

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

Lecture -35
Applications (Part II)

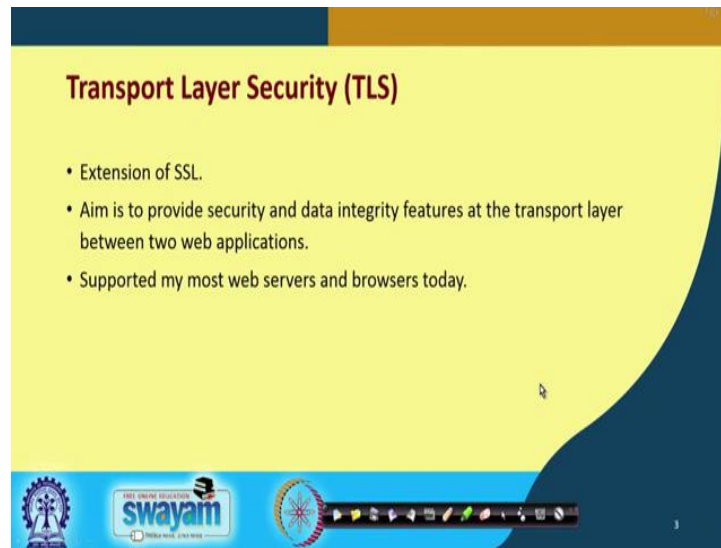
Now, we continue with our discussion on Applications of cryptographic primitives to design security protocols. This is the second part of the applications lecture.

(Refer Slide Time: 00:27)



Here we shall be talking very briefly about three different security protocols which are quite commonly used in the Internet, Transport Layer Security or TLS, IP security IPsec and secure HTTP.

(Refer Slide Time: 00:45)



Transport Layer Security (TLS)

- Extension of SSL.
- Aim is to provide security and data integrity features at the transport layer between two web applications.
- Supported by most web servers and browsers today.

The slide features a yellow background with a dark blue header and footer. The footer contains the Swayam logo, the text 'SWAYAM', and a navigation bar with various icons.

So, talking about transport layer security, in the last lecture we talked about SSL. Well SSL, we say, we saw it was a security layer which was sitting on top of TCP and was providing services like encryption, authentication etc. to the applications which are using that SSL layer. Now, this TLS or Transport Layer Security can be considered as an extension of that SSL.

Now, the primary aim of the TLS protocol is to provide security and data integrity at the transport layer level between two web applications. Now, SSL is a service which can be used by any applications where TLS is specifically for the transport layer level for end to end communication between two hosts based on the transport layer. TLS can be used to provide security and data integrity, ok. Now, most of the web servers and browsers they support this TLS today so that all communication between them can be made secure, ok.

(Refer Slide Time: 02:03)

Introduction

- Originally developed in 1995.
 - As a secure replacement for telnet, rlogin, rcp, etc.
 - Allows port forwarding (tunneling over SSH)
 - Built-in support for proxies/firewalls.
- Widely used nowadays.

So, I am not going into give any detail of the protocol. Secure shell is one protocol which is quite important, SSH. Now, you see we are very familiar with a scenario where we are sitting on a computer. We are doing a remote login to another machine and working on that. There are very common kind of programs or applications which we use to do that. One of the oldest and still very widely used commands is the telnet program or telnet command. Using telnet we can do a remote login. There are programs like rlogin, rcp, remote copy, you can copy a file from a remote machine to the local machine and so on. Now, this protocol we are talking about here, this was originally developed in 1995, SSH, ok.

Now, this allows port forwarding which is some kind of a tunneling over SSH. Tunneling, you recall is a mechanism through which some protocol data which is not supported at the current level or the layer which you are working on. The entire packet including the headers will be treated as data. It will be encapsulated with the header of the present layer protocol whatever it is and it will be tunneled or sent to the other sight. On the other sight the header will be taken out and the original data with the headers etc. will be extracted, ok.

So, this supports tunneling over SSH and here the other advantage that proxies and firewalls can be very easily configured using this protocol. So, most of the proxy servers and firewalls that we use to access them, we use SSH. This pretty widely used.

(Refer Slide Time: 04:08)

SSHv1 Protocol

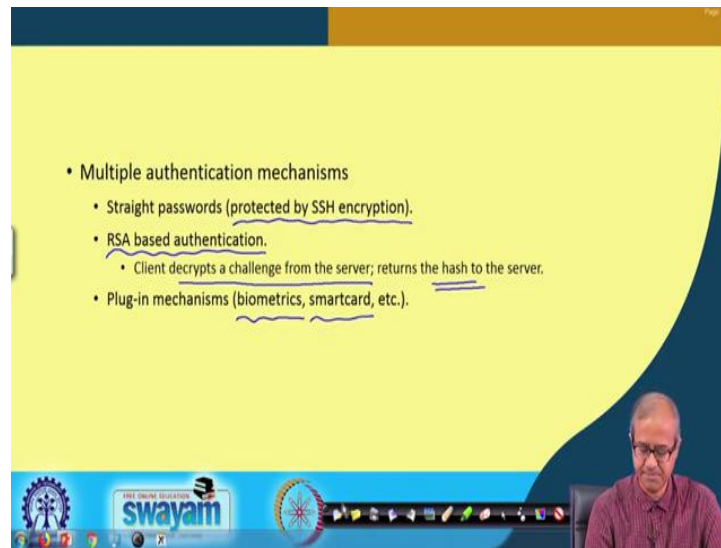
- The server uses two keys:
 - a) Long-term server identification key.
 - Binds the connection to the server.
 - 1024 bit RSA.
 - b) Short-term encryption key, changed every hour.
 - Makes later recovery impossible.
 - Short-term keys are regenerated as a background task.
 - 768-bit RSA.

Now, SSH version 1 for example, in this protocol there is a client server scenario. There is a server which is providing some kind of secure access and the clients are accessing them using the SSH protocol. There is also an SSH kind of a command on the Unix terminal if you use, ok. Now, this server here has two different keys. Now, there is a distinction which is made here. One is something called a long term key; long term key is used for server identification, for the initial, identification and authentication. So, this long term key is used to establish the initial connection.

So, you can say it binds the connection to the server and for this long term key we use 1024 bit RSA. Of course, there are later versions now which use keys with higher number of bits like 2048 and so on, but in addition to this you say 1024 or 2048 keys are good no doubt, but as I said RSA is slow. So, every time encrypting and decrypting with a longer key will take more time. It will become slow. So, there is also another key which is called as short term encryption key which is modified frequently for example, every hour or so, ok. Now, this key is relatively shorter in size typically 768 bit RSA, ok.

So, this short term key is refreshed often and during that period when the short term key is active the data which are in transmitted and flows through the connection will be encrypted using the short term key, right. This is how this protocol works.

(Refer Slide Time: 06:12)

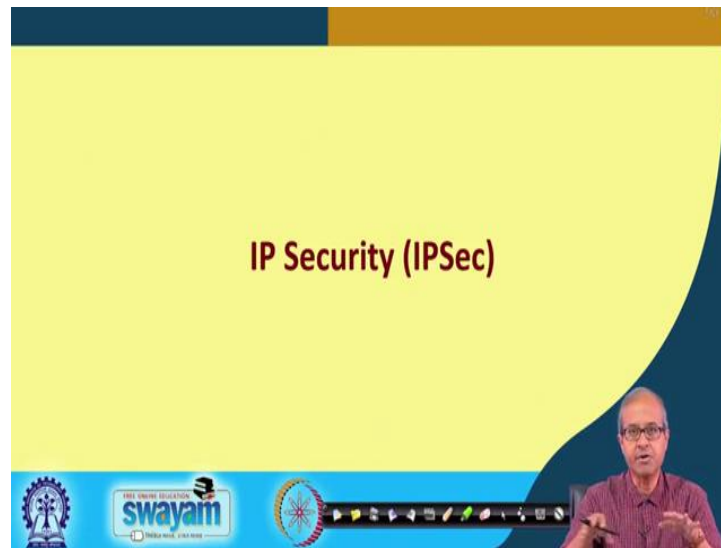


Now, there would multiple authentication mechanisms which are supported here. Now it is of course, up to the user. It is not that all these methods will have to be used simultaneously. In a particular application, these are just some options which are available. First is that you can have normal passwords, but this passwords will flow encrypted through the network. These are protected by SSH encryption.

Say unlike the older times, wherever we used to do a remote login, while a hacker which was snooping in the network can retrieve your password, because they were flowing in packets which are carrying the passwords as plain text. So, it was very easy to read them out. There is a second mechanism you can have RSA based authentication using your private key or there is something called a challenge response. Challenge response means I encrypt something using my private key. I send it to the server; server will decrypt using my public key and try to verify something like that.

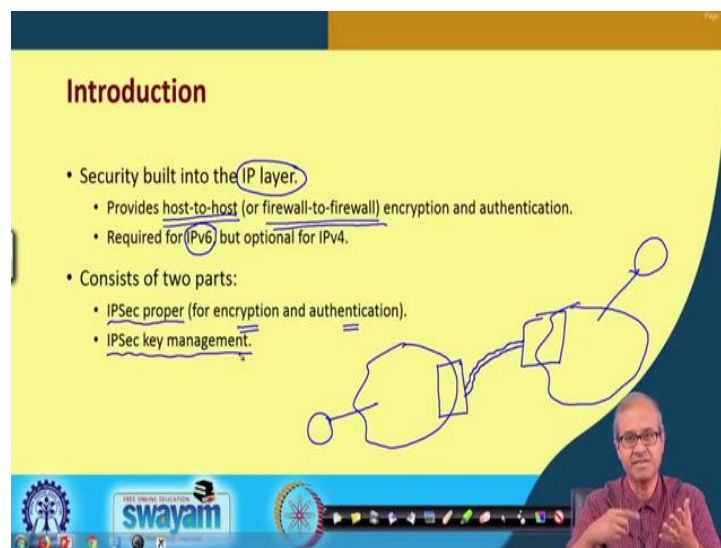
And also the other way around, the client can decrypt a challenge from the server and will return the corresponding hash value back to the server; server will verify whether its correct or not. So, there are some mechanisms. So I am not going to the detail, ok. And thirdly there are some add on mechanisms which you can add for additional security. Like, you can have some biometric mechanism like fingerprint recognition and so on; you can have smart cards. So, using smart card you can authenticate yourself and this kind of add on mechanisms are also supported by SSH.

(Refer Slide Time: 08:03)



Now, there is a security protocol even at the IP layer. Well, we talked about the protocols which work above TCP and so on, but at the level of IP, there is a protocol called IPSec. This provides secure packet transfer at the IP layer level.

(Refer Slide Time: 08:24)



So, as I said here we are trying to build some security into the IP layer and using IPSec you can have host to host or if you want firewall to firewall encryption and authentication, because you can have two organizational networks. Let us say, you have one here, one here and you are sitting here. This is one host and you are trying to

communicate it another host here. But there can be one firewall sitting in the boundary here and another firewall sitting in the boundary here. So, this authentication and this kind of protection security can be provided for the connection between these two firewalls. If you want, file, file to file or it can be even from host to host or end to end.

Now, these security features, these are normally not used in IPv4. It's optional, but if you are using IP version 6, then you must have this feature incorporated or in power bits because it will be used. There are two parts in the IPSec protocols; one is IPSec to the basic part which is responsible for encryption and authentication. Now, in methods for encryption and authentication we have already discussed all those protocols and algorithms and these mechanisms are incorporated in this protocol. This is an high level application. And there is another part which manages the key. How the two parties share key, public key, symmetric key, everything. So, that is managed by the other part.

(Refer Slide Time: 10:20)



And in terms of the protection of data there are again two different modes; one is called the tunnel mode; other is called the transport mode. We shall, we very briefly talk about these and the services that it provides. As I told you this authentication and integrity is one thing. Confidentiality using encryption, it can maintain confidentiality out of data and replay protection. Because I mentioned earlier, there is something called a replay attack which can be exploited by the intruder, if your system or network is not that well protected.

The intruder can hear or listen to a sequence of messages or packets that are flowing through the network when some legitimate user is accessing some service. Later on the intruder can try to replay those same packets send the same packets and expect a similar kind of response from the server. So, he or she can get entry into the system possibly, ok. Now, let us briefly look into these services and the modes.

(Refer Slide Time: 11:31)

(a) Tunnel Mode

- Encapsulates the entire IP packet within IPsec protection.
- Tunnels can be created between several different node types:
 - Firewall to firewall ✓
 - Host to firewall ✓
 - Host to host ✓

Diagram illustrating the structure of an IPsec packet in Tunnel Mode: A box labeled 'IPsec-H' contains a box labeled 'IP H' which contains a box labeled 'Data'.

The slide is part of a presentation with a yellow background and a blue header. At the bottom, there is a blue banner with the 'swayam' logo and a navigation bar. A small video inset in the bottom right corner shows a man speaking.

Talking about the tunnel mode, what is done here is that an entire IP packet, that means, you think about this. You have an IP packet. So, you have the IP header in one part here. You have the IP header and this is the IP data, ok. Now, this entire thing is considered as data and you add an IPsec header to it. This is the concept of tunneling. The entire IP packet you are not taking out the header, the entire IP packet is put inside a IPsec packet, high level packet and sent on the other side using all encryption whatever mechanism you are using.

Now, here I told you that there are multiple mechanisms now where this IPsec or this encryption or secured links can be maintained. You can maintain it between a pair of firewalls; between the two end machines or hosts or you can maintain it between a host to the nearest firewall. So, it depends again on the scenario, on the application, on the environment which one you want to use, fine.

(Refer Slide Time: 13:01)

(b) Transport Mode

- Encapsulates only the transport layer information within IPSec protection.
- Can only be created between host nodes.

The diagram shows a rectangular box divided into three sections. The left section is labeled 'IPSec-H', the middle section is labeled 'TLH', and the right section is labeled 'TLH'. A large 'X' is drawn over the entire box, indicating that the IP header is not present in this mode.

The slide is part of a presentation with a blue header and footer. The footer contains the 'swayam' logo and a navigation bar with various icons. A small video inset in the bottom right corner shows a man with glasses speaking.

The second one is transport mode where you encapsulate only the transport layer information within IPSec protection. So, whatever is coming from the transport layer, you do not put the IP header, you take out the IP header. So, you just imagine when packet flows down the multiple layers in the protocol stack. So, what happens? Normally with the data, with the data first the transport layer header will be appended. Transport layer header, then the IP layer header will be appended and when it goes to the physical layer, then an Ethernet level header and trailer will be appended.

But here what I am saying is that in the transport mode, in the tunneling mode, the entire thing was being carried, but here this IP header is taken out. Only the transport layer information is considered as the data part and this IPSec header is added to it; IPSec header is added to it. This is the tunnel mode and because transport layer is active only between the end to end hosts, this is only possible to be created between two hosts which are communicating.

(Refer Slide Time: 14:32)

Authentication and Integrity

- Verifies the origin of data.
- Assures that data sent is the data received.
- Assures that the network headers have not changed since the data was sent.

Now, authentication and integrity, I told you, these are some services which are supported here by IPSec. Now, what this IPSec, these authentication/integrate does? You know the definition already. The authentication means it will verify the origin of the data from where it is coming. So, the IP address is carried as part of the header, the source IP address. There is some mechanism to verify whether it is actually coming from that source. And also it verifies the integrity. It checks whether the data that is being transmitted is not modified in transit. So, you understand there has to be some kind of a hash or message authentication code mechanism built into the protocol so that this data integrity can be checked.

So, all these things whichever we have discussed in SSL, something similar is also available here and not only that, there can be some kind of attacks where the data are not changed, but the header of the packet is changed in some way that is also one kind of attack. Let us for example, if I change the destination address then the packet will not go to my intended recipient, but rather to go to some other machine that is also kind of attack.

So, here also the integrity of the header is verified whether the network headers whichever is coming along with the packet, they have not been modified also, ok. So, integrity is, integrity check is carried out in two parts; one on the data and the other one

also on the header part. Because you see this header part is important, because say, if I am the intruder and I am able to hack into some router, so that I can change the headers.

So, what I can do? I can change the destination address in all the packets so that all the packets come to my machine so that I can view and inspect and do whatever you want with all the information I get, ok. So, this is also something which has to be checked and verified.

(Refer Slide Time: 16:48)

Confidentiality

- Encrypts data to protect against eavesdropping.
- Can hide data source when encryption is used over a tunnel.

The slide is part of a video lecture. The bottom of the slide features the Swayam logo and a video feed of a presenter, a man with glasses and a beard, wearing a red shirt.

Of course in some applications confidentiality is very important. I do not want that the data I am sending should be disclosed to any third party. So, I should implement some kind of encryption mechanism here. So, you can do some encryption so that some eavesdropper who listens to your packets will not be able to decode it, ok.

Now, there is another you can say, requirement for this confidentiality I have talked about. The confidentiality of data there can be another thing like an intruder who is listening to a packet eavesdropping should not also be allowed to know that from where the packet is coming. So, the data source; that means, the source IP address for example, that also can be encrypted in some way. So, that is not directly visible to the person who is eavesdropping.

(Refer Slide Time: 17:56)

Replay Prevention

- Causes retransmitted packets to be dropped.



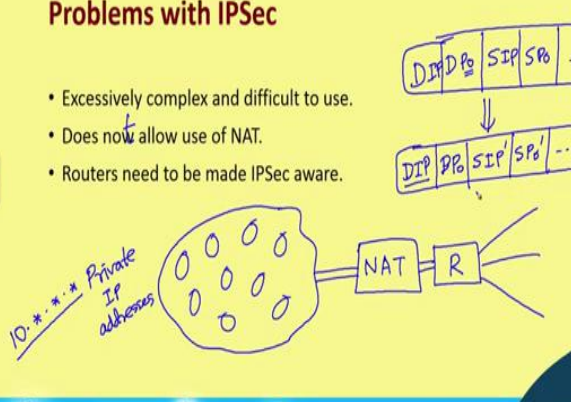
The slide features a yellow background with a dark blue header and footer. The header contains the text 'Replay Prevention' in red. The footer contains the Swayam logo and a navigation bar with various icons. A small video window in the bottom right corner shows a man with glasses and a purple shirt speaking.

And replay prevention, there is a mechanism that the protocol maintains some kind of an history so that if similar packets which were seen earlier are retransmitted, a check is made. Of course, there is a maximum time beyond which that information is not maintained, but usually replay is carried out within short durations. So, if some retransmitted packets are found again they are coming, all those packets are dropped. They are not forwarded at all. So, in this way replay prevention is also supported by IPSec.

(Refer Slide Time: 18:37)

Problems with IPSec

- Excessively complex and difficult to use.
- Does not allow use of NAT.
- Routers need to be made IPSec aware.



The slide features a yellow background with a dark blue header and footer. The header contains the text 'Problems with IPSec' in red. The footer contains the Swayam logo and a navigation bar with various icons. A small video window in the bottom right corner shows a man with glasses and a purple shirt speaking. The diagram illustrates a network topology where a cloud of private IP addresses (labeled '10.*.*.* Private IP addresses') is connected to a NAT router (labeled 'NAT R'). Above the diagram, two packet header diagrams are shown: the top one has fields for 'DIP', 'DP', 'SIP', and 'SP', and the bottom one has fields for 'DIP', 'DP', 'SIP'', and 'SP'', with an arrow indicating a transformation from the top to the bottom header.

Now, the thing is that IPSec provides you with a lot of very nice features, but nothing comes free to, have these features you will have lot of additional computations that need to be carried out, lot of encryption/decryption, hash function computation and so on. So, your effective network bandwidth, the amount of data you can send over the network per unit time that can significantly go down. This is one drawback of IPSec; this is excessively complex and obviously, not so easy to use because of this reason. And there is another thing. This should be not does not, does not allow use of something called network address translation, but of course, there are later versions which have been updated so that NAT can also be used.

So, let us briefly say what is a NAT? NAT is the short form for Network Address Translator. You think of a scenario, you have an organizational network. There are many computers which are sitting inside, ok. Now, I have talked about the IP addresses, IP address classes. Well I am taking specific example of our institution. Well at IIT Kharagpur, we have thousands of computers inside our network and inside our network we use private IP addresses. Because private address, IP addresses are available in plenty. So, I do not have to take permission from anybody to use them.

And because there are so many computers, we can assign means, one unique such private IP addresses to each machine, but the problem with private IP addresses like here we are using a class, a address that starts with 10 dot 10 dot something. This is the kind of addresses we are using insight. Now, I told you that a router when it encounters a packet with a destination address equal to one of the private addresses, it will discard that packet. It will not forward. So, such a packet will not be forwarded to the outside world. So, what happens is that these packets are first sent to a network address translator and after that our external router is sitting. So, there are connections with the outside world.

So, network address translator what it does? It translates a packet, because a packet contains what? A packet contains well I am not talking the source. Let us to talk on destination, destination IP address and there is a destination port number that is a PO. Now, IP addresses are private, so what NAT will do? NAT will convert this into a new destination IP address. Destination IP address will be the same, ok. Destination port number will also be the same, but you think of the source IP which is a private IP and the source port number.

So, what NAT will do? It will change the source IP to a new IP address and the port number to a new port number and it will maintain a table that this translation has taken place and this SIP prime is one of the public IP addresses. And this port number can be varied 1, 2, 3, 4, 5, 6. For every packet it can change so that uniqueness is maintained in terms of IP address and port number. So, this is done automatically by the NAT on the fly so that whatever packet goes to the outside world, they goes with a public IP address and a unique source port number. That is what NAT does.

(Refer Slide Time: 22:51)



Now, lastly talking about the secure version of the HTTP that we use for connection between browser and our web server.

(Refer Slide Time: 23:04)

Introduction

- An extension to the HTTP protocol to support sending data securely over the web.
- Difference from SSL:
 - SSL is designed to establish a secure connection between two hosts.
 - s-HTTP is designed to send individual messages securely.

BR ↔ WS

The slide features a yellow background with a dark blue header and footer. The title 'Introduction' is in bold red text. The bullet points are in black. The diagram shows two boxes labeled 'BR' and 'WS' with two arrows between them, one pointing in each direction. The presenter, a man with glasses, is in the bottom right corner. The bottom of the slide has a blue banner with the 'swayam' logo and various icons.

This is essentially an extension of the basic HTTP protocol which are, browser uses to fetch and retrieve some web content from web server, but here some security feature is built into it. Now, the basic differences from secure socket layer is that well, in SSL we are trying to establish a secure connection between two hosts, ok.

But in S-HTTP we are talking about individual messages that are going from a web browser to a web server. We are talking about protecting individual messages. So, this individual messages are encrypted. Similarly the web server will be sending back some response. So, I am requesting a page that page is sent back. So, individual requests and responses they will be secured, not the, not the entire connection, whatever it is flowing will be made secure not like that, ok. There is no concept of connection, individual messages that are flowing using the HTTP protocol they will be made secure.

(Refer Slide Time: 24:27)



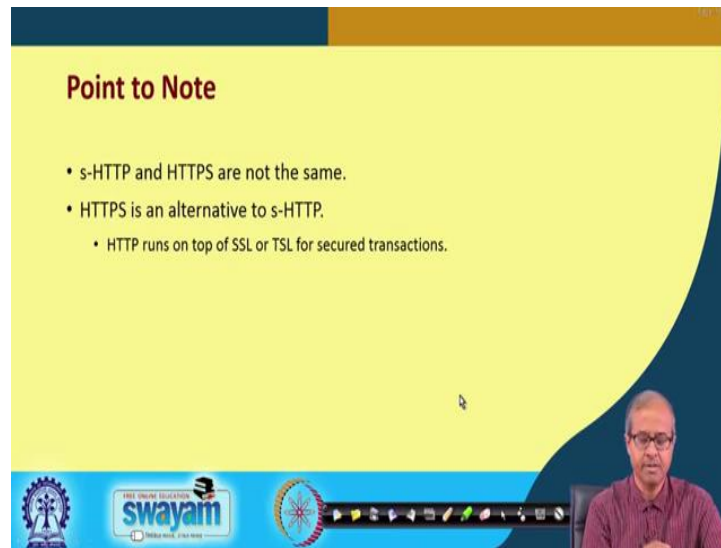
Some Features

- Provides a variety of security mechanisms to HTTP clients and servers.
- Does not require client-side public certificates (or public keys), as it supports symmetric key-only operation modes.
- Provides full flexibility of cryptographic algorithms, modes and parameters.

The slide is part of a presentation. At the bottom, there is a blue banner with logos for 'swayam' and 'Digital India'. A small inset video in the bottom right corner shows a man with glasses speaking.

Some of the features here is that it provides a variety of security mechanisms between the HTTP clients which are the browsers and the web servers. This protocol does not require the public certificate from the client side. Suppose I am using a browser. No one will ask me for this certificate rather I can ask this certificate from the browser. And this S-HTTP supports symmetric key only operation mode where use initially a symmetric key will be agreed upon and then using one of the symmetric key algorithms we can encrypt our data and send and receive right. So, here there is some flexibility on which algorithm you want to use what kind of mode that will various modes and parameters you can configure all of them.

(Refer Slide Time: 25:29)



Point to Note

- s-HTTP and HTTPS are not the same.
- HTTPS is an alternative to s-HTTP.
 - HTTP runs on top of SSL or TLS for secured transactions.

swayam
Bridging India, Empowering India

So, exactly how you want to use them. Now, one small point I want to make. Many of us are familiar with HTTPS. When we access some site, we type HTTPS followed by the name of the site that is supposed to be a secure connection. Now, S-HTTP and HTTPS they are not exactly the same. This S-HTTP is what I just now mentioned and HTTPS is an application which runs on top of SSL, typically SSL or it can be also TLS, transport layer security, transport layer, ok. So, HTTP running on top of a secure transport layer protocol SSL or TLS that we refer to as HTTPS.

So, with this we come to the end of this lecture where we have talked about some of the commonly used applications which are used in practice pretty widely. Well, you also use them either knowingly or unknowingly. Maybe some of the applications you use, they are using these insight or if you are a low level user, you can also use these commands directly from a terminal to connect to the other party and use them.

So, these features allow users and applications to have some secure exchange of data over the Internet which is otherwise a not. So, secure medium for communicating, ok. So, in the next few lectures we shall be looking at some other issues regarding security and communication and then we shall be looking at of the attacks and the corresponding remedies.

Thank you.