

Ethical Hacking
Prof. Indranil Sengupta
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture – 34
Applications (Part I)

We shall now be looking at some of these security Applications. Say, earlier we had looked at some very specific techniques for carrying out some specific operations like how to do authentication, how to ensure message integrity, how to do encryption, but now we talk about some kind of end to end applications which are used pretty widely in the Internet.

(Refer Slide Time: 00:46)



Now, in this lecture which will be the Part I of the Applications, we shall be talking about something called secure socket layer or SSL and we shall see how SSL works. Now, SSL is important from the point of view of securing an organization or any network, because if you ensure or if you can provide with the mechanism so that people use this protocol SSL for communication, for sending confidential messages, then automatically there will be some kind encryption process that will be going in and any intruder or a hacker if it tries to break into the machine and if it breaks in even if then confidential information or secure information will not be leaked away.

So, this SSL is one such protocol which provides you with an optional added layer of security with respect to whatever message you are sending and receiving over TCP/IP.

(Refer Slide Time: 01:52)

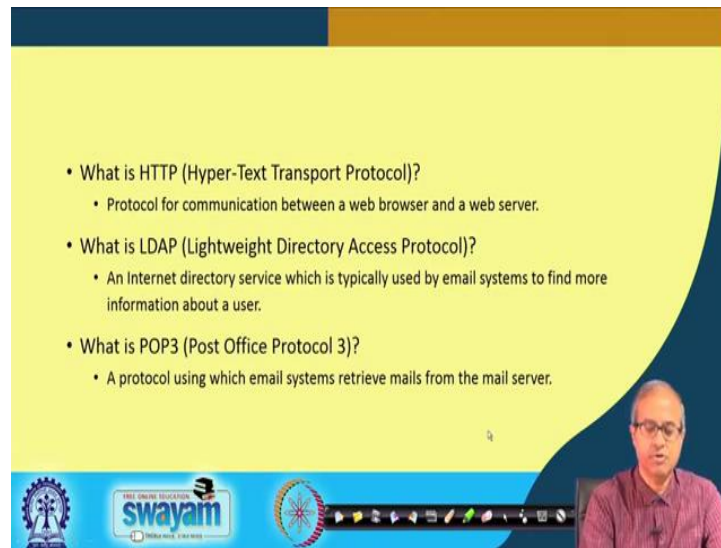
Secure Socket Layer (SSL)

- SSL was first used by Netscape.
 - To ensure security of data sent through HTTP, LDAP or POP3.
- Uses TCP to provide reliable end-to-end secure service.
- In general, SSL can be used for secure data transfer for any network service running over TCP/IP.

Let us see this, secure socket layer, SSL. Now, SSL was initially proposed and used by Netscape which is today known as Mozilla. That was the first instance where SSL was used. Subsequently this has become very popular. Now, many people use it for providing secure communication and secure transmission of data, ok.

Now, particularly this SSL was used with respect to three protocols HTTP, LDAP and POP3. We shall talk about these, because these were some of the most commonly used network traffic that were generated by users, right. And this SSL uses TCP, because it relies on TCP to provide reliable end to end service. On top of it provides some additional functionality so that additional level of security is provided, ok. So, SSL can be used, which runs on top of TCP/IP to develop any security application in general.

(Refer Slide Time: 03:08)

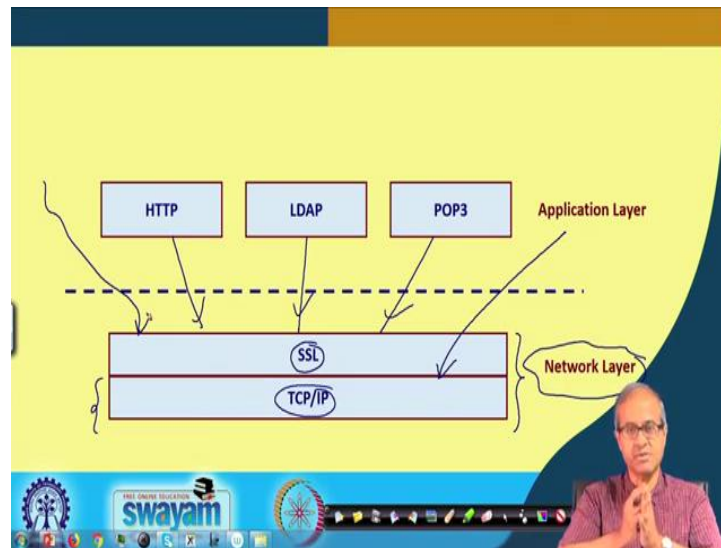


- What is HTTP (Hyper-Text Transport Protocol)?
 - Protocol for communication between a web browser and a web server.
- What is LDAP (Lightweight Directory Access Protocol)?
 - An Internet directory service which is typically used by email systems to find more information about a user.
- What is POP3 (Post Office Protocol 3)?
 - A protocol using which email systems retrieve mails from the mail server.

Let us see. Now, talking about these three protocols, as I said these are the most commonly used protocols. We generate maximum amount of traffic on the network. First is HTTP – Hyper-Text Transport Protocol which generates the requests and responses for all web applications, ok. So, here when you are looking at the Internet, browsing the Internet will be generating all the requests through this HTTP protocol, ok. So, this is the protocol to communicate between a web browser and a web server. It is a two-way communication.

And there is another very important component or typically generated this, called LDAP – Lightweight Directory Access Protocol. This is used an email and other services where information about some users and entities are stored in some directories to access them. You need LDAP messages to be send and received. And finally, for accessing electronic mails, POP3 is one of the protocols. POP is the short form for Post Office Protocol, version 3. It is used for retrieving mails from a email server, right. So, these are some examples. There are other examples also which use SSL.

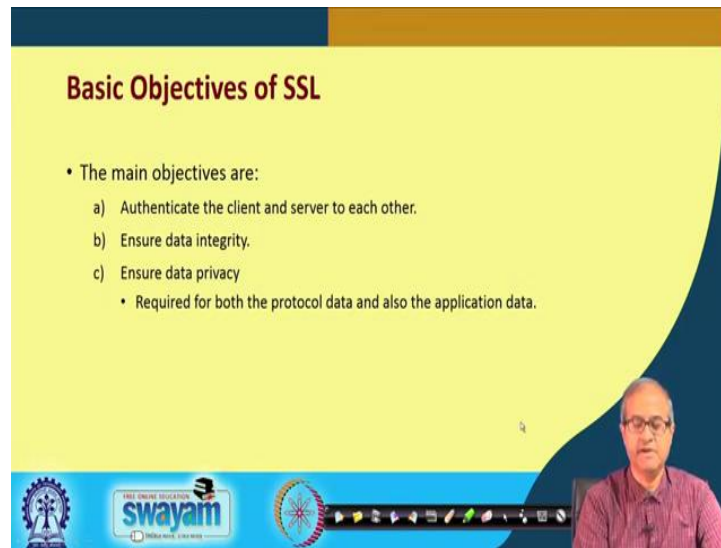
(Refer Slide Time: 04:36)



So, pictorially this is how things work. So, you see here you have TCP/IP. TCP/IP and the underlying physical layer is here that provides you with the basic network interface over which you can transmit messages and packets. Now, SSL sits on top of it. So, you can generically call them as network layer. Technically speaking this is actually a combination of network and transport layers, right, but you can say generically these are the two layers which provide transport of data over a network. That is why you can roughly call it a network layer and above that you can have various applications. So, I am showing only these three. There can be others also.

Now, these three I have shown, because they use SSL. They are known to use SSL, but there can be some other applications which may be directly using TCP/IP, but you can also develop some other applications which may be using SSL. So, SSL is a layer which sits on top of TCP and it is an optional layer. All applications do not use TCP, do not use this layer SSL. They can directly interact with TCP, if they want, fine.

(Refer Slide Time: 06:07)



Basic Objectives of SSL

- The main objectives are:
 - a) Authenticate the client and server to each other.
 - b) Ensure data integrity.
 - c) Ensure data privacy
 - Required for both the protocol data and also the application data.

The slide features a yellow background with a blue header and footer. The title 'Basic Objectives of SSL' is in bold black text. Below it, a bulleted list outlines the main objectives. A small video inset of a man is visible in the bottom right corner. The footer contains logos for 'swayam' and 'Digital India'.

Now, the basic objectives of this secure socket layer or SSL are several. First is authentication; the client and server, two parties are communicating over a network. They must authenticate each other. So, I know who is the other party. The other party also knows who I am. Then, ensure data integrity. So, it will also take care that. Data is not modified in transit. If there is a data modification, it will be immediately detected at the receiving end.

And data privacy also, if you want. So, encryption/decryption is also can be carried out as part of SSL. So, SSL also hides the data that is being communicated between the two parties. And this data privacy or this encryption is carried out not only for the application data that the user is generating, but also for the protocol data, because SSL also send some control messages. Those can also be encrypted so that an intruder does not know what kind of protocol is being used, what kind of encryption method has been used. Nothing is being disclosed in that case, fine.

(Refer Slide Time: 07:31)



SSL Architecture

- SSL consists of two layers of protocols:
 - a) SSL Record Protocol
 - Ensures data security and integrity.
 - b) Protocols required to establish SSL connection.
 - Three protocols used in this layer:
 - SSL Handshake Protocol
 - SSL ChangeCipherSpec Protocol
 - SSL Alert Protocol

The slide features a yellow background with a blue header and footer. The footer includes the Swayam logo and a navigation bar. A presenter is visible in the bottom right corner of the slide frame.

Talking about the SSL architecture, there are broadly two layers of protocols; one is called SSL record protocol and another layer, there are protocols required to establish the connection, ok. Now, SSL record protocol, all encryption and authentication hash function etc. those are handled by this layer. They take care of data security and data integrity that is the responsibility of the SSL record protocol. So, all the methods we had talked about earlier, they are handled by that particular layer.

And for establishing SSL connection that is the initial. So, whenever initially a connection is being set up here, the connection is a little different as compared with a normal TCP connection. For a TCP connection, see you recall, there was a three-way handshake through which a sender process and a receiver process can establish a connection between them.

But, for SSL such a connection is required of course, but in addition a number of other things are required, because here we are talking about data privacy. We are talking about authentication. We need hash functions. We need encryption algorithms; we need decryption algorithms. So, both the parties must agree on which algorithm to use for encryption, for hash and everything. So, it is during this initial in SSL connection phase all these things are decided by the two parties.

So, there are actually three protocols under this. SSL handshake protocol, SSL ChangeCipherSpec, as the name implies some ciphers or the algorithms for encryption

you can change here. You can specify which method to use and SSL alert, in case of some problems. These are the three kinds of different kinds of messages that can be exchanged in this second part.

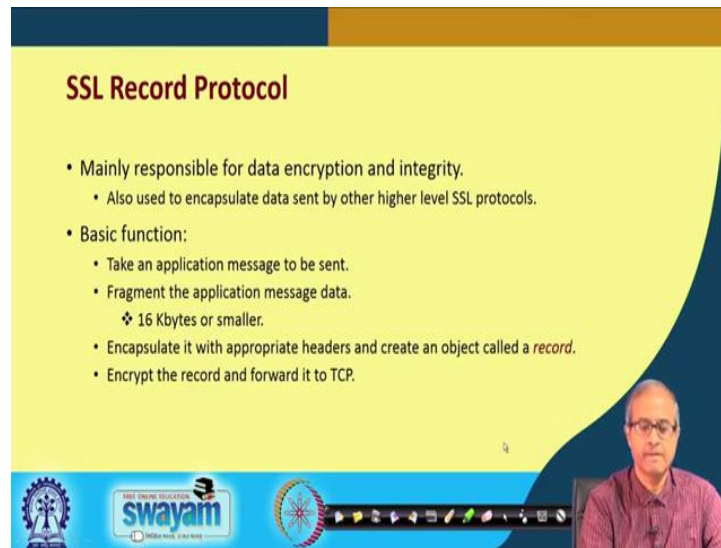
(Refer Slide Time: 10:02)



So, pictorially speaking the layers are created like this. So, earlier I had shown SSL as a single layer above TCP. What you see here is TCP which of course, is sitting above IP. And right above TCP you have first the SSL record protocol which is responsible for all the encryption and other security provisions which are provided. And on top of it you have this SSL handshake protocol, ChangeCipherSpec and alert protocols which generates messages which are required for establishing the connections.

And all of these are going through the record protocol so that they can all be encrypted and then send in addition you can have your applications. Now, applications do not interact with these three, they interact directly with the record protocol, ok. This is how the entire protocols track for SSL looks like.

(Refer Slide Time: 11:15)

A presentation slide titled "SSL Record Protocol" with a yellow background and a blue header. The slide lists the main responsibilities and basic functions of the protocol. A presenter is visible in the bottom right corner of the slide frame.

SSL Record Protocol

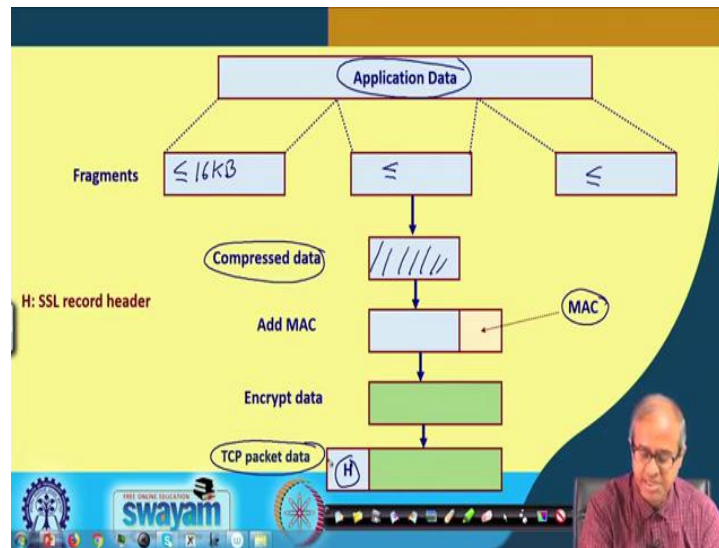
- Mainly responsible for data encryption and integrity.
 - Also used to encapsulate data sent by other higher level SSL protocols.
- Basic function:
 - Take an application message to be sent.
 - Fragment the application message data.
 - ❖ 16 Kbytes or smaller.
 - Encapsulate it with appropriate headers and create an object called a *record*.
 - Encrypt the record and forward it to TCP.

swayam

So, SSL record protocol as I have talked about, it is mainly responsible for two things. One is data encryption and other is data integrity, right. And other higher level SSL protocol like alert, ChangeCipherSpec etc. they can also be, they are also used to encapsulate data sent by those protocols. So, either to provide data encryption and integrity for application data or for SSL higher level protocols to encapsulate them and send.

Basic functions are it takes a message to be sent, first thing. Fragment the message into smaller chunks. The chunks for SSL are defined as 16 kilobytes. So, if the message is larger, it is broken up into 16 kilobyte, pieces and each of these are handled in certain way and encapsulate each of the headers and create a record, encrypt the record and forward it to TCP for delivery. The encrypted data is sent to TCP as a message. So, TCP does not know what it is. It is actually the encrypted data which is coming to TCP as a message which TCP sending to the other side, but before that all these things are happening; breaking up a larger message into smaller 16 kilobytes chunks, encrypting them and so on and so forth.

(Refer Slide Time: 12:56)



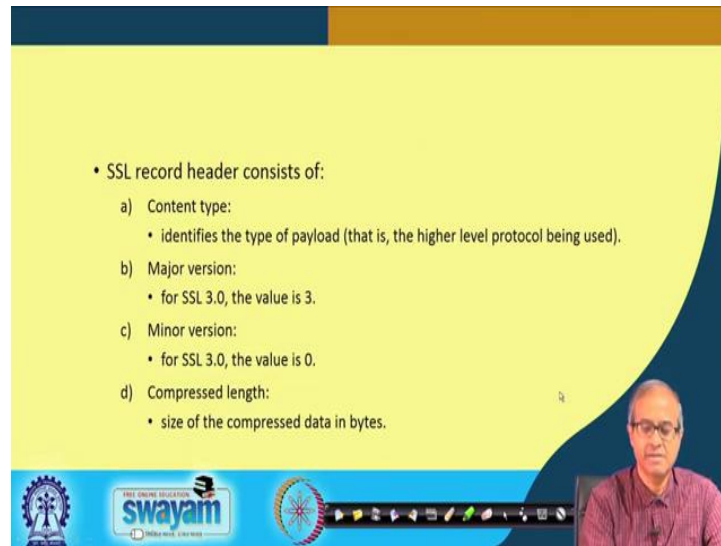
Let us look at it pictorially. This will make the thing clear. Suppose, some application is wanting to use SSL. This is your application data which can be long, larger than 16 kilobytes. So, first thing is that it is broken up into fragments. This is what SSL record protocol is doing. So, each of the fragments is maximum 16 kilobytes, less than or equal to. They are all like the less than equal to 16 kilobyte, less than equal to 16 kilobytes.

So, the steps that are carried out here in SSL, is this 16 kilobyte data whatever is received, so, each of them are being sent separately, processed separately. First there is a compression function. You do a data compression. If it is text data, you know that if you do compression it reduces in size significantly. So, you do compression. Your data gets compressed, maybe the size becomes less. Then, you generate some kind of hash. You generate a message authentication code. This can be keyed; this can be un-keyed. You can agree on exactly what method to follow.

So, with this compressed data you add the MAC. Then, you encrypt the whole thing. You, again you can decide which encryption method to use triple DES, AES or anything else. So, this green box, you see this is your encrypted data. Then, some SSL header is added. This is an SSL header which is added to this encrypted data and this is given to TCP. This is the data for TCP. So, TCP what it will do? TCP will add a TCP header before it before it can send it, ok.

So, this whole thing which comes, this comes to TCP as the basic data to be sent, ok. This is how SSL record protocol works. It breaks up larger data into smaller chunks. First it does a compression, compresses, then acts, then adds a message authentication code, encrypts the whole thing, then adds a header. H is the SSL record header. Then it gives it to TCP for delivery.

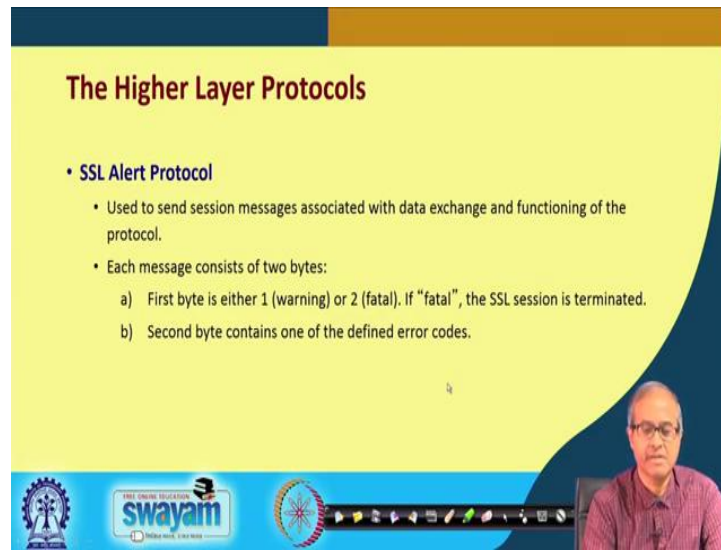
(Refer Slide Time: 15:42)



- SSL record header consists of:
 - a) Content type:
 - identifies the type of payload (that is, the higher level protocol being used).
 - b) Major version:
 - for SSL 3.0, the value is 3.
 - c) Minor version:
 - for SSL 3.0, the value is 0.
 - d) Compressed length:
 - size of the compressed data in bytes.

So, SSL record header consists of a number of fields, so, I am just showing you some of them. Content type, that what is the type of payload, is it application data or is it change cipher spec, some higher level protocol or is it SSL alert or what it is. Then the SSL version; SSL a version there are two categories of version; major version and minor version. So, SSL 3.0 the first number is the major version, the last number is the minor version; 3.0, 3.1 like that version grows right. And compress length, size of the compressed data in bytes that is also mentioned.

(Refer Slide Time: 16:29)



The Higher Layer Protocols

- **SSL Alert Protocol**
 - Used to send session messages associated with data exchange and functioning of the protocol.
 - Each message consists of two bytes:
 - a) First byte is either 1 (warning) or 2 (fatal). If "fatal", the SSL session is terminated.
 - b) Second byte contains one of the defined error codes.

At the bottom of the slide, there is a blue banner with the 'swayam' logo and the text 'swayam' and 'सुखी मन, सुखी मन'. To the right of the banner is a small video inset showing a man with glasses and a red shirt.

Talking about the higher layer protocols, the SSL alert protocols, this is used to send some messages associated with the data exchange and some errors or some warnings when the data are being sent. So, each message, these are very short messages. These are 2 byte messages.

Each message consists of two bytes. The first message is 1 or 2; 1 means it is a warning, 2 means it is a fatal error. If it is a error then this, then the SSL session will be terminated. It will not continue. The second byte will contain a code. That code will indicate what kind of warning or what kind of fatal error has occurred, ok. This is the task of SSL alert protocol. It alerts the other side.

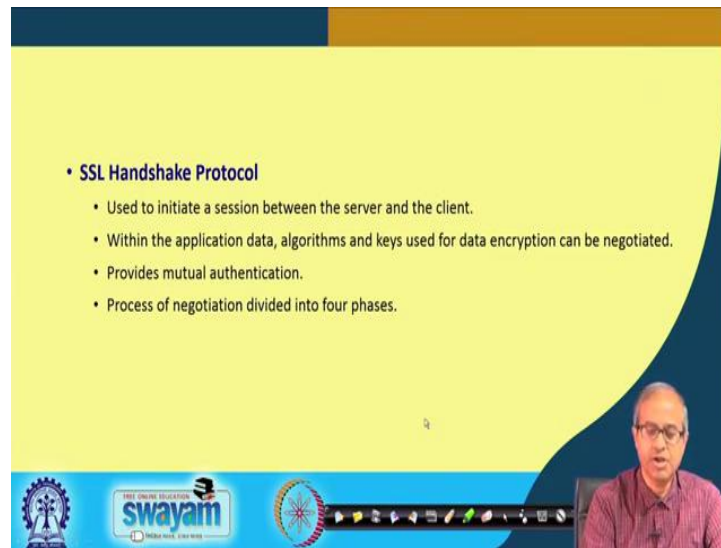
(Refer Slide Time: 17:19)

- **SSL ChangeCipherSpec Protocol**
 - Consists of a single message that carries the value of 1.
 - Purpose of this message is to cause the pending session state to be established as a fixed state.
 - ❖ Define the set of protocols to be used.
 - ❖ Must be sent from client to server, and vice versa.

And ChangeCipherSpec protocol it consists of a single message that carries the value 1. What it tells is that whatever earlier message was transmitted that what protocol to use, what exactly, which encryption algorithm to use, this stage cipher spec protocol if this message is sent, it means all those things will be taking effect immediately.

Purpose of this message is to call, is to cause the pending session state to be established as a fixed state; that means, you can say that I want to use AES, I want to use MD5 etc., etc. But, whenever you send this ChangeCipherSpec protocol message all these things you have specified will immediately take effect. They will become a fixed state. They will define the set of protocols to be used subsequently, ok. So, client must send this to server and server also must send to client so that both sides know that both sides are agreeing to this. Maybe I want AES; the other side do not have AES. So there has to be a comparability from both sides, right.

(Refer Slide Time: 18:45)



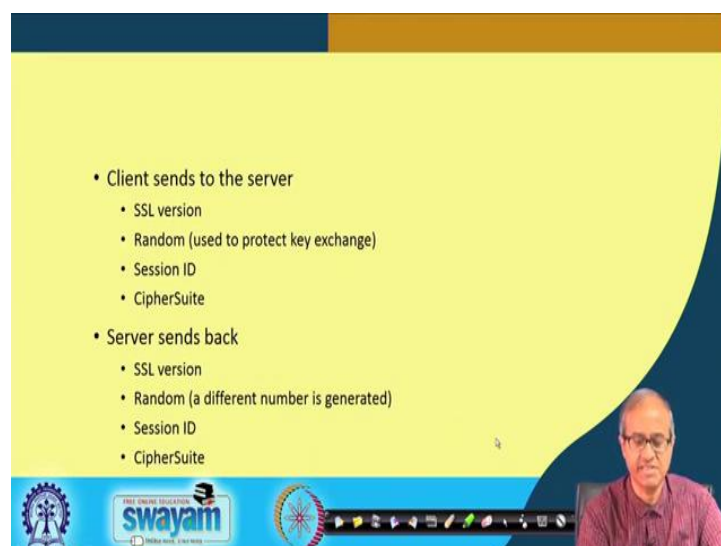
• **SSL Handshake Protocol**

- Used to initiate a session between the server and the client.
- Within the application data, algorithms and keys used for data encryption can be negotiated.
- Provides mutual authentication.
- Process of negotiation divided into four phases.

The slide features a yellow background with a blue header and footer. The footer contains the 'swayam' logo and a video inset of a man in a purple shirt speaking.

Talking about SSL handshake protocols, here all the details about the algorithms to be used or sent. This is used to initiate a session between the two parties. Within here all the algorithms and what keys to be used they can be negotiated. This is the handshake protocol. So, this also provides a mutual authentication. There is a multi way authentication protocol between the client and the server. There will be an authentication which is carried out. Now, this process of negotiation is actually divided into four phases. This handshake protocol is a little complicated. There are four phases through which this handshaking will be going on.

(Refer Slide Time: 19:36)



• **Client sends to the server**

- SSL version
- Random (used to protect key exchange)
- Session ID
- CipherSuite

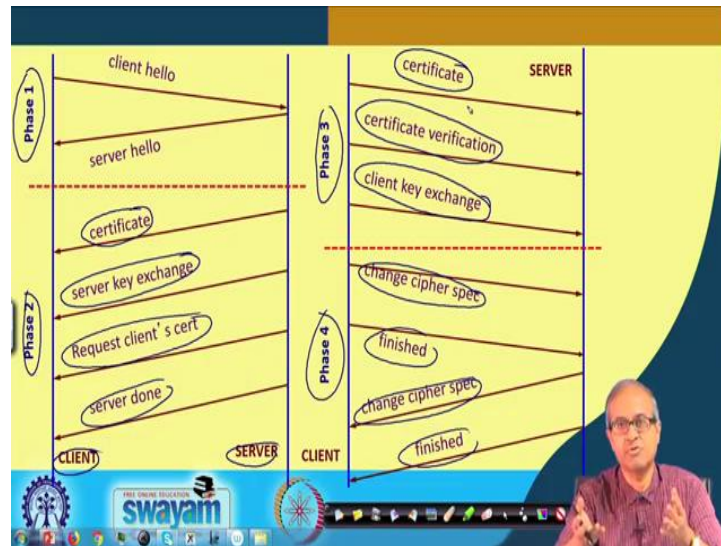
• **Server sends back**

- SSL version
- Random (a different number is generated)
- Session ID
- CipherSuite

The slide features a yellow background with a blue header and footer. The footer contains the 'swayam' logo and a video inset of the same man in a purple shirt speaking.

We will briefly, will show you what this four phases are, but the thing is that the client will send something to the server and server will send something back to the client. Like the main things that are sent out the SSL version, some random number, session ID and CipherSuite that which cipher we are negotiating right now, is it encryption, hash or whatever. Similarly, server will be sending me every similar things, ok.

(Refer Slide Time: 20:08)



Without going into detail let us see pictorially, how these things happen. This is phase 1. As you can the first phase. First phase, this is the client; this is the server. So, client sends a hello message, this is through the handshake protocol and server sends back, sends back hello message. So, both the sides know that well, the link is active. This is phase 1.

Phase 2, the server side will be sending the server certificate; certificate will contain all information including the public key of the server, right. So, certificate will be sent and server will also send the value of the key, but you see this server already had sent the certificate; that means the public key as part of it. So, now, the key will not be sent in plain text, it will be encrypted by the private key or it will be encrypted in some way and to be send so that the client can negotiate and it can decrypt.

Anyway, for first is the certificate and server key exchange, then it will request for the client certificate. It will ask the client to send certificate, because in this case both the sides will have to share certificates, because everything will be carried out in an

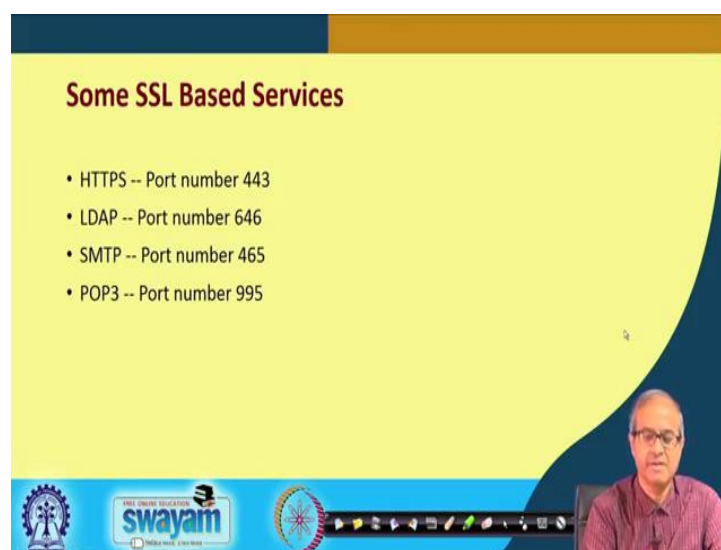
encrypted fashion. And last server done. These are the four messages which has sent one by one.

So, now, in phase 3, it is the responsibility of the client. The client will be sending the certificate first. It will also send that well, I have verified the server certificate and client key exchange, some information about the client key that which key to use right. Now, see both the parties have exchanged their certificates. Now they can encrypt a key using their own public key and send to the other side. Other side can decrypt using their private key right. Now, this client can send the key to be used for encrypting the data.

And in the phase 4, all these details about the algorithms were sent. Now, ChangeCipherSpec this was sent, then finished on the other side. Similarly, ChangeCipherSpec and finished. Now, here I am showing the minimum amount of message, but there can be more messages; there can be more means algorithms and information to be sent and received. They are all done during phase 2 and phase 3, right.

Now, as part of this certificate for example, all information about which algorithm to use they will be mentioned. So, you can negotiate tips. If the server or the clients says that well, I do not support that algorithm. He can change it and send it back. So, some more messages will be sent back and forth, ok. So, this is how the connection establishment occurs during the handshake protocol.

(Refer Slide Time: 23:41)



Some SSL Based Services

- HTTPS -- Port number 443
- LDAP -- Port number 646
- SMTP -- Port number 465
- POP3 -- Port number 995

The slide features a blue header and footer. The footer contains logos for 'swayam' and 'INDIA RISES WITH EDUCATION', along with a navigation bar with various icons. A small video inset of a man is visible in the bottom right corner.

And some SSL based services, these three already I talked about and SMTP was also there, Simple Mail Transfer Protocol. And these are the port numbers which are used standard port numbers. Secure HTTPS uses port number 443, LDAP uses 646, SMTP 463 and POP3 chooses 995.

So, with this we come to the end of this lecture where we talked about the SSL protocol which is a very commonly used secure protocol, security protocol that runs on top of the TCP and can be used to secure many applications. So, you see in an organization network whenever you detect that there are some flaws and there are some loopholes one alternative of course, is to try and use this kind of security protocol and migrate to this kind of secure message exchanges, so that confidential information or sensitive information are not leaked out to unauthorized persons who are having unauthorized access in the network.

Thank you.