Luottamus. Tietoturva. Sähköiset palvelut.

LUOTI-julkaisuja 9/2006

Information Security in Wireless Networks

Luottamus ja tietoturva sähköisissä palveluissa – kehittämisohjelma

Information Security in Wireless Networks

ISBN 952-201-782-5, 952-201-783-3 (verkkojulkaisu)
LUOTI-julkaisuja 9/2006
Helsinki 2006

Julkaisija

luoti

KUVAILULEHTI

Julkaisun päivämäärä

11.12.2006

Tekijät

VTT: Sami Lehtonen, Pasi Ahonen, Reijo Savola, Ilkka Uusitalo

Oulun yliopisto: Kati Karjalainen, Erno Kuusela, Rauli Puuperä, Juha Röning, Teemu Tokola

Julkaisun laji

Raportti

Toimeksiantaja

Liikenne- ja viestintäministeriö

Julkaisun nimi

Langattomien tietoverkkojen tietoturva

Tiivistelmä

Nykyisin ihmiset tulevat jatkuvasti entistä riippuvaisemmiksi langattomista tietoverkoista. Liikenne- ja viestintäministeriö haluaa tutkia, mitä tietoturvauhkia liittyy nykyisiin ja tuleviin langattomiin tietoverkkoihin ja millaisilla tietoturvaratkaisuilla näitä uhkia voidaan hallita.

Tämä selvitys tehtiin liikenne- ja viestintäministeriön luottamus ja tietoturva sähköisissä palveluissa (LUOTI) -ohjelmassa. Selvitys kattaa tärkeimpien langattomien tietoverkkoteknologioiden tietoturvan nykytilan, uhkat ja niiden ratkaisut. Avainteknologioiksi tähän selvitykseen valittiin WLAN, WiMAX, Bluetooth, 3G, RFID ja Flash-OFDM. Näiden tekniikoiden merkittävimmät tietoturvauhkat kartoitettiin ja niihin sopivat ratkaisut selvitettiin.

Yleiset tietoturvauhkat koskevat myös langattomia tietoverkkoja, joskin osa niistä on merkittävämpiä kuin toiset.

Palveluntarjoajan näkökulmasta uhkia ovat mm. petokset ja palveluiden luvaton käyttö, haittaohjelmat, tietoturvaongelmien julkisuusvaikutukset ja asiakkaiden yksityisyyden suojan menetys. Loppukäyttäjän tietoturvauhkia ovat yhteyden tai tunnuksien kaappaaminen, päätelaitteen eheyden menettäminen ja salakuuntelu.

Lisäksi langattomissa verkoissa on haavoittuvuuksia, jotka ovat näille verkoille ominaisia – niillä ei ole kiinteiden verkkojen luonnollista fyysistä pääsynhallintaa, vihamieliset käyttäjät ja radiohäirintä ovat heikosti jäljitettäviä ja niiden jäljittäminen vaatii usein erikoislaitteita ja valvontaa.

Avainsanat (asiasanat)

Tietoturva, langattomat verkot, matkapuhelimet, mobiililaitteet, tietoturvauhkat

Muut tiedot

Selvityksen katselmointiin ovat osallistuneet Janne Uusilehto (Nokia), Lauri Paatero (Nokia), Göran Schultz (Ericsson), Marko Helenius (Tampereen Yliopisto), Ari Vesanen (Oulun Yliopisto), Markku Kylänpää (VTT) ja Kimmo Ahola (VTT)

Sarjan nimi ja numero

LUOTI-julkaisuja 9/2006

ISBN

952-201-782-5, 952-201-783-3 (verkkojulkaisu)

Kokonaissivumäärä	Kieli	Hinta	Luottamuksellisuus
	englanti		julkinen

Jakaja

Liikenne- ja viestintäministeriö

Kustantaja

Liikenne- ja viestintäministeriö

Utgivare

PRESENTATIONSBLAD

Utgivningsdatum

11.12.2006

Författare

VTT: Sami Lehtonen, Pasi Ahonen, Reijo Savola och Ilkka Uusitalo

Uleåborgs Universitet: Kati Karjalainen, Erno Kuusela, Rauli Puuperä, Juha Röning och Teemu Tokola

Typ av publikation

Rapport

Uppdragsgivare

Kommunikationsministeriet

Publikation

Informationssäkerhet i trådlösä datanäts

Referat

Idag blir mänskor allt mer beroende av trådlösa datanät. Kommunikationsministeriet önskar undersöka vilka hot mot dataskyddet det finns i dagens och framtidens trådlösa datanät och hur dessa hot kan förebyggas.

Denna utredning gjordes som en del av kommunikationsministeriets LUOTI-program som syftar till att öka förtroendet för informationssäkerheten i elektroniska tjänster. Utredningen omfattar det dataskydd som finns idag för de viktigaste trådlösa systemen samt hot och lösningar. Som nyckelteknologier valdes WLAN, WiMAX, Bluetooth, 3G, RFID och Flash-OFDM. De viktigaste hoten mot dataskyddet i dessa teknologier kartlades och möjliga lösningar utreddes.

De allmänna hoten gäller också trådlösa datanät men vissa hot är mera signifikanta än andra. Från tjänsteleverantörens synpunkt innefattar hoten bl.a. bedrägeri och olovlig användning av tjänsterna, malware (fientlig progarmvara), dålig publicitet då säkerheten ej uppfylls och förlust av användarens integritet. Hot mot dataskyddet för slutanvändaren innebär kapning av förbindelsen eller användarprofilen, förlust av terminalens integritet och avlyssning.

Det finns dessutom sårbarheter i trådlösa nät som gäller endast för dessa nät. Näten skyddas inte av en naturlig fysisk utsträckning såsom fasta nät, fientligt sinnade användare och störsändningar är svåra att spåra och spårningen kräver ofta specialapparater och övervakning.

Nyckelord

Informationssäkerhet, trådlösa nätverk, mobiltelefoner, mobilutrustning, hot mot informationssäkerheten

Övriga uppgifter

Raporten har utvärderats av Janne Uusilehto (Nokia), Lauri Paatero (Nokia), Göran Schultz (Ericsson), Marko Helenius (Tampere Universitet), Ari Vesanen (Uleåborgs Universitet), Markku Kylänpää (VTT) och Kimmo Ahola (VTT)

Seriens namn och nummer

LUOTI publikationer 9/2006

ISBN

952-201-782-5, 952-201-783-3 (nätpublikation)

Sidoantal

Språk

engelska

Pris

Sekretessgrad

Offentlig

Distribution

Kommunikationsministeriet

Förlag

Kommunikationsministeriet

The publisher

DESCRIPTION

Date of publication

11.12.2006

Authors

VTT: Sami Lehtonen, Pasi Ahonen, Reijo Savola and Ilkka Uusitalo
University of Oulu: Kati Karjalainen, Erno Kuusela, Rauli Puuperä, Juha Röning and Teemu Tokola

Type of publication

Report

Assigned by

Ministry of Transport and Communications

Name of the publication

Information Security in Wireless Networks

Abstract

Today, there is a strong trend of people becoming more and more dependent on wireless information networks. The Finnish Ministry of Transport and Communications (MINTC) has considered this development worth of research by investigating the major information security threats concerning current and emerging wireless network technologies, and solutions managing the possible vulnerabilities.

This study was done as part of the Finnish Ministry of Transport and Communications' Development Programme on Trust and Information Security in Electronic Services, LUOTI Programme. The study covers information security in essential wireless networks technologies, information security threats and solutions. WLAN, WiMAX, Bluetooth, 3G, RFID and Flash-OFDM were chosen as the key technologies. The most significant security threats concerning these technologies were identified and solutions to secure against these threats are given.

Wireless networks share the common information security threats, however, some of them are more pronounced than others. From the service providers' point of view fraud and theft of services, malware, image problems and bad publicity relating information security incidents, and loss of privacy of the customers are main causes of worry. The end users are concerned with hijacking of connections or capturing of credentials, loss of integrity in the terminal, and eavesdropping.

Additionally, wireless networks have additional traits – they are not protected nor bound by the natural physical access control of fixed networks, the malicious users and radio interference are weakly traceable, and tracing them often requires special hardware and surveillance.

Keywords

Information security, wireless networks, mobile phones, mobile devices, information security threats

Miscellaneous

Following persons participated in the survey of this report: Janne Uusilehto (Nokia), Lauri Paatero (Nokia), Göran Schultz (Ericsson), Marko Helenius (University of Tampere), Ari Vesanen (University of Oulu), Markku Kylänpää (VTT), and Kimmo Ahola (VTT)

Serial name and number

LUOTI publications 9/2006

ISBN

952-201-782-5, 952-201-783-3 (www publication)

Pages, total

Language

English

Price

Confidence status

Public

Distributed by

Ministry of Transport and Communications

Published by

Ministry of Transport and Communications

Preface

The take-up of new wireless technologies and the increasing complexity of information networks are giving rise to new kinds of threats and challenges to information security. It is important that both the providers of electronic services and the end users of the services are aware of the security risks linked to wireless technology, and that they are able to take appropriate measures to prevent and eliminate them. At the same time it is important that service providers are able to make use of wireless networks and all their benefits as effectively as possible in their own business activities.

This report addresses security threats and solutions in wireless network technologies. It is based on a study funded by Finland's Ministry of Transport and Communications under its "LUOTI" Development Programme on Trust and Information Security in Electronic Services. The report focuses both on the end-user perspective and on the service-provider perspective. The goal of the study is to increase awareness of information security threats connected with current wireless technologies, and of possible solutions to those threats.

The study was carried out by a group of network and information security researchers at the Technical Research Centre of Finland (VTT) and the University of Oulu. It was managed by Mr. Sami Lehtonen of VTT. The research was conducted by studying technology standards and published security reports and by interviewing experts in the field. The work was supervised by Mr. Kimmo Lehtosalo of Eera Finland Oy and Ms. Päivi Antikainen of the Ministry of Transport and Communications.

The Ministry wishes to express thanks to the authors of the report and to Kari Heiska (Chief Specialist, Digita Oy), Ari Vesanen (Lecturer, University of Oulu), Kimmo Ahola (Senior Research Scientist, VTT), Jarkko Holappa (Research Scientist), Markku Kylänpää (Senior Research Scientist, VTT) and Heimo Pentikäinen (Research Engineer, VTT) for the valuable information, insights and comments that they have provided.

Helsinki, 11 December 2006

Päivi Antikainen
Ministerial Adviser
Ministry of Transport and Communications of Finland

Executive Summary

This study, a part of the LUOTI programme, is an overview of the security aspects of essential wireless networks technologies. WLAN, WiMAX, Bluetooth, 3G, RFID and Flash-OFDM were chosen as the key technologies due to being widely adopted. They differ a lot and any comparison between them would not be meaningful. However, they have some shared and some unique security threats. For instance, some uses of Bluetooth include messaging with previously unknown devices. In such cases, evaluating the security is up to the user.

Wireless networks share the common information security threats; however, some of them are more pronounced than others. From the service provider's point of view, fraud and theft of services, malware, image problems and bad publicity relating to information security incidents, and loss of privacy of the customers are the main causes of worry. End users are concerned with hijacking the connection or credentials, loss of integrity in the terminal and eavesdropping.

Additionally, wireless networks have additional traits – they are not protected nor bound by the natural physical access control of fixed networks, malicious users and radio interference are weakly traceable, and tracing them often requires special hardware and surveillance.

WLAN

Wireless Local Area Network (WLAN) technology consists of the IEEE 802.11 standards. WLAN technologies have been widely adopted in home, government and business use, WLAN being available virtually everywhere. All of these bodies have different security needs. Additionally, some WLAN networks are intentionally open, such as city WLANs. WLAN technologies have some built-in security features like Wired Equivalent Privacy (WEP, obsolete), and newer Wi-Fi Protected Access versions 1 and 2 (WPA and WPA2 respectively). WPA is a subset of mechanisms in the 802.11i standard and WPA2 is a full implementation of the encryption and key management mechanisms described in 802.11i.

As users access the internet via their WLAN connection, all the threats facing ordinary internet users apply to them. Another security threat in WLAN networks is a Rogue Access Point, which captures the connection of the end user. Quite commonly, an insecure corporate WLAN network may turn out to be an easy passage to its intranet.

The CCMP protocol and AES encryption algorithm can be considered as a useful security solution in WLAN networks in some scenarios. Some of the EAP authentication methods are not secure or suitable for wireless use. As of today, the most secure EAP methods are based on the Transport Layer Security (TLS) protocol. In large deployments, the use of IEEE 802.1x and an authentication server with PKI are also often needed for scalable, secure administration if WLAN link-level security is desired. In some deployments, the use of WLAN products with Wi-Fi Protected Access 2 (WPA2) certification is recommended for security reasons. The use of WPA is suggested if WPA2 is not available. With legacy devices, the use of VPN solutions in conjunction with WEP is advisable. In public WLAN networks where anyone can join and eavesdrop on other people's connections, corporate users should use VPN tunnels and all users should verify that application-level encryption, such as SSL or TLS, is used when necessary.

WiMAX

WiMAX (Worldwide Interoperability for Microwave Access) is described in the IEEE 802.16 standard and its official name is WirelessMAN. WiMAX provides either high bandwidth (raw data rates up to 70Mbit/s), or long reach (a maximum range of over 100 kilometres). The end-to-end authentication is adapted from the DOCSIS BPI+ security protocol and PKM-EAP, which relies on TLS. All user traffic on a WiMAX network is encrypted using AES or 3DES. WiMAX uses Time Demand Multiple Access (TDMA) so eavesdropping or a false BS attack, for example, can be difficult to conduct.

The old IEEE 802.16-2004 standard did not include the authentication of base stations, which meant that any base station could claim to be the right one. WiMAX management messages are not encrypted. The attacker may also replay previously captured packets. An attacker may also jam the terminal with modified MAC messages.

WiMAX IEEE 802.16e-2005 is currently considered as the most secure choice (PKMv2 supports mutual, manufacturer certificate-based authentication). The new standard also supports EAP-based authentication. The 2005 version is backwards compatible with the 2004 version. Hence, to attain more secure implementation, the backwards compatibility functionality should be removed from IEEE 802.16e-2005 based implementations!

Bluetooth

Bluetooth is a radio standard and communications protocol (IEEE 802.15.1) for wireless network personal area networks (PAN) that connect different, usually mobile devices together. Bluetooth offers three modes of security: 1) non-secure, 2) service level enforced security, and 3) link level enforced security. The SAFER+ algorithm is used for authentication and key generation. An E_0 stream cipher is used for encryption.

The Car Whisperer project showed that many Bluetooth devices still have the default manufacturer-set PIN code (like 0000 or 1234). Mobile malware, such as the Cabir worm, may use Bluetooth to spread. The main threats to Bluetooth users are data theft, unauthorised use and damage to devices. The Bluetooth protocol has received a significant amount of research interest and vulnerabilities have been found in a wide variety of implementations. The most significant technical security issue is the quality assurance of the growing number of Bluetooth manufacturers.

Most of the incidents where data has been compromised on mobile phones have not been caused by a problem in the standard itself, but rather in the implementation quality. The E_0 stream cipher is fairly secure, although not flawless. Many Bluetooth devices hold little information of value and require little encryption (for example, an hf-earplug – half of the conversation is audible). However, laptops and smart phones that also typically have Bluetooth, contain often significant data. Usually, it is wise to keep Bluetooth turned off, unless it is being used. Likewise, although it is a weak form of defence, it is best to choose the non-discoverable mode in your Bluetooth connection setting, so others won't discover the device. In general, a security-conscious approach for the user is advisable.

3G and 4G

3G means the third-generation mobile phone networks or UMTS in the Europe. Data services in UMTS are like an IP network from the end user's perspective, so the information security easily associates to IP network security. However, UMTS is not as open as the Internet. Securing the UMTS network is first and foremost up to the device manufacturers and network operators. For this reason and the complexity of the standardisation, 3G is in practice out of the scope of this study. 3G devices can usually be connected to the Internet so, depending on the operating system, they will be vulnerable to mobile viruses and other forms of malware. The 3G field is so wide, that not all information security threats can be thoroughly covered in this study. Rapid development and new features are making 3G terminals start to resemble personal computers. This means that the threats to 3G and 3G devices will also start to resemble those of personal computers.

The security of third-generation radio networks is under the regulatory control of governments and international organisations that support co-operation between operators. The following steps can be taken by the user to improve security: Make sure that the PIN request is activated in your mobile phone. Use the barring and restriction services provided by the operators. Keep your mobile phone's IMEI code in a separate place in case your mobile phone gets lost. Make regular backup copies of mobile device memory on your computer or memory card. Store the backup in a safe place.

You may receive a call or an SMS message in an effort to commit a phishing attack against you!

4G is an abbreviation of fourth-generation, the successor wireless communication technology to 3G. This term does not refer to one particular standard, but describes several different but overlapping ideas. 4G refers most likely to wireless technologies to be deployed between 2010 and 2015. Some of these technologies may have similar (or even the same) threats to one of the technologies evaluated in this study. Analysing the current threats against 4G security was not relevant to this study.

RFID

Radio Frequency Identification (RFID) an identification method which relies on storing and remotely retrieving data using devices called RFID tags. These can store data in their memory, which can be fetched by remote readers. RFID tags can be classified according to their source of power. The tags can be passive, semi-active or active. RFID tags operate either at High Frequencies (HF) or Ultra-High Frequencies (UHF). The cheapest tags do not have any security features, because they are not able to compute even the basic cryptography. Tags can still have static keys, PIN codes, which can be used, for example, to permanently disable the tag. More expensive tags can compute symmetric cryptography and challenge-response authentication. The most expensive tags can even utilise public key cryptography. However, these are not widely used.

RFID applications are often designed with the assumption that the designed operating range acts as a physical barrier for undesired access. However, specialised antennas can be used to radically increase range, and enable a communication range which is orders of magnitude greater. RFID does not have common information security standards or implementations; the manufacturers all have their own implementations. RFID may also be a threat to the privacy of the end user if, for example, a tag for production chain logistics is not disabled, and the unique tag is still functioning after the delivery of goods.

Many vendors have developed proprietary RFID tags and security solutions. When proprietary RFID systems are to be purchased, it is best to request a description of possible security solutions and mechanisms. Try to test the information security in practice. The RFID standards provide very little security or privacy features, if any. Some tags are able to lock their memory with the reader. Some tags can be permanently disabled with a kill command. This should be done to all tags required by logistics chain when the product is handed over to the end user. However, there are serious basic issues that are difficult to tackle using only information security protection. In most RFID applications, users or attackers could damage a tag, remove the tag or replace it, or even clone a tag. These facts must be taken into account when designing an RFID system.

Flash-OFDM

Flash-OFDM was developed by Qualcomm Flarion technologies. It is a mobile WAN cellular technology for IP-based networks. In Finland the old 450 MHz frequency band that was used by NMT is licensed to the Flash-OFDM operator Digita Oy. The network is geared mostly to the needs of people living in sparsely populated areas. It is claimed that authentication of users is based on the industry standard Radius and EAP, and data encryption is carried out with a 128-bit Rijndael Block Cipher (the same is used in AES).

Flash-OFDM uses proprietary security mechanisms. Specifications for cryptographic details, protocols and operations in layers 1 and 2 are only available under an NDA. For this reason, they have not been previously publicly analysed, and we are not able to do it now. Keeping a system secret does not add to its security. In fact it does quite the opposite, because other experts can't evaluate and analyse the security mechanisms and suggest further improvements.

We can't describe any specific solutions to possible threats as those threats remain unknown. If we had signed the NDA, we could have analysed and evaluated the security of Flash-OFDM, but then we wouldn't have been able to publish those results. However, in cases of uncertainty, it is always possible to apply *Defence in Depth* and use VPN solutions and application-level encryption (SSL/TLS).

Conclusions

Most wireless network technologies include security features, which we should use. In some cases this requires purchasing new products, even if the old ones are still working. Furthermore, it is always also advisable to apply the security features of the upper layers: corporate users should use VPN tunnels and web-based service providers should apply application-level encryption (SSL/TLS) when necessary. The end user should check that encryption is on, when sending private information through the Internet.

Abbreviations

3DES	Triple Data Encryption Standard
AES	Advanced Encryption System
AP	Access Point
BS	Base Station
BPI+	Baseline Privacy Interface Plus
CBC	Cipher Block Chaining
CCK	Complementary Code Keying
CCMP	Counter-Mode/CBC-Mac Protocol
CDMA	Code Division Multiple Access
DBPSK	Differential Binary Phase Shift Keying
DHCP	Dynamic Host Configuration Protocol
DOCSIS	Data-Over-Cable Service Interface Specification
DQPSK	Differential Quadrature Phase Shift Keying
DoS	Denial-of-Service. An attack on service availability
DSSS	Direct-sequence Spread Spectrum
DVB-T	Digital Video Broadcasting - Terrestrial
EDGE	Enhanced Data for GSM Evolution
EAP	Extensible Authentication Protocol
EAP-FAST	Extensible Authentication Protocol-Flexible Authentication Via Secure Tunneling
EPC	Electronic Product Code
ETSI	European Telecommunications Standards Institute
FICORA	Finnish Communications Regulatory Authority
FOMA	Freedom of Mobile Multimedia Access
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications

HF	High Frequency
HMAC	Hashed Message Authentication Code
HSOPA	High Speed OFDM Packet Access
IEEE	Institute of Electrical & Electronics Engineers
IP	Internet Protocol
IPSec	IP Security
IR	Infrared
ISM	Industrial, Scientific, and Medical
ISO	International Organization for Standardization
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
LF	Low Frequency
MAC	Message Authentication Code
MIC	Message Integrity Code
MIMO	Multiple-Input Multiple-Output
MINTC	Ministry of Transport and Communications
MMS	Multimedia Messaging Service
NDA	Non-Disclosure Agreement
NMT	Nordic Mobile Telephone
OFDM	Orthogonal Frequency Division Multiplexing
OMAC	One-Key CBC Mac
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKM-EAP	Privacy and Key Management-Extensible Authentication Protocol
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Server/Service
RC4	Rivest Cipher 4 (official) or Ron's Code 4
RFID	Radio Frequency Identification

SDR	Software Defined Radio
SHA	Secure Hash Algorithm
SMS	Short Message/Messaging System
SS	Subscriber Station
SSH	Secure Shell
SSID	Service Set Identifier/Identification
SSL	Secure Sockets Layer
STOA	Science and Technology Options Assessment Panel
TDD	Time Division Multiplexing
TEK	Traffic Encryption Key
TETRA	Terrestrial Trunked Radio
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TDMA	Time Demand Multiple Access
UHF	Ultra-High Frequency
UMTS	Universal Mobile Telecommunications System
USB	Universal Serial Bus
UWB	Ultra-Wideband
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WiFi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WPA/WPA2	WiFi Protected Access / WiFi Protected Access 2
WLAN	Wireless Local Area Network
WWW	World Wide Web

Terminology

- **Malware.** Malicious Software. This software category includes viruses, worms, and trojans (or trojan horses).

- **Security Downgrade Attack.** An attacker gains access to a network by forcing the use of insecure mechanisms that are supported for compatibility reasons.

WLAN terminology [800-97]:

- **Access Point (AP)**. An AP logically connects STAs with a distribution system, which is typically an organisation's wired network infrastructure. APs can also logically connect wireless STAs with each other without accessing a distribution system.

- **Ad-Hoc Mode**. This is a wireless network configuration that does not use APs; STAs communicate directly with each other.

- **Authentication Server (AS)**. Provides authentication services to STAs.

- **Infrastructure Mode**. This wireless network configuration requires APs and is the most commonly used mode.

- **Station (STA)**. A STA is a wireless endpoint device, such as a laptop, PDA, or mobile phone.

- **Wardriving** – the gathering of statistics about wireless networks by listening for their publicly available broadcast beacons. Wireless access points often announce their presence by broadcasting their service set identifier (SSID) and other data items. A stumbling utility running on a portable computer listens for these broadcasts and records the data. www.wardrivingonline.com/wardriving/faq.htm

Bluetooth terminology [BT_SEC]:

- **Pairing**. Two personal Bluetooth devices generate a secure connection by means of the initial pairing process. During this process one or both devices need a PIN code to be entered, which is used by internal algorithms to generate a secure key, which is then used to authenticate the devices whenever they connect in the future.

- **Car Whisperer**. A software tool developed by security researchers to connect to and send or receive audio to and from Bluetooth car-kits with a specific implementation. An individual using the tool could potentially remotely connect to and communicate with a car from an unauthorised remote device, sending audio to the speakers and receiving audio from the microphone in the remote device.

3G terminology [WIKI]:

- **IMSI**. An International Mobile Subscriber Identity is a unique number that is associated with all GSM and UMTS network mobile phone users. The number is stored in SIM (GSM) or USIM (3G). To preserve privacy, a temporal pseudonym is sent (when required) by the mobile phone to the network. IMSI analysis is the process of examining a subscriber's IMSI in order to identify which network the IMSI belongs to and whether subscribers from that network are allowed to use a given network

- **UMTS**. The Universal Mobile Telecommunications System is one of the third-generation (3G) mobile phone technologies. The currently most common form uses W-CDMA as the underlying air interface, as standardized by the 3GPP.

- **USIM**. A Universal Subscriber Identity Module is an application for UMTS mobile telephony running on a smart card which is inserted in a 3G mobile phone. It stores user subscriber information, authentication information and provides storage space for text messages. For authentication purposes, the USIM stores a long-term pre-shared secret key, K, which is shared with the network's Authentication Centre (AuC). The USIM also verifies a sequence number that must be within a range using a window mechanism to avoid replay attacks, and is in charge of generating the session keys CK and IK to be used in the confidentiality and integrity algorithms of the KASUMI block cipher in UMTS.

- **W-CDMA**. Wideband Code Division Multiple Access is a type of 3G cellular network. W-CDMA is the higher speed transmission protocol used in the Japanese FOMA system and in the UMTS system, an advanced 3G system, designed as a replacement for the ageing 2G GSM networks deployed worldwide.

RFID terminology [800-98]:

- **RFID tags** (or transponders) are small electronic devices that are attached to objects or embedded in them. Each tag has a unique identifier and may also have memory, environmental sensors, and security mechanisms.

- **RFID readers** (or interrogators) are devices that wirelessly communicate with tags to identify the item connected to each tag and possibly associate the tagged item with related data.

Table of Contents

Preface IX

Executive Summary X

Abbreviations XV

Terminology XVIII

Table of Contents XXI

1. Background to the research 1
   1.1 Goals 1
   1.2 Definitions of information security 1
   1.3 Wireless technologies 2
   1.4 Security threats not related to wireless technologies 3
   1.5 Generic threats 3
   1.6 Introduction to information security solutions and analysis 6
   1.7 Overview of solutions 7
   1.8 A brief look further into the future of information security challenges 11

2. WLAN 13
   2.1 WLAN Technology 13
   2.2 WLAN threats 14
   2.3 Security solutions and analysis for WLAN 16
      2.3.1 Solutions 16
      2.3.2 Analysis 20

3. WiMAX 22
   3.1 WiMAX Technology 22
   3.2 WiMAX threats 23
   3.3 Security solutions and analysis for WiMAX 25

4. Bluetooth 29
   4.1 Bluetooth Technology 29
   4.2 Bluetooth threats 31
   4.3 Security solutions and analysis for Bluetooth 33

5. 3G and 4G 37
   5.1 3G Technology 37
   5.2 3G and 4G threats 37
   5.3 Security solutions and analysis for 3G 38

6. RFID 41
6.1 RFID Technology 41
6.2 RFID threats.. 43
6.3 Security solutions and analysis for RFID 44

7. Flash-OFDM... 48
7.1 Flash-OFDM Technology 48
7.2 Flash-OFDM Threats 48
7.3 Security solutions and analysis for Flash-OFDM 49

8. Conclusions.. 51

References 53

Appendices:

Appendix A. WLAN Standards
Appendix B. WLAN communication step-by-step
Appendix C. WiMAX standards
Appendix D. RFID standards

1. Background to the research

Today, there is a strong trend towards people becoming more and more dependent on wireless information networks. The Finnish Ministry of Transport and Communications (MINTC) has considered this development worthy of research through investigating the major information security threats concerning current and emerging wireless network technologies, and solutions managing the possible vulnerabilities.

LUOTI is the Development Programme for Trust and Information Security in Electronic Services for 2005 to 2006 managed by the MINTC. This programme is one of the actions in the National Information Security Strategy. LUOTI aims to promote information security in new multi-channel services. One of the main objectives is to increase end users' confidence in new electronic services. The programme is taking place in co-operation with media companies, other content providers, service and network operators, the information security sector, research institutes, universities, authorities and legislators.

1.1 Goals

The main goal of this study is to increase awareness of current and future information security threats relating to wireless network technologies and their meaning to the end user as well as product development in electronic services. This paper lists the main threats to the key wireless technologies and solutions to control related vulnerabilities in these technologies. This study aims to gather information security know-how and expertise to benefit its target audience and in the long run to influence the development of the operating environment.

This study does not go into deep analysis of security threats to emerging technologies or novel compositions of current technologies. It is very challenging to predict security risks for forthcoming technologies because of the lack of deployment information.

1.2 Definitions of information security

Three main security objectives in information systems are Confidentiality, Integrity, and Availability (the CIA triad). Their counterparts are Disclosure, Alteration, and Destruction.

1. Confidentiality
   - When information is accessed without authorisation, the result is known as loss of confidentiality or disclosure. Authentication and access control mechanisms are used to achieve confidentiality.

2. Integrity

- Information may be erased or manipulated without notice (alteration). Data integrity means that the data is known to be unmodified.

3. Availability

- Availability is usually the most important attribute for service providers. Availability of the service provided is important for the end users. Destruction is an attack against the availability of data, and an attack against the availability of a service is known as Denial-Of-Service.

1.3 Wireless technologies

Some of these technologies have been chosen for more thorough consideration based on their popularity and widespread use. WLAN, Bluetooth and 3G have tens (or even hundreds) of millions of users. The use of RFID is foreseen to expand rapidly (billions of tags) in the next few years. GSM is beginning to become obsolete for service development.

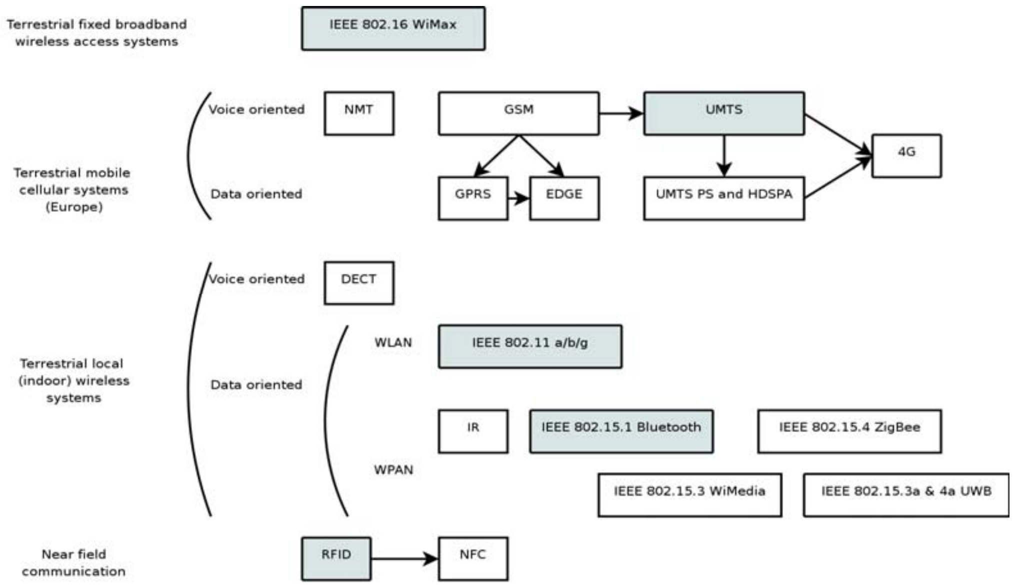


Figure 1. Some current and emerging wireless technologies and their relations. Technologies covered in this document are coloured

The following technologies may or may not be relevant in the future but they were too immature to be analysed yet.

Wibree is a recently published (October 2006) industry standard for an ultra low power consumption alternative to other wireless protocols for connecting portable devices. Wibree is designed to work side-by-side with and complement Bluetooth. Due to its recent nature, there is little security information available, but the security issues can reasonably be expected to be similar to those of Bluetooth. Implementation vulnerabilities and risks related to data leakage/espionage, hostile device takeover and damaging data and/or devices are to be expected if the technology becomes widely available which, according to some sources, is not yet guaranteed.

Ultra-Wideband (UWB) systems are an upcoming technology that is designed for short-range, low-power, high-data rate communication. Commercial implementations are not yet available, but wireless UWB implementations are projected to be made available by early 2007. Other future implementations include replacing cabling from home entertainment devices. Because standardisation attempts have failed, of the competing UWB technologies the one represented by the WiMedia alliance seems to be the one emerging as the de facto standard - WiMedia UWB has been selected both by the Bluetooth SIG and the UWB Implementers Forum as the foundation radio for their high-speed wireless specifications.

1.4 Security threats not related to wireless technologies

The image presented here necessarily becomes somewhat one-sided as we only focus on wireless-specific threats. When thinking about threats faced by service providers and users, it is essential to always keep in mind that wireless-specific threats and security problems are a small subset of all threats and threat analysis should always take into account the whole picture using a well thought-out threat model ("What are you defending against?"). For example, when using a wireless technology for Internet access, wireless-specific threats are often overshadowed by the problems related to the Internet-based applications that are used.

Another important thing to keep in mind is that vulnerabilities are often the result of unforeseen interactions between systems. In other words, some of the new security problems brought on by adoption of new wireless technologies are primarily a question of previously unseen (and sometimes unforeseen) usage models of older technology. As the number of interconnected components increases, the number of possible inter-component interactions grows rapidly. [GEER]

1.5 Generic threats

There are technology-specific vulnerabilities relating to design choices, implementation quality issues and so forth, but most of the real threats people face, are not specific to any one wireless technology. In fact, many of the threats below are not specific to wireless technologies at all, but are mentioned since they are also present when using wireless technologies.

The service provider and user share concern over confidentiality, integrity and the availability of communications itself, and to a large extent the concern of the end user is also the concern of the service provider as service providers are likely to be image-conscious and care for the perceptions of the end users. Malware can bring down networks by exhausting network and service resources, and they can infect end user’s computers or mobile phones.

Most of the confidentiality and integrity-related threats would be solved by the use of end-to-end security. This means the communication is cryptographically secured from terminal to terminal (e.g. phone to phone, PC to PC). E2e encryption has been left out in voice and messaging services in 3G and GSM (to facilitate wiretapping by security services and the police). In the Internet e2e security is frequently but not exclusively used, for example on the Web (as the "https" protocol) and in SSH terminal connections. IPSec and/or VPNs are used to secure all traffic between hosts end-to-end or to securely connect to a "home" network which can be viewed as "halfway-to-the-end" protection.

Service providers are often businesses and their organisational stake in the security of communication is often related to perceptions, costs, and continuity of operations. The concerns of individual end users are more weighted towards the confidentiality and integrity of their personal data and communications. The concerns of end users and service providers of course overlap and service providers servicing end users ought to make the concerns of end users their own.

One category of generic threats is compromise of user terminals (mobile phone, laptop computer). The compromise can be complete or partial, but usually a partial compromise can be leveraged to achieve a complete compromise. Examples of compromises include a virus infection or a targeted break-in by a specific adversary.

Fraud and theft of services is a threat faced by service providers. Most business deal with some amount of fraud and theft, and can tolerate them as long as the losses incurred, do not become too big. The threat model used for designing mobile phone systems such as GSM and 3G is heavily oriented toward preventing customer fraud.

Malware is ubiquitous today and most users and service providers encounter them in some form. The threat of malware is relevant to wireless technologies when it spreads or operates in ways that interact with unique traits of wireless technologies. For example, malware spreading over MMS messages may overload the service provider network, and some mobile phone viruses exploit the ad-hoc nature of Bluetooth networks. The most commonly encountered malware is relative to what damage it could easily do (destroy or corrupt data or hardware, intentionally overload networks), typically attaching the host computer to a botnet for spamming or fraud, or lesser nuisances. A more dangerous category is targeted malware, software designed to penetrate a specific target and employed as a method in fields such as state or industrial espionage or information warfare. Targeted malware is often not recognised by anti-virus software (since anti-virus software is based on recognising previously observed code).

Another threat category is image problems caused by widely publicised (real or not) security problems in services or technologies. Users can be discouraged from employing a technology or service if it is perceived to be prone to security problems. In many cases the threat of public image is the strongest motivator for service and technology providers to react to security problems found in their products. Once the damage is done, this sort of image problem can be hard to shake. WLAN and Bluetooth are examples of wireless technologies that have had problems in this area, but the same mechanism applies to services - for example, some web browsers and operating systems have bad enough reputations to make an impact in their market share. To counter this phenomena, there's often a backslash of highly publicised security enhancements of varying real impact (independent of whether the original concern was warranted or not).

End users and service providers are not always on the same side. Sometimes service providers want to disrupt communications by end users that are deemed unprofitable or undesired, thus each side is threatened by actions of the other. [DIGITODAY1]

Sometimes service providers cooperate with intelligence agencies or law enforcement to eavesdrop on or otherwise compromise the end users' communications. The "Lawful Access" feature is implemented in many wireless systems that are connected to the public phone network. Users of wireless devices be concerned because even if some technology is promoted as secure (i.e. it uses an n-bit brand X encryption method that can not be broken) it may have a backdoor installed for lawful access. Even though the lawful access is mainly available to authorities like intelligence services and the police, it is still a threat to the user's privacy. And even if the user is not worried about government eavesdropping, there is no guarantee that the lawful access feature is not being misused. There have been some high profile scandals concerning this. [GREECE]

Intentional radio interference, or jamming, is a threat that all the wireless technologies described below are vulnerable to. It means that an adversary is transmitting radio signals designed to disrupt the operation of targeted wireless communication. It is a technically easy attack to mount against practically all civilian wireless technology as it is sufficient to drown out the targeted signal with noise. Radio interference is normally not worried about too much in peacetime, since it only affects the availability of communications and it has not been a big problem historically. When sufficiently strong transmission power is used, it is possible to damage and permanently disable the receiving equipment. Examples of equipment for doing this on a large scale are EMP bombs and are commonly used in modern warfare.

Many radio technologies are not currently accessible for the average person by anything other than equipment specifically designed to strictly conform to the protocol specifications. The exceptions are WLAN and to some extent Bluetooth, both of which have been subject of extensive probing and mischief by interested hackers. This division is likely to start eroding in the near future with the advent of software-defined radios [GNURADIO] and SDR technology embedded in multi-access consumer devices. It is probable that the thus-far closed technologies will have a rude awakening when publicly available SDR software packages for things like TETRA, DVB-T, and GSM, etc. start to appear on the Internet.

1.6 Introduction to information security solutions and analysis

Wireless technologies offer easy connectivity and mobility [WIRE], but the drawback is that there can be other signals (radio interference) that might block the radio signals from passing through, or there can be pure information security attacks or at least vulnerabilities concerning wireless signalling, user data and system integrity.

For radio interference, the simplest solution is to put the wireless access point in a location where the signal will have as little interference as possible. Actually, this principle is also an important partial solution for information security, which aims to adjust the signal field coverage so that all unnecessary coverage (e.g. outdoors) is avoided.

However, in a wireless network there often is a possibility for an adversary to get inside the radio coverage and try to gain access to a network using insecure management signals. This possibility is due to the fact that wireless networks are by nature more complex to administrate and control access to than wire-line networks.

However, it is not enough in information security assurance to mention only the usage of a certain information security technology for protecting the use of wireless connections. Actually, it requires much more effort from all relevant parties (including the user) to enhance the security level of different wireless usages. Below are listed the threat or solution types that fall within the scope of this report, and what is left out.

Within the scope of this study. The solutions that tackle (in more or less detail):

- The most important network and information security threats (technical)
- The most obvious radio coverage related issues
- Lack of secure network administration
- Loose user behaviour
- The most obvious privacy issues

Outside the scope of this study:

- Regulated operation: there exist regulations on the information security of telecommunications operators in Finland, see for example [FIC47B].
- The details of secure network architectures and the deployment of each technology.
- Extensive listing and detailing of all the threats and solutions for technologies which are well-known to be vulnerable, i.e. if technologies that have well-documented security drawbacks and therefore their use should be avoided (such as WEP in WLAN).
- Risk analysis methods (Several risk analysis techniques are also applicable to wireless networks)
- Issues related to safety

1.7 Overview of solutions

The main threats to wireless networks requiring solutions are related to the following:

Table 1. Wireless network threat categories requiring solutions. Adapted from [800-97]

Threat categories to protect	Explanation
Eavesdropping	Monitoring transferred data. For example, user data or credentials could be discovered by decrypting weakly encrypted data.
Man-in-the-middle attack	In signalling, a hostile third party plays the role of a legitimate party obtaining user data or credentials.
Masquerading	A legitimate user's permission or username is used without consent to get access rights to protected resources or data.
Message modification/replay	A legitimate user's messages are modified or copied and replayed.
Traffic analysis (often more expensive to protect)	Transmitted communication is monitored and analysed giving possible hints about the nature of the communication. Examples include analysis of traffic instants of a key competitor.
Denial of Service (often difficult to fully protect)	The use of a network becomes difficult or impossible. In jamming a device transmits lots of energy on the used frequencies making the wireless network unusable. In flooding an attacker sends large numbers of messages to the network which cannot process them.

Threat categories to protect	Explanation
Miscellaneous attacks	For example, an attacker steals a device, deletes (e.g. via the reset button) or modifies the settings of wireless devices or network elements.

There exist a multitude of different solutions to these threat categories. The technical solutions for protecting wireless networks from information security threats include the wise utilisation of radio technology features, the selected use of strong, suitable cryptographic algorithms and protocols for confidentiality and message integrity and origin authentication with replay protection. Essential precautions also include the ability to mutually authenticate the communicating peers in the early stages by applying secure authentication and key establishment protocols, which are proven to be applicable for wireless use. Then, there are a number of different administration-related issues, such as purchasing criteria of devices, adequate management of settings and configurations of devices, the assurance of usage of secure R&D and deployment practises, the usage of malware and intrusion protection products, and other good network administration practises (however, many of these are not specific only to wireless networks therefore these are not discussed extensively in this document). Of course, network architecture design is different in a wireless network than in wired solutions. Secure network deployment, however, is far from trivial in each of the wireless technologies (See for example [802-11i] and [800-97] for WLAN), so we do not describe the detailed architectural or deployment solutions in this document.

For a brief summary of the main generic security countermeasures to be applied in various wireless networks, see our proposed list in the table below:

Table 2. The main generic countermeasures that should be used to improve the security of the various wireless networks. The main contributing actors are indicated. Note: the table includes many simplifications and only countermeasures of high importance are shown.

Security countermeasure	Service developer/-provider/-operator	Device	User
Radio technology countermeasures: Management of signal state (On/Off), signal power (adjustable), bandwidth (spreading), and field coverage (cover planned area/volume).	x	x	(x)
Encryption: Cryptographically encrypt user signalling and data.	x	x	

Security countermeasure	Service developer/-provider/-operator	Device	User
Detection of message modification: Cryptographic authentication of signalling and data messages (integrity checking).	x	x	
Authenticated actors/devices: Mutual, strong authentication of communicating devices. Also consider two-factor or multiple-factor authentication (e.g. smart card with password).	x	x	x
Secure configuration: Enable the security settings: Take strong security protocols into use, disable insecure wireless modes. Holistic access control against malicious settings. In large networks, use secure methods in remote configuration and upgrading of network elements (incl. e.g. SNMP v3, IPsec, strong admin passwords).	x	x	x
Secure key management: Cryptographic key establishment, adequate key management practises.	x	x	
Security and quality assurance of products: Integrate certified products and test the implementations.	x	x	
Secure development: Use of Security management in product and service development.	x	x	
Malware protection: Use the best available antivirus software. Increase security awareness.	x	x	x
Follow up: Log and event monitoring (automatic if possible).	x	(x)	(x)
Deploy secure network architecture: Network segregation, firewalls, defence-in-depth architecture (consider IDS as well).	x		
Secure network administration: Network planning, risk assessment, requirement definition (incl. legal), wireless network security policy, password/PIN policy, PKI certificate policy, hardening and updating of software, education, inventory of devices and network elements, system security assessment, disposal precautions.	x	x	(x)

NOTE: Privacy solutions are not tackled extensively in this document. Note, however, the statements of the Finnish Communications Regulatory Authority. (See example below.)

Regulatory example considering the balance between the privacy and security protection [FICORA]

> Identification data may only be processed to the extent necessary for the purpose of the provision and use of a network service, communications service or value-added service and for the purpose of ensuring information security in these services. In order to combat violations of information security and to remove information security disruptions, a telecommunications operator has the right to undertake necessary measures in order to prevent the transmitting and receiving of e-mail messages, text messages and other similar messages and to remove from the messages malicious software. In other words, identification data may in principle be processed for the purpose of discovering who the sender of malicious software is as well as stopping spam mail if that endangers the usability and information security of the communications service…

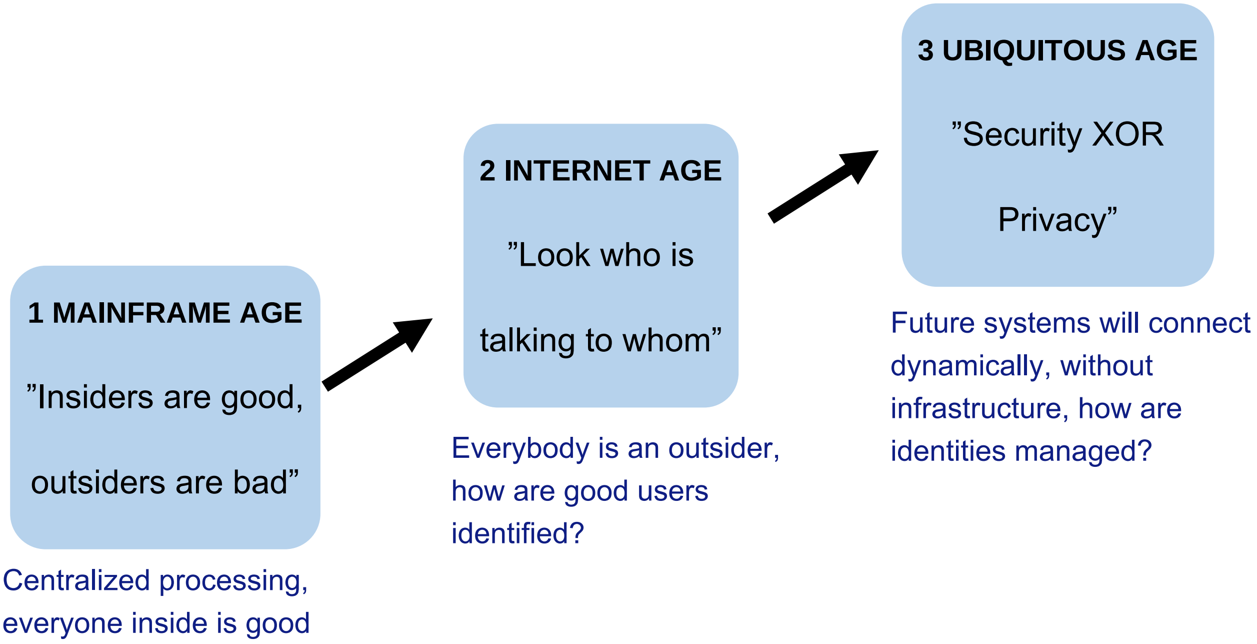
Today, any consumer should be aware and prepared for the wireless information risks when using wireless devices. The precautions that a consumer should take into account include:

- Ed
- Educate yourself, increase your security awareness
- Consider security features before purchasing
    - Decide what is secure enough for your purpose, invest for future use as well
    - Select certified products
- Install and carefully configure your equipment
    - Device positioning and usage must be under proper control. Disable the wireless component when not in use.
    - It is very important to configure settings, especially security settings, properly. For example, ensure that the security features are taken into use: set strong security protocols, authentication and passwords. Disable unnecessary broadcasting of your network or device IDs.
    - Prevent attackers accessing your device configuration. Change the default admin passwords.
- Look after your equipment, avoid robbery and do not lend a device to a stranger.
- Be careful when installing programs on a wireless device, see [FICUSER]:
    - Do not permit suspect software installation whenever offered; use only reliable sources for downloading software. Remember that a friend could also infect your device.
    - Use anti-virus software if possible. Be proactive: try malware cleaning tools beforehand.

- Be aware and prepared against social engineering attacks.
- Before disposal, delete all sensitive data and credentials etc. from the device.

1.8 A brief look further into the future of information security challenges

We can investigate the evolution of information security challenges in the future by looking at computing paradigms (see Figure 2). It is obvious that the future – and even today – of wireless networking from a security point of view means mixture of communication and computation. The role of different kinds of wireless networks is crucial in current and future computing paradigms.


1 MAINFRAME AGE

”Insiders are good, outsiders are bad”

Centralized processing, everyone inside is good

2 INTERNET AGE

”Look who is talking to whom”

Everybody is an outsider, how are good users identified?

3 UBIQUITOUS AGE

”Security XOR Privacy”

Future systems will connect dynamically, without infrastructure, how are identities managed?

Figure 2. Computing paradigms

The first computing paradigm, the Mainframe Age, included a lot of centralized computation and everything inside the system was assumed to be secure, whereas everything outside the system was assumed to be insecure. The security of wireless networks was not such a big topic in the Mainframe Age.

Currently we are living in the Internet Age, the second computing paradigm. Everybody is assumed to be an outsider in this paradigm. The main question of security is: “how do we separate the good users from the outsiders?” The world around us becomes more and more digital and networked with different kinds of users, applications, network connections and devices.

The next computing paradigm will be the Ubiquitous Age. Future systems will connect dynamically and are often without infrastructure. Most of the future security challenges will be centred on identity management and authentication in very dynamic systems. If we take a closer look at the ubiquitous computing paradigm, we can differentiate at least three emerging phases (see Figure 3): mobile computing (~2000–2010), pervasive computing (~2010–2020) and autonomic computing (after 2020).

In mobile computing, network providers typically control security, systems are becoming open, but they have only a rudimentary adaptability.

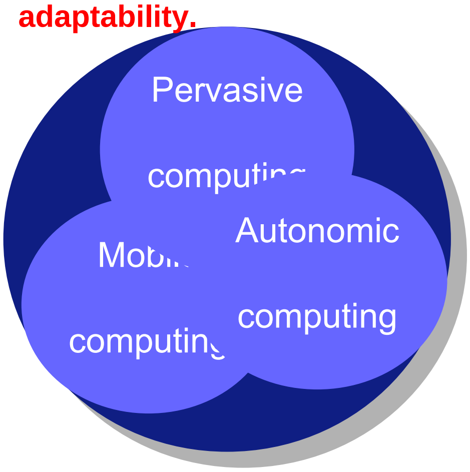
In pervasive computing, there are strong needs for mobility and context awareness. Privacy challenges especially will increase, and systems will have an increased degree of adaptability.

In autonomic computing, there are big challenges for security and privacy because of the use of machine-to-machine communication and computation. This kind of situation is new for security management, because the security management has previously been controlled by humans mainly.

2010 Pervasive Computing:
Mobility and context awareness
Privacy challenges especially increase, **systems open** with **increased degree of adaptability.**

CHALLENGE FOR SECURITY RESEARCH AND DEVELOPMENT:

Secure and increasingly insecure environment



2000 Mobile Computing:
Location-free services,
Security: typically network providers control security and therefore devices, **systems open** but only **rudimentary adaptability**

Big challenges for security and privacy (M2M communication)

Figure 3. The phases of ubiquitous computing between 2000–2020

2. WLAN

2.1 WLAN Technology

A WLAN [WIKIWLAN] is a wireless local area network, the linking of computers without wires using radio communication. The term WLAN refers most often to IEEE's 802.11 set of standards. ETSI's HIPERLAN is another WLAN standard, but it has not gained popularity.

A WLAN connects computers and other components to the network via an Access Point (AP). IEEE 802.11 is a set of WLAN standards providing transmission speeds from 1 Mbps up to 54 Mbps in either the 2.4 GHz or 5 GHz frequency bands. The most important current standards/working groups of 802.11 are described in Appendix A Table 11.

In January 2004 IEEE formed a new 802.11 Task Group (TGn) to develop a new amendment, 802.11n. The real data throughput of 802.11n is estimated to reach a theoretical 540 Mbit/s. The standardization process is expected to be completed by the second half of 2006.

802.11n builds upon previous 802.11 standards by adding MIMO (multiple-input multiple-output). MIMO uses multiple transmitter and receiver antennas to allow for increased data throughput through spatial multiplexing and increased range by exploiting the spatial diversity. The 802.11n standard is due for final approval in July 2007.

Standards 802.11c, d, f, h and j are WLAN service enhancements. [802.11d, 802.11f, 802.11h, 802.11j]

WLAN Security (802.11i, e and w) [802.11i, 802.11e]

Due to security weaknesses reported in 2001 in the 802.11 WEP security mechanism, and soon afterwards in the RC4 stream cipher, the IEEE set up a dedicated task group to create a replacement security solution, 802.11i. Previously this work was handled as part of a broader 802.11e effort to enhance the MAC layer. The Wi-Fi Alliance announced an interim specification called Wi-Fi Protected Access (WPA) based on a subset of the then current IEEE 802.11i draft. RC4 was still used as the cipher in WPA. IEEE 802.11i (also known as WPA2) was ratified in June 2004, and it uses AES, instead of RC4, which was used in WEP and WPA.

In January 2005, IEEE set up another task group (802.11w) to protect the MAC layer, namely management and broadcast frames, which previously were sent in insecure way. It is expected that 802.11w would extend 802.11i to apply to 802.11 management frames as well as data frames. The 802.11w standard is in its early proposal stages. The target for ratification is March 2008.

2.2 WLAN threats

A lot of attention has been poured onto security threats surrounding WLAN, and public discourse about WLAN security has been voluminous. Internet applications commonly use end-to-end security in sensitive tasks, and when they don't it is considered a security flaw in the Internet application as opposed to the network.

With the caveat above, security threats to WLAN networks do exist when carrying sensitive traffic that is not otherwise secured. A large number of software tools for orchestrating various attacks on WLAN networks are widely available, including tools for eavesdropping and man-in-the-middle attacks. Various WLAN security standards and schemes have resulted in interoperability problems, so the use of WLAN security features is paradoxically hampered by their great number. The large number of specifications results in a lot of implementation effort, and fertile ground for a large number of implementation-level bugs and vulnerabilities.

WLAN has many different standardised security features and design flaws in some of these have been pointed out, such as Wired Equivalent Privacy (WEP). [KENTTÄLÄ] WEP key management methods were weak and did not scale to large networks. The key length was too small and some vendors introduced extensions to try to improve the security. Finally, an attack that could successfully retrieve the secret keys by traffic monitoring was discovered. These vulnerabilities occurred because WEP was developed without proper review by security experts. More in [EDNEY].

WLAN security surveys can be found for example from Symantec [WLAN_SYM] and Uninett [UNINETT].

WLAN is very high-profile technology and has received huge amounts of media attention, including security incidents. For example, Digitoday and Tietokone reported on unauthorised use of one’s neighbour's WLAN. The case is representative of media attention to WLAN security problems: the culprit used a publicly accessible WLAN in a computer break-in. He could have used another form of semi-anonymous network access such as a public computer in a library or a pre-paid SIM card, but WLAN made it newsworthy. [TIETOKONE, DIGITODAY2]

In public WLANs, the issue most argued about WLAN security is encryption between terminals and access points. There are many different kinds of solutions to handle it, but is it worthwhile in public WLANs, taking into account the traffic on the Internet after the access points is not encrypted. One Finnish service provider providing public network access network states "Is it right to give users a misconceived feeling of security? We think that increasing awareness is better than a thousand security solutions which might jeopardise availability of information." [PANOULU] Also security expert Bruce Schneier argued that as long as people's devices were secure, having a secured home WLAN network was unnecessary. [NEWS.COM]

Threats concerning WLAN technology are due to the implicit features of the medium. The places where information travels have no clear boundaries. It is possible to intercept and thus to eavesdrop on data sent over WLANs even at high distance. Eavesdropping, hijacking and spoofing are easy attacks to launch in a WLAN in order to achieve confidentiality, traffic analysis and denial-of-service attacks.

Without understanding the security implications of connecting an open-access WLAN to their home network, users at home might suffer from someone breaking into their computer via that home WLAN. One threat to WLAN users at home is also if someone breaks into the user's computer by exploiting vulnerabilities in the WLAN driver, security software, or WLAN security protocol. Compromise of the WLAN terminal (laptop, phone, etc.) gives the attacker complete control of all the users data, i.e. the attacker can hijack electronic banking transactions, steal secrets, send messages in the user’s name, steal access credentials to other services from the terminal, etc.

Attackers are also able to setup a rogue access point which captures traffic from unsuspecting users attempting to login to their services. This exposes private information to the hackers. On the other hand the same kinds of man-in-the-middle attacks are also possible also in wired networks, but easier to implement in wireless networks.

In the future digital convergence will increase the amount of WLAN threats. Merging of WLAN, 3G and GSM has already happened and it will challenge manufacturers.

Table 3. WLAN threats

Trait	Implication
publicity, widely deployed	lots of tools for implementing attacks and developing exploits
large number of redundant but incompatible security standards	implementation-level vulnerabilities and reduced usability of security features
used mainly as access network	Easy to gain access to infrastructure network
design flaws in some security specifications e.g. WEP	possible to break the encryption
shared-media model (Ethernet compatible)	other stations in same WLAN network can eavesdrop on, interfere with or hijack communications
vulnerabilities in WLAN drivers, security software or WLAN security protocols	terminal security can be compromised by users on same network
over-the air traffic often not cryptographically secured	eavesdropping and man-in-the-middle attacks on traffic that is not secured on the network layer

Trait	Implication
digital convergence, merging of WLAN, 3G, and GSM	more threats

Relevance to WLAN-level security threats should be evaluated in the context of the application, when used for Internet access. The Internet is untrustworthy and end-to-end security is needed in any case to protect traffic that travels the rest of the way over the insecure Internet.

2.3 Security solutions and analysis for WLAN

2.3.1 Solutions

The dominant commercial WLAN standard is IEEE 802.11, so we focus on its security. The main threats categories for WLAN are the same as those of wireless networks in general. Often the biggest threats are directed towards the wireless user, his device, or the access point. The threats are focused on the confidentiality and authenticity of transferred frames, and device access control. These threats are mainly due to the nature of the unlicensed radio frequency bands used in WLANs, the operation and security of which are not regulated.

The most serious threats need to be tackled by applying systematic countermeasures by all relevant actors. The most important countermeasures for most WLAN threats are collected in a table below. **A major technology used for protection is the IEEE 802.11i amendment** [802-11i], which is designed to overcome the vulnerabilities of WEP and which can protect all IEEE 802.11 radio standards (802.11a, 802.11b, 802.11g).

The best current link-level security technologies for WLAN are the following: The most secure choice for WLAN confidentiality and integrity protection is CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) with AES. In many scenarios, defence-in-depth approach is needed; for example utilising VPN or TLS on top of WLAN security layer. See [800-48] to improve the security of existing (legacy hardware) WLAN deployments, which cannot execute CCMP. For the authentication phase, the best choice is to utilise Extensible Authentication Protocol (EAP) for establishing a secure connection. However, some of the EAP authentication methods are not secure or suitable for wireless use. As of today, most researchers argue that the most secure EAP methods are based on the Transport Layer Security (TLS) protocol. In large deployments, also the use of IEEE 802.1X and an authentication server with PKI is often needed for scalable, secure administration. **In some deployments, the use of WLAN products with Wi-Fi Protected Access 2 (WPA2) certification is recommended** for security reasons. NOTE: Even a single access point that uses weaker security than the others can compromise the security assurance of the whole administrated WLAN network. In other words, interim security networks are vulnerable to several attacks, and should be avoided.

Below is a table that summarises WLAN security countermeasures for the most essential main threat categories. In the table “Impact” and “Mature” indicate whether the described countermeasures have High/Medium/Low Impact and whether countermeasures are considered mature (Yes/No).

Table 4. Overview of WLAN security countermeasures

Threat/Reason	**Countermeasures by actor**		
Eavesdropping: Decrypting messages and user data	Detection: Difficult if not impossible. Check for possible weak encryption settings.	Impact (H/M/L): H	Mature (Y/N): Y
	User = Allow only CCMP encryption. Do not use WEP encryption (E.g. initialization vector vulnerabilities, RC4 vulnerabilities). Disable WLAN when not in use. Manufacturer = Implement CCMP encryption for new product versions. CCMP key space is 2^{128}. Provide upgrades for previous releases. Service = Deploy only CCMP encryption and allow only CCMP based security associations. TKIP can be deployed through software upgrades (without hardware replacement of WEP devices). However, TKIP uses RC4 which has known security weaknesses and it only encrypts the payload. Disable wireless radio during maintenance etc. when not in use.		
Man-in-the-middle attack: Rogue access point, station or authentication server.	Detection: E.g. NetStumbler, AirMagnet or a wireless sniffer to detect rogue access point. Also possible increased errors in communications, changed authentication user interface, duplicate or similar SSIDs give hints about intrusions.	Impact (H/M/L): H	Mature (Y/N): N
	User = Avoid suspicious access networks and locations. Take IEEE 802.1X with mutual authentication into your device security policy. Enforce CCMP (or TKIP). Manufacturer = Implement secure IEEE 802.1X authentication methods. Service = Secure the connections from all access point to the authentication server with IPSec VPN, for example. Set authentication portal’s time-out very short. Enforce CCMP (or TKIP).		

Threat/Reason	**Countermeasures by actor**		
Masquerading: Authentication only with SSID & MAC addr.	Detection: Difficult because SSID and MAC address may be sniffed and used. Check whether old WLAN authentication version in use.	Impact (H/M/L): H	Mature (Y/N): Y
	User = Take IEEE 802.1X with mutual authentication into your device security policy. Consider 2-factor authentication. Manufacturer = Implement secure IEEE 802.1X authentication methods. Service = Deploy IEEE802.1X supporting access point (e.g. EAP-TLS) and authentication server (e.g. RADIUS). Assign strong authentication policy. Secure also AP-AS connection.		
Message modification: No integrity check or integrity check with only 32-bit CRC WEP encryption. Session hijacking by stealing active MAC address.	Detection: Difficult if no security services or only WEP CRC in use. Aims to detect message modification attack by TKIP Michael MIC (Message Integrity	Impact (H/M/L): H	Mature (Y/N): Y
	User = Require the use of MAC integrity check. Require CCMP MAC if possible (regarded secure). TKIP Michael MIC: This selection might help with countermeasures in legacy networks. Manufacturer = Implement MAC integrity check into protocol: CCMP for new implementations, TKIP Michael MIC with countermeasures for software upgrades. TKIP Michael MIC: This selection might help with countermeasures in legacy networks, aiming to protect the frame header addresses (However, in one of 2^{28} messages an attacker might spoof the source or redirect the frame to an unauthorized destination. Countermeasures: Require logging, disable reception in two failures for 60 s, change the keys, and block the controlled ports.) Service = Allow only WPA(2) security associations. Deploy a secure MAC integrity checking: CCMP as default, TKIP Michael MIC with countermeasures if hardware upgrade not possible.		
Message replay: No message counter or	Detection: Detected in protocols which support frame counter, timestamps, etc. and integrity protection.	Impact (H/M/L): M	Mature (Y/N): Y

Threat/Reason	Countermeasures by actor		
timestamp used	User = Select security settings and protocols with support for replay protection. Manufacturer = Implement or integrate protocols that support replay protection. Such protocols are CCMP (uses 48-bit packet number to construct a nonce) and TKIP. Service = Deploy security policy and protocols that support replay protection. The best protocol is CCMP.		
Traffic analysis: Determination of operating system from certain frames.	Detection: Physical surveillance	Impact (H/M/L): M	Mature (Y/N): N
	User = Avoid suspicious access networks and locations. Manufacturer = Develop technologies that reduce the potential for traffic analysis. However, traffic analysis safeguards are often regarded expensive because they consume radio resources. Service = Careful wireless network planning: locations of access points, video surveillance, etc. Use only secured operating systems and applications in the network.		
DoS: Jamming, flooding	Detection: Network slows down, probing for disturbing sources.	Impact (H/M/L): H	Mature (Y/N): N
	User = Avoid suspicious access networks and locations. Manufacturer = Develop devices that discover and possibly locate malicious/erroneous radio transmitters. Implement DoS protection features. Service = Careful wireless network planning: locations of access points and range. Monitor (radio surveillance), etc. Agree on the usage of channels between providers. Minimize the usage of faulty devices (tested device set) and DoS possibilities.		

To further understand the functioning of a WLAN system, please refer to Appendix B.

The needs of application-level multicast and broadcast are not discussed much in this document. However, these are generally regarded as more challenging than point-to-point delivery from a security viewpoint and their use may open several security vulnerabilities. The technical solutions to protect against these vulnerabilities at a large scale are often very complex, and their maturity can be modest or low. The key management solutions in the applications of wireless multicast especially have limitations, for example, a suspect incident in a single station may affect all stations of the multicast group.

The home WLAN administrator usually needs to consider the simplest issues first, because he may not have time or competence for fine-tuning the security solutions. See the brief advice below:

Home WLAN administration

The security recommendations below summarise the steps one should take in home WLAN administration [COMP] and [PRACT]:

1) Change the default admin passwords and usernames of the access point. Disable remote administration capability.

2) Turn on the security protocols, such as WPA2 (or WPA if is WPA2 not available). Select the most secure protocol that works with your wireless network. Even WEP is better than nothing. Set up secure authentication.

3) Change the Default SSID to something new.

4) Keep the access point firmware up to date.

2.3.2 Analysis

There exists a pandemonium of various WLAN security solutions, standards and products.

In a scenario where WLAN is used as an access network to the Internet, the user is by definition connecting to an untrusted network (the Internet) and securing the local WLAN still leaves the communication travelling most of the way through untrusted networks.

In a scenario where WLAN is used as an access network to an organisational private network and users are using a homogeneous software base that is known to interoperate with a fixed set of WLAN security features, link layer security is often mandated. On the other hand, using a VPN through an insecure WLAN network might be a simpler and more broadly usable solution in that scenario.

Conformance to organisational security policy by the user and the configuration and upgrading of the station are very important issues for security. From the network infrastructure viewpoint, only a single access point that uses a weaker security configuration than the others can compromise the security of the whole administrated WLAN network. The existence of old wireless devices in the organisation creates a big interoperability problem when old stations have connectivity needs for example to critical business systems with the latest security technologies and configurations. In addition to security, user’s privacy considerations (e.g. MAC address tracking) may be of importance.

The root cryptographic key might have security compromises due to the use of an insecure authentication method. Before deployment, authentication methods should be carefully evaluated from a security viewpoint, and the selection should be based on the best available analysis. In enterprise deployments, the authentication server is also a critical security component: it must securely protect all credentials and keys. Masquerading authentication servers or access points should be detected during WLAN network deployment and use.

3. WiMAX

3.1 WiMAX Technology

WiMAX [WIKIWIMAX], or the IEEE 802.16 wireless network, is defined as Worldwide Interoperability for Microwave Access by the WiMAX Forum [WIMAXFORUM], formed in June 2001. WiMAX is officially known as WirelessMAN, and it is described by the WiMAX Forum as ”a standards-based technology enabling the delivery of last mile wireless broadband access as an alternative to cable and DSL.”

WiMAX provides fixed, portable or mobile non-line-of sight service from a base station to a subscriber station (customer premise equipment, CPE). WiMAX delivers either high-bandwidth (raw data rates up to 70Mbit/s), or long-reach (a maximum range of over 100 kilometres) communication. WiMAX has some similarities to DSL in this respect, where one can either have high bandwidth or long reach, but not both simultaneously. The other feature to consider with WiMAX is that available bandwidth is shared between users in a given radio sector, so if there are many active users in a single sector, each will get reduced bandwidth.

The bandwidth and reach of WiMAX make it suitable for the following potential applications:

- Connecting Wi-Fi hotspots with each other and to other parts of the Internet
- Providing a wireless alternative to cable and DSL for last mile broadband access.
- Providing high-speed mobile data and telecommunications services (4G)

The 802.16 MAC uses a scheduling algorithm which the subscriber station needs to complete once (for initial entry into the network). After that the subscriber is allocated an access slot by the base station. The time slot remains assigned to the subscriber station which means that other subscribers cannot use it. The 802.16 scheduling algorithm is stable under overload and over-subscription (unlike 802.11). It can also be more bandwidth efficient. The scheduling algorithm also allows the base station to control QoS parametres by balancing the time-slot assignments among the application needs of the subscriber stations. The most important WiMAX standards are listed in Appendix C Table 12.

WiMAX Security [WIMAX_SEC, WIKIWIMAX]

WiMAX standards define a dedicated security processor on board the base station. There are minimum encryption requirements for traffic and authentication. The authentication is adapted from the Data-Over-Cable Service Interface Specification (DOCSIS) BPI+ security protocol. There, the PKM-EAP methodology is used which relies on the TLS standard. All (user) traffic on a WiMAX network is encrypted using AES in Counter Mode with CBC MAC for confidentiality and data integrity protection. 3DES is also supported.

3.2 WiMAX threats

This section is mainly based on [KAASENBROOD]. WiMAX has some built-in security features. For example, it supports two encryption algorithms (AES and 3DES7 - which for the time being are generally considered secure) [WIMAXFAQ]. All traffic on a WiMAX network must be encrypted using Counter Mode with the Cipher Block Chaining Message Authentication Code Protocol (CCMP), which uses AES for transmission security and data integrity authentication. WiMAX uses TDMA so eavesdropping or a false BS attack can be difficult to conduct.

Even though WiMAX is in use in some locations it is fairly unknown to the public. However it is an upcoming technology and the media interest will rise as it did for wired broadband connections couple of years ago.

Physical Layer Threats

Currently WiMAX is being used as a wireless broadband technology as described in section 3.1. WiMAX uses radio frequencies to transport data between the mobile station and the base station. So if someone has the right equipment they can scramble or jam the necessary frequencies so that the WiMAX equipment cannot transfer data.

False Base Station attack

The authentication protocol used in WiMAX standards before 2005 version does not include authentication for the base station. So any agent can claim to be a legitimate base station. The intruder can misuse this property by claiming to be the legitimate base station and in this way break the confidentiality of messages. If an intruder performs a false BS attack they can pose as the legitimate user to the real BS. If a BS attack if performed successfully the attacker might get their hands on confidential information.

Eavesdropping

In an eavesdropping attack, the attacker can reveal the connection between the user and the corresponding server and the connection identity. In WiMAX the management messages are never encrypted so someone might eavesdrop on them to gain valuable information on the user or the network and use this information to inject messages etc.

Replay attack

User data is encrypted with shared secret but this will not guarantee user data freshness. An attacker can eavesdrop on messages sent and then inject them later into the network. If at that time the Traffic Encryption Key (TEK) is the same then the messages will be accepted by the receiver (TEK has a default 7-hour lifetime). However since the data is encrypted the attacker cannot see the information in the messages.

Denial-of-Service attack

A Denial of service or DoS attack is also a threat because the authentication operations trigger the execution of long procedures. So an attacker can cause harm just by sending a high number of messages to the victim to authenticate.

Data modification

The MAC messages are fairly easy to modify since they are not encrypted. This can cause a great deal of trouble to the user. For example, by modifying the MAC messages an attacker can cause the service user's terminal to enter a dead-lock state [KAASENBROOD]

Table 5. WiMAX threats

Threat	Description
Jamming/scrambling	WiMAX operates on radio frequencies
Eavesdropping	Management messages are not currently encrypted
Rogue BS	2004 WiMAX standard does not include authentication of base station
Denial of Service	Always possible, authentications operations trigger the execution of long procedures – Victim flooded with a high number of messages to authenticate
MAC management message modification	Management messages are not encrypted. Modification is possible
Data traffic modification	Authentication of traffic messages has been discussed – AES is used for protection
identity theft	Reprogramming a device with the hardware address of another device

If hardware can be developed to carry out message injection and eavesdropping, most of the security claims are broken. There is another user scenario for WiMAX. Some experts predict that WiMAX will be used like WLAN. This development hasn't started so it is hard to properly discuss it's security features and therefore it is left out of this report. However it is predictable that the same kind of problems will arise as have been threatening WLAN systems. [DARKREAD]

Most of the discussion of WiMAX is centred on economic topics, i.e. if WiMAX will be a threat to 3G mobile devices. The discussion on technological details has not yet reached the same awareness level.

3.3 Security solutions and analysis for WiMAX

Select the most secure WiMAX standard version for implementation and deployment. Currently, the older standard, IEEE 802.16-2004 is regarded as insecure (PKMv1 only supports unidirectional RSA public key authentication, leaving the base station unauthenticated). Instead, IEEE 802.16e-2005 is currently considered as the most secure choice (PKMv2 supports mutual, manufacturer certificate-based authentication). The 2005-version also supports EAP-based authentication, strong data message encryption, and strong data message integrity and authentication checking. Currently, the mutual RSA certificate-based authentication (PKMv2 using TLS via EAP, and using certificates of both BS and SS) and user data confidentiality & integrity protection by AES in counter mode with CBC MAC are regarded as secure mechanisms [KAASENBROOD, WIMAX_SEC, WIKIWIMAX]. Note that active message injection is a necessary part of almost all assumed attacks against WiMAX, the exceptions being eavesdropping and traffic analysis-type attacks. A successful injection requires an attacker to eavesdrop on the connection identifiers, used modulation techniques and MAC address in advance. Fortunately, message injection to WiMAX signalling is currently difficult due to lack of suitable devices. But in the future it is expected that more and more suitable hardware and software will become available that could make WiMAX message injection possible, and this requires manufacturers to be prepared in advance.

Remember that the 2004 version is insecure and that the 2005 version is backwards compatible with the 2004 version. Hence, for attaining more secure implementation, the backwards compatibility functionality should be removed from the IEEE 802.16e-2005-based implementations.

When going into the nuances of WiMAX security assurance by the operator, in cases where seamless handover functionality (session mobility) is deployed in the 2005 version, it necessarily brings minor vulnerabilities that concern the disclosure of cryptographic session keys. According to the standard solution, these keys must be securely transferred from the previous base station to the new base station (enabling seamless handover), which increases the possibility for key compromise because the key is stored at multiple base stations. However, there are advanced methods (e.g. re-entry, new keying material, handover keys [KAASENBROOD]) which could be used to limit the possibility of key compromise in deployments that support seamless handover, but they are not discussed extensively in this document. However, we assume initial countermeasures to include shortening of the default authorisation key lifetime of 7 days to a shorter value.

Below, we summarise the WiMAX security countermeasures for the most essential main threat categories. In the table “Impact” and “Mature” indicate whether the described countermeasures have High/Medium/Low Impact and whether countermeasures are considered mature (Yes/No).

Table 6. Overview of WiMAX security countermeasures

Threat/Reason	**Countermeasures by actor**		
Eavesdropping: Eavesdropping management messages and user data	Detection: Difficult if not impossible.	Impact (H/M/L): H	Mature (Y/N): Y: User data
	User = Disable WiMAX in suspect situations and when not used. Use end-to-end encryption on top of WiMAX. Manufacturer = For user data, implement a quality, strong encryption/decryption according to latest WiMAX standard (2005-version). For management messages, analyse new, (standard) possibilities for encryption when they come available. For example, the pseudonymity of SS could be protected by encrypting the SS certificate and the nonce. Service = Enforce strong encryption for all connections with base stations, whenever possible.		
Masquerading: BS or SS masquerading	Detection: Use intrusion detection systems (IDS)	Impact (H/M/L): H	Mature (Y/N): Y
	User = Request information and advice from your WiMAX operator about the suspect BS behaviour or conditions. Manufacturer = Implement strong, mutual authentication methods based on EAP methods. Implement PKMv2, which provides mutual authentication (BS and SS authenticate each other). Remove the functionality for backwards compatibility with PKMv1. Service = Enforce strong, mutual authentication methods based on EAP methods.		
Message modification: Management message	Detection: With radio spectrum monitoring equipment, locate rogue devices using radio direction finding tools. Try to identify any message anomalies and reduce connectivity when suspect.	Impact (H/M/L): H	Mature (Y/N): Y/N

Threat/Reason	Countermeasures by actor		
modification, Data message modification	User = Request information and advice from your WiMAX operator about the suspect BS behaviour or conditions. Use end-to-end integrity protection on top of WiMAX. Manufacturer = Implement secure message integrity and authentication for all messages, if possible. Service = Enforce management message authentication (OMAC or better) and data message authentication (AES), whenever possible.		
Message replay: Attacker can record messages and replay until session key changes	Detection: IDS, user awareness.	Impact (H/M/L): M	Mature (Y/N): N
	User = Require replay protection, when it becomes available to WiMAX. Use end-to-end replay protection protocol on top of WiMAX layers. Manufacturer = Include sequence number in the message before transmission and checking of this number at incoming interface. Service = Deploy replay protection, when it comes available. Set shorter lifetime for session keys.		
DoS: Jamming, scrambling, consecutive authentication attempts, forcing SS to deadlock, reset of SS state, etc.	Detection: Jamming: With radio spectrum monitoring equipment, track rogue devices using radio direction finding tools. Scrambling: By monitoring anomalies in performance criteria.	Impact (H/M/L): M	Mature (Y/N): N
	User = Avoid suspicious networks. Enable the connections only with networks you trust. Manufacturer = Enable adjustable power of RF transmissions, use high gain antennas, increase the bandwidth of signals using spreading techniques. Disable rogue deadlocking by digitally signing the related management messages *(auth invalid, perm auth reject*), etc. Service = Deploy IDS/IPS. Enforce such authentication methods which require work from the initiator. Analyse whether management messages could be authenticated and replay protected.		

Threat/Reason	Countermeasures by actor		
Miscellaneous attacks	Detection: Sudden interruptions or malfunctions in communications are suspicious.	Impact (H/M/L): H	Mature (Y/N): N
	User = Disable communications when observing strange behaviour. Manufacturer = test the security and interoperability with best practices. Service = Select WiMAX Forum-certified products & profiles only.		

4. Bluetooth

4.1 Bluetooth Technology

Bluetooth [WIKIBT, BT_ORG, BT_SIG] is a radio standard and communications protocol (IEEE 802.15.1)[802.15.1] for wireless network personal area networks. Bluetooth is primarily designed for low power consumption, with a short range (depending on power class, up to 100 metres). Bluetooth operates in the license-free ISM band at 2.45 GHz.

Bluetooth lets devices (such as mobile phones, hands-free sets and laptops) communicate with each other when they are in range. A Bluetooth device playing the role of the master can communicate with up to 7 active slave devices, thus forming a piconet. A piconet is an ad-hoc computer network of devices using Bluetooth technology protocols. Up to 255 further slave devices can be inactive, or parked, which the master device can bring into active status at any time.

At any given time, data can be transferred between the master and 1 slave; but the master switches rapidly from slave to slave in a round-robin fashion. Either device may switch the master/slave role at any time. The Bluetooth specification [BT_SPEC] allows the connecting of 2 or more piconets together to form a scatternet, with some devices acting as a bridge by simultaneously playing the master role in one piconet and the slave role in another piconet.

Any Bluetooth device will transmit the following sets of information on demand:

- Device Name
- Device Class
- List of services
- Technical information e.g.: device features, manufacturer, Bluetooth specification version, clock offset

Any device may perform an "inquiry" to find other devices to which to connect, and any device can be configured to respond to such inquiries. However, if the device trying to connect knows the address of the device it will always respond to direct connection requests and will transmit the information shown in the list above if requested for it. Use of the device's services however may require pairing or its owner to accept but the connection itself can be started by any device and be held until it goes out of range. Some devices can only be connected to one device at a time and connecting to them will prevent them from connecting to other devices and showing up in inquiries until they disconnect from the other device.

Every device has a unique 48-bit address. However, these addresses are generally not shown in inquiries and instead friendly "Bluetooth names" are used which can be set by the user, and will appear when another user scans for devices and in lists of paired devices.

Most phones have the Bluetooth name set to the manufacturer and model of the phone by default. Most phones and laptops will only show the Bluetooth names and special programs are required to get additional information about remote devices.

Pairs of devices may establish a trusted relationship by learning (by user input) a shared secret known as a "passkey". A device that wants to communicate only with a trusted device can cryptographically authenticate the identity of the other device. Trusted devices may also encrypt the data that they exchange over the air so that no one can listen in. The encryption can however be turned off and passkeys are stored on the device's file system and not the Bluetooth chip itself. Since the Bluetooth address is permanent a pairing will be preserved even if the Bluetooth name is changed. Pairs can be deleted at any time by either device. Devices will generally require pairing or will prompt the owner before they allow a remote device to use any or most of its services.

Bluetooth Security

According to Gehrmann [GEHRMANN], the fundamental security expectations that Bluetooth security aims to reach, are:

- Easy-to-use and self-explanatory security configuration
- Confidentiality protection
- Authentication of connecting devices
- Anonymity

There are three modes of security for Bluetooth access between two devices. [BT_SEC]

Security Mode 1: non-secure

Security Mode 2: service level enforced security

Security Mode 3: link level enforced security

The manufacturer of each product determines these security modes. Devices and services also have different security levels. For devices, there are two levels: "trusted device" and "untrusted device." A trusted device, having been paired with one's other device, has unrestricted access to all services. With regard to services, three security levels are defined: services that require authorization and authentication, services that require authentication only and services that are open to all devices.

Algorithms E_1, E_{21}, E_{22}, and E_3, used for key generation and authentication in Bluetooth, use the same underlying 128-bit block cipher SAFER+. The initialisation key and master key are generated using the E_{22} algorithm. The encryption algorithm is stream cipher E_0 based on a direct design and uses a Bluetooth proprietary algorithm. [GEHRMANN]. The next version of Bluetooth technology includes a number of features to increase the security and usability of Bluetooth [WIKIBT]:

- Atomic Encryption Change – allows encrypted links to change their encryption keys periodically, increasing security, and also allowing role switches on an encrypted link.
- Extended Inquiry Response – provides more information during the inquiry procedure to allow better filtering of devices before connection. This information includes the name of the device, and a list of services, with other information.
- Sniff Subrating – reducing power consumption when devices are in the sniff low-power mode, especially on links with asymmetric data flows.
- QoS Improvements – these will enable audio and video data to be transmitted at a higher quality, especially when best effort traffic is being transmitted in the same piconet.
- Simple Pairing – this improvement will radically improve the pairing experience for Bluetooth devices, while at the same time increasing the use and strength of security.

4.2 Bluetooth threats

Bluetooth, having been incorporated into virtually every kind of mobile device, from cordless headpieces for mobile phones to cars and laptops, has become interesting for both security analysts and malevolent programmers. The variety of devices and implementations together with the very large core specification and a number of additional specifications offer a wide range of possibilities for implementation errors and vulnerabilities.

Bluetooth is also well-known to the general audience, and security incidents have been widely reported. The first mobile phone worm, Cabir, used Bluetooth to propagate. The Car Whisperer project showed that Bluetooth devices in cars would typically use factory-preset PIN numbers of interesting cryptographic capabilities such as "0000" or "1234", allowing an attacker to listen into conversations inside a car or send his voice to be repeated via the car loudspeakers.

The main threats to Bluetooth users are data theft, unauthorised use and damage to devices. As examples of previously detected implementation vulnerabilities, the BlueSnarf attack steals personal data and the BlueBug [BLUEBUG] attack allows the attacker to use your mobile phone at will via Bluetooth to, for example, make phone calls and send messages. [TRIFINITE] lists a number of projects which have succeeded in compromising the security of

Bluetooth devices. Later product versions have typically fixed these vulnerabilities. Also, it is generally thought that the Bluetooth range is only 10 metres, and for commercial products this is the case. However, vulnerability researchers have found that with directional antennas, the possible attack range can be significantly higher, and up to 2km ranges have been reported. This means that Bluetooth devices are not necessarily safe from attack if there are no devices nearby. The attacks so far have not been dependent on vulnerabilities in the Bluetooth specification, but instead in the Bluetooth implementations of specific vendors.

Some of the publicised vulnerabilities, such as the Cabir worm, require the user to initiate the malevolent activity by allowing the Bluetooth connection. Security features and prompting the user in key situations make Bluetooth secure to these attacks as long as the user acts responsibly. However, as a result of these features, Bluetooth is sometimes considered to be cumbersome to use, and some pressure has emerged to make use of Bluetooth easier (more automatic) for the user, a development which might cause further problems.

Further problems, as shown by the Car Whisperer case, result from improperly configured Bluetooth devices - often the factory settings of Bluetooth devices may compromise the user to attack. As a result, recommendations often signify the importance of correct Bluetooth configuration to avoid harm. The most prevalent is the operation mode, which determines whether the Bluetooth device is made visible to other Bluetooth devices in the vicinity (or to the antenna 2km away). It is important for the users to realise, however, that the non-discoverable mode does not mean that the device cannot be discovered; the address space can be scanned relatively quickly to find hidden devices.

The Bluetooth special interests group [BT_SIG] acts as an umbrella organisation for Bluetooth manufacturers, and it currently has over 6000 members (manufacturers of Bluetooth devices). The Bluetooth protocol is and has been under constant development (currently at version 2.0) and future versions are to increase security further. No critical shortcomings have been observed in the current version of the Bluetooth specification.

If no vulnerabilities in the core protocol are introduced in future versions, the most significant security issue will thus be on quality assurance of the growing number of Bluetooth manufacturers. Faulty implementations are unlikely to disappear (as the protocol complexity grows, the opposite will probably be the case), but the impact is likely to be limited to certain vendors. Individual vendors can protect their customers by appropriate quality assurance and security auditing procedures for their Bluetooth products.

The impact of future vulnerabilities for individual users cover the entire range of integrity, confidentiality and accessibility: vulnerabilities may allow attackers to disable devices, to eavesdrop communications, use the devices without permission and most importantly, access the growing amount of confidential data that is carried around in portable devices.

One threat to the privacy of the user is a location attack, where a particular Bluetooth device is physically followed. This means that any person with a device that has Bluetooth turned on and in discoverable mode can be followed once found. [JAKOBSSON]

4.3 Security solutions and analysis for Bluetooth

Bluetooth wireless technology provides peer-to-peer communication over short distances. In order to provide usage protection and information confidentiality, the system provides security measures both at the application layer and the link layer [BT_SPEC] appropriate for the peer environment. The standard mandates that in each device the authentication and encryption routines must be implemented in the same way.

Four different security entities are used for security at the link layer: a Bluetooth device address, authentication and encryption keys, and a pseudo-random number that will be regenerated for each new transaction. The Bluetooth device address can be obtained via user interactions, or, automatically, via an inquiry routine by a device.

Table 7. Security entities used in Bluetooth link layer security procedures

Key	Size (bits)
Bluetooth Device address	48
Private user key, authentication	128
Private user key, encryption	8-128 (recomm. 128)
Pseudo random number	128

The security in the latest Bluetooth standards is quite extensive. This is perhaps because the standardization organisation (Bluetooth Special Interest Group [BT_SIG]) has put a lot of effort into security issues and the standard has several options for implementing security for various use cases with different requirements for computing power, security and ease-of-use. Hence, most of the incidents, where data has been compromised on mobile phones, have not been caused by a problem in the standard itself, but rather in the implementation quality.

At a high level, there are three modes of security for Bluetooth access between two devices (see section 4.1), and it is a manufacturer-specific issue of what security modes the products will support. The encryption algorithm (E_0 stream cipher) described in Bluetooth specifications can be considered as secure (one flaw that has been found [BT_FLAW]). It is implemented in services such as a mobile phone synchronizing with a PC, and a PDA using a mobile phone as a modem [BT_SEC].

Below is a table that summarises Bluetooth security countermeasures for the most essential main threat categories. In the table “Impact” and “Mature” indicate whether the described countermeasures have High/Medium/Low Impact and whether countermeasures are considered mature (Yes/No).

Table 8. Overview of Bluetooth security countermeasures

Threat/Reason	Countermeasures by actor		
Eavesdropping: Listening to BT traffic.	Detection: Difficult if not impossible.	Impact (H/M/L): H	Mature (Y/N): Y
	User = Enable encryption setting in the product. Manufacturer = Implement strong cryptographic encryption. In implementations, the encryption key size should not be changeable by the user. Service = Configure the device to use strong encryption in pairing.		
Masquerading: Calculating link’s PIN from messages. Unauthorised BT connection/ pairing and use of resources. Bluejacking, bluesnarfing, bluebugging.	Detection: Difficult because device address may be sniffed and used.	Impact (H/M/L): H	Mature (Y/N): Y
	User = Require for software upgrades which close the vulnerabilities. Employ at minimum an eight character or more alphanumeric PIN when possible. Product owners must share that PIN number only with trusted individuals and trusted products for pairing. Do not grant pairing with unknown devices. Go to a private, spacious location to pair your devices. If your device is lost, you should unpair that device from all of your previously paired devices. Bluesnarfing: Set device in non-discoverable mode. Disable BT totally when not used. Change device name for more anonymity. Manufacturer = Devices should in general require pairing and/or prompt to user before allowing remote device to use its resources/services. Bluebugging: Correct any implementation problems in products. Car whisperer: Correct certain implementation problems in Bluetooth-enabled car kits. Service = Install software upgrades which close the vulnerability. Configure the user device to only accept pairing to certain devices (own headset, own PC, etc.) automatically and inform user about the dangers in pairing with unknown devices. In each pairing, grant remote device access only to the needed resources/services of the device.		

<table>
<tr><th>Threat/Reason</th><th colspan="3">Countermeasures by actor</th></tr>
<tr><td rowspan="2"><b>DoS</b>: Unwanted connections</td><td>Detection: Rapid battery degradation, communication slows down. Probably probing for disturbing sources.</td><td>Impact (H/M/L):
L</td><td>Mature (Y/N):
N</td></tr>
<tr><td colspan="3">User = Avoid suspicious locations with BT enabled.
Manufacturer = Develop devices that discover and possibly locate malicious/erroneous radio transmitters. Implement DoS protection features. Future Bluetooth core specifications are planned to make it impossible to penetrate non-discoverable devices.
Service =</td></tr>
<tr><td rowspan="2"><b>Miscellaneous attacks</b>: Disclosure of personal data. Viruses, worms. Tracking BT devices.</td><td>Detection: Antivirus/malware alarm, entries in system & firewall logs, System software and UI that notify all BT devices nearby to the user.</td><td>Impact (H/M/L):
H</td><td>Mature (Y/N):
Y</td></tr>
<tr><td colspan="3">User = Be security aware. Never install software or accept messages or address book entries from suspect sources. Use proven products. Avoid old BT devices and software. Disable BT when not in use. Use antivirus and firewall software.
Manufacturer = Invest in quality processes and quality assurance. Implement less functionality with good quality. Apply security and vulnerability testing and evaluation methods. Implement layered access control on personal data and credentials. Distribute patches out that fix the found vulnerabilities.
Service = IT departments of organisations should select the best-quality products and be aware and continuously protect user's software against new vulnerabilities with (automatic) upgrading. Avoid old BT devices and software. Change the default factory settings for more security. Set BT to non-discoverable mode. Increase security awareness of users.</td></tr>
</table>

Some user perspective countermeasures [BT_SEC], [FICUSER2]:

- Unless you have a clear reason for allowing others to see your device, it is advisable to choose non-discoverable mode in your Bluetooth connection setting. It is important to remember that this does not prevent the dedicated attacker from finding your device by scanning the address range.
- Phone owners who receive bluejacking messages, or similar queries, should refuse to add the contacts to their address book.
- Without user permission, malware having accessed a mobile phone via Bluetooth cannot install itself. If a device requests for an installation of an unknown program, it is recommended to reject such an installation.

- It is normally possible to define a list of trustworthy devices that can be connected to your mobile phone via Bluetooth.
- If a malicious program repeatedly tries to access your mobile phone via Bluetooth, try to move outside the coverage area.

To get an impression of the Bluetooth technical specification, see below a detailed example from the link manager authentication procedure:

Technical example: Authentication in Bluetooth link manager protocol [BT_SPEC]

The authentication procedure is based on a challenge-response scheme. The verifier sends a PDU that contains a random number (the challenge) to the claimant. The claimant calculates a response that is a function of this challenge, the claimant's device address and a secret key. The response is sent back to the verifier, which checks if the response was correct or not. The response shall be calculated using:

- An authentication code which employ the encryption function SAFER+. The algorithm is an enhanced version of an existing 64-bit block cipher SAFER-SK128, and it is freely available. The block cipher uses 128-bit key.

A successful calculation of the authentication response requires that two devices share a secret key. Both the master and the slave can be verifiers (mutual authentication):

- When two devices do not have a common link key, an initialization key shall be created based on a PIN, a random number, and a device address. When both devices have calculated initialization key the link key shall be created, and mutual authentication is performed.

5. 3G and 4G

5.1 3G Technology

3g is a mobile phone technology based on (and successor to) the 2G technology. In this study, we do not cover the radio technology of 3G, but some solutions are presented mainly for the end user of 3G devices.

4G is an abbreviation of Fourth Generation, the successor wireless communication technology to 3G. This term does not refer to one particular standard, but describes several different but overlapping ideas. If a new generation is defined by the result of technological changes over a 10 to 15 year time frame, 4G would refer to wireless technologies deployed in the 2010 to 2015 period, assuming 3G deployment spans the 2000 to 2009 period. There are several 4G working groups and labs. Some examples include [4GLAB, 4GMF, MITF].

Different working groups have identified requirements and defined initial infrastructures for 4G systems. Typically the approaches concentrate on defining requirements for new radio access technologies (most popularly a type of OFDM, Orthogonal Frequency Division Multiplexing) and various types of packet-based core network technologies. In many proposals, 4G is intended to provide high speed, high capacity, low cost per bit, IP based services for video, data and voice (VoIP).

4G will most probably be an integrated, global network that will be based on an open system approach. Almost all the standards from 2G and 3G have been envisioned as being part of 4G. The system will act as an open platform where the new innovations can go. Some of the standards which pave the way for 4G systems are WiMAX, WiBro, and the proposed 3GPP Long Term Evolution work-in-progress technologies such as HSOPA (High Speed OFDM Packet Access) [WIKI4G].

A quite common opinion is that 4G will support a great number of wireless devices that are addressable and routable. Therefore in the context of 4G, IPv6 is an important network layer technology and standard that can support a great number of devices.

5.2 3G and 4G threats

3G devices can usually connect to the Internet. Therefore, 3G devices will be vulnerable to mobile viruses etc. However this kind of discussion is left out of this report. Generally the UMTS technology is more secure than its predecessor GSM. Although it is not totally threat-free. Some of the threats to 3G originate from the fact that the newest mobile phones resemble personal computers in many ways (you can install software on them, they crash more often than their predecessors, etc.). So the attacker can install some malicious software (malware) to eavesdrop on phone calls. One survey [3GPP] of 3G security was published in 2003. Some of the issues revealed then have been already covered.

The whole concept of 3G is so vast that it is really hard to properly discuss its vulnerabilities within the scope of this paper. However, the development of 3G terminals has led to a feature set that closely resembles those of personal computers. This development is likely to lead to the point at which the threats and vulnerabilities of 3G devices have a close resemblance to those in personal computers connected to public networks.

Because 4G is envisioned to be a collection of wireless standards, there should be a way to constitute all standards. This can be achieved using Software Defined Radio (SDR) architecture. Security issues related to Software Defined Radio should be carefully investigated. Since the radio can be updated and configured to various configurations, the role of security-aware configuration management is an important issue.

Since currently there are numerous opinions on what 4G should be, we cannot reasonably and holistically discuss the security issues of this future communications system. However, it is obvious that 4G is subject to all the generic threats. In general, it is very challenging to try to estimate threats of novel technologies that have not been deployed yet and the results of convergence of various current technologies.

5.3 Security solutions and analysis for 3G

The security of third-generation radio networks is under the regulatory control of governments and international organisations that support co-operation between operators. There are several reasons why the security of 3G is often assumed to be at an adequate level, including:

- National and international regulative bodies’ authorised control and telecom operator’s internal enforcement.
- Availability of accumulated security experiences during the operation of cellular networks from the very first generations to the latest cellular networks (New operators may lack this).
- The open nature of 3G standardisation (3GPP, ETSI), which includes definition of security architecture, protocols and algorithms with the defined system. Also, the effort put into selection criteria, security evaluation and testing of security algorithms has been big.

These facts and our previous experience of 3G standardisation indicate that most of the **vulnerabilities in the usage of 3G networks** come from:

- Complexity of use cases (one network may support a multitude of different usage scenarios and capabilities to extend the connectivity even further). Increased digital convergence in 3G mobile networks:
  - 3G-WLAN interworking (vulnerabilities of WLAN networks, vulnerabilities of interworking).
  - 2G-3G roaming (vulnerabilities of 2G networks and roaming).
- Hidden vulnerabilities in implementation and deployment (complexity of networks, mobiles and software).
- Increased malware execution possibilities in mobiles (increased use of “open developer” operating systems, such as Symbian OS and Microsoft Windows Mobile).
- Lack of user security awareness.

The regulation also has negative implications for security. In most countries, the law and enforcement mandate telecom operators to give clear text access to cellular communications made by a certain suspect individual, if a court order exists for this particular lawful interception. Therefore, the telecommunications operator must be able to arrange a well-secured information flow from their network to the dedicated site where the crime investigator will be able to monitor the connection information, suspect’s voice and/or clear text data. Therefore, this arrangement adds a certain vulnerability to the network itself and user data. Criminals could try to take advantage of this legal backdoor.

Some user perspective on 3G. See [FICUSER2]:

Increase your security awareness and security increasing behaviour, for example:

- Read the manual of the mobile phone and activate your mobile phone’s information security settings
- Make sure that the PIN request is activated on your mobile phone.
- Use the barring and restriction services provided by operators. Select trusted operators, technologies, services, etc.
- Keep your mobile phone’s IMEI code in a separate place in case your mobile phone gets lost. Immediately inform your operator in case of theft.
- Make regular backup copy of the mobile device’s memory on your computer or memory card. Store the backup in a safe place.

- You may receive a call or an SMS message in an effort to commit a fraud against you. (E.g. to make you call an expensive toll number or a phone number abroad). Question the request before answering or otherwise positively reacting to the request.

6. RFID

6.1 RFID Technology

Radio Frequency Identification (RFID) [WIKIRFID] is an automatic identification method, relying on storing and remotely retrieving data using devices called RFID tags or transponders. An RFID tag can be attached to objects such as consumer goods for the purpose of identification using radio waves [T2308]. The least expensive RFID tags are read-only. Writeable tags are more expensive, while rewritable tags (containing EEPROM) are the most expensive ones.

RFID tags can be classified according to their source of power. The tags can be passive, semi-active or active [RSA].

Table 9. RFID Tag types

Tag type	Description
Passive	The most inexpensive and compact tag type. Derive all of their transmission power from the reading device, and hence offer a virtually unlimited operational lifetime. The trade-off is that they have shorter read ranges than active tags and require a higher-powered reader. Tags that are read-only are typically passive and are programmed with a unique set of data (usually 32 to 128 bits) that cannot be modified [AIM]. Passive tags are the most physically robust RFID tags [RSA].
Semi-active	Make use of battery power to run local circuitry, but use reader power for communication. [RSA]
Active	Powered by an internal battery and are typically read/write, i.e. tag data can be rewritten and modified. They are capable of broadcasting at much longer distances than passive ones [RSA]. The trade-off is greater size, greater cost, and a limited operational life (which may yield a maximum of 10 years, depending upon operating temperature and battery type). Active tags are typically more reliable (e.g. fewer errors) than passive tags due to their ability to conduct a "session" with a reader. [WIKIRFID]

Another way to classify RFID tags is the frequency at which they operate. The two most important RFID-frequency categories are as follows:

Ultra-High Frequency (UHF): UHF tags operate in the 868-956 MHz frequency band. One of the big benefits of passive UHF tags is that in many environments they have a range of 3 metres, sometimes even up to 10 metres. Additionally, RFID readers can scan hundreds of UHF tags simultaneously. A drawback of UHF tags is that while higher frequencies offer greater range, they are subject to greater physical interference.

High-Frequency (HF): HF tags operate at 13.56 MHz. Passive HF tags have the drawback of low transmission range (up to 0.5 metres). In general, they are also larger than UHF tags; flat HF tags are typically about 50mm by 100mm in size. HF tags, however, have the advantage of offering better penetration of materials.

Other frequencies: RFID tags also come in a low-frequency (LF) variety operating at 120-140 KHz. These tags tend to be popular for use in building-access badges and animal tagging. RFID tags can also operate at higher UHF frequencies, most notably at 2.45 GHz.

RFID system

A basic RFID system may consist of several components: [AIM, WIKIRFID]

- An antenna or coil
- A transceiver (with decoder)
- A transponder (RF tag)
- Middleware/ application software

The purpose of an RFID system is to enable data to be transmitted by a mobile device, called a tag, which is read by an RFID reader and processed according to the needs of a particular application.

The interrogator, an antenna packaged with a transceiver and decoder, emits a signal activating the RFID tag so it can read and write data to it. Antennas are the conduits between the tag and the transceiver, which controls the system's data acquisition and communication. Often the antenna is packaged with the transceiver and decoder to become a reader, which can be configured either as a handheld or a fixed-mount device. The reader emits radio waves, the range depending upon its power output and the radio frequency used. When an RFID tag passes through the electromagnetic zone, it detects the reader's activation signal. The reader decodes the data encoded in the tag's integrated circuit and the data is passed to the application software in the host computer for processing.

Standards and regulations

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. [T2308]

There is no global public body that governs the frequencies used for RFID. In principle, every country can set its own rules for this. In Europe the bodies are ERO, CEPT, ETSI, and national administrations.

RFID Security

The most inexpensive (and widely used) RFID tags lack the computing power to perform even basic cryptographic operations. Such tags are at best capable of employing static keys, i.e. PINs, as security mechanisms. For example, the "kill codes" used to disable EPC tags for purposes of privacy are secured by PINs. The limited capabilities of such RFID tags make privacy and security enforcement a special challenge [RSA].

More expensive RFID tags are capable of advanced functionality, and often include the ability to perform basic cryptographic algorithms, such as symmetric-key encryption and challenge-response identification protocols. Public-key cryptography is expensive and used on few RFID tags [RSA].

6.2 RFID threats

RFID is commonly used as a communication protocol for contactless smart cards, access tokens or plain identification tags. RFID itself provides no security features, but applications commonly provide their own cryptography to address security.

RFID applications are often designed with the assumption that the designed operating range acts as a physical barrier for undesired access. However, specialised antennas can be used to radically increase range, and enable orders of magnitude greater range for communications.

The wide variety of custom security solutions assures a wide variety of security vulnerabilities, as proprietary solutions tend to be more poorly thought out than widely reviewed open standards.

There have been many high-profile cases of security problems in devices utilising RFID. Many nations have implemented RFID in passports, allowing passport information to be read over the air without authentication. A myriad of security concerns have been raised over this, ranging from the ability to remotely clone passports to bombs exploding when near a passport of a desired nationality. These threats are more or less hypothetical.

RFID chips are embedded underneath the skin of pets and humans for tracking purposes. This presents an obvious privacy threat (for humans at least). Cloning of passive RFID tags is a threat to many RFID applications (e.g. when passive RFID tags are used as keys or other access control, which they are not suitable for). RFID tags are easy to damage so that they no longer function. There are plenty of cases of RFID security incidents and other information in Bruce Schneiers blog [SCHNEIER_BLOG].

6.3 Security solutions and analysis for RFID

A major difficulty for successful security evaluation of RFID systems is that many vendors have developed proprietary RFID tags and solutions, which only partially implement the open standards, the rest being proprietary. In the case of proprietary design, one should request a security solution description from the vendor and study it, and/or try to security-test the devices in practise.

Looking at the Table 13 in Appendix D, we can conclude that **many RFID standards provide very little security or privacy features, if any**. This means that security often remains a vendor-specific issue, which in turn limits interoperability between the devices. On advanced RFID device types (contact-less smart cards), the information security may have been developed at a higher application layer, because there could be memory and processor available in tags. Unfortunately, this approach does not protect against all possible malicious activities, but perhaps only safeguard the application-specific data. For example, a search for tag IDs for tracking purposes may still be easily possible (if tag not killed), which erodes privacy.

Tags often have very limited computing capabilities. Most tags do not support authentication, access control, or encryption techniques. Some RFID standards specify features including passwords to protect access to certain tag commands and memory, but security assurance of its communication is often weak. Vendors can offer proprietary security features, the implication of which being interoperability and verification problems.

Technical Tag protections:

Tag Security functionality: Tags with on-board memory are often coupled with security mechanisms to protect the data stored in that memory. Some tags support a *lock* (permanent or by reader) command that can prevent modification or access of data in the tag's memory. Commonly only contactless RFID smart cards may support cryptographic algorithms for authentication and data confidentiality. Some tags offer tamper protection as a physical security feature.

Tag Privacy functionality: EPC tags support an irreversible feature called the *kill* command that permanently disables the ability of the tag to respond to commands and also access to a tag's identifier and memory. While this RFID tag then becomes permanently non-functional, it cannot be used any more for tracking purposes and hence preserves the privacy of the attached object without removal.

However, there are serious basic issues that are difficult to tackle using only information security protection. In most RFID applications the users or attackers could:

- Damage a tag
- Remove the tag or replace it
- Clone a tag

Therefore, these facts should be taken into account in system design. It is very important to be able to estimate the vulnerable area or volume that is around the reader (and the tag). See below a list of ranges that need to be estimated or experimentally measured during the system design.

Some important RFID operational ranges (distances)

- **Nominal operating range:** authorized transactions are expected to occur.
- **Back channel eavesdropping range:** a rogue receiver can reliably interpret a tag's response to a legitimate reader.
- **Rogue skimming (or scanning) range:** a rogue reader operating above regulated power limits can reliably communicate with a tag.
- **Rogue command range:** a rogue reader can execute a tag command.
- **Forward channel eavesdropping range:** a rogue receiver can reliably listen to the transmissions of an authorized reader.
- **Forward channel traffic analysis rang**e: a rogue receiver can detect the presence of an reader's signal.

For example, the rogue scanning range of an ISO 14443 contactless RFID smart card could be about 50 cm, which is five times the standard's nominal operating range.

There are a several different technical controls currently available for RFID systems, and many others are under development in industrial and university research labs. Technical controls currently available for **protecting tag data** include:

Some technical controls available for protecting tag data and RF interface

Tag memory access controls (restrict the use of tag commands and access to data). SECURITY: The password/PIN length on many tags is too short so that tags can be killed maliciously.

Kill feature. SECURITY: Stored data still exists enclosed in the tag.

Encrypting the data on tags. SECURITY: The encryption algorithm is weak and the encryption key is too short. Encryption requires key management (difficult in many RFID usage scenarios)

Authentication. SECURITY: Weak authentication protocol/algorithm used in standard. Some tags use a "rolling code" scheme to make tag cloning harder. Challenge/response protocols provide for better security but their deployment typically require dramatic costs compared to the whole RFID application.

Tamper protection. SECURITY: Still difficult to prevent theft of or damage to the tag

Selection of radio frequency to avoid interference and blocking. SECURITY: Attacker can follow the frequency

Transmission characteristics can be tuned to reduce eavesdropping. SECURITY: Reliability of normal operation decreases

Shielding can be installed to limit eavesdropping and rogue scanning. SECURITY: Shielding can be removed

Cover-coding can be used to obscure the content of messages (generates cipher text using XOR operation between plain text and 16 bits random number). SECURITY: Attacker may break the random number by brute force attack

RF interface for active tags can be shut off when not used. SECURITY: Attacker may shut off a tag on purpose

Finally, we list some basic advice for system designers to mitigate the wireless security risks of RFID. We believe that in most cases the design focus must be on the very basic issues, such as:

- Reducing the functional area/volume of RF as small as possible
  - Limitation of power. Try to find minimum but robust range
  - Check possibility to use directional antenna

- Protecting the surroundings of RF functional area/volume
  - Use mechanical shields
  - Make tampering of tags and shields visible
- Increasing user awareness of used technology
  - Use standardised physical user interface notations (industry standard label)
  - Education of users, inform users about vulnerabilities

7. Flash-OFDM

7.1 Flash-OFDM Technology

Flash-OFDM was developed by Qualcomm Flarion technologies [QUALCOMM]. Flash-OFDM is a mobile, wide-area-network cellular technology that works with all existing Internet protocols and delivers an extension to the Internet over the air. Flash-OFDM base stations are access routers that plug directly into the edge routers of an all-IP infrastructure. Mobility is managed using the mobile IP protocol. [NAP]

In Finland the old 450 MHz frequency band that was used by NMT is licensed to Flash-OFDM operator Digita Oy. It has begun deployment of its nationwide "@450" wireless network, planned to be operational in April 2007. Flash-OFDM is a relatively new technology and geared mostly to the needs of people living in sparsely populated areas.

Flash-OFDM employs unspecified cryptographic security mechanisms to provide radio link security keyed by MAC address from the user-side Flash-OFDM equipment. Specifications for cryptographic details, protocols and operations in layers 1 and 2 are only available under NDA, and have not been publicly analysed. Thus evaluating protocol- and crypto-related security threats is not possible.

Digita has provided us with a couple of details about the security features of Flash-OFDM. It is claimed that authentication of users is based on the industry standard Radius and EAP, and data encryption is carried out with a 128-bit Rijndael Block Cipher (the same algorithm is used in AES) both ways in the over-the-air interface. The actual implementation is not analysed or guaranteed to be correct.

7.2 Flash-OFDM Threats

Historically, secret and/or proprietary commercial security mechanisms have tended to be less secure than systems based on peer-reviewed and published mechanisms. Therefore Flash-OFDM security should be taken with a grain of salt.

Qualcomm is currently the only manufacturer of Flash-OFDM through supply and integration agreements with Siemens. Homogeneity of equipment may make it more vulnerable in case a common vulnerability in the software or hardware implementation of Flash-OFDM is discovered. If there is a vulnerability in some device or service, it will have an effect on all users. Flash-OFDM is a technology in its early stages of deployment, so its usage and market scenarios might evolve beyond what is described here.

7.3 Security solutions and analysis for Flash-OFDM

At the moment, the Flash-OFDM device manufacturer alone is in charge of an extreme amount of security responsibility. For example, in any cryptographic communication algorithm and security protocol design, the following challenges apply:

- Choice of cryptographic algorithm(s)
    - Each algorithm has a multitude of crucial characteristics, such as cryptographic strength, robustness, performance, bit error propagation, modularity of design, initialisation issues, key scheduling, etc.

- Design of a robust and secure communication protocol
    - Only such protocols, that have been designed, analysed, evaluated and tested in public collaboration for several years, can be regarded as secure protocols.

Especially in wireless protocols, where the transmitted radio frames are accessible by vast public audience, these selections and design choices cannot be kept secret by any manufacturer or the technology has a credibility problem.

Therefore, any general wireless threat might apply to Flash-OFDM technology, because there is no evidence of the contrary. Therefore, any miscellaneous attack, eavesdropping, man-in-the-middle attack, masquerading, message modification/replay, traffic analysis, and denial of service might be possible against Flash-OFDM. The needed countermeasures, related to this specific wireless technology cannot be given before publication of the used protocols, algorithms, etc. In the table “Impact” and “Mature” indicate whether the described countermeasures have High/Medium/Low Impact and whether countermeasures are considered mature (Yes/No).

Table 10. Brief overview of uncertain security concerning Flash-OFDM

Threat	**Countermeasures by actor**		
Technology not publicly evaluated (solution concealed)	Detection: Obvious. For information, contact public authorities, standardisation and research organisations.	Impact (H/M/L): H	Mature (Y/N): N
	User = Be aware of the risks of using concealed, non-public solution. For example, industrial espionage is easier to arrange in concealed solutions. They can also open up vulnerabilities due to unknown dependability, errors in critical parts, etc., which may have very wide influence. Manuf. = If possible, try to increase the openness of solutions in the long term. Invest in co-operation, standardisation activities and public verification. Proceed towards open interoperability testing between vendors. Invest in vulnerability and security testing. Service = Require vendors to open up their specifications for public evaluation. Avoid using non-standard wireless technologies. If you choose a concealed solution, invest in contracting plus vulnerability and security testing.		
Immature technology, limited number of vendors	Detection: Obvious. Maturity is not guaranteed if standards and interoperability test documentation are not available, for example.	Impact (H/M/L): H	Mature (Y/N): N
	User = In general, do not take an immature technology into use. Require products that are tested or certified by trustworthy communities. Manuf. = Implement public measures to increase the maturity level of used technology and products. Service = Select only mature technologies for deployment. For example, it is very expensive to upgrade all hardware after deployment. Arrange smaller-scale pilots first and carefully analyse the results. Help manufacturers to develop the technology further by giving requirements and feedback. Select only technologies that are supported by multiple vendors.		

8. Conclusions

The failure modes, or possible vulnerabilities, of a computer system grow faster than the number of features. Geer writes in [GEER] that "absent perfection, each new feature comes with new failure modes, and features can sometimes interact; therefore, the potential number of failure modes quite naturally can grow faster than the feature count." Based on this, we can confidently state that the more complex a system is, the more vulnerable it will be.

A secure system should therefore strive to be as simple as possible. However, this is often not the way that security is being introduced in modern communication systems. Rather, security is considered to be something that is glued onto an existing system. This means that instead of two systems communicating, we have a number of security systems between the systems tampering with the communication. All this is added complexity, and with sufficient overhead, the security of the overall system will decrease. Security products are no exception from other computer products - the fact that they should provide more security does not automatically mean that they are free of faults.

Antivirus system vendors and firewall manufacturers naturally recommend their products as a cure to any security problem conceivable. However, it is recommended that whenever choosing a new security product for a system, whether the added complexity is needed is carefully evaluated.

Viewing the system as a whole is critical for analysing the security of any concrete use scenario. Wireless technologies are often only a small part of the whole application. To form a useful view of threats, risks, solutions and tradeoffs in a given application, one needs to evaluate all the components of the system as a whole, in connection with the environment, context and security management practices. In most cases the wireless technologies discussed in this report are just small components of applications they support, and analysing their security separately has limited potential. A mobile phone user is affected by the security of the software in their terminal device, and the whole communication technology stack between the users and the end service that they are using.

Most wireless network technologies include security features that we should use. In some cases this may require purchasing new products, even if the old ones are still working. Furthermore, it is always advisable to also apply security features of upper layers: corporate users should use VPN tunnels and application-level encryption (SSL/TLS) should be in use when necessary.

With WLAN, home and corporate users are encouraged to use WLAN products with Wi-Fi Protected Access 2 (WPA2) when possible. The use of WPA is suggested if WPA2 is not available. With legacy devices, the use of VPN solutions in conjunction with WEP is advisable. When using WLAN as an access network, upper layer security features must be used to enable end-to-end security.

WiMAX can be considered secure if equipment is implemented according to IEEE 802.16e-2005. The introduction of PKMv2 in this standard version adds support for mutual authentication. The new standard also supports EAP-based authentication. The only downside of the 2005 version is the backwards compatibility with the older 2004 version. This compatibility introduces security threats that were covered in the design of the 2005 version. Leaving this backwards compatibility enabled makes WiMAX vulnerable to the security downgrade attack.

Bluetooth security relies mostly on user awareness. In other words, the use of Bluetooth as well as the basic configuration of the terminal must be made with security in mind. Most of the incidents where data has been compromised on mobile phones have not been caused by a problem in the standard itself, but rather in the implementation quality. The E_0 stream cipher is fairly secure, although not flawless.

The 3G radio interface was not covered in this study. However, some security threats against end user terminals were covered. The key issue in this technology area is again security awareness. The major threats against 3G end user terminals seem not to be related to 3G technology at all. It can be said that anything coming through other interfaces the terminal might have (MMS, WLAN, Bluetooth, etc.) and user actions upon received messages and data are the most significant threat to the terminal itself.

RFID technology standards do not cover security mechanisms. This leads to the fact that several manufacturers have created their own proprietary solutions. These have to be evaluated and analysed in order to decide what is needed in an RFID system. A threat to ordinary people may arise with tags required by product logistics that are not disabled correctly.

Flash-OFDM is unfortunately a proprietary system and details of its security mechanisms are not publicly available. It is claimed to be secure and quite surely the algorithms that are used are good enough. However, even the WEP in WLAN was not insecure to begin with (there's nothing wrong with RC4), but it wasn't implemented in the right way.

References

[3GPP] http://srg.cs.uiuc.edu/MobilSec/, Last accessed Dec 12th 2006

[4GLAB] http://www.cwc.oulu.fi/4glab/, Last accessed Dec 12th 2006

[4GMF] http://4gmf.org, Last accessed Dec 12th 2006

[800-48] NIST Special Publication 800-48, Wireless Network Security 802.11, Bluetooth and Handheld Devices. Available at http://csrc.nist.gov/publications/nistpubs/ Last accessed Dec 12th 2006

[800-97] NIST Special Publication 800-97 (Draft): Guide to IEEE 802.11i: Establishing Robust Security Networks. Available at http://csrc.nist.gov/publications/nistpubs/ Last accessed Dec 12th 2006

[800-98] NIST Special Publication 800-98 (Draft): Guidance for Securing Radio Frequency Identification (RFID) Systems (Draft). Available at http://csrc.nist.gov/publications/nistpubs/ Last accessed Dec 12th 2006

[802.11-1999] IEEE Standard 802.11, 1999 Edition. Available at http://standards.ieee.org/getieee802/download/802.11-1999.pdf, Last accessed Dec 12th 2006

[802.11a] IEEE Standard 802.11a, 1999 Edition. Available at http://standards.ieee.org/getieee802/download/802.11a-1999.pdf Last accessed Dec 12th 2006

[802.11b] IEEE Standard 802.11b, 2001 Edition. Available at http://standards.ieee.org/getieee802/download/802.11b-1999_Cor1-2001.pdf Last accessed Dec 12th 2006

[802.11d] IEEE Standard 802.11d, 2001 Edition. Available at http://standards.ieee.org/getieee802/download/802.11d-2001.pdf, Last accessed Dec 12th 2006

[802.11e] IEEE Standard 802.11e, 2005 Edition. Available at http://standards.ieee.org/getieee802/download/802.11e-2005.pdf, Last accessed Dec 12th 2006

[802.11f] IEEE Standard 802.11f, 2003 Edition. Available at http://standards.ieee.org/getieee802/download/802.11F-2003.pdf, Last accessed Dec 12th 2006

[802.11g] IEEE Standard 802.11g, 2003 Edition. Available at http://standards.ieee.org/getieee802/download/802.11g-2003.pdf, Last accessed Dec 12th 2006

[802.11h] IEEE Standard 802.11h, 2003 Edition. Available at http://standards.ieee.org/getieee802/download/802.11h-2003.pdf, Last accessed Dec 12th 2006

[802-11i] IEEE Standard 802.11i, 2004 Edition. Available at http://standards.ieee.org/getieee802/download/802.11i-2004.pdf, Last accessed Dec 12th 2006

[802-11j] IEEE Standard 802.11j, 2004 Edition. Available at http://standards.ieee.org/getieee802/download/802.11j-2004.pdf, Last accessed Dec 12th 2006

[802.15.1] IEEE Standard 802.15.1, 2005 Edition. Available at http://standards.ieee.org/getieee802/download/802.15.1-2005.pdf, Last accessed Dec 12th 2006

[802.16] IEEE Standard 802.16, Available at, http://standards.ieee.org/getieee802/download/802.16-2004.pdf Last accessed Dec 12th 2006

[802.16a] IEEE Standard 802.16a

[802.16c] IEEE Standard 802.16c

[802.16d] IEEE Standard 802.16d, 2004 Edition. Available at http://standards.ieee.org/getieee802/download/802.16.2-2004.pdf Last accessed Dec 12th 2006

[802.16e] IEEE Standard 802.16e, 2005 Edition. Available at http://standards.ieee.org/getieee802/download/802.16e-2005.pdf Last accessed Dec 12th 2006

[AIM] http://www.aimglobal.org/technologies/rfid/what_is_rfid.asp Last accessed Dec 12th 2006

[ANDERSSON] Andersson, Ross, Security Engineering, Wiley 2001, pages 345-366

[BLUEBUG] BlueBug, an exploitation program for certain Bluetooth cell phones,
http://trifinite.org/trifinite_stuff_bluebug.html
Last accessed Dec 12th 2006

[BT_CYBER] Cybertrust research on Bluetooth:
http://www.cybertrust.com/media/white_papers/cybertrust_wp_blue.pdf
Last accessed Dec 12th 2006

[BT_FLAW] Eric Filiol, Zero-knowledge-like Proof of Cryptanalysis of Bluetooth Encryption,
2006, http://eprint.iacr.org/2006/303.ps
Last accessed Dec 12th 2006

[BT_ORG] https://www.bluetooth.org , Last accessed Dec 12th 2006

[BT_SIG] http://www.bluetooth.com/bluetooth, Last accessed Dec 12th 2006

[BT_SEC] http://www.bluetooth.com/Bluetooth/Learn/Security/
Last accessed Dec 12th 2006

[BT_SEC2] http://www.viruslist.com/en/analysis?pubid=181198286
Last accessed Dec 12th 2006

[BT_SF] SecurityFocus review on Bluetooth security:
http://www.securityfocus.com/infocus/1830, Last accessed Dec 12th 2006

[BT_SPEC] https://www.bluetooth.org/spec, Last accessed Dec 12th 2006

[CABIR] A virus that spreads via Bluetooth
http://www.f-secure.com/v-kuvaus/cabir.shtml, Last accessed Dec 12th 2006

[COMP] http://compnetworking.about.com/od/wirelesssecurity/tp/wifisecurity.htm
Last accessed Dec 12th 2006

[DARKREAD] http://www.darkreading.com/document.asp?doc_id=101749
Last accessed Dec 12th 2006

[DIGITODAY1] http://www.digitoday.fi/page.php?page_id=12&news_id=200621476
Last accessed Dec 12th 2006

[DIGITODAY2] http://www.digitoday.fi/page.php?page_id=14&news_id=200514326 Last accessed Dec 12th 2006

[EDNEY] Edney, J. and Arbaugh, W.. (2003). "Real 802.11 Security: Wi-Fi Protected Access and 802.11i". ISBN: 0-321-13620-9, 2004

[FIC47B] FICORA 47 B/2004 M, Regulation ON INFORMATION SECURITY OF TELECOMMUNICATIONS OPERATORS", 27 August 2004" http://www.ficora.fi/englanti/document/FICORA47B2004M.pdf Last accessed Dec 12th 2006

[FICORA] http://www.ficora.fi/englanti/tietoturva/svttelefaq.htm Last accessed Dec 12th 2006

[FICUSER] http://www.ficora.fi/mobiiliturva/english/8.html, Last accessed Dec 12th 2006

[GEER] http://acmqueue.com/modules.php?name=Content&pa=showpage&pid=436 Last accessed Dec 12th 2006

[GEHRMANN] Gehrmann, Christian. Bluetooth Security. Norwood, MA, USA: Artech House Incorporated, 2004

[GNURADIO] http://www.gnu.org/software/gnuradio, Last accessed Dec 12th 2006

[GREECE] http://online.wsj.com/article_email/SB115085571895085969-1MyQjAxMDE2NTIwMTgyNTE1Wj.html Last accessed Dec 12th 2006

[GSMA50] GSM Association, Doc. ref. IR.50, 2G/2.5G/3G Roaming v.3.3, April 2006

[JAKOBSSON] Jakobsson M. and Wetzel S., Security Weaknesses in Bluetooth, Proceedings of the Cryptographer's Track at the RSA Conference (CT-RSA 2001), LNCS 2020, Springer, 2001, http://www.cs.stevens.edu/~swetzel/publications/bluetooth.pdf Last accessed Dec 12th 2006

[KAASENBROOD] http://www.win.tue.nl/~ecss/internships/reports/EKaasenbrood2006.pdf Last accessed Dec 12th 2006

[KENTTÄLÄ] Jani Kenttälä, ”Wireless Local Area Network Security – Obscurity Through Security", http://www.ee.oulu.fi/research/ouspg/frontier/sota/whitepaper-wots/index.html, Last accessed Dec 12th 2006

[LASEC] http://lasecwww.epfl.ch/%7Egavoine/rfid/, Last accessed Dec 12th 2006

[MITF] http://www.mitf.org, Last accessed Dec 12th 2006

[NAP] http://www.nap.edu/books/0309084989/html/64.html, Last accessed Dec 12th 2006

[NEWS.COM] http://news.com.com/2100-1029_3-6088741.html Last accessed Dec 12th 2006

[PANOULU] http://www.panoulu.net/blog/archive/2006-11-02/langattomien_verkkojen_tietotu, Last accessed Dec 12th 2006

[PRACT] http://www.practicallynetworked.com/support/wireless_secure.htm Last accessed Dec 12th 2006

[RSA] http://www.rsasecurity.com/rsalabs/node.asp?id=2121 Last accessed Dec 12th 2006

[RSA_SEC] http://www.rsasecurity.com/rsalabs/node.asp?id=2115 Last accessed Dec 12th 2006

[SCHNEIER_BLOG] http://www.schneier.com/blog, Last accessed Dec 12th 2006

[T2308] Ahonen et al., Information security threats and solutions in the mobile world. The service developer's perspective, 2005. VTT, Espoo. 95 p. + app. 4 p. VTT Tiedotteita – Research Notes : 2308, http://virtual.vtt.fi/inf/pdf/tiedotteet/2005/T2308.pdf Last accessed Dec 12th 2006

[TIETOKONE] http://www.tietokone.fi/uutta/uutinen.asp?news_id=24420&tyyppi=1 Last accessed Dec 12th 2006

[TRIFINITE] Collection of Bluetooth vulnerability-related projects: http://trifinite.org/trifinite_stuff.html, Last accessed Dec 12th 2006

[UNINETT] http://forskningsnett.uninett.no/wla/wlanthreat.html Last accessed Dec 12th 2006

[WIKI] http://en.wikipedia.org/wiki, Last accessed Dec 12th 2006

[WIKI4G] http://en.wikipedia.org/wiki/4G, Last accessed Dec 12th 2006

[WIKIBT] http://en.wikipedia.org/wiki/Bluetooth, Last accessed Dec 12th 2006

[WIKIRFID] http://en.wikipedia.org/wiki/RFID, Last accessed Dec 12th 2006

[WIKIWIMAX] http://en.wikipedia.org/wiki/WiMAX, Last accessed Dec 12th 2006

[WIKIWLAN] http://en.wikipedia.org/wiki/Wireless_LAN, Last accessed Dec 12th 2006

[WIMAX] WiMAX official homepage, http://www.wimax.com,
Last accessed Dec 12th 2006

[WIMAXFAQ] http://www.wimax.com/education/faq/faq29, Last accessed Dec 12th 2006

[WIMAXFORUM] WiMAX Forum, http://www.wimaxforum.org/home/,
Last accessed Dec 12th 2006

[WIMAX_SEC] http://www.wimax.com/education/faq/faq27/?searchterm=security
Last accessed Dec 12th 2006

[WIMEDIA] http://www.wimedia.org, Last accessed Dec 12th 2006

[WIRE] http://en.wikipedia.org/wiki/Wireless_network, Last accessed Dec 12th 2006

[WLAN_SYM] http://www.symantec.com/specprog/threatreport/ent-whitepaper_symantec_internet_security_threat_report_x_09_2006.en-us.pdf
Last accessed Dec 12th 2006

Appendix A: WLAN Standards

Table 11. The most important and current WLAN standards

Standard	Details		
802.11 legacy [802.11-1999]	Ratified: 1997	Frequency:	Max. data rate:
	The original version of the standard. IR remains a part of the standard but has no actual implementations. A weakness of this original specification was that it offered so many choices that interoperability was challenging to realize. Legacy 802.11 was supplemented and popularized by 802.11b.		
802.11a [802.11a]	Ratified: 1999	Frequency:	Max data rate:
	The 802.11a amendment to the legacy standard uses the same core protocol as the original standard, and it uses OFDM modulation. It is not interoperable with 802.11b. Since the 2.4 GHz band is heavily used, using the 5 GHz band gives 802.11a the advantage of less interference. However, this frequency also brings disadvantages. It restricts the use of 802.11a to almost line of sight, necessitating the use of more access points. It also means that 802.11a cannot penetrate as far as 802.11b since it is absorbed more readily. 802.11a products started shipping in 2001, lagging behind 802.11b due to the slow availability of the needed 5 GHz components. 802.11a was not widely adopted overall primarily because the less-expensive 802.11b was already widely adopted. Manufacturers of 802.11a equipment responded to the lack of market success by improving the implementations, and by making technology that can use more than one 802.11 standard.		

802.11b [802.11b]	Ratified: 1999	Frequency:	Max data rate:
	802.11b products appeared on the market very quickly, since 802.11b is a direct extension of the DSSS (direct-sequence spread spectrum) modulation technique defined in the original standard. The 802.11b standard uses complementary code keying (CCK) as its modulation technique, which is a variation of CDMA. Chipsets and products were therefore easily upgraded to support the 802.11b standard. The increase in throughput (compared to the original standard) along with substantial price reductions led to the rapid acceptance of 802.11b as the definitive WLAN technology. 802.11b is usually used in a point-to-multipoint configuration, wherein an access point communicates via an omnidirectional antenna with one or more clients that are located in a coverage area around the access point. Typical indoor range is 30 m at 11 Mbit/s and 90 m at 1 Mbit/s. With high-gain external antennas, the protocol can also be used in fixed point-to-point arrangements, typically at ranges up to 8 kilometres although some report success at ranges up to 80-120 km where line of sight can be established. 802.11b cards can operate at 11 Mbit/s, but will scale back to 5.5, then 2, then 1 Mbit/s (Adaptive Rate Selection) if signal quality becomes an issue. Since the lower data rates use less complex and more redundant methods of encoding the data, they are less susceptible to corruption due to interference and signal attenuation. Proprietary extensions have been made to the 802.11b protocol in order to increase speed to 22, 33, and 44 Mbit/s, but they have not been endorsed by the IEEE.		
802.11g [802.11g]	Ratified: 2003	Frequency:	Max data rate:
	802.11g hardware works with 802.11b hardware. In older networks, however, the presence of an 802.11b participant significantly reduces the speed of an 802.11g network. The modulation scheme used in 802.11g is OFDM for data rates of 6 up to 54 Mbit/s, and it reverts to CCK for 5.5 and 11 Mbit/s and DBPSK/DQPSK+DSSS for 1 and 2 Mbit/s. Even though 802.11g operates in the same 2.4 GHz band as 802.11b, it can achieve higher data rates because of its similarities to 802.11a. The maximum range of 802.11g devices is slightly greater than that of 802.11b devices, but the range in which a client can achieve full data rate speed is much shorter than that of 802.11b. After the 802.11g standard was ratified, most of the dual-band 802.11a/b products became dual-band/tri-mode, supporting a, b, and g in a single mobile adapter card or AP. Despite its major acceptance, 802.11g suffers from the same interference as 802.11b in the already crowded 2.4 GHz range.		

Appendix B: WLAN communication step-by-step

Below we explain in more detail the basic principles and give some security notes for each of the different phases of WLAN communication.

1. Activating the WLAN radio link

An access point send “Beacon” and “Probe Response” management frames to advertise its IEEE 802.11i security policy. The STA uses these to identify an AP for a WLAN with which it wishes to communicate. The STA associates with the AP when the Beacons and Probe Responses present a choice.

→A rogue AP can send any kind of “Beacon” and “Probe Response” management frames to stations. Before that a rogue AP may sniff the SSID and MAC address of legitimate APs:

SECURITY: The used management frames are not information security protected. It is difficult to avoid this threat because SSID is transferred in clear text. Even WPA2-certified stations may lose time and resources due to useless communication with masquerading access points.

→By the end of the phase, the STA and AP have agreed on a security policy that specifies data confidentiality and integrity protocols for protecting data traffic:

SECURITY: At this phase, a station cannot verify for sure whether it negotiated with the intended or a rogue access point. Note that CCMP and IEEE 802.1X with EAP are considered to be a secure communication policy.

2. Preparation phase for a cryptographically secure WLAN link

The STA and the WLAN network prove their identities to each other and generate and distribute the cryptographic keys.

→The security configuration setting in the access point enforces the authentication protocol and cryptographic key establishment protocols to be used with this wireless link.

SECURITY:

- In enterprise deployments, the AP configuration should be set to enforce IEEE802.1X with mutual EAP authentication based on the TLS protocol. The document [800-97] summarises the security of seven EAP methods. The EAP methods currently regarded as fairly secure are based on the TLS protocol: EAP-TLS, EAP-TTLS, PEAP and EAP-FAST. Before deployment, the EAP methods should be carefully analysed from security viewpoint.
    - NOTE: The communication between AP and AS must be very well secured (e.g. with IPsec VPN with robust mutual authentication and the use of FIPS approved algorithms)
- In small enterprises and home deployments (and in ad hoc networks), where an authentication server may not be available, a secure AP configuration may enforce pre-shared-key based authentication using AES and SHA-1. WEP-based shared key authentication is insecure.
- A particular station’s user data communication is blocked in the AP until this phase has passed successfully (IEEE 802.1X port-based access control).

→The cryptographic key generation handshakes are made (a 4-Way Handshake). It uses message encryption and integrity checking, using one of two confidentiality and integrity algorithms.

SECURITY:

- For key generation, AES Key Wrap with HMAC-SHA-1-128 (FIPS-approved) should be enforced in AP security settings instead of RC4 encryption with HMAC-MD5 (legacy hardware case).
  - Secure key wrap: □ 256-bit root cryptographic key is used to formulate a (256-bit) key derivation key. A key derivation key along with the MAC address of the STA and AP and random numbers are used as input in the HMAC derivation of a (384-bit in CCMP) Pairwise Transient Key (PTK). All this together protects against session hijacking and impersonation. The PTK consists of a “key integrity confirmation key” (128-bit), a “key confidentiality key” (128-bit) and an actual “user data protection key” (128-bit in CCMP).
- CCMP selection as the user data ciphering suite in the security settings will ensure the use of FIPS-approved (secure) algorithms.

3. Secure WLAN link

Secure data transfer occurs between the STA and the AP.

→The data transferred over the WLAN link is protected for confidentiality, message integrity & authenticity and replay. A security association exists at both ends of the wireless link which enables the functioning of selected cryptographic protocols.

SECURITY:

- STA and AP protect the user data (e.g. IP packets), utilising the security policy and cryptographic keys established during the earlier phases. If the security settings were weak, the security protection is also weak.
- Protected WLAN data transfer occurs only between STA and AP. One needs to consider protecting the user data during the rest of its transit, or to applying end-to-end protection (but this is out of scope of WLAN network security).

4. Disconnecting the WLAN link

The secure link is torn down and restored to the original state.

→During this phase, the security associations (cryptographic keys, state, etc.) are deleted from AP and STA. The link will be terminated if (not definite):
- Radio communication is lost
- Established keys expire
- Key generation fails
- Device is turned off
- Security policy indicates a termination

SECURITY: In some implementations, there may be vulnerabilities in secure link termination criteria. Certain attacks could lead to implications that tear the secure link down without user intention. For example, jamming or frame modification might lead to link release. However, the IEEE 802.11w Task Group is considering how to secure connection termination. Completion of this IEEE 802.11w standard is targeted for 2008.

Appendix C: WiMAX standards

Table 12. WiMAX standards

Standard	Details		
802.16 **[802.16]**	Ratified: 2001	Frequency:	Max. data rate:
	The original WiMAX standard. Since line-of-sight (LOS) is a primary issue in this frequency range, multipath was addressed with OFDM techniques.		
802.16a [802.16a]	Ratified: 2003	Frequency:	Max data rate:
	The IEEE 802.16a amendment to the original standard enhanced MAC modifications and covered additional PHY layer specifications for 2-11 GHz. It also incorporated non-line-of-sight (NLOS) capability and improved quality of service (QOS) features. Support for both time division duplexing (TDD) and frequency division duplexing (FDD) were incorporated. Transmission protocols such as Ethernet, ATM or IP are supported.		
802.16c [802.16c]	Ratified: 2002	Frequency:	Max data rate:
	The 802.16c standard update dealt mostly with updates in the 10 GHz to 66 GHz range. It also addressed issues such as performance evaluation, testing and detailed system profiling. Mandatory and optional features were defined to ensure interoperability.		
802.16d [802.16d]	Ratified: 2004	Frequency:	Max data rate:
	The 802.16d, or fixed WiMAX. All of the previous standards were rolled into 802.16d. The technology supports both TDD and FDD. The system profile chosen is OFDM 256-FFT. Some of the enhancements in this version are support for concatenation of both protocol data units (PDU) and service data units (SDU) which reduces the MAC overhead. The technology improves QOS, particularly with very large SDUs. One clear improvement is support for multiple polling methodologies. The MAC facilitates polling individually or in groups. It can access allocated bandwidth to make requests, or signal that it needs polling. It can also piggyback polling requests over other traffic, reducing packet collisions and system overhead.		

<table>
<tr><td rowspan="2"><b>802.16e [802.16e]</b></td><td>Ratified: 2005</td><td>Frequency:</td><td>Max data rate:</td></tr>
<tr><td colspan="3">802.16e, or mobile WiMAX, conserves the technical updates of 802.16d while adding support for mobility. It uses scalable ODFM, which brings benefits in terms of coverage, self installation, power consumption, frequency re-use and bandwidth efficiency. The IEEE 802.20 working group is expected to yield a mobility technology complementary to 802.16e, not a competing one. For example, people walking and riding in cars may use 802.16e, while users in high-speed trains might require 802.20.</td></tr>
</table>

Appendix D: RFID standards

Table 13. Weak intrinsic information security in RFID standards, see [800-98] for reference

RFID standard (application)	Nom. Range (m)	Data	Confidentiality	Integrity
EPC Class-0, Class-1 (supply chain)	3	R/W	None in standard. Cl-1 Gen-2: One-time pad stream cipher.	Parity bit. CRC.
ISO/IEC 18000-2 (item management)	< 0.01	R/W	No encryption or authentication.	CRC. Optional lockable ID code.
ISO/IEC 18000-3 (item management)	< 2	R/W	No encryption or authentication. 48-bit password protection on *read* commands. Quiet mode in tag	CRC. Mode 2: 48-bit pw on *write*.
ISO/IEC 11784-11785 (animal tracking)	< 0.01	ID	No encryption or authentication. Quiet mode.	Retagging counter. CRC.
ISO/IEC 10536 (contactless smart cards)	< 2	R/W	Masked reader-to-tag communications. Quiet mode.	CRC
ISO/IEC 14443 (contactless smart cards)	≈ 0.07 to 0.15	ID	No encryption or authentication. Encryption often available in application level.	CRC
ISO/IEC 15693 (vicinity smart cards)	1.5	R/W	No encryption or authentication.	Optional protection on *write.* Error checking

Lisätietoja:

LUOTI-ohjelman internet-sivut
www.luoti.fi

Liikenne- ja viestintäministeriön internet-sivut
www.mintc.fi/paattyneet hankkeet

www.luoti.fi