T.E.I. PIRAEUS

Faculty of Engineering

Departments of Electronics and Automation

MSc in DATA COMMUNICATIONS

COURSEWORK

MODULE:

QoS and Compression for Network Applications

CSESM00: CIM233

Module Coordinator:

Dr. Nikolouzou Evgenia

Date of Module:

3rd Term (Fall 2005-2006)

Name of Student:

Vasileios Balafas

Specific needs and requirements that mobile devices have as well as the necessary security schemes in order to support M-commerce.

Vasileios Balafas, *MSc in DCOM student*,(xwing@otenet.gr)

Abstract— **In this coursework, a current and very arising matter of nowadays will be discussed and presented as part of the QoS and Compression for Network Applications course in MSc DCOM of TEI of Piraeus. The main case is the necessity of secure and reliable suggestions in the field of the mobile commerce in the new economic, cultural and technological environment that is formed on the score of the technological progress and evolution. This progress offers new dimensions of commercial possibilities, opportunities and ideas in order to fulfill the potential of the mobile devices that are available on the market. After the unexpected breakdown of the so-promising e-commerce, the mobile commerce seems to be the last chance of the ubiquitous computing to penetrate and dominate the commercial world. Many investments have been made by commercial vast companies in the past but the retribution was not the predictable one. Maybe the hasty growth and the solicitous attitude of the e-market stalemated this attempt. On the other hand, many believe that security problems and the suspiciousness of the consumers about the reliability of the offered services were the decisive factors of the fiasco of the e-commerce. Many cunning companies were appeared that were not controlled by any authority and managed to gain an impermanent success by harming the image and the future of e-commerce. Now, a new opportunity is in front of us and the market seems to be more patient and more careful towards the requirements that have to be set in order to support M-commerce. Here, we will discuss and present some security schemes and efforts that will be applied and will add value to the emerging services.**

I. Introduction

NOWADAYS, it is well known and it is a general consensus too, that emerging mobile and wireless technologies provide convenient and scalable platforms that accelerate and give value to m-commerce business. However, there are a number of security challenges and vulnerabilities that have to be overcome in order to create reliable and secure services.

Over the last few years, a number of mobile communication systems were developed and offered to the people. Many service providers and equipment vendors are bringing new innovations and lead the people to a new concept of commercial activity. Usually the equipment vendors ride hard and offer more and more complex devices with enormous capabilities that remain inactive either because people cannot use them, or because there aren't the adequate services to make the most of them.

In Greece this is a very common phenomenon with people who buy expensive and powerful devices, but finally they send SMS and periodically they shot some pictures or use the Bluetooth technology to send pictures or messages. The issue here is that complexity sometimes acts against usability and that people are not well informed about new possibilities and operations they can use via their mobile devices. This is of course out of the borders of this coursework but is a main factor that has to be ameliorated if m-commerce is about to succeed.

This is the one aspect, which is somehow convenient for the technology pioneers who want and know how to operate their devices. On the other hand, the experience of the e-commerce shows that if one technology is not widely accepted and well supported by the majority of the consumers, then there is no future because the financial return of investment is not enough to maintain the interest of the companies hot about less traditional commercial practices.

Exactly in this point, security appears as the major obstacle against the realization of the m-commerce. Frauds and electronic crimes, which take place, make people hesitant and this is at least logical. Traditional commercial activities are considered as fully safe by people because they give money and they buy a product. They see the seller, they control their cash and they can indeed examine the object of the transaction. Sometimes, even the strongest progressionists point out the need of secure structures and practices, in order to accept to replace their cash and move to the mobile marketplace.

At this point, it is purposeful to have a look at the equipment that can be used for m-commerce. PDAs, Palmtops, cellular phones, Smart phones, tablet PCs and mobile computers are the tools of the consumers which can be used in m-commerce. If we want to enlarge the range of mobile devices we can suppose that any mobile device which can exchange messages in a wireless environment is implicitly capable to participate in mobile commercial activities. This fact shows that we have to deal with heterogeneous devices, which coexist in heterogeneous networks, with limited power capabilities and poor user interfaces in general. But, user friendly applications have to be developed, having in the same time the ability to recognize the quality and the capabilities of the device, providing the appropriate content to the user. This matter seems to be solved by content providers and developers using each time the suitable protocols. On the other hand, the primary characteristics of mobile architectures offer an easier field for satisfactory security because mobile networks are usually strictly controlled by the providers.

In this coursework, the requirements, the needs and some proposed practices will be discussed and we will try to enlighten some aspects of the dark side of security and reliability of the mobile commerce which provokes many conflicts but in the same time offers a whole new world of services and commercial opportunities.

II. Requirements for secure mobile communication

As we mentioned before, the matter is the secure mobile communication but working out more carefully, we will see that new demands rise loudly, and these demands are personalized services and privacy. Commercial services are based on the location of the consumer, the geographical facts and the cultural customs. For example it would be useless to offer a commercial service for bikini swimsuits to the women of India. All these, combined with security issues create a complex and sophisticated puzzle which has to be confronted if m-commerce is about to succeed and dominate the market.

Trying to make a general plan of security requirements, we can conclude that we basically need confidentiality, which means that information is available to those who are authorized to have access.

Then, integrity and authenticity are needed in order achieve accuracy and completeness of information. It is obvious that unauthorized entities should not exchange any information.

Another basic requirement is the availability which means that the service will be accessible and usable upon demand and this availability has to be solid because a denial of service could cost to the company and damage its trustworthiness.

Afterwards, non-repudiation should ensure that the origin or receipt of a message is fully verifiable.

Finally, we need accountability in order to guarantee that the actions of an entity will be uniquely traceable to this entity. That last requirement is very important because it shows that in mobile communications and specifically in an m-commerce environment we don't have just to ensure that the device is authenticated but we must authenticate the person who uses it too. Practically, it is possible to identify the device but is it enough effective for mobile applications? Surely not, so we need mechanisms that will be able to identify the user as well.

Making a first reference to security technologies, the above issue is exactly the weak spot of the well known practices of electronic certificates combined with the Secure Socket Line (SSL) [1]. It makes sure that the connection between a machine and the host-server is secure and that this machine really belongs to someone but it does not validate that it is indeed this person that operates the machine. So, it is obvious from the very beginning of the analysis of the requirements that we need something that only we personally know in order to validate ourselves. This something, could be a personal code like widely used PINs (Personal Identification Number). By this way we can create not just an automatic challenge-response structure but a stronger identifying scheme. With the combination of a PIN with something that is exclusively ours, like a cell-phone or a palmtop, and a certificate that is established after personal appearance or personal agreement, we can achieve a satisfactory level of security.

The above paragraph is not strongly necessary in this section but it will work as the link to the next matters that will be discussed during this coursework. It helps us starting to imagine and creating a picture of the prerequisites that we have to keep in mind towards the goal of secure m-commerce services.

Returning to the main subject of this section and after meeting some theoretical demands about exchanged information, we should consider some practical restrictions that are posed by the nature of mobile devices.

Mobile devices have properties that are different from PCs and notebooks. They have small and low-resolution displays, limited input capabilities, limited power, computing power and small memory size. Of course, all these are improved day by day and sometimes mobile devices surprise us by their characteristics. But once more we have to keep in mind that m-commerce should target all the mobile-capable consumers and not only the most streamlined ones. In the same time, the mobile networks perform low bandwidth, variable bandwidth and availability, long latency and unpredictable disconnections. UMTS [2] networks tend to solve these problems but their availability is inhibitory for large scale m-commerce implementations.

Furthermore, the nature of mobile communication brings additional problems as the environmental conditions affect the communication. Usually mobile users are in a very unstable environment and the conditions are not constant because of the motion.

From the very beginning, academic community tried to apply in mobile communications well-known technologies from the “wired world”. This strategy was very helpful because some techniques evolved in order to help in the battle for secure mobile communication. The constraints from the nature of mobile technologies led us to modifications but the main idea remains the same. Today, Wireless Transport Layer Security (WTLS), Wireless Public Key Infrastructures (WPKI), and Pretty Good Privacy (PGP) are the dominant technologies that are adopted for different layers of communication. As research continues, new technologies may appear, or composition of the above may be applied. In every case cryptography is the answer and this cryptography should take place in secure channels of communication. These technologies will be presented briefly further down.

III. Known Technologies For Security

Beginning this itinerary through security technologies, we first meet the Wireless Transport Layer Security (WTLS) protocol. WTLS, as its name shows, offers security at the transport layer. It can provide several levels of security such as privacy, data integrity and authentication. In the same time WTLS is optimized for low bandwidth and for networks that have high latency. Although WTLS takes into account the limited capabilities of mobile devices regarding their low processing power, their limited memory and their power endurance, it can’t support applications that require strong security [3].

The security offered, exists between the device and the gateway or the server. That’s why WTLS has strong handshake mechanisms. But, if an application needs to access several servers then WTLS becomes very complex and complicated and finally it cannot support these transactions in a mobile world. Furthermore, as the gateway decrypts the data between a WAP client and content server, the data becomes vulnerable if the gateway is compromised.

Examining closely WTLS, we have to say that it is a PKI-enabled protocol that has been adopted in WAP 2.0 [4] specification from the former WAP Forum which is now known as OMA (Open Mobile Alliance). WTLS encrypts the whole message, and this is a drawback, because in a mobile environment we may want to encrypt only the sensitive information for reasons of power and bandwidth economy. The WTLS specification describes three classes (levels) of WTLS implementation [5].

Class 1: Anonymous encryption. Data is encrypted, but certificates are not exchanged between the client and the gateway.

Class 2: Encryption with server authentication. Data is encrypted and the client requires a digital certificate from the server.

Class 3: Encryption with client and server authentication. Data is encrypted and the client and the server exchange digital certificates.

As we can understand, WTLS is a very useful protocol that ensures security over the communication channel. It is not purposeful to analyse its operation further, but some of the WTLS concepts will be cleared later.

At this point, it is useful to mention that although WTLS is used widely in a WAP environment, it can offer important solutions and in other wireless environments. It is known that WAP technology did not fulfilled the expectations that created, but it became the example for future implementations and determined the mistakes that don’t have to be repeated.

The next part of the presentation of the main security technologies is the famous WPKI Wireless Public Key Infrastructure. WPKI could be by itself a subject for a coursework and indeed thousands of papers and scientific researches have been written about it. It had influence in almost every security proposition and seems to be the basis for the solution of security problems in mobile communication. All the presentations that are available and the relevant bibliography introduce it by the legendary Caesar’s effort to encrypt his messages. Later, important studies demonstrated algorithms which could be used, such as RSA and El-Gamal [6]. Beyond the mathematical models and the research for the most powerful algorithm, the general PKI infrastructure fulfils the requirements for secure mobile applications and m-commerce is definitely one of them.

In general WPKI is an architecture that relies on the use of Certificate Authorities (CAs) to establish trusted and secure communications between multiple parties. The Open Mobile Alliance lately standardized Mobile PKI for m-commerce services and many companies propose their implementations.

WPKI has four primary components, the End-entity Application (EE), the Registration Authority (RA), the Certification Authority (CA) and the PKI Directory. The user must contact a PKI portal in order to be authenticated by the service provider and complete a transaction. This authentication takes place by using asymmetric keys. One key is used to encrypt the data being sent, another is used to decrypt the data. The advantage here is that only one key (the key of the private user) needs to be kept secret, while the other is put in a certificate and made publicly available through web-accessible catalogues, the portals. The associations between the private key and the certificate that contains personal info of the user ensure enough legal proof to bind the user to any transactions exercised by his private key. Public administration or other receivers will only need one key, the one in the user’s certificate to decrypt and hence verify the received transaction [7]. This simplifies the system and reduces costs significantly. Fig. 1 depicts the whole PKI operation in a WAP environment.

WPKI defines new certificate format in order to reduce the amount of storage required and adopts the Elliptic Curve Cryptography (ECC) [8]. ECC mechanisms are recognized as the best suited for supporting security in the wireless and mobile environment.

By using this scheme WPKI manages to ensure confidential sessions with strong authentication of the parties involved and it can guarantee data integrity. The most important is that it can offer non-repudiation at a level that makes it possible to turn to a third party for verification and this, as we mentioned before, is a basic requirement for successful m-commerce processes.

Another significant advantage is that WPKI can offer different keys for different functions. This happens because PKI simplifies the key management and whenever there is a need to verify a signature the public key is used without

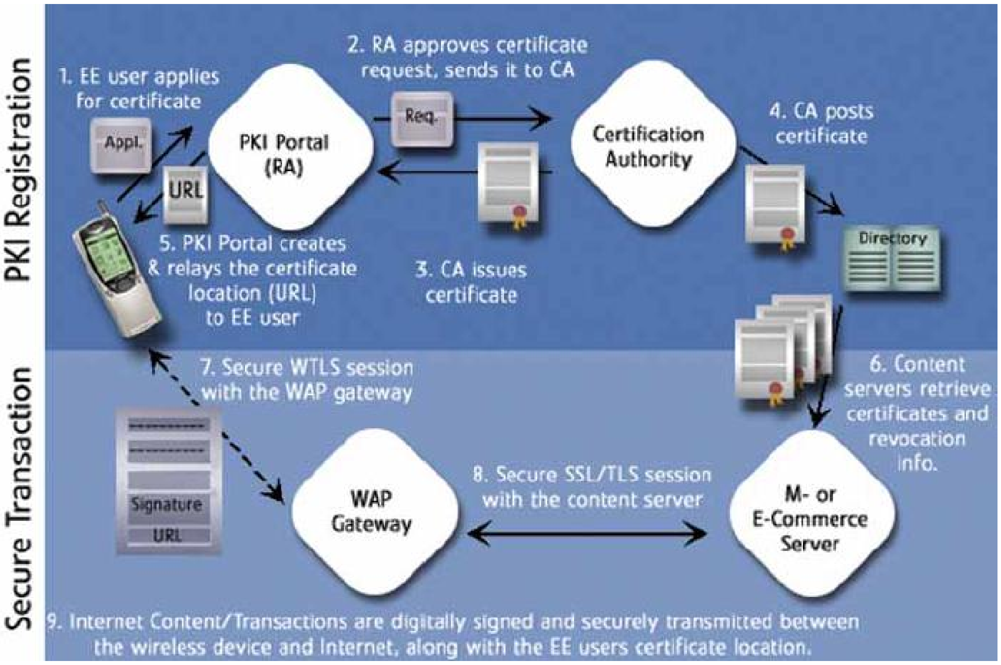
PKI Registration
Secure Transaction
1. EE user applies for certificate
Appl.
URL
PKI Portal (RA)
2. RA approves certificate request, sends it to CA
Req.
Certification Authority
3. CA issues certificate
4. CA posts certificate
Directory
5. PKI Portal creates & relays the certificate location (URL) to EE user
6. Content servers retrieve certificates and revocation info.
7. Secure WTLS session with the WAP gateway
Signature
URL
WAP Gateway
8. Secure SSL/TLS session with the content server
M- or E-Commerce Server
9. Internet Content/Transactions are digitally signed and securely transmitted between the wireless device and Internet, along with the EE users certificate location.

Fig.1 PKI Operation

needing to generate a private key and reproduce the transaction.

This is the main concept of WPKI without referring to important details. But, it is obvious by this short examination that WPKI is a matching technology to m-commerce being compatible with the requirements posed. Those requirements and specifically the non-repudiation property are mandatory in some countries by the local legislation.

The last technology that will be presented in this essay is the Pretty Good Privacy (PGP). PGP is a complete public-key cryptosystem for electronic messaging that has been released to the public domain. It was originally designed by Phil Zimmerman in 1991. Depending on the version, it uses IDEA, CAST or Triple DES for actual data encryption and RSA (with up to 2048-bit key) or DH/DSS (with 1024-bit signature key and 4096-bit encryption key) for key management and digital signatures. The RSA or DH public key is used to encrypt the IDEA secret key as part of the message.

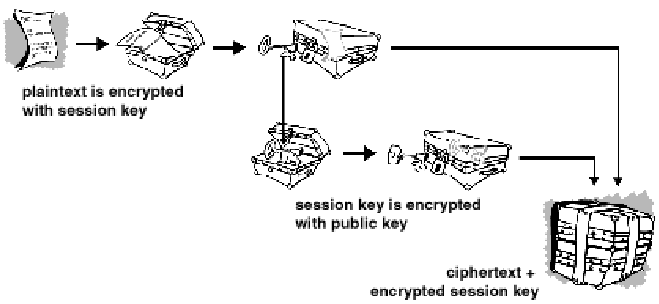
plaintext is encrypted with session key
session key is encrypted with public key
ciphertext + encrypted session key

Fig.2 PGP Operation

PGP is a hybrid cryptosystem and its advantage is that it first compresses the plaintext. This compression saves transmission time and disk space and, more importantly, strengthens cryptographic security [9].

Originally designed for mail services and internet use, it looms as an interesting solution in mobile services and to be more specific, it can offer strong digital signatures verification.

In summary, in PGP user creates a pair of keys, the private and the public key. Then the user passes his public key to anyone with whom he wants to contact. The important difference in PGP is that no trusted third party is needed. The user encrypts a message and he sends it to others using their public key. When they receive it, they decrypt it using their private key. Since encrypting an entire message can be time-consuming, PGP uses a faster encryption algorithm to encrypt the message and then uses the public key to encrypt the shorter key that was used to encrypt the entire message. Both the encrypted message and the short key are sent to the receiver who first uses the receiver's private key to decrypt the short key and then uses that key to decrypt the message [10].

The U.S. government restricted the exportation of PGP technology and the lack of a third party in its operation is a reason why. Today, however, PGP encrypted e-mail can be exchanged with users outside the U.S if you have the correct versions of PGP at both ends.

Of course PGP has serious vulnerabilities and it cannot offer a solution for m-commerce by itself. It can be used as part of a general solution or as a technology for limited e-commerce applications.

IV. General And Future considerations

At the previous section some technologies and practices about mobile communication security were presented. It is needless to say that they are not the only ones but from my study, I concluded that those are the widely proposed ones. Research is done on them and several new versions of these technologies are getting around day by day. Improvements, upgrades and research help the evolution towards a secure mobile future.

One future consideration is the implementation of SIM cards that could support cryptographic characteristics. Smart Cards based on PKI seem to be a very good solution. That solution proposes that the key will be embedded in a person’s cellular SIM-card. More ambitious suggestions propose the implementation of PKI Smart Cards. Those are smart cards, which are able to perform PKI related functions: the smart card is capable of handling sensitive encryption and of performing all digital signature and encryption functions. PKI smart cards seem to be an important element of m-commerce applications since they combine security, portability and ease of use.

Some versions of this implementation are already in use in some countries and the results are very satisfactory especially in the field of electronic payments.

All these are very encouraging but the restrictions that come to light from the capabilities of the mobile networks hold back the progress and the wide use of the mobile devices by the commercial world. The present situation is not favourable and the 3G mobile communication seems more adequate to fulfil the expectations of the m-commerce. UMTS and relevant technologies will really utilize the advanced capabilities of mobile devices. Device vendors run faster than the services providers offering the means. Complex and powerful devices are now available to everyone in very good prices.

Maybe the maturity that offered by bad experiences of the past, make service providers more patient and more careful. Starting from MMS, Video calls and even mp3 enabled devices the industry prepares the consumers for the bright future. When everybody will possess advanced devices the commercial part of mobile world will be offered as the new opportunity of the consumers.

We must not forget that few people will have a palmtop or a notebook, but everybody will have a mobile phone. In Greece mobile telephony penetration touches the 95 %. If m-commerce is secure and trustworthy, then the challenge is great for all market players.

V. Conclusion

Summarizing, it is obvious that there will be no m-commerce without security of the underlying technologies. On the other hand, the amounts of money and time society as a whole can save from implementing m-commerce are enormous. In the same time, businesses have a great opportunity to find new ways to promote and to sell their products without even needing a physical storehouse. Consumers will have control of their activities and a larger gamut of selections.

For technology itself, this is the last opportunity to prove that the underperformance of e-commerce was just a bad bracket in the evolution chain.

M-commerce is the future because will offer access to goods at any time, everywhere and on every mobile device via pervasive and ubiquitous computing. The grid will have value if it gains the trust of the consumers and the only way to achieve this is by ensuring security and trust.

References

[1] J.F. Kurose, K.W. Ross, *Computer Networking – A Top-Down Approach Featuring The Internet*, 3rd ed., Addison Wesley, 2005, pp. 708-709.

[2] J. Schiller, *Mobile Communications*, 2nd ed., Addison Wesley, 2003, pp. 137-148.

[3] J. Schiller, *Mobile Communications*, 2nd ed., Addison Wesley, 2003, pp. 397-399.

[4] http://www.openmobilealliance.org/tech/affiliates/wap/wapindex.html (URL)

[5] http://www.kannel.org/download/kannel-wtls-snapshot/wtls.html #AEN 287 (URL)

[6] J.F. Kurose, K.W. Ross, *Computer Networking – A Top-Down Approach Featuring The Internet*, 3rd ed., Addison Wesley, 2005, pp. 664-678.

[7] J.F. Kurose, K.W. Ross, *Computer Networking – A Top-Down Approach Featuring The Internet*, 3rd ed., Addison Wesley, 2005, pp. 679-690.

[8] http://en.wikipedia.org/wiki/Elliptic_curve_cryptography (URL)

[9] A.S. Tanenbaum , *Computer Networks*, 3rd ed., Prentice Hall, 1996, pp. 664-667.

[10] S. van Otterloo, *A security analysis for PGP*, 2001

Bibliography

[A] A.S. Tanenbaum , *Computer Networks*, 3rd ed., Prentice Hall, 1996

[B] J.F. Kurose, K.W. Ross, *Computer Networking – A Top-Down Approach Featuring The Internet*, 3rd ed., Addison Wesley, 2005

[C] J. Schiller, *Mobile Communications*, 2nd ed., Addison Wesley, 2003

Figures

Figure 1 is taken from PKI overview of Certicom Corporation, 2001. Wireless Public-Key Infrastructure - Certicom.pdf at WWW.CERTICOM.COM.

Figure 2 is taken from the url: http://www.pgpi.org/doc/pgpintro/#p10

Balafas Vasileios

Digitally signed by Balafas Vasileios
DN: CN = Balafas Vasileios, C = GR, O = DCOM, OU = DCOM
Reason: I am the author of this document
Date: 2005.12.11 19:43:36 +02'00'