SECURITY ASPECTS OF MOBILE COMMUNICATIONS

J. Markovski, M. Gušev
Institute of Informatics, Faculty of Natural Science and Mathematics,
Sts. Cyril and Methodius University
Arhimedova b.b., PO Box 162, 1000 Skopje, Macedonia
jasen@ii.edu.mk, marjan@ii.edu.mk

Abstract: The wireless application protocol (WAP) presents the leading standard for information services on mobile devices (mobile phones, PDAs, etc.). As the standards for presenting wireless content are entering their finishing phases, the need for secure end-to-end mobile communications is rapidly growing. In this paper we review the proposed levels of security and their implementations. We propose several models for implementing future security solutions using outdated technologies, which are most widely spread nowadays. The proposed security models are developed on application level because of the missing infrastructure and technology.

Keywords: mobile communications, WAP security, application level security, m-commerce, security implementation

1. Introduction

The wireless application protocol (WAP) presents the leading standard for information services on mobile devices (mobile phones, PDAs, etc.). As the standards for presenting wireless content are entering their finishing phases, the need for secure end-to-end mobile communications is rapidly growing.

WAP is modeled as a stack of protocol layers:

- Application layer – Wireless Application Environment (WAE)
- Session layer – Wireless Session Protocol (WSP)
- Transaction layer – Wireless Transaction Protocol (WTP)
- Security layer – Wireless Transport Layer Security (WTLS)
- Transport layer – Wireless Datagram Protocol (WDP)

with application layer at the top [4].

The Wireless Transport Layer Security (WTLS) is designed to function on connection-oriented and/or datagram transport protocols. Security is assumed to be an optional layer above the transport layer [1]. The primary goal of the WTLS layer is to provide privacy, data integrity and authentication between two communicating applications [3].

Subscriber Identity Module (SIM) is a tamper resistant device in a wireless system holding subscriber identity and authentication information. The SIM card can also be used to run applications needing a secure environment [3].

WAP Identity Module (WIM) is a tamper resistant device used in performing WTLS and application level security functions, and especially, to store and process information needed for user identification and authentication. It is used to enhance security of the implementation of the WTLS and certain functions of the wireless application environment layer [2].

Certification Authority (CA) is an entity that issues, updates and revokes public key bearing certificates in response to authenticated requests from legitimate registration authorities. The technology is based on a private key used to sign domain member key bearing certificates. CA information center provides trusted CA information, which includes the CA root certificate and information necessary to validate the CA root certificate [3].

Registration Authority (RA) is an entity authorized to make requests to issue, revoke and update certificates to a CA. The registration authority can be considered similar to an account manager in function and is responsible for member enrolment and/or attribute assignments [3].

Public Key Infrastructure (PKI) portal is the entity that performs CA and/or RA functions. It is both WAP and PKI aware. The current WAP PKI model defines the functionality required to manage the security functionality defined in WAP 1.2 [3].

Browsers capable of displaying wireless content are called microbrowsers. The microbrowsers provide support for WMLScript function Crypto.signText. This function can be used to sign data using a private key located on the SIM or the WIM card. A call to the Crypto.signText method displays the exact text to be signed and asks the user to confirm that [5].

2. Security levels of mobile communications

The mobile networks protect the users and their privacy using some sort of security methods. Every mobile device has an ID placed inside the SIM card. This ID uniquely identifies every user. The user can protect the SIM card using a personal identity number (PIN) with at least four digits.

Even though the identity of the user has a basic level of protection, there is need to secure the mobile communications during wireless sessions. The security level of the mobile communications depends on the security methods implemented by the mobile network. In this section we give a brief overview of the basic security levels of mobile communications, as well as their generic implementations using PKI infrastructure.

Level 1 security is implemented by passcode (password) identification [2][3][4][5][6]. The user sends a passcode to the mobile network. Then, the passcode is compared with the one in the device database. After validation of the passcode the user is granted access to the required resources.

Level 2 security is implemented using symmetric key schemes [2][3][4][5][6]. It is depicted in figure 1. The main feature is that the client is able to authenticate the identity of the gateway. Currently, WTLS session is established between the WAP client and the gateway. Further on, the gateway communicates with other resources using secure Internet protocols.

Future versions of WAP will allow a WTLS session to terminate beyond the gateway. In this way the routing is via gateway, but communication is not transparent to the gateway.

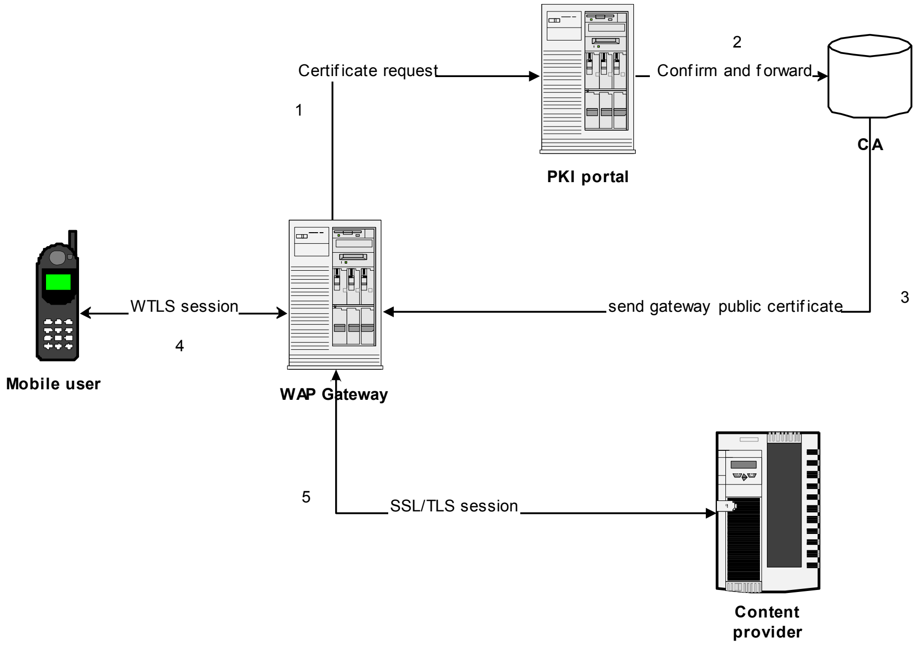

Figure 1: Generic model of level 2 secure mobile communication

The mobile device has in possession some CA root public key information. The WAP gateway generates a key pair: public key and private key.

The protocol continues as follows:

1. Gateway sends certificate request to PKI portal.
2. PKI portal confirms the gateway ID and forwards the request to CA.

3. CA sends gateway public certificate to gateway.
4. WTLS session is established between the mobile device and the gateway.
5. SSL or TLS connection is established between the gateway and the content provider server.

Level 3 security is implemented using asymmetric key schemes [2][3][4][5][6]. The client is able to authenticate the identity of the gateway. Equally, the gateway can ask the user to prove that he is in a possession of the private keys of the user with the same ID. The challenge of gateway is sent to the user. The user signs the given data with his private keys and sends it back to the gateway, which verifies the user's signature. This is depicted in figure 2.

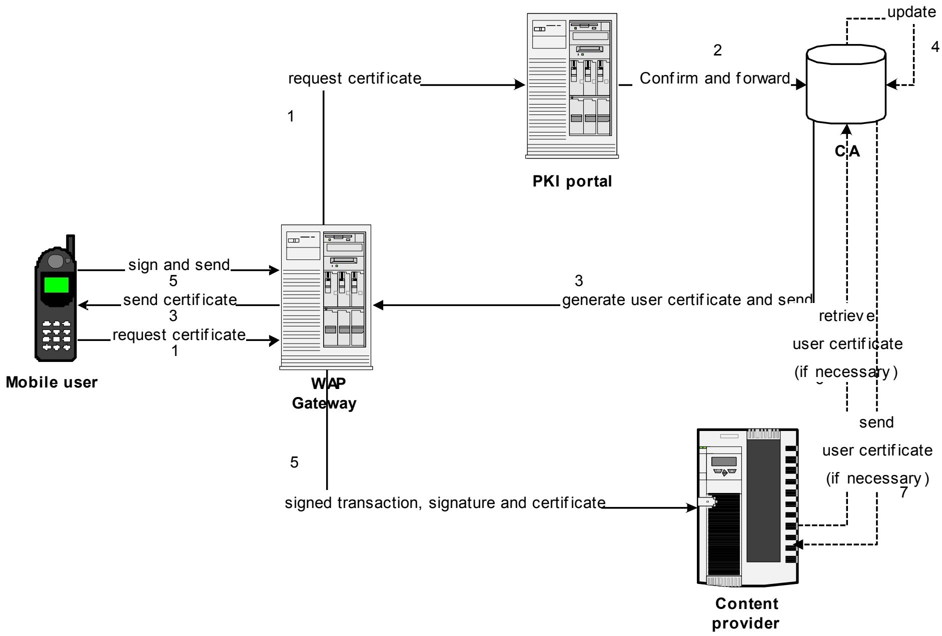

Figure 2: Generic model of level 3 secure mobile communication

In this case root CA public keys must be provisioned in both the mobile device and the server. The Crypto.signText function provides a means for a client device to create a digital signature and send it using WMLScript.

The protocol is executed as follows:

1. The client requests a certificate from PKI portal via gateway.
2. PKI portal confirms the user ID and forwards the request to the CA.
3. CA generates user certificate and sends certificate URL to the client. CA may choose to send the complete client certificate to the device. Then, for example, it can be stored on the SIM/WIM card.

4. If necessary, CA updates the database with user public key certificate.
5. The client signs the transaction and sends the transaction, signature and certificate URL to the content provider via gateway. The server may be in the possession of the client's certificate.

If the server is not in the possession of the client's certificate then:

6. The server uses Certificate URL to retrieve user certificate from CA database.
7. CA sends the user certificate to the server.

In case the gateway chooses to challenge a client to sign some data with his private key the user requests a certificate from the PKI portal. In this way the client gives prove that he is in possession of the private key of the ID that he used.

3. Implementing secure mobile communications using outdated technologies

Implementation of the security levels of mobile communications requires that the mobile devices and the mobile network support certain technologies and standards. For example, the WMLScrypt function Crypto.signText is first introduced in WAP 1.2 together with the support for the WIM cards. The WAP PKI infrastructure is implemented in WAP 2.0.

There are only few mobile devices that support WAP 2.0. Equally, not many mobile operators offer SIM cards with WIM support or separate WIM cards.

In this section we propose several models how to overcome the presented problems with the current technologies. All proposed models implement security on application level. We also give a review of the security aspects of the mobile communications on application level.

First, we choose a classification of the clients by the possibility to store or generate private keys needed to establish secure communication. In general, the clients are classified in one of the following categories [6]:

1. No private keys.
2. One private key used for authentication or signing.
3. Two or more private keys from which one is used for authentication and the others for signing.

Sometimes, private keys cannot be stored on the mobile device (for example, no WIM support, SIM cards not capable of storing private keys). In that case we have no private keys available on the client side.

Also, the mobile devices are not always capable of signing transactions (for example, only outdated WAP standard version is supported by the mobile device). In these cases the security of the mobile communications must be implemented on application level.

The implementation of security level 1 mobile communications is straightforward. The client can send the passcode by SMS or WAP and after verification of the passcode the user is granted or denied access to the information services.

The implementation of security level 2 mobile communications depends on the capability of storing private keys. If the client is not capable of storing private keys, than the private key must be stored either in the mobile device (for example, JAVA enabled phones), which is not a tamper resistant device, or entered by the user.

If the client is able to store the key in the mobile device, than it is possible to develop applications (which are phone specific) that provide the same functionality as WTLS. However, this is very expensive, narrow and unlikely solution.

It is also possible to develop WMLScript functions that will encrypt and send sensitive information to the gateway. The user will enter the private key in some input box and only the sensitive information will be encrypted and sent to the gateway as part of some WAP application. This is presented in figure 3. The gateway must know the client's public key and the client must know the passcode for the client's ID.

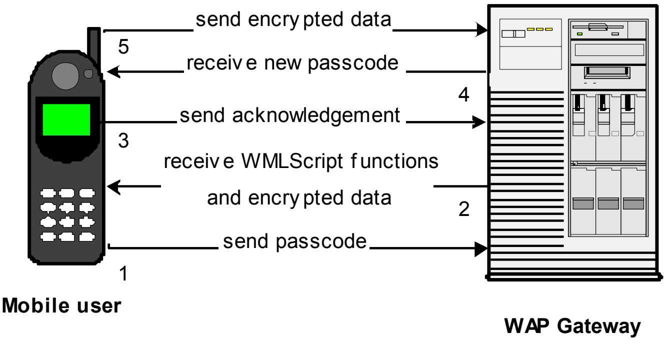

Figure 3: Implementing security level 2 of mobile communications on application level

The communication between the client and the gateway is performed as follows:

1. The user sends the passcode to the gateway.

2. The gateway verifies the passcode in the database and encrypts the sensitive information using the client's public key. Afterwards it sends the encrypted information to the user and the needed WMLScript functions.
3. The client decrypts the received data and sends acknowledgement.
4. The gateway sends new passcode to the client. The old passcode is no longer valid.
5. The client sends the encrypted data to the gateway. The gateway receives the secure data and the protocol continues as in figure 1, step 2.

Note that the gateway is treated as part of trusted environment. It holds the private and the public keys of client so that it can establish a secure session with the client. Only the sensitive data is protected.

The passcode can be intercepted if it is not sent through secure channels. However, the passcode is used only for one session and afterwards the client receives new passcode and the old one is invalidated. The private key is never sent over the air and thus is protected from eavesdroppers. The downfall of this model is that the client must find a way to memorize the passcode and the private key outside the mobile device. This means that the client must enter the passcode and the private key during every secure session.

The implementation of security level 3 depends both on the capability of the client to store private keys and the ability to generate digital signatures. If the client is not capable of storing private keys than level 2 secure mobile communications can be implemented as previously described.

If the client is not able to generate digital signatures than we use delegated PKI signing, which means that, the security server signs a contract on behalf of the mobile device [6]. Note that in this model the gateway and the security server can be implemented as one because the security server acts as the part of mobile device that generates signatures. If the phone is not capable of storing private keys than the secure connection between the mobile device and the gateway is established as in figure 3.

4. Conclusion

The current standards of WAP provide means that enable secure end-to-end communication. However, there are not many mobile operators and mobile devices that implement the proposed standards. That is why we propose a solution that implements secure mobile communication on application level with the current technologies. We give models for every security level defined by the WAP standards.

There are many m-business and m-commerce solutions that provide similar protection of the wireless transactions using application level security. They usually implement their own mobile security servers and are sometimes phone specific.

The next generation of WAP implements the security layer in the same way as Internet. In this way the security of the wireless transactions will be implemented in the same way as their web counterparts.

The future also holds the use of personal trusted devices (PTDs) that are capable of securely storing private keys and performing operations with them. The PTDs are developed using WIM and WPKI technologies.

5. References

1. Wireless Application Protocol Forum, “Wireless Transport Layer Security”, version 06-Apr-2001, WAP-261-WTLS-20010406-a, *http://www.wapforum.org*
2. Wireless Application Protocol Forum, “Wireless Identity Module”, version 12-July-2001, WAP-260-WIM-20010712-a, *http://www.wapforum.org*
3. Wireless Application Protocol Forum, “Public Key Infrastructure Definition”, version 24-Apr-2001, WAP-217-WPKI, *http://www.wapforum.org*
4. Bulbrook, D. (2001) “WAP: A Beginner's Guide”, *Osborne/McGraw-Hill*, USA.
5. Wireless Application Protocol Forum, “WMLScript Crypto Library”, version 20-Jun-2001, WAP-161-WMLScriptCrypto-20010620-a, *http://www.wapforum.org*
6. Ericsson (2002) “Reference Guide for Security API”, Mobile Commerce Platform 1.0, *http://www.ericsson.com*