's intranet to be extended securely over an unsecured public network such as the Internet.
VRK	Finland's Population Register Centre (in Finnish *Väestörekisterikeskus*)
WAP	Wireless Application Protocol
WCDMA	Wideband Code-Division Multiple-Access. A key technology for the realisation of 3G systems.
WEP	Wired Equivalent Privacy. An outdated encryption system in WLAN networks.

WiFi	Wireless Fidelity. A WLAN system conformable to 802.11.
WIM	WAP Identity Module
WLAN	Wireless Local Area Network
WPA	WiFi Protected Access. An encryption system for WLAN networks. WPA was developed to fix security holes in WEP.
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

Mobile devices are using more and more services that utilise Internet connections and the services therein. This and other trends connected with Digital Convergence increases the complexity of systems and information security threats to mobile users and services. The Finnish Ministry of Transportation and Communications (MINTC) has considered these phenomena worthy of research by investigating the major information security threats to the mobile world and the solutions to them. This investigation concentrates on service development creating new business opportunities.

This report is part of MINTC's LUOTI programme. LUOTI is a development programme on Trust and Information Security in Electronic Services that aims to promote information security in new multi-channel electronic services. In addition, LUOTI aims at increasing information security awareness in the whole service development net. The general goals of this study are the following:

- Concentration on electronic services.
- The phases of the service development process are addressed.
- Realistic information security risks and threats are identified.
- Realistic solution possibilities are found for the identified threats.
- Views are created on information security issues in multi-channel distribution: Digital TV, the Internet and mobile networks.
- To investigate how information security ease of use could be implemented by the service developer.

1.2 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 to protect against threats and damage caused by hardware and software faults, 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 is limited to a set of authorised users, and access by or disclosure to unauthorised users is prevented.

- *Integrity* – the 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* – the information and services connected to them are available to authorised users.

In addition, the following security functions are essential for the 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, or a 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 a 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

As part of this study, several industrial companies operating in Finland in the field of electronic services were interviewed (March to April, 2005) based on the Question List in Appendix A. The purpose of the questions was to ignite informal conversation. The

most important individual question was: “What information security threats do you think there are to mobile services as electronic business?”

The interviews were carried out anonymously because the goal was to achieve answers that are as open as possible, without concealing problems.

The major contributions of the interviews for the study were:

- In the future, threats will concentrate on mobile devices rather than services because the protection of mobile devices cannot be carried out so well as the protection of networks and servers. The regulatory responsibility of service providers and network operators does not solely protect mobile devices – after all, the consumer is responsible for the secure use of his/her device. However, the responsibilities depend on the business model.
- The technological complexity of services causes major problems for the quality and information security because there is not enough time for product and service development. In many cases information security has not been taken into account in an adequately early phase of development.
- From the service provider’s point of view, unauthorised copying and distribution of files and programs of the service are big and difficult problems.
- Many Internet threats will target mobile services in the future.
- New stakeholders open business-wise interesting opportunities for service development.

2. Brief technological overview

2.1 A short description of the IP world

Since the beginning of the 1990s the Internet protocol-based system solutions have been widely used in information transfer. The Internet protocols main advantages are scalability, independency of the physical network and reliability of the routing model. The Internet consists of joined IP networks and connecting a physical device to the Internet means that it is connected to the network using an IP protocol as a network layer for information transmission. A device connected to the Internet receives an IP address, which does not have to be global but is an address of a local network. The physical transmission path can be any connection, such as ISDN, ATM, GPRS or UMTS. Nowadays so-called all-IP networks are widely discussed because even the phone networks are adopting IP-based solutions.

TCP or UDP protocols are used for information transmission in IP networks. These protocols, together with other protocols, form the so-called TCP/IP protocol family. Various different service protocols can be built using these protocols. These services include routing techniques, network administration, transmission of network packets, directory services, authentication, management of network devices, information transmission, e-mail services, web page delivery, delivery of audio and video, management of service quality, management of IP calls and so on. These protocols are rarely visible parts of the services; they usually act as supporting resource.

From the ordinary users' point of view the most important services on the Internet are web browsing and communication services such as e-mail, news groups and instant messaging. The proportion of web browsing is clearly over-emphasized. Browsers are used for handling various passive and active contents and, for example, the bank, commerce and official services are transferred to the network. The importance of the Internet will grow in the future as a growing number of activities are transferred to the network. For example, some pilot projects on voting by using the network have already been made. IP calls and various one-way and interactive video and audio services are also gaining popularity.

2.1.1 Threats to the Internet world

Despite its advantages, the TCP/IP protocol family is not very resistant by design. It has been designed to cope with hardware failures but not to act against attacks inside the network. In the design phase of TCP/IP it was assumed that all the devices in the network can be trusted, so security issues were left out. Some of the common threats related to the Internet world are classified in Table 1.

Table 1. Threats to the Internet world. References i.e. [Garfinkel] and [wwwfaq].

Reason	Internet threat
Unreliable action by the user	The **user name – password** guessing by using dictionaries.
	Eavesdropping on the unsecured connections in order to gather user names, passwords or other sensitive information.
	Social engineering attacks in order to gather sensitive information (for example asking for passwords on the phone).
	Active content and plug-ins in web browsers can cause crashes, information leakage, spreading of viruses and malware, dialers calling to expensive foreign numbers, and privacy violations.
Insufficiencies of the network or the system (even the user can be involved)	**Faked network addresses** in order to access sensitive information or avoid identification methods.
	Connection hijacking in order to access sensitive information or break in.
	Spoofing in order to defame the sender or break into the system.
	Breaking into the system by taking advantage of the vulnerabilities in network programs.
	Denial-of-service attacks, especially distributed attacks made with several devices.
	Attacks against the DNS service, for example inserting faked information into the server cache, flooding it with faked replies or completely hostile DNSs.
	Resource-consuming spam, choking of the systems with a large amount of traffic, **forged messages** or header information and **distribution of malware**.

IP standards are still being developed but unfortunately this can also cause security problems. Several experimental techniques have been introduced to production and are being used in a way they were never meant to. In addition to increased reliability, the distributed management and routing techniques can also transfer faults to a widespread area. The burden of history is that IP networks were originally designed to be totally open.

Later on, several techniques were introduced to prevent IP-related risks. Firewalls and NAT techniques withstood them. NAT (Network Access Translation) hides the local network so that outsiders only see the traffic flowing to and from one address. NAT also allows non-routable addresses and thus mitigates the problem of IPv4 public addresses running out. Other tools used in patching the problems in protocols are various filters, such as content-sensitive firewalls and spam filters. These techniques also have their downsides as they violate the basic idea of IP networks, thus creating obstacles in program and service development. These faults in the protocol family are patched in the new standards, IPSec and IPv6, which are already being used in UMTS networks. IPv6 is expanding intensively in China, Japan, South Korea and Taiwan.

The threats existing in the Internet are more and more often possible in the mobile world as well. Because of this, the development of the information security situation must be followed in mobile networks and services.

2.2 On state-of-the-art mobile networks

The most important existing mobile services consist of the following groups:

- speech, SMS messages
- entertainment services (video, music and audio, ring tones, pictures, chat, games, etc.)
- utility services (news, weather, banks, event calendars, parking fees, corporate applications, etc.)
- public services (e.g. publications from authorities, end user services)
- mobile solutions of traditional industry (remote steering, information gathering, monitoring, etc.).

See also e.g. [Alahuhta]. The lifespan of a mobile phone is rather short nowadays. This gives device manufacturers and service developers good possibilities to implement new technologies enabling new services for end users. These services can be colour displays, cameras, and audio and music properties that can be easily utilized in various services or applications. More often, a mobile phone and a PDA are used as an Internet terminal.

In Finland, the current mobile networks include for example:

- GSM (voice calls, SMS messages, GSM data)
- GPRS (data services, including EDGE modulation)
- TETRA (VIRVE – the authority network)
- UMTS (voice calls and music, pictures, video – that is, data as a whole).

At the moment, WLAN networks cannot be considered as a basis for new mobile networks in Finland. This is due to the very limited network coverage, for example.

2.2.1 GSM and GPRS networks

The GSM network:

The GSM network is very well known because it has been implemented almost all over the world. Thus GSM security-related information is widely available, so it is not comprehensively explained here. The most important GSM security components are described very briefly below. General information about GSM can be found in [3GPP] and [GSMA].

The Wireless terminal is in the user's possession and consists of a phone and a smart card (SIM). The SIM enables electronic user identification regardless of the phone in use because the user identifier, IMSI (International Mobile Subscriber Identity), is on the SIM. The SIM card can be protected with PIN and PUK codes. If a PIN is entered incorrectly three times in a row, the card will be locked and can only be opened with a PUK code.

A Base station sub system routes the radio connection to the terminal.

The main component of a **switching sub system, MSC** (mobile service switching center), takes care of connecting calls. The HLR (home location register) has information on all subscribers to this GSM network as well as the current location of the user, which is usually given as a VLR (visitor location register) address. The VLR includes all the necessary information on all users in the GSM network to allow routing the calls to the users. The EIR (equipment identity register) is a database where all the relevant phones in the network might be added based on the IMEI code. The AuC (authentication center) has user's secret key information based on IMSI. This information is used in user identification and in aerial encryption.

There are many structural information security problems in a GSM network. The most common of these are introduced in Table 2 [Vesanen].

Table 2. Most common information security problems in a GSM network (simplified), some of which can be fixed afterwards [Vesanen].

Type	GSM information security problems
Identity, identification	User can't distinguish a false base station so, in principle, he can be fooled into using one set up by an attacker.
	The use of IMEI code as a means of increasing security is problematic (in practice many phones can have the same IMEI code during the manufacturing process).
	A COMP128 algorithm weakness enables exposure of the secret key in an attack against the SIM card.
Encryption	Encryption keys and data used for identification are sent unencrypted within and between networks, thus a lot of trust in the operator's security is required.
	Weaknesses in aerial encryption. Data is encrypted only until the base station. The A5-algorithm is not strong enough as it is and many networks use a weakened version or no encryption at all.
Integrity	Data integrity is not checked (unless implemented at an upper level).
Information availability	Lack of transparency: User cannot see if encryption is in use. The home network does not receive any acknowledgement if the service network uses the identification parameters correctly or not while the user is moving.
Maintenance	Inflexibility. It is hard to implement the updates for security functions even if vulnerabilities are known.

GPRS network:

Due to inefficient data transmission in a GSM network, a packet switched solution, GPRS, has been designed. With GPRS, connecting to packet switched IP networks as the Internet becomes easier and the data transmission rate becomes faster. GPRS is based on GSM technology so the base architecture is same as in a GSM network but the most important new components are SGSN and GGSN. Speech is still transmitted along the same path as in GSM networks but the GPRS data is transmitted by SGSN, which is connected to GGSN via the GPRS base network. The basic structure of a GPRS network is presented in Figure 1.

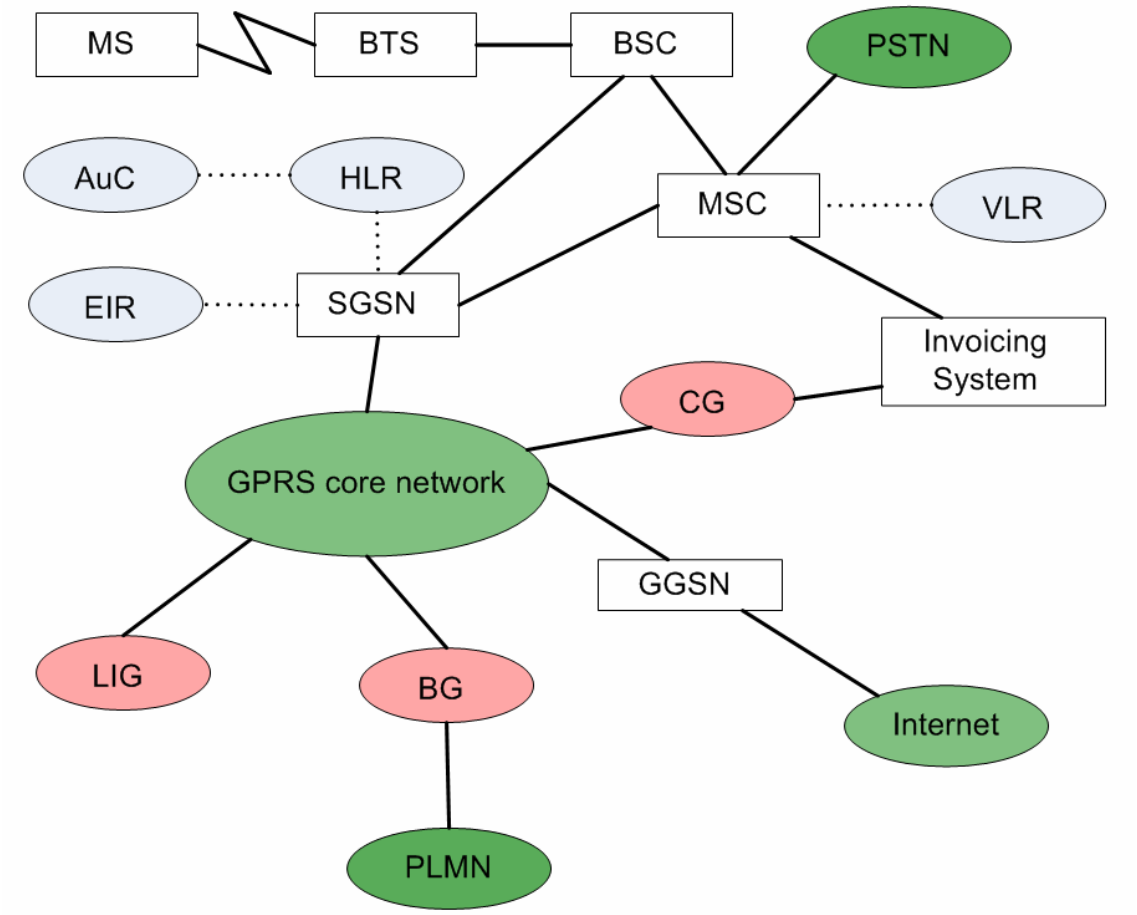

Figure 1. Basic structure of a GPRS network [Vesanen].

SGSN – among other things, identifies the user, maintains location information and produces data for invoicing.

GGSN – handles connections to external packet networks, such as the Internet. BG acts as an interface to external networks, is logically part of GGSN, and its main purpose is to allow travel between the networks.

CG – collects data from the GPRS network for invoicing and redirects it to the invoicing system.

LIG – for example, GPRS data coming from a certain device can by court order be redirected to an archive where police can read it through LIG.

There are many new threats appearing in GPRS networks due to the packet switching core network that can connect to the external packet networks. Some of the most common information security threats in a GPRS network are presented in Table 3.

Table 3. Some of the most common information security threats in a GPRS network.

Type	Information security threats in a GPRS network
GSM threats	**Almost all the same threats as in a GSM network**. Improved aerial encryption all the way to SGSN and a new encryption algorithm GEA.
System intrusion	An attack against the firewall or the NAT used to protect the GGNS.
Internet junk data, denial of service	An attack where the attacker sends junk data to find out which ports the devices are communicating with and then forges the IP packets. A hostile Internet server can send junk packets to a client to a certain TCP or UDP port.

GTP (GPRS Tunneling Protocol), used for routing the packets, can transfer various protocols of packet networks. Furthermore, GGSN does not necessarily filter the user layer traffic directed to the core network. All the interfaces to the external networks must be equipped with firewalls at least.

2.2.2 TETRA network

TETRA (Terrestrial Trunked Radio) is an open digital radio network standard for professional use. It can be used for implementing special features needed by various organization level communication data, such as efficient and fast group calls, prioritizing calls and emergency calls. A TETRA network can transfer speech and data (for example SMS message and packet data).

TETRA networks are suitable for demanding professional use, such as authorities, public transportation organizations and production plants. The Finnish authority network VIRVE (in Finnish *viranomaisverkko*), which is based on TETRA, is primarily used by the State and municipality safety authorities. More details on the VIRVE network in [VIRVE].

2.2.3 UMTS network

At the beginning of 2005 UMTS networks were commercially available in 33 countries and the number of networks was 64 [3GCO]. UMTS subscribers are increasing by about 2 million per month, the total number being about 20 million. Most of the UMTS networks have been built in Asia, for example Japan. In Finland UMTS only covers the biggest cities. Figure 2 shows a simplified model of a UMTS radio network and its connections to the operator core network via SGSN and the interface to the MSC (mobile service center).

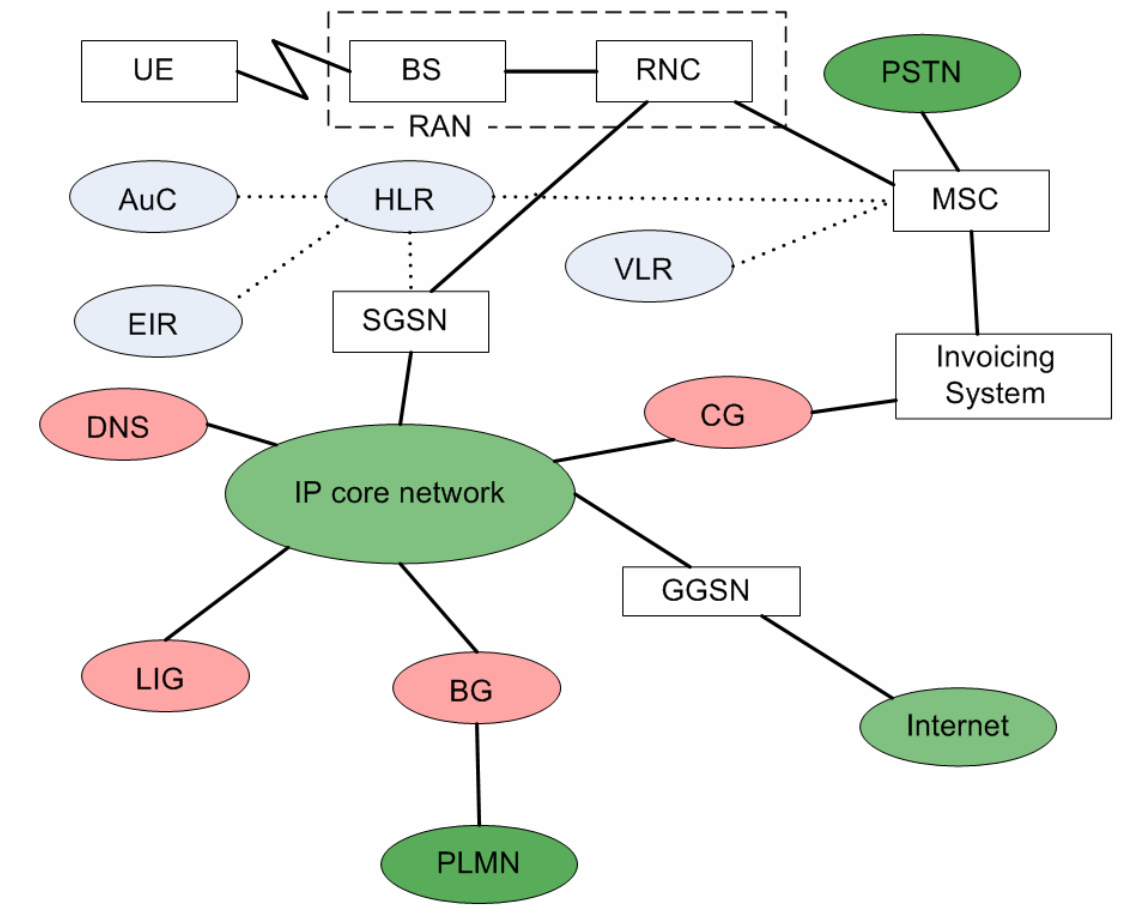

Figure 2. UMTS radio network (RAN) and its interface via SGSN to the operator core network and the interface to the MSC (mobile service center) (simplified) [Vesanen].

The development of the UMTS network is based on open standards. Standardisation documents are available on the 3GPP pages [3GPP]. The practical transmission rates of this 3G radio network are typically a few hundred kbit/s and it offers new services in addition to GPRS network services. They include, for example, location-related, concurrent calls and data connections as well as modifiable services.

The components of a UMTS network are mainly similar to GPRS but in 3G terminology, the terminal device is user equipment (UE), the radio network is (RAN) and the core network is (CN), as in Figure 2. In addition to SIM there is also USIM, which has more secure algorithms.

For practical reasons the information security management of UMTS is built on the GSM network security model, so some known weaknesses have been fixed. The security architecture of the UMTS network is divided into three layers: *application layer, home/service layer* and *transmission layer*. Moreover, the security characteristics are divided into classes, see Table 4.

Table 4. A simplified view of UMTS information security characteristics. The fifth class, transparency and modifiability of security, has been left out due to simplification.

Type	UMTS information security characteristics
Network access security on **radio link** level	Identification – both the network and the user must verify each other.
	Confidentiality – both the signalling data and the user data on the aerial are encrypted and the algorithms and keys used in the encryption are negotiated with confidence. The confidentiality of the user's identity and location is protected.
	The integrity of the signalling data is verified by algorithms and keys negotiated between the parties.
Network security – the security of the signalling data of the network components	Device identification verifies that no hostile components can be added to the network.
	The confidentiality and integrity of the network's signalling data is protected.
	System for collecting attack data.
User security	User identification is required to gain access to USIM. The access to terminal devices can be restricted to authorised USIMs only.
Application security	The traffic between USIM and the network is secured. USIM Application Toolkit services are secured. This gives an opportunity for the service providers to provide USIM-located services that require modifiable encryption level.

Most GSM network-related information security problems have been successfully solved in UMTS networks. However, the network is vulnerable to certain denial of service attacks, which are very difficult to prevent altogether in wireless networks.

2.3 Future trends

3G is bringing a wider service selection for mobile terminals. An almost unlimited possibility to listen to MP3 music, as well as cameras with around 1 mega pixels, including video recordings and sharp colour displays, are already here today. Planned 3G services, video calls and negotiations have not yet gained a wide foothold in Finland. In the spirit of digital convergence, Nokia is developing mass-market mobile services such as Mobile TV, Visual radio and advanced mobile games. The most centric future local network technologies used in mobile phones and PDA devices are summarized in the next chapter. Data transfer to other users' devices is the key factor that gives added value but, at the same time, causes many new threats.

2.3.1 WLAN connections in mobile phones and PDA devices

WLAN can be implemented with various technologies in mobile phones or PDA devices but this has been quite moderate, especially in mobile phones. Previously, the power consumption and other technical factors of WLAN were regarded as a problem. According to the research company In-Statin [INSTAT], the number of subscribers to WLAN mobile phones will be universally rising to more than 256 million by 2009. This would include about 12 % of all mobile phone users in the world. Because of this, the WLAN technology must be briefly addressed in this paper. The speed of WLAN techniques has already risen to 54 Mbit/s and a standard functioning with over 100 Mbit/s is under construction. Reasonably priced WLAN phones are already available in Finland and a group of models with combined WLAN/VoIP and GSM is coming to the markets. [Karila.]

IEEE 802.11 is the base standard of WLAN. The network topology can be ad hoc (without base station) or infrastructural (with base station). Each base station uses its own channel – in other words, frequency channel – so that traffic in different base stations will not disturb each other. Base stations are usually connected to the same core network.

Threats to WLAN are, for example [Vesanen]:

- eavesdropping, traffic analysis (can be passive, so it is hard to detect)
- disturbance or denial of transmission media use (WLAN uses a free frequency area)
- manipulation of transmitted data
- intrusion to the system of an organisation (via WLAN).

The WLAN protocol family defines the functions of the physical and transmission layers and the authentication services, and the protection of the transmission path used in them.

It has become clear that the basic WLAN information security mechanisms, SSID (Service Set Identifier), meaning network ID, and the oldish WEP (Wired Equivalent Privacy), are not sufficient. This is why the WPA (WiFi Protected Access) encryption standard was developed to patch the security holes in the WEP encryption. The information security level in WPA is already a lot higher and supports various different identification techniques. Some information on WPA versions is given in the following:

- **WPA** can be used in two modes – identification manually (using shared secret) or by using a separate server. WPA uses 128 bit encryption keys and dynamic session keys.

- The new **WPA2** is based on the IEEE 802.11i standard and implements the AES encryption algorithm. Manual identification (using shared secret) or by using a separate server. Downward compatible with WPA.

Many devices have old WLAN versions, so the devices in the formed WLAN network connection can meet them by switching to WEP encryption. Because of this, and, for example, end-to-end encryption needs, the same information security mechanisms as are used in the Internet must be applied to WLAN. These mechanisms include IPSec, SSL/TLS and key management, as well as public key infrastructure (PKI). Using these, end-to-end encryption can also be implemented in mobile devices. For example, SSL/TLS and PKI have already been implemented in most mobile phone WAP and WWW browsers. IPSec is a standard at least in 3G phones (because of IPv6).

There are a lot of documents on WLAN information security (and the lack of it), for example "Wireless Network Security 802.11, Bluetooth and Handheld Devices" [NIST800-48].

The biggest problems with the WLAN connection used in a mobile device are related to the user's uncertainty of the following:

- Which WLAN networks are secure to use? Who administrates them?
- Which network I am connecting to or am already connected to? How can I assure it? Is the network secured and how?
- What kinds of information security settings should I use?

There are some miniature WLAN network scanners already available to fulfil these needs [Canary]. With them, WLAN networks and details about their traffic, such as signal (802.11b and 802.11g networks), signal strength, network ID (SSID), use of encryption (WEP and WPA) and overlapping networks, can be scanned.

Also, the use of a SIM card in WLAN identification (EAP-SIM and 802.1x) has been defined. With this the tele operators can provide access to WLAN services by identification with SIM card identity. [WLANSC.] A telephone operator can provide solutions that utilize a SIM card in a USB memory stick or in the mobile phone itself as a means for access control to a WLAN network (the WLAN SIM interface has been implemented as a separate application in the SIM card). Thus existing roaming, information security and invoicing infrastructures can be used. The standard EAP-SC issued by the WLAN Smart Card consortium is very suitable as an interface for several various identification needs, like EAP-TLS (WWW), EAP-SIM (2G, 2,5G) and EAP-AKA (3G).

2.3.2 Bluetooth and ad hoc networks

An ad hoc network means a wireless telecommunication network that does not need any base stations or equal infrastructure in order to function. The devices, such as laptops, mobile phones, PDAs, etc., identify each other and are able to mutually form a network automatically. The basic characteristics of an ad hoc network also include that the devices transfer data to the destination via other devices – i.e. each network device is equal and can serve other devices as a router. The use of ad hoc networks has expanded exponentially over the last few years and their future aspects are very positive. Some of their biggest advantages are their fast and easy implementation and usage in any location.

There are some features of ad hoc networks that cause a bigger information security threat compared with other networks. Due to the lack of centralized management, even restricted access control can be difficult to arrange. As data traffic flows by default via any device in the network, it is easy to get hold of the signal, as well as to eavesdrop, change routing or create other disturbance. As the network itself can be mobile and the devices in the network are mobile by their nature, the structure and location of the network can change a lot within a short time. This sets vast challenges for the continuous function of the network and causes a blurred boundary between the normal and abnormal function of the network. Furthermore, because some devices in the network have limited resources, the function of complex protection can be uncertain. Some devices may have relatively limited battery capacity, so one possible attack against the network is the mere sending of unnecessary messages to the network. These challenges are being solved at the moment by developing secure routing protocols, applicable identifying methods, and stand-alone event monitoring. [Savola.]

Bluetooth

Many smart phones currently have Bluetooth (BT), which is a wireless, radio frequency, short distance communication technology. A device network made with Bluetooth sets up automatically when the devices are brought near each other (as long as the Bluetooth functionality is on). The radio frequency used is a free ISM, which exposes the network to disturbance. Bluetooth devices form a network step by step:

- When idle, the devices listen to queries unsychronously.
- A device sends a query to all frequencies. Devices nearby receive the query and reply to it with their own address and clock offset. A device can be invisible (does not reply to queries) but it can be contacted with its unique device address.
- The actual connection (Pico network) between the master and the slave is set up in the query by distributing a PAGE message (including the target address) to

which the receiver replies, for example, by exchanging channel parameters, after which the devices are ready to communicate. The master can join a maximum of seven slaves by consequent queries.

GAP (Generic Access Profile) defines the general procedures concerning the search by Bluetooth devices and link management. Other profiles rely on GAP, which is the most important profile from the information security point of view. According to GAP, there are three security modes: service level security, link level security and no security at all.

2.3.3 RFID

RFID (Radio Frequency Identification) is a low-cost radio technology for identifying an object such as consumer goods. With RFID, people and goods (objects) can be quickly identified electronically without contact or visual connection. RFID use is rapidly increasing in industry. The operating principle of RFID is shown in Figure 3.

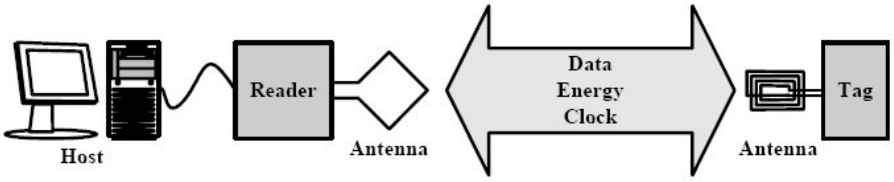

Figure 3. The operating principle of RFID [ECRFID].

The RFID Reader is an antenna and transceiver. The Object has (many times passive) an RFID microchip tag, which notifies its identification and other data to the reader when the reader asks for them. The most common frequency on which tag and reader communicate is 13.56 MHz, which is also an internationally free frequency. Two important RFID standards, ISO 14443 and ISO 15693, have been issued to this frequency. ISO 14443 is not independent of manufacturer; its most commonly known application is Philips Mifare, which is used for different payment applications. Its reading distance is limited to three or four centimetres. The ISO 15693 standard is truly independent of manufacturers. [VILANT.] Many pre-studies and pilots have been made on RFID in Finland. An RFID reader for a Symbian phone has also been made.

The most important information security problems for low-cost RFID systems are:

- The communication is unencrypted or its integrity is not checked. Non-standardised encryption is widely used in order to save licensing fees.
- The RFID tag's memory can be read if the access control has not been implemented. The RFID reader can be jammed with a frequency transmitter.

- Privacy – the location and consumer profile of the user are in danger of spreading to unsolicited parties.

More information on RFID security is widely available – see, for example, [LASEC]. A new European Commission Working document on RFID information security is also available [ECRFID] but there are still no Directives on RFID. The application centre RFID Lab Finland, which is focused on remote identification applications, was opened in the spring of 2005 at the Technopolis Helsinki-Vantaa technology center [RFIDLAB].

2.3.4 Summary of emerging mobile phone technologies

A compact summary of some upcoming technologies for mobile phones or PDAs and their information security aspects are shown in Table 5.

Table 5. Summary of a few new technologies for mobile phones and their information security.

Application/ technique	Technology	Information security		
		Threats	Impacts	Solutions
Music and audio	MP3, AAC, AACplus, AMR, etc.	complexity, illegal copying	distribution of contents slowing down?	new standards, rise in devices' capacity
Bluetooth	BT-profiles, chip technology	user's lack of knowledge	insecure or accidental connections	encryption, settings, awareness of the user
Location	GPS, A-GPS, cell-based	spreading location information	privacy decayment	settings management
Presence	SIMPLE, SIP	spreading presence information	privacy decayment	settings management
Push-to-talk	RTP, SIP	slow service, error calls	trust in service?	comprehension of the nature of the service
RFID	RFID short-distance reader	privacy protection	new use cases	Application-based information security, protocol development
E-mail	POP3, IMAP4, SMTP	spreading malware, spam	confidentiality and integrity of device must be protected	filters, prevention of malware
Video	MPEG-4, H.263, H.264	complexity, illegal copying	distribution of contents slowing down?	new standards, rise in devices' capacity
WLAN	IEEE 802.11	user's lack of knowledge, ranging quality of implementations	insecure or accidental connections	encryption, WPA, SIM, settings, awareness of the user
VoIP	RTP, SIP	advertisement calls, eavesdropping	waste of time	encryption, strong authentication of the user
WWW	XHTML, HTTP	malware, attacks	need for protection and maintenance	SSL/TLS, PKI, defence, upgrades

2.4 A short description of digital convergence

A situation where several digital services are getting close to each other and connecting to each other at the technical level is called digital 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 seen to be the different basic qualities of the integrating networks: the Internet is an open and unmanaged system, while many systems connecting to it, such as television, (mobile) phone networks and production control systems, are more centrally managed.

Even closed network environments are facing various kinds of pressure. Many organisations are outsourcing their functions intensively, causing the network to be administered by a third party. In general, network infrastructures are converging towards all-IP solutions for 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. A false sense of security is easily assumed when the whole network is handled by a single organisation and no hostile parties are assumed to be located in the network. The main characteristics of the convergence threat can be seen as the switch-over from the closed networks to the 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 in 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. 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. Nowadays the security and reliability cultures have been expanded or are expanding to application development in the IP world. 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 in the Internet.

3. Information security threats to the mobile world

The existing Finnish networks and mobile devices use GSM, SMS, GPRS and Bluetooth technologies (even UMTS to some extent). Threats and solutions due to these technologies are rather well known, but newer technologies can cause unanticipated threats.

New technologies include, e.g., UMTS, IP-based public and service networks connected to mobile networks, and their services – such as video, audio, digital pictures, push-to-talk, localisation services, IP phone calls, payment services, and contact and support services. In addition, threats are generated by new types of network connections like WLAN and PAN, and their possible effects on mobile networks and the services therein. From the service developer's perspective, information security threats are due to the following issues:

- different level of information security management of stakeholders and users
- differences in know-how between the stakeholders and rapid evolution of the field
- attacks targeted at the service or device and errors, denial of service, complexity and wrong configuration settings
- user and service identification and information confidentiality
- access control of service content and programs and unauthorised copying
- new use scenarios and technologies
- unauthorised use of services
- malware, such as viruses and worms
- mobile electronic payment service.

The threats to mobile services are different from the threats to digital convergence. In this study the focus is on risk and threat identification in mobile networks, distribution, mobile devices, services, etc. It is also important to notice the smart phones are still quite rare (they are actually still under development) and nowadays mobile networks are rather well isolated. Hence the threats should not be exaggerated. However, the world is changing rapidly and soon the emphasis of the collection of risks could be different.

3.1 General issues

Threats in the mobile world can be roughly classified into three parts: threats to mobile networks, mobile devices and users of mobile devices. In addition, of course, there are threats to service producers, which are treated later in this report.

The range of influence of threats to mobile networks is the broadest of these three classes. However, these threats are typically most unlikely, at least as far as the air interface is concerned. Threatening the operator network via the air interface requires special devices and know-how. Hence the most critical threats to mobile networks can be thought to come from digital convergence. Prior research results on network threats are available – 3GPP has listed 3G mobile network threats in [3GPP].

Digital convergence also threatens information security in mobile devices. The trend for mobile devices to become more versatile and more complex also causes new threats. Already now, a great number of conventional PC threats concern mobile devices too. At the same time, the user has more responsibility for his/her device, which could be difficult to follow.

Threats targeted at the user have increased due to the increase of mobile device use and their increased multiformity. User needs and his/her trust in mobile devices increase the threats targeted at him/her. For example, the use of mobile devices as tools, as personal information repositories and as a channel to access services cause mobile users to puzzle over many practices familiar from the Internet world, such as certificates, passwords and right configuration settings. It is very difficult for the user to realise the differences between professional and personal use of the device. The information security needs for these ways of use are different. It has long been a common practice in the PC world to utilise a separate device to protect information meant for professional use.

Threats due to digital convergence can be partially mitigated by experience gathered from implementation and network security in the Internet world. A lot of trouble can be avoided if these lessons learned can be exploited when developing new software, interfaces and networks.

This report does not present an inclusive list of threats; it just focuses on the essential ones. All threats cannot be listed beforehand since we cannot foresee the future clearly.

3.2 Threats to mobile networks

The most concrete threat to a mobile network is perhaps eavesdropping on phone calls and data traffic. The standardisation suggests encryption of information to be sent as a countermeasure for the problem. Using encryption, we can mitigate this threat. The probability of this threat depends on the strength of the encryption algorithm. In the GSM system this strength has turned out to be questionable [GSMsec]. In some cases eavesdropping on GSM traffic is possible because subscribers still have old SIM cards (using COMP128-1 A3/A8 implementation) in which stronger A5 encryption algorithm

variants do not help. Software radios targeted at consumers have made the eavesdropping technology available at amateur prices. A potential example of eavesdropping is industrial espionage, in which the threat concerns slightly different phases of the service development.

An even more critical threat than that mentioned above, although more hypothetical, is altering original mobile traffic. In this case the intruder replaces speech or data with his/her own information.

Analysis of mobile telecommunication traffic is rather easy to implement, but it still requires the correct devices, know-how and good timing. By monitoring the traffic between a mobile device and a base station one can track the position, speed, traffic time, duration, target, etc., of a mobile device. However, an intruder's exploitation scenarios are limited – the most beneficial information could be perhaps location information and user profile information.

A Denial of Service (DoS) attack on a mobile device and network traffic is a very serious threat, especially in a state of emergency. Denial of service can also be used in useful ways in some cases (e.g. in some protective scenarios), and there are commercial solutions available for this. A DoS attack requires resources, but there are intruders' exploitation scenarios in addition to sabotage and mischief. The most potential DoS threats to a network are perhaps power failures and vandalism targeted at a network appliance.

In a mobile network the user has to trust the network service operator wherever his/her mobile device is located. This can be problematic, especially in the case of roaming, because in general it cannot be assumed that all operators are fully trustworthy. The user is rather vulnerable in the case of a forged base station.

3.3 Threats to mobile devices

There are many different types of threats to mobile devices. The main threat is stealing and tampering with the device, because of the small size and easy portability. Nowadays mobile devices are often used for professional business, which creates new challenges for information security and broadens the range of influence of such risks.

Problems for mobile device users are caused by compromised SMS and MMS messages, spam, WAP pages, Internet pages and rapidly distributing malware. The standard Java software of novel mobile phone models increases the number and likelihood of virus infections due to the use of a general-purpose programming

language. New threats include those familiar from the Internet world: Trojan horses, keyloggers and spyware. Spyware investigates files and sends them forward to the address defined in the spyware program.

Security threats due to the Java language that is commonly used in mobile devices can be classified into threats arising from the design of the Java language [javafaq] [javavul] [javasec] and threats to the Java Virtual Machine. Securityfocus.com mentions 33 Java vulnerabilities using the keywords "virtual machine" [secfocus] – hence virtual machines are as vulnerable to information security flaws as any other software. There are threats that concern the use of a Java native interface. In this case a part of the code is done using a lower level programming language that is more vulnerable than Java itself. Some embedded devices compile Java into native code whereas some execute Java byte code directly. Consequently, this affects software threats. However, the range of influence of the above-mentioned threats is not particularly broad.

There has been a lot of discussion about information security issues in Bluetooth for a long time and, at least in the older implementations, the level of security can be questioned. For example, in a bluesnarfing attack the intruder can access calendar and notebook information from the mobile phone under attack, as well as call a desired number and send SMS messages via the user's subscription. In general, the problems are due to the sloppy implementation of the Bluetooth specification and errors in software production. Threats connected to WLAN and Bluetooth are, to a great extent, similar.

Other threats to mobile phones include the great number of software versions, unsatisfactory maintenance of software (e.g. updating anti-virus software and backup of information) and the more risk-prone open programming interface of the new mobile operating systems. The service developer can affect the threats by enhancing the reliability of his/her own service.

There have been pilot projects using RFID technology in mobile services. From the security point of view, RFID technology is still doubtful and needs development and rethinking. One should avoid the preservation of important information in RFID tags, although this kind of use has been planned for passports for example.

FiCom has provided an article on information security in mobile devices, see [FICOM].

3.4 Threats due to digital convergence

Because of the trend for digital convergence, the complexity and number of interfaces in devices is increasing, resulting in an increased need for management of the system as a whole. The performance and compatibility of protection programs for mobile devices is still defective and perception of the whole environment is important in the design of security solutions. It can be reflected that the same kind of relationships concern mobile devices as PCs in general. One cannot assume that the inputs to mobile devices are well defined, correct and harmless. The reliability of software is becoming more and more critical, as well as its ability to filter out data coming from its environment. The use of different kinds of broadcasting or group distribution techniques in service production also increases service threat scenarios, e.g. connected to denial of service or verification of origin.

Mobile devices are certainly as desirable a target as any networked systems for attacks originating from the Internet. Consequently, a remarkable threat due to the digital convergence is the possibility to attack software in mobile devices using the network connection. If this kind of attack were to be successful, attacks against the Internet and payment services would be possible – across the board, threats to Internet devices.

Operator networks are incorporating more and more features similar to the Internet network. They can be compared with the intranets of companies, accepting only desirable traffic. At the same time, operator networks inherit threats from Internet networks. The servers of operator networks are targeted by unsuitable and malicious network traffic, both from the Internet and from the mobile users.

3.5 Threats to authentication and identification

The threats to authentication and identification (A&I) can be roughly divided into two categories: threats connected to the user and the mobile device A&I carried out by the network, and threats connected to the network A&I by the user and the mobile device. The latter is important to the user in protection from attacks. The major authentication threats to the service developer are forged or illegally commissioned mobile devices.

Authentication and identification is based on cryptographic authentication algorithms, the strength depending on the choice of the algorithm. A bad algorithm generates a threat, enabling disclosure and copying of the secret key stored in the SIM card. As a consequence, the use of mobile certified services without an SIM card becomes possible. The attack can be very quickly implemented during the theft or disappearance of a mobile phone. The threat of an air interface attack is more unlikely due to the need

for suitable equipment to impersonate oneself as a service provider, and the longer time interval. The threat due to a bad algorithm is realistic – e.g. Comp128-1 is commonly used for authentication and its flaws were already pointed out in 1998. The strength of the new algorithms developed to replace it is unclear at present.

In addition to the threats due to the weakness of the authentication algorithms, there are threats due to *man-in-the-middle attacks*, in which the session initiated by the user is seized by a hostile user. These attacks are nothing new in the Internet world, but their implementation is more troublesome in the air interface of the mobile world.

Users face most of the threats during authentication. In addition to the technical threats, users are vulnerable to different kinds of fraud and social engineering attacks, theft of device, and other forms of impersonation.

An important threat is a combination of the above-mentioned attacks – e.g. a fraud program is first fed to the user's phone and later the user is called by someone impersonating the system administrator giving instructions to "repair a fault".

The role of the public authorities and service providers is important in increasing information security awareness, teaching the basics and in encouraging a good information security culture.

3.6 Threats to payment services

The security implementation of payment services is based on authentication – in order to enable a payment transaction, both the payer and the payee must usually be authenticated. Consequently, many threats to authentication and identification are similar to those of payment services. From the service developer's perspective, a new financial risk is the investigation of non-repudiation of transactions, which can be laborious and prolonged, and can cause loss of income. It is important to define and inform beforehand how a service user is responsible for the expenses that criminal activity such as stealing a mobile device or fraud can cause via use of the service. It is the user's duty to be aware of who is using his/her device and how – and to inform the responsible quarters if he/she no longer possesses the device.

Digital convergence introduces the different *phishing* attacks familiar from the Internet, in which attempts are made to cheat the user into using forged payment service pages resembling the correct appearance. One of the major threats to the service developer as well as to the user is disclosure of confidential information, such as account statements and credit card information. The servers of payment services are targeted by similar

kinds of threats as those of critical Internet servers. Similarly, threats to mobile devices handling and possibly storing confidential information can be compared with those of Internet devices.

3.7 Threats to service development

From the point of view of electronic content production, the most important threat is piracy. Content protection is a new field and standardised and good solutions are not visible. Content protection issues can even restrict or prevent the supply of certain services. Digital Rights Management (DRM) sometimes incorporates threats because of undetermined certificate chains. A trusted platform would minimise threats in general.

There can be threats and problems in each phase of the system and service development. Threats can be generated during the design phases by situations where a certain technology is used even though the risks are big in that technology – or automation is not exploited. 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 also generated by the supporting systems. These threats are due to weak programming languages and weak development tools – both of which can be trusted too much. Threats can be generated during the system design by wrong assumptions regarding the system environment and human behaviour, as well as faulty models and simulations. It is possible to carry out the wrong kind of testing during the implementation analysis phase and there can be errors in software debugging practices. Some general problems in development are the lack of capable human resources (e.g. slowness in absorbing new maintenance practices), rush and defective documentation.

The level of information security often changes during updates and interconnection of components. Moreover, there are threats in disposal of services, like a premature shutdown of required components and a hiding dependence on a non-existent older version. A big threat is the lack of security awareness on the part of the developers. Other threats include the short-lived operation of a stakeholder, resource allocation problems and an insecure service development process.

4. Solutions to information security threats

The most significant solutions and architectures to previous information security-related threats to the service provider are described in this chapter. Only the most important guidelines are written down since complete and durable solutions for information security do not exist.

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 to 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 related actions are completely ceased. Similarly, risks can be minimized by minimizing the frequency of occurrence the risk and its 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 the servers that are necessary for e-business and are connected to the Internet. For example, the provider of the information security software does not compensate indirect damage if the product does not notice a virus or threat. Risk management also encompasses proactive actions, such as contingency and recovery plans for server attacks.

There can be a gamut of combinations of technical solutions when Internet use is combined with mobile network use. This increases the complexity and makes the service provider's choice of solution problematic (for instance when choosing an application platform).

The most important solutions for the different threat classes for a service provider have been combined in Table 6.

Table 6. Information security solutions in relation to targets (threat classes) and information security definitions.

	Technology/Process	Target (according to classification in Chapter 3)						Information security (according to definitions in 1.2)					
								Security functions			Security concept		
		Service development threats	Payment traffic threats	Identification threats	Convergence threats	Threats in terminal	Threats in mobile network	Recovery	Protection	Observation	Availability	Integrity	Confidentiality
Service content protection	Restricting further distribution of the media content	●		●	●	●	●		●	●	●	●	●
	Encryption of the saved data	●	●		●	●			●		●		●
	Digital signing and verification of the programs	●		●		●			●	●	●	●	
Protection from attacks in service	Connection to electronic payment system	●	●	●	●	●			●	●	●	●	●
	Privacy protection	●	●	●	●	●	●		●	●		●	●
	Server protection	●	●		●		●	●	●	●	●	●	●
	Detection of attacks	●	●		●	●	●		●	●	●	●	
	Protection from malware	●	●	●	●	●	●	●	●	●	●	●	●
Service developer's information security process	Third-party assessment methods	●	●			●		●		●	●	●	●
	Risk management	●	●	●	●	●	●	●	●	●	●	●	●
	Physical security solutions, e.g. backups, tamper-resistant HW	●		●		●		●	●	●	●	●	●
	Fault situation recovery, contingency.	●	●		●		●	●		●	●		
	CERT actions	●			●	●		●	●	●	●	●	●
	Version management	●						●	●	●	●	●	●
	Information security in business management	●						●	●	●	●	●	●
	Tech. process follow-up, improvement and education	●						●	●	●	●	●	●

Table 6 has to be considered with certain reservations, because solutions related to information security have to be tailored according to each application area. For example, when distributing *video clips*, the distribution method has to ensure by technical solutions and processes the following qualities:

- authentication of capacity-competent terminals, communications
- ensuring service availability, server capacity, bandwidth of the connection (e.g. DSCP), memory use, protection from attacks, etc.
- compatibility of MPEG-4 and audio codes and distribution files
- two-way authentication, integration of payment means, etc.
- encryption
- ease of use
- restriction for further distribution (e.g. DRM), copyrights, related rights.

It can be further concluded that for *mobile games* the solutions include the same elements as for the distribution of videos and music, but special attention should be paid to digital signature, protection from malware, group games and related technical solutions, such as payment for group games. The terminals' graphics-related HW and SW modules require special attention to information security so that data cannot "leak" out of the module.

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; in addition, understanding of the application level in the network is crucial in order to ensure availability. Thus understanding the entirety of networks can be insufficient, which not only complicates network management itself but also 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 primarily important 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 with normal vulnerability analysis.

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. 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 the 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 the different protocol implementations are especially important for the analysis.

The purpose of the solution model is to achieve a 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 a means of informative communication between the actors in the field. The model enables the study of different practical scenarios and the factors affecting them. One of these scenarios includes certain network components and the protocols implemented by them. In addition to the data gathered from the protocols, this scenario can take account of the network administrating the organization's own vulnerability analysis, 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 also paves 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 a function 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 has proven 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 where 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 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 being changed can be identified. A preliminary study can be done in the concept stage. Subcontracting increases complexity in change management and this must be taken into account when agreeing upon the practices. A common documented model is necessary in change management, and also in other administrative processes, especially in a networked environment.

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 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.

4.1.3 Management of information security risks

In general, the information handling risks can be divided into accidents (for example administrative errors and gossiping) and intentional acts. Technical risks are e.g. viruses and unauthorized intrusion to the system. Risks that are difficult to manage are errors in the standard applications. Notable risks are also those targeting administrative information security, such as

- defective classification of data items
- lack of strategy planning

- lack of knowledge
- responsibility for definitions related to information security tasks.

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 the different stages of risk management separates its actions and aims at seeing their conditions and connections, after which the risk management can also have a generally strengthening affect on the actions. Methodicalness and regular assessment is important. Management commitment is also essential because the management define the tolerable risk level and allocate the resources for protective actions. The success of the risk protection has to be constantly measured. Valuable information on potential risks is also obtained by observation and reporting of so-called "near-miss" situations. It is important to form a connection between the risk management processes of subcontractor actors throughout the chain.

The conditions for the actions are listed and related threats are sought in the identification stage. The threats recognized at this stage can be as unlikely as possible; 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 to avoid the risk before its realization. An avoidance plan can be created at this stage or in the last stage together with a contingency plan.

The severity of the threat realization related to the action and the probability of the threat itself are considered in the assessment stage. 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 the symptoms related to the 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 the easier manageability. Still, users can often foil the technical solutions with their actions.

User-related risks have to do with the 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 of using or configuring 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. Administrators and their knowledge are the key factor of course.

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 should be used. They should be acquired from several producers – the dependency on a single producer can cause problems for example when the product line is ended or when 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 available quickly in order to minimize damage caused by a 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 required conditions have to be ensured. Data items are also printouts and verbal information, etc.

4.2 Technology-oriented solutions

Technological solutions to mobile world threats are manifold. It is impossible to describe them exhaustively and at the same time briefly. The most important technological solutions according to our study are listed in Table 7.

Table 7. Technology-centred solutions to mobile world threats.

Solution	Current technology	New technologies
User and service authentication	SIM, USIM, WIM, SWIM, IKE, passwords, SMS, etc.	HST, biometrics, HIP, DNSSEC
Digital signature and verification	Browser signatures	Application-dependent or universal smart card, signatures
Media distribution restriction	OMA-DRM, manufacturer-dependent DRM, protected memory cards, scanning of peer-to-peer networks	Trusted platforms
Encryption of saved data	Memory encryption programs	Strong cryptographic protection of all memory devices.
Connection to the electronic payment system	ssl/tls encrypted wap or web, one-time passwords for banking (Tupas)	Trusted HW/SW platforms, HST-SIM
Privacy protection	ssl/tls, PKI, VPN, SIM auth, NAT, anon. services, register protection, SAML, Liberty	E.g. spontaneous and peer-to-peer networks, onion routing
Protection of servers	FW, SW-auto updates, etc.	Automatic quality assurance tools
Detection of attacks	Local DBs in IDS systems, distribution of black lists (hosts)	Global, shared DBs in IDS systems
Protection from malware	Identifier-based antivirus programs	Latest heuristic analysis, memory areas
Secure settings	Manually or with SMS	Remote configuration standards, OMA SyncML DM

The most important technology-centred practices in the service development environment for securing information and systems are listed in the following example (sources e.g. [CERT]):

Example: Technology-centred information security practices in the service development environment.

- Design overall architecture.
- Choose server equipment with basic information security qualities corresponding to the requirement level of the applications. Ensure expandability properties. A cheap server with low information security qualities cannot usually be used for demanding applications.
- Update operating systems and applications quickly enough as the faults are detected. Nowadays updates have to be followed even daily. Make support agreements and ensure availability of required patch updates.
- Set an obligatory user authentication for all users. Base authentication methods required from the user on application and access rights – for example strong authentication (such as SecurID card + passwords) if the remote user name has administrator rights. Teach the correct way to use passwords. 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 long-term and secure backup storage of good quality for all system files, including user data and system configurations. Discover legislation effects and possible branch obligations.
- 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.
- Protect required connections with VPN.
- Use system replication to ensure service availability. This has to be done with expertise and with premature testing using secure replication methods.
- Isolate/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.
- Utilize systems that detect actions against presumed access rights or other kinds of suspicious and unexpected action. Use intrusion detection and prevention systems (IDS).
- 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 possible outsourcing of the system's information security administration and bind different responsibilities by contracts. Often, some of the most serious consequences will not be aimed at the party responsible for the protecting actions.

4.2.1 Authentication and identification of users, devices and services

Manufacturers have embedded an IMEI code into their mobile phones, but this code is rather seldom used. Basically, the use of a stolen phone could be prevented by putting an IMEI code into the blocking list, but in practice IMEI lists beyond national borders are not used. Instead, the subscriber to a mobile connection is authenticated with a SIM card located in his mobile phone.

Authentication can utilize certificates. A cryptographic certificate system can be based on mutual trust or a trusted third party. The global public key infrastructure has run into a crisis of confidence. Instead, there is a "patchwork", where the user has to respond to questionable trust issues in real time: "Do you accept a certificate issued by N to verify service X?" However, the connection between an Internet address and a corresponding public key has to be verified in important connections. A commonly used method for secure network browsing is an "https:" certificate verification with an encrypted TLS/SSL channel. Email systems use the certificate-based S/MIME certificate. Distributing keys and identities is a challenge, but distributing the cryptographic identity of the connection subscriber is easy to implement by means of a traditional SIM card.

The Finnish chip-based Personal Certificate (HST), like the authentication methods used by banks, is based on the fact that the user is personally identified at the moment of registration. Another commonly used model is based on instant initiation, whose result

is that there is cryptographic certificate information saved on both sides of the connection. This information is only used during the connection and then stored securely so that the next time the other party is recognized as the same as earlier. A prime example of this is SSH protection. Among amateurs this has evolved into circles of trust (the PGP-model), in which the public keys of trusted and verified parties are stored in their own computers. If a collectively familiar person is found when forming a new connection, the trust between the name and identity can be based on this kind of triangle.

The connection between the name and the address is generally complex. The connection between the name and the identity can be poorly defined and presentation of the identity can depend upon its environment. Address means the amount of data that is needed to find the object in the network, be it a phone number or an IP address. Name resolution is a basic function with which the presentation of identity is transformed into an IP address. Thus an Email address can be presentation of identity from the network's point of view, but address from the application's point of view.

The basic division is between phone numbers and Internet spaces. Phone numbers are only global when their international prefix presentation is used. Internet addresses are part of a universal hierarchic name space with a root directory at the bottom, from which everything else can be directed.

In GSM and UMTS networks the user is authenticated with the IMSI code that is found in the SIM card. For security reasons, it is rarely used and thus a one-time code TMSI (P-TMSI separately for GPRS use) is created from it, which is replaced after every use and sent to the user via a secure channel. The SIM card can include USIM, (in which IMSI is part of it) and ISIM for multimedia use. A UMTS network's USIM card can include, in addition to IMSI, the private key needed in verification as well as private identities that are needed if the aim is to have a connection simultaneously from many terminals with the same public identity. As a conclusion, SIM includes a shared secret (private key) with its own home network.

Example of a new authentication technology: The latest, and still at the experiment /standardization level, HIP (Host Identity Protocol) technology is based on isolation of authentication and location. There the identity and address are separated from each other, so the device can naturally utilize changing transport layers (WLAN, UMTS, …) and the user's application only recognizes cryptographic identity. The rest is handled in the transport layer, in which various addresses can be used simultaneously. See [HIP].

Replacing recent phone numbers with other user identifiers is mostly a political decision. As phone numbers have become transferable, the numbers nowadays authenticate the subscribers to the connection instead of the telephone lines. Still, all address spaces are not administratively equal; a system built hierarchically is better

scaleable than planar. It is also necessary to inspect vulnerabilities against attacks. It is essential is to protect name servers, for which purpose a new standard, DNSSEC, already exists, but it is not extensively used yet.

A great watershed at the moment is the circuit-switched or packet-switched way of thinking. The SIP protocol is used for different purposes on both sides, and new XML-based web services will diminish the significance of the address in future. In addition, the management of user identity, identifiers and profile data is a great challenge in current user directory solutions. In a networked environment in particular, administrative challenges are caused by authorizations, among other things. The significance of directory management tools is emphasized.

Example: The Tunnistus.fi service offers access to authorities' net services, through which about 20,000 authentications are performed in a month. By far the largest part is performed with banking IDs. The service is used with basic Internet-browsers that utilize the SSL/TLS protocol. Authentication requires either a personal identity card with chip, or personal or company network banking IDs. The user can access all services in the list with a single sign-on.

Additional example: Biometric identification. Regarding mobile communication, identification of a person may in future be possible using a physical feature or behaviour. At the moment, typical products and services of *biometric identification* are device access control, biometric locks and access control, National Defence Force applications, passport control, authorities' actions and documents. Nowadays there is speech, face, iris, retina, hand and fingerprint recognition as well as signature recognition (fingerprint recognition is the most sophisticated technique) on the market. It has to be remembered that using fingerprint (and other biometric) identification also relates to privacy protection, which means that the data should not be used unnecessarily, which could, e.g. in special situations (theft, device failure), end up in the wrong hands. The biometric application area will probably expand to the following areas:

- e-business, mobile terminals, future Internet mobile phones
- individualization of device and services to the user; safety of the elderly.

Restrictions and information security threats can appear when biometric sensors are attached to mobile phones (e.g. via USB) and, in general, to integrated mobile phone software. Fingerprint and voice recognition are most promising techniques for mobile phones. See, for example, the BioSec (Biometrics & Security) project of EU IST [BIOSEC]. There are not many encompassing international standards in the biometrics area, but the BioAPI consortium [BIOAPI] has standardized the API and ICAO biometrics of travel documents; ISO is also active.

4.2.2 Digital signatures and certificates

Signatory and signed information can be identified with a digital signature. The signature has to be created with a key that only the signatory can possess. Non-repudiation can be achieved in this way, which verifies the signed information, the origin of the signatory and the integrity of the information. The position of the digital signature has been clarified by Directive 1999/93 approved by the European Parliament. This has enabled companies to perform legally conclusive business actions in the network with greater trust than ever before.

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. The signature so formed is added to the message to be signed that is sent to the receiver. In order to check the message, the receiver has to decrypt the encryption with the public key of the sender and save it. If the compression of the received message matches the original compression, the receiver can be assured of the origin and integrity 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 have been confirmed by the trusted 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 the case of a service delivered to an end user, for example a Java application, a compression is calculated from it which then is signed with the service provider's private key that the third party has verified. The end user can check the origin and unchangeability of the application with accompanying certificate. 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 actual ending of its period of validity, for example when the private key is exposed to publicity.

A digital signature is at its safest in a mobile device when the related algorithms and keys are located in a device protected from being lost, such as in a SIM card. This kind of situation is WAP identity in a module (WIM) and in HST-SIM, so they are fairly secure technologies (if the SIM itself and the mobile phone have been implemented securely). The SIM card was initially meant for the challenge/response verification of GSM subscribers, but nowadays it includes a microprocessor, ROM, EEPROM and RAM memory, I/O port, operating system and file system. Thus challenging and reliable applications can be built on SIM. A reliable platform can mean different things, depending on the standard. Below is an example of a reliable mobile phone platform.

Example of reliable mobile platform: A Trusted Mobile Platform [TMP] is one way to ensure the security of partly strong cryptographic methods in a mobile phone, because it includes definitions of e.g. three different information security levels of the device architecture. At the highest security level the user authentication must be processed in a HW encryption module and the CPU has to be in different HW area, using a trusted memory bus.

4.2.3 Restriction of media distribution and encryption of saved data

Generally, *copyright* gives a producer of copyrighted work some privileges, which are on a time scale and limited to, for example, 70 years after the death of the producer in the case of a published work. Similarly, *related rights* protect, among other things, performing artists, producers and photographers from copying, distribution and negotiation of the artwork, the protection period lasting 50 years from the time it was saved. In the digital world, perfect and lossless copying of the files is easy. Every time the rights owners have found a way of protecting the content from extensive copying, the users have found a way to evade it. Transferring the work from digital form to analogical – i.e. into a form understood by humans – is the ultimate point at which copyrights can be broken, regardless of the means of protection. In other words, copyright protection in the digital environment does not prevent copying. Thus, the copyright protection seems to have no effect on professional copy retailing – in other words, piracy. It is worth mentioning that because of the so-called "network effect", copyright violations can also have a positive effect on the sale of the legal work.

For example, the copyright protection for Apple's iTunes music service was only broken (by Pymusique) to enable listening to iTunes music on Linux computers, which increased the number of potential users.

The magnitude of the effort used for copyright protection 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 and its content is worthless to the consumer. On the other hand, the sale time of a mobile game or program can expand to cover several years, after which competitive products, new features or even a new mobile user generation can diminish its value close to nothing. In the long term, copyright protection can be more of a hindrance than a help, even if content producers mostly require its use. New copyright law is being handled by the Finnish Secretariat of Parliament, so new regulations regarding the matter are on their way.

Technically, one can attempt to monitor copyrights in mobile terminals just as in home PCs. However, bypassing the protection mechanism can be slightly more difficult (physical and program structure being closed) in a mobile phone than in a PC, even if open OSs, such as Symbian, bring smart phones very close to the qualities of PCs regarding the copyright protection.

Device and platform manufacturers have had very different and incompatible solutions, which they have tried to fit under common standards. The most important of the standardization communities seems to be the Open Mobile Alliance (OMA), which has defined OMA DRM (Digital Rights Management) standards aiming at protecting copyrights. Implementations of the first stage of OMA DRM can already be found in several manufacturers' phone models.

OMA DRM version 1.0 defines the prevention of send-on (forward-lock) as well as the hardware-independent mechanisms of combined and separate delivery. The use of material can be given additional restrictions in a combined delivery, such as “may be used only once” or “may be used for a week”. In a separate delivery the user rights and content are delivered with data transfers independent of each other, where totally separate parties can more easily control content delivery and user rights. A draft OMA DRM 2.0 standard already exists.

How are the user rights described? The most important standard is perhaps Open Digital Rights Language (ODRL), which is a relatively light and simple language describing rights; it is also independent of the content type and way of transfer. ODRL in itself is an open standard free of licence fees, but OMA has adopted it in its DRM standard by defining an OMA ODRL profile. The latest ODRL version 1.1 [W3ORG] and the requirements for the next version [ODRL] are available.

ODRL’s permissions enable versatile definition of user rights (see Figure 4).

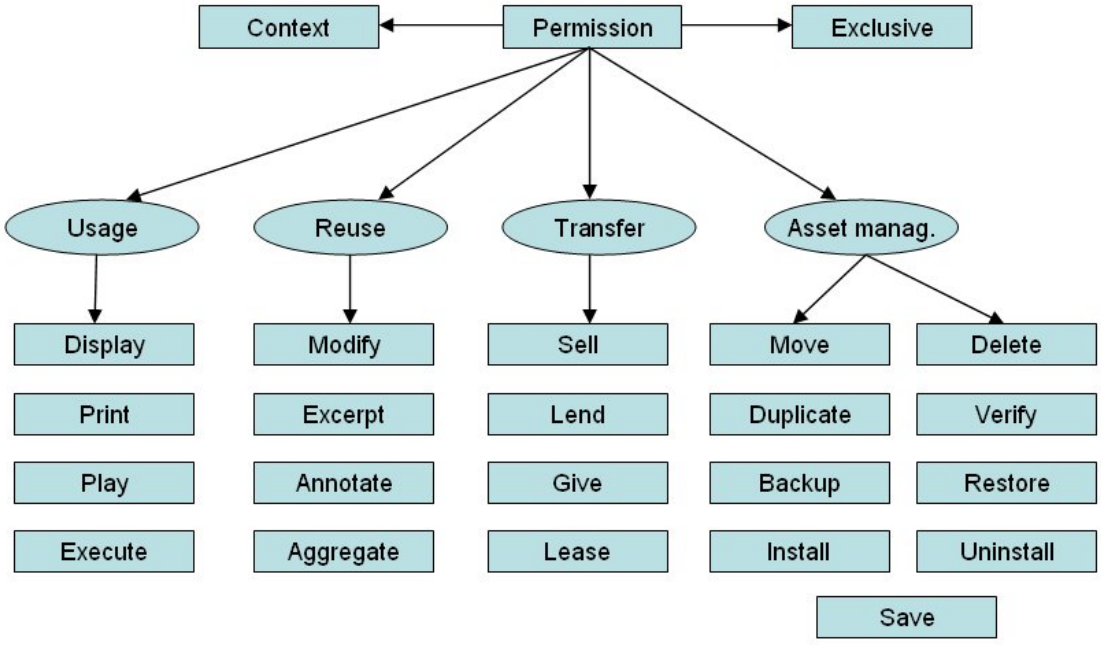

Figure 4. User rights model of ODRL v1.1.

These functions pertaining to permissions for further content handling are naturally implemented case by case in a used device, such as in a mobile phone. For example, if a DRM permission targeted at content were to give the user a right to, say, *modify* content, the user’s device may not necessarily include a modification function; thus the other rights (e.g. *transfer*) define whether the user can in reality legally modify the content in question or not.

Example of copyright protection of multimedia distribution. The organization managing MPEG patents, MPEG LA [MPEGLA], made a proposal to the OMA in January 2005 that network operators utilizing the OMA DRM 1.0 standard should pay 0.01 dollars on every transaction and 1 dollar on every phone call to the holders of the patent. The GSM Association [GSMA] has, based on the feedback given by operators, strictly refused to accept such conditions by saying they are as impractical as they are unreasonable and shortsighted. Operators are now frantically seeking replacement (non-standardized?) DRM solutions, whose licensing would be simple and more profitable. The GSMA has asked all providers of alternative DRM solutions to make their suggestions to GSMA, who could then recommend some DRM solution to their member operators. Unfortunately, from the user's point of view, this may lead to a situation where content services do not work during network visits, transferability of the content from one device to another weakens, and so on.

4.2.3.1 Examples of saving and encryption of data

Nowadays there are several "additional technologies" and tools that enable a mobile phone or PDA user to save masses of useful information. The amount of main memory of a mobile phone (in some phones even tens of megabytes) is growing continuously, but even that is no longer a restricting factor because the use of new memory storages, such as a USB memory stick, is explosively coming into use in mobile phones as well – for example for the needs of saving voice and picture data. Some examples of mobile phone storages are presented in Table 8.

Table 8. Physical storages of mobile phones.

Memory type	Examples
Main memory, additional memory	Internal ROM and RAM and their different solutions, joint use memories, cache memories, registers, flash.
Memory card	CompactFlash (CF) card. Flash memory based on the PCMCIA standard (43x36 mm), e.g. 1 GB available.
	MultiMediaCard (MMC) card. Includes ROM and Flash (read/write) technology. In addition, MMCplus 24x32x1.4 mm and MMCmobile 24x18 x1.4 mm cards.
	Secure Digital (SD) card sized 24x32x2.1 mm.
	MiniSD card. Like SD card, but sized 20x21.5x1.4 mm.
Memory stick for user data	USB memory stick. E.g. SanDisk has presented a 512 megabyte USB 2.0 memory stick secured with fingerprint recognition and data encryption.
Hard drive	Small-sized hard drive combined with a mobile phone, such as MP3 players.

There are general use file encryption programs already available for some smart phones (Series 80) and PDAs, with which data saved in the phone's internal as well as external memory can be encrypted. The programs use access control protected with a password and 128-bit data encryption (e.g. Psiloc Secure Storage). However, there can be

problems in their automation (e.g. securing all files automatically) due to the device's restricted processing capacity. In the future, more add-ons can be attached to a mobile phone's memory card connection, such as camera, Bluetooth, GPS and WLAN. The divergence of securing solutions for the saved data is illustrated in the following example.

Example of mass memory: The SD memory card uses the CPRM (Content Protection for Recordable Media) technology defined by the closed 4C consortium (IBM, Intel, Matsushita and Toshiba) to prevent pirating. Features:

- Bilateral device authentication is required before access to the SD card, after which a new random number is generated. Copying from a PC to the SD card is restricted to three copies. The encrypted data cannot be decrypted without a key.
- With an SD card according to the SDIO (Input/Output) definition, add-ons can be attached to the card slot, such as camera, Bluetooth, GPS and WLAN.

4.2.4 Connection to electronic payment system

The biggest problem for pay services is customer authentication, because customers do not willingly get separate IDs for services bought only occasionally. A positive aspect are the recent developments in the public sector – e.g. the co-operation project between metropolitan area cities regarding transactions with authorities**,** in which a common network authentication and payment service is built together with the State administration. Tupas bank authentication and HST certifications are parallel "authentication technologies" in this service (see Figure 5).

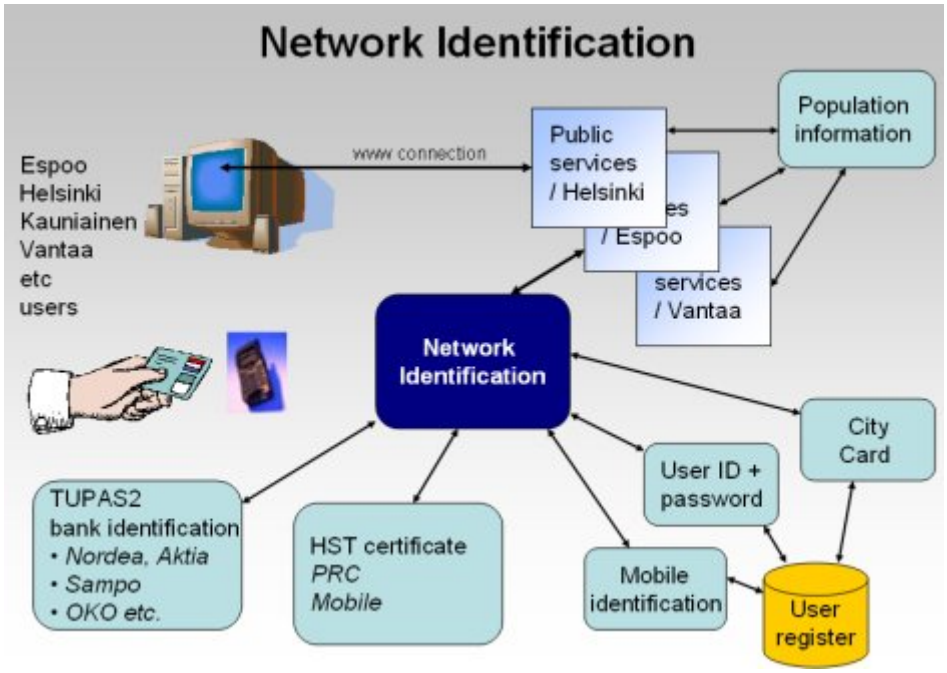

Figure 5. Authentication in the metropolitan area co-operation project [HEL].

The Finnish Ministry of Finance recommends the following for public services (see also Table 9):

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

Table 9. Brief introduction to the Tupas and HST solutions.

Payer authentication solution	**Description**	**Frequency**
Tupas	Tupas service of the Finnish banks (more information e.g. [PANKKIYHD]: • The bank authenticates the customer on behalf of the service provider. Based on use of the 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. The 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 bank service IDs. Nordea, Osuuspankit, Sampo, Säästöpankit, Tapiola, Ålandsbanken.
HST	The 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. The 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). By using the HST authentication, only the person's SATU is known. Strengths are the 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.

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). Solutions do exist, but they should be easily adoptable by every actor, and function in every technology platform, etc. Because it is chip-based, HST has stricter requirements for the technology platform as it requires changing the traditional SIM card into one in which the HST certificate is implemented.

An example of more detailed user access to the HST infrastructure is presented in Figure 6.

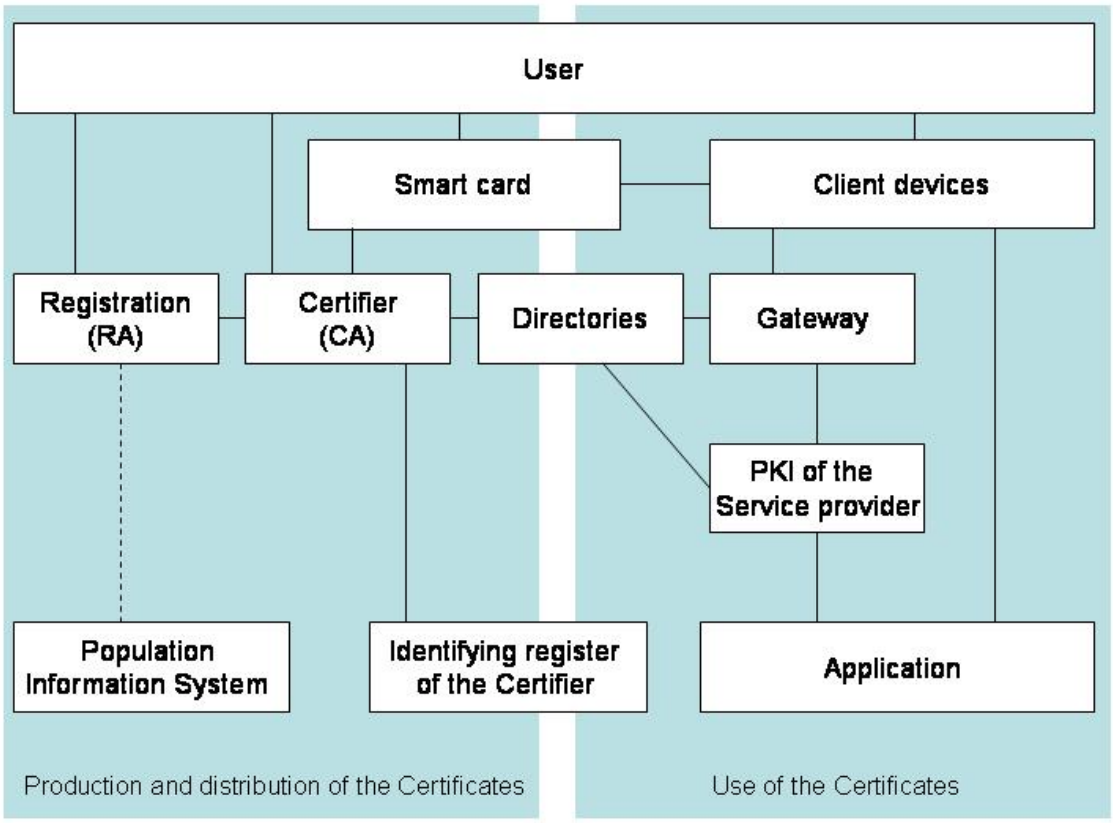

Figure 6. Example: General view of HST architecture [HST].

A credit card in a mobile phone? A lack of co-operation between competitors has long existed as different actors focus on developing their own credit card solutions. Credit card payment is a reasonably functioning system on the Internet (through a PC), but even then the terminal has to be protected from spyware (malware can copy the user's credit card data, etc.). Nowadays there are Wallet applications for smart phones, in which credit card data saved on the user's phone is kept covered by the application and can be practically copied to the website of the service vendor. This does not, however, remove the need for user attention when giving out credit card data. Nowadays service providers other than just network operators may save their own applications onto a SIM card. This leads to questions: Do the incompatible applications of competing actors (e.g. banks and credit card companies) in a SIM card benefit the consumer in the end? Will changing a bank become easier or yet more difficult?

Digital money is a way of paying for *small* purchases on the net or transferring money to another person's wallet, even with a mobile phone. It will be available by opening a wallet on the Internet (www.digiraha.net) and transferring money to the wallet from

one's own bank account. One can already transfer money between one's own wallet and another party, or transfer money to another person's wallet with a text message (usable for customers of Sonera, Elisa, Saunalahti and DNA).

The basic problems with mobile payments are mainly related to *usability*. For example, MeT [MET] aims at strengthening the secure practices of mobile payments to back up the equipment manufacturers' implementation congruity. With regard to usability, MeT has defined "Consistent User Experience" (CUE), which considers the situation understood by the user, especially when using payment services.

A user should experience as uniform a payment logic as possible when using different services, after which the trust towards mobile payment will increase. The convergent phases that users experience, as defined by MeT CUE, are mainly

- initiation of the device, certification download, registration
- transaction stages (opening the connection, user authentication, digital signing, handling of special situations)
- management of PIN code, certificates and tickets.

4.2.5 Privacy

Privacy means an end user's right to control the information concerning him, to affect the handling of this information and, when necessary, get information from the parties that manage it. From the privacy point of view, it has to be remembered that as a service platform mobile phone 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. A mobile device as a use environment is rather restricted, so the service developer has great influence on how the end user can manage information related to his privacy. The need for privacy protection is guaranteed in the Finnish constitution.

Example: 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 a service is offered from a country with no legislation

forbidding this. Generally, collecting personal information always has to be justified and no end user information should be collected or stored unnecessarily.

As the volume of service use increases, the possibility of collecting so-called profiling information about viewers also increases – for example statistics on music listening habits. By default, there has to be permission from the user for this kind of information collection. Profiling data should not be transferred from the mobile device without user acceptance in any phase.

Privacy also means anonymity, which is secured with session keys in the mobile world. The correct identifier has to be used when the phone is turned on, but after that the connections are handled and transferred with pseudo identifiers that are disposable. When an Internet dimension is added to mobile use, privacy protection has different solutions in the current IPv4 networks and new (e.g. UMTS) IPv6 networks. There are solutions on the horizon, where the user identity is handled with so-called public crypto keys. One dimension of anonymity has to do with the prepaid connections. Whereas most of the users in Finland are identifiable by means of their SIM card (invoicing is done using that), elsewhere in the world a prepaid SIM card with a related phone number that cannot be directly connected to a person is generally used.

An interesting aspect of mobile anonymity is related to localization information. The authorities, under certain conditions, have the right to obtain information on phone location for localization purposes. If the phone is within the range of audibility of many base transceiver stations, this particular location can be very accurate indeed. This information would certainly be exploitable for other purposes as well, for example for family or friend use, but possibly also for advertising. In Finland this requires permission from the user, but there are plenty of possibilities for misuse. The special character of localization information for privacy has gained attention with the legislators. Localization information use for electronic communication is separately restricted in the Data Protection Act.

Privacy regulations have been defined in the EU directives 95/46/EY (personal data), and 2002/58/EY (data protection of electronic communication). Thus privacy means the right of an individual to decide for himself when, where, how comprehensively and for what purposes information about him is given to others. A good example of data transfer requiring privacy is health-related information. Some proposed business models can even be in contravention of a citizen’s privacy protection.

4.2.6 Resource protection

The system producing mobile services, as a whole, consists of different kinds of networks and devices connected to the networks. 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 subsystem, or other parties. Resource misuse is prevented by monitoring and restricting its use. Examples of misuse-restricting mechanisms are access rights for users or files, firewalls and antivirus programs.

Computers – from mobile phones and PDAs to PCs, servers and supercomputers – are usually based on a couple of basic components and the functionalities offered by them. A processor is the heart of the calculation and it offers applications processing time, whose use 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, whose usage restriction is usually possible by operating system settings.

Computer data buses and bus connections enable data transfer between different computers, networks and users. It is usually possible to restrict data transfer with the network settings of the operating systems and equipment, as well as the access rights of external devices.

Because the resources needed for processing the protocols used in data transfer, like processor time and memory size, are increasing as the abstraction level increases, the lack of these resources becomes a hindrance for higher level protocol data transfer speed. Because of this, for example, restrictions on processor time and memory use have an effect on the data transfer speed. In addition to just monitoring the restriction of a single resource usage, one must also look at 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 in which the system cannot offer services to the users. Likewise, one erroneous process inside one device should not jam the whole device by excessively using processor time and RAM memory. How much use one server process or subsystem computer can make of common shared resources, like data transfer capacity, processor time or memory, is a question of design. For example, the processor time and memory usage of the server processes can be restricted so that the resources are sufficient for a certain number of service processes, and the subsystem data connections can be limited so that the transfer capacity is enough for a certain number of simultaneous service requests.

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

Computer processing capacity and memory size increase according to the so-called Moore law. Because of this, the number of programs has been able to increase in such a way that new and always easier-to-use functionality has been built on top of existing functionalities and implementations. Because of this increase in the abstraction level, attacks are always targeted at utilizing the 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 is to be expected that when new, easy-to-use techniques, 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. Mobile phones and PDAs will also need a more sophisticated firewall in the future.

There already is a Symantec firewall and antivirus program available for WLAN smart phones (Nokia Series 80) that prevents intrusion to corporation networks via phones, with properties such as remote administration as well as definition and configuration of information security practices.

The rapid growth in the abstraction level and more and more hostile application environments have revealed that all existing programs have included programming errors that an attacker can use to run malicious programs in the target computer. Correcting these errors and updating the applications is nowadays easy in general purpose systems, but in closed 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 digital signature of program files, has made exploiting such vulnerabilities more and more difficult. These restrictions have been successfully evaded by using higher level protocols, such as html and programming languages like JavaScript. In addition, on top of the protocols and programs there is still a human as 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 the program execution and other rights can be more accurately restricted. However, this power to restrict execution is questionable because it is way too easy to misuse it for financial advantage, so its future in 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; the threats in closed systems, such as forging pay cards, can be very different to those in open systems.

4.2.6.1 Protecting servers in practice

A server is a software or computer with its software that 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 the new attack methods and vulnerabilities are found. The means of administration are different in various service platforms 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 notify information security threats [FICORA]. Servers' administrators should follow this kind of current, general security-related information. For example, according to CERT-FI's "annual review 2004", malicious programs targeted at mobile phones have developed in a more practical direction, so programs accessing mobile phones should be carefully controlled on many levels, such as the servers for mobile services. Generally speaking, preparing actions against Internet threats will be emphasized in the future and will require more and more active actions and practising of the situations. The use of IRT (Incident Response Team) groups is emphasized.

Securing a server that is providing services is an on-going process. When choosing the service-producing protocols, network architecture, server platform, etc., in the design phase one has to pay attention to the effect these choices 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 the level they require. General protocols, such as SMTP, POP, IMAP, http, TELNET or SMB, should not be used as clear text in network traffic if transferring information can be confidential and the network unreliable.

The backup and access control of the data needed to produce the service and 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

the server platform – i.e. the computer architecture, 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 on the platform's security features. The most secure environment will deteriorate over 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 by 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 according to 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 copy, cryptographic protocols, VPN devices and software, firewalls and antivirus programs, make the system more complicated and thus possibly more vulnerable. The more surfaces in the system there are, the easier it is to attack it. The administrator has to know how to act in fault situations, so understanding the functioning of the whole assembly and a single component is crucial. Any component whose function is not understood should not be used in servers. Using a separate test system is recommendable, as there the service developers and administrators can act as they please without jeopardizing the actual system.

When the server is functioning the administrator has to observe its function regularly, at least 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 for 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, preparations should be made for the failure of these services for one reason or another.

Because a corporation's internal threats should be prepared for as well, the permitted and forbidden actions of a server and system's legal users (and administrators) should be in the public domain inside the company. The requirements set by legislation, for example concerning handling personal data and messages, also have to be known by the individuals that work with the system and service. If the employees understand their

tasks and responsibilities, they are most likely 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.

Example of protection: Actions related to protecting mobile servers:

- Choose the protocols providing the service and mobile platform according to one's own knowledge, standards and recommendations by others. Restrict services (attachment interfaces) to cover only the essential.
- Prevent mobile user mistakes concerning server identity. Use server certificates that include a server domain description. Ensure that the mobile user clearly notices which domain's service he is aiming at.
- Centralize user rights management and monitoring. Ensure the implementation of two-way authentication with a mobile terminal.
- Update software regularly. Use a security program, like a firewall and antivirus program. Backup server data with log file collecting.
- Constantly monitor and analyse possible mobile-related threats. Manage dependencies and complexity by sharing implementation of functionalities among different devices.

4.2.6.2 Intrusion detection practices

A general approach to detecting system attacks is:

- Follow the unexpected and suspicious events that face the system and network traffic in an automatic and systematic manner. Do not forget physical protection and detection if it gets broken. Always use other people's observations to complement your own detections and compare them.
- Check further if something unusual has been 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.

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 concludes decisions based on known attack patterns or by artificial intelligence studying network behaviour. Attacks based on attack patterns are quite clear and there are ready action plans for them. Network sensors are quite general. Information security software producers integrate IDS features into their own packages. A notable point is that encrypted connections can prevent IDS devices from finding forbidden messages of in network traffic.

The control system manages the 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 the ICT architecture is still challenging and difficult to implement.

A system's own management applications (mainly) produce only a very initial analysis of the exceptions in the network events. In most cases the final analysis requires much knowledge with which to interpret the effect on the used environment. Interpreting misuse cases always requires a lot of knowledge among the employees. The challenge is still the attacks detected from network deviations. Certain qualities can be analyzed in many points. For example, peer-to-peer connections can be caught in IDS, proxy, antivirus or firewall device, or some intelligent switch. Then the skill to manage the whole system is emphasized.

Companies and organizations have traditionally used several small-scale attack databases to manage information security threats. This work has been frustrating when new attacks have occurred without warning. At the end of March 2005 the large telecommunications companies decided to share information on information security attacks in the Fingerprint Sharing Alliance [ARBOR]. This coalition collects and analyses information about all potential attack attempts and an automatic system warns all parties as soon as possible, for example denial-of-service attacks. A special program in the system monitors the networks and aims at recognizing 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.

It would be useful if in future active attacks detected by network operators were reported to other service providers. and possibly to end user devices (for example by SMS), in real time.

4.2.6.3 Anti-virus software and malware in practice

Table 10. Malware with related subtypes. Sources [VAHTI 3/2004] and [Korhonen].

Malware	Subtypes/spreading	Significance in a wireless terminal	Basic protection
Viruses – copy and spread themselves into new targets.	File viruses – attach into program files and spread in every way that transfers program files.	Not yet a problem in Finland. Problems increase as the mobile viruses and downloadable programs become general. **Lasco** virus/worm.	**Virus scanning** and **deletion**.
	Macro viruses – attach into application documentation files. Spread with the documents regardless of the operating system.	Not yet a problem, at least in Finland. Problems may increase as the office applications increase in wireless terminals.	**By preventing** macro execution, using file types without macros.
Worms – (subset of viruses) – spread by deliberately using a network connection.	Command line viruses– utilize scripts in the target system.	Not yet a problem, at least in Finland.	E.g. **settings**.
	Mail worms – spread in MMS, email or its attachments.	**CommWarrior** has been found in Finland (sends MMS messages without permission). **Mabir** sends MMS messages. Not yet a particular problem in Finland.	Firewalls, automatically updated virus scanning, network segmentation and gateway virus protection, choosing system, information security updates.
	Network worms – utilize network connections independently.	Worms exploiting Bluetooth are **Lasco** (contaminates program files), **Cabir**, **CabirDropper** (destroys other programs) and **CommWarrior**. Cabir has been found in Finland, but is not yet particular problem.	
Troijan 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.	Groundless invoicing and use of services. **Brador** opens a backdoor. **Dampig** destroys system files. **Drever** prevents functions of antivirus programs. **Fontal** prevents turning the phone on. **Locnut** destroys the operating system. **MGDropper** causes dusturbances in the programs. **Mquito** sends SMS messages.	E.g. user **awareness** in software installations.
Spy and adwares	Programs including spy components. Spy feature can be notified, but some are installed secretly.	No significant problems noticed in mobile devices.	**Protection programs**, secure **file system** and user **awareness.**
Hoaxes, chain letters and joke programs	Hoaxes e.g. waste time, ask to remove files. Joke programs give false warnings. Spread by unsuspecting users that send them forward.	Hoaxes can often be found.	E.g. user **awareness**.

Malware can spread in smart phones through games and music programs via an Internet connection, peripheral device connection, or workstation synchronization. These risks have to be prepared for with planning and managed usage policy.

Malware means harmful computer programs. Malware becoming relevant to a smart phone and PDA in the near future are classified in Table 10.

Viruses cause at least indirect damage by using disk space, causing compatibility problems and slowing down device functioning. They often include programming errors that may cause damage, even against the virus programmer's wishes. If device and system providers consider information security in the design phase (e.g. in architectures) as much as possible, customer satisfaction will increase as misdemeanours and the need for protection implemented afterwards will decrease.

A virus called CommWarrior has been found in mobile phones in Finland. The virus functions in Symbian Series 60 phones and spreads using MMS messages and Bluetooth. The Cabir worm has also been found in Finland. Spam messages and viruses have to be considered when securing a mobile phone, e.g. in the mobile phone network's gateways and with filters used in email servers.

The network operator must protect the network interfaces and devices with virus protection programs. This is not entirely enough, even if the network is a separate network with access to the Internet in certain places. A single actor cannot generally take responsibility for the whole of the information security; effective protection also requires daily international co-operation between operators. Network protection can occur by monitoring data transferred by the following protocols: SMTP, POP3, HTTP, TFP, IMAP4, NNTP and SOCKS.

There already are antivirus programs, malware protection programs and firewall programs available for smart phones (e.g. some of the Symbian phones). Antivirus programs for smart phones are sold by F-Secure, Symantec, Trend Micro and McAfee. Unfortunately, their full-scale use when running in the background can slow down the phone's other functions considerably because of its restricted computing capacity. In the future the need for using security programs in portable terminals will increase significantly. An especially important for technological protection are the properties of the device's memories, such as closed memory areas, areas that do not execute programs, ROM areas, and so on. Both device and SW implementations for these exist already. The program functions should be monitored with methods by which both known and future viruses can be effectively detected (e.g. Norman). New malware spreads really fast, so a mere search for the virus identifier is not enough.

Example of protection from malware: The following actions will assist in managing protection from malware in service development and service production organizations:

- Workstations and servers administration should be handled by a specialized backup organization that knows all the vulnerabilities. Devices should be 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 LAN. In addition, critical servers, test and production systems, as well as workstations in the LAN, should be separated into their own segments. Possibilities for malware should be limited by means of device and network architecture.
- The LAN must be separated at network connection points with malware protection, firewall and router security features. Remote connections have to be secured separately. Protection programs removing malware from user messages can be installed into a mobile phone network's gateways.
- The same protection for smart phones and PDAs as portable computers. Secure settings and automatic updates of terminal programs and protection are to be taken care of (e.g. preinstalled security programs in the factory, organization actions). Users must be forbidden to install unknown programs into smart phones and PDAs.

5. Special characteristics of mobile service development

Due to the previously mentioned complexity of threats and solutions, the development of mobile terminal services is difficult. This is slowing down the emergence and deployment of competent services. This is why this chapter will try to address the service developer's information security solutions and processes that have been proved or are estimated to be best practices (especially on the server side). The most important terminal device-related problems and solutions are also examined.

The information security integration and ease of use, and how they are best implemented from the service developer's point of view, are studied in this chapter. 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 the 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. Not even using industrial company interviews was enough to drill into this problem at a satisfactory level because no such industrial case could be found that could have been freely discussed or which all the interviewed people would have been familiar with at an adequate level.

New kinds of trust models will be built on new services in the future. For example, in the Visual Radio service launched by Nokia the actors include a radio station, a service developer, a network operator and a device manufacturer. All these actors should have a common body of trust. As for Mobile Television, for example, a broadcasting company, a television network operator and a mobile network operator can get added value from each other. Could an independent actor, the trusted third party, be used to ensure trust?

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 users' actions (possibly due to an inadequate amount of

information given to them) and only 20 % is caused by information technology [YRTI]. It is clear that to build trust in organisations attention must be paid to the way in which important data for both the organisation and the customers is being stored and how it is distributed. Unclear methods of handling data may cause breaches of contracts or even illegal actions. 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 prepare to maintain the service level necessary for functioning.

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

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

In an international comparison the banks are highly trusted as electronic banking service distributors in Finland. 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 and how these are carried out in practice. The development of information security must be a part of the strategic planning and goal setting of the organisation. Furthermore, the organisation must have a defined information security policy and practical guidelines for implementing it.

The trust of the users and other actors taking part in the service development for the chosen service concept can be raised by using known reference implementations, the best tools, applicable methods, and standards as a basis for 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 the added value for an actor in the network could be increased fame or marketing put into practice through a service/pilot.

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

An example of technological factors for building trust:

- Reliable identification of the user and service.
- Use of a well-known service platform, assuring 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 (for example, OMA standardized).

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 functions (including information systems and systems).

Other trust-related factors are

- 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.

5.3 General considerations of service development

5.3.1 Stakeholders – value net

A mobile service value net is traditionally presented as in Figure 7.

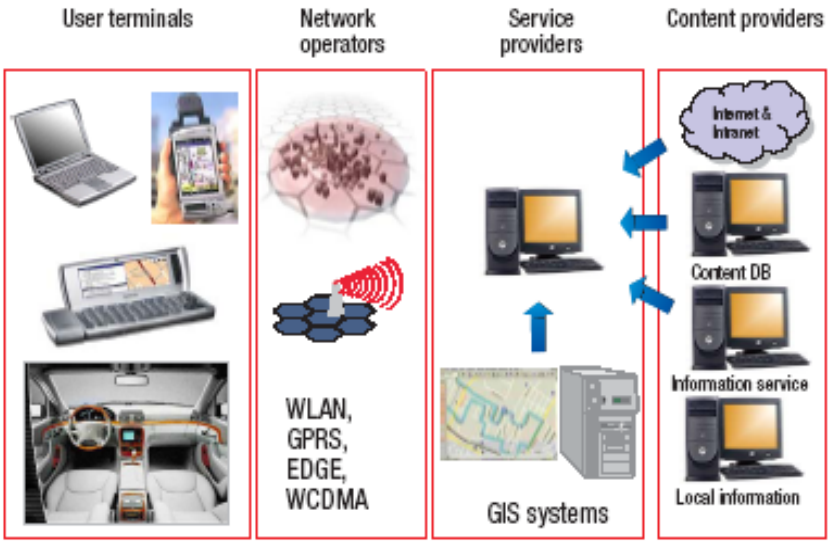

Figure 7. The mobile service value net [Alahuhta].

A value net is beginning to be an outdated concept. Nowadays the focus is more and more on the business environment, where networks and alliances are made for entering markets. The revenue logic in the Internet is often launched by using free services, and the same logic could be applied to mobile users. In this case one could speak about a value net where each actor can utilize the network by various ways. An example of this is presented in Figure 8.

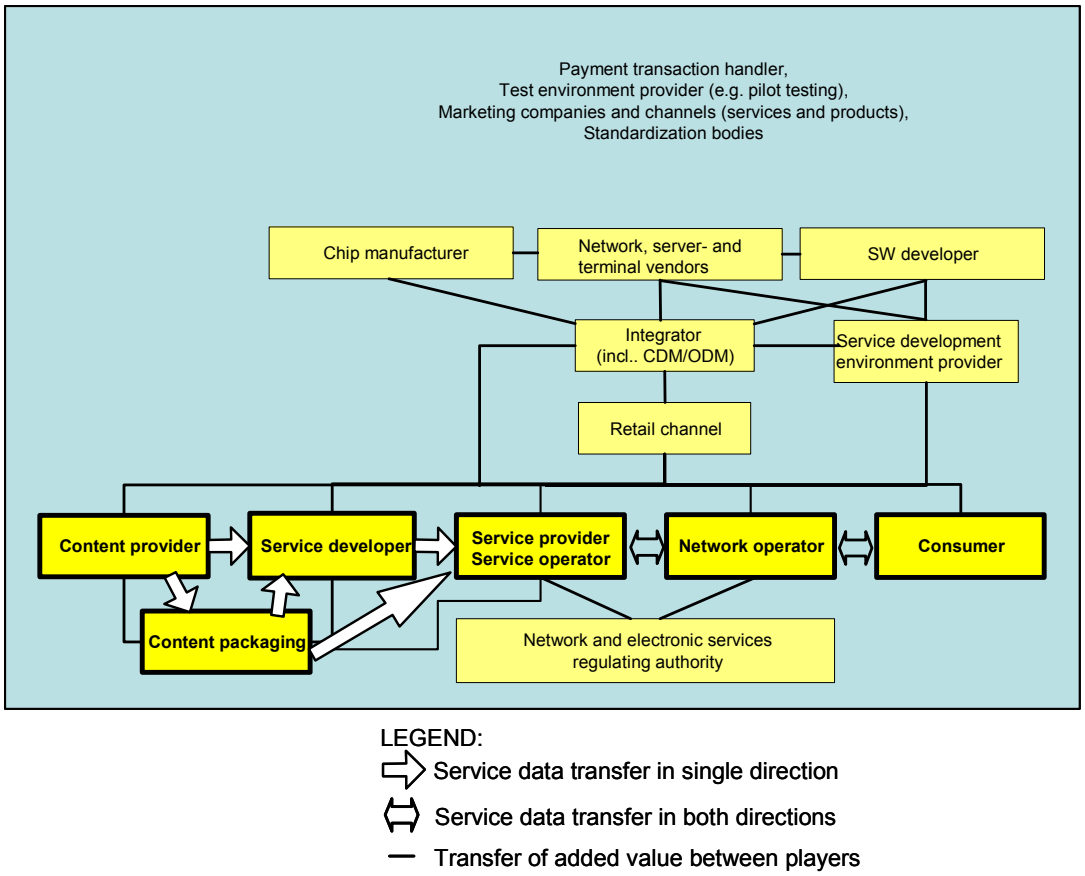

Figure 8. A simplified generic model of the mobile service value net.

An example of the actors: In Figure 8, the copyright organisations (such as Teosto) can be included in the content providers on the left. The consumers may directly need the service development environment (on the right). That is due to the existing PC applications for mobile phones, which even an ordinary user can use to make his smart phone's interface as individual as possible (including fonts, graphics and audio).

A very centric actor in a service and development process is the integrator who bundles up products made by various manufacturers and developers as one functioning service entity (see Figure 8). A service developer can itself act as an integrator, at least to a certain degree. However, this kind of action usually requires a specialized party who has already gained the necessary know-how with the technical environment for the integration of implementation and testing. Regarding the server side development, the integrator often co-operates directly with the service developer or provider, so no distinct retail channel needs to be used. Furthermore, the products used by the integrator are typically formed from earlier value chains, such as technology platforms (HW and SW) in the terminal and server side, and general purpose tool and application programs and circuits.

The service developer has a very centric role because it has to co-ordinate its actions with, for example, content providers, content packagers, integrators, development environment providers and service providers. When generating the ideas, and in the design phase, the active part of the value net should be as well defined and durable as possible in the long run.

An example of a value net: A functional value net is a mobile phone ring tone service. Teosto r.y. (registered association) has defined the licence terms [TEOSTO] (simplified):

- Length of the composition no more than 30 seconds, including monophonic, polyphonic and sound recording ring tones.
- The fee is on 12 % consumer price (excl. vat), at least 10 cents/download.

At the launch of the LUOTI program it was noted that the customer feedback should be available for the whole value chain. This naturally requires good co-operation between all actors. The cost of the used information security elements must also be in balance with the service fees, otherwise the service is not profitable.

The service developer and provider have a centric role in threat prevention. New actors coming into the field may be small-sized in comparison with the responsibilities they are facing. On the other hand, many innovations (also in services) arise in small-sized companies, which would possibly want to implement their own innovations. This is why the authorities should be consulted to find out if the actors have enough resources to carry out such actions in a secure way. Resources are the key word. There are always bigger risks and more information security holes in a complex environment. Everyone must ensure that the information security services and practices in use are of the correct scale.

5.3.2 Information security orientation

Information security orientation in an organisation can be composed of risk management, strategic planning and resource allocation.

An example – One solution for information security-centric action in developing a service:

- Protect your own network.
- Create the development environment and/or test network and isolate it (at least partly).
- Find good actors – check the information security level of different actors.
- Inspect the delivery chain (from whom and how each component has been acquired, etc.).
- Keep in mind that information security is involved in every phase of service development.

5.4 Service development process

A predetermined process is often followed when developing electronic services. The service development consists of different phases, each of which has their 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 the different actors communicate and what information do they transfer? In practice, various issues may proceed along an unplanned route, so the process is only just an aid helping to understand the big picture.

Even if the service development process were very well defined it is crucial to remember that it can never take account of all the information security factors 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 the threats. An example of the phases in the service development process according to the LUOTI programme is presented in Figure 9.

Figure 9. An example of the phases in 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 11.

Table 11. 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.		○	●	●	○	○	○	

Furthermore, a more detailed table (Found Threats at Each Development Phase) is presented in Appendix B. There the best effort is made to estimate the impact of the actors concerning the threats in different service development phases.

5.4.2 Generation of service idea/concept

A service idea can often be generated by the content producer or service distributor, or, of course, by the service developer itself. These actors have responsibility for their own products and their quality. When generating ideas one has to consider which 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 can 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. Finally, the service quality and robustness is tested.

An example of the idea generation phase actions:

- Create a threat analysis, define the target group and service accurately.
- Define the interfaces; which issues can become threats (and how).
- Create a threat tree (root causes). Use information security experts to evaluate the threats and counter measures.
- Define which threats can be realized in practice and do we have resources to protect from them.
- Manage risks.
- Make preliminary plans for all the processes included in the development. Find usable standards.

5.4.3 Design

The service design process is very dependent on the service being developed. If the implementation of the service requires a technology enabler such as Bluetooth, it is important to carefully choose and evaluate the technology platform suppliers, circuit

manufacturers and driver developers. Often the reliance is on the software developers' and device manufacturers' ability to maintain solid information security and quality in their own environment and technology platforms. Suitable tools related to the chosen technology, deployment design and training are important for the integration to be successful.

If the service development does not require the design or implementation of a technology (for example a protocol), the focus can 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 what kind of experiences 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 which user groups will be using the service. This clarifies the criteria for the ease of use (for example the parameters and settings for information security features), which is especially important for the targeted service. In some cases the service users can be very demanding. In those cases they must be given a chance to change the information security settings when needed. Then extra care must be taken to ensure that the user is informed of the consequences of these setting changes.

A service implementation often requires programming and using different program libraries, which are typically called Software Development Kits (SDK). Programming must be phased beforehand to include the business planning, requirement specifications, and implementation plans, as well as 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.

An example of the actions related to the service design phase:

- Define any needed technology enablers. Choose the best technology suppliers; ask for examples of where their technologies are already in use.
- Make yourself familiar with the tools needed in the technology and plan their purchase if necessary.
- Do preliminary research, for example what pilots have been made earlier.
- Define the usability requirements for the planned user group. By what means can they be carried out?
- Ensure the quality of the business plan, requirement specifications, implementation specifications, testing and deployment plan.
- Plan the auditing of the development environment and documents.

5.4.4 Implementation

An important part of the service implementation phase is evaluation of the different implementation alternatives and choosing the best of them. Choosing the right actors is very important. Information security is a fairly new issue in the implementation of mobile services because the mobile networks and devices have previously been apart from the Internet. An appropriate development history creates the basis for implementing new services. This is not typically the case in implementing mobile 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 proven to be secure in any circumstances in advance. Information that is secure and reliable in ways that are suitable for the application development system being used should be put into practice when implementing the service, especially in the terminal devices.

Special attention should be given to the tools being used (for example encryption libraries, protocol implementations, user interface development environments). Ready-made solutions already exist on the server side. On the other hand, the tools used for implementing the terminal information security are varied and it is hard to find a functional entity for product development. So, the services must be developed separately for each mobile platform. The smart phones have eased this dilemma a bit. The Nokia Series 60 is the best example of Symbian interface versions where, among other things, IPSec and SSL/TLS are included. The smart phones are not very common yet. As a result, the service developer and the provider are dependent on several different mobile manufacturers, each of them having their own solutions for information security. In many cases the end-to-end compatibility of the information security features of the server and the mobile phone has not been properly tested in practice.

There are information security responsibilities according to the Act on the Protection of Privacy in Electronic Communications (PPEC 516/2004) and strict regulations for personal data handling by information security, purpose of which are vital liability risks concerning mobile communication. How suitable the regulations are depends on many issues. For example, is the mobile device connected to a public communication network or only to a local network (e.g. Bluetooth), is it a question of communication or purely about data transfer between the devices (which is often the case in RFID), and are there confidential messages transmitted in the network? Defining these liabilities and responsibilities, and understanding one's own role in this issue are centric demands when taking information security into account. If the regulations are to be applied, the party handling the communication identification data is responsible for storing detailed

event logs about who, when and for how long he handled the data. To clarify this it must be noted that the log events of the personal data items (for example who has processed the data in the organisation) are in question, not the storage of the message identification data.

An example of the actions to be kept in mind during the service implementation phase:

- Define different implementation possibilities and select the best. Select the actors.
- Decide the secure process to be used. Remember to ensure the subcontractor's process as well.
- Decide the encryption libraries, protocol stacks and development environments of the user interfaces to be used. Leave enough margins to change some of them if needed.
- Check that the processing of the person and identification data will be done appropriately.

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 analysis of the program should be used. The program should be seen as both an open and a 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 whenever possible. The evaluation should also include the normal functioning of the program when the system is strained. The strain can cause denial of service or enable attacks due to the non-atomicity of the operations. Fail-over testing is used to find the consequences of the service overload.

The importance of interface testing is emphasized in the network environment. To ensure the correctness of the input from the environment the program should be tested all-round. The correct syntax of the all interfaces in the program must be tested extensively with both legal and totally false and malicious inputs (hacker testing). In other words, reliability tests in addition to integration tests are run in the environment interfaces. One solution is to use external penetration testing services that try to find the application faults commonly used in breaking into the system. Regression tests are very important when iterating the program so that old faults will not reappear when the code is renewed.

5.4.6 Deployment

It is wise to be prepared to use experts and special tools at the beginning of the deployment phase. Information security auditing should be done before the deployment to ensure that everything necessary to implement information security is done. Patch management (application patches and service packs) must be taken care of before 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 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 the 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.

From the customer's point of view it would be simpler if the mobile phone and the subscriber connection (SIM) could be purchased as an integrated, pre-installed package. The drawback would then be an unintended commitment to operator services due to the customer's lack of knowledge. The marketing material would also be a part of the contract. If information security is promised in the marketing material, the user has the right to demand it. He also has the right to claim compensation if he has relied on the promised security and has suffered damage in some way – for example by losing contact information stored in the service.

5.4.7 Maintenance

If there are defects and faults in the products and services, they are vulnerable to unauthorized use during the maintenance phase of the service. Program updating is a very important way of protection against found faults. Information sources for preventing vulnerabilities can be found through SANS (SysAdmin Audit Network Security Institute), [SANS].

The vulnerability handling process is a centric part of the service maintenance phase. This means 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]:

- the party who has found the vulnerability

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

The information security actions are unfortunately usually reactive in the maintenance phase; 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. At best, they succeed in guaranteeing the data integrity and reliability, but often the drawback is a slight weakening of the availability. Complexity avoidance has proved to be a positive factor in all areas.

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, as they are independent organisations, they can support the smooth success of the process.

An example of the actions during the service maintenance phase:

- Define the actors taking part in the vulnerability handling. Use processes to detect vulnerabilities and plan new ways of detection. Agree on the processes that can be used for handling and fixing the found vulnerabilities (both internal and external actors).
- Observe attacks. Plan the counteractions against a detected attack.
- Use a process to update all applications (patch management). Define responsibilities.
- Arrange the collection of the log events and anomalies.

5.4.8 Enhancing a service

Service enhancement can be due to several reasons – for example the system cannot serve the increasing number of service users. These new users may have different service expectations than the ones the service was originally created for. One reason can also 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 from a new kind of network, e.g. a mobile network through GPRS or EDGE, in addition to the previous GSM data. 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, future capacity needs have to be considered. The capacity of

the servers or applications as well as the sufficiency of the information security services can cause problems in the old architecture. The user identification methods may need altering. Then the use of the service via the new network may require a new type of user identification. The user management should be consistent in general.

Change management is centric when enhancing the service. It must be defined by using a matrix to show all the items the change impacts on and how these impacts are taken into account in the implementation. Of course, the service testing should be done as soon as possible after the changes.

Although problems in the pilot phase may not have been detected, the increase in the number of users and new users' different attitudes can become a factor that must be taken into account in advance of 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 the 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. Consistent practices should be developed to support different actions.

An example of the actions during the service enhancement phase:

- Go through the service design phase once again and define the changes to the environment or the assumptions for the service.
- Design the changes to the architecture and information security services.
- Unify the actions (for example user management).
- Manage the changes step by step, testing the impacts of each change.
- Plan the feedback gathering from the system functionality and utilize it.

5.4.9 Terminating a service

The questions related to customer information security are emphasized when terminating service. 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 also exist. Their obedience ensures the correct actions when terminating the service. New and small-sized actors do not always have an appropriate culture for terminating the service. Then the procedures must be created and written down so that they are available to all parties. The security policy related to service termination must be in balance with the services offered, the liabilities and the risks.

References

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

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

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

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

[BIOAPI] http://www.bioapi.org/

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

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

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

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

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

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

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

[Garfinkel] Garfinkel, S., Spafford, G. & Schwartz, A. 2003. Practical Unix & Internet Security. 3rd edition. Sebastopol, CA: O'Reilly. 986 p.

[GSMA] http://www.gsmworld.com

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

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

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

[HST] HST Arkkitehtuurit ja liiketoimintamallit määrittely. Versio 1.0. 12.5.2003. (In Finnish.)

[INSTAT] http://www.instat.com

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

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

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

[Karila] Karila, A. 2005. Internet-puhelut (VoIP) – Selvitys. Liikenne- ja viestintäministeriön julkaisuja 16/2005. ISBN 952-201-332-3; 952-201-333-1. http://www.mintc.fi/oliver/upl402-Julkaisuja%2016_2005.pdf (In Finnish.)

[Korhonen] Korhonen, H. 2005. Haitalliset ohjelmat mobiilipäätelaitteissa. Harjoitustyö, toukokuu 2005. Tampereen yliopisto, tietojenkäsittelytieteiden laitos. (In Finnish.)

[Laakso] Laakso, M., Takanen, A. & Röning, J. 1999. The Vulnerability Process: A Tiger Team Approach to Resolving Vulnerability Cases. In: 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 (In Finnish.)

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

[LUOTI] http://www.luoti.fi

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

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

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

[ODRL] http://odrl.net

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

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

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

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

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

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

[TMP] http://www.trusted-mobile.org/

[VAHTI3/2004] VAHTI – Haittaohjelmilta suojautumisen yleisohje. (In Finnish.)

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

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

[VIRVE] http://www.virve.com

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

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

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

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

Appendix A: Questions in industrial interviews

General questions

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

From the point of view of a service developer, 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 the 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 on 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 give information 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 our 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 the 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, what currently used protocols most clearly form a joint between the IP and GSM worlds?

In your opinion, what 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 a vulnerability process do you have? Describe.

> (The interviewee is presented with a sketch of a general level diagram depicting the 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 we are heading in? For example: what functionalities/applications are to be taken into use in the near future?

What 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 and critical actors in each service 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 user's location data.	service operator, network operator
	Rights to use and copy contents (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
	Confidentiality of the user's location data.	consumer, service provider, service operator, network operator
	Rights to use and copy contents (such as video and audio).	consumer, content wrapper, service provider, service operator
	New kinds of use and operating situations (incl. e.g. WLAN, Bluetooth, RFID).	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, for example, by oversupplying, denying the traffic, spamming.	consumer, service provider, service operator, network operator
	Infallibility of emergency calls (due to e.g. devices and programs being incompatible).	consumer, service provider, service developer, service operator, network operator
	Viruses, malware.	consumer, service provider, service developer, service operator, network operator
	Risks of mobile 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 contents (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

Further information

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

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

Published by

Series title, number and report code of publication

VTT Research Notes 2308
VTT–TIED–2308

Author(s)
Ahonen, Pasi, Eronen, Juhani, Holappa, Jarkko, Kajava, Jorma, Kaksonen, Tiina, Karjalainen, Kati, Karppinen, Kaarina, Rapeli, Mikko, Röning, Juha, Sademies, Anni, Savola, Reijo, Uusitalo, Ilkka & Wiander, Timo

Title

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

Abstract

This study examines the major information security threats relating to mobile services and solutions to these threats from the service developer's perspective. Research methods employed include interviews with enterprises, literature searches, expert opinions and extensive rounds of commentary.

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

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

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

Keywords
information security, threats, wireless telecommunication, mobile services, mobile networks, mobile devices, authentication, identification, privacy

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

ISBN			Project number
951–38–6737–4 (soft back ed.) 951–38–6738–2 (URL: http://www.vtt.fi/inf/pdf/)			E5SU00589
Date October 2005	Language English, Finnish abstr., Swedish abstr.	Pages 95 p. + app. 4 p.	Price B
Name of project LUOTI		Commissioned by Ministry of Transport and Communications of Finland	
Series title and ISSN VTT Tiedotteita – Research Notes 1235–0605 (soft back edition) 1455–0865 (URL: http://www.vtt.fi/inf/pdf/)		Sold by 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 2308
VTT–TIED–2308

Tekijä(t)
Ahonen, Pasi, Eronen, Juhani, Holappa, Jarkko, Kajava, Jorma, Kaksonen, Tiina, Karjalainen, Kati, Karppinen, Kaarina, Rapeli, Mikko, Röning, Juha, Sademies, Anni, Savola, Reijo, Uusitalo, Ilkka & Wiander, Timo

Nimeke

Mobiilimaailman tietoturvauhkat ja -ratkaisut

Palvelunkehittäjän näkökulma

Tiivistelmä

Tässä julkaisussa kartoitetaan mobiilimaailman tärkeimmät tietoturvauhkat ja niiden ratkaisut palvelunkehittäjien näkökulmasta. Kartoituksen tutkimusmenetelminä olivat yrityshaastattelut, kirjallisuushaut, asiantuntijoiden näkemykset ja laaja-alaiset kommentointikierrokset.

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

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

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

Avainsanat
information security, threats, wireless telecommunication, mobile services, mobile networks, mobile devices, authentication, identification, privacy

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

ISBN			Projektinumero
951–38–6737–4 (nid.) 951–38–6738–2 (URL: http://www.vtt.fi/inf/pdf/)			E5SU00589
Julkaisuaika Lokakuu 2005	Kieli Englanti, suom. tiiv., ruots. tiiv.	Sivuja 95 s. + liitt. 4 s.	Hinta 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 2308
VTT–TIED–2308

Författarna
Ahonen, Pasi, Eronen, Juhani, Holappa, Jarkko, Kajava, Jorma, Kaksonen, Tiina, Karjalainen, Kati, Karppinen, Kaarina, Rapeli, Mikko, Röning, Juha, Sademies, Anni, Savola, Reijo, Uusitalo, Ilkka & Wiander, Timo

Namn

Hot och lösningar beträffande mobilvärldens informationssäkerhet Serviceutvecklarens perspektiv

Referat
I utredningen beskrivs de viktigaste hoten mot informationssäkerheten i mobilvärlden och lösningar på hoten ur serviceutvecklarens perspektiv. Som forskningsmetoder användes företagsintervjuer, litteratursökningar, expertutlåtanden och en omfattande insamling av kommentarer.

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

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

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

Nyckelord
information security, threats, wireless telecommunication, mobile services, mobile networks, mobile devices, authentication, identification, privacy

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

ISBN			Projekt nummer
951–38–6737–4 (häftad) 951–38–6738–2 (URL: http://www.vtt.fi/inf/pdf/)			E5SU00589
Datum Oktober 2005	Språk Engelska, finsk. ref., svensk ref.	Sidor 95 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	

New forms of electrical communications have emerged in recent years. Services with new functionalities such as Bluetooth, WLAN, localization, music, camera, and video can be used with mobile phones and PDA devices. This trend is opening up new business opportunities for the industry. However, it is also bringing new challenges for information security management.

This report includes an analysis of the most important information security threats and solutions from the service developer's perspective. The main observation from this report is to realise that mobile services include security threats and they should be taken seriously. However, security threats should not be considered a barrier to the development and deployment of new services. Easy-to-use security should be integrated everywhere in networks, devices and the net of stakeholders. Technological solutions should be adaptable to different kinds of business processes, so that they can be reused and the whole system does not need to be replaced by a new one during a change of business. Risk management and life cycle management are essential in the information security management of a product and service development environment. In order to include the whole value net of service development in the security management, it is important to analyse subcontractors' processes and test the quality and robustness of the service well in advance of the introduction of the service.

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 951–38–6737–4 (soft back ed.)
ISSN 1235–0605 (soft back ed.)

ISBN 951–38–6738–2 (URL: http://www.vtt.fi/inf/pdf/)
ISSN 1455–0865 (URL: http://www.vtt.fi/inf/pdf/)