Proceedings of the 7th WSEAS International Conference on Mathematics & Computers in Business & Economics, Cavtat, Croatia, June 13-15, 2006 (pp24-28)

A Comparison of Secure Mechanisms for Mobile Commerce

Hann-Jang Ho [1] and RongJou Yang [2]
1 Department of Computer Science and Information Engineering
2 Department of Information Management
WuFeng Institute of Technology
117, Chian-Kuo Rd., Sec. 2, Ming-Hsiung , Chia-yi 621
Taiwan, R.O.C.

Abstract: - Mobile commerce has emerged as an innovative technology due to the prevailing of pervasive computing. However, on-line secure transaction mechanisms can not 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 mandatory 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. However, the secure connection mechanisms can be modified to apply to the mobile devices. This paper focuses on the comparison and analysis of the secure connection mechanisms in the mobile commerce.

Key-Words: - Mobile Commerce, Secure Transaction Mechanism, WTLS, KSSL, WAP, WML

1 Introduction

Since the invention of World Wide Web (WWW) by Tim Berners-Lee in 1990, Internet has gradually been employed to conduct the marketing activities and change the buying behavior of consumers following the development of EC-related technology. E-Commerce has numerously been employed as another virtual channel which is different from traditional brick-and-mortar channel in order to create business opportunity. Internet population increases rapidly following the rising and flourishing development of Internet. According to the investigation by ACI-FIND, Institute of Information Industry, Taiwan, the Internet population arrives 8 million and 920 thousands (39%) by June, 2004, which is 80 thousands more than in 2003 and has a 1% growth rate. Commercial Internet accounts arrived 1 million including most of the mobile accounts [1] which means much more enterprise have entered the EC market.

Security is still a big issue concerning Internet shopping. According to eBrain Market Research, Consumer Electronics Association (CEA) conducted an investigation on the consumers' intension of Internet shopping so as to understand the favorites of consumers and found that the lower price of the product is still one of the key factors and the convenience, privacy, and security are the next. Also, according to the investigation on the mandatory factors of Internet shopping from Princeton Survey Research Associates for Consumer Web Watch, the convenience, security, and trust are three most mandatory factors for consumers [1]. Therefore, the security of Internet shopping is a matter of importance.

The development of EC is getting matured. Nowadays, mobile EC is topical subject in the area of mobile Internet. According to the investigation of ECRC-FIND, III, Taiwan, the mobile phone subscribers have arrived 23 million which is 102%, in the second quarter, 2004, meaning the era of mobile EC has emerged in order to get rid of the restriction of time and space [1]. However, there exists universal security concern in mobile EC in the environment of wireless network which has higher security risk than in wired network due to the data transmission in the air.

A digital certificate, issued by a certification authority (CA), is an electronic "credit card" that establishes your credentials when doing business or other transactions on the Web. It contains applicant's name, a serial number, expiration dates, a copy of the certificate holder's public key which is used for encrypting messages and digital signatures, and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. The digital certificates usually conform to X.509 standard and can be kept in registries so that authenticating users can look up other users' public keys.

A PKI (public key infrastructure) enables users of a basically insecure public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The public key infrastructure provides for a digital certificate that

can identify an individual or an organization and directory services that can store and revoke the certificates which can be checked by Web Sentry from Xcert based on the Online Certificate Status Protocol (OCSP).

A PKI, known as asymmetric cryptography, uses the public key cryptography, which is the most common method on Internet for authenticating a message sender or encrypting a message consists of a digital certificate, issued by CA which is verified by registration authority (RA), which includes the public key or information about the public key, one or more directories where the certificates (with their public keys) are held, and a certificate management system. In public key cryptography, a public and private key are created simultaneously using the same algorithm (a popular one is known as RSA, an Internet encryption and authentication system that uses an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman) by CA. Then, we can send an encrypted message using the receiver's public key and decrypt an encrypted message using the receiver's private key, or send an encrypted signature using the sender's private key and decrypt an encrypted signature to authenticate the sender using the sender's public key.

A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message (encrypted or not) or the signer of a document in order to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. The ability to ensure that the original signed message arrived also means that the sender cannot easily repudiate it later. In digital signature, a message hash (mathematical summary) of the document, sent by the sender, is obtained by using special software and encrypted as the signature by using a private key that has been previously obtained from a public-private key authority. The receiver makes a hash of the received message (signed document), decrypt the message hash or summary, and compares if the hashes match.

In [7], the security of WAP WTLS was analyzed, the most important parts of the specification of WTLS and the reason of defects was presented, the existing security threat of WTLS was discussed, and an acceptable level of security was proposed. In [8], the authors proposed a building block for M-Commerce security platform constructed by WTLS security mechanism and based on J2ME MIDP and integrated with J2ME and WTLS security technology to provide more secure mobile business. In [9], a WTLS Crypto Module Security Policy encapsulated (embedded) in AirBEAM Safe software components using the WTLS layer to establish a secure tunnel between the client and the server, which is performed using the WTLS handshake protocol, was presented. WAP WTLS protocol was designed to provide privacy, data integrity, and authentication for wireless terminals. In [10], a number of security flaws, such as a chosen plaintext data recovery attack, a datagram truncation attack, a message forgery attack, and a key-search shortcut for some exportable keys were identified and discussed.

2 Secure Transaction Mechanisms in Mobile Commerce

The secure encryption technology of WTLS in WAP, SSL, and SET are employed to integrate with WAP Gateway so as to provide a platform for the payment fulfillment for the card holders. A WAP gateway, for instance, decrypts encrypted data sent by a WAP phone using WTLS and re-encrypts it using SSL before forwarding it to the eventual destination server. The reverse process is used for traffic flowing in the opposite direction. Such a proxy-based architecture has some serious drawbacks. The proxy is not only a potential performance bottleneck, but also represents a “man-in-the-middle” which is privy to all “secure” communications. This lack of end-to-end security is a serious deterrent for any organization thinking of extending a security-sensitive Internet-based service to wireless users.

In [3], a solution using standard security mechanisms and protocols on small wireless devices was implemented based on the Java 2 Micro-Edition (J2ME) platform that offers fundamental cryptographic operations such as message digests and ciphers as well as higher level security protocols like SSL and their results show that SSL is a practical solution for ensuring end-to-end security of wireless Internet transactions even within today’s technological constraints.

Following the vigorous development of mobile EC, the emerging WAP moves EC forward to mobile EC. As Internet is mentioned, computer virus, hackers, public key, encryption, etc. come to one’s mind. What about the security concern in mobile devices? Some security mechanisms in mobile devices are discussed in section 3 and 4.

3 Wireless Transport Layer Security

WTLS is the security level for Wireless Application Protocol (WAP) applications. Based on Transport Layer Security (TLS) v1.0 (a security layer used in the Internet, equivalent to Secure Socket Layer 3.1), WTLS was developed to address the problematic issues surrounding mobile network devices - such as limited processing power and memory capacity, and low bandwidth - and to provide adequate authentication, data integrity, and privacy protection mechanisms. Wireless transactions, such as those between a user and their bank, require stringent authentication and encryption to ensure security to protect the communication from attack during data transmission. Because mobile networks do not provide end-to-end security, TLS had to be modified to address the special needs of wireless users. Designed to support datagram in a high latency, low bandwidth environment, WTLS provides an optimized handshake through dynamic key refreshing, which allows encryption keys to be regularly updated during a secure session.

WTLS is the security layer of the WAP, providing privacy, data integrity and authentication for WAP services. WTLS, designed specifically for the wireless environment, is needed because the client and the server must be authenticated in order for wireless transactions to remain secure and because the connection needs to be encrypted. For example, a user making a transaction with a bank over a wireless device needs to know that the connection is secure and private and not subject to a security breach during transfer (referred to as a man-in-the-middle attack). WTLS is needed because mobile networks do not provide complete end-to-end security.

WTLS is based on the widely used TLS v1.0 security layer used in Internet. Because of the nature of wireless transmissions, modifications were made to the TLS v1.0 in order to accommodate for wireless' low bandwidth, datagram connection, limited processing power and memory capacity, and cryptography exporting restrictions. The Wireless Transport Layer Security (WTLS) protocol provides the mechanism for obtaining secure sessions using public key cryptography. WTLS supports two public key cryptosystems: RSA and Elliptic Curve Cryptography (ECC).

In [4], an analytical performance model of the WTLS handshake protocol was derived by using two public key cryptosystems supported by WTLS: RSA and Elliptic Curve Cryptography (ECC). ECC provides much more security than RSA at a lower computational cost and their experimental evidence shows that ECC indeed outperforms RSA in realistic wireless secure scenarios. National Institute of Standards and Technology (NIST) [5] announced a Draft Federal Information Processing Standard (FIPS), proposing Rijndael as AES expected to replace Data Encryption Standard (DES). WTLS provides related services concerning authentication, encryption, and integrity and supports RC5, SHA-1, IDEA, and AES algorithms. WTLS internal architecture [6] is indicated in Table 1.

Tab. 1 WTLS Internal Architecture

Full Handshake Protocol	Alert Protocol	Application Protocol	Change Cipher Specification Protocol
Record Protocol			

The Record Protocol takes care of the data integrity and authentication and supports four protocol clients: the full handshake protocol, the alert protocol, the application protocol, and the changer cipher spec protocol. External applications have direct access to the WTLS layer using the Wireless Markup Language (WML) Script. All the security related parameters are agreed on during the handshake. These parameters include attributes such as protocol versions, cryptographic algorithms, and information on the use of authentication and public key techniques to generate a shared secret. There are three descriptions of alert messages: fatal, critical, and warning. Alert messages are sent using the current secure state, i.e. compressed and encrypted, or under null cipher spec, i.e. without compression or encryption. The Change Cipher Spec is sent either by the client or the server. By means of this message, both parties decide that they start using the negotiated session parameters. When the Change Cipher Spec message arrives, the sender of the message sets the current write state to the pending state and the receiver also sets the current read state to the pending state. The Change Cipher Spec message is sent during the handshake phase after the security parameters have been agreed on.

WAP stack protocol is indicated in Figure 1. WAE and the application for wireless phones (Wireless Telephony Application WTA) are the main interface to the client device, which gives and controls the description language, the script language of any application and the specifics of the telephony. WSP delivers all functions that are needed for wireless connections. A session mainly consists of 3 phases: start of the session, transferring information back and forth and the end of the session. Additionally, a session can be interrupted and started again (from the point where it was interrupted).

Like the User Datagram Protocol (UDP), the WTP runs at the head of the datagram service and supports chaining together protocol data and the delayed response to reduce the number of transmissions. The protocol tries to optimize user interaction in order that information can be received when needed. WTLS is an optional layer or stack which consists of description devices and contains a check for data integrity, user authentication and gateway security. A secure transmission is crucial for certain applications such as e-commerce or WAP-banking and is a standard in these days. WDP represents the transfer or transmission layer and is also the interface of the network layer to all the above stacks/layers. With the help of WDP the transmission layer can be assimilated to the specifications of a network operator. This means that WAP is completely independent from any network operator. The transmission of SMS, USSD, CSD, CDPD, IS-136 packet data and GPRS is supported. The Wireless Control Message Protocol (WCMP) is an optional addition to WAP, which will inform users about occurred errors.

<table>
<tr><td colspan="3">WAE (Wireless Application Environment) – Application layer</td><td colspan="4">Other Services and Applications</td></tr>
<tr><td colspan="3">WSP (Wireless Session Protocol) – Session layer</td><td colspan="4">Other Services and Applications</td></tr>
<tr><td colspan="4">WTP (Wireless Transaction Protocol) – Transaction layer</td><td colspan="3">Other Services and Applications</td></tr>
<tr><td colspan="5">WTLS (Wireless Transport Layer Security) – Security Layer</td><td colspan="2">Other Services and Applications</td></tr>
<tr><td colspan="7">WDP (Wireless Datagram Protocol) – Transport Layer</td></tr>
<tr><td colspan="7">Bearers:</td></tr>
<tr><td>GSM</td><td>IS-136</td><td>CDMA</td><td>PHS</td><td>CDPD</td><td>iDEN</td><td>Etc</td></tr>
</table>

Fig. 1 WAP Protocol Stack [7]

For instance, in the transaction processing of mobile banking, the connection is established between mobile device and WAP gateway after WTLS security verification and then between WAP gateway and Web server of the bank after SSL encryption transformation. Afterwards, Web server issues a “navigation document” which is responded to in reverse direction and used by mobile device so as to commit the transaction in a private and secure area.

4 Wireless Transport Layer Security

Nowadays, SSL is in widespread use in secure on-line transaction but unsuitable for mobile device due to the inadequacy of computing capability and memory. Therefore, WAP Forum proposed WTLS for secure wireless transmission in which a proxy server is mandatory for decoding and encoding between SSL encryption and WTLS encryption. However, there exists security vulnerabilities exposure to intrusion in the small period of time between decoding and encoding. J2ME MIDP supports KSSL and provides API for secure wireless network transaction in mobile devices. KSSL (Kerberized or KiloByte SSL), based on SSL 3.0, is for wireless or small devices. J2ME MIDP for developers supports a development platform for the information interchange between SSL and network by providing API for secure wireless network.

An SSL client, called KSSL, was implemented on a Palm PDA and its performance was also evaluated in [11]. In MIDP 1.0 specification, the software vendors are mandatory to provide HTTP support. In MIDP 1.0.3 and above, in addition to http://urls we can use https://urls to connect to Web server. Sun J2ME Wireless Tool Kit 1.0.4 supports KSSL. In WTK1.0.4, the way using HTTPS is simple and described as follows:

String url = https://host.com/files;

HttpConnection hc = HttpConnection Connector.open (url);

After the connection is established, HTTPS server can verify, deny, or install the certificate.

The comparison of WTLS and KSSL security mechanism based on privacy, integration, identification is indicated in Table 2. In WAP, unencrypted transmission data are inclined to attacks. J2ME provides end-to-end security through KSSL instead of the gateway between mobile device and server and allows local processing of the data instead of remote processing in WAP, thus reduces enormously the possibility of attacks.

Tab. 2 Comparison of WTLS and KSSL [12] [13] [14]

Functionality	WTLS	KSSL
Privacy	RSA, Diffie-Hellman, and Elliptic Curve Diffie-Hellman encryption algorithm supported	RSA (key exchange) and RC4 (encryption) supported

Integrity	SHA-1 and MD5 MAC algorithms; Message protected with SHA-1	Message protected with MD5 and SHA
Authentication	RSA, Elliptic Curve Diffie-Hellman, and Diffie-Hellman based key exchange suites; Verified for upper layers of WAP	X.509 certificate

5 Conclusion

Secure payment mechanisms can set consumers' mind at ease to conduct the on-line transactions. It also provides the convenience for consumers by applying it to mobile device. This paper investigates the on-line security mechanisms and its application in mobile EC. The on-line security mechanisms can not completely be applied to mobile EC due to the lack of computing capability of the mobile device. A secure payment mechanism is an efficient instrument to promote EC.

This paper investigates the mainstream of secure transaction mechanism in mobile commerce: Wireless Transport Layer Security (WTLS) and KSSL (Kerberized or KiloByte SSL).

Under the investigation, we find that the security level of WTLS employed in mobile device is still inadequate at present. In recent years, WAP users have substantially decreased. Therefore, KSSL being employed in WAP to redeem the drawback of WTLS and how to ensure the security in mobile EC are future directions.

Acknowledgement

This work was supported by Taiwan NSC under grant no. NSC-94-2622-E-274-002-CC3.

References:

[1]http://www.find.org.tw/ , "FIND Internet Information Center", *Institute of Information Industry*, Taiwan

[2]http://www.itri.org.tw/, I*ndustrial Technology Research Institute*, Taiwan

[3]V. Gupta and S. Gupta, "KSSL: Experiments in Wireless Internet Security", *Sun Microsystems Laboratories*, http://research.sun.com/techrep/2001/smli_tr-2001-103.pdf, 2001

[4]F. R. Henriqueq, C. E. LbpeEPeza, and M. A. Leon-Chivez, "Comparative Performance Analysis of Public -Key Cryptographic Operations in the WTLS Handshake Protocol", *1st International Conference on Electrical and Electronics Engineering*, pp. 124-129, 2004

[5]http://csrc.nist.gov/encryption/aes/index.html - comments, *National Institute of Standards and Technology*

[6]Thanh V. Do and Kris Gaj, "WAP Security: WTLS", INFT 931, *Secure Telecommunication Systems*, 2001

[7]G. Radhamani and K.Ramasamy, "Security issues in WAP WTLS protocol", *IEEE International Conference on Communications, Circuits and Systems and West Sino Expositions*, vol.1, pp. 483 – 487, 2002.

[8]N. J. Park and Y. J. Song, "M-Commerce Security Platform based on WTLS and J2ME", *ISIE*, 2001.

[9]Columbitech, "WTLS Cryptographic Module Version 1.2, 1.3.1, 1.3.3", Level 1 Validation, *Symbol Technologies*, http://csrc.nist.gov/cryptval/140-1/140sp/140sp307.pdf, 2005.

[10] M. J. Saarinen, "Attacks against the WAP WTLS Protocol", http://www.freeprotocols.org/harmOfWap/wtls.pdf

[11] V. Gupta and S. Gupta, "KSSL: Experiments in Wireless Internet Security", *Sun Microsystems Laboratories*, http://research.sun.com/techrep/2001/smli_tr-2001-103.pdf, 2001

[12]WAP Forum. Wireless Transport Layer Security Specification Version 1.1, November 2, 1999, http://www.wapforum.org/

[13]F. R. Henriqueq, C. E. LbpeEPeza, and M. A. Leon-Chivez, "Comparative Performance Analysis of Public -Key Cryptographic Operations in the WTLS Handshake Protocol", *1st International Conference on Electrical and Electronics Engineering*, pp. 124-129, 2004

[14]A. Macphee, "Understanding Digital Certificates and Wireless Transport Layer Security (WTLS) Version 1.1", http://www.entrust.com/resources/pdf/understanding_wtls.pdf, *Entrust*, 2001.