International Journal of Advanced Technology in Engineering and Science
Vol. No.5, Issue No. 06, June 2017
www.ijates.com
ijates
ISSN 2348 - 7550

DESIGN LIMITATIONS CHARACTERISTICSAND ANALYSIS OF SECURE MOBILE TRANSACTION AND PROTOCOLS

Narinder Bali[1], Raghav Mehra[2], Anita Gupta[3]

[1,2] Department of Computer Sciences, Bhagwant University. Ajmer, Rajasthan(India)

[3] Govt. College for Women, Parade Ground, Jammu, J&K (India)

Abstract

Today, new technologies that allow cellular (mobile) phones and other handheld devices to access the Internet have made wireless business transactions possible. This phenomenon is known as mobile commerce or M-Commerce. What must be done to secure financial transactions via mobile commerce? Due to the advent of the Internet, electronic business transactions have exploded around the globe. Generally speaking, M-Commerce creates more security concerns than traditional E-Commerce. Mobile payment is defined as any payment transaction involving the purchase of goods or services that is completed with a wireless device. In this paper let us have a brief survey on security issues when designing, implementing, and deploying secure m-payment systems with a focus on threats, vulnerabilities and risk. The first problems come from the limitation of wireless environments that are primarily from mobiles devises which have connection cost, low bandwidth, and low reliability. The second problem is the lack of sufficient security of existing mobile payment systems mainly due to improper protocol design and deployment of lightweight cryptographic operations. . .

Keywords- cryptographic operations, micropayment protocol, m-payment, , mobile devices.

I. INTRODUCTION

M-Commerce is a subset of electronic commerce where the Internet-enabled HWDs and wireless networking environment are necessary to provide ‘location independent connectivity’. It is predicted that M-Commerce services would be the next biggest growth area in the telecommunications market, represent-in the fusion of two of the current consumer technologies: wireless communications and E-Commerce .Generally speaking, The discipline of M-Commerce includes reference to the infrastructures and electronic technologies necessary for wireless data and information transfer in the form of text, graphics, voice, and video. Mobile payment system provides attractive opportunities to, merchants financial and users. These opportunities were simplicity and ease of a-payment transaction for the user and they also enable merchants to access customer information and target specific customer through various incentive programs such as discount coupons and reward programs.. According to orange Mobile Payment (Danish Company) the entire transaction should take not more than 10 seconds. In order to provide a secure and comprehensive m-payment, the payment scenario should be designed so that it performs fast and simple for the end-use, but secure and comprehensive for the provider. An efficient payment scenario takes efficient steps in performance.

1.1 Mobile Commerce

Two main areas in which e-commerce grew significantly in recent years are Internet banking and conducting business on the Internet. With Internet banking, the way customers make use of banking services has changed. They do not have to go to ATM (Automatic Teller Machine) terminals or stay in-line at a bank branch to withdraw or transfer money between accounts, but simply log on to a bank's website which provides. Internet technology offers extensive ranges of services such as electronic mails, file transfers, etc., and one of the most popular services offered on the Internet is “Electronic Commerce" (or e-commerce).

1.2Applications of M-Commerce

In France, some 35 million Smart cards are in circulation and every year they process over three billion transactions. Wireless banking refers to purchasing over Internet-enabled HWDs like wireless application protocol (WAP) phones or PDAs. Interactive TV is enhanced TV where additional content is added to an existing broadcast format that the viewer can query, request or even interact live with the program. Smart Cards with an embedded integrated microchip can be used as prepaid phone cards, ATM cards, or public transportation cards. They can be biometrically enhanced to include voice recognition, iris and face scans, and finger print authentication. It has reserved channels and bandwidth for data applications such as weather, news, games, or commerce. It also offers services like Video on Demand (VOD) or Personal Video Recording (PVR). Companies are providing facilities to track stocks on HWDs. Aspiro, a Swedish company, allow its customers to check stock prices or look at their portfolios and even trade using WAP phones or PDAs. Accessing information using WAP mobile phones and PDAs is significantly becoming popular for business-to-business (B2B) and business-to-consumer (B2C)

II. WIRELESS APPLICATION PROTOCOL (WAP)

WAP-enabled phones can access interactive services such as information, location-based services, corporate information and inter-active entertainment. WAP is targeted at various types of HWD and Bluetooth enabled mobile phones. WAP is “an open, global specification that empowers mobile users with wireless devices to easily access and interact with information and services instantly.” WAP is currently the only publicly available solution for wireless communication and enables M-Commerce where Internet data moves to and from wireless devices

2.1 WAP Security

WAP 1.x security uses 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 has three levels, all have privacy and integrity: (i) Class-1 has no authentication (anonymous), (ii) Class-II has server authentication only, and (iii) Class-III has both client and server authentication. WTLS supports some familiar algorithms .

Since Web- and WAP-based protocols are not directly interoperable, a component knows as the WAP gateway is needed in order to translate Web-based protocols to and from WAP-based protocols. The WAP gateway is 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 known as WAP gap.

Public key cryptography (PKC) is used to exchange a symmetric or private 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. Figure 1 shows WAP gap model.

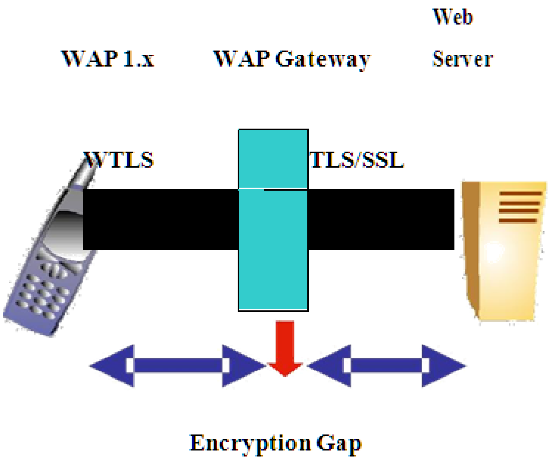

Figure 1 WAP Gap Model (not a full end-to-end security)

WAP 2.0 security uses TLS (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 (PKI) 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, RC4, 3DES, and SHA-1 algorithms for encryption. Wireless PKI (WPKI) is released for the first time. Figure 2 shows the WAP proxy model.

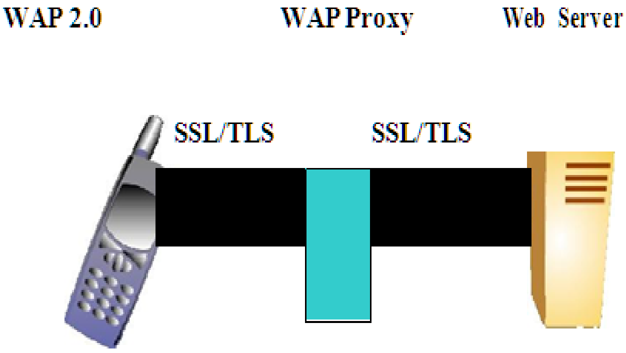

Figure 2 WAP Proxy Model (end-to-end security)

2.2 PKI/WPKI

PKI systems and WTLS are at the heart of today’s mobile security technology. In a WAP environment WTLS must be translated at the WAP gateway into SSL, the Internet standard. A PKI is a set of policies, processors, software, hardware, and technologies that use PKC and certificate management to secure communication. PKI’s trusted services enable the secure transfer of information and supports a wide variety of M-Commerce applications. PKI must ensure the following: (i) confidentiality, achieved by cryptography, (ii) authentication, achieved by digital certificates, (iii) integrity, achieved by digital signatures, and (iv) 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 soft-ware 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.

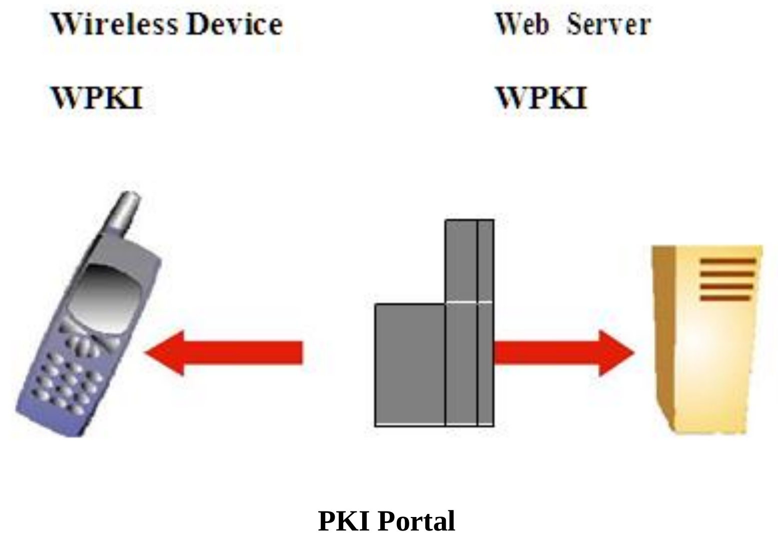

Figure 3 Wireless PKI

The private keys are stored in WIM or SWIM. Two main components of WPKI are the PKC and the key certification management. In order to perform globally, worldwide PKI legislation is required.

III. CRYPTOGRAPHY

The two types of cryptography currently available are (a) symmetric or secret-key and (b) asymmetric or public key cryptography (PKC). In secret-key cryptography, two devices must share their secret key in order to communicate securely. Thus two concerns arise: How to exchange the secret key securely; and if n HWDs must communicate with each other, a total number of $O(n^2)$ secret keys must be exchanged. The management of such a number of secret keys should consider the scalability issues.

4 Elliptic Curve Cryptography (ECC)

What is really needed is a public key algorithm that achieves a high level of security using short keys. Algorithms based on mathematical objects known as elliptic curves offer interesting possibilities. Elliptic curve discrete logarithm problems (ECDLP) is defined as “give a base point P and the kP lying on the curve, find the value of k”. For suitable curves and base points, this is a very hard problem. From cryptographic point of view, a new cryptographic system needs to be defined based on elliptic curves. Any standard system that relies on the discrete logarithm problem has a direct analogy based on the ECDLP. For example, Elliptic Curve DSA (ECDSA) has already been standardized. Diffie-Hellman key exchange can be easily implemented in an elliptic curve system.

Table 1 EEC Key Size compared to RSA

ECC Key Size (bits)	Traditional RSA Key Size (bits)	Key Size Ratio
109		1:5
131		1:6
163	1,	1:6
283	3,	1:11
409	7,	1:19
571	15,	1:27

Recently, ECC has been deployed on Smartcards without coprocessors . Weimerskirch et al implemented ECC on a Palm OS device. Their study showed that the normal transaction, such as a key exchange or signature verification, can be done in less than 2.4 seconds while signature generation can be done in less than 0.9 seconds.

Table 2 shows the three major industry-standard PKC systems that can be considered secure, efficient, and commercially available .

Table 2 Three Major Industry-Standard PKC

PKC	Mathematical Problem	Algorithm
Integer Factorization	Given a number n, find its prime factors	RSA, Rabin-Williams
Discrete Logarithm	Given a prime n, and numbers g and h, find x such that $h = g^x \bmod n$	ElGamal, Diffie-Hellman, DSA
EC discrete Logarithm	Given an elliptic curve E and points P and Q on E, find x such that $Q = xP$	EC-Diffie-Hellman, ECDSA

4.1 Problems with Elliptic Curve System

The true difficulty of the ECDLP is not yet fully under-stood . Recent research has shown that some elliptic curves that were believed suitable for ECC are, in fact, not appropriate. For example, if the order of the base point P is equal to the prime number p then it turns out that the ECDLP can be solved efficiently. Such curves are known as anomalous curves. For a given curve and base point, it is trivial to generate public and private keys (the private key is simply a random integer k and the public key is the point kP on the curve). However, it is an extremely difficult problem to generate a suitable curve and base point in the first place.

The main problem is how to count the number of points on the curve. Having done this, it is then necessary to select a suitable base point P, which must have a large order to ensure the difficulty of the ECDLP. But the order of P must divide the number of points on the curve. Having found the number of points on the curve, it is quite likely that a suitable base point cannot be found. Users may use random curves or special curve generating soft-ware, such as the "Elliptic Curve Generation Bureau" created by Zaxus.

4.2 Digital Certificates and Digital Signature

In a PKC, a message is encrypted using a public key and is decrypted using a secret key. However, there is no inherent way of knowing the person who has the corresponding secret key. This is where the idea of certificates arises. Certificates confirm that the public key given in the certificate belongs to a private key held by the legitimate person, not by an imposter. To trust a certificate means to trust the party who issued the certificate, not the person for whom the certificate is issued. To protect a certificate from being modified one uses digital signatures. The message can only be created from the ciphertext by the private key holder. This provides authorization and non-repudiation. That is the basis for digital signature.

How to protect private keys? The private key is stored in a Smart card, where all crypto operations with it are performed. The Smart card access gets restricted by the use of a PIN. The place where a user's private credentials are stored is called Personal Security Environment (PSE).

V. WIRELESS LAN (WLAN) SECURITY

5.1 IEEE 802.11b

The WLAN standard IEEE 802.11b provides a mechanism for authentication and encryption. It provides a maximum of 11 Mbps wireless Ethernet connections using the band at 2.4 GHz. 802.11b security features consists of security framework called Wired Equivalent Privacy (WEP) . WEP is based on RC4, a symmetric stream cipher. It has a pseudo-random number generator, whose output is XORed to the data. WEP can use 40 or 128 bits key size. However, using a 128 bits key size, 802.11b throughput drops much due to heavy calculations. In August 2001, RC4 was announced to be broken and can be cracked in less than half an hour. Consequently, WEP can be broken. WEP with 40 bits key size can be broken in real time.

5.2 Bluetooth

Bluetooth technology, developed by Ericsson in 1998, is used to connect different HWDs and provides a method for authenticating devices. Device authentication is provided using a shared secret between the two devices. The common shared secret is called a link key, generated from PIN. This link key is established in a special communication session called pairing. All paired devices share a common link key. There are two types of link keys: (i) unit keys and (ii) combination keys . The link key is a 128-bit random number.

VI.CHARACTERISTICS OF WIRELESS NETWORKS

Wireless networks have the following characteristics:

Wireless networks have lower bandwidth than fixed networks.

Connections over wireless networks are less reliable since packet losses occur more frequently than that of fixed networks. Packets need to be retransmitted which may result in high latency.

Connection cost of wireless networks is higher compared to that of fixed networks.Data transmitted over wireless networks is easily eavesdropped.

From the above limitations, mainly due to poor performance, performing payment transactions over wireless networks is time-consuming. Moreover, performing payment transactions on low computational capability mobile devices will spend longer time to complete each transaction.

VII. BACKGROUND AND RELATED WORK

This section provides the background and related works of the mobile payment.

- ### 7.1 Primitive Payment Transaction

The primitive mobile payment is composed of three basic steps Payment—Client makes a payment to the merchant, Value Subtraction—Client requests to the payment gateway for his debit, and Value Claim—Merchant requests to the payment gateway to credit transaction amount into his account.

7.2 Mobile Payment Components

Mobile payments the components from the existing researches related to mobile payment protocols.. Fun, Beng, Roslan and Habeeb stated that mobile payment protocols are composed of five principals which include client, merchant, issuer (client's financial institution), acquirer (merchant's financial institution) and payment gateway (PG. Kungpisdan, Srinivasan and Le also defined that five parties on mobile payment protocols are client, merchant, payment gateway, issuer and acquirer Fun, Beng and Razali stated that the com-ponents of mobile payment scheme consist of seven main actors: Financial Service Providers (FSPs), Payment Service providers (PSPs), Payee, Payer, Mobile Network Operator (MNOs), Device Manufacturers, and Regulators. Singh and Shahazad stated that the components of mobile payment protocol consist of three participants: payee, payer and financial institution

7.3 Review and Comparison of Mobile Payment Protocol

Dowling stated that the components of mobile payment protocols are composed of four parts: customer, merchant, payment service provider and trust third party (TTP)

The number of components mentioned above by researchers is different due to the design of payment protocols. However, we conclude that the components of mobile payment protocols, in general, consist of only three main parts: buyer, payment channel and seller.

VIII. TECHNOLOGY OF MOBILE PAYMENT

We studied and assessed technologies in mobile payment systems from the existing researches as described below P. Pukkasenung and R. Chokngamwong

- SMS—Short Messaging Service is a text messaging service used to send and receive short text messages. The maximum length of messages is less than 160 alphanumeric characters, to and from mobile phones.
- WAP—Wireless Application Protocol is a technology which provides a mech-anism for displaying internet information on a mobile phone.

- NFC—Near Field Communication is the communication between contactless smart cards and mobile phones.
- RFID—Radio Frequency Identification is a method of identifying an item wirelessly using radio waves
- Smart Card—Smart cards and plastic cards normally appear in the same shape as credit cards are embedded with a chip or microprocessor that can handle and store 10–100 times more information than traditional magnetic-stripe cards.
- Internet—the internet is a publicly accessible, globally interconnected network. It uses the internet protocol to enable the exchanging and sharing of data among computers in the network
- USSD—Unstructured Supplementary Services Data is a mechanism of trans-mitting information via a GSM network. Unlike SMS, it offers a real-time connection during a session
- IVR—Interactive Voice Response is a telephony technology where the users can interact with the database of a system without any human interaction
- Magnetic—Data is stored in a magnetic stripe on a plastic card. It is read by swiping the card in a magnetic card reader.

IX. SECURITY PROPERTIES

A secure mobile payment system must have the following properties

- Confidentiality—The system must ensure that private or confidential informa-tion will not be made available or disclosed to unauthorized individuals.
- Integrity—The system must ensure that only authorized parties are able to modify computer system assets and transmitted information.
- Authentication—The system must ensure that the origin of a message is correctly identified, with an assurance that the identity is not false.
- Non-repudiation—The system must ensure that the user cannot deny that he/she has performed a transaction and he/she must provide proof if such a situation occurs.
- Availability—The system must be accessible for authorized users at any time.
- Authorization—The system must verify if the user is allowed to make the requested transaction.

X. PERFORMANCE ASPECT

Protocol's performance is analyzed by counting the number of operations needed for encoding and decoding. This includes operations related to data transmission between three parts. which consist of public encryption–decryption, signature verifications, symmetric key encryption-decryption, a hash function, keyed-hash function and key generations. The researchers presented secure mobile payment protocols providing a high level of security and low computation, cost and power.

XI. CONCLUSION

M-Commerce security is a very crucial issue that needs further research to introduce efficient and effective solutions. In this article, various security concerns were expounded. ECC certainly appears to provide a viable alternative to RSA. There are potential advantages, especially when used in devices with limited processing capability and memory**.** Typical applications include M-Commerce using handheld wireless devices. There are, however, some problems and issues that are inhibiting the widespread adoption of EEC. These include (i) the real security of such systems is still not well understood**,** (ii) difficulty of generating suitable curves**,** and (iii) relatively slow signature verification. Time will tell its future.. All protocols provided four main security properties: con-fidentiality, integrity, authentication, and non-repudiation. As a conclusion, to discover the best secure mobile payment protocol, the protocol standard must be the same all over the world and the communities and industries must be adopting the standard. In this paper we proposed a secure payment protocol, considering the restrictions of mobile networks in developing countries. The proposed protocol not only satisfies the convenience and ease of use that is generally required for mobile users in small payments, it also provides the transaction security level and non repudiation property that is necessary for macro payments. Although the proposed technique has been optimized for the current GSM network, but its modular design enables it to accept future improvements of the mobile network technology and infrastructure, such as EMS and MMS, with minimum change in the protocol structure

REFERENCES

1. Fun TS, Beng LY, Razali MN (2013) Review of mobile macro-payments schemes. J Adv Comput Netw 1(4).
2. Singh A, Shahazad KS (2012) A review: secure payment system for electronic transaction. Int J Adv Res Comput Sci Softw Eng 2(3)
3. Ahamad SS, Udgata SK, Nair M (2014) A secure lightweight and scalable mobile payment framework. In: FICTA 2013. Advances in intelligent system and computing, vol 247. Springer International Publishing, Switzerland
4. Mathew M, Balakrishnan N, Pratheeba S (2010) A study on the success potential of multiple mobile payment technologies. In: Technology management for global economic growth (PICMET), Proceedings of PICMET '10
5. Smart Card Alliance (2008) Proximity mobile payments business scenario: research report on stakeholder perspectives
6. www.deloitte.com/assets/DcomChina/Local%20Assets/Documents/Industries/Financial%20services/cn_gfsi_TrendsProspectsChinaMobilePaymentIndustry_041212.pdf., Retrived on 27th January, 2016.
7. Li Y, Wang Y Secure electronic transaction. http://people.dsv.su.se/*matei/courses/ IK2001SJE/li-wang_SET.pdf
8. Kungpisdan S, Srinivasan B, Le PD (2003) Lightweight mobile credit-card payment protocol. Lect Notes Comput Sci 2904:295–308
9. Fun TS, Beng LY, Likoh J, Roslan R (2008) A lightweight and private mobile payment protocol by using mobile network operator. In: Proceedings of the international conference on computer and communication engineering 2008 May 13–15, Kuala Lumpur, Malaysia, 2008
10. Alizadeh Dizaj MV, Moghaddam RA, Momenebellah S (2011) New mobile payment protocol: Mobile Pay Center Protocol 2 (MPCP2) by using new key agreement protocol: VAM. In: 3rd international conference on electronics computer technology (ICECT)
11. Isaac JT, Zeadally S (2012) An anonymous secure payment protocol in a payment gateway centric model. In: The 9th international conference on mobile web information system (MobiWIS). Elsevier

12. Sekhar VC, Sarvabhatla M (2012) Secure lightweight mobile payment protocol using symmetric key techniques. In: International conference on computer communication and informatics (ICCCI), pp 1–6, 10–12 Jan 2012

13. Tripathi DM, Ojha A (2012) LPMP: an efficient lightweight protocol for mobile payment. In: 3rd national conference on emerging trends and applications in computer science (NCETACS)

13"certicom," [Online]. Available: http://www.certicom.com/index.php/an-introduction-to-the-uses-of-eccbased-certificates. [Accessed 01 01 2013].

14."RSA Laboratories," RSA, [Online]. Available: http://www.rsa.com/rsalabs/node.asp?id=2129. [Accessed 10 12 2012].

15.Sekhar VC, Sarvabhatla M (2012) Secure lightweight mobile payment protocol using symmetric key techniques. In: International conference on computer communication and informatics (ICCCI), pp 1–6, 10–12 Jan 2012

16. Christopher Hall and Tiffany Smith, "Mobile Payments Security 101", . Robin Arnfield, Tom Harper, Kathy Doyle, Will Hernandez, Published by Networld Media Group @ 2015, Networld Media Group, 2015.

17.Green, Mr Jeremy Swinfen. Cyber Security: An Introduction for NonTechnical Managers. Ashgate Publishing, Ltd., 2015.