Security Challenges and Solution to M-commerce

Angitha Jeesis C

Assistant Professor,
BCM College

***Abstract*: In this material security of m-commerce are defined. M-commerce has emerged as an innovative technology due to the prevailing of pervasive computing. It enables users to engage wirelessly in online trading regardless of time or location. However, on-line secure transaction mechanisms cannot be applied to the mobile commerce due to the inadequate computing capability of mobile devices and lower security of wireless transmission than that of wired transmission. It is important how to proceed securely with the transaction of on-line ordering and, in the meantime, to obtain proper protection of transaction issued by consumers via mobile devices. Security in m-commerce applications is very important both at the administrative level and from the user perspective. The new trend in the field is the m-commerce that involves making purchases through mobile devices. For m-commerce transactions the security is a very important thing. Here how to analyze the security of m-commerce transactions and ways to increase security for these transactions taking into account the organization of m-commerce applications, software used, hardware used and other important issues in the development of these applications. This paper project on the analysis of the secure connection mechanisms in the mobile commerce.**

INTRODUCTION

Mobile Commerce is the use of information technologies and communication technologies for the purpose of mobile integration of different valued and business processes, and for the purpose of management of business relationships. The core of mobile commerce is the use of a terminal (telephone, PDA, PC device, or custom terminal) and public mobile network to access information and conduct transactions that result in the transfer of value in exchange for information's, services or goods.

M-Commerce makes people's lives comfortable and provides the security to the user. M-Commerce had a use of technological shift from 2G to 4G. Fourth generation provides a wide array of abilities besides basic voice communication, such as multimedia transfer and streaming, video conference, and complete connection to the web. 4G systems with more security, high speeds, high capacity, low costs and more intelligent infrastructures and devices will help realize m-commerce applications.

Mobile commerce represents the using of mobile devices for communication and implementation of electronic commerce transaction or any transactions with monetary value achieved through mobile devices. It appeared due to the rapid evolution of the mobile devices and connection among internet became more accessible regardless of the geographical location of the person.

SECURITY CHALLENGES TO M-COMMERCE

As stated earlier, M-Commerce is not possible without a secure environment, especially for those transactions involving monetary value. The security challenges of M-commerce are listed below:

1. Accessing the internet by mobile phones is currently slowed down transmission speeds, frequent disconnects, cost of wireless connection and wireless communication standards over which data is transmitted.
2. High speed bandwidth internet connection not available to most citizens at an affordable rate.
3. Payment system that connects the utility of the mobile phone and the Internet together.
4. Limited Internet access, lack of awareness about services and security.
5. Lack of penetration of mobile device in rural area.
6. Multiple issues of trust in M-Commerce technology, doubts about M-Commerce security, and lack of widely accepted standards and lack of payment gateways.
7. To implement Ubiquitous IT Infrastructure and its maintenance

A customer must be able to trust a mobile payment application provider that his or her credit or debit card information may not be misused. When these transactions become recorded customer privacy should not be lost that the credit histories and spending patterns of the customer should not be openly available for public scrutiny. The system should be fool proof, resistant to attacks from hackers and terrorists.

Data security is importance due to the fact that online transactions processing personal data, especially data regarding bank accounts and financial resources of the users. Internet transaction has three components,

1. User - the person entering the site to buy;
2. Server - representing business owner;
3. Connection of the two components

Security Threats

We can go through mainly three common security threats: spoofing, sniffing and tampering. Whenever data is being transferred, either over a wireless or wired network, we need to take precautions against these risks.

Spoofing:

Spoofing is important threats that an attempt by a party to gain unauthorized access to an application or system by pretending to be someone he or she is not. If the spoofer gains access, he can create fake responses to messages and gain further knowledge and access to other parts of the system. Spoofing is a major problem for Internet security, because a spoofer can make application the users believe that they are communicating with a trusted source, such as bank, when in reality they are communicating with an attacker machine. Without knowing, users often provide additional information that is useful to the attacker to gain access to other parts and other users of the system. The process of sniffing is often used in conjunction with spoofing to get enough information to access the system in the first place. For this reason, implementing both authentication and encryption is required to combat spoofing.

Sniffing

Sniffing is another technique used to monitor data flow on a network. While sniffing can be used for proper purposes, it is more commonly associated with the unauthorized copying of network data. In this sense, sniffing is essentially electronic eavesdropping. By listening to network data, unauthorized parties are able to obtain sensitive information that will allow them cause any damage to the application users, the enterprise systems, or both. It is dangerous because it is both simple to do and difficult to detect. Sniffing tools are easy to obtain and configure. In fact, Ethernet sniffing tools come with the Microsoft Windows NT and 2000 operating system; fortunately, these tools are simple to detect. For this combat the more sophisticated sniffing tools, data encryption is the best defence. If an unauthorized user is able to access encrypted data, he or she will lack a way to decrypt it, essentially making it useless.

Tampering

Data tampering is also called an integrity threat, involves the malicious modification of data from its original form. In this involves intercepting a data transmission, although it also can happen to data stored on a server or client device. The modified information is then passed off as the original. Employing data encryption, authentication and authorization are the ways to combat data tampering.

SECURITY ENVIRONMENT

Five basic security concepts are:

A. Confidentiality

Today one of the major assets for any organization is data. To make it secure and confidential, we need to keep information safe from unauthorized access, for example, any personal information, bank account, government documents, credit card numbers etc. For privacy reasons, we need to keep data safe and secure.

B. Integrity

Data integrity is assurance that the data has not been altered or corrupted in any way during the transmission from the sender to the receiver. This can be accomplished by using data encryption in combination with a cryptographic checksum or Message Authentication Code (MAC).This information is encoded into the message by applying an algorithm to the message. When recipients received the message, they compute the MAC and compare it with the MAC encoded in the message to see if the codes are the same. If they are, recipients can be confident about that the message has not been tampered. If the codes are different, recipients can discard that data as inaccurate.

C. Availability

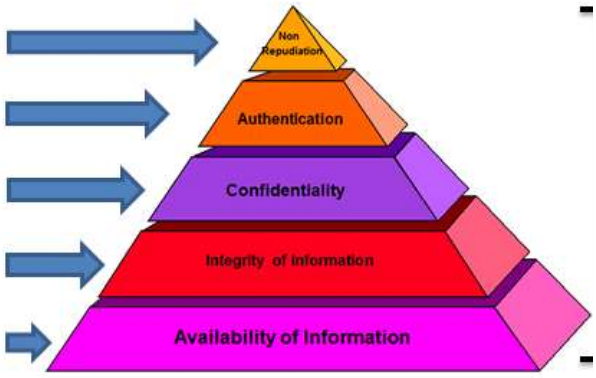
Authorized user can access data only when data is available. Data holds value only if the right user can access at the correct time. Hence to access data, the user needs to have permission to use the data.

D. Authorization

It is the process of determining the user's level of access, whether a user has the right to perform certain actions. Authorization is often closely tied to authentication. Once a user is authenticated, the system can determine what that party is permitted to do so.

E. Non repudiation

Non repudiation is about making parties accountable for transactions in which they have participated. This concept involves identifying the parties in such a way that they cannot at a later time deny their involvement in the transaction. In essence, it means that both the sender and the recipient of a message can prove to a third party that the sender did indeed send the message and the recipient received the identical message.



M- Commerce Security Concern

SECURITY TECHNOLOGIES

M-COMMERCE needs several layer of security

i) Device security

Design of mobile device there are number of high quality security features

a) A build in password mechanism which will lock after several mistyped attempts

b) An industry approved, tamper-proof smart card known as SIM

ii) Language security

Language Security is an important feature in M-Commerce. There are several ways for this. Java execution is one among the method, which is feasible for PDA, Smartphone's, laptop and other platform.

iii) Wireless security

WAP

Wireless Application Protocol is an open, global specification protocol which empowers mobile users with wireless devices to easily access and interact with information and services instantly. WAP is the only publicly available solution for wireless communication and it enables M-Commerce where internet data moves to and from wireless devices in a secure way with the help of various protocols and security features. The phones with WAP can access interactive services such as information, location-based services, corporate information and inter-active entertainment. WAP is targeted at various types of HWD(Handled Wireless Device) and Bluetooth enabled mobile phones.

WAP Security

WAP 1.x security used the Wireless Transport Layer Security (WTLS) protocol. This protocol is the WAP equivalent of Secure Socket Layer (SSL) and it provides authentication, encryption and integrity services.

WTLS supports some important algorithms like Diffe-Hellman, RC5, SHA-1, IDEA. It also supports some methods like DES and 3DES, but it does not support Blowfish and PGP. Since Web and WAP-based protocols are not directly interoperable, a component knowns as the WAP gateway is needed in order to translate Web-based protocols to and vice-versa. The WAP gateway is a software which runs on the computer of the Mobile Service Provider (MSP). Thus sensitive information is translated into original unencrypted form at the WAP gateway. This problem is called as WAP gap. PKC is used to exchange a symmetric key using certificate and then all transmission is encrypted. A short key size of 40 bits is used because of power limitation. A tamper-proof component, known as WIM (Wireless Identity Module) is designed as part of the WAP architecture to store private data, such as key pairs, certificates, and PIN numbers within the mobile device. In practice, a WIM is implemented using a smart card. Wireless Markup Language (WML) is used in WAP 1.x technology.

WAP 2.0 security uses Transportation Layer Security instead of WTLS due to requiring end-to-end security with all IP based technology in order to overcome the WAP gateway security breaches. It is a Public Key Infrastructure enabling protocol that provides the services such as authentication by using digital signatures and public key certificates, confidentiality by encrypting data, etc. This protocol uses RSA, 3DES, and SHA-1 algorithms for encryption.

PKI/WPKI

PKI(Public Key infrastructure) systems and WTLS(Wireless Transport Layer Security) are at the heart of mobile security technology. In a WAP(Wireless Application Protocol) environment WTLS must be translated at the WAP gateway into SSL, the Internet standard. A PKI is a set of policies, processors, software, hardware that enables the use of technologies, such as digital signatures and encryption. PKI's deliver the elements essential for a secure transfer of information and supports a wide variety of M-Commerce applications.

PKI must ensure the following security concerns:

1) Confidentiality, achieved by cryptography
2) Authentication, achieved by digital certificates

3) Integrity, achieved by digital signatures and
4) Non-repudiation, achieved by digital signatures and certificates.

PKI consists of the following components:
(i) Certificate Authority (CA)- responsible for issuing and revoking certificates, (ii) Registration Authority (RA)- binding between public key and the identities of their holders, (iii) Certificate Holders- people, machine or software agents that have been issued with certificates and can use them to sign digital documents, (iv) Verification Authority (VA, Clients)- validate digital signatures and their certificates from a known public key of a trusted CA, and (v) Repositories- stores that make available certificates. WPKI is an optimized extension of traditional PKI for the wireless environment. WPKI encompasses the necessary cryptographic technology and a set of security management standards that are widely recognized and accepted for meeting the security needs of M-Commerce

IV) Cryptography security

Cryptography

The basic concept of cryptography is to allow two parties to communicate over an insecure channel without a third party being able to understand what is being transmitted. This capability is one of the important requirements of a secure environment, as it deals with all aspects of secure data transfer, including authentication, digital signatures, and encryption.

Algorithms and Protocols

The algorithms describe the steps required to perform a particular computation, typically the transformation of data from one format to another. The protocol describes the complete process of executing a cryptographic activity. Because an excellent cryptographic algorithm does not necessarily translate into a strong protocol. The data transmission and key exchange are also properties of a protocol. A strong protocol does not guarantee strong security, as the application itself may lead to further problems. In order to create a secure solution, a strong protocol is required, as well as a good, robust application implementation.

Data Encryption

The main concept of any cryptographic system is encryption, the process of taking a regular set of data, called plaintext, and converting it into an unreadable form, called cipher text. Encryption allows maintaining the privacy of sensitive data, even when accessed by unauthorized users. The data can be read only by transforming it back to its original form using a process called decryption. The method of encryption and decryption are called algorithm or cipher.

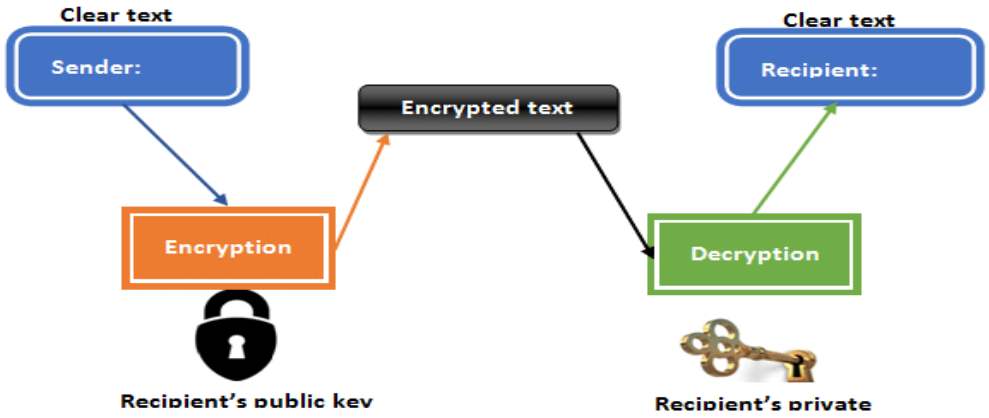


Figure: demonstrates the concept of encryption.

If the message is transported over an insecure public channel, it is encrypted, preventing eavesdropping on the line from being able to understand the data being sent. Modern algorithms use keys to control the encryption and decryption of data. Once a message has been encrypted, it can only be decrypted by users who have the corresponding key. Two types of algorithms are: symmetric and asymmetric.

Symmetric algorithms:
They are efficient. It use a single key to encrypt and decrypt all messages. The sender uses the key to encrypt the message and then sends the message to the intended recipient. Once the message is received, the recipient uses the same key to decrypt the message. Unfortunately a big problem arises when exchanging data between loosely related parties, such as an e-commerce Web site and a customer. Exchanging the key is a problem, this method is only useful between private parties. Symmetric encryption is also known as secret-key encryption. The most popular form of this method is the Data Encryption Standard (DES). More secure forms of symmetric encryption is Advanced Encryption Standard (AES), Triple DES; International Data Encryption Algorithm (IDEA); Blowfish; and the Rivest family of algorithms, RC2, RC4, RC5, and RC6.

Asymmetric algorithm:
The main problem that has plagued symmetric key systems is the use of a single key. Diffie and Hellman developed a solution using two separate but related keys one to encrypt the data and another to decrypt it. The key is used to encrypt the data is public key. Public key can be widely distributed over insecure lines, for general public use. The key used to decrypt the corresponding data is private key. 64 bit key systems, such as DES, are capable of being attacked by brute force. The more common 128-bit systems,

such as ECC, have proven invulnerable to brute-force attacks. Here is an example of how asymmetric, or public key cryptography works. Suppose a person A wants to send a secure message to the person B. A can use B's public key to encrypt the message. It then sends the message to B. When he receives the message, he uses his private key, to decrypt the message. Now A is able to send a secure message to B without having to do a key exchange. If the information is to be exchanged in both directions using asymmetric encryption, each party must have his or her own public key and private key combination.

Some asymmetric key algorithm are RSA, Elliptic Curve Cryptography (ECC) and Diffie-Hellman (DH). ECC, which is much less expensive in terms of processing power and key size, which are essential attributes in mobile computing than RSA .Asymmetric ciphers provide a solution to the key distribution problem by using a public key and a private key, but computationally slower than symmetric ciphers.

Conclusions

Due to increasing the number of users who choose to order products and services online led to the implementation of new methods and concepts of online business. The future seems promising with new 4G technology. Mobile-commerce solutions increase the number of users and thus increase the number of potential customers. However, an increased number of possible mobile users in the field of online commerce are also a growing number of potential people to be victims of cybercrime. Therefore, the implementation of mobile services to ensure access to the m-commerce options must take into consideration the security for these services, so the transfer of data with personal character and especially of bank accounts accessing data is to be achieved only by people legal owner. Identifying vulnerabilities and their control or eradication increase trust that users give mobile commerce services. The M-commerce is expected to become more secure as government and companies alike are investing on security etc. to provide better services to safeguard interests of users of M-commerce.