Mobile Commerce and Its Security Issues

A.O.M Asaduzzaman, Md. Nazrul Islam

Abstract— **This paper deals with m-commerce and its security issues. We described m-commerce in detail from theoretical perspective. In the early age of the world, transactions in commerce were performed by some means of exchange of physical goods or wealth in face-to-face and hand-to-hand manner. Over time it became some means of symbolic wealth called money or coin. After the invention of telecommunication, commerce is done by telephone with e-money (in e-commerce) by Internet. However, for further evolution of technology such as telecommunication, e-commerce is evolved to m-commerce (mobile commerce). We described the m-commerce system structure and related technologies which conduct m-commerce. All types of threats and challenges are described from their field of affection. The contemporary solutions and protections against these threats are properly outlined.**

Index Terms— **M-commerce, E-commerce, GSM, UMTS, 2G, 2.5G, 3G**

I. INTRODUCTION

With the introduction of the World Wide Web, electronic commerce has revolutionized traditional commerce and boosted sales and exchanges of merchandise and information. Recently, the emergence of wireless and mobile networks has made possible the extension of electronic commerce to a new application and research area i.e. mobile commerce. An m-Commerce transaction is defined as any type of transaction of an economic value that is conducted through a mobile device that uses a wireless telecommunications network for communication with the e-commerce infrastructure. Future applications include buying over the phone, purchase and redemption of ticket and reward schemes, travel and weather information, and writing contracts on the move. However, the success of m-commerce very much depends on the security of the underlying technologies. For m-commerce to take off, fraud rates have to be reduced to an acceptable level. As such, security can be regarded as an enabling factor for the success of m-commerce applications. The objective of this paper is to explore mobile-commerce and its security threats associated with m-commerce and its underlying technologies.

II. MOBILE COMMERCE

"M-Commerce is the buying and selling of goods, services or information without any location restrictions, by mobile device which uses a wireless connection to establish communication between all necessary parties to complete the transaction" [1]. Mobile commerce can be B2B (Business to Business), B2C (Business to Customer), C2C (Customer to Customer). M-Commerce is nothing but E-Commerce with mobile devices. M-Commerce has some challenges, which is not present in E-Commerce such as security challenges, heterogeneous technology challenges and usability challenges. Mobile-Commerce is superior from e-commerce for following features: Ubiquity, Accessibility, Localization, and Personalization. M-commerce has some limitations as well i.e. limited capacity, heterogeneity, theft, easy destruction and security threat.

Manuscript received Jan 14, 2015

A.O.M Asaduzzaman, Dept. of Computer Science & Engineering, Islamic University, Kushtia-7000, Bangladesh

Md. Nazrul Islam, Dept. of Computer Science & Engineering, Islamic University, Kushtia-7000, Bangladesh

III. M-COMMERCE SERVICES

Some common m-commerce services are [2]: Mobile Security Services, Mobile Shopping (m-reservation, m-auction, m-post card etc.), Multimedia Messaging Service (MMS), Mobile Financial Services (m-bank, m-stock exchange, m-money, m-invoice), Mobile Instant Messaging (MIM), Mobile Dynamic Information Management (m-subscriber, m-passport, m-games, m-music), Mobile Advertising [3].

IV. M-COMMERCE SYSTEM STRUTURE

A mobile commerce system is inherently interdisciplinary and could be implemented in various ways. Fig.-1 shows the structure of a mobile commerce system and a typical example of such a system [4]. The system structure includes six components: i) mobile commerce applications, ii) mobile handheld devices, iii) mobile middleware, iv) wireless networks, v) wired networks, and vi) host computers.

4.1 Mobile commerce applications

E-commerce applications are numerous, including auctions, banking, marketplaces and exchanges, news, recruiting, and retailing, to name but a few. Mobile commerce applications not only cover the electronic commerce applications, but also include new applications, which can be performed at any time and from anywhere by using mobile computing technology, for example, mobile inventory tracking.

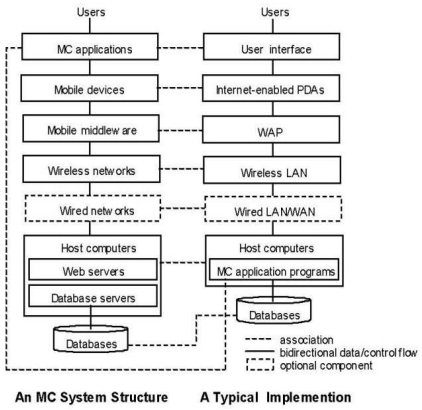

Fig-1: Mobile-commerce system

4.2 Mobile handheld devices:
An internet-enabled mobile handheld device is a small general-purpose, programmable, battery-powered computer that is capable of handling the front end of mobile commerce applications and can be operated comfortably while being held in one hand. It is the devices with which mobile users interact directly with mobile commerce applications. Examples are PDAs, Smart Phones, Pagers, Palmtops, and GPS devices.

4.3 Mobile middleware:
The term middleware refers to the software layer between the operating system and the distributed applications that interact via the networks. The primary mission of a middleware layer is to hide the underlying networked environment's complexity by insulating applications from explicit protocols that handle disjoint memories, data replication, network faults, and parallelism [5]. The major task of mobile middleware is to seamlessly and transparently map Internet contents to mobile stations that support a wide variety of operating systems, markup languages, micro-browsers and protocols. WAP and i-mode are the two major kinds of mobile middleware.

4.4 Wireless and wired networks:
Wireless communication capability supports mobility for end users in mobile commerce systems. Fast, secure and user-friendly mobile telecommunication technologies are a crucial factor for the commercial success of Mobile Commerce, since it is largely dependent on the acceptance of Mobile Commerce applications amongst targeted consumer groups and relevant business firms. Wireless and wired networks technologies which conduct m-commerce are described below:
2G: It is Second Generation mobile network based on CDMA and TDMA. It supports voice and SMS service. They make use of encryption techniques to enhance confidentiality of the transmitted data. Examples of 2G systems are GSM, PACS, and DECT. GSM is relatively advanced technology. However, for some limitations for video support, another enhancement of GSM called HSCSD is introduced. Its transmission rate is 28.8kbps that provides three times faster non-voice (data) service.
2.5 G: The transit between 2G and 3G is known as 2.5G. The General Packet Radio Service (GPRS) is the main standard of this phase. Another standard that arguably belongs to both 2.5G as well as to 3G and builds on GPRS is the Enhanced Data-rates for Global Evolution (EDGE). GPRS offers following advantages: speed, immediacy, and innovative service, cost advantage, low actual transmission rates, priority for voice transmission. EDGE allows subscribers to access the Internet and to send and receive data, e.g. digital images and videos, with a broadband like transmission speed of 384 kbps that is about three times faster than an ordinary GPRS network
3G: It is called UMTS and is based on WCDMA. It provides interactive multimedia services, video telephony and high speed internet access. UMTS splits into four hierarchical transmission cells [6]: **Pico** cells (2048kbps at low mobility within less than 50m), **Micro** cells (384kbps at limited mobility area ranging from 50m to 350m), **Macro** cells (144 kbps at full mobility area ranging from 350m to 20km) and **Satellite** cells (9.6 kbps with universal roaming and geographical coverage).

4.5. Host computers:
User requests, such as database access or updating are actually processed at a host computer, which contains three major kinds of software: i) Web servers, ii) database servers, and iii) application programs and support software.

4.6 Mobile handheld devices:
Mobile handheld devices have the following components: mobile operating systems, mobile central processing units, micro-browsers, input/output devices memory, and batteries.

V. SECURITY CHALLENGES

M-commerce is not possible without a secure environment, especially for those transactions involving monetary value. The screen size of mobile devices is very crucial when designing interfaces for users. Mobile devices offer limited display, which is difficult for users to display and browse online catalogues. It is highly personalized and contains confidential user information; therefore they need to be protected according to the highest security standard. Depending on the point of views of different participants in an m-commerce scenario, there are different security challenges [7]. The security challenges relate to the following: -

The Mobile Device: Confidential user data on the mobile device as well as the device itself should be protected from unauthorized use. The security mechanisms employed here include user authentication (e. g. PIN or password authentication), secure storage of confidential data (e.g. SIM card in mobile phones) and security of the operating system.
Malicious SMS Messages: Applications such as mobile advertising and mobile alerts typically send advertising and alerts to mobile users using short messaging service (SMS) messages or short paging messages. A malicious service provider or participant may send out malicious SMS messages that hide nefarious instructions [8].

The Radio Interface: Access to a telecommunication network requires the protection of transmitted data in terms of confidentiality, integrity and authenticity. In particular, the user's personal data should be protected from eavesdropping. Different security mechanisms need for different network technologies (i.e. in 2G, 3G and other systems) (Schwiderski-Grosche & Knospe, 2000).

The network operator infrastructure: Security mechanisms for the end user often terminate at the access network. This raises questions regarding the security of the user's data within and beyond the access network. Moreover, the user receives certain services for which he or she has to pay. This often involves the network operator and he or she will want to be assured about correct charging and billing.

The kind of m-commerce application: M-commerce application, especially those involving payment, need to be secured to assure customers, merchants and network operators. For example, in a payment scenario both sides want to authenticate each other before committing to a payment. Again, the customers want assurance about the delivery of

goods and services. In addition to the authenticity, confidentiality and integrity of sent payment information, non-reputation is important.

Virus Attack: Consider the mobile software-downloading scenario where a mobile user is asking for a resource from the network. An adversary can respond by a fake resource with the same name as the real resource the original user is looking for, but the actual file could be a virus. The first wireless virus has been discovered in PalmOS, which is called PalmOS/Phage1, and it infected all third-party applications on the PDA device. Other wireless virus examples include the PalmOS/LibertyCrack2 Trojan that arrives masquerading as a crack program for an application called Liberty, which allows PalmOS devices to run Nintendo GameBoy Games. During running, however, the Trojan attempts to delete all applications from the handheld and then reboot it [8].

DoS Attack: The first cell phone virus hacked users of GSM mobile phones and broadcasted a disparaging remark through SMS3. Although the virus caused no damage, it foreshadowed a potential DoS attack. If an adversary can disseminate a worm that send out millions of such messages, it could deluge cell phones with them, thereby overwhelming the short message system.

VI. SECURITY SOLUTIONS

In above, we show some security challenges involved in m-commerce. Solutions of these security problems are ensured in various levels. These levels are below:
Security of network technology
Transport layer security
Service security

6.1 Security of network technology

Network technologies involved in m-commerce are GSM, UMTS, WLAN, and Bluetooth. Security steps taken for them are given below:

6.1.1 GSM Security: GSM provides the following security features for the link between the mobile station and the network [9] [10],
IMSI confidentiality
IMSI authentication
User data confidentiality physical connections
Connectionless user data confidentiality
Signaling information element confidentiality
GSM provides the basic security mechanisms for m-commerce transactions. In particular, the *mobile customer authenticates* towards the network with a challenge/response protocol based on the secret key *K*. Furthermore, the *wireless link between the mobile station and the BTS is encrypted* with a symmetric key which is also derived from *K*. The secret key *K* is never sent over the network.

6.1.2 UMTS Security: UMTS (Universal Mobile Telecommunication System) is the next generation (3G) mobile telecommunication system and a further development of GSM. The major difference to GSM is the radio network (UTRAN) with its transition to the WCDMA (Wideband Code Division Multiple Access) radio technology. The security architecture of UMTS is carefully designed to fix the security weaknesses of GSM. The main problems of GSM originate from two facts: authentication is one way (the mobile station does not authenticate the network), and encryption is optional. In UMTS, authentication is mutual, and encryption is mandatory unless the mobile station and the network agree on an un-ciphered connection. In addition, integrity protection is always mandatory and protects against replay or modification of signaling messages. Sequence numbers in authentication vectors protect against reuse of authentication vectors by network impersonators. UMTS introduces new cipher algorithms and longer encryption keys. UMTS does not seem to have any obvious security holes.

6.1.3 WLAN Security: The IEEE standard 802.11 specifies families of WLAN which operate in the unlicensed 2.4 GHz and 5 GHz band. The standards specify the physical layer (PHY) and the medium access control layer (MAC). For the network layer and above, WLAN employs a classical IP stack. A number of commercial products (even for PDAs) are available, and IEEE 802.11b, offering 11 Mbit/s raw bandwidth, is currently very popular. When operated in the infrastructure mode, the mobile station attaches to an Access Point (AP) which provides connectivity to fixed net IP networks (e.g. the internet) or to other mobile stations. In the default mode, WLAN does not provide any security. In order to provide a certain level of security, the IEEE defined WEP (Wired Equivalent Privacy). WEP was designed to provide:
Authentication to protect the association to an AP
Integrity protection of MAC frames
Confidentiality of MAC frames
The protection is based on secret WEP keys of either 40 or 104 bits. Concatenated with a clear text initialization vector, the secret key serves as input for the RC4 stream cipher. But authentication and integrity protection is completely insecure and encryption at least partly insecure. It suffices for an attacker to intercept a single successful authentication exchange between a mobile station and the AP to be able to authenticate without knowing the secret keys. Furthermore, since a CRC checksum is used for integrity protection, an attacker can modify the data and adapt the checksum accordingly. For example, if the position of commercially sensitive information (e.g. an amount) within a datagram is known, the corresponding private networks and impossible for public WLAN hotspots. In recent work of the IEEE Task group on security (TgI), the new security standard IEEE 802.1X has been adopted. 802.1X is a framework for authentication and key management which employs the Extensible Authentication Protocol (EAP) for a variety of authentication mechanisms, e.g. certificate based TLS. But the weaknesses of WEP cannot be remedied by the new authentication and key management schemes in 802.1X. The IEEE is currently working towards a new standard (WEP2), and a number of proposals are in circulation.

6.2 Transport layer security

The above technologies provide security for the wireless link between mobile customer and access network or access device. If the access network is considered secure and the m-commerce transaction is completely handled within the access network, this may be sufficient. But often, an m-commerce transaction involves parties outside the access network (merchant, payment service provider etc.). It is two of types:

6.2.1 SSL/TLS: The SSL/TLS (Internet Secure Socket Layer) [11], protocol is by far the most widely used internet security protocol. Its main application is the HTTPS protocol (HTTP over SSL), but it may also be used as a standalone protocol. SSL requires a bidirectional byte stream service (i.e. TCP). SUN has implemented a client side version of SSL for limited devices, called KSSL (Kilobyte SSL). KSSL does not offer client side authentication and only implements certain commonly used cipher suites, but it has a very small footprint and runs on small devices using the J2ME platform.

6.2.2 WTLS: The WAP forum has standardized a transport layer security protocol (WTLS) as part of the WAP 1 stack [12].WTLS provides transport security between a WAP device (e.g. a mobile phone) and a WAP gateway which performs the protocol transformation to SSL/TLS. Hence, no real end-to-end security is provided and the WAP Gateway needs to be trusted. Note that the WAP Forum now proposes a WAP 2 stack which is a classical TCP/IP stack on a wireless bearer medium. This permits end-to-end SSL/TLS sessions.

6.3. Service Security:
The security of network services which can be used for m-commerce transactions. These are below:

6.3.1 Intelligent Network: The IN architecture for GSM (called CAMEL, Customized Application for Mobile Enhanced network Logic) [13] was adapted from the fixed network standard ETSI Core INAP, and was originally designed for circuit switched calls (CAMEL phase 1 and 2). Prominent examples of IN services are the transformation of dialed numbers (e.g. to realize Virtual Private Nets) and prepaid services. The IN platform provides some flexibility for the generation of m-commerce services. The security of an IN service depends on the underlying GSM or UMTS network security (see above) and on the specific characteristics of the service application.

6.3.2 SMS: SMS (short message service) is a very popular data service for GSM networks. Although SMS messages are limited to 160 characters, a considerable number of m-commerce scenarios are based on this service. The sender and receiver of an SMS is identified by its IMSI which an attacker cannot forge without breaking the GSM/UMTS security mechanisms (e.g. by cloning a SIM card). Hence SMS messages can be used for authentication (at least towards the network). Furthermore, SMS data is transmitted in the GSM (UMTS) signaling plane, which ensures the confidentiality of messages. However, the protection ends in the GSM or UMTS network, there is no end-to-end security, and the network operator and its infrastructure (e.g. SMSC, Short Message Service Centre) must be trusted (when no other security mechanisms are applied to the SMS message, confer section on SIM/USIM Applications).

6.3.3 USSD: The GSM Unstructured Supplementary Service Data (USSD) service allows data communication between a mobile station and either the HLR, VLR, MSC or SCP in a way transparent to other network entities. Unlike the asynchronous SMS service, an USSD request opens a session which may induce other network operations or an USSD response before releasing the connection. Mobile originated USSD may be thought as a trigger for a network operation. USSD works with any mobile phone since the coded commands are entered in the same way as a phone number (e.g. *123#235484968#). With USSD, roaming can be offered for prepaid GSM customers before IN services (CAMEL) are implemented in a network. Another USSD application (requiring CAMEL phase2) is replenishing a prepaid account by incorporating the voucher number in an USSD string. In principle, any transaction, e.g. a payment operation, could be triggered by USSD data. USSD possesses no separate security properties; instead it relies on the GSM/UMTS signaling plane security mechanism.

6.3.4 SIM/USIM Application Toolkit: The SIM and USIM Application Toolkits (SAT and USAT respectively) allow operators and other providers to create applications which reside in the SIM/USIM. These applications can e.g. send, receive and interpret SMS or USSD strings. The required security mechanisms are:
Authentication
Message Integrity
Replay detection and sequence integrity
Proof of receipt and proof of execution
Message Confidentiality
Indication of the security mechanisms used
However, it depends on the applications whether these security mechanisms are implemented and whether their cryptographic strength is sufficient.

CONCLUSION

M-commerce is an emerging way of business and services where transaction and/or service can be conducted very easily with mobile device from anywhere of the world where associated network is available. M-commerce provides a lot of facilities but it has some limitations too. Security challenges of m-commerce sometimes make it vulnerable to go forward for any operation. In spite of all limitation, it is hoped that m-commerce will be the only way of conducting all functions of business and it's covering arena. The purpose of this study is dedicated to develop the m-commerce and its service as well as spreading the knowledge about it worldwide.

REFERENCES

[1] http://www.cbs.nl
[2] M. Nusret SARISAKAL, M. Ali AYDIN, "Mobile Commerce", Journal of Electrical & Electronics Engineering, Istanbul University, vol. 52, 2005,
[3] "Mobile Commerce: opportunities and challenges", A GS1 Mobile Com White Paper, February 2008 Edition.
[4] Hu, W., Lee, C., Yeh, J., "Mobile commerce systems", in Shi, N. (Ed.), Wireless communications and mobile commerce, Idea Group, Inc, 2003.
[5] Geihs, K., "Middleware challenges ahead". IEEE Computer, 34(6), 24-31, 2001.
[6] Schell, A. J., "Preismechanismen fur Netzwerkressourcen im Electronic und Mobile Commerce", Hamburg, 2002.
[7] Schwiderski-Grosche, Scarlet; Knospe, Heiko, "Secure M-commerce", 2000.
[8] Xiong, Li & Liu, Ling, "Reputation and Trust", Idea Group Inc. pp. 19-35, 2005.
[9] GSM 02.09 version 7.0.1 Release 1998. Digital cellular telecommunication system (Phase2+); Security Aspects.

[10] M. Walker, T. Wright, Security Aspects. In: F. Hillebrand, "GSM and UMTS: The Creation of Global Mobile Communication", John Wiley and Sons Ltd.
[11] T. Dierks, C. Allen. The TLS protocol, Version 1.0. RFC 2246.
[12] WAP Forum, Wireless Transport Layer Security, Version 06-Apr2001, http://www1.wapforum.org/tech/documents/WAP-261-WTLS-20010406-a.pdf
[13] 3GPP TS 03.78 version 7.7.0 Release 1998. Digital cellular telecommunications system(Phase 2+); Customized Applications for Mobile Network Enhanced Logic (CAMEL) Phase 2; Stage 2