University of Oslo
Department of Informatics

Mobile security using PKI
INF5260

Thomas Kvalvåg
Institutt for informatikk
Universitetet i Oslo
thomaskv@ifi.uio.no

12th May 2004

Contents

List of Figures

Abstract

As part of INF5260 we are assigned to create a paper/project on related technology to the subject. This will be part a part of the learning perspective and will be used as part of the evaluation. We will be working with this project through out this semester. The project will include learning objectives of this course. This project will only be a theoretical view on the subject reflected in this paper. The paper will reflect on issues with non-secure mobile communication. The paper will give an overview on how mobile-PKI can be used to solve some of these issues. And as well introduce why security is required on mobile devices. By the means of mobile devices we will be focusing on cell phones in this paper. This paper will go into detail of how to secure communication between servers located on a base network and a mobile device by using PKI. The paper will be limited to only look at security schema on top of the Wireless Application Protocol (WAP) which is, as for now, the most wide spread-ed protocol for handheld wireless devices. The content of this project will be a theoretical analysis of security in mobile devices. This is a wide area to investigate. To reduce we will be looking on technologies to enable security on application communicating over the gsm and gprs protocol. We will be focusing on using the WAP protocol as a platform for the applications. By this means a thin client architecture. The paper could be extend to look at fat application running on eg. PDA or other gadgets.

1 Introduction

Wireless devices have exploded in number and their complexity which has lead to increasing mobility usage and as a result of this, users will demand new functionality. To follow this demands more and more businesses is moving from traditional web site applications to a more wireless profile. This leads to higher requirements to mobile devices and higher availability of application. Today almost everyone have a cell phone or any other type of mobile device with connection to a base/ground station offers more services than calling and SMS. As more business is moving application to mobile devices the requirement for secure transaction between mobile devices, base stations, and application servers. This has lately been the case for financial institutions which wants to enable banking for a cell phone or other mobile devices like PDA. To enable financial transactions from a cell phone a security schema has to be introduced to make sure no uninvited people can get information they are not supposed to get. As for the Internet this has been a big issues for many years and there are still work being done to make digital transaction even more secure than today. This will probably be a field of work fore as long as the Internet lives. But for mobile digital transaction this is quite new and in the start of development. For application running on cell phones the WAP 2 protocol where introduced some years ago.

1.1 Why do we need security?

To reflect back to Internet usage, security has become one of the hottest topic. As more sensitive data and more business critical transaction has made their way to the Internet the need for security has raised. To protect private data and data integrity security has been developed and implemented in the Internet. Several security schemas has been introduced to protect data from malicious activity. As for financial transaction on an open network, as the Internet, the need to protect these transactions from malicious users is required. People and businesses communication over an open network do not want criminals to interact in their private transaction. This to protect money transfer and other sensitive information.
This is also the case now that transaction clients is going wireless as for cell phones. The need to protect communication going across a wireless link and to a base station is necessary. Since communication from a cell phone to the base station goes through the air it is vulnerable for eaves dropping and "man in the middle" attack. To protect against these kind of malicious acts, the need for a good security schema is required in transaction over wireless links. As for financial transaction there also exists laws about how these transaction must be secure to reduce the possibility of malicious user interfering in the transaction. And of course to make sure that now "money" disappear into the hands of criminals.

1.2 Financial industry

The financial industry has been in front of implementing new technology. As from when the Internet becomes available for most people, by the means of more people where connected to the net. The Financial industry has been fast to adopt these new technologies as Internet banking and stock exchange. Now more businesses including the financial industry are looking at the possibility to move banking to mobile devices as well. There are being done a lot of work today to enable this. The scepticism related

to this has mostly been concerned about security, and of course the potential clients. One company that has done a lot of work for the financial industry related to mobile financial application is a Finish company, Meridea (www.meridea.com). Their business idea is to create an architecture to enable financial companies to easily implement their business solution on both the Internet and mobile network.

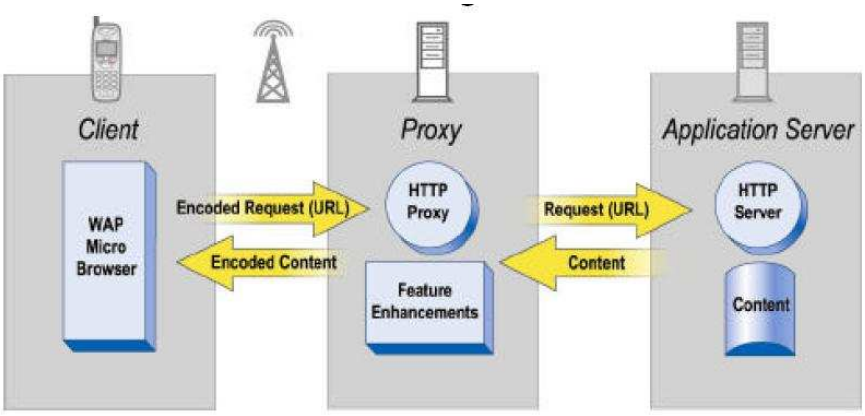

Figure 1: Feature/Performance-Enhancing Proxy

2 WAP

The scope of the wap as defined by the WAP Forum [3]. "The Wireless Application Protocol (WAP) is a result of continuous work to define an industry wide specification for developing applications that operate over wireless communication networks." The Wireless Application protocol is a standardized protocol for developing application on mobile devices. The purpose of the protocol is to create a standardized API for mobile application to run on top of and a common set of services for wireless applications. The WAP protocol is build using a proxy/gateway, see Figure 1. This is used to translate communication from Mobil devices to other devises. A typical scenario is to convert from WML(Wireless Markup Language) [8] to HTML use in normal web pages. The purpose of WAP [3] is to bring Internet content and advanced data services to digital cellular phones and other wireless terminals. To create a global wireless protocol specification that will work across differing wireless network technologies. To enable the creation of content and applications that scale across a very wide range of bearer networks and device types. And to embrace and extend existing standards and technology wherever appropriate. The WAP protocol is designed for wireless devices. By this the protocol will have to reduce the amount of bandwidth used in the network, since bandwidth is limited in todays wireless devices. As for cell phones the most common link speed is 9600 bauds. This will limit the amount of data that would be transfered between a cell phone and the ground network. The WAP protocol is designed to reduce the amount of data over the link. One way this is done is using WML [8], which is designed with the intention to reduce the size of a page build up using this markup language.

2.1 Architecture

The WAP architecture is designed to reduce overhead in the protocol. On important goal of the WAP architecture is to provide security to application running on mobile devices. The architecture is divided into different layers, see Figure 2. There is two main horizontal layers, the Protocol Framework and the Application Protocol. And there is two vertical layers, which provides services across the horizontal layers, the Directory Service and the Security Services layers.

2.1.1 Protocol Framework

The protocol frameworks provides services to the application layer and other services and is divided into 4 sublayers with different purposes as described below.

Session services: The Session services provides mechanisms for controlling state in a communication. This could be shared states between different service providers.

Transfer Service: The Transfer Services provide different services for how to send data, this could be streaming and other types of transfer mechanisms.

Transport Service: The Transport Services layer offers a set of consistent services to the upper layer protocols and maps those services to the available bearer services. The Transport Services transport unstructured data across the underlying bearer networks. These transport services create a common abstraction that is consistent across all the bearers. Definition from reference [3].

Bearer Networks: This layer defines the technology to be used to communicate with the ground network. The Layer offers different well known bearer services to be used as the communication protocol. The different services provided by this layer offers different level of quality and other options. This layer can be seen as the network layer of the OSI stack [2].

2.1.2 Service Discovery

This layer provides service discovery functionality to all the other layers. The service discovery can be lookup services and other discovery schemas.

2.1.3 Security Services

The Security Services provide security functionality available for all the horizontal layers, see Figure 2. This layer provides the following set of functionality available to be used by both application layer and protocol layer.

- Privacy - To ensure that data is kept private so non intermediate intruders may interrupt.
- Authentication - To enable authentication to access limited data by eg. login.
- Integrity - To make sure that data sent or received is not modified
- Non-Repudiation - To enable a way to trace back that the communication has taken place.
- Cryptographic Libraries - A service to enable the application level to encrypt and decrypt data.
- Identity WIM [5] provides the functions that store and process information needed for user identification and authentication
- PKI - Public Key Infrastructure, see 3, enabled in the WAP Protocol·
- Secure Transport - Secure transport of data on the transport level, this could be seen as the WAP equal to the HTTPS as known from the Internet.

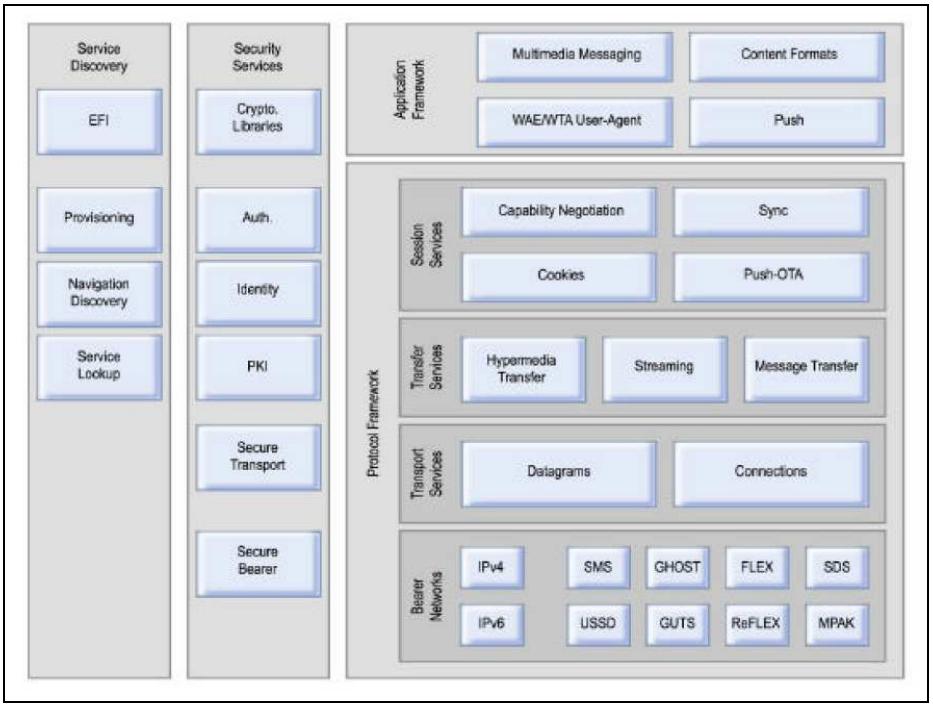

Figure 2: WAP protocol stack

- Secure Bearer - This is a service provided by some of the network protocols, this could be security using IPSec [9].

3 PKI

Short for public key infrastructure, a system of digital certificates, Certificate Authorities, and other registration authorities that verify and authenticate the validity of each party involved in an Internet transaction. A PKI (public key infrastructure) enables users on a unsecured public network such as the Internet to securely and privately exchange data through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The public key infrastructure provides for a digital certificate that can identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates. A public key infrastructure consists of:

- A certificate authority (CA) that issues and verifies digital certificate. A certificate includes the public key or information about the public key..
- A registration authority (RA) that acts as the verifier for the certificate authority before a digital certificate is issued to a requestor.
- One or more directories where the certificates (with their public keys(keystore)) are held.
- A certificate management system

PKI is based around the acronym ACIN, for confidentiality, authentication, integrity, and non-repudiation. Definition from [1].

Confidentiality: The protection of data against unauthorized access or disclosure. This service is typically provided via access controls (possibly in conjunction with encryption) for data storage, and via encryption during data transmission. It s the encryption part that the PKI can provide. Access controls are really a combination of authentication and authorization.

Authentication: The verification of an individual s identity and/or the verification of data origin. In other words, a person (or even a computer) needs to verify that the entity (computer or person) he or she is communicating with, or receiving data from, is indeed who he or she thinks it is, and who the other entity claims to be.

Integrity: The protection of data against unauthorized modification or substitution to information. This service is provided by cryptography mechanisms called a message authentication code (MAC) or a digital signature.

Non-repudiation: The combined services of authentication and integrity that is provable to a third party. This implies a legally unproven presumption that the originator cannot deny having originated the message. Asymmetric cryptography provides a mechanism called a digital signature such that only the originator could have produced the digital signature. Therefore, anyone else, including the receiver of the signed message, can verify the digital signature.

3.1 WTLS

The security in defined in the WAP protocol is called Wireless Transport layer Security (WTLS). This layer operates in the layer above the transport protocol layer (see Figure 2). WTLS main goal is to provide privacy, data integrity and authentication in communication between application. The WTLS protocol is designed to reduce the bandwidth in the network and support low latency.

3.2 WPKI

Wireless Application PKI(Public Key Infrastructure) or Wireless PKI(WPKI) [7]. WPKI tries to define a model of the functionality needed to manage security defined in WAP version 1.2. When a WAP device connects to it's representative proxy, it can choose to connect in a secure manner. This implies the use of the WAP wireless transport layer security(WTLS) [6], the WAP cryptographic API (WAP-CRYPTO) [4] and the Wireless Identity Model (WIM) [5]. Wireless PKI is an optimized extension of traditional PKI for the wireless environment. WPKI is primarily concerned with policies that are used to manage E-Business and security services provided by WTLS and WMLSCrypt [4] in the wireless application environment. The WPKI architecture goal is to implement a minimized PKI solution for mobile devices with their limited capacity. The main goal of the current specification of WAP PKI is to implement the WTLS certificate format specified and supported in current devices. An other important point in the current deployed WTLS and WAP solution is that there exists more clients than gateways in the mobile network. This will be a challenge when deploying new technologies and standards in the existing topology of mobile equipment. To get a perspective of the steps involved in communication using WPKI please see Figure 3. The steps involved in the figure is outlined below.

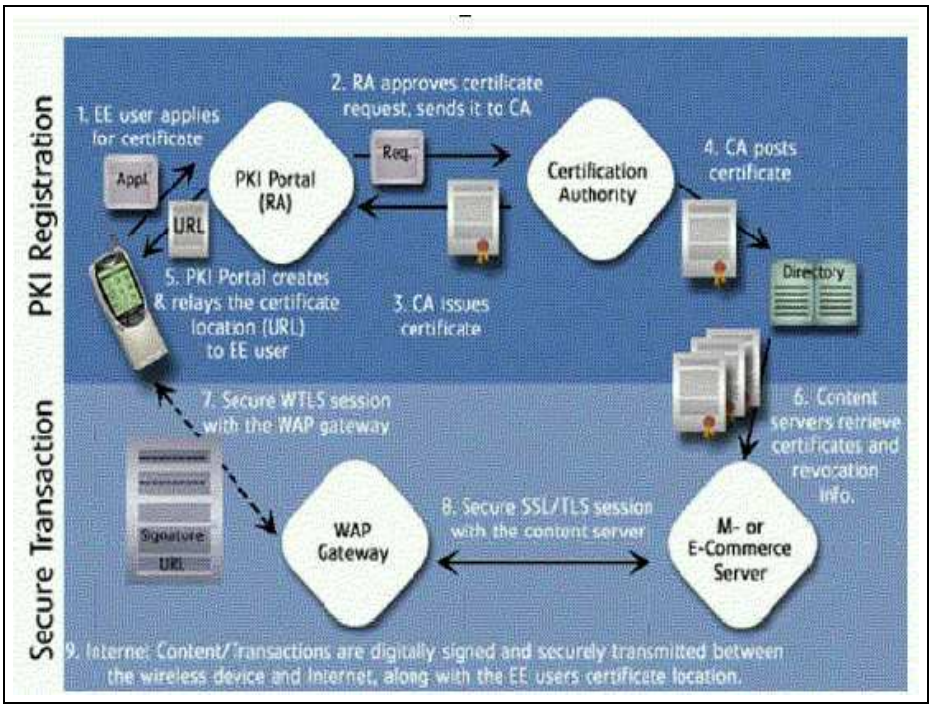

Figure 3: Wireless Public-Key Infrastructure

1. EE (End-Entity) applies for a certificate
2. Registration Authority approves certificate request and sends it to the Certificate Authority
3. Certificate Authority issues certificate to the PKI Portal
4. CA posts certificate to the directory
5. The PKI portal creates and relays the certificate URL to the end user
6. Content server receives the certificate
7. Secure WTLS session created between the client device and the gateway
8. Secure SSL/TLS session established between gateway and content server
9. Secure communication between the End-Entity and the content server is established.

3.3 Other security scheme's

One security schema that has, the latest days, been taken more and more into use is IPSec [9]. This is a security protocol running on the network layer in the OSI model [2]. This protocol will implement security on a lower that will be transparent to application running ontop.

4 Future

To use cryptography requires a lot of mathematical calculations. As at the present time and technology in cell phones the processor unit has a limited power by the means of calculation power. To enable a better form of cryptography the need for key generation is necessary, and this again requires a powerful processor unit. One nearby solution to this, that is being done a lot of work these days are an extra simcard in the cellphone. The purpose of this extra sim card is to work as a key generator. This will enable better security due to the possibility of randomly generated keys by the mobile device. Other possibilities is to put in more power in the processor chip to enable this. The challenge is this is the need for battery power and the size of devices.

5 Conclusion

As discussed through this paper the need and requirement to security in mobile devices exists. And especially in vulnerable transaction or communication as for the financial industry security is needed. The solution provided through the use of WPKI is the most widespread ed solution today for mobile security. There are a lot of work being done to improve security in both wired and wireless networks. And will probably be a field of work for as long as mobile devices exists. For application running on mobile devices which serve the purpose of enabling sensitive data to be transfered from the mobile device and a server on the base network, security is an absolute requirement. We believe that the security provided by WPKI is a good start, but still there will have to be done more to secure transactions over wireless networks. The reason for this is that the ease of picking up signals, with the right equipment, going over wireless is a threat. As security in mobile devices is improved we will probably see more application and businesses moving to mobile devises. We will probably see in the near future that application like banking and stock exchange will be enabled from cell phone. Sill it remains to see if there is a market for this.

References

[1] Tom Austin. Pki: A wiley tech brief. Wiley Europe, page 288, January 2001.

[2] International Organization for Standardization. Information technology – open systems interconnection – basic reference model: The basic model. (ISO) International Organization for Standardization, 1984.

[3] Wireless Application Protocol Forum Ltd. Wireless application protocol architecture specification. WAP Forum: http://www.wapforum.org/, 12-July-2001.

[4] Wireless Application Protocol Forum Ltd. Wml script crypto api. WAP Forum: http://www.wapforum.org/, 1999-11-05.

[5] Wireless Application Protocol Forum Ltd. Wireless identity module specification. WAP Forum: http://www.wapforum.org/, 2001-07-12.

[6] Wireless Application Protocol Forum Ltd. Wireless transport layer security specification. WAP Forum: http://www.wapforum.org/, 2001-10-06.

[7] Wireless Application Protocol Forum Ltd. Wireless application protocol public key infrastructure definition. WAP Forum: http://www.wapforum.org/, 24-Apr-2001.

[8] Wireless Application Protocol Forum Ltd. Wireless markup language specification. WAP Forum: http://www.wapforum.org/, 30-Apr-1998.

[9] R. Atkinson @Home Network S. Kent BBN Corp. (rfc2401) security architecture for the internet protocol. Network Working Group, November 1998.