INSTITUTE OF INFORMATION TECHNOLOGY

Jahangirnagar University

জাহাঙ্গীরনগর বিশ্ববিদ্যালয়

IT-4259: Computer Network Security

for

4th Year 2nd Semester of B.Sc (Honors) in IT (4th Batch)

Lecture: 14

Web Security

Prepared by:

K M Akkas Ali
akkas_khan@yahoo.com, akkas@juniv.edu
Associate Professor
Institute of Information Technology (IIT)
Jahangirnagar University, Dhaka-1342

Prepared by: K M Akkas Ali, Assistant Prof

Objectives of this Lecture:

- ❖ To define some keywords related to web security.
- ❖ To define web security and its importance.
- ❖ To discuss some web security protocols such as SSL, S-HTTP, and SET.

Prepared by: K M Akkas Ali, Assistant Professor, IIT, JU

Web Security: An Introduction

- In a virtual world, there is always an element of doubt when sending or receiving sensitive information.
- We frequently read about website security problems in the newspaper almost weekly. Let us look at a few examples of what has already happened:
  - First, the home page of numerous organizations has been attacked and replaced by a new home page of the crackers' choosing. Sites that have been cracked include Yahoo, the U.S. Army, the CIA, NASA, the New York Times, etc.
  - Numerous sites have been brought down by denial-of-service attacks, in which the cracker floods the site with traffic, rendering it unable to respond to legitimate queries. Often the attack is mounted from a large number of machines that the cracker has already broken into (DDoS attacks). These attacks cost the attacked site thousands of dollars in lost business.
  - In 1999, a Swedish cracker broke into Microsoft's Hotmail Web site and created a mirror site that allowed anyone to type in the name of a Hotmail user and then read all of the person's current and archived e-mail.

Prepared by: K M Akkas Ali, Assistant Professor, IIT, JU

Web Security: An Introduction

- A 19-year-old Russian cracker, named Maxim, broke into an e-commerce website and stole 300,000 credit card numbers. Then he approached the site owners and told them that if they did not pay him $100,000, he would post all the credit card numbers to the Internet. They did not give in to his blackmail, and he indeed posted the credit card numbers, thereby causing a great damage to many innocent victims.

- A 23-year-old California student e-mailed a press release to a news agency falsely stating that the Emulex Corporation was going to post a large quarterly loss and that the C.E.O. was resigning immediately. Within hours, the company’s stock dropped by 60%, causing stockholders to lose over $2 billion. The perpetrator made a quarter of a million dollars by selling the stock short just before sending the announcement. While this event was not a website break-in, it is clear that putting such an announcement on the home page of any big corporation would have a similar effect.

- In 1994, from CITY Bank of USA, 11 million US dollar was hacked by breaking mainframe system of bank’s New York branch.

Prepared by: K M Akkas Ali, Assistant Professor, IIT, JU

Web Security: An Introduction

- In Washington DC, a 16-year-old juvenile, who is known on the Internet as "c0mrade", illegally accessed a total of 13 NASA computers. He obtained and downloaded proprietary software from NASA valued at approximately 1.7 million dollars. The software supported the physical environment of ISS (International Space Station), including control of the temperature and humidity within the living space. As a result of the intrusions and data theft, the NASA computer systems were shut down for 21 days in July 1999.

- In Israel, a group of hackers named "Team-Evil" targeted Israeli websites for cyber-vandalism. In 2006, the hackers managed to shut down about 750 Israeli websites and replaced with a screen displaying the message: "Hacked by Team-Evil Arab hackers. U KILL Palestine people, we KILL Israeli servers." The attacks have caused millions of shekels in damage.

Web Security: An Introduction

Let us examine some of the technical issues related to web security.

Example-1: Man-in-the-middle attack:

- Alice wants to visit Bob’s website.
  - ❑ She types Bob’s URL address into her browser and a few seconds later, a webpage appears. But is it Bob’s website? May be yes or may be no.
- Eve (an adversary) might be up to her old tricks. For example,
  - ❑ Eve might be intercepting all of Alice’s outgoing packets and examining them. When she captures an HTTP GET request headed to Bob’s website, she could go to Bob’s website herself to get the page, modify it as she wishes, and return the fake page to Alice.
- Eve could slash the prices at Bob’s e-store to make his goods look very attractive, thereby tricking Alice into sending her credit card number to Bob to buy some merchandise.

Prepared by: K M Akkas Ali, Assistant Professor, IIT, JU

Web Security: An Introduction

Example-2: DNS Spoofing:

- Tricking a DNS server into installing a false IP address is called DNS spoofing.

- For example, suppose Eve is able to crack the DNS system, maybe just the DNS cache at Alice's ISP and replaces Bob's IP address (say, 36.1.2.3) with her (Eve's) IP address (say, 42.9.9.9).

- The way it is supposed to work is illustrated in the figure below.

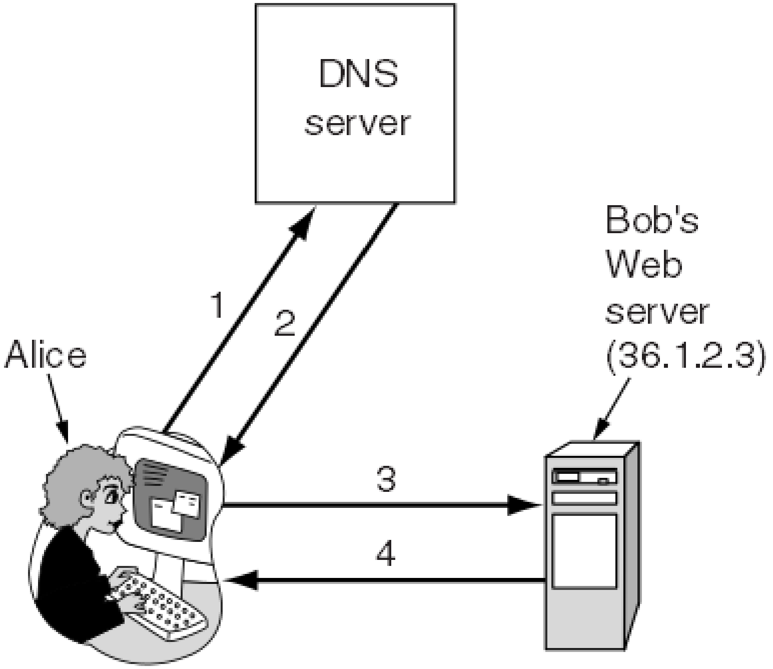
- Here

  (1) Alice asks DNS for Bob's IP address,

  (2) She gets it,

  (3) Alice asks Bob for his home page, and

  (4) She gets that, too.



1. Give me Bob's IP address
2. 36.1.2.3 (Bob's IP address)
3. GET index.html
4. Bob's home page

(a)

Figure: Normal situation

Prepared by: K M Akkas Ali, Assistant Professor, IIT, JU

Web Security: An Introduction

DNS Spoofing (continue…):

- ➢ After Eve has modified Bob’s DNS record to contain her own IP address instead of Bob’s, we get the situation of figure below.
  - ❑ Alice asks DNS for Bob’s IP address,
  - ❑ She gets Eve’s IP address. So all her traffic intended for Bob goes to Eve.
  - ❑ Alice asks Bob (but it is Eve’s) for his home page, and
  - ❑ She will get Eve’s home page instead of Bob’s.
  - ❑ Eve can now mount a man-in-the-middle attack without having to go to the trouble of tapping any phone lines. Instead, she has to break into a DNS server and change one record.
- ➢ A cache that holds an intentionally false IP address like this is called a poisoned cache.

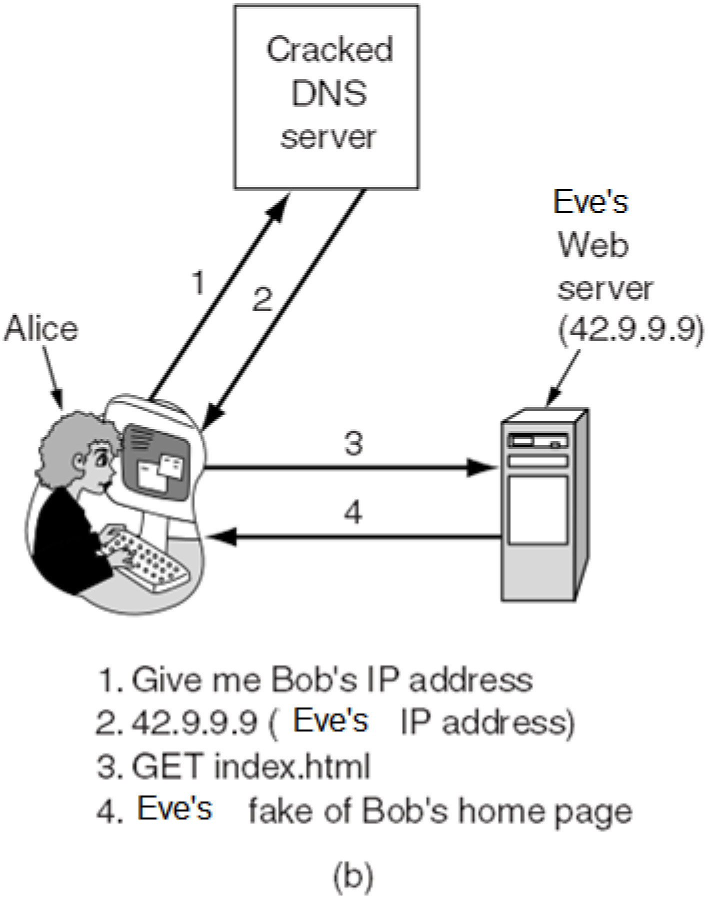

Cracked DNS server
Eve's Web server (42.9.9.9)
Alice
1
2
3
4
1. Give me Bob's IP address
2. 42.9.9.9 (Eve's IP address)
3. GET index.html
4. Eve's fake of Bob's home page
(b)

Figure: An attack based on breaking into DNS and modifying Bob’s record

Tools Available to Achieve Website Security:

- The following tools may be used to achieve the security of a website.

  1. Encryption
  2. Firewalls
  3. Security tools and protocols
  4. Security management
  5. Access control
  6. VPN
  7. Antivirus
  8. Authentication
  9. Proxy system
  10. Intrusion detection
  11. Tunneling

Prepared by: K M Akkas Ali, Assistant Professor, IIT, JU

What is Web Security?

- The web is where most of the intruders hang out now-a-days and do their dirty work. Web sites are unfortunately prone to security risks. And so are any networks to which web servers are connected.
- In a virtual world, there is always an element of doubt when sending or receiving sensitive information.
- Now-a-days, millions of people are spending their valuable time online- searching, surfing, shopping and connecting with friends and customers, coworkers and family etc.
- However, some companies got the idea of using web for financial transactions, such as purchasing merchandise by credit card, on-line banking, and electronic stock trading.

Prepared by: K M Akkas Ali, Assistant Professor, IIT, JU

What is Web Security (continue...)?

- The e-commerce business is all about making money and then finding ways to make more money. Of course, it is hard to make (more) money, when consumers don't feel safe executing a transaction on your Web site. Many types of threats can compromise the security of the business process. With the open exchange of information on the Internet, more security measures are needed to minimize vulnerability.
- So whether you are a merchant who wants to keep your shoppers safer, or a shopper looking for proven merchants, whether you're a high tech superstar or a newcomer to web, you have demand for establishing a secure connection to transmit critical information on the web. But how this secure connection can be achieved?
- Web security has become a serious issue for anyone connected to the Internet. Even if you don’t think you have anything worth protecting on your computer, it is still important that you keep it locked down. Your files are not the only thing at stake here. If someone gains access to your computer, it can be used for hacking into other computer, hiding the trail of the person who is actually doing it.

What is SSL?

- SSL, short for Secure Socket Layer, is a widely used security protocol developed in 1995 by Netscape Communication Corporation, the then-dominant browser vendor.
- This protocol is designed to provide security (e.g. data encryption, server authentication, and message integrity) for the transmission of private or sensitive data over the Internet.
- SSL encrypts the data (like credit cards numbers) and other personally identifiable information while it is being transmitted over the Internet which prevents the "bad guys" (unauthorized people) from stealing your information for malicious intent. The encryption is done in the background, without any interaction from the user, so there is no password to enter or remember.
- This protocol is used for establishing a secure connection between the server and the browser. It controls the communication between the SSL server and the browser.

Prepared by: K M Akkas Ali, Assistant Professor, IIT, JU

What is SSL (continue…)?

- SSL is called secured socket, because it uses a "secure socket" or port for transferring encrypted information between the server and the browser.
- SSL is a key to e-commerce security. Since its introduction, SSL has been the de facto standard for e-commerce transaction security and is likely to remain so into the future.
- SSL is used by all URLs that begin with http. SSL is used by all of Netscape’s browser products, as well as Microsoft’s Internet Explorer 3.0 or higher. In addition, it is built into products such as Apache and Internet Information Server. Most browsers and computers today can exchange secure transactions using this protocol across the Internet.
- One requirement for proper use of SSL is that the merchant’s Web server and the customer’s Web browser must use the same security system.

Prepared by: K M Akkas Ali, Assistant Professor, IIT, JU

Algorithms and Options SSL Supports:

- **SSL supports multiple cryptographic algorithms:**
  - ❑ The strongest one uses triple DES (Data Encryption Standard) with three separate keys for encryption and SHA-1 (Secure Hash Algorithm) for message integrity. This combination is relatively slow, so it is mostly used for banking and other applications in which the highest security is required.
  - ❑ For ordinary e-commerce applications, RC4 (Ron's Code 4) is used with a 128-bit key for encryption and MD5 (Message Digest 5) is used for message authentication.

- **SSL also supports a variety of different options that includes:**
  - ❑ presence or absence of compression,
  - ❑ cryptographic algorithms to be used, and
  - ❑ some matters relating to export restrictions on cryptography.

- The last option is mainly intended to make sure that serious cryptography is used only when both ends of the connection are in the United States.

Prepared by: K M Akkas Ali, Assistant Professor, IIT, JU

SSL Subprotocols:

- SSL consists of two subprotocols:
    - one for establishing a secure connection
    - other one for transmission of data using the secure connection.

How does SSL Work:

Establishing Secure Connection:

- SSL establishes a secure, negotiated client-server session in which URL of requested document, along with contents, is encrypted.
- Let us start out by seeing how secure connections are established. The SSL handshake consists of nine steps that authenticate the two parties and create a shared session key.
- The simplified version of the connection establishment subprotocol is shown in the figure below.

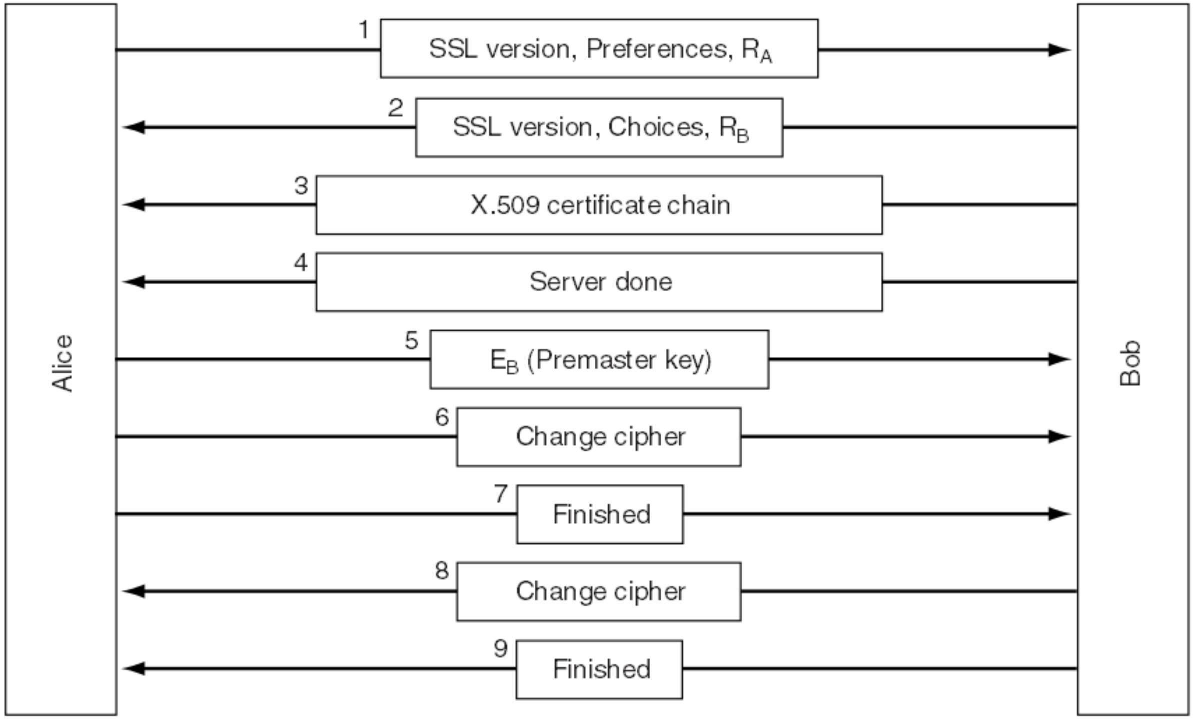


Figure: SSL connection establishment subprotocol

Prepared by: K M Akkas Ali, Assistant Professor, IIT, JU

How does SSL Work:

Establishing Secure Connection (continue…):

Alice’s turn-1:

- In message 1, Alice sends a request to Bob to establish a connection.
- The request specifies the capabilities of Alice which includes-
  - ❑ the version of SSL Alice has.
  - ❑ the data compression methods she supports.
  - ❑ the cryptographic algorithms she supports.
  - ❑ A nonce (a random number that can be used only once), R_A of Alice to be used later.

How does SSL Work:

Establishing Secure Connection (continue…):

Bob’s turn-1:

- ➢ In message 2, Bob replies to Alice’s request. The reply message contains-
  - ❑ the version of SSL Bob has.
  - ❑ the data compression methods he has chosen.
  - ❑ the cryptographic algorithms that Alice can support.
  - ❑ a session ID that identifies the connection.
  - ❑ A nonce R_B of Bob.
- ➢ **Note:**
  - ❑ The server is responsible for choosing the cryptographic algorithms and compression methods.
  - ❑ If there is no match between the sites supported by the client and server, then the server sends a “handshake failure” message and hangs up.

Prepared by: K M Akkas Ali, Assistant Professor, IIT, JU

How does SSL Work:

Establishing Secure Connection (continue…):

- ➢ Then in message 3, Bob sends a certificate containing his public key.
- ❑ If Bob is using certificate-based authentication, then he sends his signed X.509 certificate.
- ❑ If the certificate is signed by a non-root certifying authority, he then sends the chain of signed certificates that lead up to the primary CA.
- ➢ **Note:**
- ❑ All browsers, including Alice’s, come preloaded with about 100 public key certificates.
- ❑ When Bob sends his certificate, Alice will be able to verify Bob’s public key which indicates the authentication for Bob. At this point, Bob may request Alice for her certificate containing her public key to verify Alice.
- ➢ When Bob is done, he sends message 4 to tell Alice it is her turn.

Prepared by: K M Akkas Ali, Assistant Professor, IIT, JU

How does SSL Work:

Establishing Secure Connection (continue…):

Alice’s turn-2:

- In message 5, Alice responds by choosing a random 384-bit premaster key and sending it to Bob encrypted with Bob’s public key. The actual session key used for encrypting data is derived from the premaster key combined with both nonces in a complex way.
- **Note:**
  - ❑ If Bob has requested for Alice’s certificate containing her public key, Alice then returns her signed X.509 certificate.
  - ❑ If Alice has no certificate, she then sends a ""no certificate" alert. Then Bob may choose to abort at this point with a handshake failure, or continue onward.
- After message 5 has been received, both Alice and Bob are able to compute the session key. For this reason, Alice tells Bob to switch to the new cipher (message 6).
- When Alice is done, she sends message 7 to Bob to tell that she has finished with the establishment subprotocol.

Prepared by: K M Akkas Ali, Assistant Professor, IIT, JU

How does SSL Work:

Establishing Secure Connection (continue…):

Bob’s turn-2:

- After message 7 has been received, Bob computes the session key. For this reason, Bob tells Alice to switch to the new cipher (message 8).
- When Bob is done, she sends message 9 to Alice to acknowledge the finishing of establishment subprotocol.
- After that, both Alice and Bob switch into encrypted mode. Now they are ready to start communicating using the agreed-on symmetric cipher and session key.

Prepared by: K M Akkas Ali, Assistant Professor, IIT, JU

How does SSL Work:

Data Transmission using Established Secure Connection:

- After establishing a secure connection, a second subprotocol is used for actual transport, as shown in the figure below.

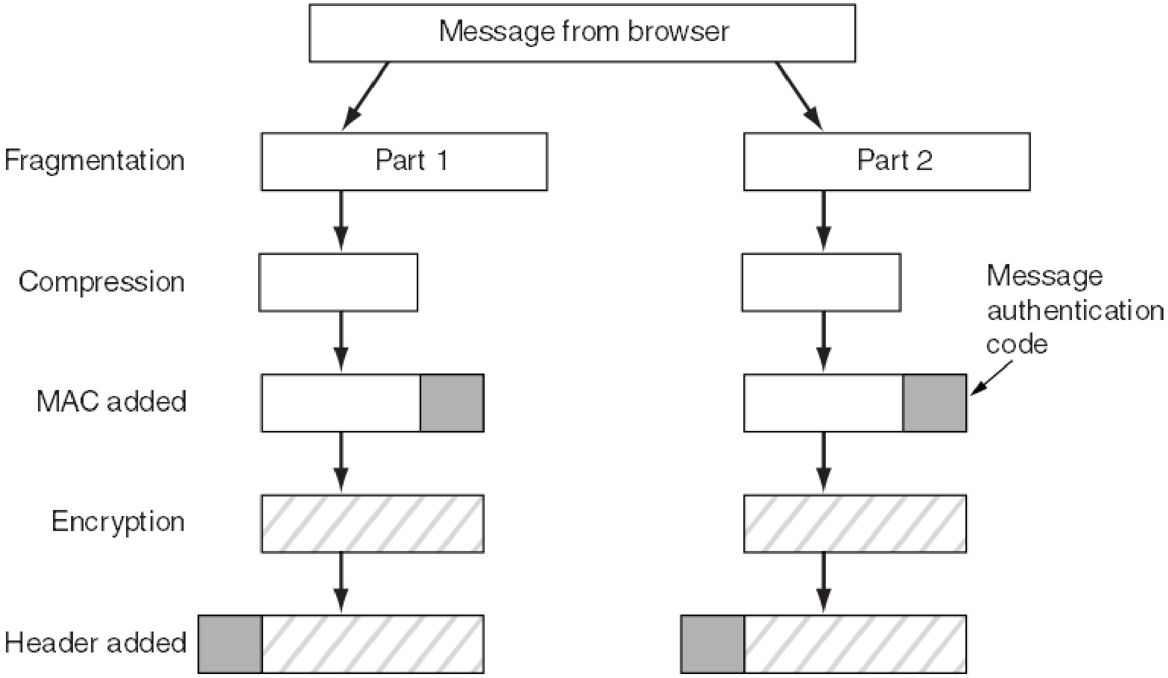


Figure: Data transmission using SSL connection

Prepared by: K M Akkas Ali, Assistant Professor, IIT, JU

How does SSL Work:

Data Transmission using Established Secure Connection (continue…):

- As seen in the picture, messages from the browser are first broken into units of up to 16 KB. If compression is enabled, each unit is then separately compressed.
- After that, a secret key derived from the two nonces and premaster key is concatenated with the compressed text and the result hashed with the agreed-on hashing algorithm (usually MD5). This hash is appended to each fragment as the MAC.
- The compressed fragment plus MAC is then encrypted with the agreed-on symmetric encryption algorithm.
- Finally, a fragment header is attached and the fragment is transmitted over the TCP connection.

Prepared by: K M Akkas Ali, Assistant Professor, IIT, JU

Basic Services Provided by SSL:

- SSL builds a secure connection between two sockets, including-

  1. Parameter negotiation between client and server.
  2. Mutual authentication of client and server.
  3. Secret communication.
  4. Data integrity protection.

- Therefore, SSL provides THREE basic services:

(1) Server authentication:

- ❑ Server authentication uses public-key cryptography to validate the server’s digital certificate and public key on the client’s machine.

(2) Client authentication:

- ❑ It is performed in the same way on the server machine. During authentication process, SSL allows client and server machines to jointly select an encryption algorithm which will be used for the secure connection. The key to this algorithm is transmitted using public-key cryptography, after which client and server may communicate using the secret key.

(3) Encrypted SSL connection.

Prepared by: K M Akkas Ali, Assistant Professor, IIT, JU

Merits and demerits of SSL:

Advantage of SSL:

- It ensures the secure transmission of credit card information over the internet.

Disadvantage of SSL:

- It is not a complete credit card payment method. For example, it cannot support on-line credit card authorization.

Prepared by: K M Akkas Ali, Assistant Professor, IIT, JU

Transport Layer Security (TLS):

- In 1996, Netscape Communications Corp. turned SSL over to IETF for standardization. The result was TLS (Transport Layer Security).
  - ❑ A URL associated with TLS begins with https.
  - ❑ TLS allows for encrypted communication to occur between browsers and servers.
  - ❑ It secures usernames, passwords, credit card information.

What is HTTP?

- Hypertext Transfer Protocol, abbreviated as HTTP, is a set of file transfer rules used on the World Wide Web.

- It is a “request-response” type protocol that defines communication between a web client (web browser, e.g. IE) and a HTTP server.

- HTTP allows Web browsers to submit information to Web servers as well as fetch Web pages from them.

  - A client is the end-user; the server is the web site. The client making a HTTP request—using a web browser, spider, or other end-user tool—is referred to as the user agent. The responding server—which stores or creates resources such as HTML files and images—is called the origin server. In between the user agent and origin server may be several intermediaries, such as proxies, gateways, and tunnels.

- Web browsers also can use other protocols such as FTP (file transfer protocol) for file transfer and SMTP (simple mail transfer protocol) for electronic mail.

Prepared by: K M Akkas Ali, Assistant Professor, IIT, JU

What is S-HTTP?

- S-HTTP, short for Secure-Hypertext Transfer Protocol, is a method of establishing a secure HTTP connection.
- It is an extension to HTTP that provides various security features such as client/server authentication. S-HTTP allows a client machine and a server machine to communicate securely using HTTP, to provide immediate transmission of secure data over the Internet.
- S-HTTP is syntactically identical to the http: scheme used for normal HTTP connections, but it signals the browser to use an added encryption layer of SSL/TLS to protect the traffic.
- This protocol supports only symmetric or private key cryptography, and therefore does not require digital certificates or public key.
- Secure HTTP is notated by the prefix HTTPS:// instead of HTTP://

Prepared by: K M Akkas Ali, Assistant Professor, IIT, JU

Difference between SSL and S-HTTP:

- Whereas SSL creates a secure connection between a client and a server, over which any amount of data can be sent securely, S-HTTP is designed to transmit individual messages securely.
- SSL and S-HTTP, therefore, can be seen as complementary rather than competing technologies. One can use S-HTTP with the SSL for increased protection.
- Both protocols have been approved by the Internet Engineering Task Force (IETF) as a standard.
- By convention, an SSL protected page (URLs that require an SSL connection) starts with https: instead of http: and there is a padlock icon at the bottom of the page.

Prepared by: K M Akkas Ali, Assistant Professor, IIT, JU

Secure Electronic Transaction (SET)

- The growth of the Internet over the past few years has been explosive. It is also changing its character from merely being a purveyor of information to being a complete transaction enabler. Thus, today a surfer can purchase a variety of goods on the Internet, as opposed to merely accessing information.

- However, what is impeding rapid growth of this business is the consumer perception of poor security on the Internet.

- Most payment methods revolve around the credit card, and consumers remain hesitant to reveal their card information on the Internet. Also, not surprisingly, credit card frauds on the Internet have registered a dramatic increase.

- To address these growing security concerns and pave the way for uninhibited growth of electronic commerce on the internet, the two leading bankcard associations **Visa International** and **MasterCard International** with the cooperation from Microsoft, Netscape, IBM and many other leading technology companies around the world developed a common standard to process card transactions on the Internet in 1996, called the Secure Electronic Transaction (SET) standard.

Prepared by: K M Akkas Ali, Assistant Professor, IIT, JU

Secure Electronic Transaction (SET) (continue…):

- The Secure Electronic Transaction, abbreviated as SET, is a recent protocol designed specifically to secure payment-card transactions over the Internet.

- As the name implies, SET is a standard which will ensure that credit card and associated payment order information travels safely and securely between the various involved parties on the Internet.

  - The SET protocol is designed to operate both in real time, as on the World Wide Web, and in a store-and-forward environment, such as e-mail.

  - Furthermore, as an open standard, SET is designed to allow consumers, merchants, and banking software companies to independently develop software for their respective clients and to have them interoperate successfully.

- The SET protocol involves four parties: the **cardholder**, the **merchant**, the **bank that issues the credit card**, and the **merchant's bank**.

Secure Electronic Transaction (SET) (continue…):

- ➢ Like other encrypting protocols, SET uses a combination of public and private key cryptography to establish involved parties' identity and to ensure payment data security.

- ➢ SET employs digital signatures to enable merchants to verify the identity of buyers. It also protects buyers by enabling their credit card number to be transferred directly to the credit card issuer for verification and billing without revealing the number to the merchant.

- ➢ However, in order for secure transactions to work, SET must possess the following qualities:

  - ❑ **Confidentiality**: others cannot eavesdrop on an exchange.
  - ❑ **Integrity**: the messages received are identical to the messages sent.
  - ❑ **Authenticity**: you are assured of the persons with whom you are making an exchange.
  - ❑ **Non-Repudiability**: none of the involved parties can deny that the exchange took place.

Prepared by: K M Akkas Ali, Assistant Professor, IIT, JU

Phases of SET Protocol:

SET protocol has four phases:

- **Initiation:**
  - ❑ First, the cardholder sends a purchase initiation request to the merchant for initializing the payment.
  - ❑ Then the merchant returns a response message to the cardholder.
- **Purchase:**
  - ❑ In the second phase, the cardholder sends the purchase order together with the payment instruction to the merchant.
- **Authorization:**
  - ❑ In the third phase, the merchant obtains the authorization from the issuer via the payment gateway.
- **Capture:**
  - ❑ Finally, the merchant requests a money transfer to its account.

A Sample SET Session:

- Before getting into details of SET, we shall take a simple example to describe how SET works from the consumer's perspective.

1. The consumer-
   - accesses the merchant's web site
   - goes through the various goods on display
   - selects what he or she wants to buy.
2. Perhaps there is a **virtual shopping cart** where he or she drops all the items to be purchased. At the end, the customer proceeds to the virtual checkout counter. A screen pops up giving details, including the cost of all the items the shopper is purchasing, plus taxes and shipping costs.
3. Then the screen asks for the payment method and the consumer chooses to pay through a credit card using SET.
4. Immediately, a special software on the consumer's PC called **Digital Wallet** is invoked, and it asks the customer to choose one credit card from the many he or she possesses.
5. The consumer chooses a card, and the electronic transaction using SET is underway. A few seconds later, there is a confirmation that this order has been processed.

Key participants in a SET Session:

Following are the key participants in processing online credit card payments :

Merchant:

- Merchant is a seller, who is connected to an acquirer bank.
- A merchant can process various credit cards through a single acquirer.
- To accept credit-card payments, a merchant must have a merchant account at the acquirer or acquiring bank.

Cardholder/ Customer:

- Cardholder is a registered holder of the credit card who is a buyer and has an account at the issuer or issuing bank.

Prepared by: K M Akkas Ali, Assistant Professor, IIT, JU

Key participants in a SET Session:

Issuer or issuing bank:

- It is the bank that issues the credit card to a cardholder and processes transactions.
- That means it is the bank from which the buyer obtained the credit card, and the credit-card association.

Acquirer or acquiring bank:

- The bank that serves as an “agent” to link a merchant to multiple issuers.
- That is it is the bank with which the merchant holds an account.

Key participants in a SET Session:

Credit Card Associations:

- They are nonprofit associations that set standards for issuing banks.
- Visa, MasterCard, Discover, American Express etc. are some credit card associations.
- A credit or debit card will use a merchant account affiliated with one or more traditional credit card associations.

Payment Gateway Service:

- The payment gateway is situated between the SET system and the financial network of the current credit card system for processing the credit card payment
- This is typically connected to the acquiring bank.

Prepared by: K M Akkas Ali, Assistant Professor, IIT, JU

How does SET Work?

- Figure below illustrates how the SET protocol coordinates the activities of the customer, merchant, merchant's bank, and card issuer.

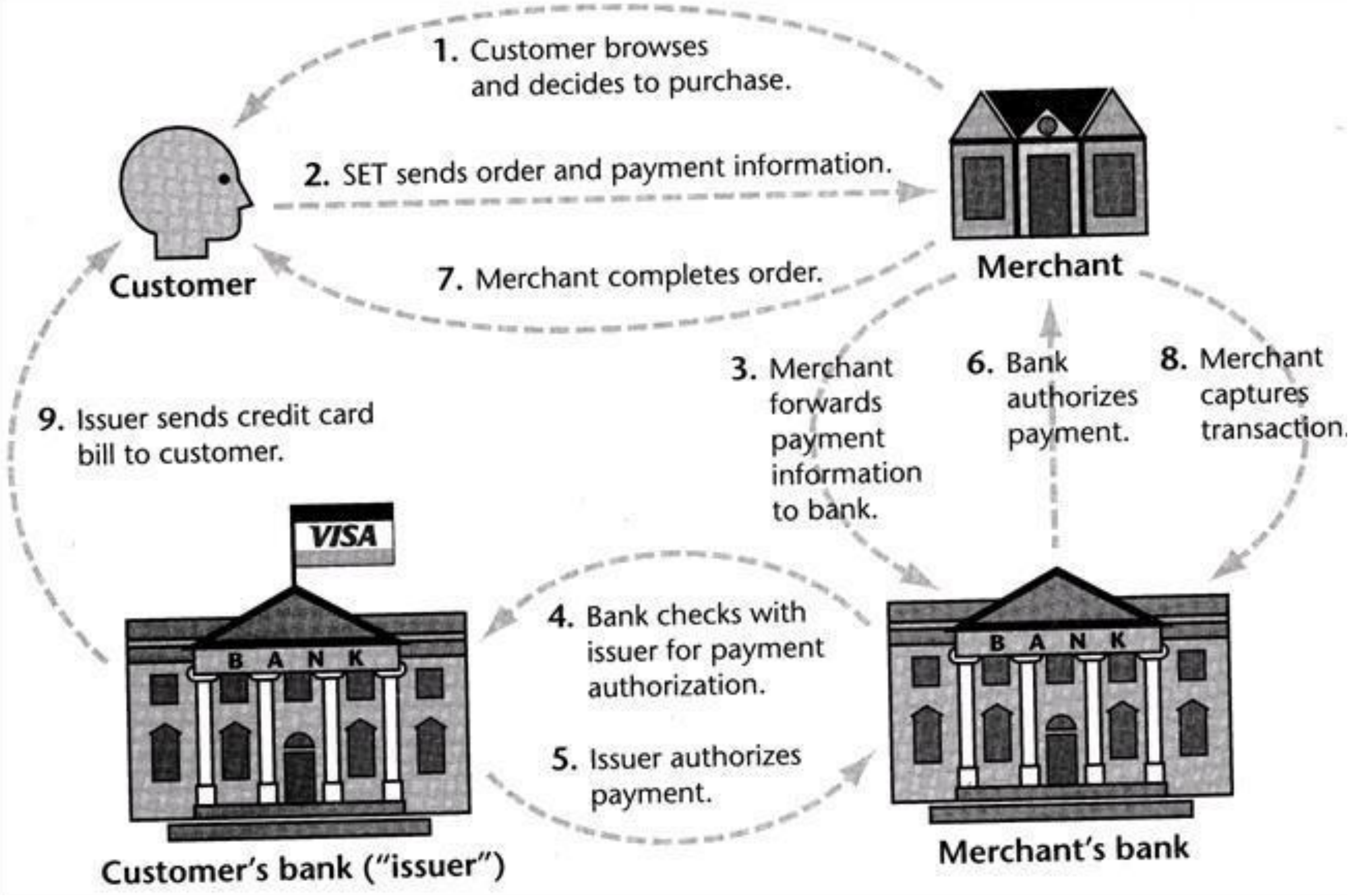

1. Customer browses and decides to purchase.
2. SET sends order and payment information.
7. Merchant completes order.
Customer
Merchant
3. Merchant forwards payment information to bank.
6. Bank authorizes payment.
8. Merchant captures transaction.
9. Issuer sends credit card bill to customer.
VISA
BANK
4. Bank checks with issuer for payment authorization.
5. Issuer authorizes payment.
BANK
Customer's bank ("issuer")
Merchant's bank

Figure: Activities of the customer, merchant, merchant's bank, and card issuer in SET

Prepared by: K M Akkas Ali, Assistant Professor, IIT, JU

How does SET Work?

1. **The customer initiates a purchase:**

    - ❑ The customer browses the merchant's web site.
    - ❑ He/she goes through the various goods and services on display and decides to buy something.
    - ❑ He/she selects items to buy.
    - ❑ Then, he/she fills out an order form containing the description of the merchandise and shipping information.

- ➢ This is all done before the SET protocol starts.
- ➢ The SET protocol begins when the user presses a "pay" button.
- ➢ The server now sends the customer's computer a message that launches SET software on his/her personal computer.

Prepared by: K M Akkas Ali, Assistant Professor, IIT, JU

How does SET Work (continue…)?

2. **The client's software sends the order and payment information:**

- ➢ The customer's SET software creates two messages.
  - ❑ The first message contains order information consisting of the total purchase price and the order number. The order information is encrypted using a random symmetric session key and packaged into a digital envelope using the merchant's public key.
  - ❑ The second message is payment information that consists of the customer's credit card number and bank information. The payment information is likewise encrypted, but this time using the merchant's bank's public key. This prevents the merchant from peeking at the credit card number or the bank from peeking at the order information.
- ➢ The software now computes a hash of the order and payment information jointly and signs it with the customer's private key. This creates a "dual signature" that allows both merchant and merchant's bank to validate the integrity of both messages without being able to read the part addressed to the other party.

Prepared by: K M Akkas Ali, Assistant Professor, IIT, JU

How does SET Work (continue...)?

3. The merchant passes payment information to the bank:

- SET software on the merchant's Web server generates an authorization request, forwarding the customer's payment information to a SET server maintained by the merchant's bank (or more likely, a "payment gateway" working on behalf of the bank.

- The merchant signs a hash of the authorization request with its private key in order to prove its identity to the bank. This request is encrypted with a new random session key and incorporated into a digital envelope using the bank's public key.

4. The bank checks the validity of the card:

- The bank decrypts the merchant's authorization request and verifies the merchant's identity.

- It then decrypts the customer's payment information and verifies the customer's identity.

- Now the merchant's bank needs to check with the customer's bank for authorization.

- It generates its own authorization request, signs it, and forwards it to the card issuer.

Prepared by: K M Akkas Ali, Assistant Professor, IIT, JU

How does SET Work (continue…)?

5. The card issuer authorizes and signs the charge slip:

- ➢ The customer's bank confirms the merchant's bank identity, decrypts the information, and checks the customers account. If the account is in good standing, the card issuer approves the authorization request by signing it and returning it to the merchant's bank.

6. The merchant's bank authorizes the transaction:

- ➢ The merchant's bank now authorizes the transaction and signs it, sending the OK back to the merchant's Web server.

7. The merchant's Web server completes the transaction:

- ➢ The merchant's Web server acknowledges that the card was approved by showing the customer a confirmation page and then enters the order into the merchant's order processing system.

- ➢ In due course, the merchant ships the goods or provides the service.

Prepared by: K M Akkas Ali, Assistant Professor, IIT, JU

How does SET Work (continue…)?

8. The merchant "captures" the transaction.

- ➢ In the final phase of a typical SET interaction, the merchant sends a "capture"' message to its bank. This confirms the purchase and causes the customer's credit card account to be charged. The merchant's checking account will be credited.

9. The card issuer sends a credit card bill to the customer:

- ➢ The SET charge appears on the customer's monthly statement, along with other charges.

Prepared by: K M Akkas Ali, Assistant Professor, IIT, JU

Merits and Demerits of SET:

Merits of SET:

- SET is Extremely secure.
- Fraud reduced since all parties are authenticated.
- Requires all parties to have certificates.
- So far has received lukewarm reception.
- 80 percent of SET activities are in Europe and Asian countries.

Demerits of SET:

- Not easy to implement.
- Not as inexpensive as expected.
- Expensive to integrated with legacy applications.
- Scalability is still in question.

Objectives of SET/ Important Goals of SET:

SET was developed with FOUR important goals in mind:

- **Confidentiality of payment:**
  - ❑ It means that as the payment is processed electronically, SET will enable payment security for all involved in the commerce. It provides confidentiality of payment information and enable confidentiality of order information that is transmitted along with the payment information.
- **Integrity of transmitted data:**
  - ❑ This means that the payment data will not be corrupted during transmission or during processing.
- **Authentication of the person using the card:**
  - ❑ It means that the cardholder is authentic. It also verifies that the merchant handling a sale can accept an authorized card via the acquiring bank.
- **Interoperability across network providers:**
  - ❑ This means a comprehensive way of making electronic payments over the Internet 24 hours a day, seven days a week, without delay. SET will also strive to achieve market acceptance on a global scale.

Prepared by: K M Akkas Ali, Assistant Professor, IIT, JU

SET Vs. SSL:

- SSL is a protocol for general-purpose secure message exchanges (encryption). A part of SSL is available on customers’ browsers.
  - It takes order, queries and other applications.
  - It does not protect against all security hazards.
  - It is mature, simple, and widely used.
- SET is tailored to the credit card payment to the merchants.
  - SET protocol hides the customer’s credit card information from merchants, and also hides the order information to banks, to protect privacy. This scheme is called **dual signature**.
  - SSL protocol may use a certificate, but there is no payment gateway. So, the merchants need to receive both the ordering information and credit card information, because the capturing process should be initiated by the merchants.
- SET involves interaction among credit card holders, merchants, issuing banks, payment processing organizations, and public key certificate authorities. So it is much more secure than SSL.
- SET is much more complex and comprehensive security protocol than SSL. SET is used very infrequently due to its complexity and the need for a special card reader by the user.
- SET is more costly to implement than SSL.

SSH:

- SSH stands for "Secure Shell".
- It is commonly used to connect your computer to another computer on the Internet.
- It is most often used by network administrators as a remote login / remote control way to manage their business servers.
- Example: your email administrator needs to reboot the company email server from his home, or your network administrator needs to reset your office password while she is away at a conference. He or she can use SSH.

Prepared by: K M Akkas Ali, Assistant Professor, IIT, JU

VPN:

- VPN stands for ‘Virtual Private Network’.
- VPN Allows remote users to securely access internal network via the Internet, using Point-to-Point Tunneling Protocol (PPTP)
- It refers to the secure way of connecting to a LAN using encryption through the Internet or another type of public network.
- It is called so, because the private communication flows over a public network, the Internet.
- The primary purpose of VPNs is to allow remote workers or companies with remote offices to share private data and network resources with a central location, head office or headquarters.
- VPN uses authentication to prevent unauthorized users from gaining access to the private data in the event that they attempt to intercept it. It can be used to send any kind of network traffic securely.
- VPN reduces network costs for companies and individuals because it avoid the need for physical leased lines to connect remote offices or users to a private internal network.
- With a VPN, users are able to transfer and exchange their private data safely and securely without the need for such physical lines.

Prepared by: K M Akkas Ali, Assistant Professor, IIT, JU

Tunneling:

- It is a technology that enables one network to send its data via another network's connections. Tunneling is when instead of sending a packet directly through the network you send it inside another (often encrypted) connection by means of encapsulation. Tunneling is a general term that refers to the encapsulation of one protocol within another.
- Tunneling works by encapsulating a network protocol within packets carried by the second network. For example, Microsoft's PPTP technology enables organizations to use the Internet to transmit data across a VPN. It does this by embedding its own network protocol within the TCP/IP packets carried by the Internet.
- Tunneling is a protocol that allows for the secure movement of data from one network to another. Tunneling involves allowing private network communications to be sent across a public network, such as the Internet, through a process called encapsulation. The encapsulation process allows for data packets to appear as though they are of a public nature to a public network when they are actually private data packets, allowing them to pass through unnoticed.

Prepared by: K M Akkas Ali, Assistant Professor, IIT, JU