2011

Teaching Secure Applications using Sequence Diagrams

Ajantha Herath
University of Bahrain, ahertah@itc.uob.bh

Suvineetha Herath
University of Bahrain, shertah@itc.uob.bh

Khalid Ahmed Al-Mutawah
University of Bahrain, khalid@itc.uob.edu.bh

Rohitha Goonatilake
Texas A&M International University, harag@tamiu.edu

TEACHING SECURE APPLICATIONS USING SEQUENCE DIAGRAMS

Ajantha Herath
University of Bahrain
ahertah@itc.uob.bh

Suvineetha Herath
University of Bahrain
shertah@itc.uob.bh

Khalid Ahmed Al-Mutawah
University of Bahrain
khalid@itc.uob.edu.bh

Rohitha Goonatilake
Texas A&M International University
harag@tamiu.edu

Hasan Yousif Kamal
University of Bahrain
hasank@itc.uob.bh

Amira Abdulrazaq
University of Bahrain
amira@itc.uob.bh

ABSTRACT

Authentication is the validation provided by the communicating entity's identity as the one that it claims to be. Integration of confidentiality, integrity and authentication into web applications is necessary to prevent unscrupulous attacks. For many years, we have been experimenting with methods for introducing important concepts related to secure transactions and improving undergraduate curricula and research experiences for Computer Science and Information Systems students. To achieve this goal, sequence diagrams which represent the progression of events over time are introduced to our students. This paper describes a learning module developed to help students understand authentication and integration of confidentiality, integrity and authentication into modeling web applications using sequence diagrams.

Key words: Digital transaction, Kerberos authentication, Sequence diagrams

Introduction

E-commerce transactions, electronic fund transfers and digital cash are transforming society into a cashless society. During the last two decades postal mail became e-mail, cash transactions became cashless, libraries became digital libraries, education is becoming online education, banking became online banking, news, TV and games became online entertainment.

As soon as a computer starts to share the resources available on the web or local network, it immediately becomes vulnerable to attacks or infiltration. Confidentiality guarantees privacy and no loss of information from the client or the server. It ensures that information is protected from unauthorized listening, reading or exposure. Integrity assures that the data or messages received are the same as those sent by an authorized person with no modifications of data, messages or impersonation. Confidentiality, integrity and authentication are achieved through the encryption of the message. In the case of providing integrity a message is transformed to a fixed size message digest using an encryption function or a specialized function. Authentication is implemented through encryption, signatures and certificates. Single, session or symmetric key cryptography, consists of a private key that is used for both encryption and decryption.

Public or asymmetric key cryptography, consists of a pair of public and private keys. The private key is kept secret whereas the public key is distributed for use by multiple parties. The RSA Algorithm is the most popular among asymmetric cryptosystems. A message encrypted with the public key can be decrypted only with the corresponding private key and it is nearly impossible to compute the private key from the available public key. This provides confidentiality as only the party with the private key can convert the message to plaintext. The merchant generates a pair of RSA private/public keys and the public key distributed to the consumers will be used during transactions.

Digital Signatures are used to provide authenticity. A message signed with the merchant's private key can be verified by any consumer who has access to merchant's public key. This provides confirmatory evidence that the signed message has not been tampered with by any unauthorized party. A public key certificate contains the identity of the certificate holder such as name and the digital signature of the certificate issuing authority. A public key certificate is used to validate the sender's identity. The certification authority attests that the public key indeed belongs to the sender [1, 2, 3].

In a transaction diagram, the major players are represented by nodes and directed arcs with labels presenting the messages transferred. In a sequence diagram the agents involved in the transaction are listed from left to right, messages are represented by directed arcs and time is presented from top to bottom. The transaction diagram could be easily transformed into a sequence diagram that will illustrate the snapshot of the sequence of events taking place represented on the horizontal axis, message transmissions and the particular time slot of the event taking place, shown on the vertical axis progressing from top to bottom [4,5].

The remainder of this paper is organized as follows. Section 2 of this paper provides a brief description of an online airline ticket purchase using a transaction diagram and Kerberos authentication using a sequence diagram. Section 3 presents the derivation of a sequence diagram from a more complex online transaction. Section 4 describes major threats that might be seen in an e-commerce transaction. It also, discusses five major security concepts that can be used to avoid those threats. Section 5 presents the integration of confidentiality into the transaction using SET protocol. Section 6 presents the integration of confidentiality, integrity and authentication to the transaction. Section 7 concludes the paper.

Authentication

Authentication is the validation provided by the communicating entity's identity as the one that it claims to be. Authentication helps identify the user. The consequence of the misrepresentation of a user can be impersonation and forgery. The Kerberos authentication service restricts access to authorized users all the time with single sign-on. It is secure and scalable to support a large number of clients and servers[2]. Kerberos ticket generation resembles social systems such as an airline system where a user purchases a ticket to receive the service. Figure 1 illustrates online airline ticket purchase.

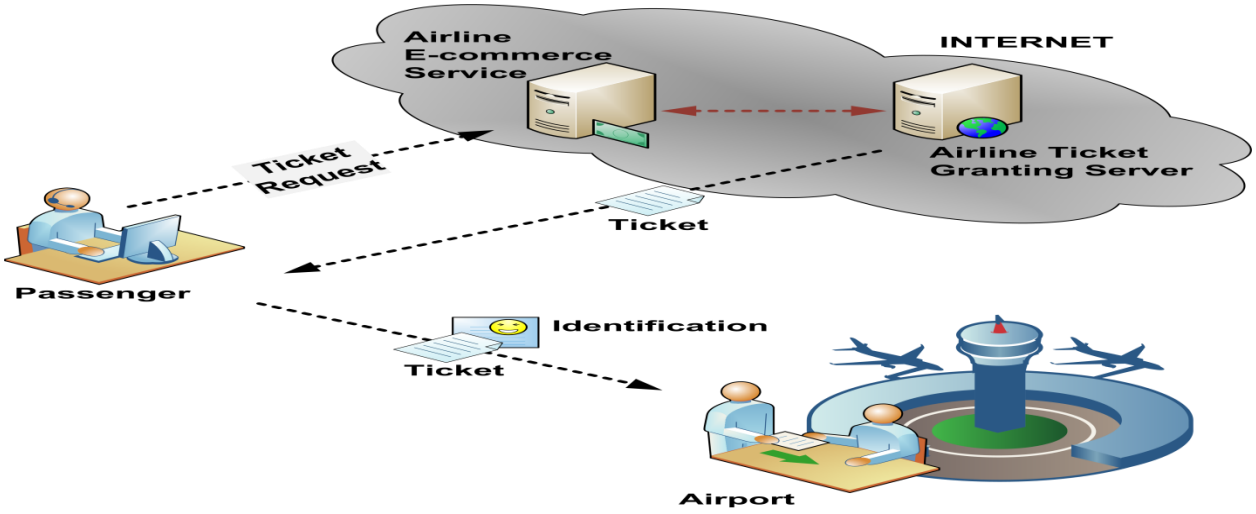

Figure 1: Airline Ticket Processing

The Kerberos authentication scheme consists of a client, Kerberos Authentication Server, Ticket Granting Service and a service provider. Kerberos communications are represented using a sequence diagram as shown in Figure 2. Encrypted keys and tickets help sharing symmetric keys.

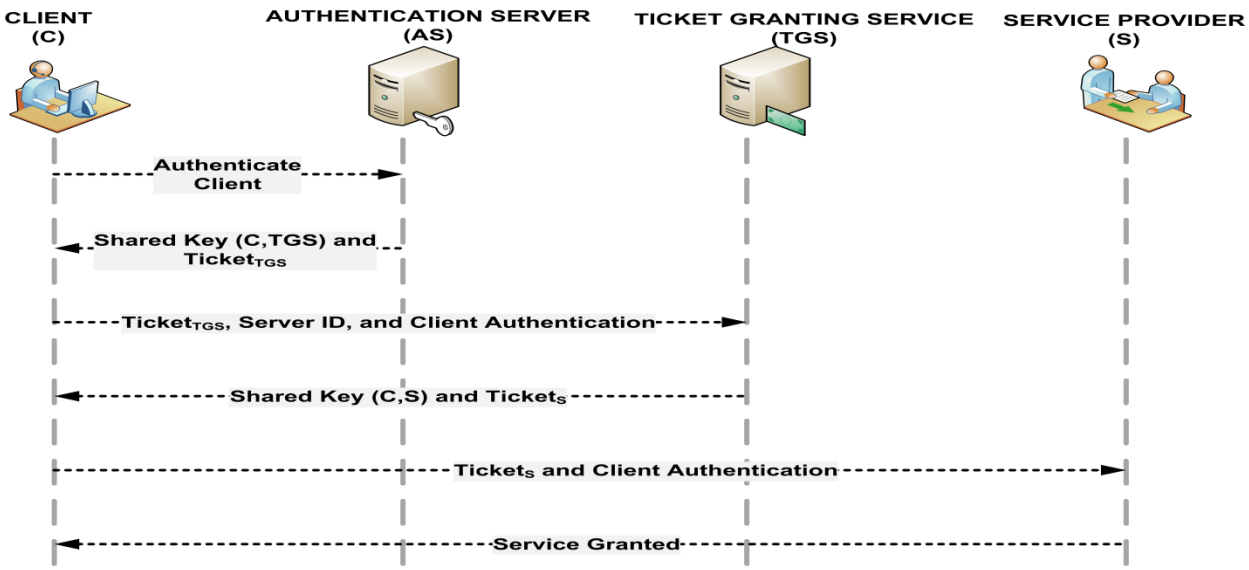

Figure 2: Kerberos Authentication

More detailed message exchanges are given below:

1) Obtain a Ticket Granting Ticket, TGT:

C -> AS:

$ID_C \| ID_{TGS} \| TS1$

AS -> C:

$E_{KC}[K_{C,TGS} \| ID_{TGS} \| Lifetime \| Ticket_{TGS}]$

Here $Ticket_{TGS} = E_{KTGS}[K_{C,TGS} \| ID_C \| AD_C \| ID_{TGS} \| TS2 \| Lifetime]$

2) Obtain Service Ticket, ST:

C -> TGS:

$ID_S \| Ticket_{TGS} \| AuthenticatorC$

TGS -> C:

$E_{KC,TGS}[K_{C,S} \| ID_S \| TS4 \| Ticket_S]$

Here $Ticket_S = E_{KS}[K_{C,S} \| ID_C \| AD_C \| ID_S \| TS4 \| Lifetime]$

$AuthenticatorC = E_{KC,TGS}[ID_C \| AD_C \| TS3]$

3) Obtain Service:

C -> S:

$Ticket_S \| Authenticator_C$

S -> C:

$E_{KC,S}[TS5 + 1]$

Figure 3 depicts these symbolic message communications using a sequence diagram.

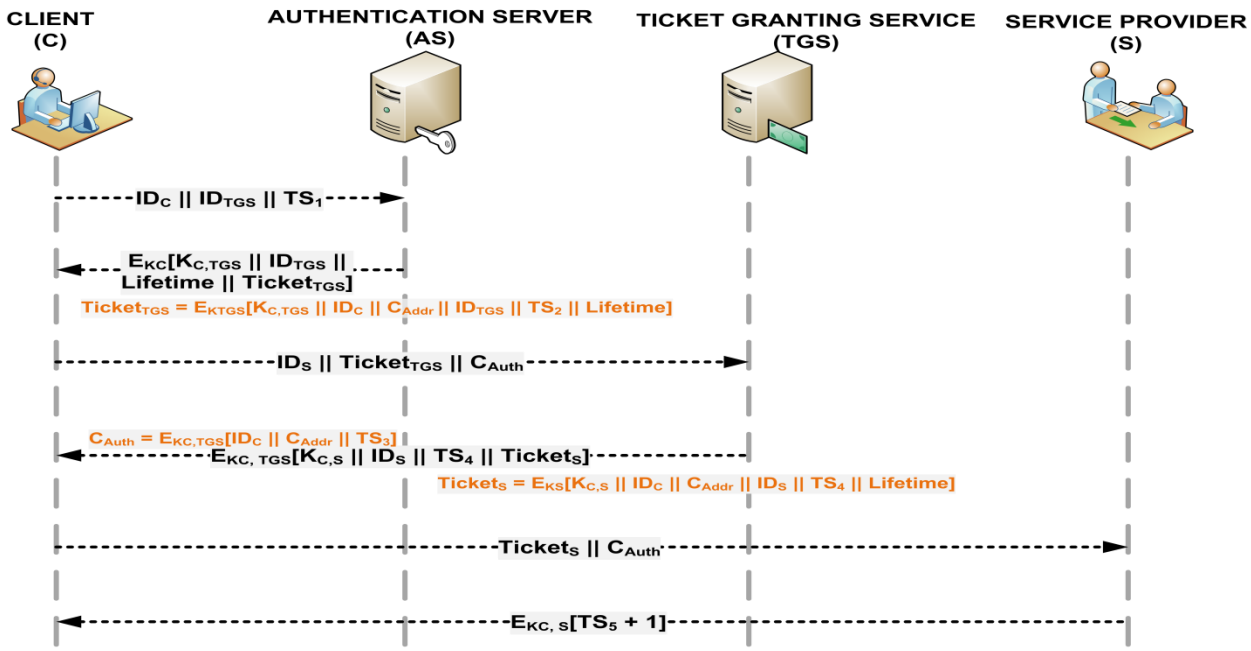

Figure 3: Kerberos Authentication with Symbolic Message Representation

Figure 3 shows the symbolic message representation of Kerberos.

ID_C = client's ID,
ID_{TGS} = Ticket Granting Server's ID,
TS1-5 = timestamps,
E_{KC} = encryption based on user's password,
$K_{C,TGS}$ = session key between client and ticket granting server,
Lifetime = lifetime of the ticket,
$Ticket_{TGS}$ = ticket to be used by client to access TGS,
AD_C = network address of client,
ID_S = Server's ID,
AuthenticatorC = Produced by client to validate ticket,
$Ticket_S$ = ticket used by client to access server S,
$K_{C,S}$ = session key between client and server.
AS: Kerberos Authentication Server,
TGS: Ticket Granting Server,
TGT: Ticket Granting Ticket,
ST: Service Ticket,
AR: Access Request

E-Cashless Transactions

The major players of electronic cashless transactions are clients, internet service providers, the merchant's servers, the client's and merchant's banks, warehouses and delivery services. The purchase of goods from the internet can be represented as a transaction diagram as shown in Figure 4. In this diagram each link is numbered to represent the order of the progression of events and communications. Label 1 represents the client sending the message to an internet service provider. Label 2 represents the ISP sending the message to the merchant's web server, located in the internet. Label 3 denotes the merchant's web server communications with the e-commerce server Label 4 shows the merchant's e-commerce server communications with the payment gateway and the database server. Label 5 depicts the payment gateway communications with the client's bank. Label 6 shows the payment gateway communications with the merchant's bank. Label 7 denotes the merchant's e-commerce server sending a message to the warehouse. Label 8 presents the warehouse sending goods to the delivery service. Label 9 shows the delivery service sending goods to the client.

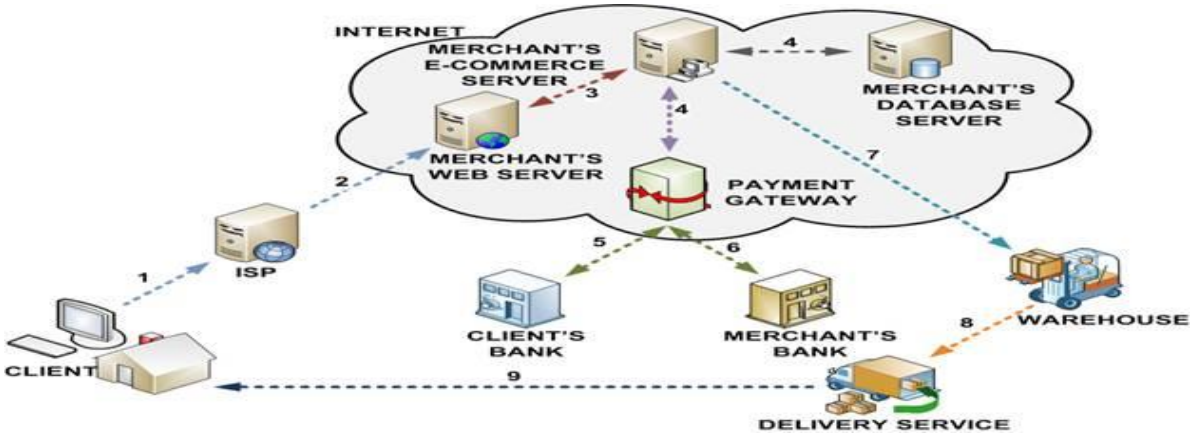

Figure 4 E-Cashless Transaction Diagram

Sequence Diagrams from Transactions

Figure 5 illustrates the sequence diagram for the transaction described in section 2 above. The client first sends payment and order information to the merchant's server via his or her internet service provider. Then the merchant's server sends payment information to the client's bank. The client's bank then sends payment to the merchant's bank. Payment confirmation will be issued by the merchant's bank to the merchant's server. Thereafter the payment and order confirmation will be sent to the client by the merchant's server via the ISP. The merchant's server sends the order issue request to the warehouse. The warehouse issues goods for delivery. The delivery service delivers the goods to the client.

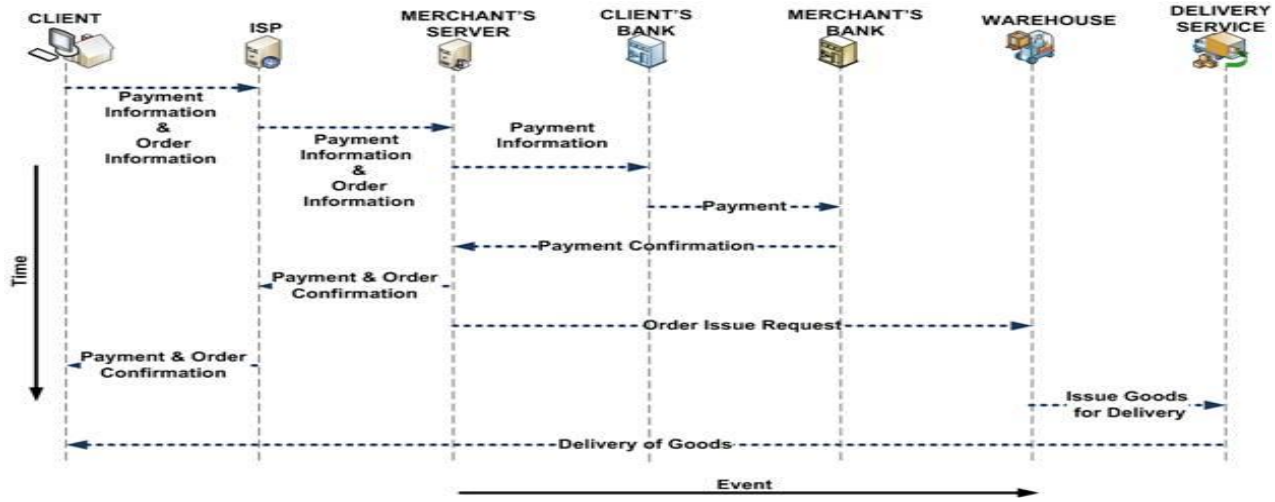

Figure 5 Sequence Diagram for the Transaction

Particularly, E-cashless transactions involve the client's and merchant's secure information such as credit/debit card numbers and private information. Most of the communications among the client, merchant and banks are done via the internet. Much of the communication, billing and payments are done by electronic message transfers. There is a higher possibility of stealing, losing, modifying, fabricating or repudiating information. Such systems and messages transmitted need extra protection from eavesdroppers. Many threats such as Denial of Service, DoS, Distributed Denial of Service, DDoS, Trojans, phishing, Bot networks, data theft, identity theft, credit card fraud, and spyware can be seen in these systems. These attacks might cause the loss of private information or revelation of sensitive information such as credit card numbers and social security numbers, misinterpretation of users, gaining unauthorized access to sensitive data, altering or replacing the data. Sniffing can take place at vulnerable points such as the ISP, the merchant's server, the client's bank, the merchant's bank or at the internet backbone [6]. Figure 5 also depicts an insecure e-commerce transaction. In this transaction anyone can read or modify the payment and

order information. An intruder can interrupt, modify or initiate the transaction. The client's bank information can be stolen by a third party.

Confidentiality in E-Cashless Transaction

Providing confidentiality is vital for this system. The transaction can be made secure by converting the plain text message to cipher text so that the holders of the keys can decrypt and read the messages. Common algorithms used to achieve this encryption and decryption goal are AES, DES with single symmetric keys and RSA with public/private asymmetric key pairs. Encryption will prevent strange third parties from obtaining the client's credit/ debit card numbers, passwords, pin numbers or personal details. But in e-transactions, there are many possibilities for an unauthorized third party to obtain this sensitive and private information and violate the privacy of the people, particularly in e-commerce service, the privacy of the consumer and the merchant. Thus, this e-commerce system needs to be assured that the information is not to be spread to unauthorized people in order to provide a genuine and reliable service. Symmetric encryption plays a key role in assuring the confidentiality of the data because, even if an unauthorized third party intercepts the message, usage of the unique session key, which can be accessed only by the two parties involved, prevents that person from viewing the message. Hence, the encryption of the information not only guarantees authentication, but also assures the confidentiality of the information. Figure 6 shows a transaction with confidentiality.

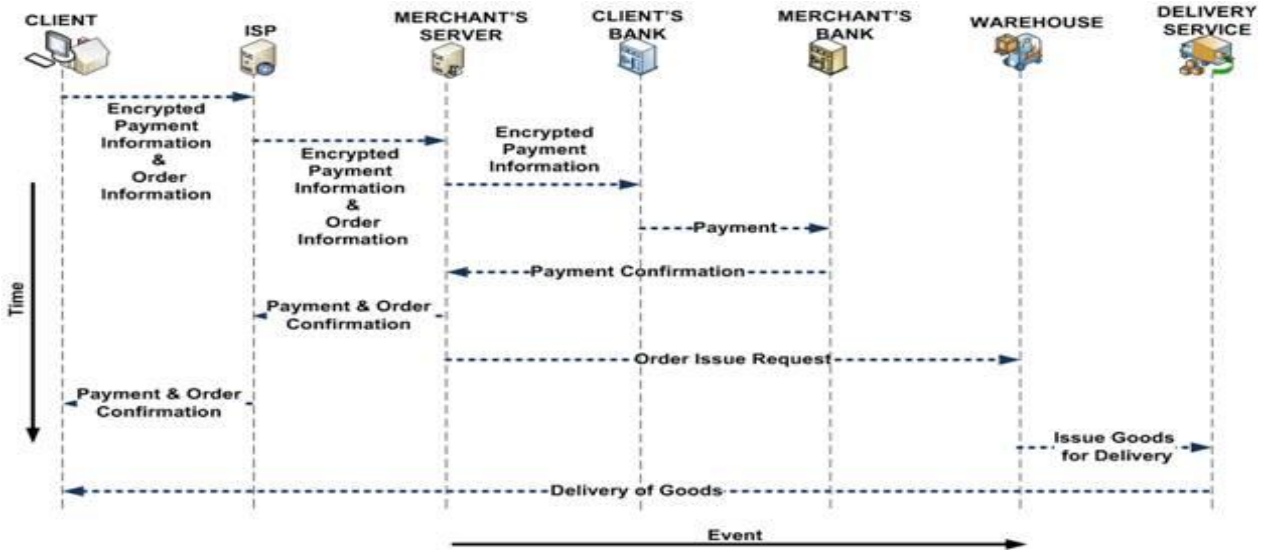

Figure 6 E-Cashless Transaction with Confidentiality

Consolidation of Integrity, Confidentiality and Authenticity

To make the e-cashless transaction secure, the data need to be received free from modification, destruction and repetition. When we consider the security of the electronic transaction, data integrity is another significant feature, because changing address, order information, or payment information may have possibly happened in this system. Therefore, to get the message free from modifications, the e-commerce system should provide protection of the message during transmission. This can be achieved by encryption and message digesting.

A unique message digest can be used to verify the integrity of the message. To do this, hash functions take in variable length input data and produce fixed length unique outputs that are considered the fingerprint of an input data/message. Thus, it is very likely that if two hashes are equal, the messages are the same. Specialized hash

functions are often used to verify the integrity of a message. To begin, the sender computes the hash of the message, concatenates the hash and the message, and sends it to the receiver. The receiver separates the hash from the message and then generates the hash of the message using the same hash function used by the sender. The integrity of the message is said to be preserved if the hash generated by sender is equal to the hash generated by the receiver. This implies that the message has not been altered or fabricated during the transmission from sender to receiver.

Encryption algorithms such as AES, DES could be used to generate message digests. In addition there are special purpose hash functions such as SHA and MD for this purpose. SHA is a message-digest algorithm developed by the National Institute of Standards and Technology and the National Security Agency. SHA is secure, but slower than MD5. MD5 produces the digest of 128 bits whereas SHA1 produces a 160-bit message digest and is resistant to brute force attacks. It is widely used for digital signature generation. Figure 7 shows how authenticity, confidentiality and integrity can be used in our example. It uses the encryption, message digest, digital signature and a digital certificate to ensure the authenticity, confidentiality and integrity of the order and payment information.

One of the most important aspects of the security of the transaction is authenticating that the suppliers and consumers are who they say they are and assure the trustworthiness of the sources they are exchanging. This is really important in cashless e-commerce transactions because the supplier and consumer never meet face to face. Authentication can be presented in different ways. Exchanging digital certificates helps the seller and buyer verify each other's identity so that each party knows who is on the other end of the transaction. The digital signature is another method to be certain that the data is indeed from a trusted party. In addition, symmetric encryption can also be used in certifying authenticity. In this way, the receiver of the information can make sure that the information that they received is sent by a trusted party, because the key that is used to encrypt and decrypt the information is shared only by the sender and the receiver.

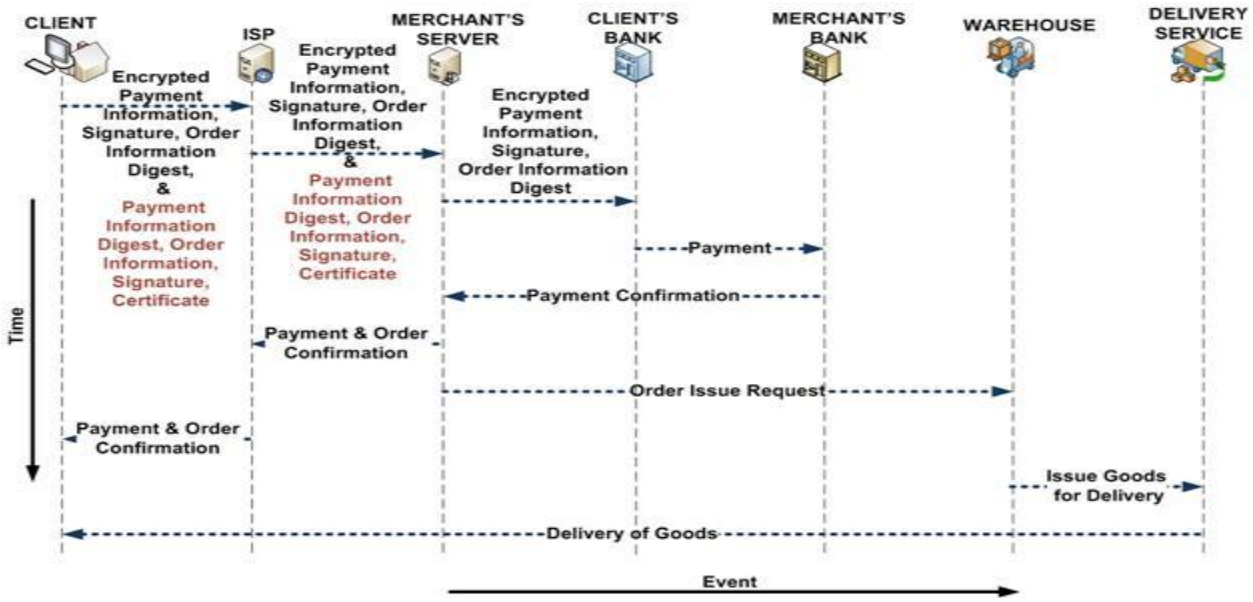

Figure 7 Secure E-cashless Transaction

Figure 8 illustrates integration of confidentiality, integrity and authentication using symbolic messages. In this figure 8 K_s represents the temporary symmetric key, PI, Payment Information, DS, Dual Signature, OIMD, Order Information message digest, K_{pubB} ,the Bank's public key-exchange key, PIMD, PI message digest, OI = Order Information and Certificate, Cardholder Certificate [1,2].

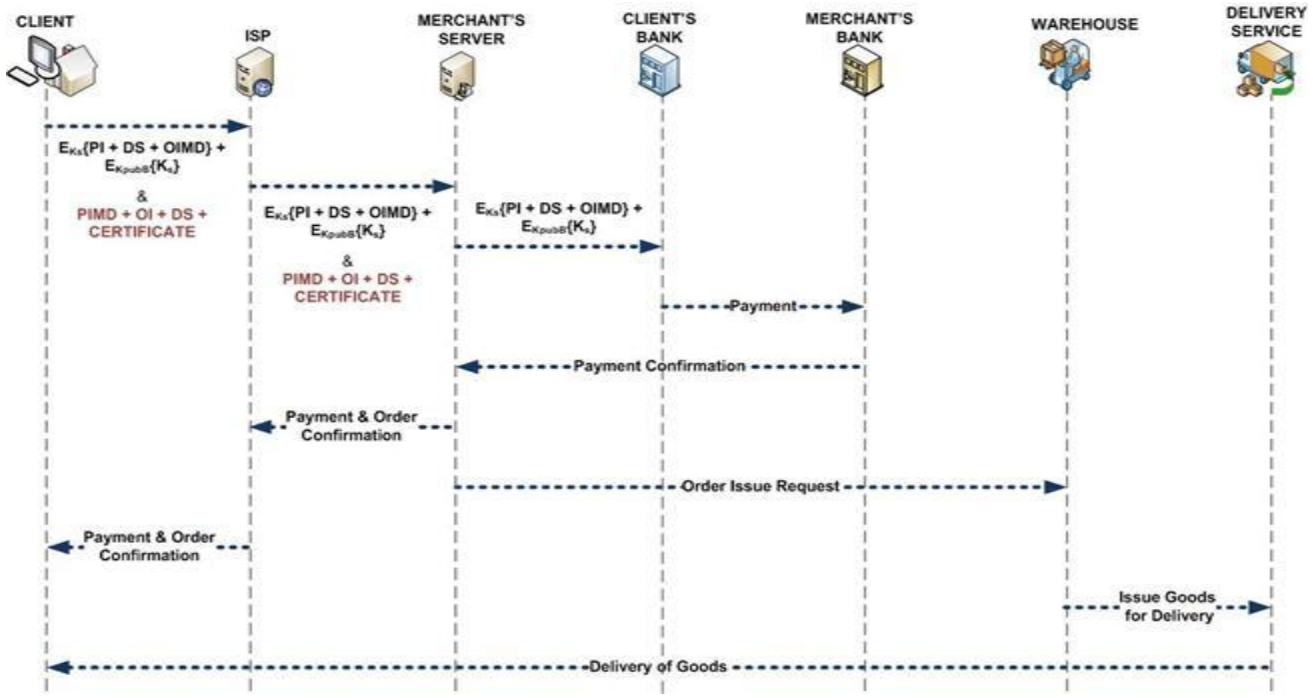

Figure 8 Secure Transaction with Symbolic Message Representation

The equation in Figure 8

E_{ks} {PI + DS + OIMD} + $E_{k\ pub\ B\{}$ {K_s} & PIMD +OI + DS + Certificate

summarizes the message generation in Secure Electronic Transaction protocol, an application of hashing and encryption algorithms in providing integrity, confidentiality and authentication for messages. This message consists of two parts: one for the client's bank and the other for the merchant. The request message part **{PI + DS + OIMD}** is encrypted by using the session key $\mathbf{K_s}$. The Digital Envelope consists of the session key encrypted by using the public key of the Bank $\mathbf{K_{pubB}}$. Secure transactions use both public and private key encryption methods for message exchange between the merchant and consumers. Light-weight-crypto algorithms such as Simplified-DES take an 8-bit block of plaintext and a 10-bit key as input to produce an 8-bit block of ciphertext.

The goal of dual signature generation and use is to send a message that is intended for two different recipients. Each recipient has access to the message, however only a part of the message can be read by each. In the case of SET protocol, the customer sends the order information (OI) and payment information (PI) using dual signature. The merchant can only see the OI and the bank can only access PI. Dual signature could be generated by using the order information and payment information. This information is securely delivered to the two recipients – the merchant and the bank. The digital envelope combines the speed of DES and the efficient key-management of RSA. The envelope and the encrypted message is sent to the recipient who decrypts the digital envelope using his private key to generate the symmetric key and then uses this symmetric key to regenerate the original message.

Conclusion

Internet users demand fast, reliable and secure transactions [11]. Also they want their information to be private and protected. Thus electronic cashless services rely upon the security provided in crypto systems provided for the transaction. To survive in a highly competitive world the service provider should be able to provide fast, reliable and secure service to their customers. Providing a safe and trustworthy environment among the merchant, the consumer, and their financial institutions is always essential. It is hard to determine the degree of safety and trustworthiness in electronic transactions. Introducing crypto system concepts to future designers, developers and students are not an easy task. This paper first presented how to integrate confidentiality, integrity and authentication using sequence

diagrams to students in computer science, information system and network security courses to make the task easier. Thereafter it presented the sequence diagram derivation from equations. Reading, interpreting and developing crypto equations and algorithms are important in Computer Security classes. This paper summarized mathematical representations used in security as well as sequence diagram to represent cryptographic algorithms, providing examples related to confidentiality and integrity and their combinations. The active learning module developed is easily adapted and effectively used in classrooms with senior undergraduate and graduate students in Computer Science, Engineering and Information Systems to teach other symmetric key algorithms and help students understand crypto system quickly.

References

1. IBM International Technical Support. Secure Electronic Transaction: Credit Card Payment on the Web in Theory and Practice. 1997. http://www.redbooks.ibm.com/redbooks/pdfs/sg244978.pdf
2. Stallings, Williams. "Cryptography and Network Security Principles and Practice Second Edition" Prentice Hall, 2007
3. K. Laudon, C.G. Traver, E-Commerce, Pearson Publishing, 2009
4. B. Bruegge, A. H. Dutoit Object-Oriented Software Engineering Using UML, Patterns, and Java, 3/E, Pearson Publishing, 2010
5. A. Herath and S. Herath, Case Studies for Learning Software Security Engineering, 9th International Conference on Humans and Computers, Aizu University, Japan, 2006
6. A. Herath, R. Gunathilake et al, Mathematical Modeling of Cyber Attacks: A Learning Module to Enhance Undergraduate Security Curricula, Journal for Computing Sciences in Colleges, Consortium for Computing Sciences in Colleges. South Central Region 18th Conference, 2007
7. Cox, B.Tygar, J.D. and Sirbu, M., "NetBill security and transaction protocol." Proceedings of 1st USENIX Workshop on Electronic Commerce, New York. 1995
8. iPAID. http://www.ipaid-insurance.com/. 2008
9. Mevinsky, G. and Neuman, B.C., "NetCash: a design for practical electronic currency on the Internet." Proceedings of 1st ACM Conference on Computation Communication and Security. 1993
10. Troncoso, Carmela. Danezis, George. Kosta, Eleni. Preneel, Bart. "PriPAYD: Privacy Friendly Pay-As-You-Drive Insurance." Workshop on Privacy in the Electronic Society. 2007
11. A.Herath et al, Learning Digital Cashless Applications with the Consolidation of Authenticity, Confidentiality and Integrity using Sequence Diagrams, ICCSEA Conference , Dubai , 2011