Hardware Security Concept for Spontaneous Network Integration of Mobile Devices

Igor Sedov[1], Marc Haase[2], Clemens Cap[1], Dirk Timmermann[2]

[1] University of Rostock, Department of Computer Science
Chair for Information- and Communication Services[†‡]
{igor,cap}@informatik.uni-rostock.de
[2] University of Rostock, Department of Electrical Engineering
and Information Technology
Institute of Applied Microelectronics and Computer Science[‡]
{marc.haase,dtim}@e-technik.uni-rostock.de

Abstract. In this article we introduce an architecture of a mobile device that enables safe and authenticated data-transmission in a spontaneously configured network environment. The usage of this device is illustrated by a number of examples. The hardware and software components are presented. Particular, we compare Bluetooth and Infrared (IrDA) wireless networking technology, explain the usage of biometrics recognition methods, clarify the choice of the cryptographic module and consider possible platforms for the integration of this trustworthy device into a ubiquitous environment. Subsequently a first realization of the concept will be explained. Referring to feasible possibilities of realization, different attack scenarios together with appropriate solutions are considered.

1 Introduction

Impetuous miniaturization of electronic components leads to rapid growth of the amount of portable mobile devices. Introduction of new technologies increases possibilities of usage Business-to-Business (B2B), Business-to-Customer (B2C) and M-Commerce applications. Secure data transfer between a sender and a receiver is required to preserve privacy of the transmitted information. At the same time, the usage of only internal security solutions in wireless protocols is not sufficient. Mobile units employ mostly radio waves, which can be easily detected, received and decoded in comparison with permanent wire connection. On the other hand, the weakness of existing wireless communication protocols [5, 1] is that they make eavesdropping possible and unauthorized usage of transmitted data. Therefore, it is necessary to apply additional trustworthy protocols and algorithms for protection of transmitted data not only on the hardware layer but also on the application layer. Moreover, mobile devices can be easily lost

[†] Supported by Heinz-Nixdorf Stiftung
[‡] Research supported by the SPP "Sicherheit" of the German national research agency DFG

or stolen, while the true owners of the Digital Assistants (DAs) do not notice it. In this case to exclude potential vulnerabilities, the authentication of the user to his portable device through a Personal Identification Number (PIN) or a biometric recognition procedure should be guaranteed. The main disadvantage of the PIN approach is the usage of mostly four digit numbers. Third parties access to sensible data by searching through all possible PINs. Thus, the PINs length should be now at least 64 bits long. For ordinary people it becomes more and more difficult to remember all their PINs [6]. Our concept provides an identification of a user through a biometric technique, in particular, through a finger print recognition procedure. Biometric tokens are stored within a mobile device in an inaccessible secure memory and never left the device. Moreover, the human biometrics characteristics are not transmittable or forgettable.

In Section 2 we present some reference scenarios which illustrated the use of spontaneously networked mobile devices. Section 3 describes a secure hardware conception, gives an overview of state-of-the-art mobile devices, biometrics recognition methods and cryptographic modules. In Section 3.3 we introduce major properties of modern wireless network technologies and compare Bluetooth and IrDA wireless technologies. Security manager architecture is for management of safety related aspects responsible and presents in Section 3.6. The article closes with a conclusion and directions for future work.

2 Reference Scenarios

The proposed architecture corresponds with the paradigm postulated in [8] , that a combination of software, dedicated hardware and reconfigurable logic is the basis for an application-specific optimum. We consider the following reference scenarios for the usage of mobile devices in ubiquitous network market.

- A doctor in a hospital prescribes several medicaments to a patient. However, he does not know which medicaments are available now in the pharmacy. Moreover, the doctor does not know which preparations have already been prescribed to the patient and on which of them he reacts allergically. With the help of digital assistant the doctor can interrogate the required information wirelessly from a server. This scenario requires that doctors, nurses and students are to be distinguished and must to have different access rights. For example, male nurses are allowed to know, when the next medicament must be taken by the patient but not allowed get the other information from disease-history of the patient.
- Suppose that all employees in a hospital have personal digital assistants. If somebody enters or leaves the building, the server registers the time and the date. Besides that, the authorized employees having appropriate access rights to the server, can find out the current location of their colleagues and send to them short messages. Everything is carried out wireless from DAs.

3 Concept

In this section we introduce a concept for a mobile device with the ability for secure spontaneous networking. At the beginning we take a look at state-of-the-art mobile devices and the requirements for trustworthy user devices. Then we explain our architecture for a spontaneous networking mobile device and introduce additional hardware components for the device. At the end of this section we will present a first realization step of a mobile device containing the new functionalities.

3.1 State-of-the-art Mobile Devices

At the moment several mobile devices are available on the market. There are various groups, i.e., Notebooks, Pocket PC, Personal Digital Assistants (PDA), mobile phones and others. The differences between these devices are CPU performance, system resources, power consumption, peripheral extension possibilities, weight and size. To use these devices as a personal trustworthy user device for security related applications several requirements are recommended.

Regarding to [7] a trusted device should provide an own user interface, i.e., key-pad and display. This ensures that for signing contracts the user can read the contract on his own device and signing the contract with his own keypad. Common Attacks against user terminals will be useless, because manipulating the user interface is not possible. Pocket PC, PDA or mobile phone are devices which provide such an user interface and fulfill the mechanical requirements on a mobile device, that carried permanently. For secure transmissions it is required to combine mobile devices with additional security functions like ciphering, key management, biometric recognition methods. A disadvantage of current available mobile devices is the lack of a wireless communication capability supporting spontaneous networking. We think that IrDA available on most devices is not suitable for this.

Based on the requirements for trustworthy mobile devices with the ability for spontaneous networking we present a new enhanced security architecture for a mobile device that will be implemented.

3.2 Enhanced Security Architecture for Mobile Devices

Our concept provides a mobile device named *SmartBadge*. It consists of a wireless network interface for spontaneous networking in a ubiquitous environment, a cryptographic module for secure data transmission, a processor module for device control and software applications, a secure memory area for private keys and a biometric sensor for user authorization. We will merge these modules and an additional autonomous power supply module to an active device that can be used in a ubiquitous environment. The dimension of this device will be fit to the PCMCIA form factor. It will be controlled by a software architecture especially designed for security.

In difference to [7] we will not implement a user interface in the device because this increases the size of the device and the electric power consumption. For configuration purposes a secure connection to a trustworthy terminal is necessary. This connection can be established over the wireless network interface with strong encryption. Nevertheless we provide an optional hardware connection for a trusted user interface on the card.

Figure 1 shows the architecture of the SmartBadge in a wireless environment especially a Bluetooth network.

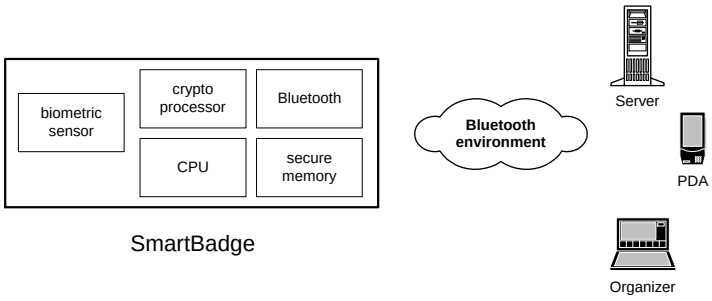

Fig. 1. SmartBadge Concept

3.3 Wireless Network Interfaces

The communication and the data interchange for mobile devices is ideally achieved by wireless network technologies. This ensures the greatest possible mobility. Table 1 shows common wireless network technologies and their major properties [2].

Table 1. Overview of Wireless Network Technologies

Name	Frequency	Range	Data rate
Ricconet	902-928MHz	800m	55Kb/s
IEEE 802.11	2.4GHz	30-360m	10Mb/s(100Mb/s)
DECT	1.8-1.9GHz	100m	522Kb/s(bis2Mb/s)
HomeRF	2.4GHz	50m	2Mb/s
Bluetooth	2.4GHz	10m(100m)	720Kb/s(2Mb/s)
IrDA	light	1-2m	9.6Kb/s-4Mb/s

The use of this technologies depends on the appropriate area network. Referring to the scenarios in section 2 we will concentrate on personal area networks

(PAN). IrDA (Infrared Data Association) and Bluetooth are suitable technologies in this case.

IrDA is a popular technology available in most mobile devices. A disadvantage is that IrDA supports connections between two devices with a narrow focused angle of cone maximum 30° [11]. The transfer of the data over infrared-light waves, in spite of the limited range of 1–2 meters between the senders and recipients, enables a "eavesdrop" of reflected infrared-light waves. There is no protection on the link layer. For avoiding any unauthorized use, additional cryptographic algorithms must be implemented in the application layer [4].

Bluetooth is a network technology for wireless data and voice transmissions over short distances up to 100m. An advantage are "Point-to-point" and "point-to-multi-point" connections of Bluetooth devices with a transfer rate up to 721 Kb/s [3]. Up to seven active slave-devices and one master-device form a "pico-network". Each user device from one "pico-network" can participate at the same time in other "pico-networks".

In comparison to IrDA Bluetooth includes different security mechanisms:

- a "frequencies hopping spread spectrum"- technique with a "time division duplex" scheme (FH/TDD). The signal frequency changes up to 1600 times per second in a pseudo-random sequence, which is given by the master,
- error correction methods on link layer,
- four LFSR (linear feedback shift registers) for encoding link layer data,
- a enhanced version of an existing block cipher SAFER-SK128 algorithm for the authentication [3] [10].

In Bluetooth systems there are 79 channels for usage of a complete frequency range. The narrow bands signal carrier hops between the available channels in case of the use of the "Frequency Hopping Spread Spectrum". The narrow signal carrier can be detected with standard receiver, which knows the transferred frequency. The receiver does not have the possibility to grasp the complete data spread, because it receipts only some of FH signals and the consequence of frequency changes is not known.

The sensitivity of the attacker devices and the signal/noise ratio must not be worse than the parameters of the transferring system. Besides the opponent should observe the same sequence of hops, as well as the initial system.

To release a radio jamming, the opponent should block all frequent ranges in which the signal is transferred. In the case of the Bluetooth technology a radio jamming must cover the frequency range from 2.400 GHz to 2.4835 GHz. This requires an increased capacity of the attacker system and therefore can be easily localized.

According to the Bluetooth security architecture and the future plans of integrating Bluetooth in the next generation of mobile devices we decide to use this technology for the SmartBadge concept. The data transmission range of Bluetooth is sufficient for private area networks. The relatively high data

transmission rate with small energy consumption and the possibility of "point-to-multi-point" connections enables the usage of Bluetooth technology within the area of wireless communication services.

Unfortunately, actual analyses show security weakness in Bluetooth architecture [5]. To avoid eavesdropping of transmitted data we implement a additional cryptographic module.

3.4 Cryptographic Module

Our concept provides the encoding and decoding of personal data over an independent ciphering module. It supports asymmetrical and symmetrical algorithms, e.g. RSA, DES, TDES. This additional hardware based ciphering module enhances the security functions already implemented in the Bluetooth architecture. The module can be configured and controlled by the software application to encrypt only sensible data.

There are already developed generic VHDL models [9] for the ciphering algorithms. The models can be parameterized according to the data and key lengths defined by the security requirements. We will implemented these algorithms into a field programmable gate array (FPGA). Delegating the encoding algorithm to the hardware components reduces the load on the processor of the mobile device.

3.5 Biometric Sensor and Secure Memory

Today there are too many smart-cards or mobile devices with various PINs and many people are not able to remember all codes. The biometric system applies unambiguous tokens of a person, that depends on physiological or genetic attributes and cannot get lost, nor can be transmitted to other persons. Therefore, the integration of a biometric sensor and a secure memory on the SmartBadge is a most suitable solution for security approach. We recommend for usage a biometric sensor, which unlocks the cryptographic system. After successful authorization of the user the crypto processor generates a session key for further secure wireless communication. Without biometric authorization the private key can not be read from the secure memory and therefore, the session key can not be decoded and the device can not be slated.

Most suited biometric procedure for mobile devices is the fingerprint authentication of the user. The sensor necessary for this integrates easily in the system because of its small size. However in addition to the sensor, the software for the control of the sensor must also be integrated into the system. The processor of the mobile device fulfills this task or the recognition software runs on a processor specially added for this task. Through this the hardware effort is increased on the one hand, on the other hand the biometric recognition method of the system is decoupled completely, and thus possible abuse of the biometric data is eliminated.

3.6 The Function of the Security Manager

Security Manager is the main component for security related aspects. It is responsible for communication with secure hardware and software components and fulfills the function of:

1. Key management
2. Definition of security levels for all devices and services
3. Distinguish device trust levels
4. Storage identifications information about devices and services
5. Set up Encryption with a necessary key length

The Security manager must define different admission levels for every communication service and device. If an authentication fails, a possibility to register this service manually must be available. This must be carried out on two sides. If no registration has taken place or the attempt fails, the Security manager must determine a standard security level. Also, if authentication attempt fails, a waiting interval, that increases exponentially, must be applied. The device should administrate a list with individual intervals of delay for each communication partner. Due to the small storage capacity of the mobile device the list can contain only the last n units. The user defines the size of the list, that depends also on the memory capacity.

3.7 Concept Realization

Now we present a first realization of the concept shown in section 3.2. The idea is to use an existing mobile device and expand it with required additional hardware components (Fig. 2). For this we use a PDA supporting PCMCIA cards. The PDA itself stands for the processor module and the user interface (key-pad and display). The wireless network interface will be established by a PCMCIA Bluetooth card. The crypto-processor module, the secure memory and the biometric sensor will be integrated on a second PCMCIA card. The advantage of this architecture is that it enables other mobile devices with PCMCIA support to participate on a spontaneous networking environment.

4 Conclusion and Outlook

Wireless mobile devices offer numerous new applications in the environment of the ubiquitous computing. Mobile access to financial transactions, dynamic information in hotels, airports, offices was some years ago only an unattainable dream. Significant problems of transition to wireless transfer of sensible data are low security features of mobile data communication technologies. The primary goals of this project are implementation of reliable protocols and algorithms for protection of the transmitted data in spontaneously networked mobile devices. Another important issue is the concept of personal identification on a basis of a biometric recognition procedure, that allows to avoid an unauthorized use of the device.

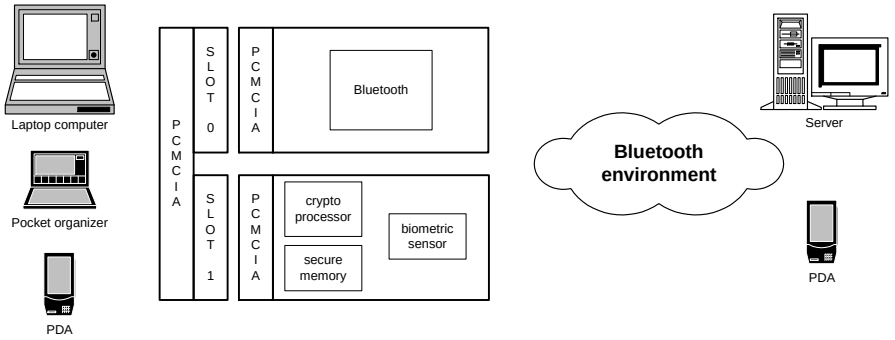

Fig. 2. Concept Realization

References

1. Nikita Borisov, Ian Goldberg, and David Wagner. Intercepting mobile communications - the insecurity of 802.11. *University Berkley*, 2001.
2. F. Buchert, W. Bütow, P. Eschoholz, A. Polonsky, F. Quintero, and D. Tavangarian. Ubiquitous Internet and Intranet Access Using WLAN. In *Proceeding of the Workshop on Ubiquitous Computing, International Conference on Parallel Architecture and Compilation Techniques, Philadelphia*, 2000.
3. Bluetooth Consortium. Specification of the Bluetooth System Version 1.0B - Core. http://www.bluetooth.com, 2000.
4. The Infrared Data Association IrDA. http://www.irda.org.
5. M. Jakobsson and S. Wetzel. Security Weaknesses in Bluetooth. *RSA Conference 2001*, 2001.
6. Nico Maibaum and Clemens Cap. Javacards as Ubiquitous, Mobile and Multiserve Cards. 1st Pact 2000 Workshop on ubiquitous Computing, Philadelphia, USA, 15.-19. October 2000.
7. Andreas Pfitzmann, Birgit Pfitzmann, Matthias Schunter, and Michael Waidner. Trustworthy user devices. In Günter Müller and Kai Rannenberg, editor, *Multilateral Security in Communications*, pages 137–156. Addison-Wesley, 1999.
8. Jan Rabaey and et al. PicoRadio Supports Ad Hoc Ultra-Low Power Wireless Networking. *IEEE Computer*, pages 42–48, July 2000.
9. M. Schmalisch, H. Ploog, and D. Timmermann. SECOM: Sichere Online Verschlüsselung fuer ISDN Geräte. 35. Sitzung des Arbeitskreises Technische und organisatorische Datenschutzfragen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Rostock, September 2000.
10. Bruce Schneier. *Angewandte Kryptographie*. Addison-Wesley, 1998.
11. Dave Suvak. IrDa and Bluetooth: A Complementary Comparison . http://www.palowireless.com/infotooth/download.asp, 2000.