Proceedings of International Conference on Wireless Networks (ICWN), Las Vegas, Nevada, 2003.

Secure Wireless Payment Protocol

Hong Wang
School of Computer Science
Carleton University
1125 Colonel By Drive, Ottawa, Canada

Evangelos Kranakis
School of Computer Science
Carleton University
1125 Colonel By Drive, Ottawa, Canada

Abstract

With the convergence of wireless data communication and the Internet, more and more Internet services are now being used in the wireless area. Mobile payment protocols are necessary for online transactions. A good payment protocol should balance the requirements of security and convenience.

WAP (Wireless Application Protocol) is one of the prevalent wireless technologies being embraced by the banking sector. Compared with WLAN (Wireless Local Area Network), WAP can satisfy the strong security requirement of banking services.

WPP (Wireless Payment Protocol) is a convenient lightweight protocol that supports both credit card and debit card transactions in wireless environment. The shortcoming of WPP is that it does not actually address security. In this paper, we propose a new wireless payment protocol, SWPP (Secure Wireless Payment Protocol), to address security and convenience based on WAP for WTLS (Wireless Transport Layer Security), WIM (Wireless Identity Module) and WMLScrypt, WPKI technology.

Keywords: SWPP, WAP, WTLS, WIM, WMLScrpt, WPKI.

1. Introduction

Mobile Payments are becoming more and more important with the increase of wireless services. Improved data transfer and the easier use of such services will also increase demand among end users. Using a mobile handset for on-line transactions is relatively more complex than using a fixed-location terminal, such as a desktop PC, for the same purpose because of the shortage of power and memory.

Convenience and security are two important factors in a payment service. From the consumer's point of view, "convenience" means to pay quickly and without an additional cost or too much effort. From the bank's point of view, "convenience" means low deployment and operational cost. Convenience is sometimes more important than security in the end user's eyes.

Security is the utmost concern for customers. Customers would have little or no confidence in a payment method that cannot provide ways to ensure authenticity, confidentiality, integrity and non-repudiation. A good payment protocol should be both "convenient" and "secure".

Till now, there is no well-accepted standard for wireless payment protocol. The one proposed by MeT [2], which is based on SET, can address the security issue well but it falls short on convenience. Compared with MeT, WPP [1] addresses convenience by changing message flow. Higher performance is achieved in WPP by reducing the number of messages, thereby lowering bandwidth and computation requirements. The shortcoming of WPP is that security is not designed and implemented.

In this paper, we propose SWPP, which tries to address the security problem of WPP based on WAP technology. Having taken the limitations of the wireless environment into account, WAP [4] is widely accepted as a de-facto standard. With many network operators upgrading their network to GPRS, the latency problem resulting from the circuit-switched network can be solved. WAP has provided different security level solutions according to the business requirements. One

important reason for WAP to be chosen here is political: WAP is embraced by the banking sector. According to Roy Smith, managing director at Brokat: "Banks are buying WAP servers despite not knowing what WAP is or how it will help their organization." [8]

1.1 Motivation

Although security of an e-payment method is very important for all parties involved in a transaction, security alone does not guarantee success in the marketplace. An e-payment system must also be convenient. A good payment system should be both "secure" and "convenient". SSL and SET [3] are considered as two standards for Internet payment protocols. The difference between them for online payment is that, SSL based protocols are convenient but have some authentication and non-repudiation problems while SET based protocols, which require intermediary agents are secure but not so convenient.

Although SSL and SET are standards for Internet payment protocols, they cannot be directly adopted in wireless area as they do not address the limited resources of the wireless environment such as high communication cost, weak reliability, limited computation capability, lower transmission rate, lower power and less memory. A new payment protocol suitable for the wireless environment is required to make online banking services accessible to portable devices. MeT and WPP protocols are two wireless payment protocols based on SET and SSL separately.

The MeT account-based system can be considered as a standard for credit card based systems. MeT is quite similar to SET, except that it is based on the WAP architecture. The data flow in MeT is the same as that in SET, using the merchant to make contact with the acquirer. The same as SET, security in MeT is well addressed by sacrificing "convenience".

WPP tries to find a middle ground in the security versus convenience tradeoff suitable for wireless environment. WPP uses different data flow from MeT in order to make the protocol convenient. In WPP, Customer Agent interacts directly with the Customer's bank to make sure data does not pass through any intermediary. Simple protocol such as WTLS [5], SSL can be used to satisfy the requirement of "security". Convenience is well addressed at the same time. However, security is not designed and implemented in WPP, and this gives the motivation for the development of the SWPP.

1.2 Contribution of the Paper

The main contribution of this paper is the design and implementation of SWPP. SWPP is based on WAP infrastructure that provides a fast, secure, on-line and interactive connection method. Security and convenience are well addressed in this protocol, making the protocol practical to be used. In SWPP, data flow is quite similar to that in WPP. Convenience is well addressed as SWPP starts when the merchant sends an invoice to a customer and ends when the merchant receives a confirmation of payment from his or her bank.

SWPP relies upon a secure environment provided by the WAP specification to address security requirements. Confidentiality and integrity can be addressed through the use of Wireless Transport Layer Security (WTLS), while customer and server authentication are achieved by combining WTLS with the Wireless Identity Module (WIM). The WIM will also facilitate the use of digital signatures, which will help ensure non-repudiation. End-to-end security is achieved by combining TLS/SSL and WTLS. SWPP also supports established techniques for data integrity and encryption, including WPKI. WPKI consists of protocol extensions, together with software and hardware additions to terminals and networks that extend traditional PKI to wireless networks. SWPP uses proxy technology, in conjunction with firewall technology, to define the boundary for the service domain. By owning the gateway in its private service network, the security gap introduced by WAP is addressed.

2. Basic characteristics of WPP model

The main difference between MeT and WPP is the transaction flow. Compared with MeT, WPP is more convenient by providing the same level of security as that proposed by MeT. By changing the transaction flow, WPP can address the same security level by embracing SSL technology instead of SET. The main

characteristics of WPP are summarized as follows:

Eliminating fraud source for online transaction:

Credit card fraud is a serious problem on the Internet. WPP eliminates the source of fraud by altering the direction of the transaction flow. The credit card information can only be given to the customer's bank. WPP is convenient, with the addition of a strong security element.

Dual signature is not required:

Compared with MeT, a dual signature is not required in WPP since customer's payment instructions are sent directly to the Customer's Bank. The merchant's banking information (previously encrypted by the bank) is sent to the customer and then forwarded to the customer's bank.

Using Smart Cards:

In WPP, smart card is used to store encrypted banking information. It can also store Personal Identification Numbers (PINs) so that credit card payments can incorporate other types of payments, such as debit card payments.

End to end security:

End to end security is guaranteed through a Gateway, which acts as a bridge between the SSL and WTLS protocols.

In WPP, security is addressed with the assumption that the WTLS protocol will provide the confidentiality and integrity of all messages exchanged between all participants of the protocol. To put WPP in practical use, WPP must be redesigned to fulfill its security requirements.

3. Wireless Application Protocol

WAP is considered as the de-facto world standard developed by the WAP Forum with the aim of establishing a common format for Internet transfers to mobile telephones. The WAP stack is basically divided into five layers including WAE, WSP, WTP, WTLS and WDP. We can take any subset of WAP layers and use them in an already existing framework. WAP encompasses WIM (WAP Identity Module), WMLScrypt, WTLS (Wireless Transport Layer Security) and WPKI (Wireless Public Key Infrastructure), which all apply security at the application, transport and management levels in the wireless environment.

WIM: The WIM is used to store and process information needed for user identification and authentication such as certificates and keys. It is also used in performing WTLS and application level security functions. WIMs are most commonly implemented using smart card chips that optionally reside in the WAP device.

WMLSCrypt: The WMLScript Crypto Library Specification provides cryptographic functionality for message signing. The WAP WMLScript signText function provides digital signatures in WAP-compliant customer devices.

WTLS: WTLS is a security protocol originated from TLS/SSL, and takes into account the specific features of the wireless environment. In order to be used in wireless applications, WTLS has a number of additional characteristics which SSL lacks, such as compact coding, datagram support, optimized handshake, fast encryption and decryption algorithm, etc. There are three levels of security provision at various stages of adoption. WTLS Class 1 provides confidentiality and data integrity between the wireless device and the WAP gateway. Class 2 adds the authentication of the WAP gateway to the security services provided by Class 1. Finally, Class 3 is built on Class 2 by adding support for the authentication of the wireless customer.

The WTLS Handshake is very similar to the SSL handshake. The handshaking protocol is to establish a secure session between a WAP Customer and a WAP gateway. To accommodate the unreliability and unpredictability of connectionless datagram communication, messages are always packed as one Record Protocol packet when sent in one direction, to ensure that they are either received or lost on the other side.

A Digital Certificate is very important for customer authentication and non-repudiation. The X.509 Certificate is the most widely accepted Internet standard. However, X.509 is not supported by the current generation of WAP Customer devices, as they are marked by limited capacity. The WTLS certificate is similar to the X.509 certificate but is coded more compactly, and satisfies the high latencies and low bandwidth of wireless networks, as well as the limited processing resources of WAP Customer devices.

WPKI: Similar to the IETF PKI standards that are most commonly used in wired networks, WPKI standards are the most commonly used in

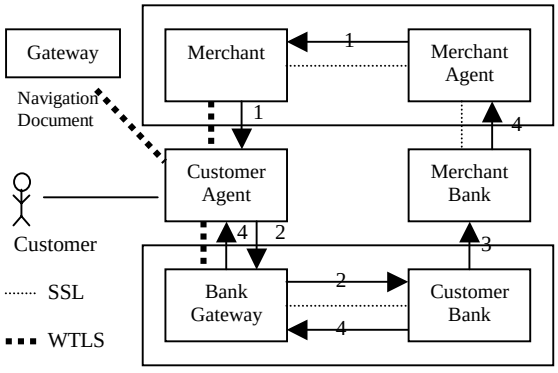
wireless networks. WPKI, an extension of traditional PKI, is used to leverage security features including WIM, WMLSCrypt and WTLS. Like all security and application services within the WAP environment, WPKI must be optimized, using more efficient cryptography and data transport techniques, in order to work with personal wireless devices and the narrow-band wireless networks. WPKI has optimized PKI protocols, certificate format, cryptographic algorithms and keys.

4. Secure Wireless Payment Protocol

SWPP is proposed to make up for WPP's security deficiencies. SWPP draws upon WAP, which is designed to make full use of Internet services, for WTLS, WIM, WMLScrypt and WPKI to guarantee the security requirement presented in WPP. SWPP uses proxy technology in conjunction with firewalls to define the boundary for the service domain.

4.1 Architecture of SWPP

A generic infrastructure of SWPP and its transaction flow is presented in Fig 4-1.



(1 – acknowledging order 2 – request for payment
3 – Notification of payment 4 – Confirmation of payment)

Fig 4-1 SWPP architecture

SWPP process commences when the merchant sends an invoice to the customer and terminates when the merchant receives confirmation from its Bank. The gateway in Fig 4-1 is used to locate the bank gateway or merchant gateway as requested by the customer. A security channel between the Merchant Agent and the customer is assumed here, as it is quite similar to that between the customer and the customer's bank. In this way, we do not have to take into account a Merchant Gateway between the customer and the Merchant Agent. On the customer side, they can use SWIM to store personalized data such as certificates, keys, PINs and encrypted information. Fig 4-2 presents the payment flow.

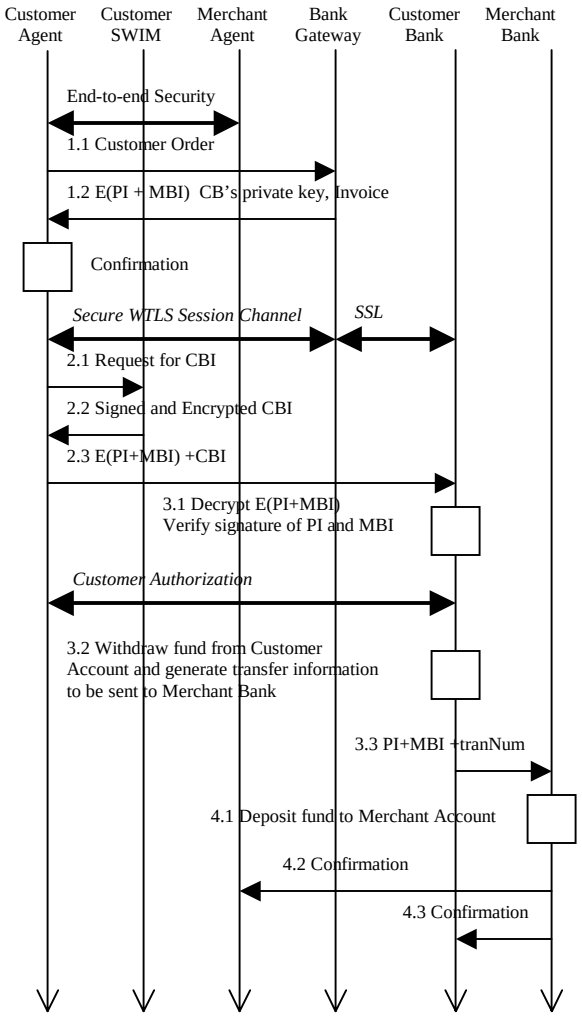


Fig4-2 Secure Payment Transaction Flow

4.2 Secure WTLS session channel

In SWPP, secure WTLS Session Channel is built between the customer and the bank gateway before the message is sent from Customer to Customer Bank. Using the storage and functionality of the WIM, the Customer Agent can now build a secure session with the bank gateway. The full process for building a secure session is presented in Fig 4-3.

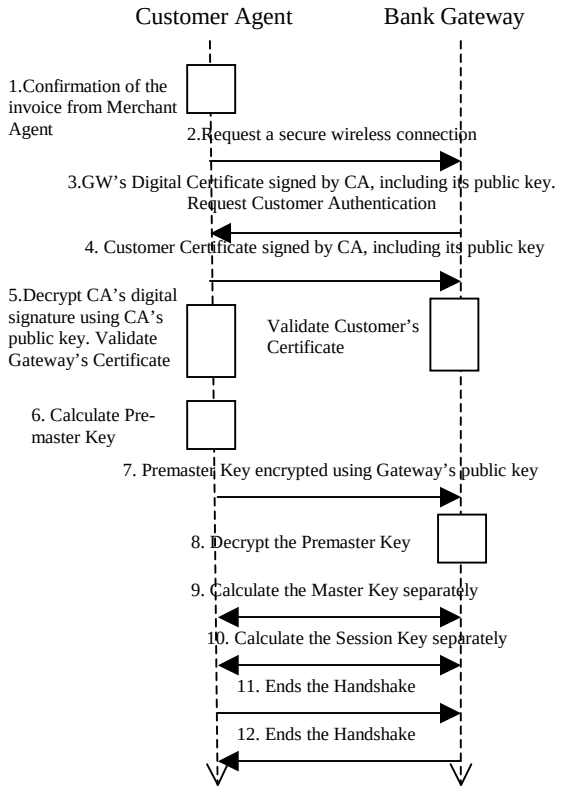


Fig 4-3 Secure Transport Session between Customer Agent and Bank Gateway

4.3 End to End Security

End-to-end security between the customer and the customer's Bank cannot be built only based on WTLS. A WAP gateway must be used as a bridge between the different protocols. Not WTLS but SSL is supported when the WAP gateway makes the request to the origin server. As the data is decrypted and again encrypted at the WAP gateway, the gateway introduces a security hole which renders WAP unsuitable for any security-sensitive services.

In SWPP, with the strong security required by the banking sector, the gateway is hosted by the content provider and placed behind the content provider's firewall. In Fig 4-1, the merchant's and the customer's bank have their own gateways in their own network. By placing a WAP gateway in their own network, the connection between the customer and different services (including the merchant service and the bank service) is to be trusted, as the decryption will not take place until the transmission has reached the service provider's own network, and not in the mobile operator's network. To provide the highest security solution, the functionality of the WAP gateway to the origin server can be included. This is the way that is used in our implementation. This set-up obviates both the WAP Gap and the need for SSL between the gateway and the HTTP server.

Since both the merchant's and the customer's bank provide WAP services to the customer, they have their own gateway in their own network. With these two gateways in SWPP, the customer agent needs a mechanism to navigate between them. The gateway in Fig 4-2 acts as a master WAP gateway, which supplies a navigation document to the customer. The other two gateways are subordinate WAP gateways supplying WAP services.

In Fig 4-4, there are three key components that provide total navigation for the Customer Agent, including: Navigation Document, Master WAP gateway and Subordinate WAP gateway. In SWPP, we focus mainly on the gateway between the customer and the customer's bank. The bank gateway acts as both master gateway and subordinate gateway. A navigation document is unnecessary.

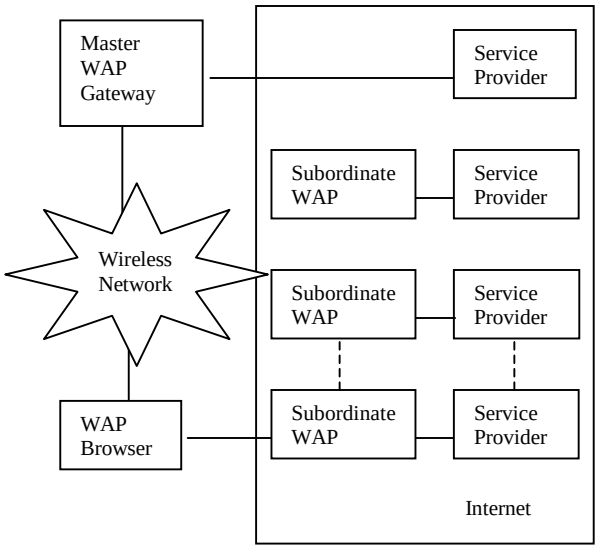


Fig 4-4 Transport Layer in an end-to-end Security Architecture

4.4 Customer Authorization

Once the secure transport session is established, payment information and other

relevant information are sent to the customer's bank via a secure channel that is built. After the customer's Bank decrypts the information from the Merchant and verifies its signature, certain information is generated and sent back to the user as a string to sign for signature. Customer Authorization is necessary for security on the application layer.

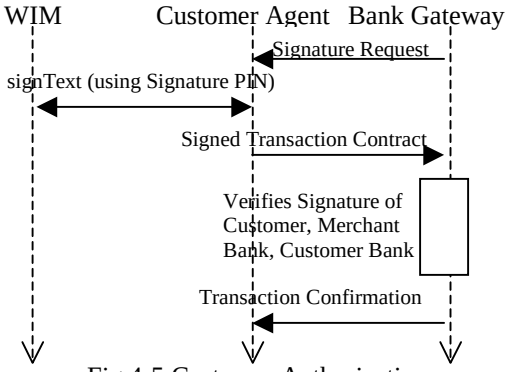


Fig 4-5 Customer Authorization

Customer Authorization in SWPP is implemented using the WMLScript signText function. The following transpires in the signText function:

- The customer's bank provides a text to be signed and an indication of the required user certificate (as a list of accepted certificate issuers) or key (as a key identifier)
- The customer confirms the text and certificate being used
- The customer is prompted to input a signature PIN
- WIM executes a sign function on the hashed text using a signature key

5 **Simulation**

Emulators are used to simulate the mobile device during development. In this paper, the Nokia Activ Server is used as the WAP gateway. An added-on product, Nokia Activ Security, a product that ensures secure communication and supports WTLS all the way from the WAP terminal to the origin server, is used to supply security. It encrypts the traffic between the WAP terminal and the Nokia Activ Server, and provides methods for certificate-based server authentication. A Key Exchange algorithm, Ciphersuites (which includes a bulk algorithm and an MAC algorithm) and server certificates can be deployed on the gateway. The certificate used in SWPP is self-signed for test purposes.

Nokia Activ Server acts as both a bank content provider and a WAP gateway to guarantee end-to-end security for customers. Although only WTLS Class 2 is supported on the gateway, customer authentication is implemented through the use of external authentication, in addition to the existing security infrastructure. To authorize a customer, a message from the customer's bank is signed by calling the function: Crypto.signText(), using a non-repudiation key stored in Nokia SoftID.

Fig 5-1 WTLS Connection Parameters

Connection Parameters: After the handshake between the customer and the bank gateway has been completed successfully, a WTLS Class 2 is built. The parameters are shown in Fig 5-1.
Process Time: Process time in SWPP is different when different algorithm is adopted. When using 1024-bit for asymmetric and 128-bit for symmetric algorithms, the total process time is around 8 seconds, which is about twice longer than that by using 768-bit for asymmetric and 56-bit for symmetric algorithms. Since the message exchanged between the customer and bank is not much, process time delayed by strong security can be accepted. Considering the strong security requirement of banking service, 1024-bit for asymmetric and 128-bit for symmetric algorithms are suggested in SWPP.

Key Exchange	RSA - 1024		RSA - 768	
Cipher Suites:	RC5+ SHA	RC5_56+ SHA_80	RC5+ SHA	RC5_56+ SHA_80
Process Time:	8450 ms	5900ms	6374 ms	4376ms

Fig 5-2 Processing Time

6. WPP and SWPP

A comparison between WPP and SWPP protocols based on selected criteria is given below.

	WPP	SWPP
Transaction Flow	Customer-Bank-Merchant	
Security Mechanisms	Not actually implemented	Implemented at both the application layer and WTLS class 2/3
Number of certificates used	None	One
Server Authenticati on	None	Provided by WTLS class 2
Customer Authenticati on	None	Using Plug-in Authentication Module
Data Integrity	Implemented	Message from the merchant is signed using its private key. Message from the customer to the bank gateway is signed based on the definition of WTLS Class 2.
Customer Authorizatio n	None	Uses Access Control provided by Nokia Activ Server and signText function defined in WMLScrypt.
Number of certificates used	None	Two. One for signature, one for encryption.
User of Gateway	Nokia Server is used to simulate merchant site	Nokia Activ Server is used as a gateway between customer and merchant. It also acts as a gateway and bank server to the customer.
End to end Security	None	By putting gateway function and bank server together on Nokia Activ Server
User of WIM Cards	None	Yes
Use of Smart Cards	Yes	

Fig 6 –1 Comparison between WPP and SWPP

7. Conclusion

SWPP is a well-designed protocol with many advantages over the SSL and SET protocols. SWPP inherits the basic idea of WPP, which is to use the customer's bank, instead of the merchant, to verify the customer's signature over the payment request. It aims to prevent personal information being presented to the merchant site. SWPP satisfies the security requirement assumed in WPP based on WIM, WMLScript, WTLS and WPKI. WAP Gateway is introduced as a bridge between different protocols. To solve the problem caused by Gateway when the message is decrypted and encrypted, we host the gateway's function on Customer Bank behind firewall. This brings the highest security for SWPP. The performance of SWPP satisfies the requirement for online payment very well.

Acknowledgements

The research presented in this paper has been supported in part by NSERC (Natural Sciences and Engineering Research Council of Canada) and MITACS (Mathematics of Information Technology and Complex Systems) grants.

References

[1] J. Hall, S. Killbank, M. Barbeau, E. Kranakis, WPP: A Secure Payment Protocol for Supporting Credit- and Debit-Card Transactions over Wireless Networks. In proceedings of ICT 2001 (International Conference on Telecommunications), Romania, Bucharest, June 4-7, 2001

[2] Mobile electronic Transactions. (2001). "MeT Account-Based Payment," http://www.mobiletransaction.org/pdf/MeT-Account-Based-Payment-20010221.pdf

[3] A. Levi and Ç. K. Koç, "CONSEPP: CONvenient and Secure Electronic Payment Protocol Based on X9.59, " presented at The 17th Annual Computer Security Applications Conference, New Orleans, Louisiana, pp. 286-295, Dec. 10-14, 2001.

[4] WAP Forum, "WAP Architecture: Wireless Application Protocol Architecture Specification," 2001, http://www.wapforum.org

[5] WAP Forum, "WAP WTLS: Wireless Application Protocol Wireless Transport Layer Security Specification," 2000, http://www.wapforum.org

[6] Y. C. Cheong and C. L. Tan, "Payments In Mobile Commerce," http://www.cgey.com/tmn/nmi/3g/downloads/3gpayments.pdf

[7] X. Song, "Mobile Payment and Security," 2001, http://www.tml.hut.fi/Studies/T-110.501/2001/papers/xing.song.pdf

[8] K. Young, "WAP fever – have you got it?" *The banke*r, vol.150, pp.20-26, April 1, 2000.

[9] H. Wang, MCS Thesis, Carleton University, School of Computer Science, Aug. 2002.