MOBILE COMPUTING AND M-COMMERCE SECURITY ISSUES

Krishna Prakash[1] and Balachandra[2]

[1,2]Department of Information and Communication Technology, MIT Manipal
[1]kkp_prakash@yahoo.com,[2]bala_muniyal@yahoo.com

ABSTRACT

The radical evolution of computers and advancement of technology in the area of hardware (smaller size, weight, low power consumption and cost, high performance) and communications has introduced the notion of mobile computing. Mobile Commerce is an evolving area of e-commerce, where users can interact with service providers through a mobile and wireless network using mobile device for information retrieval and transaction processing. Mobile wireless market is increasing by leaps and bounds. The quality and speeds available in the mobile environment must match the fixed networks if the convergence of the mobile wireless and fixed communication network is to happen in the real sense. The challenge for mobile network lie in providing very large footprint of mobile services with high speed and security. Online transactions using mobile devices must ensure high security for user credentials and it should not be possible for misuse. The paper discusses issues related to M-Commerce security.

KEYWORDS

PKI, WPKI, Certificates, M-Commerce

1. INTRODUCTION

Mobile computing provides flexibility of computing environment over physical mobility. The user of a mobile computing environment will be able to access to data, information or other logical objects from any device in any network while on the move. To make the mobile computing environment ubiquitous, it is necessary that the communication bearer is spread over both wired and wireless media [2].

Mobile Computing technology evolved in various generation with changing technologies. The First generation (1G) mobile network was developed in USA and it was using Frequency Division Multiplexing technique (FDM). A data service was then added on the telephone network which was Cellular Digital Packet data (CDPD). The network could offer data rate of 19.2 kbps. The second generation (2G) mobile network is mainly Global System for Mobile Communication (GSM) and introduced in Europe and rest of the world. The network has dedicated data channels for data transmission.

The Third generation standards (3G) are developed by International Telecommunication Union (ITU) under International Mobile Telecommunication-2000 (IMT-2000) in order to create a global network. They are scheduled to operate in the frequency band around 2 GHz and offer data transmission rate up to 2Mbps. In Europe the ETSI (European Telecommunication Standard

David C. Wyld et al. (Eds) : COSIT, DMIN, SIGL, CYBI, NMCT, AIAPP - 2014
pp. 205–216, 2014. © CS & IT-CSCP 2014 DOI : 10.5121/csit.2014.4920

Institute) has standardised UMTS (Universal Mobile Telecommunication System) as the 3GNetwork.

The ITU has stated the flow expected by 4G generation should be around 1GBPS static and 100 Mbps on mobility regardless of the technology or mechanism adopted.

The rapid development of mobile communication technologies and rapidly growing number of mobile devices result in fast growth of Mobile commerce.

1.1 Mobile System Infrastructure

One of the most widely deployed cellular infrastructures is GSM or 2G and its designers had several goals. Better quality for voice, higher speeds for data, international roaming, protection against charge fraud and eavesdropping. The UMTS or 3G promised advanced services such as mobile internet, multimedia messaging, video conferencing etc. UMTS standards were defined by an international consortium called 3GPP (Third generation partnership project) [3].

Fundamentals of a cellular system

The generic block diagram of a cellular system is shown in the Fig 1 below.

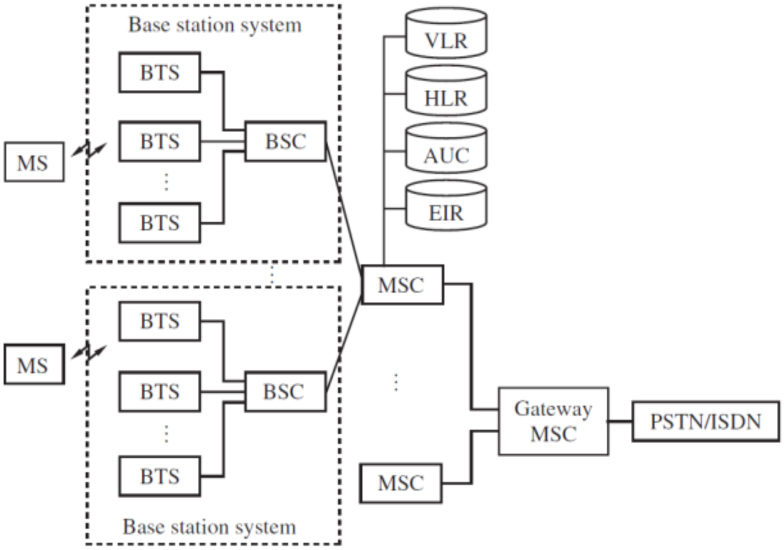

Fig 1: Cellular System

The basic geographical unit of a cellular system is called a cell is the geographical area covered by a transmitter. At the lowest level, a cell phone is connected to a base station (or base transceiver station) by a radio link. Multiple base stations are connected to and controlled by a base station controller. The connection between a base station and its controllers could be a microwave link, optical link in general any radio link. Multiple base station controllers and upstream are connected to Mobile switching centre. The Mobile Switching Centre (MSC) forwards an incoming call to the destination MSC. The MSC also keeps track of accounting and billing information. MSC are connected each other through wired networks such as Public Switched Telephone Network (PSTN).

The user has a subscription to some networks called as his home network. A one to one association between MSC and a network is maintained. An MSC has a database, called the Home Location Register (HLR) having information of all its subscribers. The data base contains the information of subscriber's mobile number, the services availed and a secret key stored in the mobile known only to the HLR. HLR also maintains the dynamic information of its roaming customers for charging. It includes the current location of a user and the cellular network used by the user [4].

A subscriber may avail the services of other networks (called as foreign networks) that have an agreement for roaming with subscriber's home network. Each cellular network also maintains a database called as Visitor Location register (VLR) of users currently visiting that network with the list of services the subscriber entitled to.2G technology introduced Subscriber Identity Module (SIM) card which stores three secrets used for cryptographic operations [5].

2. SECURITY IN POPULAR MOBILE NETWORKS

2.1 Security in GSM

There are two principal tasks involved for providing GSM Network security. They are:

a) Entity authentication and Key agreement
b) Message protection.

The integrity and encryption keys are agreed up on as a part of (a) and then they are used to protect messages between cell phone and base station.

a) Entity Authentication and Key Agreement

The GSM perform authentication to identify genuine users. The frequency of authentication is not specified, but the process is necessarily performed when the subscriber moves from one network to a new network. Fig 2 explains main steps involved in authentication.

1. Authorization request from Cell Phone: During authorization request step, the cell phone sends the encryption algorithm it can support to the base station and IMSI/TMSI number to the MSC. If the cell phone is away from its home network, the IMSI will be received by the MSC of the visited network. The latter communicates the IMSI to the MSC/HLR of the cell phones home network with a request to provide a challenge that will be used to authenticate by a cell phone.

2. Creation and transmission of authentication vectors:
   The IMSI obtained by the MSC is used to index the home location registers to obtain a shared key, Ki known only to the SIM and HLR of the home network. The MSC/HLR generates 128 bit random number, RAND, which functions as a challenge in the challenge-response authentication protocol. The two quantities XRES and Kc are computed as below.

XRES=A3 (RAND, Ki)
Kc=A8 (RAND, Ki)

Where, A3 and A8 are two keyed hash functions. XRES is the expected response in the challenge response authentication protocol. Kc is the encryption key. The HLR creates five authentication triplets, each seeded by freshly chosen random numbers. Each triplet is of the form-

<RAND, XRES, Kc>

The triplets are sent to the MSC of the home network by the HLR. If the cell phone is visiting a foreign network, the MSC forwards the triplets to the MSC of the visited network. Five triplets are sent so that four subsequent authentications may be performed without the need to repeatedly involve MSC/HLR of the home network.

The MSC sends the challenge (RAND) from the first triplet to the base station and it is forwarded to SIM on the cell phone.

3. Cell Phone response:

Once the SIM has received RAND, it computes SRES (Signed Response) similar to XRES. It can be computed by an entity with the knowledge of Ki, key shared between the SIM and HLR. The cell phone sends SRES to the base station and it is forwarded to MSC. The MSC compares if SRES is equal to XRES and if they are same MSC concludes that SIM knows Ki and identifies it as a genuine subscriber.

4. Computation/Receipt of encryption key:

The SIM computes Kc and MSC extracts Kc from its authentication triplet and communicates it to the base station. Further all communications between cell phone and base station are encrypted using Kc.

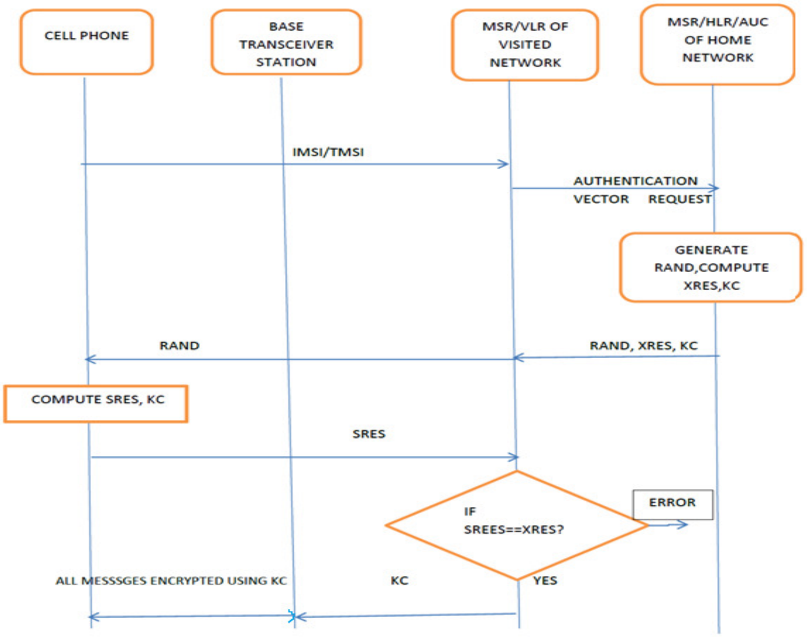
CELL PHONE
BASE TRANSCEIVER STATION
MSR/VLR OF VISITED NETWORK
MSR/HLR/AUC OF HOME NETWORK
IMSI/TMSI
AUTHENTICATION VECTOR REQUEST
GENERATE RAND,COMPUTE XRES,KC
RAND
RAND, XRES, KC
COMPUTE SRES, KC
SRES
IF SREES==XRES?
ERROR
ALL MESSSGES ENCRYPTED USING KC
KC
YES

Fig 2: Authentication steps in GSM

b) Message Protection

Stream cipher technique is used to encrypt the message transmission between cell phone and base station. The key stream generator for this is denoted as A5. The key stream is a function of the 64 bit encryption key, Kc, and 22 bit frame number.

KEYSTREAM= A5 (Kc, FRAME_NUMBER)

For each frame transmitted, the frame number is incremented which changes the key stream for each frame sent during a call. Usually cipher text is generated by X-OR ing the plain text and the key stream.

Computation of the key stream and encryption do not require any static information stored in the SIM. Computation of XRES and Kc requires the subscriber authentication key, Ki. Hence the functions A3 and A8 must be supported by the SIM and A5 typically not.

2.2 Problems and drawbacks

There are some security shortcomings identified in GSM. The first flaw is related to authentication of the subscriber as illustrated in the following Fig 3 The system uses temporary identifier, Temporary Mobile Subscriber Identity (TMSI) to prevent the identity. If the VLR could not recognize or TMSI is lost, the IMSI is transmitted in plain text. There is no possibility of encrypting IMSI with A5, RAND is transmitted only after the successful authentication of the system is happened. This flaw may be exploited by using forged BTS and BSC. Unless the IMSI is transmitted in plain text subscriber is rejected. This type of attack is not common in principle in GSM networks and could be fought by a mutual subscriber-BSS authentication.

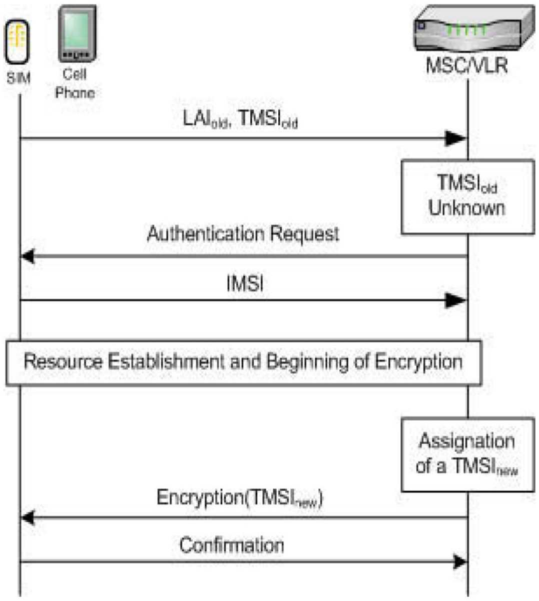

Fig 3: Unknown TMSI and plaintext IMSI transmission

In GSM, the SIM is authenticated to the network, but authentication of network is not carried out as a part of GSM protocol. This could result in false base station attack where an attacker poses as base station by sending more powerful beacon signals than legitimate base station. The attacker may spoof the cipher mode command from base station and it suppresses the encryption in cell phone. As a result attacker may eaves drop entire communication.

The messages are encrypted only between the base station and cell phone, not beyond. The link between the base station and the base station controller is a microwave link and messages are transmitted in clear. Such links can be eaves dropped and defeating the purpose of GSM encryption.

Another flaw comes from SIM card cloning. If an attacker succeeds in cloning a SIM card and then turns a Mobile Network (MN) on, the network will detect two mobile devices with same identifiers at same time and will close the subscription and thus impeding identity thefts. Such attacks go undetected if the attacker is only interested about eavesdropping. If the intruder has access to secret key Ki and receives RAND may generate the encryption key Kc and passively decrypt the communication between cloned MN and attached BTS. This may be prevented by injecting copy protections and making them un clonable.

The major GSM security flaws find their origin in lack of any form of mutual authentication and plain text transmission of secrets. These flaws are identified and addressed in UMTS.

2.3 Security enhancements in UMTS

The 3G Security system define a higher security management for UMTS networks. New security provisions have been added such that detection of rogue base stations, network mutual authentication, strict control over the transmission of secret keys, longer encryption keys etc. GSM SIM card is replaced with more powerful chip called as USIM (Universal Subscriber Identity Module). Following features are built into UMTS to overcome the shortcomings of GSM.

1. False base station problem is impossible in UMTS, since each signalling message is individually authenticated and integrity protected.
2. GSM does not support mutual authentication of network and cell phone. In UMTS, as a part of mutual authentication protocol, the SIM card and the network agree on an encryption key and also a key for integrity protection of messages. To prevent replay attacks, the sequence numbers and nonce are used.
3. Data and signalling messages are encrypted. Both integrity protection and encryption are based on KASUMI-a 128 bit block cipher.
4. Messages on all wireless links are encrypted, not the link between cell phone and the base station. The algorithms for encryption and integrity can be negotiated between the SIM and the network.

2.4 Authentication and Key Agreement (AKA) in UMTS

The Fig 4 and Fig 5 discuss the AKA in UMTS by exploring the main difference with GSM.

a) Authorization request from cell phone:

This step is identical to that of GSM.

b) Creation and transmission of authentication vectors:

The HLR for the home network generates a random number, RAND functioning as a challenge in challenge-response protocol. Various keys such as “anonymity key (AK)”, an integrity check key IK and a cipher key CK, a MAC and an authentication token (AUTN) are computed. The keys and expected response, XRES are derived using keyed hash functions F2, F3, F4, and F5 as follows.

XRES= F2 (RAND, Ki) ……… ..(1)
CK= F3 (RAND, Ki)………… . . (2)
IK= F4 (RAND, Ki)……………. (3)
AK= F5 (RAND, Ki)…………… (4)

The HLR computes MAC (Message Authentication Code) using another keyed hash function F1.
MAC= F1 (RAND, Ki, AMF, SQN) ………. (5)

Here AMF is the Authentication Management Field containing the lifetime of the key. SQN is the secret sequence number known only to the HLR and SIM to maintain the synchronization between two. The HLR next creates an authentication token as follows.

AUTN= (SQN XOR AK, AMF, MAC)

Finally HLR produces five authentication vector quin tuplets as shown in Fig 2.6. each of the form,

(RAND, XRES, CK, IK, AUTN)

The SQN is incremented each time when a new authentication vector is created and RAND for each authentication vector is chosen a new.

The Authentication vectors are forwarded to the MSC/VLR of the visited network. Only once a single authentication vector is used for the authentication of SIM and MSC/VLR. The remaining authentication vectors may be used by MSC/VLR in future without the involvement of home network of the cell phone.

The RAND and AUTN of the first authentication vector is dispatched to the base station controller by MSC/VLR. The BSC forwards it to the SIM.

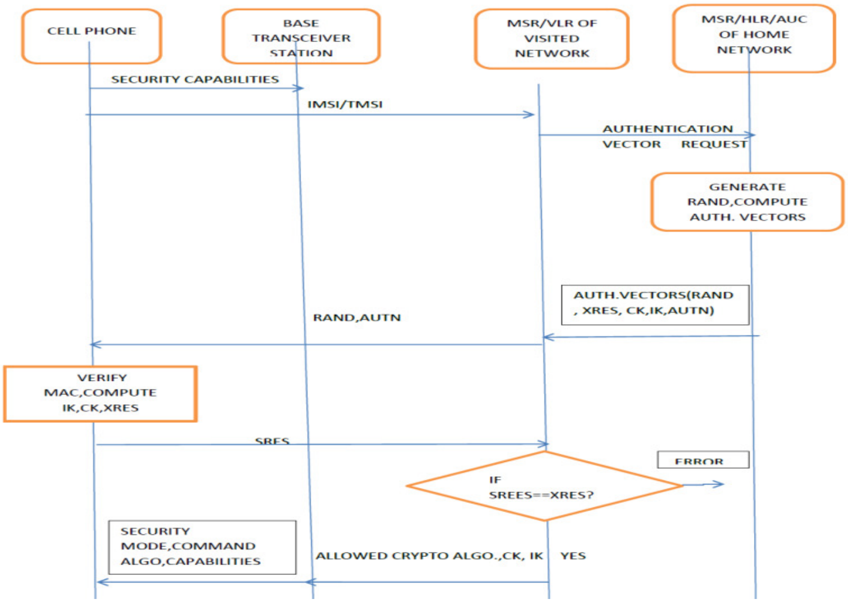
CELL PHONE
BASE TRANSCEIVER STATION
MSR/VLR OF VISITED NETWORK
MSR/HLR/AUC OF HOME NETWORK
SECURITY CAPABILITIES
IMSI/TMSI
AUTHENTICATION VECTOR REQUEST
GENERATE RAND,COMPUTE AUTH. VECTORS
AUTH.VECTORS(RAND , XRES, CK,IK,AUTN)
RAND,AUTN
VERIFY MAC,COMPUTE IK,CK,XRES
SRES
ERROR
IF SREES==XRES?
SECURITY MODE,COMMAND ALGO,CAPABILITIES
ALLOWED CRYPTO ALGO.,CK, IK
YES

Fig 4: Authentication Protocol

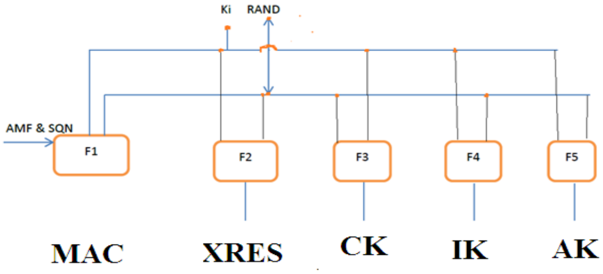

Fig 5: Authentication vector computation

c) Verification of authentication token and cell phone response

The SIM computes Authentication vector AK using equation (1) , the RAND it received and its copy of Ki. Also it retrieves first element of received AUTN, (SQN XOR AK) and it computes the value of SQN from (SQN XOR AK) XOR AK. After computation, it checks whether the difference between computed SQN and stored SQN is with in acceptable range. If it is OK, the SIM computes the MAC using equation (5). If the computed MAC and received MAC in AUTN matches , the SIM concludes that the authentication vector is created by HLR of the home network and authentication vector is fresh and not a replay. The SIM stores the SQN value it stored with the new value computed.

The SIM computes the response, SRES to the challenge, RAND (from HLR) using equation (1) and sends SRES to the MSC/VLR. The MSC/VLR compares both and if matches it proves that the SIM know Ki and completes authentication of SIM to the network.

At the SIM computes CK and IK and conveys these to the cell phone for providing encryption and integrity checking for all future communication between BSC and cell phone.

d) Agreement on Encryption and Integrity check Algorithms

The MSC/VLR sends a list of permissible MAC and encryption algorithms to the base station controller. The latter has received that from the first step and the BSC sends the list of supported algorithms back to cell phone. This message has an integrity check to prevent an attack from spoofed messages with weak options (may be no encryption). The BSC also receives CK and IK to be used for encryption and integrity protection of all messages between it and the cell phone.

3. Mobile Commerce - Risks, Security And Payment Methods

A Mobile Payment is defined as a payment for product or services between two parties for which a mobile device plays a key role in the realization of payment. In an M-Payment activity a mobile phone is used by the payer in one or more steps during banking or financial transactions. The ubiquity of cell phones together with the convenience it offers suggests that mobile payments will constitute an increasing proportion of electronic payments.

Mobile applications can be either be mobile web or native. Security issues in mobile web applications closely resemble those of traditional web applications because of homogeneity in underlying development technologies and protocols [6]

There are mainly two types of mobile payments as listed below [7].

1. Proximity Payment
2. Remote Payment

In Proximity Payment, the payer and payee are located nearby and they are very close to each other. Some examples for this category of payment are the customer paying the money using their plastic cards in a Point of Sale Terminal or Customers Cell phone making a payment in a vending machine.

In remote Payment, the payer and payee are located at different locations –for example they may be at different cities.

3.1 M-Payment Life cycle

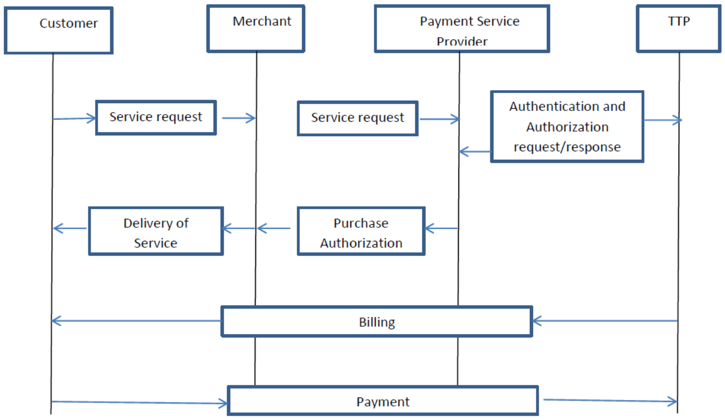

Fig 6: M-Payment life Cycle

Payment transaction in a mobile environment is very similar to a typical payment card transactions shown in Fig 6. It differs in the transport of payment detail involved i.e. wireless device using WAP/HTML based browser.

Mobile payment lifecycle has the following main steps.

1. Registration: Customer opens an account with payment service provider for payment service through a particular payment method.

2. Transaction: Transaction mainly comprised of following four important steps.

a) The desire of a customer is generated using a SMS or pressing a mobile phone button.
b) The content provider forwards the request to the payment service provider.
c) Payment service provider then requests a trusted third party to authenticate and authorize the customer.
d) Payment service provider informs content provider about the status of the authentication and authorization. If successful authentication of the customer is performed, content provider will deliver the requested goods.

3. Payment settlement: This operation can take place during real time, prepaid or post-paid mode. A real time payment involves the exchange of some form of electronic currency, for example payment settlement directly through a bank account. In prepaid type of settlement customers pay in advance using smart cards or electronic wallets. In post pay mode the payment service provider sends billing information to the trusted third party, which sends the bills to customers, receives money back, and then sends the revenue to payment service provider.

3.2 Wireless Public Key Infrastructure (WPKI) based M-Commerce Security System

Public key cryptography technique is used as backbone for the WPKI to provide security in m-commerce. The entire certificate management life cycle activities starting from certification creation, generation, storing, distribution and revocation of public key certificate is supported by an WPKI architecture. Fig 7 below illustrates various components existing in an integrated WPKI system [8]

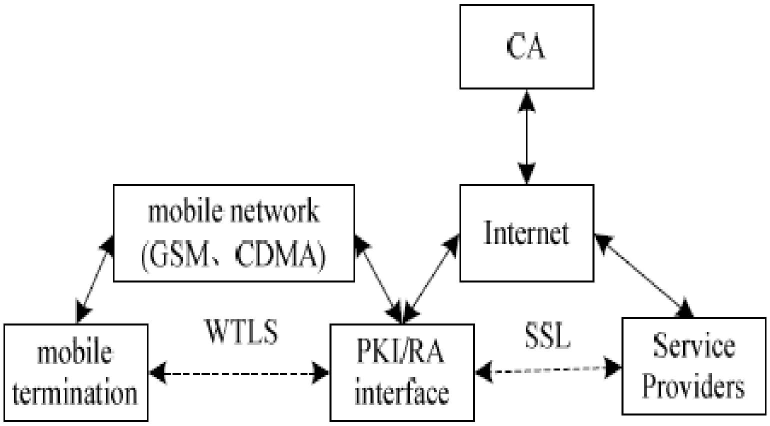

Fig 7: Components of M-Commerce security architecture

WAP is the key entity in an wireless environment for connecting the internet. WTLS is the lighter version of TLS and it is suitable for wireless environment. For the secure connection and communication between service providers SSL is used.

3.3 Secure Transmission Process between Mobile terminal and application server

The following Fig 8 depicts the architecture of secure transmission adopted in mobile commerce proposed by [9][10].

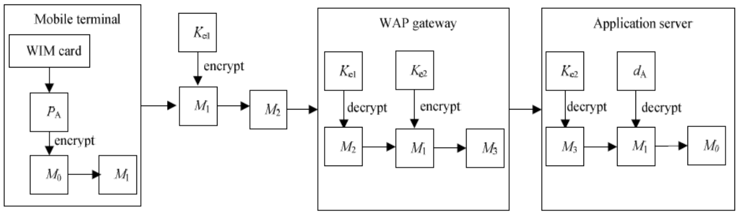

Fig 8: Secure data transfer between source and server

Following are the notations used in above diagram.

P_A- Public key of the application server
K_{e1}- The key between mobile terminal and WAP gateway
K_{e2}- The key between WAP gateway and application server
M_0- Message at mobile end
M_1- Message encrypted by P_A
M_2- Message encrypted with K_{e1}
M_3- Message encrypted with K_{e2}

The public key of application server P_A is used to encrypt the message M_0 and produces M_1. The message M_1 is then encrypted using the key K_{e1} of WAP gateway to get M_2 and sent to WAP gateway. The WAP gateway decrypts the message M_2 with Key K_{e1} to get original encrypted message M_1. The WAP gateway encrypts the message M_1 using K_{e2} and obtains M_3 and sends M_3 to application server. The application server will decrypt M_3 with K_{e2} and get M_1, and decrypts M_1 with its own private key and gets original message.

The above model has some draw backs.

1. The symmetric keys K_{e1} and K_{e2} needed to be generated and shared between WAP gateway and mobile device and Application server and WAP gateway securely.
2. The mechanism does not have any mechanism of verification of mobile user, WAP gateway and application server, so the chances of fraud is high. The following suggested modifications could be implemented for improved security.
3. Public key cryptography can be used to generate a pair of public key and private key and it can be used for both authentication and confidentiality.
4. The use of digital certificates can be used as a mean for authenticating mobile device and application server.

5. CONCLUSION

The widespread use of mobile devices now a day generates huge amount of revenues by reducing time and money needed for multiple purposes. The rapid development in mobile computing technology not only creates several opportunities for the business and also opens the door for doing disasters using misuse of technology. The information residing in the mobiles and integrity of the information, security of the information during its journey over the air security of the information with in the wireless network has to be given much importance.

Because of Mobile Computing or Mobile networks, M-Commerce has become reality today. The support of large number of cellular network service providers with competing speed made user to use his mobile device as a transacting module rather than simply using it for making calls.

REFERENCES

[1] Mahmoud Elkhodr, Seyed Shahrestani and Kaled Kourouche,“ A Proposal to improve the security of mobile banking applications”, IEEE International conference on ICT and Knowledge Engineering, 2012

[2] Ashok K Talukder and Roopa R Yavagal, “Mobile Computing”, TaTa McGraw Hill Education, January 2005

[3] Hua Ye, “Design and Implementation of M-Commerce system applied to 3G Network platforms based on J2ME”, IEEE International conference on Electrical and Control Engineering, 2010

[4] Dharma prakash agrawal and Qing An Zeng, “Introduction to Wireless and Mobile Systems”, Third Edition, Cengage Learning USA

[5] Hakima Chaouchi and Maryline Laurent maknavicius, “Wireless and Mobile Network Security”, Second Edition, Wiley Publishers

[6] Anurag Kumar jain and Devendra Shanbhaug, “ Addressing Security and Privacy Risks Mobile applications”, IEEE Computer society, 2012

[7] Bernaard menezes, “ Network security and cryptography”, CENGAGE Learning, econd edition

[8] Feng Tian et al., “ Application and Research of Mobile E-commerce security based on WPKI”, IEEE International Conference on Information Assurance and Security, 2009

[9] CUI Jian-qi and YAO Dan-li, “ New secure mobile Electronic commerce solution based on WAP [J].Application Research of Computers Vol.24 No.9 2007(9)

[10] ArunKumar Gangula et al., “Survey on Mobile Computing Security”, IEEE Computer Society, 2013