TOWARDS AUTHENTICATION USING MOBILE DEVICES

An Investigation of the Prerequisites

E. Weippl, W. Essmayr, F. Gruber, W. Stockner, T. Trenker
Software Competence Center Hagenberg

Abstract: In this paper we show how mobile devices can be used as authentication tokens. We highlight the prerequisites such as mobile device security and mobile communication security. We elaborate on already existing solutions and on what issues in the context of security remain to be addressed. Beside the comprehensive overview, our main contribution is to explain how the different characteristics of wireless communication can be abstracted. Based on this abstraction an implementation of mobile authentication is transparent both to the application programmer and to the end users.

Key words: security, mobility, authentication

1. INTRODUCTION

Business analysts predict great strategic and technical prospects to upcoming mobile business applications using short distance as well as wide area wireless communication facilities. Among others, the most striking benefit is that information may "really" be accessed at any time, anywhere, and with any device, available.

A very promising service that can be delivered to mobile users is that of authentication - referred to as mobile authentication. Since mobile devices are portable, personal, useful, and valuable, users tend to carry them everywhere they go. A number of applications are feasible based on mobile authentication such as login, logout, locking, and unlocking a computer or signing in on attendance lists etc. However, the acceptance of such mobile services will strongly depend on the degree of trust the user can have in mobile and wireless facilities thus making their security decisive for mobile

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35612-9_23

B. Jerman-Blaži et al. (eds.), *Advanced Communications and Multimedia Security*

authentication. In this paper we investigate the prerequisites for mobile authentication.

2. PROPERTIES AND APPLICABILITY OF MOBILE DEVICES FOR SECURITY SERVICES

This section discusses the main characteristics that are relevant when using these mobile devices for security services.

2.1 Mobility

Since devices are small and portable users tend to carry them along most of the time, at work and after office hours. This makes the devices an ideal platform to implement additional security services such as authentication. Unlike with key cards users are not required to carry an additional item that serves one purpose only. Beside all the functionality available, the devices are programmable. Therefore various degrees of authenticity can be implemented offering also protection of the user's privacy.

Privacy concerns are especially important as mobile devices connect to other services using wireless communication. Wide area wireless networks allow users to use Web services independent of their current location. Wireless LANs (WLANs) or Bluetooth allow to connect to local services, which makes it well suited for local authentication services such as unlocking doors or signing in on attendance lists. One drawback of technologies is that it is difficult to establish the intent of the user merely by his/her presence.

2.2 Value

Mobile devices are rather expensive. They are valuable not only because of the price of the device but also because they store private data. Nonetheless most devices lack effective authentication mechanisms; anyone who possesses the device can use it. Cell phones use PINs but they are often only required when switching the phone on. In most cases the devices will constantly remain on and thus users are never authenticated to the mobile device again.

Since the devices are valuable people always carry them along; thus the devices are extremely well suited for applications that identify people to services.

2.3 Personal Property

As previously mentioned cell phones and PDAs are personal devices that people do not share. Unlike [Eckert, 2000] we therefore do not believe that multi-user support on PDAs is essential. In future such devices could supersede traditional keys or ATM cards. To guarantee that mobile devices really remain personal, strong and convenient authentication towards the device is required. This paper does not address the issue of how a user authenticates to the device but how the device can be used to authenticate the user to other services.

2.4 Security and Usability

Based on the aforementioned arguments, mobile authentication promises to increase both usability and security. Users of mobile devices should not have to be concerned about and should be safe from threats while using their device for secure actions. Furthermore, an increased subjective perception of security will foster a broader spectrum of use cases and thus also increase usability.

Moreover, usability will inevitably be increased, as users will not have to carry additional devices; instead, their mobile devices will also perform authentication services. Generally it does not depend on what kind of device is used. Programmable devices will have a greater chance of fulfilling the need of providing different levels of security.

Security obviously involves both the device itself and the (wireless) connection of the device to its environment. In the following sections we first elaborate on the security of the mobile device and second on wireless communication security.

3. MOBILE DEVICE SECURITY

Figure 1 illustrates a typical mobile environment in which mobile devices are used for conducting mobile business.

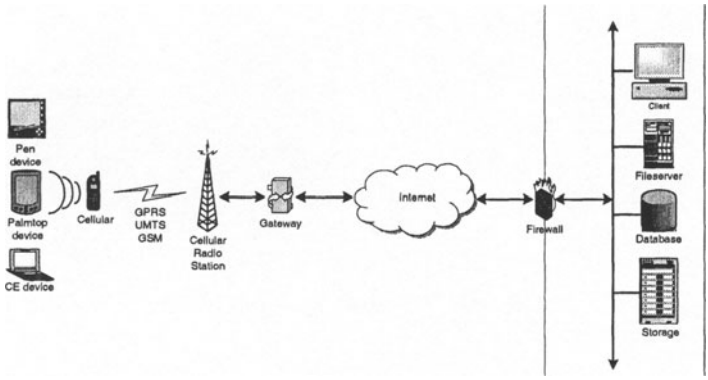

Figure 1: Typical Mobile Business Environment

The mobile business environment includes mobile devices, communication infrastructure, multiple wireless communication protocols, Internet related communication protocols, and different (corporate) networks with all its components such as firewalls, backend systems, or client applications. Within the scope of this paper we do not concentrate on corporate network or Internet related security issues, since these topics are well covered in literature. Instead, we provide an overview of the prerequisites for our vision of mobile authentication as described in section 5, namely, mobile device security (covered in the remainder of this section) and wireless communication security (covered in section 4).

3.1 Security Risks of Mobile Devices

The security risks particular to mobile devices result from the typical properties inherent to such devices, namely, they are personal, portable, have limited resources and are used for roaming through networks with different levels of trust.

Mobile devices are felt to be highly personal equipment inducing their users to have increased trust and manage confidential private and corporate information or even conduct security relevant actions like payment, for instance.

The portability makes mobile devices subject to loss or theft. If a mobile device has been stolen or lost, unauthorized individuals may gain direct access to the device's resources. Furthermore, the identity of the device's owner may be claimed when roaming through the owner's networks and the resources there might be exploited. In the worst case, devices could be faked

and accidentally returned to the user who from now on unconsciously delivers valuable information to the potential attacker.

The limited resources of mobile devices increase the probability of denial-of-service risks. For instance, if a cell phone can be used for authentication, a power failure suffices to prevent legitimate access. Unfortunately, the current practice when addressing resource limitations is to ignore well-known security concepts. For instance, to empower WML scripts, implementations lack the established sandbox model and downloaded scripts can access local resources without restriction [Gosh, 2001].

Moreover, roaming through different cells and networks with varying degrees of trust and different security policies renders current techniques such as SSL and even protocols specifically designed for mobile use (e.g. WTLS) vulnerable to new forms of attack [Gosh, 2001]. The mobile device has to be compliant to multiple security policies and frequently adapt to different trust levels found within the visited networks. Furthermore, the user might be subject of undesired tracing and profiling due to the location awareness of particular devices, which can lead to substantial privacy problems.

3.2 Security Services

To address the security risks identified within the previous sub-section, a number of security services are used. Within an industry project we searched for security enhancements available for PalmOS and WinCE devices according to our partners' requirements.

3.2.1 Physical Protection

Steel cables, holsters, etc. to fix the mobile device on a person's body or e.g. a computer chassis provide protection against theft, loss and damage. They allow attaching the mobile device to a neck strap or key chain. Several products for physical protection of Palm handheld devices are available such as Bond, e-Holster, or PDA Saver.

3.2.2 Authentication

Authentication on the mobile device establishes the identity of the user to the particular mobile device. Most of the available mobile devices only provide basic authentication using personal identification numbers (PINs) or passwords. Frequently, users may also turn off authentication for their convenience. Thus, more convenient and more secure authentication

mechanisms will be needed when using the mobile device for mobile authentication as suggested in this paper. These mechanisms should at least be based on something the user *has* (e.g. a smart card that must be inserted into the mobile device for critical actions) or something the user *is* (exploiting a biometric signature such as a fingerprint for authentication).

At least some products are yet available that provide prominent PDAs with enhanced authentication features. For instance, PDASecure (PalmOS) and Sing-On (PalmOS, WinCE), that enable password encryption or PINPrint (PalmOS, WinCE) that provide fingerprint authentication.

3.2.3 Access Control

Based on a legitimate identity proved by authentication, the mobile device should further restrict access to its resources. Although a PDA will mostly be used only by its owner, there might also be the need to share such devices in some cases. Most of the mobile devices do not provide any access control at all. For PalmOS, some products (e.g. Enforcer, Restrictor) are available that provide profiles to limit access to specific data.

3.2.4 On-Device Encryption

Authentication and access controls may not suffice to protect highly sensitive corporate or private data stored on the mobile device. It is often necessary to provide a redundant level of protection by encrypting all or parts of the devices data storage. Several products can be installed in order to get on-device encryption, such as JawzDataGator or MemoSafe for PalmOS, and CryptoGrapher for confidential information kept on flash cards, PocketLock for encrypting documents, or seNTry 2020 for protecting volumes, files, folders and programs all of which can be used on WinCE devices.

3.2.5 Anti-Virus issues

Anti-virus software should be used to protect both the handheld and the (corporate) network against malicious software. Products that support anti-virus protection for mobile devices are, for instance, InoculateIT and Palm Scanner for PalmOS respectively VirusScan, and Anti-Virus for WinCE.

3.2.6 Application Security

It is not enough to secure the mobile device itself and the wireless communication protocols as reported in section 4. Also the applications

running on the mobile device have to be secured. Applications should be designed enabling authentication, authorization, access-control, and encryption mechanisms that can operate across platforms and technology domains. At least some products supporting basic cryptographic algorithms and applied cryptographic mechanisms like SSL, for instance, are available (e.g. Security Toolkit for PalmOS or Security Builder for PalmOS and WinCE).

4. WIRELESS COMMUNICATION SECURITY

Security does not end at the device, thus a general security concept including wireless media must be developed. In the last section we described the security aspects of the mobile device itself. This section describes in short terms special security threats when dealing with wireless communication technologies. In a subsection we will summarize the security aspects, which the existing wireless technologies have already built-in. Moreover we will show potential weaknesses of each communication technology.

4.1 Wireless Security Threats

The following security threats are not particularly special for mobile computing, but with wireless communication technologies certain new aspects arise, which we will describe in the following enumeration (compare [SANS, 2001] and [Eckert, 2000]).

- Denial of Service (DoS) occurs when an adversary causes a system or a network to become unavailable to legitimate users or causes services to be interrupted or delayed. A wireless DoS attack could be the scenario, where an external signal jams the wireless channel. Up to now there is little that can be done to keep a serious adversary from mounting a DoS attack. A possible solution is to keep external persons away from the signal coverage, but this is rarely realizable.
- Interception has more than one meaning. An external user can masquerade himself as a legitimate user and therefore receive internal or confidential data. Also the data stream itself can be intercepted and decrypted for the purpose of disclosing private information. Therefore some form of strong encryption as well as authentication is necessary to protect the signals coverage area.
- Manipulation means that data can be modified on a system or during transmission. An example would be the insertion of a Trojan horse or a

virus on a computer device. Protection of access to the network and its attached systems is one means of avoiding manipulation.
- Masquerading refers to claiming an authorized user while actually being a malicious external source. Strong authentication is required to avoid masquerade attacks.
- Repudiation is when a user denies having performed an action on the network. Strong authentication, integrity assurance methods and digital signatures can minimize this security threat.

4.2 Wireless Communication Security

In this section we describe how the various communication technologies try to overcome the potential security issues mentioned above.

4.2.1 Wireless LAN (IEEE 802.11)

Wireless LAN (WLAN) specifies two security services; the authentication and the privacy service. Mostly these services are handled by the Wired Equivalency Privacy (WEP). WEP is based on the RC4 encryption algorithm developed by Ron Rivest at MIT for RSA data security [RSA, 2002]. RC4 is a strong encryption algorithm used in many commercial products. The key management, needed for the en/decryption is not standardized in WLAN but two key-lengths have come up: 40bit keys for export controlled applications and 128bit keys for strong encryption. Some papers on the uncertainty of the WEP standard have been published [Borisov, 2001] but [Kelly, 2001] from the 802.11 standardization committee responded in the following way: WEP was not intended to give more protection than a physically protected (i.e. wired) LAN. So WEP is not a complete security solution and additional security mechanisms like end-to-end encryption, Virtual Private Networks (VPNs) etc. need to be provided.

4.2.2 Bluetooth

In the Bluetooth Generic Access Profile (GAP, see Specification [Bluetooth, 2002]) the bed-rock on which all other profiles are based, 3 security modes are defined:
- 1: non-secure
- 2: service level enforced security
- 3: link level enforced security

In security mode 1 a device will not initiate any security - this is the non-secure mode. In security mode 2 the Bluetooth device initiates security procedures *after* the channel is established (at the higher layers), while in

security mode 3 the Bluetooth device initiates security procedures *before* the channel is established (at the lower layers). At the same time two possibilities exist for the device's access to services: "trusted device" and "untrusted device". The trusted devices have unrestricted access to all services. The untrusted device does not have fixed relationships and its access to services is limited. For services, 3 security levels are defined: services that require authorization and authentication, services that require authentication only and services that are open to all devices. These levels of access are obviously based on the results of the security mechanisms themselves so they are not really of interest to us. Thus will concentrate on the two areas where the security mechanisms are implemented: the service level and the link level. Details on how security is handled in these levels can be found in [Palowireless, 2001].

Though Bluetooth has a large concern on security, Bluetooth is not free from vulnerabilities, what is shown in following papers and web sites [Vainio, 2000; Sutherland, 2000] and so additional security and encryption must be provided for an acceptably secure data transmission.

4.2.3 Infrared Media

The infrared communication technology does not provide any security mechanism incorporated into the transmission protocol. The standardization committee, the Infrared Data Association (IrDA, [IRDA, 2002]) justifies this with the very limited spatial range of infrared media and with the required sight-to-sight connection of the involved devices.

4.2.4 Wireless Wide Area Networks

The security of digital wireless WANs (GSM, GPRS, HSCSD, etc.) is described in this section in an abstract manner, taken from [SCCH, 2001].

Following [Walke, 2000] and [Hansmann et al., 2001], the user of a network must on the one hand be identified for billing purposes; on the other hand the transmitted data must be protected for privacy reasons. For digital wireless WANs cryptographic methods are used to implement the security features.

The first level of security concerns the mobile device. When a device is manufactured, a unique ID is assigned to each mobile device. When a user wants to access a network, first the ID of the used device is sent to the network. A device can be classified into three categories:

- White-listed: Access is allowed,
- Gray-listed: Access is allowed, but mobile device is under observation, and

- Black-listed: Access is not allowed (e.g., mobile device is reported stolen)

In a next step the user that wants to access a network is identified. Each subscriber to a network is issued a unique security key and a security algorithm. Both are stored in the system and in the mobile device of the user. If a user wants to access a network, the security system of the network sends a random number to the mobile device. The mobile device encrypts the random number with its security key and algorithm and sends the encrypted number back to the network. The security system of the network encrypts the random number itself and compares the result with the number sent by the mobile device. If both numbers are equal, user authentication succeeded. Using this concept the security key is never sent over the network.

The transmission of data in a digital wireless WAN is encrypted as well. When a connection is established, a random session key is generated. With this session key and a security algorithm, a security key is generated. With this security key and another security algorithm the data is encrypted. A different session key is generated for each connection and as a result a different security key is used for each connection to encrypt the transmitted data.

However, these security mechanisms are not sufficient since, for instance, GSM can easily be intercepted by externals as described in [Pesonen, 1999].

5. MOBILE AUTHENTICATION

In this section we describe our vision of using mobile devices for authentication purposes.

Authentication is the process of establishing the identity of one party to another [Sandhu&Samarati, 1996]. Authentication verifies the (claimed) *identity* of a user (or a process on behalf of a user) using a particular *identifier* that has to be provided by the user or the process. Well-known types of identities/identifiers are user name/password, certificate/digital signature, or biometric features that do not necessarily require claiming the identity in advance.

We then call authentication to be mobile, if the following criteria hold:

a) The same identity can be used for any service.
b) The same identifier is always available.
c) The same identifier is always applicable.

Following these criteria, authentication based on "what a user knows" (e.g. passwords) is not necessarily mobile, since it is not the same identity that can be used for different services (criterion a). In fact, a user has to have

a different account for every service although the account's name could be equal. Furthermore, authentication based on "what a user is" (biometric approaches) is also not necessarily mobile, though the same identifier is always available (criterion b) but not always applicable (criterion c), since biometric interfaces are not standard equipment, yet.

Hence, we specifically concentrate on mobile tokens ("what a user has"), which further allows us to extend basic authentication in order to provide services such as pseudonymous or anonymous authentication (compare section 5.1). These advanced services have to be implemented on the user's device (the token). On the one hand, if biometric authentication was used, a user cannot authenticate using multiple identities in order to foster privacy. On the other hand, even though password based approaches would allow using different pseudonymous the user has to remember all user name / password combinations – an extremely cumbersome process.

Based on mobile tokens, we envision the following scenario for mobile authentication services: we assume a token that is highly portable and personally valuable to the user (e.g. a mobile phone) and a short-range wireless communication technology with ad-hoc properties that is becoming a standard on nearly any kind of mobile and stationary devices (e.g. Infrared, Bluetooth). The mobile phone serves as the token holding the identifier for proving one's identity.

5.1 Degrees of Security

Different applications may require different degrees of security regarding mobile authentication. In the following, we describe simple identification, identification with authentication, pseudonymous authentication, and anonymous authentication.

Mobile identification is a service that provides identification but no authentication. Thus, security requirements are very low. This service is useful to e.g. automatically sign in on attendance lists, which traditionally does not require verifying the identity that someone claims to have.

Mobile authentication is required in cases when a service has to be reasonably sure about the correctness of the identity of the accessing person. For instance, when a computer screen should be unlocked the identity claimed by the user has to be checked.

Mobile pseudonymous authentication can be used in situations when a person wants to identify with a fake name but wants to reuse the same name every time he or she uses the same service. For different services, different identities are claimed to prohibit profiling across services. Other people should not be able to claim the (fake) identity. Therefore authentication is required.

Mobile anonymous authentication allows a user to remain anonymous even if the service requires authentication. For instance, on the Web many services require identification (e.g. username) and some sort of authentication such as a password that is emailed to an existing email account; however, since users want to protect their privacy they will want to generate anonymous accounts automatically.

5.2 Realization Issues

We identified a number of issues when starting pilot applications on mobile authentication. The issues are user/device binding, use of communication protocol features, user intention, multiple devices in place, and un-intentional tracking as explained below.

We assume that a mobile device represents a user based on an a-priori authentication between the device and the user. Mobile devices can then be identified by their device name. Unfortunately, the device name can easily be changed by the user and therefore provides no assurance that the device really is the device it claims to be. However, for simply identifying devices the device name suffices. Furthermore, the identifier used for mobile authentication has to be securely stored on the mobile device. The facilities provided by current mobile devices are however insufficient and the topic has to be further researched.

Depending on the wireless technology used it is feasible to employ security mechanisms provided by the communication protocol itself. For instance, Bluetooth supports three different levels of security. Bluetooth devices can authenticate using a 128bit key – the highest level offered by the protocol itself. Infrared, however, does not support any form of authentication. It is therefore necessary to implement all security features required for authentication on top of the protocol. To abstract the different levels of security intrinsically provided by the different wireless protocols we implement an API that offers two basic services: (1) registering a new user and (2) un-registering users. The API hides the different ways in which the registration is performed from the programmer so that the programmer does not need to be aware of which wireless technology is employed.

The user's intention to authenticate to a particular service may be difficult to recognize, also depending on the underlying communication protocol. Using Infrared, for instance, the approach could be that the user registers by establishing a line-of-sight connection. The next time he establishes a connection again he is unregistered. Connecting yet another time would register again etc. Bluetooth is a protocol that does not require a line-of-sight connection. It is therefore difficult to establish whether a user truly intended an action. For instance, by simply passing by a computer a

user does not necessarily want to log in. Therefore, the authentication process has to work differently. One approach could be that as soon as the user enters the area he is authenticated; leaving the area he automatically unregisters. No specific action is required. This, however, may cause a problem because the user gave no explicit consent to authentication when registering. If this consent is required, the mobile device should not automatically register the user but instead display a dialog asking the user whether he wants to authenticate or not.

Knowing what the user really intends to do – by explicitly asking for his consent – is especially important in settings where multiple devices are located in one place. For instance, when a user enters a room he might want to log into a computer but since the location data provided by some technologies (e.g. Bluetooth) is not detailed enough it is impossible to know which computer the user approaches. Moreover, he might also decide not to use a computer at all.

A user carrying a Bluetooth device can be tracked and identified. We envision some method to protect the user's privacy – he should be able to choose which kind of devices or services may observe his presence and which not. Furthermore, there are also services that do not require a username. In these cases no pseudonyms have to be generated and one would assume that by simply establishing a connection the user remains anonymous. However, this is not the case as wireless technologies such as Bluetooth automatically authenticate whenever they establish a connection. Even though the service may not require a login, the user can still be traced because the authentication information is available at the access node. The basic idea to avoid this form of tracking is to regularly change the device address. This prevents the profiling of users that connect to access nodes.

6. CONCLUSIONS AND OUTLOOK

In this paper, we gave an overview of security in mobile communication and mobile device security. Having identified shortcomings we elaborated on the requirements for mobile authentication, gave a definition of mobile authentication and showed which services can be offered based on mobile authentication. Our approach is based on using mobile devices that possess processing capabilities in order to implement services such as mobile authentication and mobile pseudonymous authentication.

The main contribution of this paper is to highlight the rationale for such an approach, to identify the prerequisites, and to argue that a relatively simple API suffices to provide such services. This approach has its advantages over previous forms by relieving the application developer from

the burden of having to design, implement, and test authentication mechanisms.

However, two major obstacles were identified that need to be addressed in future efforts in this direction. Firstly, the security of the mobile device itself is not sufficient; this lack of security jeopardizes the reliability of the whole process of authentication. Second, even though Bluetooth is a well-defined standard, integrating it into applications still remains a challenge. We experienced that many program-level APIs do not work reliably with certain devices or some Bluetooth devices do not seem to be supported at all. Moreover, even if a connection can be established it is not sure that this connection can be reestablished. In some cases we had success rates well below 10% without any obvious cause.

Once the aforementioned issues have been addressed, we are convinced that mobile authentication will be useful to implement e.g. mobile signatures scenarios. *Mobile signatures* are digital signatures that are applied to documents displayed on the mobile device. Unlike traditional digital signatures, the mobile device is used as a secure viewer. Therefore the user does not have to trust the external viewer but can be sure that the documents he or she signs are correctly displayed.

REFERENCES

[Bluetooth, 2002] Bluetooth SIG Home page, http://www.bluetooth.org, last accessed on March 6, 2002.

[Borisov, 2001] Borisov, Goldberg, Wagner, Intercepting Mobile Communications: The Insecurity of 802.11, http://www.isaac.cs.berkely.edu/isaac/mobicom.pdf, last accessed on March 6, 2002.

[Eckert, 2000] Eckert, Mobile Devices in E-Business – New Opportunities and New Risks, Proceedings of SIS 2000, Zurich, 2000.

[Gosh, 2001]Ghosh, K.A., and Swaminatha, T.M. Software security and privacy risks in mobile e-commerce, Communications of the ACM, Volume 44 (2), Feb 2001, pp 51-57

[Hansmann et al., 2001] Hansmann, Merk, Nicklous, Stober, Pervasive Computing-Handbook, Springer Verlag, 2001.

[IRDA, 2002] The Infrared Data Association, http://www.irda.org, accessed March 6, 2002.

[Kelly, 2001] Kelly, Chair of IEEE 802.11 Responds to WEP Security Flaws, February 15, 2001, http://slashdot.org/articles/01/02/15/1745204.shtml, last accessed on March 6, 2002.

[Microsoft, 2001] Securing the handheld environment – An enterprise Perspective, White Paper, Microsoft, 2001, http://www.microsoft.com/mobile/enterprise/papers/security.asp (last visited Feb 19, 2002);

[Palm, 2001] Pocket PC Security, White Paper, Palm, 2001, http://www.palm.com/enterprise/resources/securing/index.html (last visited Feb 19, 2002);

[Palowireless, 2001] Mc Daid, Bluetooth Security, Parts 1, 2, and 3, http://www.palowireless.com/bluearticle/cc1_security1.asp, http://www.palowireless.com/bluearticle/cc1_security2.asp,

http://www.palowireless.com/bluearticle/cc1_security3.asp, last accessed on March 6, 2002.

[Pesonen, 1999] Pesonen L., GSM Interception, Helsinki University of Technology, Dpt. Of Computer Science and Engineering, November 21, 1999, last accessed on March 6, 2002.

[RSA, 2002] RSA Security Inc., http://www.rsa.com, last accessed on March 6, 2002.

[SANS, 2001] Robert E. Mahan, Security in Wireless Networks, SANS Institue, http://rr.sans.org/wireless/wireless_net3.php, last visited:March 6, 2002.

[Sandhu&Samarati, 1996] Sandhu R.S., Samarati P. Authentication, Access Control, and Audit. ACM Computing Surveys, Vol. 28, No. 1, March 1996.

[SCCH, 2001] Gruber, Wolfmaier, State of the Art in Wireless Communication, Technical Report SCCH-TR-0171, Software Competence Center Hagenberg, www.scch.at, 2001.

[Sutherland, 2000], Sutherland, Bluetooth Security: An Oxymoren?, http://www.mcommercetimes.com/Technology/41, last accessed on March 6, 2002.

[Vainio, 2000] Vainio J., Bluetooth Security, May 25, 2000, http://www.niksula.cs.hut.fi/~jiitv/bluesec.html, last accessed on March 6, 2002.

[Walke, 2000] Walke, Mobilfunknetze und ihre Protokolle – Band 1, B. G. Teubner Verlag, Stuttgart, 2000].