UOC
IN3 Internet Interdisciplinary Institute
www.uoc.edu

PhD paper

Strong Personal Authentication Scheme Using Mobile Technology

Josep Prieto (jprieto@uoc.edu)
Professor within the department of Computer Science and Multimedia (UOC)
Director of the Technical Engineering for Information Systems programme

PhD papers TD03-007
PhD programme on Information and Knowledge Society
Research seminar on Information and Communication Technologies
Paper Director: Jordi Herrera-Joancomartí
Published on: June 2003
Internet Interdisciplinary Institute (IN3): http://www.uoc.edu/in3/eng/index.htm

ABSTRACT

Security is a major concern in computer networks. Authentication is possibly the most important factor since achieving privacy and integrity may make no sense without a guarantee of receiver identity. Cryptographic strong authentication protocols are well known but the real problem is to protect secret information, such as shared or private keys, used in these protocols. In regard to the problem of smart card availability (devices and readers), we propose a mobile architecture using more deployed technologies such as cellular phones or PDAs and wireless personal area networks (WPAN) like Bluetooth. The mobile device (cellular phones or PDAs) acts as a smart card, storing private information and performing cryptographic operations while WPANs replace smart card readers. The risk of insecure wireless networks inclusion is studied and solved using suitable authentication protocols.

KEYWORDS

Authentication, mobile devices, wireless networks, Bluetooth, cryptography

SUMMARY

To cite this document, you could use the following reference:

PRIETO, Josep (2003). Strong Personal Authentication Scheme Using Mobile Technology [online PhD paper]. IN3 : UOC. (PhD papers; TD03-007). [Date of citation: dd/mm/aa].
<http://www.uoc.edu/in3/dt/20273/index.html>

Strong Personal Authentication Using Mobile Devices and Wireless Networks

Josep Prieto-Blázquez*

Universitat Oberta de Catalunya
Av. Tibidabo 39-43
08035 Barcelona, Catalonia, Spain
jprieto@uoc.edu

Abstract. Security is a major concern in computer networks. Authentication is possibly the most important property in a network environment since achieving privacy and integrity may have no sense without the guaranty of the receiver identity. Cryptographic strong authentication protocols are known but the hard problem is to protect secret information, like shared or private keys, used in these protocols. Regarding the problem of smart cards availability (devices and readers) we propose a mobile architecture using more deployed technologies like cellular phones or PDAs and wireless personal area networks (WPAN) like Bluetooth. The mobile device (cellular phones or PDAs) acts as a smart card storing private information and performing cryptographic operations while WPAN replace smart card readers. The risk of insecure wireless networks inclusion is studied and solved using suitable authentication protocols.

Key words: Authentication, mobile devices, wireless networks, Bluetooth, cryptography.

1 Introduction

Security is a major concern in computer networks. Security main goals are the four basic properties: privacy, authentication, integrity and no-repudiation. From those properties, authentication is the most important in a network environment since achieving privacy and integrity may have no sense without the guaranty of the receiver identity.

Technically, authentication can be successfully solved using cryptographic strong authentication protocols [5]. However, the hard problem is how to protect secret information, like shared or private keys, needed in the authentication protocol. A tipical example of this problem can be found when a single computer, in an office, is used by different users to login the intranet. The way private information of every user is stored into the desktop memory often rends useless the strongest authentication protocol. Furthermore, desktops are physically placed in a non-restricted area and then apart from those authorized other people can have physical access.

* This work has been supervised by Prof. Jordi Herrera-Joancomartí

For those reasons, strong personal authentication has been frequently subordinated to trusted devices like smart cards. Smart cards can store and compute authentication protocols offering a high security level. Furthermore, its small size allows the user to control physically the device anytime, anywhere since the smart card can be placed into the user's pocked.

Despite the advantages of smart cards in security field their use as authentication token has not been generalized as expected. The inherent problems of smart cards are, on one hand the standardization of protocols and languages, despite efforts like PC/SC, and on the other hand, the lack of smart card readers in the existing notebooks and desktops.

In this paper we present a mobile architecture that provide strong personal authentication. The key issue is to use a mobile device like a cellular phone or a PDA to store private information and to perform cryptographic operations during the authentication process. Such mobile devices offer the same advantages of smart cards in terms of portability and physical control. However, smart cards are not completely forgiven since their value as a tamper resistant device is still valuable. We solve the connectivity problem encountered with smart cards readers using wireless personal area networks such as Bluetooth [2] or IEEE 802.15 standard [4]. Those technologies allow to connect different mobile and fixed devices within a short physical range.

Enhanced security using wireless networks could seem a contradiction, regarding security flaws found in every new wireless technology. However, wireless networks could be efficiently applied once the security flaws have been analyzed. For instance, some security flaws on wireless networks follow from the use of symmetric cryptography: security problems related with Bluetooth technology derives from the improper assignment of the link key shared by two devices. Symmetric cryptography has been typically used in mobile environments in order to avoid the complex computation needed in public key cryptography. Such computations consume power resources and need hight storage requirements which could be a drawback regarding the constrains of mobile devices. Nevertheless, capabilities of mobile devices have been drastically increased and public key cryptography could be used. For instance, in [11] this fact is pointed out and the paper proposes different public key based protocols suitable for application in third-generation mobile systems like Universal Mobile Telecommunications Service.

On the other hand, wireless networks have already been used to enhance security properties. For instance, in [13] a cellular phone network is used to authenticate users in Internet systems. The main idea is that information of the authentication process is sent and received through the phone wireless network, although the authentication process has been started from and for a PC desktop Internet session. Also in [7] cellular phone networks are used to enhance security in an electronic payment system.

However, the proposals cited above are different to our approach. While we use a WPAN as a substitute of the mobile device connection those schemes use cellular phone networks as a separate communication channel to increase the

security of the system. This fact has the problem of latency, as it is pointed out in [13], since the synchronization of both networks, the wired and the wireless could not be easy to achieve. Another problem of using cellular phone connection refers to legal regularions of the radio frequency band which implies the need of a non-free mobile phone operator. MASPA uses WPAN technology working in the 2.4 GHz unlicenced ISM band.

1.1 Plan of the paper

This paper is organized as follows. Section 2 describes the new Mobile Architecture for Strong Personal Authentication (MASPA). Descriptions of entities and protocols are presented as well as its main properties. In section 3 security of the new architecture is discussed focus mainly in the proper use of insecure WPAN within MASPA. Finally, conclusions are presented in section 4.

2 MASPA - Mobile Architecture for Strong Personal Authentication

In this section we describe an Mobile Architecture for Strong Personal Authentication (MASPA). MASPA is based on different entities, algorithms and protocols. The main entities are the user, the mobile device owned by the user and the access point. For clarity, the names of those entities have been borrowed from a general mobile network, like cellular phone networks. Nevertheless, the specification of each entity is not restricted so an access point could be either a normal PC desktop or an electronic device attached to a lock-door. Although other different entities such as authentication servers or certification authorities can be added to our architecture, for conciseness they are not detailed in this paper.

The protocols used in MASPA architecture are basically the communication protocol and the authentication protocol. The former is the protocol used by the mobile device and the access point to communicate. The latter deals with the authentication process itself.

Since security is a major concern in MASPA, the main algorithms used in the architecture are cryptographic primitives like hash functions, symmetric and asymmetric encryption including digital signatures which are used in the authentication protocol.

The general authentication process is depicted in figure 1. The user that wants to be authenticate by an access point, must carry his personal mobile device. Once the physical distance between the mobile device and the access point is appropriate, the user initiates the authentication process. The authentication process starts with an authorization procedure between the user and his mobile device during which the mobile device checks the user identity. Then, the mobile device and the access point exchange different information using the authentication protocol. The information exchanged is validated using suitable cryptographic algorithms and then the outcome of the authentication process is

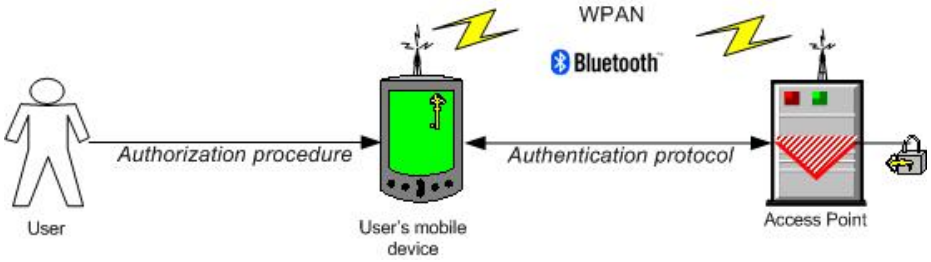

Fig. 1. The general authentication process

either the acceptance of the user identity for the access point or the termination without the acceptance. In fact, the authentication process also generates a symmetric key that can be used to obtain privacy in later communications.

Information between the mobile device and the access point is exchanged through a WPAN. The specific technology used as a WPAN determines the physical distance within the user can initiate an authentication process.

A particular example of MASPA implementation and application could be a user owning a cellular phone which has booth Bluetooth technology and a WAP Identity Module (WIM) [1] that wants to get access to the intranet office through a desktop computer.

In next subsections, more detailed descriptions of each entity and protocol are given.

2.1 The mobile device

The mobile device is the entity that acts for the user. The role of the mobile device is the same of a smart card in a traditional authentication scheme in the sense that it supports the user to store and compute the cryptographic values needed in the authentication process.

The basic properties of the mobile device are the following:

1. The mobile device must provide a limited amount of non-volatile memory.
2. The computational power of the mobile device must allow to execute cryptographic algorithms such as symmetric and public encryption in a reasonable time.
3. The mobile device must be able to transfer data through a WPAN such like Bluetooth.
4. The mobile device should be highly portable in the sense that ideally the user should permanently carry the device.

The first and second properties allow to store secret information into the device and provide a secure and trusted environment where the user can execute his authentication protocol part. In this way, secret information needed in the authentication process, like shared or secret keys, never leaves the mobile device.

The inclusion of a Bluetooth module in different electronic devices (mobile phones, PDAs, notebooks, etc.) starts to be in everyday use. The third property cited above ensures that such communication technology is available in the mobile device so data transfer between the mobile device and the access point is guaranteed.

Security of the mobile device is partly guaranteed by user physical control over his mobile device. Such physical control will become easier if the mobile device is portable as it is suggested in the fourth property. For instance, a PDA suits better the requirements than a notebook.

Examples of mobile device could be a cellular phone or a PDA. New cellular phones already includes a Bluetooth module as well as WAP identification Module (WIM [1]). WIM will implement WTLS Class 3 (mutual authentication) so it will be able to store and perform cryptographic operations as required in first and second properties. PDA are also good candidates for mobile device. New PDAs contains a Bluetooth module and its computer power, memory capacities together with the availability of different operating systems and programming languages makes them more powerful than cellular phones.

2.2 The access point

The access point represents the entity that verifies the identity of the user. In this paper, we present a basic scheme where the whole verification process is performed into and by the access point. Nevertheless, a more decentralized proposal can be obtained by performing the verification process outside the access point, for instance, in an authentication server.

The access point should provide the next features:

1. The access point must be able to store information exchanged during the authentication protocol.
2. Cryptographic computation power of the access point is also assumed in order to execute the authentication protocol.
3. The access point must be provided with the same WPAN technology of the mobile device in order to transfer data between both entities.
4. For *ad-hoc* authentication applications, the access point must be able to store a user profile that fixes the relation between users and their privileges.

Notice that properties are similar to the mobile device ones since the interaction during the authentication process must be ensured. However, portability of the access point is not needed.

The last property stated above anticipate that authentication process can be used to access different services and resources. However, in this paper we focus on a generic authentication process without worry about the final purpose of the authentication.

Examples of access point can be very different. For instance, a desktop computer can be an access point to an intranet network. On the other hand, a electronic lock can also be regarded as an access point to control room physical access. As soon as WPAN technology will be extended to different devices,

authentication using MASPA will increase its possibilities thanks to the wide range of possible access points (vending machines, phone boxes, etc.).

2.3 The communication model

Descriptions of the mobile device and the access point require WPAN technology to connect both entities. MASPA could be implemented in any available WPAN technology. However, for implementation purposes we choose Bluetooth technology as a WPAN. The advantages of such technology are the availability of devices supporting it and the fact that new WPAN standards, like IEEE 802.15, support Bluetooth specifications.

Bluetooth is low cost, low-power, short-range wireless technology designed as a replacement for cables and other short-range technology like IrDA. It operates in personal area range that typically extends up to 10 meters.

The architecture of Bluetooth is a design that has been divided into easily describable independent layers (see figure 2). The Bluetooth Protocol Stack consists basically of three bottom layers (Radio, Baseband and Link Manager Protocol) which are typically implemented in hardware/firmware. Above these layers there is the Logical Link Control and Adaptation Protocol (L2CAP). Such protocol often resides on the Bluetooth module and can directly communicate with the LMP and baseband. The Applications reside above L2CAP.

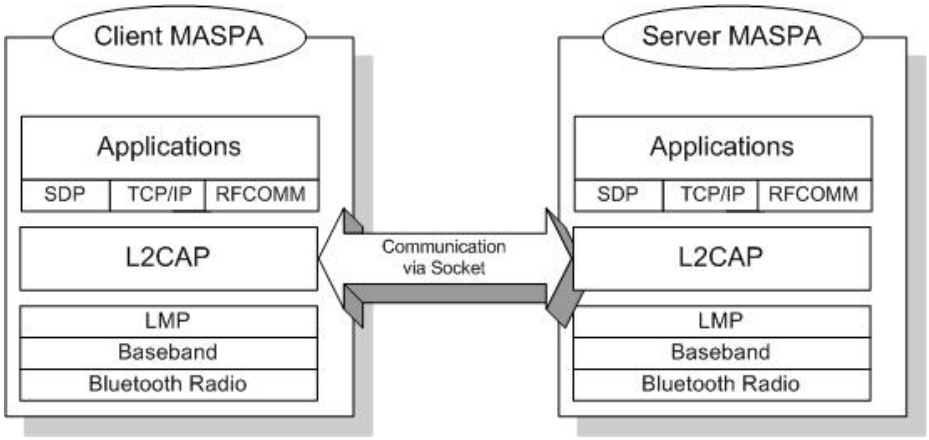

Fig. 2. The Bluetooth protocol stack

L2CAP provides connection-oriented and connectionless data services to upper layer protocols with protocol multiplexing capability, segmentation and reassembly operation, and group abstractions. L2CAP permits higher level protocols and applications to transmit and receive L2CAP data packets up to 64 kilobytes in length.

L2CAP layer is packet-based but follows a communication model based on channels. Channel identifiers (CIDs) are local names representing a logical channel end-point on the device. These channels are used in MASPA to send information between the mobile device and the access point during the authentication protocol.

MASPA can be implemented using Bluez. BlueZ [3] is the official Linux Bluetooth protocol stack. It is an Open Source Project distributed under GNU General Public License (GPL). It provides support for core Bluetooth layers and protocols. The BlueZ protocol stack, shown in figure 3, is interfacing to the Linux socket layer, providing a new address family. BlueZ can be used with USB or Serial interface based Bluetooth devices and additionally it provides a Virtual Host Controller Interface device (VHCI) which can be used to test Bluetooth applications before real Bluetooth devices are used.

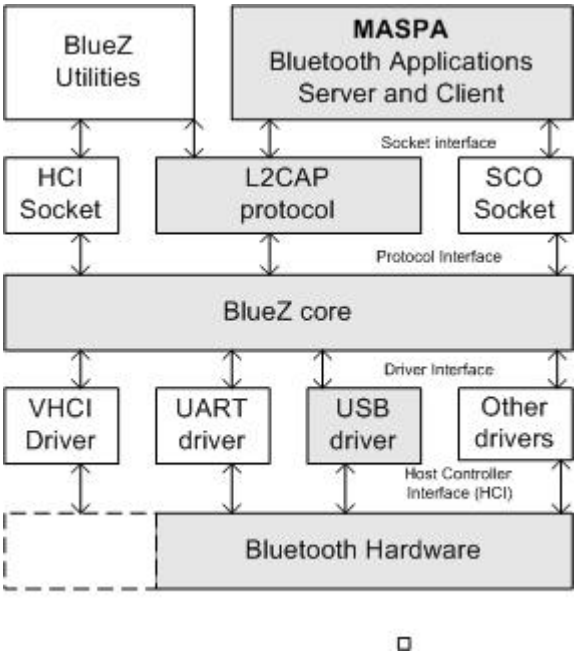

Fig. 3. BlueZ Overview Diagram

Figure 3 also shows that MASPA is placed up to the L2CAP and uses the L2CAP to transfer data to the lower layer protocols that physically send the data to the other Bluetooth device.

2.4 The authorization procedure

The authorization procedure is performed by the user and his mobile device at the beginning of the authentication process. The authorization procedure goal is to ensure that the user having the mobile device is its real owner and that is the owner of the secret information stored into the device.

MASPA uses password-based procedure. The user enters a passphrase into his mobile device and the mobile device verifies the correction of such information.

Although this procedure seems too weak for a strong authentication scheme, notice that smart cards use the same procedure with a four digit PIN. In fact, security is ensured thanks to the physical control of the device as it is pointed out later in Section 3.

2.5 The authentication protocol

The authentication protocol that has been chosen for our architecture is a mutual entity authentication protocol based on the one proposed by Diffie *et alter* [8]. The protocol is a three-pass Diffie-Hellman variant that establishes a shared session key between the mobile device and the access point. Such authentication protocol is one of the candidates described in [11] for mutually authenticate a mobile user and the network in upcoming third-generation mobile systems such as Universal Mobile Telecommunications Service. Then, security requirements (see section 3) and performance criteria for mobile environment are meet.

The authentication protocol as described in [11] is depicted in figure 4.

$$
\begin{aligned}
M \longrightarrow A &: g^{r_m} && (1)\\
A &: K = (g^{r_m})^{r_a}\\
M \longleftarrow A &: g^{r_a}, E_K\{Sig_a(g^{r_a}, g^{r_m})\}, Cert_a && (2)\\
M &: K = (g^{r_m})^{r_a}\\
M \longrightarrow A &: E_K\{Sig_m(g^{r_a}, g^{r_m}), Cert_m\} && (3)
\end{aligned}
$$

Fig. 4. The authentication protocol

This protocol assumes that both the mobile device (M) and the access point (A) have a public key pair $\{PK, SK\}$ related to a public key cryptosystem and a certificate of the public key $Cert$. Subindex are use to identify the owner of each element, so PK_m stands for the public key of the mobile device while r_a is a random number generated by the access point.

In (1), the mobile device takes g a generator of a multiplicative group in which discrete logarithms are hard to compute. Then it generates a random value r_m and then g^{r_m} is send to the access point. The access point then computes a symmetric key $K = (g^{r_m})^{r_a}$ using a random value r_a. In step (2) the access

point computes g^{r_a} and signs g^{r_a}, g^{r_m} with his private key SK_a. The resulted signature is encrypted using a symmetric algorithm with key K generated in step (1). The value g^{r_a} together with the certificate of the access point $Cert_a$ and the encrypted value of the signature is sent to the mobile device. Then the mobile device can compute the symmetric key K, he obtains the digital signature and validates it. Finally, in step (3) the mobile device sings g^{r_a}, g^{r_m} with his private key SK_m and encrypts the resulted signature and the certificate $Cert_m$ with the shared key K. The inclusion of the certificate into the cipher text offers anonymity for the mobile device in front of eventual eavesdropping of the authentication messages.

Notice that the authentication protocol implicity assumes the use of different cryptographic algorithms. For instance, both the mobile device and the access point must be able to perform and verify digital signatures (and therefore hash functions must be used) and a symmetric key encryption algorithm is also used. Properties of the mobile device and the access point have already been stated to allow such operations.

3 Security assessment

In this section we analyze the security properties and possible vulnerabilities of the architecture proposed in Section 2

3.1 The authentication protocol

The adoption of protocol described in section 2.5 satisfies different security properties as it is pointed out in [11].

It provides mutual authentication since both the mobile device and the access point must authenticate each other through their digital signatures and certificates. Furthermore, the authentication protocol generates a shared key between both parties. The key generation is performed by mutual agreement so joint key control, mutual implicit key authentication and mutual assurance of key freshness is provided. Finally, confidentiality of the user identity is provided against and eavesdropping attack, since user identity information is encrypted with the shared key before its transmission.

The security properties described above prevents different possible attacks such as source substitution attack, signer verification attack, content verification attack and codebook attack, among others (see [11] for details).

3.2 Using insecure wireless network technology

The architecture proposed in Section 2 uses wireless network technology to connect the mobile device and the access point. The insecurity of such technologies has been pointed out in different papers [6,12,14]. However, MASPA architecture uses wireless personal area networks only as a transmission channel and as we

will show later the flaws encountered in this technologies does not affect MASPA security.

Since MASPA description of Section 2 is based on Bluetooth technology, we analyze here the Bluetooth security mechanisms and why the known attacks over these mechanisms do not affect our architecture.

In Bluetooth Generic Access Profile, the Bluetooth security is divided into three modes:

- Security Mode 1: non-secure.
- Security Mode 2: service level security
- Security Mode 3: link level security

Three main vulnerabilities are pointed out in the second and third security modes where security is added. The first flaw refers to eavesdropping and impersonation due to the key management implementation. The second one makes possible an attack in which the attacker is able to identify and determine the geographic location of victim devices. Finally, the third vulnerability refers cipher robustness which weaken confidentiality. (see [12,14] for more details).

MASPA architecture is able to use Bluetooth technology with Security Mode 1 (no security is added) since the authentication protocol itself have its own mechanism to obtain security properties (see Section 3.1). Then, using Security Mode 1 the vulnerabilities described above can be leaved out since no protection is added and then vulnerabilities of such security modes does not affect our authentication process.

Properties of Security Mode 2 and 3 are basically the same and the main difference is when they are applied. While in Mode 2 security restrictions are applied at service level once the devices are already connected, Mode 3 applies the security constrains at link level before connection takes place. Both security modes try to offer privacy, authentication and integrity.

Nevertheless, the authentication protocol described in section 2.5 includes its own mechanisms to obtain those properties and then Bluetooth Mode 2 or 3 are not need. Privacy is achieve in the authentication protocol thanks to the symmetric encryption algorithm with the shared key exchanged. Integrity is obtained using digital signatures. Authentication itself is the purpose of the protocol and digital signatures help to obtain.

3.3 The authorization procedure

The authorization procedure is the link between the user and his mobile device. It is performed during the authentication process and ensures that the user that performs the authentication process is indeed the owner of the mobile device and then the owner of the secret information used during the authentication process.

This is the weakest step of the authentication process since the security of the system can be compromised by a weak chosen passphrase. However, in a practical environment, the mobile device is almost a user extension since people always carries his cellular phone or PDA everywhere. Such physical control makes

the attack difficult since physical access to the device is not ease without user permission.

To increase security in the authorization procedure, biometric technology could be used. However, since MASPA's main goal is to avoid the lack of smart card devices and readers, it has no sense to include biometric technology in our architecture because deployment of such technology is even lower than smart cards. Furthermore, as it is pointed out in [10] the combination of biometrics and access control is not so simple.

Parasitic authentication [9] could also strengthen the link between the user and his mobile device. The user delegates his authorization procedure to another small, portable secondary device which he carries (like an earring or necklace). Nevertheless, such technology seems too far from practical.

4 Conclusions

In this paper we have presented a Mobile Architecture for Strong Personal Authentication (MASPA). The authentication process is performed using a mobile device and wireless personal area networks instead of smart cards (devices and readers). Such technologies have the advantages of fast deployment, in the case of wireless personal area networks (Bluetooth), and already extended use in the case of mobile devices (cellular phones and PDAs). These advantages imply our authentication scheme relays only on hardware devices already owned by the potential users. This is an interesting feature for MASPA deployment since only software modifications of the existing hardware devices are needed.

The scheme proposed relays on a strong authentication algorithm which uses public and symmetric cryptography. Since security is a major concern in an authentication process, wireless networks has been accurately analyze before their inclusion into MASPA architecture since different security flaws have been encountered in such technology.

MASPA applications include a wide range of possibilities. For example, authentication in a network computer environment, access to a specific contents (regarding Digital Management Rights applications), accessibility to corporative applications or automatic vending machines, among others.

Acknowledgements

This work is partially supported by the Spanish MCYT and the FEDER funds under grant no. TIC2001-0633-C03-03 STREAMOBILE.

References

1. Wireless application protocol identity module specification, 2000. `http://www1.wapforum.org/tech/documents/WAP-198-WIM-20000218-a.pdf`.
2. The Bluetooth specification, v.1.1, 2001. `http://www.bluetooth.com/dev/specifications.asp`.

3. Official Linux Bluetooth protocol stack, 2001. `http://bluez.sourceforge.net/`.
4. IEEE Std 802.15.1, June 2002. `http://ieee802.org/15/pub/TG1.html`.
5. P.C. van Oorschot A.J. Menezes and S.A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, October 1996.
6. N. Borisov, I. Goldberg, and D. Wagner. Intercepting mobile communications: The insecurity of 802.11. pages 180–188, July 16–21 2001.
7. J. Claessens, B. Preneel, and J. Vandewalle. Combining world wide web and wireless security. In *Proceedings of the IFIP I-NetSec. Advances in Network and Distributed Systems Security*, pages 153–171, Leuven, Belgium, November 2001. Kuwer Academic Publishers.
8. W. Diffie, P. C. van Oorschot, and M. J. Wiener. Authentication and authenticated key exchanges. *Designs, Codes and Cryptography*, 2(2):107–125, June 1992.
9. T. Ebringer, P. Thorne, and Y. Zheng. Parasitic authentication to protect your E-wallet. *Computer*, 33(10):54–60, October 2000.
10. F. K. Gal Hachez and J.J. Quisquater. Biometrics, access control, smart cards: a not so simple combination. In *Proceedings of the Fourth Working Conference on Smart Card Research and Advanced Applications (CARDIS 2000)*, pages 273–288, Bristol, United Kingdom, September 2000. Kuwer Academic Publishers.
11. K.M.; Mitchell C.J. Horn, G.; Martin. Authentication protocols for mobile network environment value-added services. *IEEE Transactions on Vehicular Technology*, 51(2):383–392, March 2002.
12. M. Jakobsson and S. Wetzel. Security weaknesses in bluetooth. *Proceedings of the RSA Conference 2001*, 2020:176–191, 2001.
13. M. Looi. Enhanced authentication services for internet systems using mobile networks. In *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM'01)*, volume 6, pages 3468–3472, Bristol, United Kingdom, November 2001. IEEE Press.
14. J.T. Vainio. Bluetooth security. In *Proceedings of Helsinki University of Technology*, Telecommunications Software and Multimedia Laboratory, Seminar on Internetworking: Ad Hoc Networking, 2000.