

Design and Evaluation of Adaptive Secure Protocol for E-Commerce

Sung Woo Tak, Yugyung Lee, Eun Kyo Park, and Jerry Stach
Computer Science Telecommunication Program
University of Missouri - Kansas City
5100 Rockhill Rd. Kansas City, MO 64110
Email: {swtak, yugi, ekpark, stach}@cstp.umkc.edu

Abstract - As Internet business exponentially grows, the need for high security level categories to identify groups of connections or individual transactions is manifest. The development of an efficient and secure communication protocol seems to be highly demanding. In this paper, we propose Adaptive Secure Protocol to support secure e-commerce transactions. Our Adaptive Secure Protocol dynamically adapts the security level based on the nature and sensitivity of the interactions among participants. The security class incorporates the security level of cryptographic techniques with a degree of information sensitivity. We implement Adaptive Secure Protocol and measure the performance of Adaptive Secure Protocol. The experimental results show that the Adaptive Secure Protocol provides e-commerce transactions with high quality of security service.

1. Introduction

As an electronic commerce exponentially grows, the number of transactions and participants who use e-commerce applications has been rapidly increased. Since all the interactions among participants occur in an open network, there is a high risk for sensitive information to be leaked to unauthorized users. Since such insecurity is mainly created by the anonymous nature of interactions in e-commerce, sensitive transactions should be secured. However, cryptographic techniques used to secure e-commerce transactions usually demand significant computational time overheads, and complex interactions among participants highly require the usage of network bandwidth beyond the manageable limit.

A current study in the area of e-commerce has been leading toward a design of a secure but an efficient transaction protocol that supports diverse security levels according to a degree of information sensitivity. Current e-commerce protocols do not still support such diverse secure interaction mechanism, although there are some exceptions of [4][7][20]. Some recent researches [15][25] focus on commercial protocols, such as STT (Microsoft Secure Transaction Technology), SEPP (Secure Electronic Payment Protocol) and SET (Secure Electronic Transaction). Some cryptographic researches study the areas related to digital receipt [2], digital signature [17][28] as a resolution of disputes, and validation of evidence [27][24]. Also, some researches deals with building a secure infrastructure based on XML and designing a fair non-repudiation protocol [2][26][29][5][6]. There are security services in distributed systems, which are built for an open and heterogeneous e-commerce in mobile communication, CORBA,

and agent-based e-commerce systems [13][16][22][26].

The design of a secure but efficient transaction protocol in e-commerce is a highly challenging task due to tradeoffs between efficiency and security. For a desired quality of transaction service in e-commerce, a secure transaction protocol should protect sensitive information while maintaining efficiency. Therefore, the secure transaction protocol should be more dynamic and adaptive so that an appropriate security level can be selected according to a degree of information sensitivity.

To address efficiency and security tradeoffs in e-commerce environments, we developed a dynamically configurable and adaptive secure transaction protocol called the Adaptive Secure Protocol. Our Adaptive Secure Protocol dynamically adapts the security level according to the degrees of complexity of network congestion and the sensitivity of information enclosed in transactions among participants.

In order to develop the Adaptive Secure Protocol, we first define an explicit notion of security levels considering the inherent tradeoffs between performance vs. security in e-commerce transactions. The development of security class aims to overcome the limitation of the traditional transaction model, which sticks on a uniform use of cryptographic techniques, by employing classification of computational and domain-specific aspects. Diverse aspects are considered to determine the security levels. They are domain-independent perspective (system and network capabilities), domain-dependent perspective (e-commerce) and customer's personal perspective. Our security classes describe the security levels and their associated cryptographic technologies to meet the requirements of the diverse perspectives.

Second, our Adaptive Secure Protocol comprises a suite of heuristics that realize dynamic security levels as well as heuristics that decide when and how to apply dynamic security. We emphasize the provision of dynamic user and application-driven security levels adjusting transaction environment and content during an application execution. Heuristics vary security levels to remain within a domain-specific level and user specified range while adapting to changing network congestion and system capability. The dynamic decision rules are employed to make the best decision on the security level of e-commerce communication. The adaptation process depends on information sensitivity, identity of transaction participants, system and network situations.

Our Adaptive Secure Protocol is fully implemented in our system, called the ASE-COM (Adaptive Secure E-Commerce) by utilizing a security class library and dynamic heuristics. The paper is organized as follows. Section 2 identifies the requirements to

adjust the level of security and describes the ASE-COM architecture. Section 3 describes the detailed design of our Adaptive Secure protocol. Section 4 presents the experimental results. Section 5 concludes this paper.

2. Adaptive Secure E-commerce (ASE-COM) System

To build an efficient and secure e-commerce system, it is necessary to identify the requirements inherent to complex and diverse e-commerce transaction. Before presenting Adaptive Secure Protocol, we will identify requirements for adaptive secure e-commerce transaction and classify them into four categories: system dependent perspective, network dependent perspective, domain-specific perspective (e-commerce) and customer's personal perspective. The meaning of "secure" is to protect any information from leakage using cryptographic techniques and "adaptive" means the system bears the system and network level changes and security level evolution to meet those changes. The architecture of the proposed ASE-COM system, which is composed of a security class library as a framework, a security classifier component with a set of heuristics, a message generator component for message encryption and a message retriever component for message description, will be presented.

2.1. Requirement Classification for Secure E-commerce Transaction

We have classified the requirements for adaptive security services into the following four categories: system, network, domain, and user. Well-classified requirements can serve as one of the important bases for the adaptive mechanism development.

(1) System dependency: There are domain-independent features in determining the security level. For instance, system configuration such as CPU and memory, is domain independent. The time to generate, deliver, and retrieve an e-commerce transaction message can be predicted for a given system capability.

(a) Computational overhead: The computational overhead for a specific cryptographic method can be quantified. The number of security operations performed over time measures the performance of message generation (encryption) and retrieval (decryption). This is a generic requirement, which is not determined by either domain or user. Under a same hardware and operating system configuration, the overhead measurement will be always consistent.

(b) Message/Key size: The size of message and the size of key used for cryptographic algorithm can be quantified. It is important to measure them, since the message/key size directly affects the computational overhead of a given cryptographic method. Sometimes, different cryptographic algorithms can be applied to different parts of a message and different size of keys can be applicable according to their sensitivity. However, how to determine/select sensitive parts in a message is a user and domain specific issue.

(2) Network dependency: This is also a generic requirement, because the security level is not effected ether by the domain or a user under a same network configuration.

(a) Network congestion: The network congestion can be quantified as the time required for message transmission. An average network transmission time during a certain period of time can be computed and applicable for an adaptive security. The rate is automatically changed by an adaptive heuristic that modifies this value with changes in system capability or user requirements.

(b) Message size: It is necessary to quantify the size of message, because the message size to be delivered also directly affects the message transmission overhead.

(c) Network type: It is necessary to identify the network type required for communication between Participants: It can be determined by not only the physical network location or configuration (LAN, WAN or Internet) of the participants but also the degree of interaction through the network.

(3) Domain dependency: E-commerce application itself may have some notion of what the secure information is, who the important participants are, when to apply and what kind of the cryptographic technologies can be applied.

(a) Message Size: It is necessary to quantify the size of message. The message size directly affects the computational and message transmission overhead. Among the whole message, a certain part may be more sensitive than other may. The selection of the sensitive portion is domain specific.

(b) Message Sensitivity: It is necessary to quantify the degree of sensitivity of messages in the e-commerce transactions because the sensitivity degree affects the selection of cryptographic methods.

(c) Participants: It is important to identify the participants and their roles in e-commerce transactions. Then it is possible to determine the degree of interactions in such transactions and the degree of sensitivity of messages used in the interactions.

(4) User dependency: Each participant may specify what information and which participants are important or how many resources (time, cost, computing power and security) are available for e-commerce transaction. So the user may select security level, specify the priority of heuristics, or leave this task to the automated option provided.

In this section, we reviewed requirements for adaptive secure e-commerce transaction from four different perspectives. For these identified requirements, we will further classify them into security classes (Section 3.1) and determine how certain heuristics dynamically adjust security levels (Section 3.2). This allows applications to execute with a specified degree of strong authentication while avoiding some performance bottlenecks often associated with these types of security procedures.

2.2. Architecture of ASE-COM System

The ASE-COM system is developed for an efficient and adaptive ecommunication transaction. The architecture (Fig. 1) shows four primary components: Cryptographic Class Library, Security Classifier, Message retriever, and Message Generator. The library provides a well-defined interface that can be embedded in application programs to the message generation and retrieval components. As a part of the interface, the security classifier dynamically provides a set of heuristics for reasonable mapping

between an e-commerce transaction database (DS-DB) and security classes in the security library. The adaptive decision on how to generate and deliver messages among the transaction participants is made according to four aspects described in Section 2.1. The message generator and the message retriever utilize the security classes in the cryptographic class library and the dynamic heuristics for the most appropriate security level at a certain situation for inter-party communication in an e-commerce transaction. The key to this flexibility and efficiency is that the protocol incorporates diverse cryptographic techniques and time functions.

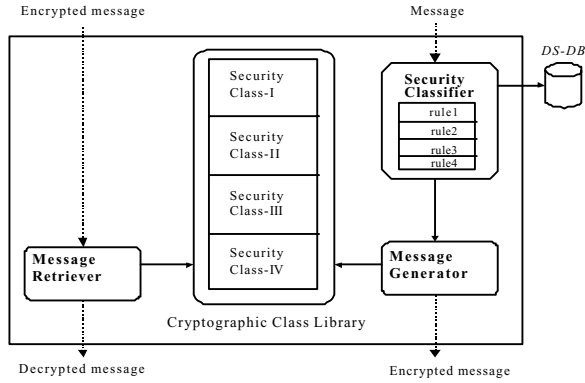


Fig. 1. Architecture of ASE-COM system

The ASE-COM system simplifies the complex e-commerce transaction by utilizing the protocol interface with pre-defined classes of common security messages and heuristics on when and how to generate and deliver the message. In addition, the system, which provides a rich set of communication mechanisms, can reduce the computational overhead required at runtime invocation and may support an efficient e-commerce transaction environment in terms of generating/delivering/verifying messages.

3. Design of Adaptive Secure Protocol

The security classes in the Cryptographic Class Library (Fig. 1) are formalized by prioritizing credential messages with their corresponding security levels. Thus, the class library provides a framework in selection of an appropriate security class for transaction message according to the degree of information sensitivity. The security classifier component contains a set of rules describing heuristics, which can dynamically map between prioritized credentials and computational environment.

3.1. Formalization of Security Class

We classify communication messages used among e-commerce transaction participants into four-security classes according to their security level. Four primary criteria of the classification of security levels are described in Section 2.1: (1) Domain dependent aspect

such as the protection degree of sensitive information, (2) System dependent aspect such as the cost measured by the computational speed performance of cryptographic techniques, (3) Network dependent aspect such as the message transmission rate between a sender and a receiver, (4) User dependent aspect which is an optional case for user-driven selection on the degree of message sensitivity. Table 1 describes the formal notations used in our protocol definition.

Table 1. Formal Notations for Adaptive Secure Protocol

X	Stands for the message,
Secret key	Stands for secret key encryption,
Public key	Stands for public key encryption,
Dynamic key	Stands for a key determined by a dynamic heuristic.
$RAND_{letter[number]}$	Represents a random number technique, where letter = {a, ..., z} and number = {1, 2, ..., N}
$K_{[A][B]1}$ and $K_{[A][B]2}$	Represents the first and second shared secret keys used in communication between A and B using DES, where A, B ∈ Participants
$K^{[A]}$	Stands for A's private key where A ∈ Participants
$K^{[A]-1}$	Stands for A's public key where A ∈ Participants
$MD = H(X)$	Represents that the value of MD (Message Digest) is produced by one-way hash function, H(), for input X
$\{X\}_K$	Represents the content of message, X, encrypted by the key K. For instance, $\{\{X\}_{K_{[A][B]1}}\}_{K_{[A][B]2}}$ stands for X encrypted under 3DES with $K_{[A][B]1}$ and $K_{[A][B]2}$.
$\{A B\}$	Represents the content of message containing A and B.
$S \rightarrow R [X]$	Represents the flow of a message X transmitted from S (sender) to R (receiver).

First, we prioritize cryptographic techniques and formalize their degree of security. The formalization is determined in terms of message confidentiality [21][23] and message integration [3][18], and origin authentication [8][9]. The message confidentiality can be described by secure and public key encryption techniques such as DES or 3DES. Our security levels are determined by the number of secret and public keys and the way to encrypt the keys. In our formula as shown below, as the number of keys is increased, the security level becomes higher but the computational overhead is increased.

(1) Message Confidentiality

$$\{X\}_{secret\ key\ 1} \leq \{\{X\}_{sec\ ret\ key\ 1}\}_{sec\ ret\ key\ 2} \leq \{\{\{X\}_{sec\ ret\ key\ 1}\}_{secret\ key\ 2}\}_{...sec\ ret\ key\ n}$$

∈ Secret key Encryption

$$\{X\}^{public\ key\ 1} \leq \{\{X\}^{public\ key\ 1}\}^{public\ key\ 2} \leq \{\{\{X\}^{public\ key\ 1}\}^{public\ key\ 2}\}^{...public\ key\ n}$$

∈ Public key Encryption

The public key encryption is more secure than secret key encryption because the secure key encryption shares a key among participants and the public key encryption has two different keys, private and public, to encrypt and decrypt the message.

Second, the message integration and the origin authentication use message digest techniques such as SHA-1. Multiple message digests ($Md_{dynamic}$) signed with a private key is stronger than a single message digest signed with a private key. However, An intruder can attack message digests ($Md_{dynamic}$) signed with a private key by tricking message digest [18]. Therefore, the original whole message signed with a private key is much stronger than multiple message digests ($Md_{dynamic}$) because it is not easy for an intruder to steal the whole original message without knowing a private key. We prioritize the strength of message integration and origin authentication as follow:

(2) *Message Integration and Origin Authentication*

$$\{MD\}^{private\ key} \leq \{MD_{dynamic}\} \leq \{X\}^{private\ key}$$

$$MD = H(X), X = Original\ Message$$

Based on (1) and (2), we formalize our four security classes. These security levels are prioritized according to the order of security level/performance from lowest/fastest to highest/slowest as follow.

$$\begin{aligned} & SL1 \left[\left\{ X \right\}_{secret\ key1} \mid \left\{ \left\{ MD \right\}^{private\ key} \right\}_{secret\ key2} \right] \leq \\ & SL2 \left[\left\{ \left\{ X \right\}_{secret\ key1} \right\}_{secret\ key2} \mid \left\{ \left\{ MD \right\}^{private\ key} \right\}_{secret\ key1} \right] \\ & \leq SL3 \left[\left\{ \left\{ \left\{ X \right\}^{private\ key} \right\}_{secret\ key1} \right\}_{secret\ key2} \right] \\ & \text{or} \left[\left\{ \left\{ MD_{dynamic} \right\}_{secret\ key1} \right\}_{secret\ key2} \right] \\ & \leq SL4 \left[\left\{ \left\{ X \right\}^{private\ key} \right\}^{public\ key} \right] \end{aligned}$$

Table 2. Description of security classes

Security Class	Cryptographic Algorithms	Encoding
SC-1	DES, SHA-1, Random number, RSA	$S : MD = H(X)$ $S \rightarrow R : \{X\}_{K[S][R]1}, \{ \{ MD \mid RAND_1 \}_{K^{[S]}} \}_{K[S][R]2}$ Latency
SC-2	DES, 3DES, SHA-1, Random number, RSA	$S : MD = H(X)$ $S \rightarrow R :$ $\{ \{ X \}_{K[S][R]1} \}_{K[S][R]2},$ $\{ \{ MD \mid RAND_1 \}_{K^{[S]}} \}$ $K[S][R]1$
SC-3	3DES, Random number, RSA	$S \rightarrow R : \{ \{ X \mid RAND_1 \}_{K^{[S]}} \}_{K[S][R]1} \}_{K[S][R]2}$
SC-4	Random number, RSA	$S \rightarrow R : \{ \{ X \mid RAND_1 \}_{K^{[S]}} \}_{K^{[R]-1}}$

Table 2 describes the details of our four security classes in terms of cryptographic algorithm, encoding, latency, and security level. The Security Class 1 (SC1) is the lowest security level in our Adaptive Secure Protocol and is defined in a combination of DES, SHA-1 and RSA. In the SC1, RSA is used for digital signature for digested message, one-way hash function SHA-1 for message digesting and DES for the encryption and decryption of message. This security class is similar to SET's shared key exchanging technique, except we use the two different keys in stead of one key. In the Security Class 2 (SC2), 3DES is additionally used for encrypting and decrypting message. Compared to SC1, the security level in the SC2 is increased and the computational overhead is also increased. In the Security Class 3 (SC3), private key is used to sign the message instead of signing the digested message. In the Security Class 4 (SC4), two shared secret keys, supported by Public key encryption (RSA), are used to encrypt message (shared secret keys) and to decrypt the message (receiver's private key). RSA requires the most expensive computational cost but it supports the highest security capabilities. Since the SC4 is restricted to the message sized less than 1K bytes, the performance of SC4 is relatively acceptable.

3.2. Making an Adjustment Decision

The security classifier component in our ASE-COM system supports the selection of the most appropriate security class in a given situation (Fig 1). The e-commerce transaction situations are considered to decide whether to increase, hold or decrease the security level for communication. The security level of the e-commerce transaction is adjusted according to the decision of the transaction state analysis (system and network level). The user can set the range of adjustable security, i.e., specify the minimum and maximum security.

The security classifier component contains a set of adaptive decision rules about security class. The rules are defined from four requirement perspectives described in Section 2.1. The first rule allows involvement of participants or domain expert to make a decision on a security level. A participant or domain expert may determine the threshold on sensitivity of message and maximum period time he/she wants to investigate for the services (generation, transmission, and retrieval). The adjustment decision about the security level is determined by the inputs from participants or domain experts. Unlike the first rule, the rest of rules consider an automated decision making situation for the adjustment of the security level. The second rule is when the message size or security level is higher than a certain threshold, it is partitioned into several sub-messages, include digital signatures, then encrypt them separately using message digest techniques. In this case, the receiver may have a responsibility to decrypt each of them and combine them in order. The third rule is for the security level adaptation according to the system computational capability (encryption and decryption). The fourth rule is for the security level adaptation by the network dependency (the highest average network delay, message sensitivity, and message size). A final decision on security class is made by Rule 5. The dynamic decision making (DDM) algorithm specified in Rule 5 makes a collective decision based on local decisions from four different perspectives (Rules 1-4). We now review the rules in detail.

Adaptive Decision Rule 1: This rule determines a security level based on the characteristics of domain dependent features or user driven selection. Specifically, the security class is determined according to the information sensitivity, the message size, the sender and the receiver of the message which the ecommerce domain or user specified.

Algorithm 1: User/Domain Driven Security Level

Input: M
Output: SL

$ST \leftarrow Sensitiveof(M)$

$MS = Sizeof(M)$

$Sender = Sender(M)$

$Receiver = Receiver(M)$

$SL \leftarrow Level - selection(ST, MS, Sender, Receiver)$

Adaptive Decision Rule 2: To apply this rule, there are two conditions to be satisfied: (1) the sensitivity level determined by Rule 1 is higher than 3 and (2) the message size is bigger than the threshold ($Size_{threshold}$). The rule describes a method, called iterative message digest, to partition a message into several sub-messages and encrypting them. The steps in the iterative message digest method are as follows: (1) produce the message digest of the message ($MS[S][R]$) between Sender (S) and Receiver (R) (2) retrieve the block size ($Block_{division}$) of the message based on the total number of message digests (MD_{total_num}) (3) retrieve blocks ($Block_n, n = 1, \dots, total_num$) and (4) sign the message digests generated from the blocks. (5) attach signed message digests ($MD_{dynamic}$). By generating multiple message digests, we can maintain the security level without much affecting the performance.

Algorithm 2: Adaptive Message Digest Function

Input: SL, M

Output: MD

if ($SL \geq 3$) and ($Sizeof(M) \geq Size_{threshold}$) then

(1) $MD = H(MS[S][R])$

(2) $Block_{division} = \left\lceil \frac{Sizeof(MS[S][R])}{MD_{total_num}} \right\rceil$

$1 \leq Block_{division} \leq Sizeof(MS[S][R]), MD_{total_num} \geq 1$

(3) $Block_N = \left\lceil \frac{Sizeof(MS[S][R])}{Block_{division}} \right\rceil, N = 1, \dots, total_num$

(4) $MD_{dynamic} = \{MD\}K^{[NA]} \mid \sum_{i=1}^{total_num} \{MD_i = H(Block_i)\}K^{[ASE]}$

$i = 1, \dots, total_num$

(5) $MS[S][R] = MS[S][R] + MD_{dynamic}$

(6) $ASE \rightarrow R: \{MS[S][R]\} RAND_{a[1]} \{ASE\}[R] \{K[ASE][R]\}^2$

Adaptive Decision Rule 3: This rule describes the system dependent aspect such as different costs of the communication and in particular, how they might change with different processors and to adapt the heuristics to adjust the security level accordingly to the cost. There are two algorithms to handle the encryption time (time to generate an encrypted message) and the retrieval times (the time to retrieve a decrypted message). Algorithm 3-1 receives M, the message to be generated, and SL determined by Rule 1 as input and returns TI, the message generation time extracted from pre-computed lookup table where n is the number of encoding method. Algorithm 3-2 computes the decoding time of the message to be transmitted.

The Parameter Sys specifies the computational capacity of participant systems for the message generation and verification. Refer to [12] for the details.

Algorithm 3-1: Estimated Time for Message Generation

Input: M, SL

Output: Tg

$Tg \leftarrow \prod_{i=1}^n Lookup_{encoding}(Sys, Sizeof(M), SL)$

Algorithm 3-2: Estimated Time for Message Verification

Input: M, SL

Output: Tv

$Tv \leftarrow \prod_{i=1}^n Lookup_{decoding}(Sys, Sizeof(M), SL)$

Adaptive Decision Rule 4: The message transmission times are the one-way times to transmit the encrypted message from sending to receiving machines. When the network traffic is high (measured by manipulating the average round trip time of the previous messages), the class adjustment rules are applied to adjust the network situation. Algorithm 4 estimates the message transmission time at the current network situation computed based on the round trip time of the previous message. There are two cases to be consider for the message transmission time: In case of the initial message, a sender uses initial estimated time Td' for the message transmission time. For subsequent messages, the sender estimates the transmission time Td" based on the round trip time (RTT) of previous messages. Algorithm 4 is designed followed by [10], [11], and [19]. We consider the message size as a variance (a is the ceiling ratio of the message to be delivered with at least 1). Therefore, depending on the size of message, the estimated message transmission time will be varied.

Algorithm 4: Estimated Time for Message Transmission

Input: M, M', M, A, D, g, h, E_i

Output: Td

(1) $Td' = \prod_{i=1}^n A_{initial} + E_i D_{initial}$

(2) $Err = RTT - A$
 $A \leftarrow A + gErr$
 $D \leftarrow D + h(|Err| - D)$
 $Td' = A + 4D$

(3) $Td = \begin{cases} Td' * \alpha, & \text{if Message = First Message} \\ Td'' * \alpha, & \text{Otherwise} \end{cases}$

$RTT : RTT(Round-Trip Time) Measurement of Each Message$

$A : An Estimator of the Average$

$D : Smoothed Mean Deviation$

$Err : Difference between the measured value$

$g : Gain for the Average$

$h : Gain for the Deviation$

$E_i : Exponential Backoff, E_i = \{2, 4, 8, 16, 32, 64, \dots\}, 1 \leq i \leq n$

$M' : Current Message To be Delivered$

$M : Previous Message Delivered$

$\alpha : \left\lceil \frac{Sizeof(M')}{Sizeof(M)} \right\rceil, \alpha \geq 1$

Adaptive Decision Rule 5: The security classifier component in our ASE-COM system supports to select the most appropriate security level for an e-commerce transaction in a given situation. The dynamic decision making function (DDM) adapts actual e-commerce transaction situations for the decision on whether to increase, hold or decrease the security level for communication. The selected security class represents a "best selection" at a given transaction situation to protect transaction information with an appropriate degree of encryption. Algorithm 5 describes the detailed adaptation behaviors of Adaptive Secure Protocol by employing the adaptive decision rules (Rules 1 - 4).

Algorithm 5: Dynamic Decision-Making Function (DDM)

Input: M

Output: Security Class

```

SL ← Rule1(M)
Tg ← Rule3 - 1(M, SL)
Tv ← Rule3 - 2(M, SL)
Td ← Rule4(M, SL)
ET ← Tg + Tv + Td
if (SL == 1) SC ← MSSC1
else if ((SL == 2) ∧ (ET > Tthreshold)) SC ← MSSC1
    else SC ← MSSC2
else if (SL == 3)
    if (Sizeof(M) ≤ Sizethreshold)
        if (ET > Tthreshold) SC ← MSSC2
        else SC ← MSSC3
    else if (ET > Tthreshold) SC ← MSSC2
    else SC ← Rule2(M, SC3)
else if (SL == 4) SC ← MSSC4
M : Current Message
SL : Level of Information Sensitivity
SC : Security Class
Tthreshold = Threshold of Message Delivery
Sizethreshold = Threshold of Message Size

```

4. Experimental Results

The prototype of the ASE-COM system is implemented under an Ultra10 SUN workstation with 64 MB physical memory and 100 clock tick scales in a second. The Adaptive Secure Protocol used in ASE-COM system is implemented with the RSAEURO cryptography library [1] and gnu c compiler. In our experiments, we measured the performance of the security classes and the effects of our dynamic decision rules.

4.1. Performance of Security Classes

We performed a set of experiments to measure the performance of security classes under conditions of different message size and security levels. Also, we measured the optimal size of message and total computing time taken for en/decryption in each security class. Table 3 shows the performance of four security classes applied to the secure message transaction occurred in the ASE-COM system. The performance of security classes seems to be proportional to the level of security classes and the size of en/decrypted message.

However, the degraded performance of security classes seems to be much worse with respect to the message size. Especially, the performance of SC3 shows a significant performance falloff in encryption and decryption of a message as the message size increases. It is necessary to take full advantage of Rule 2 (Adaptive Message Digest) described in section 3.2 for lower computational time in SC3.

4.2. Effects of the Adaptive Decision Rules

We also analyzed effects of the dynamic adapting mechanism of our ASE-COM system. In order to measure the effects, three variables are considered: message size and computational time and network situations. To show the effects of dynamic decision in terms of message size, we first measure the performance of transactions occurred in the ACE-COM system when adaptive decision rules are applied to SC3. Dynamic message digests ($|MD_{dynamic}|$) varying from $|MD_{dynamic}|=2$ to $|MD_{dynamic}|=4$ are generated to model the parameter of message size in experiments. When adaptive decision rules are applied, the performance of Adaptive Secure Protocol in ASE-COM system (Fig. 2-b) is almost 100 times faster than that of SC3 without adaptive decision rules (Fig. 2-a) where the message size ranges from 8K to 64K. Fig. 2 demonstrates a remarkable performance improvement through the utilization of adaptive decision rule mapping between dynamic environmental factor (i.e., message size) and dynamic message digest mechanism. Note that the performance is slightly decreased as the number of message digests increases shown in Fig. 2-b. The reason is the computational overhead required for encrypting the increased message digests.

Second, we attempt to improve subsequent round trip time of a message transmission by applying the adaptive decision rules

(Rules 3 and 4). In a heavy network traffic situation, the level of security class for a message may be degraded. The performance of the Adaptive Secure Protocol under adaptive decision rules (Fig. 3-b) is almost 100 times faster than that of Adaptive Secure Protocol without adaptive decision rules (Fig. 3-a) when a heavy traffic situation occurs.

5. Conclusion

A prototype of the Adaptive Secure Protocol was implemented and a set of experiences was performed. The experimental results showed that the Adaptive Secure Protocol improved the interacting performance, while providing high quality of security service for desired e-commerce transactions. Our ASE-COM system with secure class concept and dynamic authentication heuristics seems to be a suitable protocol for adaptive secure processing and offers the ability to make a dynamic decision dealing with the tradeoff between security and performance. The proposed protocol can be used to resolve impending problems in e-commerce and has huge potential to penetrate into the Internet markets.

Table 3. Performance of Security Classes

Message Size (Bytes)	SC1		SC2		SC3		SC4	
	Generation (sec)	Verification (sec)	Generation (sec)	Verification (sec)	Generation (sec)	Verification (sec)	Generation (sec)	Verification (sec)
8	0.85	0.05	0.85	0.05	0.85	0.05	0.9	0.9
64	0.85	0.05	0.85	0.05	0.85	0.05	0.9	0.9
117	0.85	0.05	0.85	0.05	0.85	0.05	0.9	0.9
256	0.85	0.05	0.85	0.05	1.85	0.109	1.96	1.96
1K	0.85	0.05	0.85	0.5	7.43	0.43		
8K	0.87	0.07	0.89	0.1	59.54	3.53		
64K	0.99	0.19	1.11	0.31	476.31	28.20		
256K	1.43	0.63	1.9	1.1	1905.26	112.82		
1M	3.11	2.31	5	4.2	7621.06	451.30		
2M	5.37	4.57	9.15	8.35	15242.12	902.61		

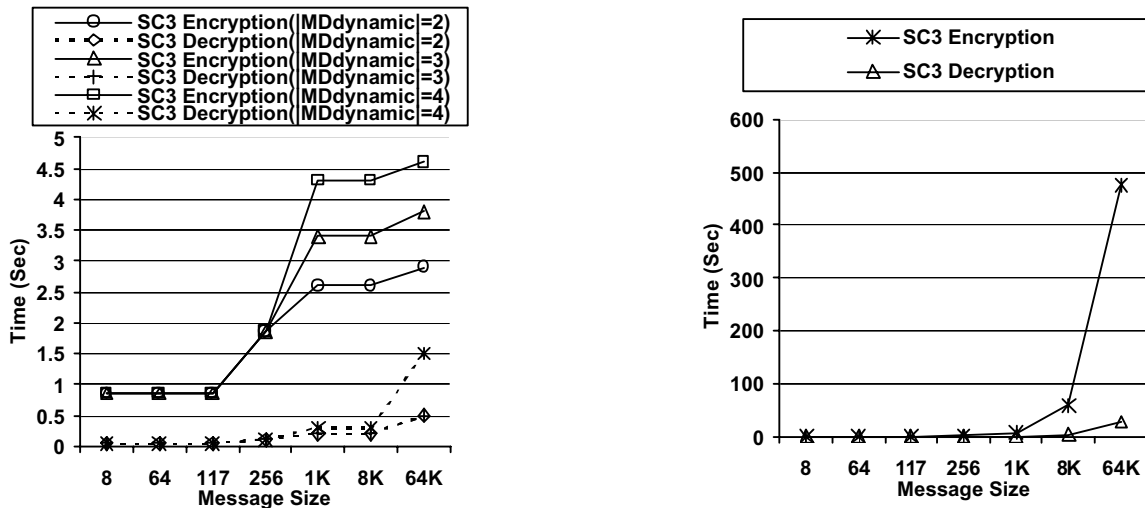


Fig. 2. (a) En/decryption execution time of SC3 without adaptive decision rules and (b) SC3 with adaptive decision rules

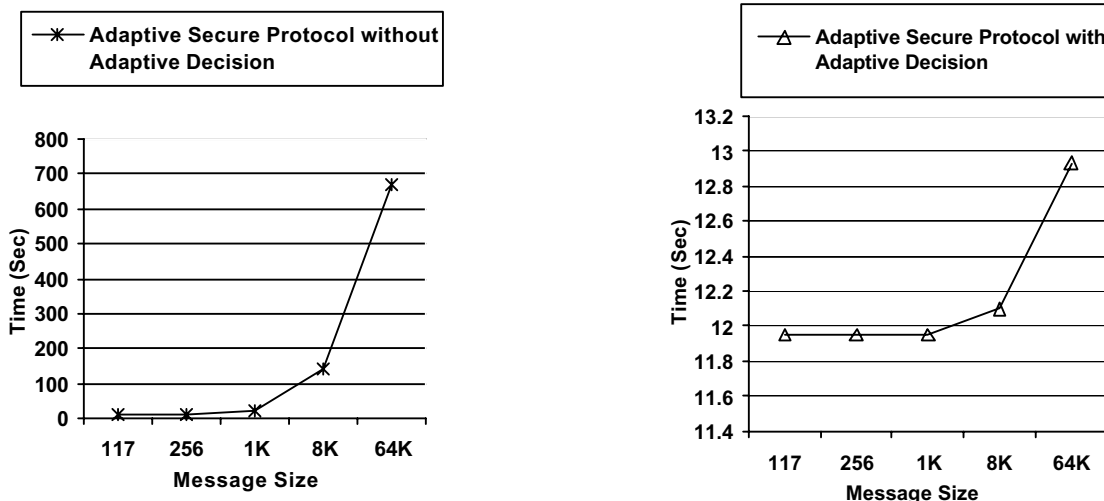


Fig. 3. (a) Adaptive Secure Protocol without adaptive decision rules and (b) Adaptive Secure Protocol with adaptive decision rules in a heavy network traffic situation

References

- [1] N. Barron, RSAEuro Technical Reference, RSAEuro Co., 3rd edition, Nov.,1996.
- [2] B. Blair, J. Boyer, "XFDL: creating electronic commerce transaction records using XML", Elsevier. *Computer Networks: the International Journal of Distributed Informatique*, vol.31, no.11-16, 1999, pp.1611-22.
- [3] S. Castano, M. Grazia Fugini, G. Martella, P. Samarati, 'Database Security,' Addison Wesley Publishing Company, 1994.
- [4] A. Dandalis and V. K. Prasanna, An Adaptive Cryptographic Engine for IPsec Architectures, *IEEE Symposium on Field-Programmable Custom Computing Machines, April 2000*.
- [5] V. Hassler, H. Biely, "Digital signature management", *Internet Research-Electronic Networking Applications & Policy*, vol.9, no.4, 1999, pp.262-71.
- [6] C. Holloway, "Controlling digital signature services using a smartcard", *Computers & Security*, vol.14, no.8, 1995, pp.681-90.
- [7] D. Ivan-Rosu and K. Schwan, Improving Protocol Performance by Dynamic Control of Communication Resources, Georgia Tech. Technical Report, GIT-CC-96-04
- [8] W. Ford, M. Baum, "Secure Electronic Commerce," Prentice Hall, Inc. 1997.
- [9] R. Housley, W. Ford, W. Polk, D. Solo, "Internet Public Key Infrastructure Part1: X.509 Certificate and CRL Profiles," *PKIX Working Group Internet Draft*, Dec. 1996
- [10] V. Jacobson, "Congestion Avoidance and Control," *Computer Communication Review*, vol. 18, no. 4, pp.314-29, Aug., 1988.
- [11] P. Kan and C. Patridge, "Improving Round-Trip Time Estimates in Reliable Transport Protocols," *Computer Communication Review*, vol. 17, no.5, pp.2-7, Aug., 1987.
- [12] Y. Lee, S. Tak, J. Stach, E. K. Park, An Adaptive Class based Notarial Protocol for Non-repudiation Services in Electronic Commerce, submitted for publication.
- [13] C. Liew, W. Ng, E. Lim, B. Tan, K. Ong, "Non-repudiation in an agent-based electronic commerce system", *Proceedings. Tenth International Workshop on Database and Expert Systems Applications. DEXA 99*. IEEE Comput. Soc. 1999, pp.864-8.
- [14] MasterCard and Visa, SET: Secure Electronic Transaction Specification – Book 1: Business Description, Version 1.0 May 31, 1997.
- [15] W. Mao, "On cryptographic techniques for online bankcard payment transactions using open networks", *Security Protocols. International Workshop Proceedings*. Springer-Verlag. 1997, pp.1-17.
- [16] M. Merz, F. Griffel, T. Tu, S. Muller-Wilken, H. Weinreich, M. Boger, W. Lamersdorf, "Supporting electronic commerce transactions with contracting services", *International Journal of Cooperative Information Systems*, vol.7, no.4, Dec. 1998, pp.249-74.
- [17] T. Pedersen, "Signing contracts and paying electronically", *Lectures on Data Security. Modern Cryptology in Theory and Practice*. Springer-Verlag. 1999, pp.134-57.
- [18] C. Pfleeger, 'Security in Computing,' Prentice Hall, 1997.
- [19] RFC 793, "Transmission Control Protocol Darpa Internet program Protocol Specification," Sep., 1991.
- [20] P. A. Schneck, K. Schwan, Dynamic authentication for high-performance networked applications Quality of Service, 1998. (IWQoS 98) 1998 Sixth International Workshop on QOS , pp.127 -136
- [21] J. Seberry, J. Pieprzyky, 'Cryptography : An Introduction to Computer Security,' Prentice Hall, 1989
- [22] J. Stach, E. K. Park, K. Makki, "Performance of an enhanced GSM protocol supporting non-repudiation of service", *IEE Computer Communications*, vol. 22, 1999, pp. 675-80.
- [23] D. Stinson, 'Cryptography Theory and Oractice,' CRC Press, 1995.
- [24] D. Steves, C. Edmondson-Yurkanan, M. Gouda, "Properties of secure transaction protocols", Elsevier. *Computer Networks & Isdn Systems*, vol.29, no.15, Nov. 1997, pp.1809-21.
- [25] M. Wright, "Securing Internet commerce", *Computer Fraud & Security*, Sept. 1996, pp.10-12.
- [26] M. Wichert, D. Ingham, S. Caughey, "Non-repudiation evidence generation for CORBA using XML", *Proceedings 15th Annual Computer Security Applications Conference (ACSAC'99)*. IEEE Comput. Soc. 1999, pp.320-7.
- [27] C. You, J. Zhou, K. Lam, "On the efficient implementation of fair non-repudiation", *Computer Communication Review*, vol.28, no.5, Oct. 1998, pp.50-60.
- [28] J. Zhou and D. Gollmann, "Evidence and Non-repudiation", *Journal of Network and Computer Applications*, 28(5), 1998, pp50-60.
- [29] J. Zhou, R. Deng, B. Feng, "Evolution of fair non-repudiation with TTP", *Information Security and Privacy. ACISP'99*. Proceedings. Springer-Verlag. 1999, pp.258-69.