Computers & Security Vol.19, No.5, pp.453-465, 2000

0167-4048/00$20.00

A Generic Electronic Payment Model Supporting Multiple Merchant Transactions

Yu-Lun Huang, Shiuh-Pyng Shieh, and Fu-Shen Ho[1]

Department of Computer Science and Information Engineering, National Chiao Tung University, Hsinchu, Taiwan 30010.

This paper presents a generic electronic payment model which is intended for a multi-merchant transaction, in which more than one merchant (the retailer, multiple resellers and content providers) are involved in the distribution of electronic contents. With our payment model, every involved merchant will be notified to verify the license information of a content on the settlement day before the customer actually pays for his purchase. Thus, piracy can be discouraged, intellectual property rights of electronic contents can be protected. Each of the involved merchants can obtain his own deserved share of the customer's payment in accordance with their union agreement on this content. As examples to demonstrate the applications of our generic payment model, two well-known payment systems are enhanced herein, based on our payment model.

Keywords: Payment model, electronic commerce, network security, copyright protection, electronic content distribution.

1. Introduction

Advance of modern network technologies makes electronic distribution of contents increasingly popular and meanwhile promotes the acceptance of electronic commerce. The facile distribution of electronic contents also has side effects that make illicit copying and dissemination rather easy. Recently, many online payment systems [1-7] were proposed to achieve the confidentiality of a transaction and the privacy of an electronic content. With these payment systems, customers can select a retailer and order any desired contents over the network. Unfortunately, manufacturers who produce the contents have no control over them after they have been delivered to the retailers. Even if the content providers hold the copyrights of the contents, retailers can still sell to customers as many pirate copies as they wish. In this situation, customers pay directly to retailers whenever they order the contents, and the retailer can obtain the total purchase amounts from customers regardless of the methods of payment (e.g. using a credit card or electronic wallet [8, 9]).

To solve the problem described above, copyright controls over electronic contents must be incorporated into current payment systems to meet the future trends. *Figure 1* illustrates an experimental environment developed in the "Multimedia Interactive Information System" project supported by the National Science Foundation, Taiwan and Mentor Data System Inc. since August 1996. The goal of this project is to design and implement a high-speed multimedia interactive information system over Hybrid Fiber Coax (HFC) networks.

In the system, service providers offer video-on-demand services and sell electronic contents to their local subscribers via community coax-cable networks and content providers offer electronic contents (e.g. movies or news) to service providers via high-speed backbone networks. When a customer (i.e. local subscriber) orders a movie from his local service provider using his set-top-box at home, he must pay for the

[1] This work is supported in part by National Science Council, Taiwan and Mentor Data System Inc.

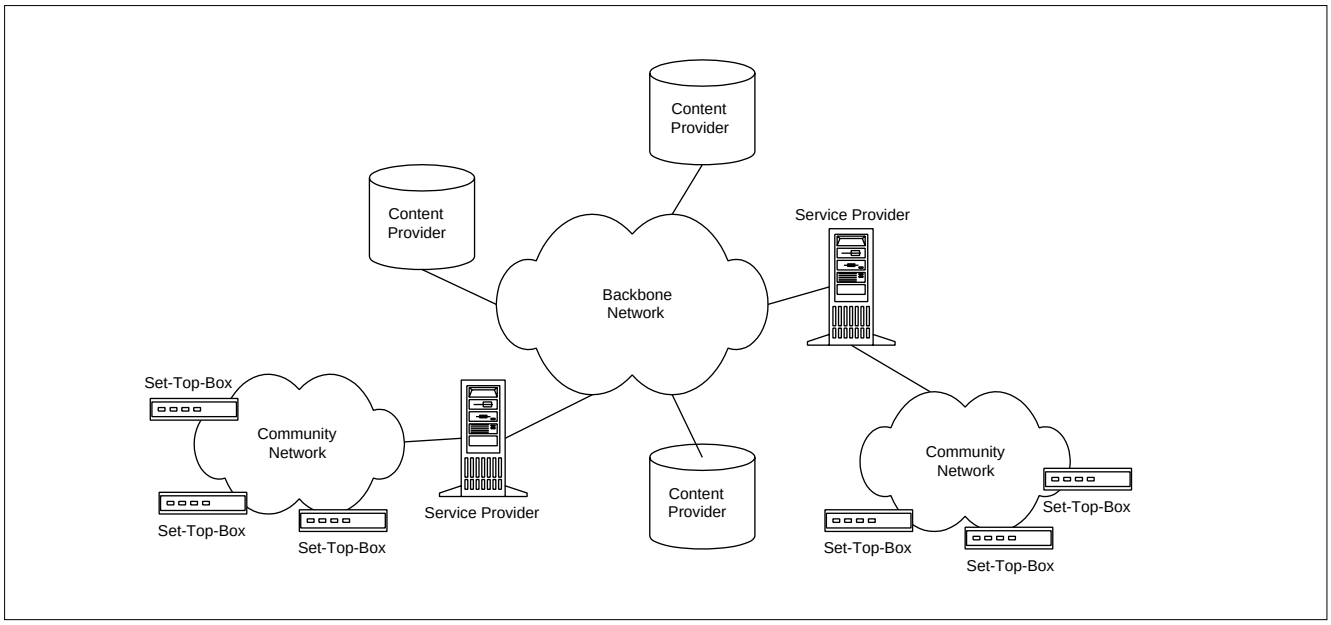

Figure 1: The multimedia interactive information system.

movie. Since the copyright of the movie still belongs to the content provider, the local service provider and the content provider must agree on a royalty for the movie whenever a copy of the movie is sold. Thus, the customer's payment must be divided into two parts, one for the service provider and the other for the content provider, according to the agreement.

In this environment, a service provider acts as a retailer that is the agent of the content provider or reseller to sell electronic contents. Moreover, a content may be produced by more than one collaborative content provider. In this case, the apportionment of royalty among the co-producers must be stated in their union agreement on the content. According to the agreement, all of the involved merchants (the retailer and co-producers) can obtain their own shares of the customer's payment whenever the retailer sells a copy of the content produced by the collaborative content providers.

To protect the intellectual property rights of electronic contents from illicit copying and distribution, watermarking [10-11] and steganography [12] techniques can be adopted as the fundamental means. Nevertheless, an online retailer in current payment systems can still duplicate and sell a watermarked content to customers without the knowledge of and the payment to the corresponding content provider. A customer can recover the copyright information from the purchased content and know its original provider or producer. Despite this, a customer is unable to know if the purchased content is a legal or pirate copy, and a retailer can still gain benefits by selling pirate copies of contents even if they have been watermarked. As a result, a content provider cannot obtain his deserved share of customer's payments according to the union agreement on this content because the protection of a content's copyright cannot be ensured. As another means to protect copyrights, Choudhury et al. proposed two simple cryptographic protocols [13] to discourage the distribution of illicit electronic copies. Their protocols can also make electronic document distribution secure. However, payment support is not present in their proposed protocols.

This paper proposes a generic electronic payment model for a multi-merchant transaction. In a multi-merchant transaction, more than one merchant (i.e. at least a retailer and multiple content providers) may be involved. Every involved merchant is notified to verify the license information upon settlement before the customer pays for his purchase. Incorporated with

watermarking techniques, pirate copying can be discouraged and intellectual property rights of electronic contents can be protected. Moreover, each of the involved merchants can obtain his own share of customer's payment in accordance with the agreements on the contents. Our payment model does not specify any procedures of customer authentication, transaction authorization and payment transfers. It can be applied to the existing payment systems without significant modifications.

In our payment model, the content provider sends a copy of the electronic content to the retailer together with the content's digital selling license to the retailer. A trusted third party is involved to judge the legality of a transaction. Then, a digital receipt for this transaction dual-signed by both the customer and the trusted third party is forwarded to the retailer. Periodically, the retailer can request for payments according to the collected dual-signed receipts. A transaction will only be successful with the presence of an authorized selling license and a dual-signed receipt. By sending a selling license and a dual-signed receipt to the trusted third party, the copyright of an electronic content can be protected, and the piracy can be eliminated.

This paper is organized as follows. In Section 2, the overview of our payment system will be presented. Then, we will propose a secure electronic payment model with supports of multi-merchant transactions in Section 3, and give the application of our payment model to the enhancement of two well-know protocols in Section 4. Finally, security analysis of our payment model is discussed, and conclusions are given in Sections 5 and 6, respectively.

2. System Overview

In this section, we describe the necessary system components and security requirements of our payment model when applied to the existing online payment systems.

2.1 System Components

The payment-related components required by our payment model, as shown in *Figure 2*, are customers, merchants (retailers, resellers and content providers), delivery networks, certificate authorities (CA), payment gateways (PG) and existing authorization/financial networks.

In our model, a customer can order electronic contents from a retailer or service provider, which is a type of merchant involved in a transaction. A content provider (CP) is another type of merchant that produces electronic contents and sells them to retailers. In general, only one retailer and one content provider participate in a transaction. Sometimes, more than one content provider may be involved, because it is likely that a content may be produced by more than one collaborative content provider.

A certificate authority is a trusted third party on a delivery network, in charge of management of certificates. Customers, retailers and content providers must register with their local certificate authorities and obtain their own certificates. Our payment model will work only when every participant has his own certificate. A payment gateway is a bridge between the delivery network and the authorization/financial network. The former is a network where the transaction takes place, and the latter is responsible for authentication of customers, authorization of transactions and settlements. The main components on the authorization/financial network are authentication centres, which play the role of financial institutions or banks.

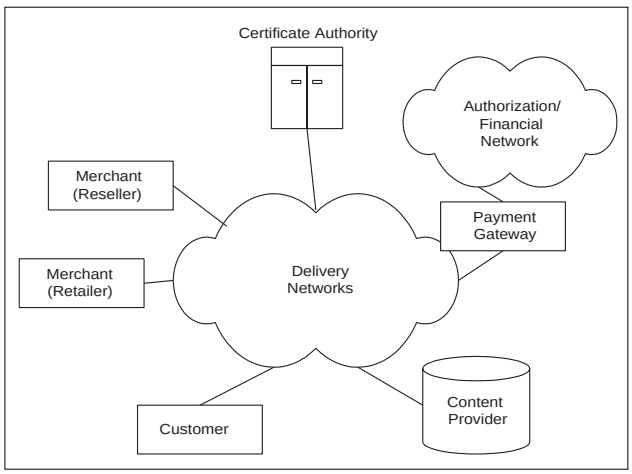

Figure 2: Payment-related system components.

2.2 Security Requirements

The aim of our model is to address certain security issues related to multiple merchant mechanisms conducted over the service networks. Copyright protections, content integrity, content confidentiality, transaction privacy, non-repudiation and authentication are the most important issues to achieve the goals of our model.

Copyright protection can prevent the electronic contents from illicit copying and distribution. Watermarking and steganography techniques can be adopted as the fundamental means to protect the intellectual property rights. Integrity is the assurance that the data received is exactly the data sent. Cryptographic message digest function [14] must be applied to assure the integrity of a content. Confidentiality is the protection of private information from unintentional and intentional attacks and disclosure. To reach the content confidentiality, we can use any symmetric encryption algorithm [15]. Transaction privacy indicates that only the intended receiver can realize the content of encrypted transaction message. Asymmetric encryption algorithm [16] can be used for attaining the privacy of the transaction. Non-repudiation means if the customer has ordered an electronic content, he or she can never repudiate the transaction and has to pay for the ordering. A digital signature algorithm [17] can be taken to achieve non-repudiation. Authentication provides assurance that the data received was sent by the entity that claims to have sent it. In our payment model, the authentication of a customer is accomplished by the applied payment protocols such as Secure Electronic Transaction (SET) [1-3] and NetBill [4-5].

3. The Payment Model

In this section, we describe the proposed payment model in detail. In our payment model, there are three phases: sale preparation phase, purchase phase and payment capture phase. The sale preparation phase starts when a new content is produced. The first phase finishes when the content is ready for sale by retailers. The purchase phase begins when any customer issues a purchase request message and continues until the customer gets the ordered content. In this phase, the retailer involved in the transaction can also hold a customer non-repudiated credential for the transaction. The payment capture phase starts when a retailer requests the payment gateway to acquire the payment and ends with the completeness of the clearing.

We first define the notations and cryptographic functions which will be used in our payment model in *Tables 1* and *2*, respectively, before the three phases are introduced.

Notation	Description
CD	content description
Chall	a challenge text for authentication
CID	customer identifier
CPID	content provider identifier
ExpDate	the expiration date of a message which contains the issued time and the expired time
Kss	session key to encrypt or decrypt the content
ReqDate	date for request message
RID	retailer/reseller identifier
CERT(x)	certificate of entity *x*
MAC(x)	message authentication code of message *x*

Table 1: Notation Definitions.

Function	Description
E(k, x)	encrypts message *x* with the key *k* in the symmetry key cryptosystem
P(k, x)	encrypts message *x* with the public key *k* in the public key cryptosystem
S(r, x)	signs message *x* with the signature key of entity *r*

Table 2: Cryptographic Function Definitions.

3.1 Sale Preparation phase

In the first phase, each participant must register with his local certificate authority, and obtain his own certificate and secret key. The certificate authority may issue X.509 [18] standard compatible certificates. Then, the content provider must apply for an authorized digital license for a newly produced electronic content.

Notation	Description	Content
PAN	Publication Authorization Number	
SAN	Selling Authorization Number	
CPIDList	content provider identifier list	
Prop	proportions of apportionment among the involved merchants.	
PubDate	publication date of a content	
PAL	publication authorization license	S(LICA, {PAN, CPIDList, PubDate, MAC(content)})
SL	Selling License of a content	S(CP, {RID, CPID, ExpDate, SAN, PAL, Prop, MAC(content)})
PALReq	PAL request message	E(Kss, Content), P(LICA, S(CP, {Kss, ExpDate, CPID, MAC(Content), Chall}))
PALRes	PAL response message	P(CP, {PAL, Chall})
ContentReq	content request message	{RID, CD, ExpDate, Chall}
ContentRes	content response message	E(Kss, Content), P(M, S(CP, {SL, Kss, Chall}))

Table 3: Licence definitions.

A digital license is a certificate indicating a merchant is legally authorized to sell the content. The concepts of our digital licenses are introduced herein to solve the problems resulting from the intellectual property protection and apportionment among multiple merchants for various kinds of network systems. After the idea of digital licenses is introduced, we extend it to accept multiple content providers and resellers. The notations used in the first phase are defined in *Table 3*.

Every time the production of new content is completed, the content provider should apply for a Publication Authorization License (PAL). The license application can be accomplished by traditional or electronic procedures. If an electronic procedure is used, a content provider sends a PAL request (PALReq) message to a License Issuing Certificate Authority (LICA) to apply for a PAL for this new content. A PAL request contains the encrypted content and all necessary information and decryption key to the content to apply the PAL. A LICA can be an online public service provided by government agency or trusted organizations. A LICA issues PALs after verifying the legality of the content provider and the content.

On receiving a PALReq from the content provider, the LICA will issue a PAL of an electronic content after the content is examined and certified according to the related regulations. A PAL signed by the LICA consists of a Publication Authorization Number (PAN), the name of the content, the message digest of the content, the content provider list or copyright owner list, content category, issued date and other related information.

After the PALRes containing the PAL of the content is obtained, the content provider is able to issue the self-signed Selling License (SL) of this content. A SL consists of a Selling Authorization Number (SAN), the PAL, proportion of apportionment and other information. In our payment model, the retailers who want to sell this content to customers need SLs. A retailer can sell a content legally only when he owns the SL. Since the linkage between a content provider and a content is presented in the PAL and cannot be modified without the signature key of the LICA, therefore, protection of intellectual property rights can be ensured. The contents of a digital license will be defined in Section 4.1. The flows of licenses described above are be summarized in *Figure 3*.

Sometimes, a content can be produced by more than one collaborative content provider. In such a scenario, as the new content is submitted to a LICA for certification, the content's PAL includes the list of

identifiers of all involved content providers and the proportions of apportionment among these content providers.

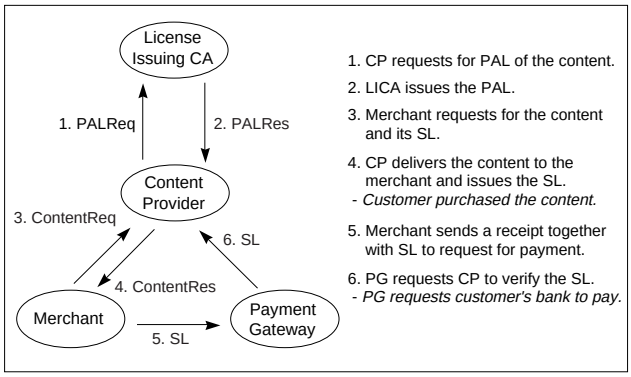

Figure 3: Flows of digital licenses.

Consider another scenario (shown in *Figure 4*) where a content is first sold to a merchant (say M_1), and then sold to the second merchant (M_2), the third merchant (M_3) and the retailer (M_n). In the scenario, the content provider needs to deliver to M_1 the requested content along with a selling license (SL_1) which contains the PAL of the content. M_1 then sends to M_2 the requested content along with another selling license (SL_2) in which the PAL has been replaced with SL_1. The same process repeats until the content reaches the retailer (M_n).

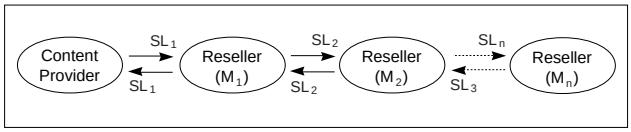

Figure 4: Issuance of selling licenses between merchants.

Later, when the retailer sells the content and requests for the payment, the selling license (SL_n) will return to his parent merchant (M_{n-1}) for verification, and in turn M_{n-1} will return SL_{n-1} to M_{n-2}, and finally back to the content provider. Only when all selling licenses are verified, can the customer's bank pay each of the designated merchants. As a result, no matter how many merchants are involved in a transaction, apportionment among multiple merchants can still be guaranteed and illegal content copying can be discouraged by applying our payment model.

3.2 Digital Receipts

Before we introduce the purchase phase, the concept of a digital receipt must be presented first. The purpose of a digital receipt in our payment model is to achieve the customer non-repudiation of a transaction. The receipt of a transaction can be issued either by a payment gateway or a customer. The payment gateway is a party involved in the online transaction to judge the validity and legality of the transaction. The information required by a receipt depends on the applied payment protocol. However, no matter what payment protocol is applied, the indispensable information in the receipt is the SL of the ordered content, the merchant and the customer identifiers.

If the receipt is initially signed by a payment gateway, it will not be valid before the customer also signs this receipt at the end of the transaction. Similarly, if the customer initially signs the receipt, the receipt will not be valid before the payment gateway also signs this receipt at the end of the transaction. In both cases, the customer can verify the validity of the SL by himself if he wishes, or he can leave the work to the payment gateway if he has less computing power. The latter choice does no harm to the customer, because the customer's bank will pay for the transaction only if the SL is valid.

In this paper, we refer to an initially signed receipt as a Half-Signed Receipt (HSR) and a dual-signed HSR as a Full-Signed Receipt (FSR). If the HSR is initiated by a payment gateway (shown in *Figure 5(a)*), the retailer can receive a FSR from the customer at the end of a transaction. Alternatively, the retailer can obtain a FSR from the payment gateway while the HSR is initiated by the customer (shown in *Figure 5(b)*). Periodically, the merchant can send the collected FSRs to the payment gateway and requests for the payments.

A payment gateway also acts as a trusted third party that bridges between the service network and the authorization/financial network. A PG extracts an SL from a received FSR and requests the corresponding content provider to verify the validity and legality of the SL. Then, according to the selling license wrapped

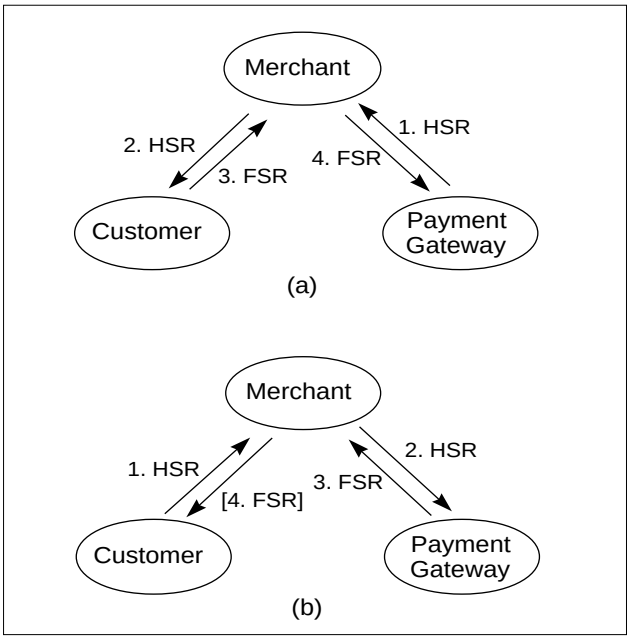

Figure 5: Flows of a receipt (a) with a PG-initiated HSR, and (b) a customer-initiated HSR.

in the FSR, the PG signals the customer's bank to apportion the payment proportionally among the involved merchants. The per-transaction fee of a PG is a policy issue, which is out of the scope of this paper.

3.3 Purchase Phase

The customer will finish all necessary processes of a transaction in the purchase phase. The retailer should obtain the selling license of the requested content in the sale preparation phase prior to purchase phase. The purchase phase starts with a purchase request message issued by a customer after the price of the content has been negotiated. The customer authentication is also attained in the purchase phase. Since there are two modes for an HSR initiation, the steps of the purchase process differ slightly.

3.3.1 PG-Initiated HSR Mode

In PG-initiated HSR mode, a payment gateway issues a receipt signed with his own private key for a transaction before the customer also signed the receipt. The receipt will not be valid until the payment gateway and the customer both sign the receipt. The notations used in the purchase phase are defined in *Table 4*.

Function	Description
PurchaseReq	Purchase request from a customer
PurchaseRes	Purchase response from a retailer
AuthReq	Authentication request from a retailer
AuthRes	Authentication response from a customer's bank
EKE	Encrypted Key Envelope

Table 4: Purchase message notation definitions.

The steps of a PG-initiated HSR payment process are described as follows and shown in *Figure 6(a)*.

1. Customer→Retailer: PurchaseReq

   At the first step, when a customer wants to order a content, he will send his own certificate and the purchase request message to the retailer. The information given in PurchaseReq must be capable of proving the customer's identity. The actual contents of PurchaseReq differ according to the chosen payment protocol and the operating environment. Since the focus of our paper is a new payment model suitable for multi-merchant payments, the actual contents of common authentication messages are not addressed. We will give a practical example in Section 5, where our payment model is used to enhance SET protocol and NetBill system.

2. Retailer→PG: AuthReq

   Upon receiving the request message from the customer, the retailer verifies the contents of the message and looks up the customer's certificate in the Cetificate Revocation Lists (CRLs) or any other access control lists which may prevent some customers (e.g. kids) from ordering contents of certain categories (e.g. adults movies). If the customer's certificate is still valid and permitted to order the content, the retailer will continue to authenticate the customer. Since the retailer

cannot authenticate the customer by himself, he will request PG to authenticate this customer for him. The retailer will generate and send out an authentication message that includes the SL of the content.

3. PG→Retailer: AuthRes (including the HSR)

   Upon receiving the authentication request from the retailer, PG further requests the customer's bank or authentication server to authenticate his identity and check the customer's credit limit according to the authentication message from the retailer. After the authentication server replies, PG checks the result of authentication. If the customer is authenticated and the amount of purchase does not exceed his credit limit, PG continues to check the SL of the content. If the copyright is not violated in this transaction, PG will issue a half-signed receipt (HSR) which is signed with the signature key of PG. Then, PG will send back the authentication response together with the HSR to the retailer. The HSR will be signed later by the customer at the end of transaction and becomes a full-signed receipt (FSR).

4. Retailer→Customer: PurchaseRes (including the HSR and EKE)

   Upon receiving the authentication response from PG, the retailer stores all necessary information. Then, according to the response, the retailer sends back the purchase response (PurchaseRes) message to the customer that indicates the result of the transaction. Moreover, the retailer also sends back the HSR obtained from PG and an encrypted key envelope (EKE) which is encrypted with the customer's public key. An EKE consists of the encryption key of the purchased content and other information needed for the prevention of replaying and forging of the envelope.

5. Customer→Retailer: FSR

   Upon receiving the authentication response from the retailer, the customer keeps this response in memory and decrypts the HSR with PG's public key. After the customer has successfully verified the correctness and authenticity of the HSR, he will generate the FSR by signing the verified HSR with his own signature key. Then, the FSR will be sent to the retailer, and after some time, the retailer can request for the payment of this transaction according to this FSR. The customer cannot repudiate this transaction, because he has signed the receipt.

6. Retailer→Customer: Encrypted Content

   Upon receiving the FSR from the customer, the retailer decrypts it with the customer's public key and compares the contents of the FSR with the HSR previously issued by PG. If the contents of both receipts match, the retailer will accept the purchase request and keep the FSR into a safe storage for future payment capture. It is at this time that the retailer delivers the ordered content to the customer, and finally, the content is encrypted with the previously negotiated encryption key wrapped in EKE and sent to the customer.

3.3.2 Customer-Initiated HSR Mode

In customer-initiated HSR mode, the PurchaseRes generated by the retailer is different from that in PG-initiated HSR mode. The PurchaseRes contains the selling license and the ordered content encrypted using an encryption key randomly generated by the retailer. The customer cannot decrypt the encrypted content until the encryption key is obtained. On receiving the PurchaseRes message, the customer generates a HSR that includes the selling license of the ordered content and sends it to the retailer. The customer-initiated HSR payment process is shown in *Figure 6(b)*.

First, upon receiving the HSR issued by the customer, the retailer checks its content and sends the payment gateway an AuthReq message which includes the HSR signed by the customer. The payment gateway signals the customer's bank for authentication. If the result is legal and valid, the payment gateway generates the FSR by signing the HSR and sends the AuthRes to the retailer. On receiving the FSR from

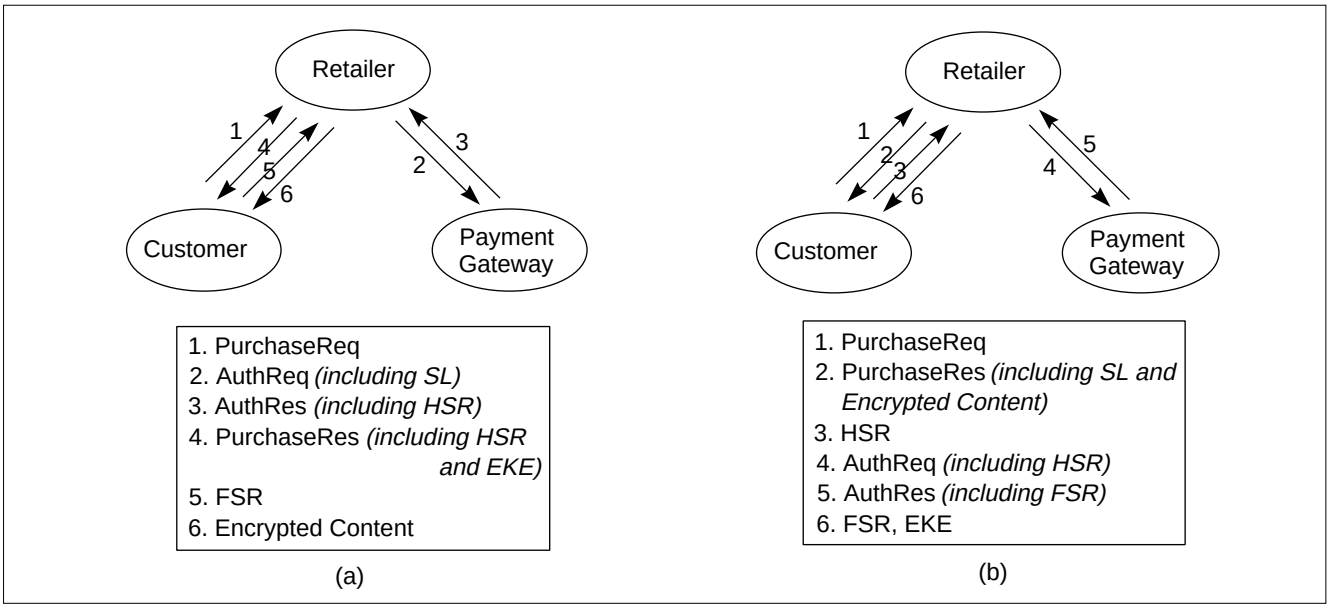

Figure 6: Flows of purchase phase with (a) a PG-initiated HSR, and (b) a customer-initiated HSR.

the payment gateway, the retailer sends out the FSR and the encryption key wrapped in the EKE for the customer. If the customer finds that the encrypted content is not exactly the one he ordered, he may ask the retailer to retransmit the ordered content or prosecute the retailer according to the purchase policies.

3.4 Payment Capture Phase

No matter what mode the applied payment system adopts, payment capture phase is the same. Periodically (e.g. on monthly settlement day), a retailer can send the collected FSRs to PG and request for the payments. On recipient of each FSR, PG must recover the SL from it and request the corresponding content provider to verify the validity and legality of the license.

When the SL is verified to be valid and legal, PG can receive a response from the content provider. Then, PG separates the amount into multiple items according to the proportions of apportionment listed in the SL and its PAL. After transforming these payment items to the messaging protocol of the authorization/financial network, PG sends out the clearing messages and requests the customer's bank to pay for this transaction. All of the payment processes afterwards can be accomplished by the existing financial network [19] and thus they are not discussed in this paper.

4. Applications of our Generic Payment Model

In this section, we give the application of our payment model to two well-known online payment protocols (e.g. SET and NetBill). Based on our payment model, these two protocols are enhanced such that the copyright of an electronic content can be protected and the piracy can be eliminated.

4.1 PG-initiated HSR: example of SET

Secure Electronic Transaction (SET) [1-3] is a famous payment protocol proposed by VISA and MasterCard Inc. in early 1996. In SET protocol, even though a merchant (retailer) and a customer (cardholder) can achieve a secure transaction over the Internet, the problems addressed in Section 1 still cannot be solved. This is because all SET transactions are transparent to the content provider. However, if our payment model is

used to extend SET protocol, not only fair apportionment among multiple merchants can be guaranteed, but copyrights of the contents can also be protected. The extended SET protocol is shown in *Figure* 7.

The sale preparation phase consists of two steps (steps 1 and 2), the purchase phase consists of seven steps (steps 3-9) and payment capture phase consists of two steps (steps 10 and 11). The bold messages are the additional fields compared to the original SET protocol contents (in normal style), and the bold lines (steps 1, 2 and 9) are the additional messages. Messages in brackets are optional and fields in parenthesis are additional fields compared to the original SET protocol. For each content, sale preparation phase is performed only once when it is initially requested by the retailer.

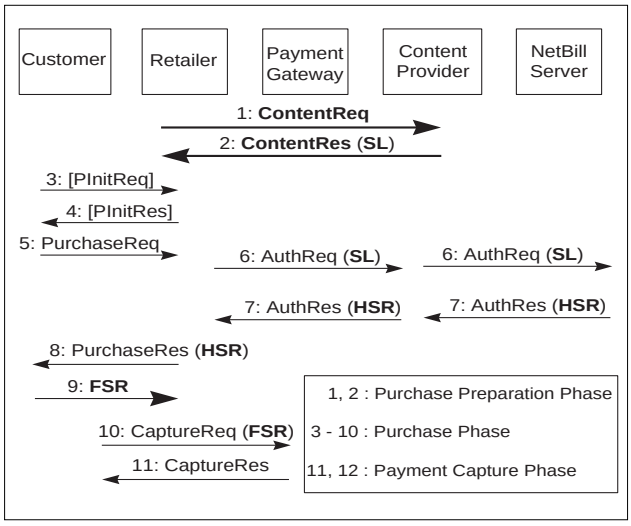

Figure 7: The extended SET protocol.

As described in SET specification [1-3], steps 3 and 4 can be omitted if the price information can be obtained from offline mechanisms (such as CD-ROM). Step 5, the PurchaseReq message, is the same as the PurchaseReq message specified in SET, while the PurchaseRes message (step 8) contains both the original PurchaseRes message and the HSR issued by the payment gateway. Steps 6, 7, 10 are also the modified SET messages. They contain not only the original SET messages, but also the selling license or the receipt. The extra field compared to the original SET protocol is specified in the parentheses shown in *Figure* 7. The contents of the HSR and the FSR may be as follows.

HSR: S(PG, {LID_M, LID_C, SL, ExpDate, TransID, [Chall_C], [Chall_M]});

FSR: S(C, S(PG, {LID_M, LID_C, SL, ExpDate, TransID, [Chall_C], [Chall_M]}).

The ExpDate, and SL are defined in Tables 1 and 3. The TransID is a unique transaction identifier defined in SET. The LID_M (merchant's local identifier), LID_C (customer's local identifier), Chall_C (challenge issued by the customer), and Chall_M (challenge issued by the merchant) are also defined in SET. Since the HSR is initiated by the payment gateway in the extended SET protocol, the receipt will not be valid before the customer also signs this receipt at the end of the transaction. Therefore, copyright protection and apportionment among multiple merchants can be achieved in the extended SET protocol.

4.2 Customer-initiated HSR: example of NetBill

NetBill [4] proposed by B. Cox, J. D. Tygar and M. Sirbu in 1995 is a system for micropayments for information goods on the Internet. In the NetBill system,

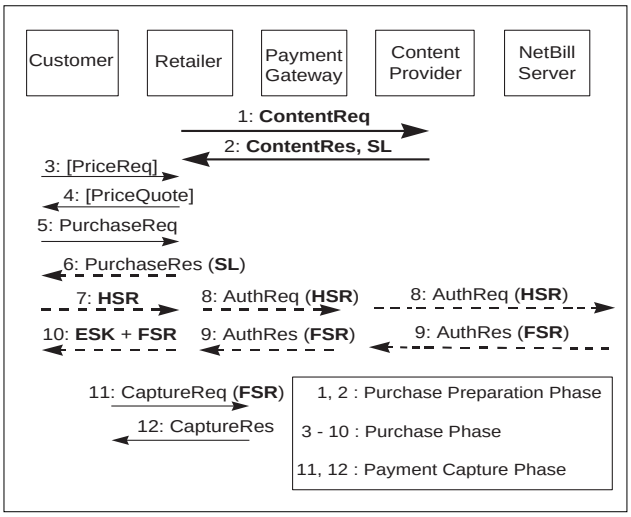

Figure 8: The extended NetBill protocol.

even though a merchant (retailer) and a customer (cardholder) can achieve a secure transaction over the Internet, the problems occurred in SET also exist. However, if our payment model is applied to be an extension of the current NetBill protocol, both fair apportionment and copyright protection can be achieved. The extended NetBill protocol based our payment model is shown in *Figure 8*.

In *Figure 8*, sale preparation phase consists of two steps (steps 1 and 2), purchase phase consists of eight steps (steps 3 to 10) and payment capture phase consists of two steps (steps 11 and 12). The modified messages are presented in broken lines, and the bold lines (steps 1 and 2) are the additional messages. For each content, sale preparation phase occurs only once when the retailer initially requests the content. Data in steps 3 and 4 are used for price negotiation. Step 5, PurchaseReq message, contains the same fields as those provided in GoodsRequest message in the original NetBill protocol. Upon receiving the PurchaseReq message from the customer, the retailer issues the PurchaseRes message (step 6) which contains the ordered content and the selling license of that content. The ordered content is encrypted with a randomly generated encryption key. The key is still unknown to the customer, when he receives PurchaseRes message. Steps 7-11 are also the modified NetBill messages. They contain not only the original NetBill messages, but also the receipts of the transaction. The additional fields are specified in the parentheses and shown in *Figure 8*. The content of the HSR and the FSR may be as follows.

HSR: S(C, {EPO, SL});

FSR: S(PG, S(C, {EPO, SL}).

The Electronic Payment Order (EPO) is a customer-signed electronic payment order defined in NetBill, which presents the non-repudiation for the customer. Since the HSR is initiated by the customer in the extended NetBill protocol, the receipt will not be valid before the payment gateway also signs this receipt at the end of the transaction. Thus, fair apportionment among involved merchants and copyright protection can be guaranteed as well.

5. Security Analysis

In this section, we analyze the security of our payment model by presenting three possible attacks and our solutions to these problems. Consider the following scenarios:

1. A customer repudiates a transaction.

   When a retailer starts his payment capture process, the acquirer bank requests customers to pay for their previously purchased contents. If any customer denies the payment request, none of the involved merchants can receive their share. In this case, the retailer can request the payment gateway for arbitration. To receive the decryption key of the content from the retailer, the customer must sign a digital receipt (either a HSR or FSR). On the other hand, the payment gateway that has authenticated the customer also signs the digital receipt. Since a customer has agreed on a transaction by signing the receipt with his private key, the presence of a full-signed receipt becomes a non-repudiated evidence for the transaction. Therefore, a customer cannot repudiate the transaction in our model.

2. A retailer defrauds in a transaction.

   In most online payment systems, either the customer receives the content before he signs the receipt, or the retailer obtains the payment before he delivers the content to the customer. If a customer does not receive his ordered content from the retailer at the end of the transaction, he can ask the retailer to deliver the electronic content again. If the retailer defrauds maliciously and is unwilling to deliver the content to the customer, the customer can ask for human arbitration.
   In addition, a retailer may claim the rights to sell the content, which in fact he does not possess. In this case, the content provider cannot obtain his deserved benefits. However, this problem does not exist in our model because the retailer must acquire a selling license from the content provider in advance before the transaction can be successful. Moreover, a forged selling license can be detected easily in our model, because a selling

license will not be valid before the content provider signs it. Therefore, any party who receives the selling license can verify its validity using the public key of the content provider.

3. Collusion of a retailer and a customer

   In current payment systems, since there is no copyright information bundled into a content, a retailer is able to sell an illicit copy of the content to the customer by giving a discount. As a result, the content provider cannot acquire his deserved benefits. In our payment model, all transactions must be approved by the payment gateway. If a retailer does not possess a legal selling license, the content provider will reject the payment of the transaction in the payment capture phase. Furthermore, although the pirate retailer can sell an illicit copy through other channels without the payment to the content provider, the illegal dissemination can be detected because all contents have been watermarked with the copyright information.

Therefore, in our proposed model, not only apportionment among multiple merchants is supported, but also the attacks mentioned above can be prevented effectively.

6. Conclusion

To date, many online payment protocols were proposed by researchers to achieve privacy of transactions and secrecy of electronic contents. However, little work has been done to protect copyrights of purchased contents and to guarantee the deserved profits of the content providers, especially when multiple merchants are involved. Without a secure payment system, most content providers are unwilling to sell their contents through online merchants. In this paper, we presented a secure payment model that can enable many current payment systems to handle multiple merchant transactions. In a multiple merchant transaction, illicit copying and dissemination directly affect the benefits of the original content providers.

In our payment model, the concept of digital licenses and digital receipts was proposed, and watermarking techniques were incorporated as the solution to this problem. By applying our generic payment model to the existing payment systems (such as SET and NetBill), copyright protection of electronic contents and fair apportionment can be guaranteed. Also, the new task to the payment gateway is to apportion the customer's payments proportionally among the involved merchants. However, the settlement process is a lightweight task on the payment gateway because it is performed only on monthly settlement days.

6. References

[1] VISA and MasterCard Inc., "Secure Electronic Transaction (SET) Specification: BOOK I: Business Description", Draft for testing, 31 May 1997.

[2] VISA and MasterCard Inc., "Secure Electronic Transaction (SET) Specification: BOOK II: Programmer's Guide", Draft for testing, 31 May1997.

[3] VISA and MasterCard Inc., "Secure Electronic Transaction (SET) Specification: BOOK III: Protocol Description", Draft for testing, 31 May 1997.

[4] M.S. and J.D. Tygar, 1995. "NetBill: An Internet Commerce System Optimized for Network Delivered Services," *IEEE Personal Communications*, August 1995, pp. 6-11.

[5] M.S. and J.D. Tygar. "NetBill Security and Transaction Protocol," Carnegie Mellon University, Pittsburgh, PA 15213-3890.

[6] M. Bellare et al., 1995. "iKP - A Family of Secure Electronic Payment Protocols," *IBM Journal*, 12 July 1995.

[7] J.P. Boly et al., 1994. "The ESPRIT Project CARE - High Security Digital Payment Systems," ESORICS '94, LNCS 875, Springer-Verlag, Berlin 1994, pp. 217-230.

[8] DigiCash, "About ecash," <http://www.digicash.com/ecash/ecash-home.html>.

[9] M. Jakobsson and M. Yung, 1996. "Revokable and Versatile Electronic Money," 3rd ACM Conference on Computer and Communications Security, 14-16 March 1996.

[10] J.T. Brassil et al., 1994. "Electronic Marking and Identification Techniques to Discourage Document Copying," *Proceedings of IEEE INFOCOM '94*, (Toronto, Canada), IEEE, June 1994, pp. 1278-1287.

[11] S.H. Low et al. "Document Marking and Identification using Both Line and Word Shifting", AT&T Bell Laboratories.

[12] W. Bender et al., "Techniques for data hiding," Massachusetts Institute of Technology, Media Laboratory, Cambridge, Massachusetts 02139 USA.

[13] A.K. Choudhury et al., 1994. "Copyright Protection for Electronic Publishing over Computer Networks," Submitted to *IEEE Network Magazine*, June 1994.

[14] National Institute of Standards and Technology, "FIPS 180: Federal Information Processing Standard: Secure Hash Standard (SHS)," April 1993.

[15] NBS FIPS PUB 46-1, "Data Encryption Standard," National Bureau of Standards, US Department of Commerce, January 1977.

[16] R. Rivest et al., 1978. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM*, 21(2), February 1978.

[17] National Institute of Standards and Technology, "FIPS 186: Federal Information Processing Standard: Digital Signature Standard (DSS)," May 1994.

[18] Recommendation X.509 and ISO 9594-8, Information Processing Systems – Open System Interconnection – The Directory – Authentication Framework, CCITT Technical report, March 1988.

[19] ISO 8583, Financial Transaction Card Originated Messages - Interchange Message Specification, *CCITT Technical Report*, December 1993.