NET Institute*

www.NETinst.org

Working Paper #03-09

October 2003

The Delft UMTS Testbed and End-user Security Features

by

Dr. Carleen Maitland

School of Information Sciences and Technology, The Pennsylvania State University

* The Networks, Electronic Commerce, and Telecommunications ("NET") Institute, http://www.NETinst.org, is a non-profit institution devoted to research on network industries, electronic commerce, telecommunications, the Internet, "virtual networks" comprised of computers that share the same technical standard or operating system, and on network issues in general.

The Delft UMTS Testbed and End-user Security features

Prepared by:

Dr. Carleen Maitland[1]
Ankur Tarnacha
Annemijn van Gorp
J. Rudi Westerveld

For the NET Institute
October 13th, 2003

[1]Assistant Professor, School of Information Sciences and Technology, The Pennsylvania State University, 3A Thomas Bldg., University Park, PA 16802. Email: cmaitland@ist.psu.edu; Phone: 1-814-863-0640.

1. Introduction

The advent of the UMTS mobile network technology and recent advances in wireless LANs create new possibilities for network and Internet access. This in turn may provide the basis for a range of new services, which itself will change the roles of existing mobile firms and new entrants. A significant challenge for the industry will be safeguarding user data and protecting network and end-user equipment from malicious attacks. These problems are currently the concern of desktop computer users and network administrators, who are struggling to keep ahead of the latest security threats. With the distributed nature of mobile devices it is likely that the management of network and end-user security will only become more complicated.

To better understand this challenge this research has investigated the security features of a UMTS network testbed as well as the possibilities of integration with WLANs at Delft University of Technology in the Netherlands. In particular this research addresses the following questions from a user perspective:

1. What security features are theoretically available in UMTS handsets and are likely to be offered by UMTS network operators?
2. What factors are likely to influence end user acceptance of these features?
3. What role does security play in UMTS/ WLAN integration?

In addition to addressing these questions this research also provided an opportunity to observe certain aspects of the relationship between the network operator and equipment manufacturer and handset providers, as well as the role of standards in the diffusion of a new technology. In what follows we first describe the Delft UMTS testbed. This description provides the context of the research as well as its limitations in terms of generalizability of results. This is followed by our findings, which are divided into security, industry relations and standards, and handset issues. Section 4 presents our conclusions and the report concludes with a series of appendices, which contain detailed information about UMTS standards and security features, WLAN technologies and WLAN & cellular network integration.

2. Description UMTS Testbed

The UMTS testbed at Delft University of Technology is a project of T-Mobile in the Netherlands. The university educates roughly 15,000 students and is located approximately 1 hour south of Amsterdam. The goal of the testbed is to serve as a platform for research on application development and use, rather than as a basis for network performance evaluation. As a pre-commercial implementation the testbed network represents a particular incarnation of the UMTS technology and as such presents a platform with unique features and functions. These features and functions are the result of a long process of standards development, hard- and software design, and implementation. Hence we perceive the UMTS technology that we observe as existing at five levels that range from the theoretical to that experienced by the end user:

1. UMTS standard (3GPP.org)
2. Interpretation by various network equipment manufacturers
3. Implementation by the operators
4. Testbed
5. End-user (handset level)

By taking into account the constraints that each of these levels presents, our analysis is able to focus on the realities of UMTS security features, as opposed to what is merely theoretically or technically feasible. The extent to which the features and functions are those that will be available in a commercial offering is unclear.

The testbed UMTS network (number 4 on the list above) was built to be partially integrated into the existing T-Mobile GSM network. In particular the UMTS network consists of the parts as shown in the blue box in Figure 1, thus of the components 'Node B' and 'RNC'[2]. The components (yellow 'boxes') shown above the UMTS network constitute the GSM network, to which the UMTS testbed has not been connected. The UMTS testbed is however linked to the components that provide GPRS capabilities (components 'SGSN' (Serving GPRS Support Node) and 'GGSN' (Gateway GPRS Support Node), which in turn are linked to the Internet (component 'IP'). The way this network has been set up means that from the testbed in Delft no phone calls can be made to the GSM network (and also not to the fixed PSTN network as this is also linked to the GSM network) but data transfer is possible to and from the Internet, and GPRS could be used, provided the mobile phone that is used supports an appropriate browser. As the WAP gateway is also located within the GSM network, WAP services also cannot be used.

[2] The RNC (Radio Network Controller) and Node B together constitute the UTRAN (UMTS Terrestrial Radio Access Network). The UTRAN provides functions that are related to access, radio mobility and resource. The Node B provides the physical resource to the user equipment, and information on uplink and downlink is routed towards the RNC. (See http://www.mobileguru.co.uk/Mobile_Technology_globe.html)

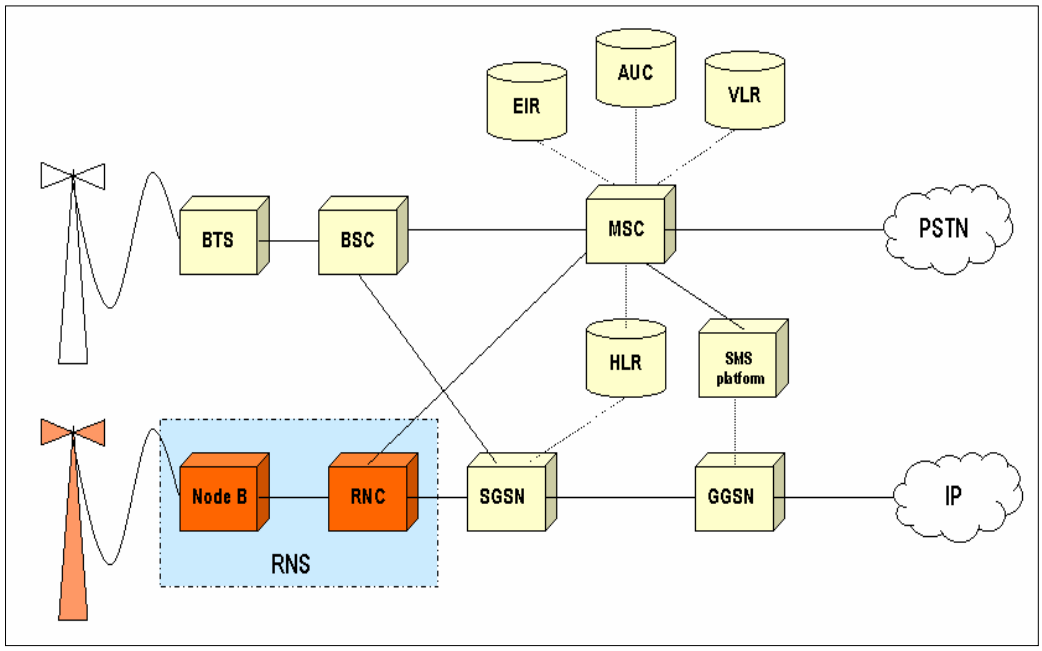

Figure 1 – Cellular Network consisting of GSM and UMTS connected to Internet and PSTN

Arrangements for the network and planning occurred during the fall of 2002 and the spring of 2003 and the network was operational in June of 2003. This was later than originally planned and thus the testbed is scheduled to remain operational until the spring of 2004, instead of through the end of 2003 as was originally planned. The operation of the testbed network benefited from the experience of T-Mobile staff with their own testbed in their local office. During this process of planning for the UMTS testbed Delft University of Technology was also planning the rollout of WLAN service by the end of 2002. Despite having equipment in place WLAN access was available only in August 2003. The delay in the availability of the network contributed to a delay in the delivery of WLAN-enabled PDAs, thus hindering testing of WLAN/UMTS integration.

For the UMTS testbed T-Mobile deployed Nokia network equipment. In accordance with our perception of the technology presented above, we attempted to ascertain which version of the UMTS standard was the basis for the testbed network equipment however we were unable to gather this information from either T-Mobile or Nokia. Nokia was also the manufacturer of one of the handsets for the testbed. The research projects associated with the testbed all faced significant delays in the delivery of handsets. Although 50 handsets were supposed to arrive in April, May and then June as of this writing in October only a few handsets have been delivered. We were able to examine two handsets, a Nokia 6650 and the Siemens U10. This report and the findings presented below are based on observations and experiences of researchers involved in both the planning and the first four months (June – October) of operations of the testbed.

3. Findings from the UMTS Testbed

These findings are the result of experiences and observations gained from the testbed described above informed by background material. Although we cannot accurately assess the extent to which the testbed environment will be similar to a commercial rollout, we believe that the following observations do reflect trends beyond the idiosyncrasies of the Delft testbed. In what follows we present our findings, grouped into 3 categories, security, industry relations and standards and UMTS handsets.

3.1 Security

End-user perspectives of security are shaped by first the availability of security features and subsequently by their ease of use.

1. *UMTS security is not a primary concern among network equipment manufacturers or operators.*

   This lack of interest is likely driven by the lack of an urgent need, especially since the 2G and 2.5G networks have been relatively free of viruses. Thus, security has been deemed an issue to be addressed when the technology is more mature. Furthermore, given the complexity of UMTS technology, operators are concerned with more fundamental aspects of network performance such as reliability and coverage. Only after a stable network is achieved will engineers be able to assess features such as security.

   This attitude is not only present in the implementation stage of UMTS deployment, but is also present in the standard setting process as well. The UMTS standards are developed by the 3GPP organization, which represents a wide range of standards bodies including ETSI, ARIB and TTC in addition to market partners such as the UMTS Forum. The standard currently has 3 versions, release '99, release 4 and release 5. A new release 6 is expected to be frozen in late 2003 [24]. The current network setup at the Delft University is believed to be based on 'Release '99'. Release 99 was first frozen in March 2000. Like all releases Release 99 had many "change requests" filed after the specification freeze date. These "change requests" were required to either clarify a frozen feature or to add a new feature. Every "change request" adds a new version to the frozen release. Although this process is valuable for sharing knowledge and experience, it does complicate matters. For details refer to sections 1.1 and 1.2 of appendix A.

   Defining the security features for UMTS occurred in this context. The process began by assessing the security weaknesses of GSM and GPRS, which are the foundation for the UMTS standards. These UMTS security requirements were identified well in advance of the freeze and are specified in 3GPP TS 21.133 [47]. Despite this advance work the security section of Release '99 was

established only one week before the freeze date (see 3GPP TS 33.102) [48]. Given the delayed attention given to security there is yet work to be done on this section of the standard. For further details refer to appendix A.

2. *End user perspectives of security are likely to be different from those of hard- and software designers.*

   With UMTS mobile services end user security concerns are likely to be the practical issues similar to those in GSM and GPRS, namely protecting the device, the user account, privacy and data protection. These are however different from the perspectives of designers who see security as associated with applications. The result may be a mismatch between how end users approach and use security features and how they are presented on the mobile device. See section 1.2 of appendix A for a description of how designers (standards bodies) perceive security features.

3. *The increased security requirements created by the increased functionality of the UMTS technology has resulted in a greater number of passwords and PIN codes for users.*

   The end-user of the UMTS handsets and services would have to deal with an increased number of codes and passwords to benefit from the security features provided in the 3G setup. For example Nokia 6650 handset with the SIM card provides the user with various codes and passwords which include a *Security code* which can be used to change the access and security level of the phone, a *PIN code* which is provided for the SIM card to protect the SIM card against unauthorized use, a *PIN2 code* which is also provided for the SIM card to protect certain functions like charging unit counters, a *PUK code* which is provided for the SIM card to unlock the SIM if incorrect PIN code is used for 3 successive times, a *PUK2 code* which is used to unlock the SIM if incorrect PIN2 code is used for 3 successive times, a *Barring password* which is used to protect the call barring security feature, a *Module pin* which is supplied with the SIM card to access the information in the security module, a *Signing pin* which is supplied with the SIM card to sign data with digital signatures, and a *Wallet code* which is needed for protecting the wallet services like credit card information. So many security codes for a security minded end-user might cause confusion, problems and eventual limited use of 3G security features.

4. *All UMTS security features may not be universally available as availability of some features is at the discretion of the network operator.*

   The operator through offering particular network services (such as call barring) and by influencing the features of the SIM card will shape the security features available to the end user. Examples of codes that may or may not be available depending on the SIM card are the PIN2, PUK and PUK2 codes.

5. *When a WLAN provides access to an existing organizational network, security issues are likely to limit UMTS/WLAN integration.*

   WLANs have been deployed in public spaces such as coffee houses and airports and in private residences with the primary purpose of providing Internet access. In these scenarios WLAN/UMTS integration faces a more limited range of security issues. However, where WLAN deployment serves the dual purpose of providing Internet access as well as access to an existing organizational network, security concerns pose a bigger problem to WLAN/UMTS integration. Security issues can hinder WLAN deployment by limiting first the geographical range of the deployment (limited to one floor of a building for example), second the speed of deployment (as policies or mechanisms for security are designed), and third the range of persons allowed to access the network. This is particularly relevant for systems deployed in public buildings where both passers-by and those who work there would like to access the WLAN.

   The security issues related specifically to WLAN are described in greater detail in appendix B, section 3. For a discussion on WLAN/UMTS integration and the possibilities of using SIM card access to resolve security issues in an integrated environment see appendix C.

3.2. Industry relations and standards

The availability (or lack thereof) of security features in UMTS networks will be determined by the broader context of industry relations and the standard setting and adoption process.

6. *Network operators and equipment manufacturers must work closely together as the operator relies heavily on the equipment manufacturer for technical knowledge.*

   The operator and equipment manufacturer must work together closely as the operator relies on the technological knowledge of the equipment manufacturer. This division of labor enables operators to focus more resources on areas such as customer service however it increases their dependence on the equipment manufacturers. This reliance may leave operators unaware of the precise configurations of their networks and unaware of the implications for service characteristics, including security.

7. *Given the complicated nature of the standardization process, it is unclear which version of the standard will serve as the basis of commercial implementations and this may result in a variety of versions being deployed.*

   The standards process involves a wide variety of organizations and takes place over the course of several years. In an effort to integrate knowledge and experience the standard is continually updated through a process of submitting

'change requests'. These 'change requests' are required to either clarify a frozen feature in the release or to add/remove an implementation mechanism/approach. Thus, after the release is frozen implementation guidelines may be updated.

Given the time-to-market pressures faced by the industry, the choice of standard release version and implementation guideline for equipment design thus becomes as much a strategic issue as a technical one. For details concerning the standards update process refer to Section 1.1 and 1.2 of appendix A.

3.3 UMTS Handsets

Users' experience of security features will also be influenced by the broader experience with the UMTS handset.

8. *Although generalized descriptions of new UMTS features can be identified, it appears that not all UMTS handsets will contain the same features.*

   The mobile devices have increasingly targeted the success of the Internet. A move towards mobile Internet browsers is on the horizon with 3G handsets. These changes have been driven by the availability of java applications and the limited number of WAP gateways compared to the Internet. For more information about UMTS handsets and WAP, see appendix A, section 2.

   The handset providers have through the following mechanisms focused on increasing the number of features and improving performance of UMTS phones:

   - Implementation of a device operating system resulting from a strategic choice of a mobile operating system provider.
   - Implementation of device applications like anti-virus software from a strategic choice of application providers.
   - Implementation of security features based on standards like WAP 2.0
   - Multiple security codes for SIM and device security
   - Bluetooth 1.1 compatibility

   Such features have changed the UMTS phones, which in general now include a high resolution color screen, increased Internet access, increased encryption processing and in turn a heavier battery to support such rich features. For details refer to section 1.5 of appendix A.

   The UMTS handsets examined in the testbed differed predominantly in their browsers (WAP vs. Internet) and support for viewing streaming video; however, the next versions of the phones are all likely to include browsers capable of Internet access.

9. *The ability to easily use the phone as a modem to provide an Internet connection to a PDA via Bluetooth is an example of the trend toward greater connectivity between devices, which has security implications.*

   The UMTS phones in general have explored technologies like Bluetooth which has given the users flexibility of using the phone as a modem. This process of using the phone as a modem via a Bluetooth connection to a computer or a PDA is more or less on the lines of 'plug n play'. The ease of using the phone as a modem may increase user choice of interface (computer, PDA or phone). However, this increased connectivity increases the number of ways in which the mobile handset can be compromised. Although the technical feasibility of such connections is not new, the increased ease of use is likely to increase the frequency of such connections.

10. *Despite greater functionalities that are making mobile phones increasingly similar to PDAs and computers, the operating system vendor is still not transparent.*

    The 3G mobile device manufacturers have in general outsourced the operating system requirements of the mobile device to specific mobile operating system providers. This we believe would give the handset manufacturer the freedom to provide better end-user security (especially in terms of virus control as most of the virus attacks and security breaches in the computer and PDA market are operating system and application specific) through their choice of operating system vendor. However, operating system vendor relationships with other relevant firms (for example Microsoft or Intel) may complicate this choice. For details refer to section 1.5.1 and 1.5.2 of appendix A.

11. *Handset availability continues to be a problem.*

    Operators continue to have a lack of control over the availability of handsets. Even in the case where handset providers are in the same organization as the network equipment providers, this relation appears to provide little leverage in terms of the availability of handsets. As handsets become increasingly complex the likelihood of initial incompatibility with network equipment appears more likely and hence there may be a greater lag time between delivery and actual availability for use. For example, in the testbed handsets required software upgrades to be compatible with the network equipment.

4. Conclusions

This research has provided a glimpse at the possibilities and challenges for UMTS through observations of a UMTS network testbed in a university context. Through observations of the operations of this testbed and background research it is clear that the increased functionality of

UMTS services has expanded the range of security features available to end-users. However, the development of some of these features is still underway and it is as yet unclear which features will be offered by network operators. Furthermore, the number of PIN and passwords required to use all of the security features available on pre-commercial handsets may pose a challenge to end-users. Although a test of the compatibility of WLAN and UMTS security features was not possible, the problems encountered in merely setting up the networks for such an investigation points to first the diversity of environments within which UMTS/WLAN integration will be implemented and how the context of those environments, whether a public access point or private organization, will influence the degree to which security concerns could limit such use.

The development of UMTS security will occur in the broader context of new network technology deployment as well as an increased awareness of the importance of security. In general, deployment of a new network technology such as UMTS faces many hurdles from standardization of network and terminal equipment to its implementation. In this context where reliable network operation, and the transfer of any data is a challenge, security concerns will naturally be secondary. In the past this has been accepted practice as there is usually a time lag between new technology introduction and security problems. However, given increases in computer network security breaches it is likely the time window between new technology introduction and security breaches will become smaller and this could pose a challenge for UMTS. Furthermore, in an era of rapid technical development and where investors in 3G technologies fear competition from 4G, it seems reasonable to question whether or not time and resources will ever be allocated to focus on security concerns.

This in turn raises the question of which market players should be responsible for insuring end users are provided secure services. Currently a 'buyer beware' orientation to security is the norm and in the desktop world this has proven a costly strategy for private users and organizations. Given the nature of the division of labor in the mobile industry, with operators focused on managing customer relations and technical expertise residing with equipment manufacturers, it would be risky to place the burden of security entirely on the operator. The decisions made by equipment manufacturers, of both network and handset components, at the design phase play a significant role in defining the nature of security features and functions. Furthermore, these firms also play a role in implementation. At the network level, equipment manufacturers work hand-in-hand with operators to configure network equipment and hence will influence which functions are available. Handset manufacturers, by making decisions about menus and the ways in which security features are presented to end-users, also have an important role to play in whether or not security features are actually used.

Appendix A - UMTS standard and security features

1. Introduction

The UMTS standards are developed by the 3GPP organization, which represents a wide range of standards bodies including ETSI, ARIB and TTC in addition to market partners such as the UMTS Forum. The original scope of 3GPP was to produce globally applicable Technical Specifications (TS) and Technical Reports (TR) for a 3rd Generation Mobile System based on evolved GSM core networks and the radio access technologies that they support (i.e., Universal Terrestrial Radio Access (UTRA)). The scope was subsequently changed to include the maintenance and development of the Global System for Mobile communication (GSM) Technical Specifications and Technical Reports including evolved radio access technologies (e.g. General Packet Radio Service (GPRS) and Enhanced Data rates for GSM Evolution (EDGE)). To meet new market requirements, 3GPP specifications are continually being enhanced with new features. In order to provide developers with a stable platform for implementation while at the same time allowing the addition of new features, the 3GPP uses a system of parallel 'releases', The standard currently has 3 parallel releases, 'release 99', 'release 4' and 'release 5'. A new 'release 6' is expected to be frozen in late 2003 [24].

1.1. Navigating the UMTS standard and the specification series

The UMTS standard is broken into series, which reflect both the topic being addressed by the part of the standard as well as the platform to which it applies (3G, GSM, or Both).[49]. All 3G and GSM specifications have a 3GPP specification number consisting of 4 or 5 digits. (E.g.: 09.02 or 29.002). The first two digits define the series. They are followed by 2 digits for the 01 to 13 series or 3 digits for the 21 to 55 series. The issues and subjects dealt with in specific series are listed in the Table 1 below [49].

Table 1: Subjects handled by specification series
Source: www.3gpp.org

Subject of specification series	3G/GSM Release 99 and later	GSM only (Release 4 and later)	GSM only (before Release 4)
General information *(long defunct)*			00 series
Requirements	21 series	41 series	01 series
Service aspects	22 series	42 series	02 series
Technical realization	23 series	43 series	03 series
Signalling protocols (user equipment to network)	24 series	44 series	04 series
Radio aspects	25 series	45 series	05 series
CODECs	26 series	46 series	06 series
Data	27 series	47 series (none exists)	07 series
Signalling protocols (RSS-CN)	28 series	48 series	08 series
Signalling protocols (intra-fixed-	29 series	49 series	09 series

network)			
Programme management	30 series	50 series	10 series
User Identity Module (SIM / USIM)	31 series	51 series	11 series
O&M	32 series	52 series	12 series
Access requirements and test specifications		13 series (1)	13 series (1)
Security aspects	33 series	(2)	(2)
Test specifications	34 series	(2)	*11 series*
Security algorithms (3)	35 series	55 series	(4)

Note (1): The 13 series GSM specifications relate to European-Union-specific regulatory standards. On the closure of ETSI TC SMG, responsibility for these specifications was transferred to ETSI TC MSG, (Mobile Specification Group) and they do not appear on the 3GPP file server.
Note (2): The specifications of these aspects are spread throughout several series.
Note (3): Algorithms may be subject to export licensing conditions. See the relevant 3GPP page. See also the relevant ETSI pages.
Note (4): The original GSM algorithms are not published and are controlled by the GSM Association.

The term '3G' in the above table means a 3GPP system using a UTRAN (Universal Terrestrial Radio Access Network). UTRAN is a conceptual term identifying that part of a UMTS network, which consists of one or more RNC (Radio Network Controller) and one or more Node B. The term 'GSM' in the above table means a 3GPP system using a GERAN (GSM Edge Radio Access Network). The GERAN supporting the EDGE (Enhanced Data rates for Global Evolution) modulation technique has been specified to connect interfaces to the core network. The architecture allows two BSS (Base Station Subsystem) to be connected to each other. Thus 'GSM' includes GPRS and EDGE features. The 'GSM' term here particularly describes the 3G system with backward compatibility to the 2G GSM and 2.5G EDGE.

A specification in the 21 to 35 series may apply either to 3G only or to GSM *and* 3G. A clue lies in the third digit, where a '0' indicates that it applies to both systems. For example, 29.002 applies to 3G and GSM systems whereas 25.101 and 25.201 apply only to 3G. All other series apply only to GSM systems. However, as the specification numbering space has been used up, this guide is more frequently broken, and it is necessary to examine the information page for each specification or to check the lists in standardization documents 01.01 / 41.101 (GSM) and 21.101 (3G) for the definitive specification sets for each system and each Release.

The 3GPP Specifications are stored on the file server as zipped MS-Word files. The filenames have the following structure:

SM[-P[-Q]]-V.zip

Where the character fields have the following significance:
S = Series number - 2 characters (see Table 1 above)
M = Mantissa (the part of the spec number after the series number) - 2 or 3 characters (see above)

P = Optional part number - 1 or 2 digits if present
Q = Optional sub-part number - 1 or 2 digits if present
V = Version number, without separating dots - 3 digits

So for example:

- 21900-320.zip is 3GPP TR 21.900 version 3.2.0
- 0408-6g0.zip is 3GPP TS 04.08 version 6.16.0
- 32111-4-410 is 3GPP TS 32.111 part 4 version 4.1.0
- 29998-04-1-100 is 3GPP TS 29.998 part 4 sub-part 1 version 1.0.0

Further information about the Specification numbering scheme, 3GPP releases, phases, file naming conventions, and other related information can be found in 3GPP TR 21.900 "Technical Specification Group working methods" [58]. The full title, specification number and latest version number for every specification can be found in the status list [50] and more information about terms such as Release 99 and Release 4 can be found on the release and phases page [51] page.

1.2. The UMTS standard and security

In general the specification series we are interested in are identified as follows:

- **01 and 21-series:** Requirements specifications for GSM only and 3G/GSM network and equipment providers, respectively
  Example:

TS	21.101	3rd Generation mobile system Release 1999 Specifications
TS	21.111	USIM and IC card requirements
TS	21.133	3G security; Security threats and requirements

- **33 series:** Security aspects for GSM/3G network and equipment providers
  Example:

TS	33.102	3G security; Security architecture
TS	33.103	3G security; Integration guidelines
TS	33.105	Cryptographic Algorithm requirements
TS	33.106	Lawful interception requirements
TS	33.107	3G security; Lawful interception architecture and functions
TS	33.120	Security Objectives and Principles
TR	33.901	Criteria for cryptographic Algorithm design process
TR	33.902	Formal Analysis of the 3G Authentication Protocol
TR	33.908	3G Security; General report on the design, specification and evaluation of 3GPP standard confidentiality and integrity algorithms

The specifications in 01 and 21 series are often transient and contain requirements towards other specifications. For example TS 01.01 and TS 21.101 have a list of all the documents which define the complete 3G standard for GSM only and 3G/GSM network and equipment providers. These may become obsolete when technical solutions have been fully specified; they could then, e.g., be replaced by reports describing the performance of the system, they could be deleted without replacement or be kept for historical reasons but turned into background material. When

found necessary and appropriate, the transient or permanent nature of a requirement specification may be expressed in the scope section of the document.

A security feature is a service capability that meets one or several security requirements. The complete set of security features, address the security requirements as they are defined in TS 21.133 (3G Security: Threats and Requirements). The implementation of these security objectives and principles is described in TS 33.120. The current network equipment security standards at the university of Delft are based on 'Release '99' [3GPP TS 33.102; V3.13.0 (2002-12), titled 3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects; 3G Security; Security architecture (release 1999)] [25].

In general the UMTS standards by 3GPP (all releases) divides security features into 5 levels [26]:

1. Network access security
2. Network domain security
3. User domain security
4. Application security
5. Security visibility and configurability

1.3. Defining end-user security issues

Security refers to the range of administrative, technical and physical mechanisms that aim to preserve privacy and confidentiality. Information security in general has three basic guidelines: [52]

- **Confidentiality**
  Confidentiality refers to limiting information access and disclosure to the set of authorized users, and preventing access or disclosure to unauthorized ones. Authentication methods that identify a system's users and access control mechanisms that define each user's access underpin the goal of confidentiality. (Confidentiality is related to the broader concept of privacy.).
- **Integrity**
  Integrity refers to the trustworthiness of information resources. It includes the concept of 'data integrity' which means that data has not been changed inappropriately, whether by accident or by deliberate maligning activity. It also includes 'origin' or 'source integrity' which means that the data actually came from the person or entity the user thinks it did, rather than an imposter. Integrity can even include the notion that the person or entity in question entered the right information i.e., information that reflected the actual circumstances (in statistics, this is the concept of 'validity') and that under the same circumstances would generate identical data (what statisticians call 'reliability'). On a more restrictive view, however, integrity of an information system includes only preservation without corruption of whatever was transmitted or entered into the system, right or wrong.
- **Availability**
  Availability refers, to the availability of information resources. An information system that is not available when you need it is at least as bad as none at all. It may be much

worse, depending on how reliant the organization has become on a functioning computer and communications infrastructure. Availability, like other aspects of security, may be affected by purely technical issues (e.g., a malfunctioning part of a computer or communications device), natural phenomena (e.g., wind or water), or human causes (accidental or deliberate).

1.4. Mobile end-user security concerns

The mobile end-user security guidelines are similar to general end-user information security guidelines described above. The challenge for adhering to these guidelines lies in the difficulty to administer the wireless medium and unrestrained mobility of the user. Security concerns in the mobile end-user domain include but are not limited to:

- Cellular cloning
- Cellular eavesdropping and Packet sniffing
- Email borne viruses, spoofing
- Trojan horse programs, Back door and remote administration programs, Mobile code (Java/JavaScript/ActiveX)
- Denial of service
- Physical Theft
- Memory failure

There was a time in the early 1990s when concerns about 'Cellular cloning' and 'Cellular eavesdropping' were on everybody's lips and in every newspaper and news magazine. The advent of digital phones and digital network systems in recent years has sharply curtailed the ability of criminals to steal cell phone identification codes (Cellular cloning), and the ability to snoop the airwaves and listen to others cellular conversations (Cellular eavesdropping).

Cloning and Eavesdropping haven not disappeared, even though the incidences have declined dramatically. It is still possible to 'clone' someone's cell phone I.D. and it's still possible to listen in on cellular conversations, and every cell phone user should be aware of the dangers and how to minimize them. Analog phones were susceptible to cloning and eavesdropping. Anyone with a scanner could tune in and listen for transmissions. Today's digital cell phones are equipped with a unique electronic 'Fingerprint' which is transmitted to the cell tower of their provider where it is read and identified [59]. Nowadays transmissions are digital and require decoding, help in eliminating eavesdropping. Unfortunately, digital phones and digital systems still rely on analog towers and networks, especially during peak call times when the systems are overloaded, or when calls are being transferred to other companies' networks (roaming) [59]. While using analog transmission, sophisticated black box-users (who are waiting for just these occasions), may be able to capture the electronic serial numbers of the cell phone and 'clone the phone' just like in the early '90s.

Cellular Cloning is a big End-User concern as a cloned Cell phone is equivalent of a stolen calling card. Various companies are targeting cloning issues. Many have come up with solutions like a small fingerprint scanner built into a short, thin cylinder for use in cellular telephones [60]. Eavesdropping is being targeted with enhanced secure and complex algorithms in the 3G setup.

Various other content based security concerns like email borne viruses, spoofing, Trojan horse programs, remote administration programs, mobile code (Java/JavaScript/ActiveX) have had tremendous impact on the information industry [37]. These concerns have forced many handset manufacturers to provide different anti-virus packages with their handsets as we explain in the next section.

1.5. Handsets

1.5.1. Security features

The security features in today's mobile devices is a result of an ongoing effort from of the mobile content providers, mobile operating system providers and the hardware chipset providers. But a complete end-user satisfying and secure mobile devices are far from reality. A synchronized effort from all the providers to ensure greatest privacy and security for the end-users is the requirement of the hour.

The processors and displays of mobile handset devices support many kinds of applications. The operating system is open and well documented and software development kits are freely downloadable. Content security solutions are needed on the end device to protect the handheld terminals against content security issues quite similar to the ones in the PC environment. Major players in securing the mobile enterprise with anti-virus software and secure applications include Symantec [28], McAfee [29], and F-Secure [30] with various other organizations. F-Secure Anti-Virus for Pocket PC is an anti-virus software solution that runs locally on the Pocket PC device. It provides up-to-date and always available protection for these new mobile corporate computing devices. Since the solution runs on the mobile device, it is able to detect and delete all malicious software that enters the device through wireless connections.

Data can be transferred to the mobile device in a number of different ways, including synchronization, removable memory cards, infrared connections and wireless IP connectivity. To properly protect the data on the device, it is essential that the software solution resides locally on the Communicator. F-Secure has taken its award-winning Anti-Virus technology and optimized it for Nokia 9200 Series Communicators [3]. F-Secure Anti-Virus for Nokia 9200 Communicator Series is an antivirus application, which together with a virus signature update service, provides fully automatic protection for mobile devices against viruses and harmful content in all file types. Noticeable contributions from major antivirus application providers like F-Secure include:

- Always available protection locally on the handheld device [4] & [5].
- Automatic Antivirus Scanning in the background
- Automatic scanning of inserted Removable memory, such as Compact Flash cards, and Micro-drives and
- Automatic antivirus database updates over the air.

Also, devices using Microsoft's Pocket PC 2002 [31] and Smartphone 2002 [32] operating systems for connectivity to back-end corporate software (a key feature of wireless synchronization to Outlook for e-mail with attachments) could cause worsening of the epidemic

of viruses spreading through emails [37]. However, that capability is not always on, so consumers will have to set synchronization times. Such issues and concerns of user intervention play a very important part in the growth of a secure mobile environment.

Other security features include location, tracking and security control of the mobile device. In the recent past encryption used in GSM handsets was deliberately disabled on Moscow's networks for 24 hours, at the request of the Communications Ministry [36]. Such incidents may cause security and privacy concerns for the end-user. Within the industry the user specific information is just treated as another piece of data. There is even talk of selling the data to Internet content providers so they can send information to your Internet phone based on your location, for example reviews of nearby restaurants. This location information in the hands of unwanted organizations could be a security breach for the end-users requirements.

Is encryption and user privacy guaranteed for the end-user? Are various security features user-controlled or operator controlled? There are many policy issues in terms of security for the user to understand and use for ensuring a highly secure wireless environment. Various policy-related questions still remain to be answered.

1.5.2. Operating system in mobile security

The mobile device operating system has a huge role to play in the security of the handset. How secure or insecure the mobile device is largely depends on the platform the mobile content providers and mobile software developers use. Security damages through e-mail attached viruses are largely evident in the internet that we know today [37]. How these viruses spread and what information and security holes they make use of to render claimed secure information out in the open is enough to show that a secure operating system should have a lot more than it provides today, particularly when the industry is moving towards m-commerce. Cellular phones today have a few options on the operating systems to choose. The ones worth mentioning include Symbian OS [34], Smartphone [32], Palm OS [33], Pocket PC OS [31].

Major players in the market for providing operating systems to the mobile devices are include Symbian, Microsoft, Palm, and Linux. [35]:

Table 2: Subjects handled by specification series
Sources: IDC mobile operating system forecast July 15th 2003 for Asia and Cellular News

Company	**Market share Asia (2003)**	**Market Share Europe, Middle East & Africa (2003)**
Symbian	53%	53%
Microsoft	27%	24%
Palm	10%	19%
Linux	4%	N/A
Other	6%	N/A

Symbian mobile operating system [34] is an advanced, open operating system licensed by the world's leading mobile phone manufacturers (Ericsson, Fujitsu, Matsushita, Motorola, Nokia,

Psion, Samsung, Sanyo, Siemens and Sony Ericsson). Symbian OS is designed for the specific requirements of advanced 2G, 2.5G and 3G mobile phones and combines the power of an integrated application environment with mobile telephony, bringing advanced data services to the mass market. Diversinet's Symbian OS security client enables application developers to permit end-to-end application-level security on Symbian OS phones, providing end-users with a means for secure data transmission. Diversinet's security facilitates the strong user and server authentication, privacy, and non-repudiation in wireless transmissions and transactions.

In joining the Embedded Technology Partner program of Symbian is F-Secure, the leading provider of content security applications for wireless devices intensifies its development efforts for one of the most important and fastest-growing platforms in the world. The joint agreement gives F-Secure advance access to technology information from Symbian. Majority of the world's handset manufacturers are Symbian OS licensees, Symbian OS phones are set to become mainstream for providing advanced 2.5G data services. The availability of Diversinet's certificate client for Symbian OS is a significant addition to the security toolbox available to Symbian OS developers.

On the other hand Microsoft Corp. has officially unveiled an upgraded version of its Pocket PC mobile operating system that's designed to provide users with improved support for accessing Wi-Fi wireless LANs. Devices using Microsoft's Pocket PC 2002 and Smartphone 2002 operating systems will be able to handle both voice and data access. For devices that are connected to back-end corporate software, a key feature will be wireless synchronization to Outlook for e-mail with attachments, appointments and contacts. However, that capability is not always on, so consumers will have to set synchronization times. Pocket PC 2003 - which is being renamed Windows Mobile 2003 - includes a new network connection manager that can be used to set up WLAN access with 'zero configuration'.

Palm Inc. released a beta-test version of its upcoming Palm OS 5 operating system, which is expected to include expanded security, wireless and multimedia features. The upgraded operating system will include 128-bit security and support for the Wi-Fi wireless LAN standard as well as Bluetooth short-range wireless devices. Palm OS 5 will also have multimedia hooks that are designed to support the development of larger screens.

2. UMTS Handsets

Handsets have taken on the roll as the limiting factor in the deployment of new mobile technologies. While network manufacturers have limited opportunities to sell network equipment, handset manufacturers face a greater number of competitors but do have the opportunity to sell again through replacements. One of the hurdles to 3G implementation will be convincing users to purchase new handsets and thus the success of service launches may depend on how recently consumers purchased their last phone and the terms of that purchase.

Traditionally, the purchase price of handsets has been subsidized by network operators in exchange for subscription commitments, for example of one or two years. Although operators were hoping to do away with these subsidies with UMTS services, it appears they will continue

the practice. The decision is typically made on market conditions and if one operator offers subsidies it is so attractive to consumers that the others must adopt the same practice. For example, "three" an operator in the UK offers both subsidized and unsubsidized plans for its handsets.

An analysis of the near term market for handsets found that among the five major handset manufacturers Motorola, Sony-Ericsson and Siemens have adopted a strategy of offering low-end handsets and lower prices for mass market appeal. Nokia and Samsung, on the other hand, are focusing on brand equity and increasing functionality as the basis for value-added for their phones.

3G handsets have been named as one factor delaying the rollout of commercial services. One of the problems is that the handset testing involves more than 1,000 different parameters, while traditional phones require only 300. Also, software glitches have been a problem such as NTT DoCoMo's FOMA problem where calls were missed while the phone was in sleep mode. However, NTT DoCoMo's 3G technology is not exactly UMTS but a propriety W-CDMA technology.

Given the relative newness of UMTS technology and available handsets, we will examine some security features of GPRS phones to better understand user functionality. The i-mode phone of NTT DoCoMo is one example. The i-mode service makes of SSL for security and handsets designed for use on i-modes may incorporate this use. To help limit distribution of terminal ID information, which may be requested by a website, the handset must request user permission to send the ID [61].

The NEC i-mode phone designed to operate on a GSM network has the following security features. The features rely on 5 different security codes: PIN 1 code, dial lock code, PIN 2 code, SIM lock code and the PUK code. The PIN 1 code is provided by the network to protect the SIM card in case of theft. The phone may be set up such that it requires the PIN 1 code before the phone can be used at all. It may also be the case that entering the PIN 1 code incorrectly more than three times blocks the code and the user must contact the service provider to unblock the SIM card. It is possible with some SIM cards to disable this feature allowing easy, although less secure, phone start-up, however some SIM cards are set up so that PIN 1 number entry cannot be turned off. The PIN 2 code restricts access to advanced features. The dial lock security feature allows the user to give their phone to another user while limiting the second user to receiving calls only. Enabling this feature requires the dial lock code, which like the PIN 1 and PIN 2 codes, can be changed by the user.

The fifth security code is the SIM lock. The SIM lock prevents the phone from being used with another SIM and thus makes it less useful if stolen. The i-mode phone also has a call barring feature that allows the user to restrict the types of calls made or received on the phone. Barring options include preventing all outgoing international calls or incoming calls while roaming.

2.1. WAP

WAP (Wireless Application Protocol) is a specification for presenting and interacting with information on wireless (and other) devices. Technically speaking communications systems consist of many layers (in many cases 7 or more): physical layers (optical fibers, wireless transmission systems, lasers, antennas etc), and software layers (transmission protocols, etc). Good engineering practice requires that these layers are decoupled as much as possible. WAP, as a protocol for presenting and interacting with information is positioned near or at the top of these layers. Therefore WAP can be used on top of different communication systems. There are many different ways to implement commercial services using the WAP protocol. For example, present (November 2001) implementations of commercial services using WAP in Japan and in Europe differ substantially - the user experience is different, commercial models are different, handsets have very different characteristics etc. Therefore it is not useful to identify WAP with one particular implementation. Mostly, the user experience is related to factors which have nothing to do with the WAP specification themselves, but are specific to a particular implementation. In addition, WAP specifications change over time, and are coordinated within the WAP-Forum.

2.1.1. WAP and i-mode

WAP based wireless internet services today are used in Europe, Japan, Korea and other areas in the world. WAP implementations use a page description language called wml (wireless markup language) while i-mode uses chtml. Different companies implement wireless internet services using WAP as a protocol in very different ways. For example, WAP based services in Japan, which are in competition with i-mode, provide a very different user experience than WAP based services in Europe, demonstrating the flexibility of the WAP approach. One important difference from the user and site developer perspective of wireless services is that websites for i-mode are very similar to ordinary html based internet websites. I-mode uses chtml as a page description language for i-mode websites. Therefore a very large number of private i-mode sites are being created. I-mode sites can also be inspected with ordinary internet web browsers (although the result differs somewhat from the display of the same pages on i-mode handsets). Websites for WAP-based services on the other hand need to be written in a new and WAP-specific page description language (wml). However, the real business differences between today's WAP implementations and i-mode are more in the way these services are marketed, advertised, business models, charging models, the handsets, battery life, handset display quality etc.

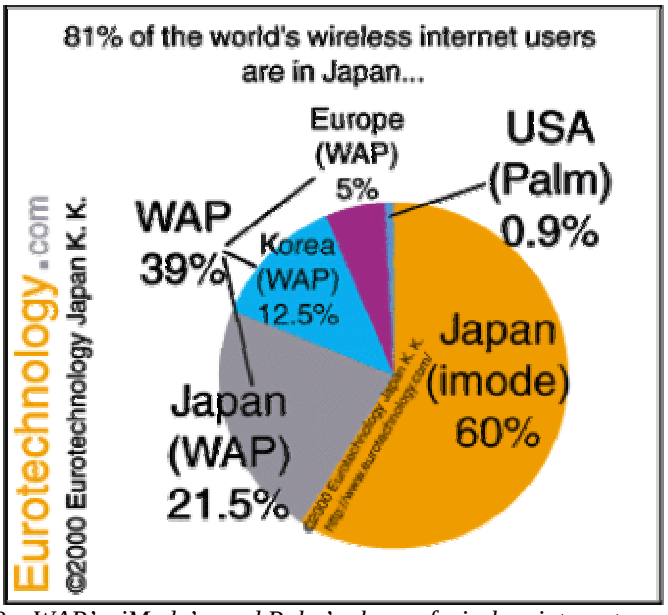

Figure 2 – WAP's, iMode's, and Palm's share of wireless internet user market
Source: Eurotechnology.com

WAP implementations in Europe till the end of 2000 were circuit switched (users need to dial-up in order to connect), i-mode is packet-switched (always connected, as long as the user's handset is reached by the i-mode radio signal). In Japan WAP implementations also use packed switching. Also, i-mode includes images, animated images and color on the other hand WAP implementations in Europe at the moment only use text and no images.

There are great differences in the business models, charging systems and marketing of different WAP implementations and i-mode:

- I-mode handsets in Japan have large full color (256 colors) displays and can display animated full color gifs and ten lines of text or more, while European implementations of WAP today have handsets showing four lines of text in black/white without images. Note that this is not a limitation of the WAP protocol itself (as Japanese WAP implementations demonstrate) but rather a limitation of present day implementations in Europe. WAP-implementations in Japan do include full color images and many other features not found in Europe at present.
- Content: Marketing of WAP based services in Europe presently focus on business applications (banking, stock portfolio, business news, flight booking), while marketing of WAP-based services in Japan and i-mode in Japan focus on fun and everyday life-style: restaurant guides, games, images, ringing melodies.

Appendix B - WLAN Technologies

1. IEEE Specifications

Many studies show forecasts of public wireless LAN hotspots to grow at fast pace. Also some studies show that the deployment of WLAN will stimulate the uptake of UMTS/ GPRS. Furthermore, forecasts have been made that mobile operators will bill most of the WLAN subscribers in the near future [20].

In the wireless LAN market several technologies have been identified. All have some pros and cons with regard to their deployment. HiperLAN2 was for example promoted by ETSI (European Standards Telecommunications Institute) to offer similar services like the now most widely deployed IEEE 802.11b. The latter's success however has outplayed the likelihood of deployment of HiperLAN2 applications. *802.11* standards refer to a family of specifications developed by the IEEE for wireless LAN technology. 802.11 specify an over-the-air interface between a wireless client and a base station or between two wireless clients. The IEEE accepted the specification in 1997.

The following are specifications in the 802.11 family as accepted by IEEE:

1.1. IEEE 802.11

The IEEE 802.11 standard applies to wireless LANs and provides 1 or 2 Mbps transmission in the 2.4 GHz band using either frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS).

1.2. IEEE 802.11b

The IEEE 802.11b, also referred to as Wi-Fi, is the most widely deployed technology. It is an extension of 802.11 accepted in 1999, allowing wireless functionality comparable to Ethernet. It operates in the 2.4 GHz band and has a maximum throughput of 11 Mbps with a fallback to 5.5, 2 and 1 Mbps [20], [55]. It uses only DSSS (direct sequence spread spectrum). The 2.4 GHz frequency band is shared with certain applications like wireless phones, microwave ovens, video transmitters and Bluetooth devices. Interference from Bluetooth might reduce the throughput of 802.11b products to around 2 Mbps. A forthcoming standard, IEEE 802.11g aims to offer 54 Mbps in the 2.4 GHz band [20]. Since 1999 the Wireless Ethernet Compatibility Alliance (WECA) issues WiFi certificates to certify interoperability among 802.11b products from different vendors.
Currently 802.11b is the only widely available WLAN technology in the market.

1.3. IEEE 802.11a

The IEEE 802.11a is an evolution of 802.11b and offers more bandwidth. It operates in the 5 GHz band. This band is not used for other short-range applications. Also, the 5 GHz band is much larger than the 2.4 GHz band. Maximum throughput is 54 Mbps [20]. 802.11a uses an orthogonal frequency division multiplexing encoding scheme rather than FHSS or DSSS. A new

standard, 802.11h will add the Transmit Power Control (TPC) and Dynamic Frequency Selection (DFS) features to the 802.11a standard.

1.4. IEEE 802.11d/e/f/I

Besides the definition of the physical layer, there are taskforces working on issues such as QoS and security. This work is mostly still in progress [20].

- 802.11d (Regulatory) defines how access points communicate information to the user devices over the permissible radio channels and power levels. This work has already been completed and is now part of the standard.
- 802.11e (Multimedia and QoS) defines classes of services with managed levels of QoS for data, voice and video applications.
- 802.11f (Mobility) recommends practices for an Inter-Access Point Protocol.
- 802.11i (Security) specifies new security features, including integration of IEEE 802.1X within IEEE 802.11 (see also section 4.2). An interim draft of IEEE 802.11i is now shipping, also known as Wi-Fi Protected Access (WPA).

2. Components of the IEEE 802.11 architecture

This section describes certain basic components of the 802.11 architecture which would help us better understand the information in securing today's WLANs. This basic information would also help the users to understand the interoperability issues with cellular networks. For detailed description of the standard refer to the IEEE 802.11 specifications [14] and [57].

The IEEE 802.11 architecture consists of several components that interact to provide a wireless LAN that supports station mobility transparently to upper layers.

- **Station (STA)** is a device that contains an IEEE 802.11 conformant medium access control (MAC) and physical layer (PHY) interface to the wireless medium (WM).
- **Access Point (AP)** is an entity that has station (STA) functionality and provides access to the distribution services, via the wireless medium (WM) for associated stations.
- **Basic Service Set (BSS)** is the basic building block of an IEEE 802.11 LAN. A BSS is a set of stations (STA) controlled by a single coordination function.
- **Extended Service Set (ESS)** is a set of one or more interconnected BSSs and integrated local area networks (LANs) that appears as a single BSS to the logical link control layer (LLC) at any station associated with one of those BSSs.
- **Distribution System (DS)** is a system used to interconnect a set of BSSs and integrated local area networks (LANs) to create an extended service set (ESS).
- **Distribution System service (DSS)** is a set of services provided by the DS that enable the medium access control (MAC) to transport MAC service data units (MSDUs) between stations that are not in direct communication with each other over a single instance of the wireless medium (WM). These services include
  - Transport of MSDUs between the APs of BSSs within an extended service set (ESS)
  - Transport of MSDUs between portals and BSSs within an ESS, and

  - Transport of MSDUs between STAs in the same BSS in cases where the MSDU has a multicast or broadcast destination address or where the destination is an individual address, but the station sending the MSDU chooses to involve DSS. DSSs are provided between pairs of IEEE 802.11 MACs.
- **Independent basic service set (IBSS):** is a BSS that forms a self-contained network, and in which no access to a DS is available.

The IBSS is the most basic type of IEEE 802.11 LAN. A minimum IEEE 802.11 LAN may consist of only two STAs. This mode of operation is possible when IEEE 802.11 stations are able to communicate directly. Because this type of IEEE 802.11 LAN is often formed without pre-planning, for only as long as the LAN is needed, this type of operation is often referred to as an *ad hoc network.*

The association between a STA and a BSS is dynamic (STAs turn on, turn off, come within range, and go out of range). To become a member of an infrastructure BSS, a station shall become "associated." These associations are dynamic and involve the use of the DSS. PHY limitations determine the direct station-to-station distance that may be supported. For some networks this distance is sufficient; for other networks, increased coverage is required. Instead of existing independently, a BSS may also form a component of an extended form of network that is built with multiple BSSs. The architectural component used to interconnect BSSs is the DS.

IEEE 802.11 logically separates the wireless medium (WM) from the distribution system medium (DSM). Each logical medium is used for different purposes, by a different component of the architecture. The IEEE 802.11 definitions neither preclude, nor demand, that the multiple media be either the same or different. Recognizing that the multiple media are *logically* different is a key to understanding the flexibility of the architecture. The IEEE 802.11 LAN architecture is specified independently of the physical characteristics of any specific implementation.

The DS enables mobile device support by providing the logical services necessary to handle address to destination mapping and seamless integration of multiple BSSs. An access point (AP) is a STA that provides access to the DS by providing DS services in addition to acting as an STA. Data move between a BSS and the DS via an AP. Note that all APs are also STAs; thus they are addressable entities. The addresses used by an AP for communication on the WM and on the DSM are not necessarily the same.

The DS and BSSs allow IEEE 802.11 to create a wireless network of arbitrary size and complexity. IEEE 802.11 refers to this type of network as the *extended service set* network. The key concept is that the ESS network appears the same to an LLC layer as an IBSS network. Stations within an ESS may communicate and mobile stations may move from one BSS to another (within the same ESS) transparently to LLC.
All of the following are possible:

a) The BSSs may partially overlap. This is commonly used to arrange contiguous coverage within a physical volume.
b) The BSSs could be physically disjointed. Logically there is no limit to the distance between BSSs.

c) The BSSs may be physically collocated. This may be done to provide redundancy.
d) One (or more) IBSS or ESS networks may be physically present in the same space as one (or more) ESS networks. This may arise for a number of reasons. Two of the most common are when an ad hoc network is operating in a location that also has an ESS network, and when physically overlapping IEEE 802.11 networks have been set up by different organizations.

3. Authentication services

IEEE 802.11 defines two subtypes of authentication service [41]

- *Open System* and
- *Shared Key*

The subtype invoked is indicated in the body of authentication management frames. Thus authentication frames are self identifying with respect to authentication algorithm. A mutual authentication relationship shall exist between two stations following a successful authentication exchange as described below. Authentication shall be used between STAs and the AP in an infrastructure BSS. Authentication may be used between two STAs in an IBSS.

3.1. Open System authentication

Open System authentication is the simplest of the available authentication algorithms. Essentially it is a null authentication algorithm. This means that the Access Point (AP) is connected to the LAN and no further authentication is activated on the AP [50]. Thus every device can see and use the WLAN, while the IP address can be assigned by DHCP. In more detail the authentication is as follows: Any STA that requests authentication with this algorithm may become authenticated if the dot11 Authentication Type at the recipient station is set to Open System authentication. Open System authentication is not required to be successful as a STA may decline to authenticate with any particular other STA. Open System authentication is the default authentication algorithm.

Open System authentication involves a two-step authentication transaction sequence. The first step in the sequence is the identity assertion and request for authentication. The second step in the sequence is the authentication result. If the result is “successful,” the STAs shall be mutually authenticated.

3.2. Shared Key authentication

Shared Key authentication supports authentication of STAs as either a member of those who know a shared secret key or a member of those who do not. IEEE 802.11 Shared Key authentication accomplishes this without the need to transmit the secret key in the clear; however, it does require the use of the WEP privacy mechanism. Therefore, this authentication scheme is only available if the WEP option is implemented. Additionally, the Shared Key authentication algorithm shall be implemented as one of the dot11 Authentication Algorithms at any STA where WEP is implemented. The required secret, shared key is presumed to have been delivered to participating STAs via a secure channel that is independent of IEEE 802.11. This

shared key is contained in a write-only MIB attribute via the MAC management path. The attribute is write-only so that the key value remains internal to the MAC.

During the Shared Key authentication exchange, both the challenge and the encrypted challenge are transmitted. This facilitates unauthorized discovery of the pseudo-random number (PRN) sequence for the key/IV pair used for the exchange. Implementations should therefore avoid using the same key/IV pair for subsequent frames. A STA shall not initiate a Shared Key authentication exchange unless its dot11PrivacyOptionImplemented attribute is "true". The STA initiating the authentication exchange is referred to as the *requester*, and the STA to which the initial frame in the exchange is addressed is referred to as the *responder*.

3.3. The Wired Equivalent Privacy (WEP) algorithm

Eavesdropping is a familiar problem to users of other types of wireless technology. IEEE 802.11 specifies a wired LAN equivalent data confidentiality algorithm. To this extent *Wired Equivalent Privacy* (WEP) is defined as protecting authorized users of a wireless LAN from casual eavesdropping. This service is intended to provide functionality for the wireless LAN equivalent to that provided by the physical security attributes inherent to a wired medium.

The WEP protocol secures the data link layer, which is the link between the wireless device and the Access Point (AP). This data confidentiality depends on an external key management service to distribute data enciphering/deciphering keys. This means that on the AP a so-called WEP-key, which is a large cipher that serves as a key, is implemented. The clients have to know the WEP key in order to be authenticated, and if the key needs to be replaced, the whole user group must enter the new key. The IEEE 802.11 standards committee specifically recommends against running an IEEE 802.11 LAN with privacy but without authentication. While this combination is possible, it leaves the system open to significant security threats: WEP has proven to contain security flaws and does not operate on the earlier claimed security level. It lacks a key management protocol, as the secret key is chosen manually. Mechanisms should be established to dynamically assign and renew WEP keys [50]. However, the WEP mechanism is so far the only specified confidentiality algorithm and has the following properties:

- *It is reasonably strong:*
  The security afforded by the algorithm relies on the difficulty of discovering the secret key through a brute-force attack. This in turn is related to the length of the secret key and the frequency of changing keys. WEP allows for the changing of the key (*k*) and frequent changing of the IV.
- *It is self-synchronizing:*
  WEP is self-synchronizing for each message. This property is critical for a data-link level encryption algorithm, where "best effort" delivery is assumed and packet loss rates may be high.
- *It is efficient:*
  The WEP algorithm is efficient and may be implemented in either hardware or software.
- *It may be exportable:*
  Every effort has been made to design the WEP system operation so as to maximize the chances of approval, by the U.S. Department of Commerce, of export from the U.S. of

products containing a WEP implementation. However, due to the legal and political climate toward cryptography at the time of publication, no guarantee can be made that any specific IEEE 802.11 implementations that use WEP will be exportable from the USA.

- *It is optional:*
  The implementation and use of WEP is an IEEE 802.11 option.

The IEEE 802.11 Task Group is currently studying for a secure protocol on the wireless network level. This is not available yet. The Temporal Key Integrity Protocol (TKIP) will most likely constitute the interim solution. It makes the WEP key dynamic. The long-term solution will be based on the Advanced Encryption Standard (AES) that has a much better underlying cipher.

3.4. Other Security for WLANs

As the security measures mentioned above are not fully reliable, the following other authentication mechanisms are in use [50]:

- WEB-based authentication: As an extension to open access, limitation of the open network can be achieved by connecting a gateway between the WLAN and the corporate network. This is secure WEB-based authentication that uses a username/ password pair. This pair is submitted to the Home AAA (Authentication, Authorization, Accounting) server. The password might be a onetime password, and the end-user has to know the key to get access. However, the network is not totally secure as it can be eavesdropped by other WLAN users, with which they can find out what passports or IP-addresses are so that hackers can get actual access to the network.
- VPN: On the network layer the communication between the wireless device and the (corporate) network could be kept secure using a Virtual Private Network (VPN). This software is largely dependent on the vendor. It can be established using IPSec based VPN. In this case when IP connectivity is set up, the end-user is authenticated when the IPSec tunnel to the corporate network is set up. To this extent, it is required for terminals to have an IPSec client. When using a VPN the userdata between the user and gateway is encrypted. Hackers will only see packets with IP addresses and unexplainable data.
- PPPoE: Just like PPP is being used for regular dial-up to the internet, it could be used to log in to a central point in the wireless network. Implementations look rather similar to the VPN and web-based solutions and have pretty much the same pros and cons.

It has been noted that WLAN security slippages in the industry are very basic. The most common slippages include failure to use basic, industry-standard security features. It is the most likely cause of unauthorized access to a network. Excessive security measures used for non-sensitive applications can reduce throughput and make a wireless network cumbersome to use. Also, the amount of security should be calibrated to business needs. Few networks, for example, need the degree of security required by computer networks used in national defense. Common security errors include: not changing a default SSID; failing to change keys regularly; not protecting shared drives and folders with passwords; improper access point placement; not changing an administrative password; and not using VPN for highly sensitive data.

A report from Datacomm Research suggests that the problem is not that wireless networks are inherently insecure, but that wireless hackers are generally untraceable, using an invisible link to infiltrate into the system. This combined with the fact that networks are increasingly combining wired and wireless connections, has made improved security a top priority for the wireless LAN industry.
Please refer to [17], [18], [19], [20] for further details on WLAN security.

4. Interoperability

A lot of work has been done in the area of making WLANs more secure and also of merging cellular networks and WLAN technology. WLAN hot spots in the GSM cellular network are very helpful in integrating multimedia, data and voice services into a "single bill". There have been proposals for reuse of GSM (SIM) and 3G (AKA) security mechanisms within 802.11. SIM authentication offers the most security however it requires some software installed on the terminal. Also, on the application layer - this constitutes the communication between the wireless device and an application server like a critical Web server – extra security measures should be taken. This can be achieved by using HTTPS/SSL.

To understand the interoperability issues in terms of security of the cellular and WLAN networks we need to look into authentication and encryption protocols of both the standards. We also need to have an understanding of the work that has been done on merging the two standards together for a smooth and secure integration of the systems.

4.1. EAP and PPP

PPP (Point to Point Protocol) evolved beyond its original use as a dial-up access method and is now used all over the Internet. One piece of PPP defines an authentication mechanism. With dial-up Internet access, that is the username and password. PPP authentication is used to identify the user at the other end of the PPP line before giving them access.

Most enterprises want to do more for security than simply employing usernames and passwords for access, so a new authentication protocol, called the Extensible Authentication Protocol (EAP), was designed. EAP sits inside of PPP's authentication protocol and provides a generalized framework for several different authentication methods. EAP is supposed to head off proprietary authentication systems and let everything from passwords to challenge-response tokens and public-key infrastructure certificates all work smoothly [16].

With a standardized EAP, interoperability and compatibility of authentication methods becomes simpler. For example, when you dial a remote-access server and use EAP as part of your PPP connection, the RAS doesn't need to know any of the details about your authentication system. Only you and the authentication server have to be coordinated. By supporting EAP authentication a RAS server gets out of the business of acting as middle man, and just packages and repackages EAP packets to hand off to a RADIUS server that will do the actual authentication.

4.2. 802.1X

This brings us to the IEEE 802.1x standard, which is simply a standard for passing EAP over a wired or wireless LAN. With 802.1x, EAP messages are packaged in Ethernet frames without making use of PPP. Thus this means it is authentication and nothing more, which is desirable in situations in which the rest of PPP is not needed, if protocols other than TCP/IP are being used, or when the overhead and complexity of using PPP is undesirable.

The 802.1x protocol defines access as low as possible in the OSI layer model, after which in higher layers the access is transparent. This means that handovers from AP to AP will go faster than the earlier described mechanisms. 802.1x uses three terms. The user or client that wants to be authenticated is called a *supplicant*. The actual server doing the authentication, typically a RADIUS server, is called the *authentication server* and the device in between, such as a wireless access point, is called the *authenticator*. One of the key points of 802.1x is that the authenticator can be simple and dumb - all of the brains have to be in the supplicant and the authentication server. This makes 802.1x ideal for wireless access points, which are typically small and have little memory and processing power.

The protocol in 802.1x is called EAP encapsulation over LANs (EAPOL). It is currently defined for Ethernet-like LANs including 802.11 wireless, as well as token ring LANs such as FDDI. EAPOL is not particularly sophisticated. There are a number of modes of operation, but the most common case would look something like this:

The authenticator sends an "EAP-Request/Identity" packet to the supplicant as soon as it detects that the link is active (e.g., the supplicant system has associated with the access point).

- The supplicant sends an "EAP-Response/Identity" packet to the authenticator, which is then passed on to the authentication (RADIUS) server.
- The authentication server sends back a challenge to the authenticator, such as with a token password system. The authenticator unpacks this from IP and repackages it into EAPOL and sends it to the supplicant. Different authentication methods will vary this message and the total number of messages. EAP supports client-only authentication and strong mutual authentication. Only strong mutual authentication is considered appropriate for the wireless case. Within EAP several types of authentication are possible, like username/ password, certificates, etc.
- The supplicant responds to the challenge via the authenticator and passes the response onto the authentication server.
- If the supplicant provides proper identity, the authentication server responds with a success message, which is then passed onto the supplicant. The authenticator now allows access to the LAN- - possibly restricted based on attributes that came back from the authentication server. For example, the authenticator might switch the supplicant to a particular virtual LAN or install a set of firewall rules.
- After authentication the data are encrypted, and even IP-addresses are hidden for hackers.

Appendix C - WLAN & Cellular Network Integration

1. Introduction

WLAN is interesting for certain applications and finds its origin in enterprises. So far WLAN has mostly been deployed at companies as part of the internal intranet. For business people on the move it is very attractive: Therefore nowadays WLAN for the public arises at more and more places. Besides this, WLAN is currently often being deployed in the residential space by connecting WLAN to for example a DSL connection. In the public space, WLAN is mostly deployed by private owners, like airport owners, hotel owners etc [53]. Also some local ISPs use WLAN technology to offer broadband Internet access to rural areas and small cities. The next step, and what is currently already happening, is mobile operators buying capacity on networks deployed by others to manage customer care and billing. This means that the mobile operator bills the end-user. The mobile operator could also deploy its own WLAN, or could establish a partnership with a WISP (Wireless Internet Service Provider) to market their services.
So in short there are the following market segments for WLANs [15]:

- Enterprise: Here WLAN is mostly used as an extension to the already existing intranet (fixed LAN). Here people in the office get the opportunity to move around and visitors can also get attached to the network easily.
- Small Office, Home Office (SOHO): Here WLANs are used as the main hub for all wireless Internet connections. The WLAN is connected to a major backbone often via fixed networks, like DSL or cable connections.
- Public Access LAN (PAL): This is what is widely known as public 'hot spots'. It provides access in public spaces that are densely populated and where people are rather stationary, like airports, shopping centers and hotels.

However, bandwidth is limited with WLAN. IEEE 802.11b provides shared bandwidth with a maximum of 5.5 Mbps switched, while fixed networks often provide speeds up to 100 Mbps. The real bandwidth also depends on the distance to the base station (coverage up to 50m.), number of users (shared aspect), the used system and sometimes the reflection of signals by walls and furniture (also see Appendix B on WLAN technologies) [53] and [55]. IEEE standard 802.11a describes a bandwidth of 54 Mbps, but these products are not available in the market yet. However, currently WLAN does provide the fastest speeds available wireless. Therefore it is an attractive access technology. Also the cost ration is very attractive: Cellular data communication, as the most widely deployed wireless technology, is more expensive. For WLAN the main costs are in WLAN access cards, access points and extra security, but costs are decreasing all the time. These aspects together make WLAN an interesting complement to other wireless communication technologies; cellular 2.5G and 3G services.

However still there are some aspects of wide WLAN deployment that need to be taken care of: Security is still a big issue (see appendix B), and furthermore billing, session continuity and roaming are points of focus currently that however seem to provide good solutions in the future. This will be described in sections 1.2 and 1.3. Only one negative aspect remains: The predicted

exponential growth of WLAN in the future could become a problem: WLAN operates in the unlicensed 2.4 GHz frequency band, and with an enormous amount of users interference could become a problem, which would make it difficult to guarantee quality of service.

1.1. WLAN/ GSM&UMTS integration

Currently mobile operators are starting to exploit WLAN technology and want to integrate WLAN into their cellular data networks [20], [53], and [54]. This highlights the need for inter-working mechanisms and cellular data networks. These integrated wireless data networks should be capable of providing data services at very high speeds in hotspot locations.

Already 2G cellular systems provide a high level of mobility; however it is only for voice services and low speed data. As today communicating on the move is becoming a more and more important necessity, 3G is entering the market in order to meet the end-users; data communications needs. 3G cellular systems will be able to allow high speed data rates, as comparable to wired data services. Speeds up to 300 Kbps will be available and will increase up to 2 Mbps. However, as the rollout of 3G is delayed mobile operators try to already offer services that are like 3G to meet end-users' needs and also to generate new revenue streams. 2.5G cellular data technology, of which GPRS is the most famous one, already provides speeds up to 100 Kbps with which data services can be delivered. However, it is still limited as higher data rates are needed to meet user needs for businesses and multimedia applications. Thus, as 2.5G cannot meet market needs yet and 3G is still not widely in the market, mobile network operators turn to WLAN deployment in hotspot areas. This has also to do with the fact that WLAN is already deployed worldwide at more and more places, and it provides rather high data rates.

As cellular data networks provide relatively low speed data services over a large coverage area (100 Kbps currently), and WLAN provides relatively high speed data services (currently up to 11 Mbps with 802.11b and in the near future 54 Mbps with 802.11a) over a rather small coverage area, integration of both combines the advantages of both access networks. With full deployment of 3G however, the cellular networks will be capable of indeed delivering high speed data services. The advantage of GPRS and UMTS over WLAN is to provide both data and voice services and also personalization to end-users. Besides this guarantees bandwidth and Quality of Service. Thus this makes WLAN good for coverage in small hot-spot locations, and cellular telecommunications for broad umbrella coverage. At hot-spot locations, cellular networks will be used for voice communication, and furthermore according to the application to be used the best network can be used. [15]

In order to provide convenience to customers and thus to meet market needs, operators must provide seamless mobility between the cellular and WLAN networks. Therefore interworking mechanisms between WLAN and cellular networks must be provided that can take care of the following aspects: integrated authentication, integrated billing, roaming, terminal mobility, and service mobility. These integration issues will be discussed below.

1.2. Roaming

There are two examples of configurations for roaming between WLAN and cellular data networks. Variations depend on the ownership or management of the WLAN. It is possible for the cellular operator to own and manage the WLAN, or a wireless Internet service provider (WISP) could deploy the WLAN or the enterprise/ owner of the hotspot location.

In operator owned WLANs the mobile operator has the advantage of an already existing customer base. The mobile operator also already has authentication and billing mechanisms for their users, what can be used in the WLAN network. If the WLAN network is not owned by the mobile operator, the same user experience could be achieved by making roaming agreements between the WISPs and mobile operators. Then the billing and authentication services could still be offered by the mobile operator.

If an enterprise establishes a WLAN network, the enterprise takes care of the (mostly limited) authentication and only sometimes billing systems. Also here the mobile operator could come in to provide these services [54]. There are two roaming methods: IP roaming and GSM roaming. IP roaming makes uses of AAA mechanisms, while GSM roaming makes us of SS7 mechanisms [20].

1.3. Session Mobility

Session mobility is an extension of roaming in the integrated wireless communication environment. A session is the flow of IP packets between the end user and an external entity which could be for example an FTP or HTTP session. Session mobility is then the change during one session between WLAN and the cellular network when the coverage of the first network that one is connected to is not sufficient anymore. Then the IP flow should seamlessly be switched to the other network, with the end-to-end session remaining unaffected, and no end-user intervention being required. This is different from roaming as no user intervention is needed and the IP session is preserved. This could either address the change between WLANs itself or between WLAN and UMTS/ GPRS networks. The mobility is merely coordinated at the IP level using Mobile IP [20]. This allows a tolerable interruption and recovery of the ongoing session, and is not a conventional network handover.

2. Interworking Scenarios

Currently many standardization activities are going on. A few standardization bodies have been working on integration standards for WLAN and cellular telecommunication networks. The goal of the standardization efforts is to define standard interworking interfaces to make sure interworking across multivendor equipments and across several types of WLANs and cellular networks. For WLAN integration WIG has been set up (Wireless Interworking Group) to deal with the interworking between WLANs and cellular networks. The following bodies are represented in WIG: ETSI BRAN, IEEE 802.11, IEEE 802.15, and MMAC. However, currently the most intensive standardization activities are taking place at 3GPP, the Third Generation Partnership Project. They are involved in the GSM and UMTS specifications. They have also

approved a WLAN/ cellular network interworking item, that specifies some interworking techniques. Also related to this have been the requirements that have been specified and categorized into six interworking scenarios [54]:

2.1. Scenario 1 – Common Billing and Customer Care

This features no real interworking between the WLAN and GPRS except for the common bill and customer care to the end-user. Thus no further standardization activities are required. It is the simplest form of integration.

2.2. Scenario 2 – 3GPP System-Based Access Control and Charging

This requires authentication, authorization and accounting (AAA) for subscribers in the WLAN to be based on the same procedures as used in the GPRS system. So this means the end-user can use his or her SIM card for authentication in the WLAN network just as he or she normally does in the cellular network.

2.3. Scenario 3 – Access to 3GPP GPRS-Based Services

The cellular operator should be allowed to provide access to the GPRS services to users in the WLAN network: This means the user can get access to GPRS services over both the GPRS network as the WLAN network. We should think of IP multimedia services, location based services, instant messaging, and presence-based services. It must be noted that there is no service continuity across the networks in scenario 3.

2.4. Scenario 4 – Service Continuity

Here access to GPRS services just as mentioned for scenario 3, but then also with service continuity included. So the user must be able once accessing a certain service over one network infrastructure, to move to the other infrastructure where the service is continued. However, in scenario 4 the service continuity requirements are not very strict; some service may not be able to continue after a hand-over.

2.5. Scenario 5 - Seamless Services

Here seamless service continuity should be provided between GPRS and WLAN. This means the user should not note any significant differences between the different networks.

2.6. Scenario 6 – Access to 3GPP Circuit-Switched Services

Here the operator could offer access to circuit-switched services (like voice calls) from the WLAN system. This should also include seamless mobility.

3. Interworking Architectures

There have been a few approaches to interworking architectures. The European Telecommunications Standards Institute specifies two generic approaches: Loose coupling and tight coupling. Loose coupling defines the WLAN network to be deployed as complementary to the cellular network. Then the WLAN uses the subscriber databases in the cellular network but

there are no data interfaces to the cellular network. Thus with loose coupling the WLAN bypasses the cellular network and provides direct access to the external environment. With tight coupling the WLAN is connected to the cellular core network and therefore the data traffic goes through the cellular network before reaching the external environment [54].

Currently loose coupling is used most with making use of SIM based authentication and billing. However, this provides limited session mobility capabilities compared to tight coupling.

3.1. Loose Coupling Architecture

With loose coupled architecture the WLAN network is coupled to the GPRS network in the operator's IP network. This means that it is contrary to a tight coupled infrastructure in that the WLAN data traffic does not pass through the GPRS core network. It goes directly to the operator's IP network or to the Internet. SIM based authentication may also be used to get access to operator's services. Integrated billing is also offered. This WLAN network could either be owned by a third party and could use roaming via a connection between the operator and WLAN or over an existing public network, like the Internet. Cellular technology does not have to be incorporate into the WLAN network like with tight coupling as IETF based protocols are used for the billing, authentication and mobility. [54]

- Reuse of SIM based authentication
- Session mobility: Mobile IP could be used to provide session mobility across GPRS and WLAN networks. (No GPRS mobility management as with tight coupling)
- Security: As WEP is known as an inefficient encryption scheme, 802.1x could be implemented. Also other more enhanced encryption schemes might be used.

3.2. Tight Coupling Architecture

Tight coupling can fulfill the requirement scenarios 1-4. Depending on the WLAN technology and whether it can support Quality of Service (QoS), it can also fulfill requirement scenario 5.
The tight coupling architecture provides solutions for interworking between WLAN and GPRS, with the following features [54]:

- Seamless service continuation between WLAN and GPRS
- Reuse of GPRS AAA
- Reuse of GPRS infrastructure: The core network, subscriber databases, billing systems)
- Support of lawful interception for WLAN subscribers
- Increased security – GPRS authentication and ciphering can be applied on top of WLAN ciphering
- Access to core GPRS services (e.g. SMS, location-based services, MMS)

References

Wireless security white papers

1. Better security: A Practical guide, Watchgaurd, 2002
2. Wireless security: Its like securing your home, Intermec Inc., 2002
3. Computer viruses – From an annoyance to a serious threat, f-secure, Sept 2001
4. Protecting stored data with f-secure FileCrypto, f-secure, 2000
5. Content security at hand: A white paper on handheld device security, f-secure, November 2002
6. Security risks in telecommuting, f-secure, April 2000
7. A Plan for no span, Verisign, 2003

UMTS security white papers

8. 3G: Another technology cycle, Ericsson Australia, March 2002
9. Calling next generation, Nokia, 2003
10. A history of third generation mobile: 3G, Nokia, March 2003
11. 3G wireless networks, Wi-Fi wireless LANS, and secure VPNs: Perspectives for mobile operators, Lucent technologies, March 2003
12. Ensuring wireless security with 3G, Lucent technologies, 2002
13. Packet core network security white paper, Nortel networks, October 2001

WLAN security white papers

14. IEEE 802.11 WLAN MAC and PHY specifications, IEEE, 1999
15. WLAN as a compliment to GPRS and 3G services, Ericsson Australia, 2002
16. EAP methods for wireless authentication, Intermec Networks Inc., April 2003
17. Understanding the layers of WLAN security and management, AirDefense Inc., 2003
18. WLAN security: What hackers know that you don't, AirDefense Inc., 2003
19. WLAN policies for security and management, AirDfense Inc., 2003
20. Public WLAN for mobile operators, Alcatel, 2003
21. Cisco SAFE: WLAN security in depth, Cisco, 2003
22. Building sustainable 802.11 service offerings: A white paper for service providers, Bridgewater systems, March 2003
23. MobiLAN secure POSITION, Intermec Inc., 2001

Articles and miscellaneous

24. Reid, P. (2003) 3G Standardization; Meeting Market Requirements. Presentation to the UMTS 2003 Deployment Congress, Amsterdam, The Netherlands June 11-12, 2003.
25. 3GPP website: http://www.3gpp.org
26. UMTS Security features: http://www.umtsworld.com/technology/security.htm
27. Cell phone security: http://www.cit.cornell.edu/cellphone/security.html
28. Symantec: http://www.symantec.com/
29. McAfee: http://us.mcafee.com/default.asp
30. F-Secure: http://www.f-secure.com/index.shtml
31. Pocket PC: http://www.microsoft.com/windowsmobile/resources/technicalarticles/pocketpc/default.mspx
32. Smartphone: http://www.microsoft.com/windowsmobile/products/smartphone/default.mspx
33. Palm OS: http://www.palmos.com/dev/tech/palmos5/
34. Symbian mobile operating system: http://www.symbian.com
35. Mobile OS market share:

    a. http://www.newlc.com/article.php3?id_article=132
    b. http://www.techweb.com/wire/story/TWB20030620S0008
    c. http://www.nordicwirelesswatch.com/wireless/story.html?story_id=2347
36. Russian GSM security disabled: http://www.cellular-news.com/story/9262.shtml
37. Virus articles:
    http://news.com.com/2100-1023-241489.html
    http://www.ecommercetimes.com/perl/story/3502.html
    http://www.symantec.com/avcenter/venc/data/mobile-phone-hoax.html
    http://news.bbc.co.uk/2/hi/technology/2690253.stm
38. Intel security solution:
    http://www.intel.com/network/connectivity/solutions/wireless/deploy_security.htm
39. Dell security solution:
    http://www.dell.com/us/en/esg/topics/power_ps4q02-lowery.htm?mc=%M&DGVCode=BA
40. GSM Security Flaw: http://www.isaac.cs.berkeley.edu/isaac/gsm.html
41. 802.11 Security: http://www.drizzle.com/~aboba/IEEE/
42. WEP Flaws: http://www.drizzle.com/~aboba/IEEE/wireless.pdf
43. WEP Cracks:
    a. To crack the Key:
        i. http://airsnort.sourceforge.net/
        ii. http://sourceforge.net/projects/wepcrack/
    b. To brute force enter into WLAN, select THC-RUT from
        i. http://www.thehackerschoice.com/releases.php
44. WPA Q & A: http://www.wi-fi.org/OpenSection/pdf/Wi-Fi_Protected_Access_QA.pdf
45. WAP Gateway: http://www.mobileways.de/WAP/index.html
46. WAP and imode information: http://www.eurotechnology.com
47. 3G security; Security threats and requirements: http://www.3gpp.org/ftp/Specs/html-info/21133.htm
48. 3G security; Security architecture: http://www.3gpp.org/ftp/Specs/html-info/33102.htm
49. 3GPP numbering scheme: http://www.3gpp.org/specs/numbering.htm
50. 3GPP status list: http://www.3gpp.org/specs/specs.htm
51. 3GPP releases and phases: http://www.3gpp.org/specs/releases.htm
52. Handbook of Information Security Management, (Imprint: Auerbach Publications), (Publisher: CRC Press LLC), Authors: Micki Krause, Harold F. Tipton, ISBN: 0849399475, 1999 Edition.
53. Lehr, W. and L.W. McKnight, 'Wireless Internet Access: 3G vs. WiFi?', August 2002
54. Salkintzis, A.K., C. Fors, R. Pazhyannur, 'WLAN – GPRS Integration For Next-Generation Mobile Data Networks', *IEEE Wireless Communications* (2002), P.112-124
55. Project WLAN rollout at university campus: www.dto.tudelft.nl
56. WLAN authentication methods: www.surfnet.nl
57. IEEE 802.11 Specification: http://standards.ieee.org/getieee802/802.11.html
58. 3GPP Technical specification group working methods:
    http://www.3gpp.org/ftp/Specs/html-info/21900.htm
59. Article: Analog vs Digital cellphones:
    http://www.telecom.globalsources.com/MAGAZINE/TS/0209/ANALOG.HTM
60. Article: Fingerprint security
    http://www.pcworld.com/news/article/0,aid,109597,00.asp
61. NTT DoCoMo i-mode Service Guideline
    http://64.56.185.29/i-mode/introducing/guideline/guideline.html