IEEE International Conference on Telecommunications (ICT), Bucharest, June 2001

WPP: A Secure Payment Protocol For Supporting Credit- And Debit-Card Transactions Over Wireless Networks

Jeyanthi Hall, Susan Kilbank, Michel Barbeau and Evangelos Kranakis

Carleton University, School of Computer Science
1125 Colonel By Drive
Ottawa, ON K1S 5B6 Canada

Email: jeyanthihall@home.com, kilbanks@magma.ca, {barbeau,kranakis}@scs.carleton.ca

ABSTRACT

The proliferation of wireless devices, offering connectivity and convenience, continues to exert tremendous pressure on merchants to deploy secure wireless applications including electronic commerce. One key element, which would assist them in fulfilling this requirement, is a standard protocol for supporting both electronic credit card and debit card transactions over wireless networks. Although the Secure Electronic Transaction (SET) protocol offers end-to-end security for credit card transactions over a wired infrastructure, there are several factors including bandwidth requirements which make it unsuitable for wireless applications. This paper presents the Wireless Payment Protocol (WPP) that supports both credit-card and debit-card transactions using the Wireless Application Protocol's (WAP) Wireless Transport Layer Security (WTLS) and Smart Card technology. In addition, a brief comparison to SET is made in order to illustrate the key attributes of the WPP.

INTRODUCTION

If the explosive growth in the use of mobile devices (428 million mobile users in 1999 [1]) is indicative of the next computational platform, then consumers will soon have the option of accessing web-based applications using personal computers or mobile devices. This tremendous growth fueled by consumers' need for mobile access to information and other services, is serving as a catalyst for the development and deployment of secure wireless applications including electronic commerce.

Currently, there are different payment protocols being used to support electronic payments over the Internet : E-cash for electronic cash [2], eCheck for electronic cheque [3], Secure Electronic Transaction (SET) for credit card payments [4] and micropayments .

While these methods of payment do fulfill the customer's needs, the underlying protocols have been developed in an uncoordinated manner . Whereas an attempt to standardize credit card payments through SET has proved beneficial, standards do not necessarily exist for the remaining types of payments.

Subsequently, any attempt to migrate these payment protocols from the wired to the wireless environment will more than likely result in a similar plethora of protocols. For example, an optimized and wireless-version of SET using mobile software agents has been proposed by [5] to permit credit card transactions over the Internet. Although this represents a step in the right direction, this version of SET only focuses on the front-end (client to merchant) of the transaction.

Another issue, which has attracted a lot of media attention, is credit card fraud perpetrated over the Internet. In 1998, Visa USA reported a loss of approximately $9.75 million due to on-line fraud [6]. These reports as well as consumers' skepticism of merchants' ability to store credit card numbers in a secure manner, outline the need for enhanced security. Unlike the SET protocol which offers end-to-end security, all others based on peer to peer security e.g. Secure Socket Layer (SSL) will more than likely be exposed to security violations if an intermediary is involved. In fact, it is the lack of sufficient security associated with peer to peer protocols that has prevented the use of debit cards and associated Personal Identification Numbers as a means of electronic payments on the Internet.

What will prove beneficial is a standard payment protocol that supports both credit and debit card payments over wireless networks in a secure and efficient manner. This paper presents our lightweight protocol, the Wireless Payment Protocol (WPP), for making payments over wireless networks. It supports credit and debit card payments, offers enhanced security by altering the traditional flow of payment transactions and reduces the processing time of payment transactions.

The remaining sections of the paper will introduce the WPP and how it differs from SET. Section 1 will present a brief overview of the SET, On-line Payments [7] and WAP protocols which contributed towards the development of WPP. Section 2 will describe the WPP

and compare it to SET in order to illustrate the key characteristics. The implementation of the protocol will be briefly discussed in section 3. Finally, the conclusions and future direction will be presented in section 4.

I. EXISTING STANDARD PROTOCOLS

As our objective was to develop a wireless payment protocol which supports credit card payments as well as debit card payments in a secure manner, three existing protocols were taken into consideration; the SET protocol, On-line payments and the Wireless Application Protocol (WAP). This section provides a brief overview of the protocols.

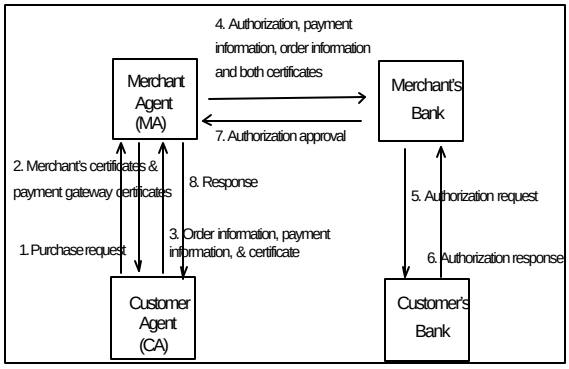

Figure 1 SET Protocol

A. Secure Electronic Transaction (SET)

The emerging standard for credit-card payments resulted from a call for security standards by MasterCard and Visa in Feb. 1996. The Secure Electronic Transaction is an open encryption and security specification designed to protect credit card transactions on the Internet. Companies which collaborated in the development of the specification included IBM, Microsoft, Netscape, RSA, Terisa and Verisign. Although SET had been designed to operate in a wired infrastructure, it is the transaction flow as well as the implementation of security which were of particular interest to us.

A high-level overview of the SET protocol is illustrated in Fig. 1. Please note that a detailed description of the mechanisms used for enforcing security requirements of the protocol will not be presented in this paper. For additional information, please refer to [4]. In addition, the ordering phase (selecting items to be purchased) as well as the settlement phase (request for payment and the transfer of funds between merchant and customer at the bank) are considered to be out of scope.

In a typical scenario, the merchant's site will be accessed via the Internet by customers using their personal computers. The payment transaction flow commences once the customer has completed the selection and ordering phase.

1) Customer Agent (CA) sends purchase request to Merchant Agent (MA).
2) MA sends certificates of merchant and payment gateway (bank) and other information to CA.
3) CA creates order information (OI) and payment instructions (PI), encrypts them using the multiple certificates received from the MA, and returns the encrypted PI/OI to the MA.
4) MA requests payment authorization from Customer's Bank via Merchant's Bank.
5) Merchant's Bank contacts Customer's Bank for authorization.
6) Customer's Bank responds with status of authorization.
7) Merchant's Bank forwards status of authorization to MA.
8) MA prepares a purchase response and sends it to the CA.

If this payment transaction flow looks very similar to that of a Point of Sale (POS) transaction, it is not coincidental. One of the key objectives in designing SET was to minimize the impact to existing merchant and banking applications and leverage on existing payment infrastructure.

The security and performance aspects of SET will be discussed in the following section when we make a comparison between SET and the Wireless Payment Protocol.

B. On-line Payments

While the SET protocol permits customers to make credit-card payments to any of the merchants offering a web-based service, customers also have the option of paying for other types of services using the on-line banking facilities (Internet).

On-line Payments, a web-based service provided by most banks, permit customers to make payments on-line to utilities, universities and other institutions that have previously registered themselves with the banks. Customers, using the web-based application, specify the institution, account (i.e. savings, chequeing) and the amount to be paid. The bank, in turn, confirms the successful completion of the transaction by sending them a reference/transaction number for audit purposes. At the end of the day, it also sends each merchant a database of the transactions which had transpired during the day.

One key element is the transaction flow. Unlike the customer-merchant-bank flow associated with the SET protocol, customers interact directly with their banks in a secure manner using such protocol as the SSL. The use of SSL in this case can be considered as sufficient since the confidential data of the customer does not pass through an intermediary (i.e. institution being paid).

C. Wireless Application Protocol (WAP)

Minimizing the need for application-level security by exploiting the security services offered at the Transport level of the TCP/IP protocol stack was one of our objectives in developing the WPP. To this end, the Wireless Transport Layer Security (WTLS), of the WAP stack was used to address the security requirements of the WPP. However, we could have used any other protocol stack which provided similar security services as the WTLS layer.

The WAP represents the de-facto world standard for the presentation and delivery of wireless information and telephone services on mobile phones and wireless terminals. Currently over 90% of the companies providing wireless devices have accepted the WAP protocol [7]. The development of this protocol was intended to make the services of the Internet available to mobile users. Formally released in November 1999 (v 1.2 issued in June 2000), the key elements of the WAP specification which were of particular interest to us is the WAP Programming Model based on the existing WWW Programming Model and the lightweight version of the TCP/IP protocol stack streamlined to minimize bandwidth requirements.

The selection of the Wireless Application Protocol as a framework provides considerable benefits. First, as the protocol is gaining both recognition and widespread acceptance, it will continue to be supported for some time to come[8]. Second, the Wireless Transport Layer Security (WTLS) fulfills most of the key security requirements (data integrity, authentication, encryption and denial of service) of WPP. Third, a number of enhancements to the session , transaction, security and transport layers of the protocol stack have been implemented to optimize the protocol and take into consideration the constraints of wireless networks, namely, low bandwidth and high latency conditions. Finally, the micro browser, proxy technology and compression in the network interface works in concert to reduce the processing load, to reduce power consumption and to extend battery life of mobile devices.

II. WIRELESS PAYMENT PROTOCOL

After having analyzed SET, On-line Payments and WAP and having taken into consideration the constraints of the wireless infrastructure, we developed the secure Wireless Payment Protocol (WPP) for supporting credit and debit card transactions over wireless networks.

The key elements of the underlying architecture is depicted in Fig. 2. As with the SET protocol, the Merchant Agent (MA) represents a web-based application which executes on the merchant's server. The application would be made available to the customers through a WAP Gateway (converts HTML to WML and uses the WAP protocol stack to communicate with the wireless/mobile devices of the customer).

The Customer Agent (CA) is an application running on the wireless device. It is used as an interface between the WAP Scripts and the Smart Card (SC). The SC provides a static storage mechanism for personalized data such as encrypted banking information of the customer.

As far as the banking institutions are concerned, both the Customer's Bank and that of the merchant are responsible for issuing digitally signed and encrypted banking profiles (banking information). As with SET, security of the banking infrastructure is assumed to be sufficient and outside the scope of WPP.

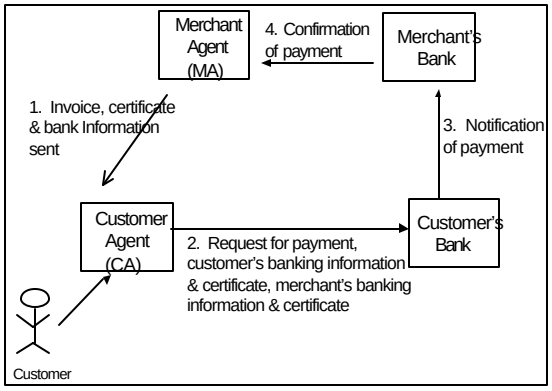

Figure 2 Wireless Payment Protocol

The protocol commences when the MA sends to the CA an invoice and terminates when the MA receives a confirmation of payment from the Merchant's Bank. Please refer to Fig. 2. As with SET, the ordering and payment/settlement phases as well as recourse mechanisms are outside the scope of this protocol. Although, only a brief description and subset of data elements are provided in this paper, details of the protocol is available [9].

The payment transaction flow is as follows.

1) MA prepares invoice and sends the merchant's certificate, encrypted banking information and the invoice to CA (see Table 1).

2) Customer confirms accuracy of the invoice. Once satisfied with the invoice, the customer is prompted to enter the Personal Identification Number (PIN) to authorize access to the SC. Once the PIN has been validated by SC, the CA presents the customer with payment options (i.e. credit-card, debit-card). After a method of payment has been selected by the customer, the CA prepares a payment request. It is digitally signed by SC and is forwarded to the Customer's Bank along with certificates and encrypted banking information of the customer and merchant (see Table 2).

Data Element	Description
Merchant ID	Uniquely identifies merchant
Transaction ID	Uniquely identifies invoice
Invoice: Date Items - Quantity - Description - CostperItem Taxes ShippingCost PaymentAmt	Details of invoice
Banking info: BankID BankLocation (e.g. URL) Profile number (merchant)	Unique number identifying the bank and its location

Table 1 Invoice and banking data sent by MA to CA

Data Element	Description
Client ID	Uniquely identifies the bank's client.
Payment Request Number	Uniquely identifies the request.
Banking Info Bank ID BankLocation BankingProfile AccountType	This provides the customer's bank address and the information about where the payment is to come from.
Invoice Info: Merchant ID TransactionId Date Amount	The Merchant ID should be the same ID that is recorded in the certificate. This is used to validate that the client is paying whom he thinks he is paying.
Merchant Identification Info: Certificate (Merchant) Profile number (Merchant)	The merchant digitally signs its profile number and encrypts it with the banking association (e.g. Interact, Plus) public key prior to sending it to the customer. The CA then transfers this information to Customer's Bank.

Table 2 Payment request sent by CA to Customer's Bank

3) Customer's Bank fulfills payment request and forwards response (approved or denied) to both the CA and Merchant's Bank (see Tables 3,4).

4) Merchant's Bank forwards payment confirmation to MA (see Table 5).

Data Element	Description
ReferenceNumber	Uniquely identifies the response Used for audit purposes
PaymentRequest Number	To match with the payment request Used for audit purposes
ResponseMessage	If authorization was unsuccessful, message indicating reason

Table 3 Payment response sent from Customer's Bank to CA

Data Element	Description
TransactionId	Uniquely identifying the notification
Payment Request Number	To match with the payment request
Merchant Identification Info: Profile number (Merchant)	In order to credit the account of the proper merchant
Client Identification	Information forwarded to the MA
Invoice Info: TransactionId Date Amount	Information forwarded to the MA

Table 4 Payment notification forwarded by Customer's Bank to Merchant's Bank

Data Element	Description
TransactionId	Uniquely identifying the notification
PaymentNumber	To match with the payment
Invoice Info: TransactionId Date Amount	To match the payment with the invoice

Table 5 Payment notification forwarded by Merchant's Bank to MA

One thing to note is the transfer of certificates from both the merchant and customer to the Customer's Bank. Although the certificates are used by the bank to validate the digital signature of the merchant and customer, it is possible that the bank could make use of a distribution service to obtain these certificates. This will, of course, further reduce the size of data being transmitted and improve the overall performance of the protocol.

A. Comparison to SET

The following section provides a comparison of the SET and WPP protocols based on selected criteria. On-line payment protocol was not included in the comparison since it is not an open specification. For the purpose of the comparison, it is assumed that SET can be migrated to a wireless infrastructure.

Transaction Flow

In terms of the payment transaction flow, there are two key differences. First, a reduction in the number of messages exchanged between the participating agents of the WPP is expected to reduce the overall processing time of wireless payment transactions and subsequently reduce communication costs for mobile users. In addition, the data being transmitted will become less vulnerable to various attacks. The second element is the direction of the transaction flow. With WPP, transactions are carried out between the CA and the Customer's Bank (without an intermediary – MA). By altering the traditional flow of transactions, we have addressed consumers' concern of transmitting private information via the merchant.

Security

As the SET protocol was designed to preserve the traditional flow of payment data (CA – MA – Merchant's Bank), an end-to-end security mechanism was required. As a consequence, the provision of security (encryption, data integrity, authentication and non-repudiation) was fulfilled at the application layer. The use of two certificates per participant (one for encryption/decryption and one for signature) and dual signature for linking and protecting order and payment information (e.g. account number) fulfilled the security requirements. The biggest problem is the need for clients to acquire/purchase two certificates should they opt to initiate a SET-based transaction.

WPP, on the other hand, does not route payment transaction data via the MA. As a result, the implementation of security becomes less onerous. A dual signature is not required since customer's payment instructions are no longer sent to the merchant and thus cannot be altered by the merchant. In fact, in WPP it is the banking information of the merchant (previously encrypted by the bank) which is sent to the CA and then forwarded to the Customer's Bank. In addition, as the WTLS provides most of the security services required, only one certificate is required by the participating entities to sign key data (e.g. purchase request from customer and purchase invoice from merchant) at the application layer. Although customers will be required to obtain a certificate, as with SET, we expect that certificates will be made available (free of charge) in the near future.

Finally, the use of SCs for storing encrypted banking information and Personal Identification Number (PIN) permits us to incorporate other types of payments including debit card payments. Since PINs are strictly used for authorizing access to the SCs and are not transmitted over the network, the security of PINs are preserved. If, on the other hand, the encrypted PINs are stored in workstations and transmitted via the Internet, as it could be with the SET protocol, the security of the PINs is questionable. This is one of the main reasons why debit card payments have not been made available via the Internet.

Performance

The issue of performance is equally important to mobile users since improved performance (lower processing time) results in reduced communication costs. The performance of a protocol is dictated by the following key factors : transaction flow, bandwidth requirements (number and size of messages) and computational requirements.

In terms of the transaction flow, it is already clear that WPP is expected to provide a faster processing time per transaction than SET due to the reduced number of messages in the protocol.

As far as bandwidth requirements are concerned, the exchange of multiple certificates and data in the SET protocol requires considerably more bandwidth than WPP. By keeping the size of messages to a bare minimum, we were able to lower the requirements for precious bandwidth.

Finally, the computational requirements of the protocol is clearly a contributing factor in the area of performance. In terms of SET, the need for dual signature and multiple layers of encryption at the application layer has resulted in a protocol too demanding for mobile computing [10].

WPP, on the other hand, is optimized to operate more efficiently over wireless networks. This includes limited number of security mechanisms (e.g. digital signature) implemented at the application layer as well as the use of SCs to enhance the processing capabilities of the mobile devices.

III. RESULTS OF IMPLEMENTATION

In order the test the feasibility of the Wireless Payment Protocol, we installed an Intranet and used the Nokia WAP server and toolkit to simulate a wireless infrastructure. While the WAP server (running servlets) represented the merchant site, the toolkit simulated the Nokia phone (model 6150), see Figure 3. The banking service was developed using Java 1.2 and Java Cryptographic Extension (JCE).

In the process of implementing the protocol, the following issues became apparent. First and foremost, is the lack of sufficient intelligence on the part of the mobile devices. For example, it was not possible to carry out cryptographic functions such as digital signature using only the scripts in WAP. We, therefore, supplemented the scripts with a small Java program. Second, in order to reduce the size and number of data packets being transmitted, we did not transmit certificates. Instead, a distribution service was used to fulfill that requirement. Finally, the need to store data such as reference numbers (sent by the bank) on mobile devices has yet to be addressed. Perhaps SCs will provide this capability in the near future.

Figure 3 Simulation using Nokia phone

IV. CONCLUSION

The WPP represents a non-proprietary solution designed to provide the following benefits : enhanced security, increased performance and support for debit card payments and perhaps other types of payments as well. Enhanced security is achieved by leveraging on the security services of the WTLS layer of the WAP protocol stack and by sending customer's private data directly to the bank. This routing strategy was intended to address customer's greatest concern : transmission of confidential information to the merchant, especially if merchants are using a peer-to-peer protocol such as SSL.

Given that WPP would be implemented over a wireless network marked by limited bandwidth and high latency, every effort was made to reduce the size and number of messages exchanged between all agents participating in the protocol. In addition, the number of cryptographic functions to be carried out on the wireless devices was also kept to a minimum in order to accommodate the processor and battery-constrained devices.

Unlike POS purchases and ATM machines which use private networks to support debit-card transactions (transmit the account and PIN numbers), this type of transaction has not been made available over the Internet for a good reason. Storing encrypted PIN numbers on workstations and transmitting them over an open network poses serious security concerns. It is clear that an alternate strategy is required if WPP is to support debit-card transactions as well. By using the PIN number to authorize access to the Smart Card storing confidential banking information, the need to transmit PIN number was eliminated. In fact, the same PIN number will now be required to authorize both credit and debit-card transactions.

While a brief comparison to the SET protocol was made to illustrate these benefits, readers are encouraged to consult [9] for additional details.

Although results of the implementation suggest the need for greater intelligence on the part of mobile devices (than supported by WAP), we are confident that it is only a matter of time before this issue is addressed.

In the meantime, the use of mobile software agents to further alleviate the resource requirements of mobile devices will be analyzed. Although the use of mobile agents, which carry out their tasks within the operating environment (place) of the merchant, remains controversial with respect to security, the transaction flow of the WPP may minimize the security threats surrounding mobile agents.

REFERENCES

[1] Brokat, Business goes Mobile, Mobile Business Applications, Version 1.2 Business White paper, 1999, Available at www.brokat.com

[2] Ghosh, Anup K. E-Commerce Security Weak Links, Best Defenses, 1998, pp. 137-146

[3] Anderson, Milton M. The Electronic Check Architecture, Financial Services Technology Consortium, Version 1.0.2, September 29, 1998.

[4] VISA & Mastercard, SET Secure Electronic Transaction Specification, 1997.

[5] Romao, Artur and Mira da Silva, Miguel. An Agent-Based Secure Internet Payment System for Mobile Computing. Proceeding of International IFIP/GI Working Conference. Germany, 1998, pp. 80-93.

[6] Brunker, Mike. E-business vs. the perfect cybercrime, 2000. Available at www.msnbc.com/news/376973.asp

[7] Website of Bank of Nova Scotia, www.scotiabank.com

[8] WapForum, Wireless Application Protocol (WAP) White Paper, October 1999, Available at www.wapforum.com

[9] Hall, Jeyanthi and Kilbank, Susan. WPP: A Wireless Payment Protocol, 2001, Available at www.scs.carleton.ca

[10] Daswani, Neil and Doneh, Dan, Experimenting with Electronic commerce on the PalmPilot, Financial Cryptography : 3rd International Conference, 1999, pp. 1-16