

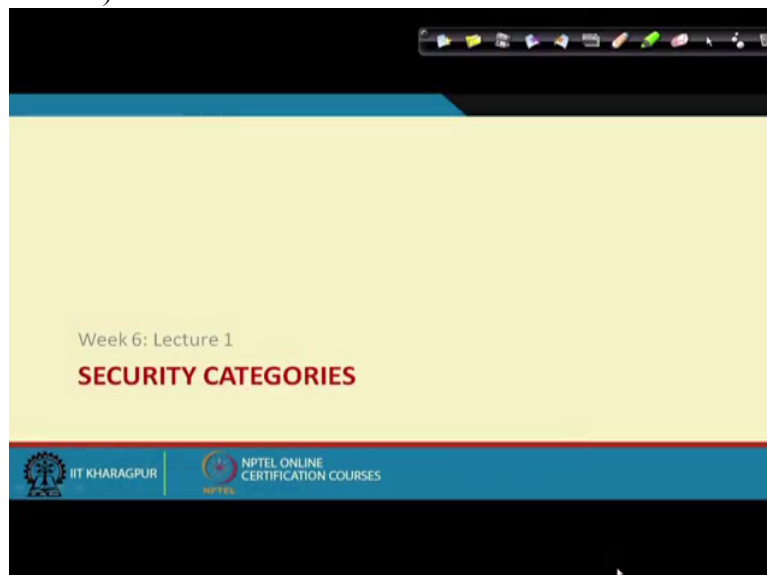
Course on E-Business
Professor Mamata Jenamani
Department of Industrial and Systems Engineering
Indian Institute of Technology, Kharagpur
Module 06
Lecture Number 28
Security Categories

(Refer Slide Time 00:18)



Welcome back. Today we are going to learn about

(Refer Slide Time 00:22)



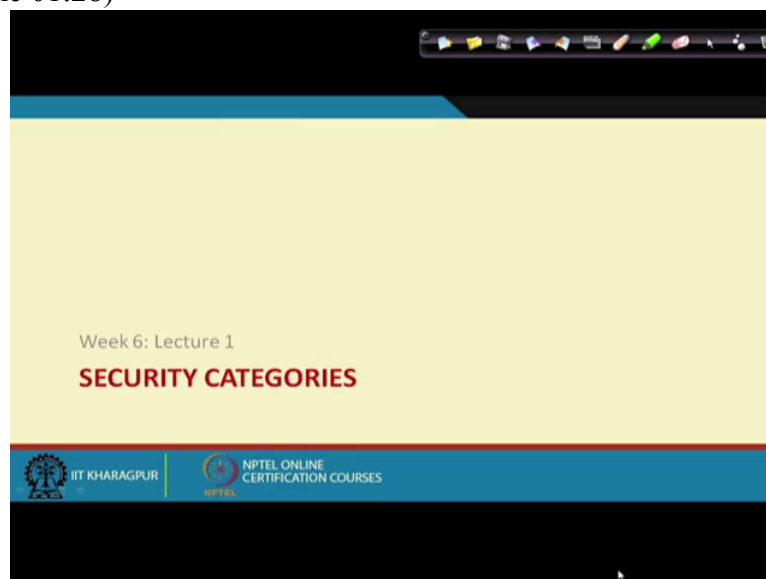
security technologies. So far we have been discussing

(Refer Slide Time 00:25)



about infrastructure for E- Business. In this context we have learnt about four major infrastructures. One is network; another then is your hardware and software and finally database technologies. We got a brief overview of all this. Now when this internet becomes commercialized, at that point of time, the business, the business houses adopting internet as it is for displaying their website etc was fine. But subsequently when there was a need for transferring secure material and specifically for online payments security started playing a major role. In fact all these E- Business transactions are based on these security ideas. Unless otherwise there would have been no security, this E Business would not have been adopted

(Refer Slide Time 01:28)



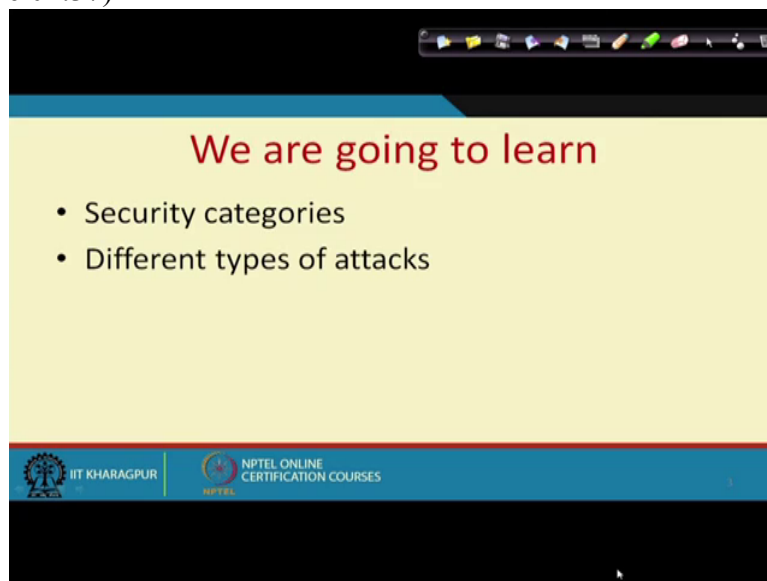
the way it is adopted today.

(Refer Slide Time 01:30)



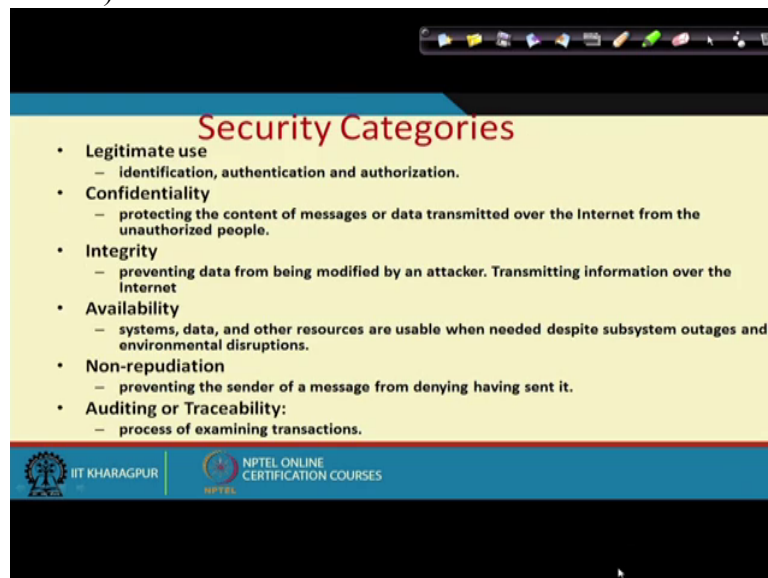
So today in this security category, the first lecture we are going to learn about various types

(Refer Slide Time 01:37)



of security and threats, attacks that happen in the internet.

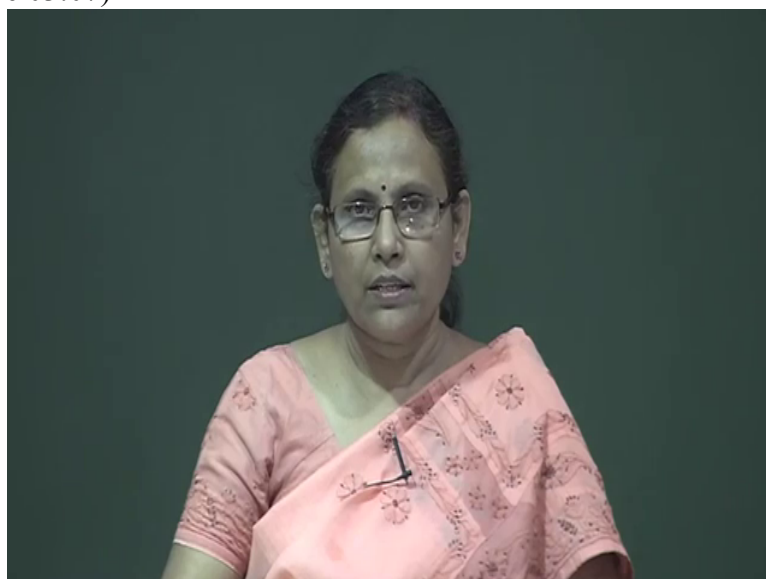
(Refer Slide Time 01:43)



So there are six categories which play, security categories which play crucial role in, in secure E- Business transactions. So first one is your legitimate use. So this legitimate use about, is about identification, authentication and authorization. By identification we mean identifying some entity correctly. For example when you log into a system, you provide your password and you get identified. And by authentication we mean this is a level of the identification where the identity gets verified. Then there is authorization. Authorization again, once you are identified and authenticated, then you are authorized to conduct certain transactions. So these three things are actually related in some way.

To cite one example let's say you are trying to log into

(Refer Slide Time 03:07)



a, into your banking system and you provide your username and password. You got identified. Then whether you are the right person at this end, understanding that is actually authentication. Then you identified as well as authenticated to use bank's system does not mean that you will be allowed to view everybody else's bank account. No. You are authorized only to see your part of the bank account. So this is the difference between identification, authentication and authorization. Then comes the term confidentiality.

(Refer Slide Time 03:54)

Security Categories

- Legitimate use
 - identification, authentication and authorization.
- Confidentiality
 - protecting the content of messages or data transmitted over the Internet from the unauthorized people.
- Integrity
 - preventing data from being modified by an attacker. Transmitting information over the Internet
- Availability
 - systems, data, and other resources are usable when needed despite subsystem outages and environmental disruptions.
- Non-repudiation
 - preventing the sender of a message from denying having sent it.
- Auditing or Traceability:
 - process of examining transactions.

IIT KHARAGPUR NPTEL ONLINE CERTIFICATION COURSES

Quick Heal Total Security
virus Protection
Removable Drive (G:) scan completed
virus found

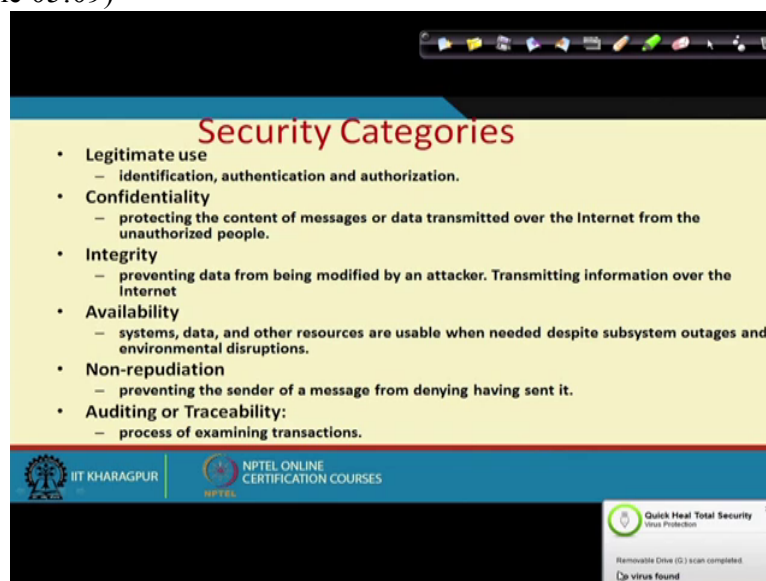
This is about protecting the content of the message or data transmitted over the internet from unauthorized people who are not supposed to see it. Then the third one is actually integrity. So this is about preventing the data from being modified by an attacker. While transmitting, I mean when it is supposed to be when transmitting the data over the internet. Then next category is availability. So this is about, you know making the system available when it is needed. So which means, if by chance because of any attack, if part of the system is not usable, a part of system is disrupted, then another, it should not be disrupting the entire system. This is about availability.

(Refer Slide Time 05:02)



Then next category is non-repudiation. This non-repudiation is about preventing

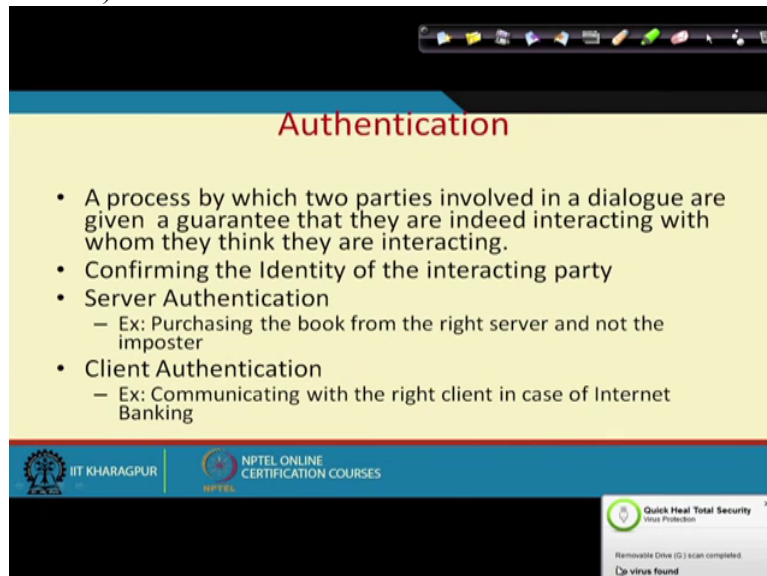
(Refer Slide Time 05:09)



the sender of the message from denying having sent it. Then the last one is about auditing and traceability. This is about after something has happened, after some security breach has happened, it is about examining the transactions once again to understand because of what such kind of security breach happened. So this is about auditing the system.

So some of these important categories we are going to now describe in detail.

(Refer Slide Time 05:45)



Authentication

- A process by which two parties involved in a dialogue are given a guarantee that they are indeed interacting with whom they think they are interacting.
- Confirming the Identity of the interacting party
- Server Authentication
 - Ex: Purchasing the book from the right server and not the imposter
- Client Authentication
 - Ex: Communicating with the right client in case of Internet Banking

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

Quick Heal Total Security
Virus Protection
Removable Drive (G:) scan completed
No virus found

So first one is authentication. This is a process by which two parties involved in a dialog are given a guarantee that they are indeed interacting with whom they are interacting; which means, suppose you are

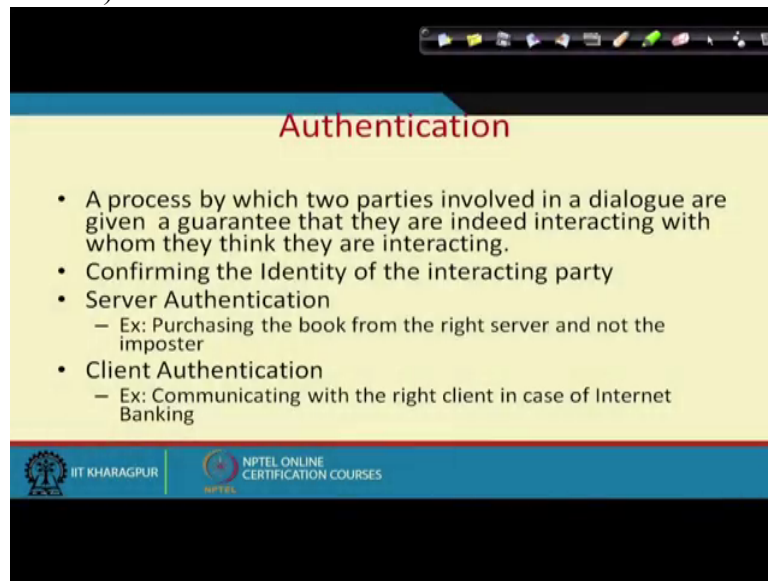
(Refer Slide Time 06:07)



connecting to your bank. You are identified using your login and password; what about the fact that the entity to which you are connecting is actually your bank? It may be somebody else has created a website which is exactly looking like that of the bank. And it is created with the purpose to get your user name and password. So the moment you enter into that site, you give your user name and password it is recorded. So how do you know that you are actually interacting with your bank? So this is about authentication.

So the

(Refer Slide Time 06:57)



Authentication

- A process by which two parties involved in a dialogue are given a guarantee that they are indeed interacting with whom they think they are interacting.
- Confirming the Identity of the interacting party
- Server Authentication
 - Ex: Purchasing the book from the right server and not the imposter
- Client Authentication
 - Ex: Communicating with the right client in case of Internet Banking

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

the authentication is the process of confirming the identity of the interacting party. It can happen in two ways. First of all, the client may

(Refer Slide Time 07:09)

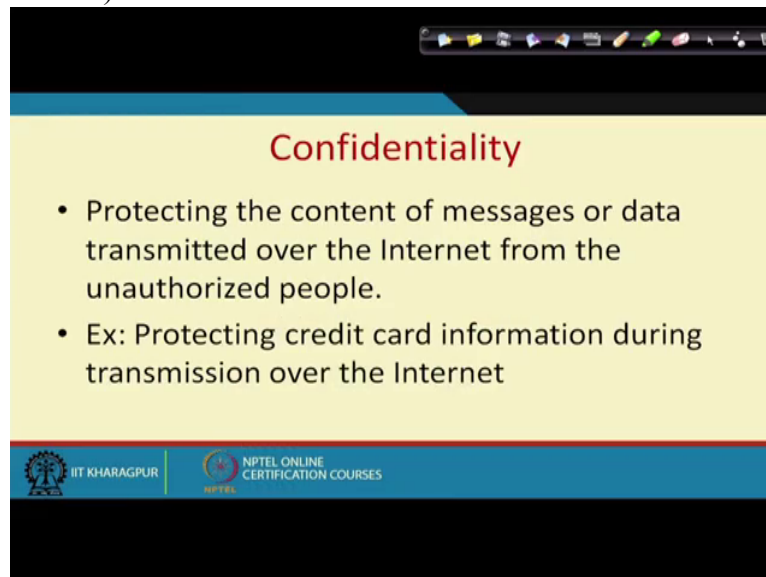


sometimes authenticate the server. And sometimes the server has to authenticate the client. So, for an example consider the case of server authentication. Suppose you are purchasing a book and you are giving your payment details in the book server. So what about the fact that you are the right person who is actually purchasing the, you are the right person who is actually, whether it is the right server to which you are connecting? Because you are providing your payment information, you are giving many of the details, your address etc., so what about the fact that you are actually connecting to the right bookstore.

Then the second one is your client authentication. So in this, the server authenticates whether it is interacting with the right client or not. Now in case of a banking system, let us say bank has to authenticate. In case of a credit card system the company has to authenticate whether it is connecting with the right client or not.

Then next category is your

(Refer Slide Time 08:22)



Confidentiality

- Protecting the content of messages or data transmitted over the Internet from the unauthorized people.
- Ex: Protecting credit card information during transmission over the Internet

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

confidentiality. It is about protecting the content of the message or data while being transmitted over the internet from unauthorized people. See we have already discussed about the internet and we know that internet is a very insecure medium. And while transmitting the data, what happens? The data goes as it is. Only thing is that in order to have this end to end connectivity and routing it through the, to the right host, you follow certain protocol, this T C P / I P protocol in particular. So during this protocol, the application data is broken into small, small packets and with each packet some header information is attached. So there is no provision for securing this data; which means anybody who has the idea of how this data is being, I mean how this various header information is being added to the data, so that person if connects to your network, can take your packet, can remove all kind of header information, get the application data, then because your T C P maintains the sequence numbers, it can go through the sequence numbers and connect those small packets to know about your data.

So therefore there has to be some mechanism in which the data that you send is represented in some other way.

(Refer Slide Time 09:57)



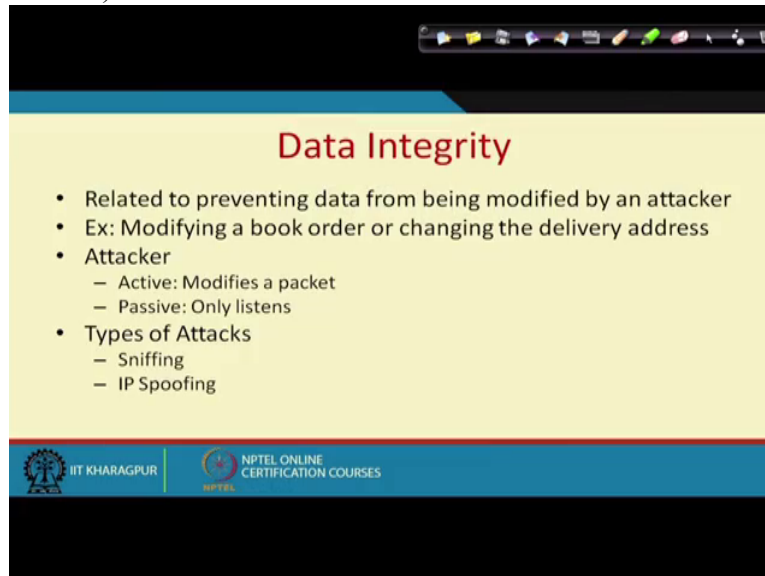
So this process is called encryption. So it is, for example when you are sending your credit card information while it gets transmitted over the internet you have to be encrypting that credit card information.

Then next category is your data integrity. It is about preventing your data from modified by an attacker while it is sent over the internet. So just now I told you, the data that you send is insecure. The only thing is that it is broken into small packets and header information are added. Now what is there in the header information? It is your, it is your I P address, it is the sequence number, in case of I P header, your I P address both of the hosts, both the hosts, the source and the destination it is there. In case of T C P it is the sequence number, acknowledgement number all those stuffs are there. So anybody can actually delete or modify this data. It can modify the application data; it can modify these header data as well.

For example suppose somebody modifies your, the host address to which you are sending the packet, so which means the packet will be diverted elsewhere and it will not reach the final host. So there will be packet lost, packet loss in the process. So the attacks that can, that come under this data integrity can be either active where the packets get modified or it can be passive. In case of a passive attacker who may be your business competitor or some enemy in that sense will actually be listening to all your packets. It will be removing the packet header information. Then it can take those small chunks of data, small chunks of application data, combine it together to make, to understand what kind of documents you might be sending.



So these types

(Refer Slide Time 12:31)



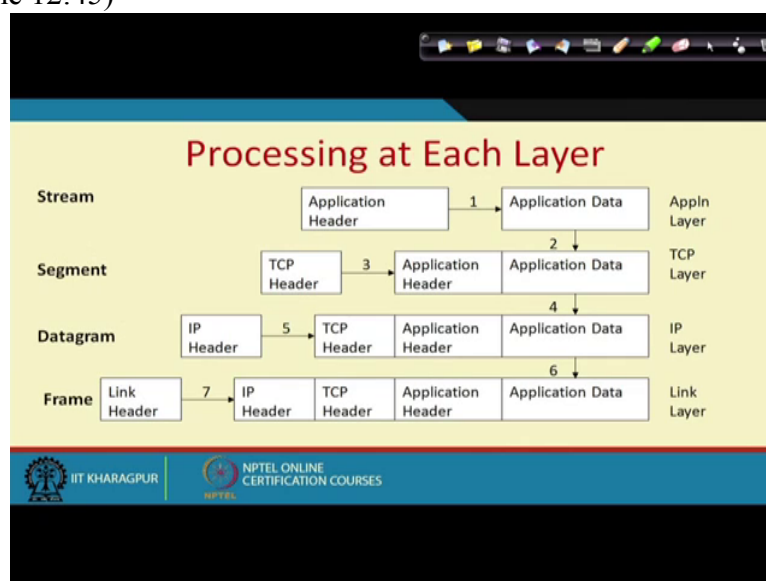
Data Integrity

- Related to preventing data from being modified by an attacker
- Ex: Modifying a book order or changing the delivery address
- Attacker
 - Active: Modifies a packet
 - Passive: Only listens
- Types of Attacks
 - Sniffing
 - IP Spoofing

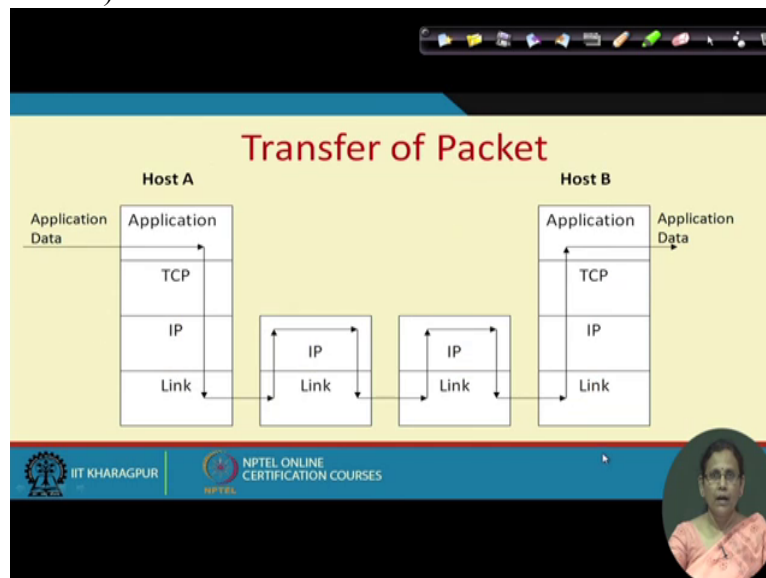
of active attack, so these types of attack on the integrity can be of two types, one is of sniffing, another is I P spoofing. Now what about the sniffing?

(Refer Slide Time 12:45)



This is what I was telling you. In case of, let us try reminding you about how the processing happen at each layer. This application data, when you send, let us say you are sending a big file, that file will be made into small, small parts called data packets. So these packets, every layer of T C P/ I P protocol stack some header will be added and

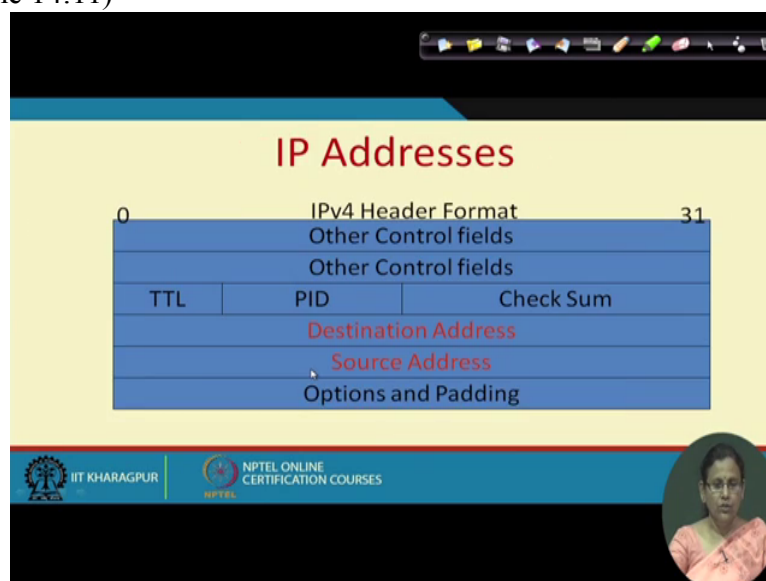
(Refer Slide Time 13:17)



while it goes from one host to the other, every part can be read by somebody who is in-between.

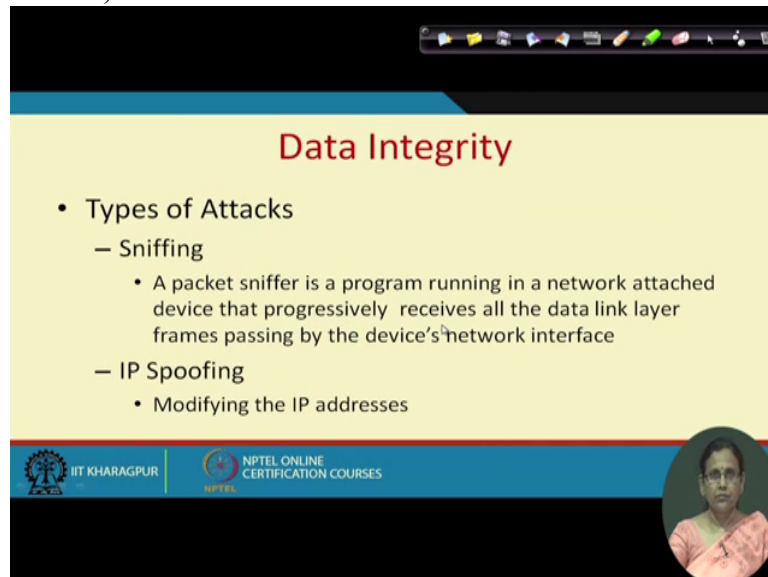
For example here the routers read your IP header and know in which direction the data has to go. So anybody who is there in-between installs a device or writes some network program can actually read this information which passes through a number of entities when it starts from one host and reaches its destination. Internet is an insecure medium and it is not owned by anybody so the data packet can move in any direction they like.

(Refer Slide Time 14:11)



So , if you look at this I P address header, there is this source address, and this is your destination address. This is what I was telling you. So your source address and destination address can be tampered.

(Refer Slide Time 14:29)



Data Integrity

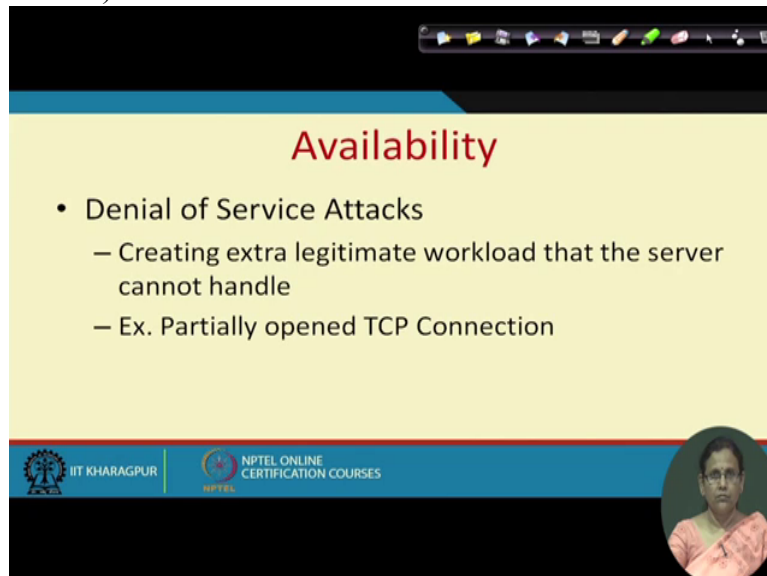
- Types of Attacks
 - Sniffing
 - A packet sniffer is a program running in a network attached device that progressively receives all the data link layer frames passing by the device's network interface
 - IP Spoofing
 - Modifying the IP addresses

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

Now in case of sniffing, a packet sniffer program which is running in the network or some network attached device like that of router receives all the data link layer frames passing through the device network interface and tries removing the application data part and reads. So it is about sniffing. Dog sniffs and finds out. It is just like that.

Then about I P spoofing. It is about modifying the, it is again there will be some kind of network program which will be not only reading the content of the message you are sending, it will also modify this I P address and so that the packets will not reach the destination.

(Refer Slide Time 15:26)

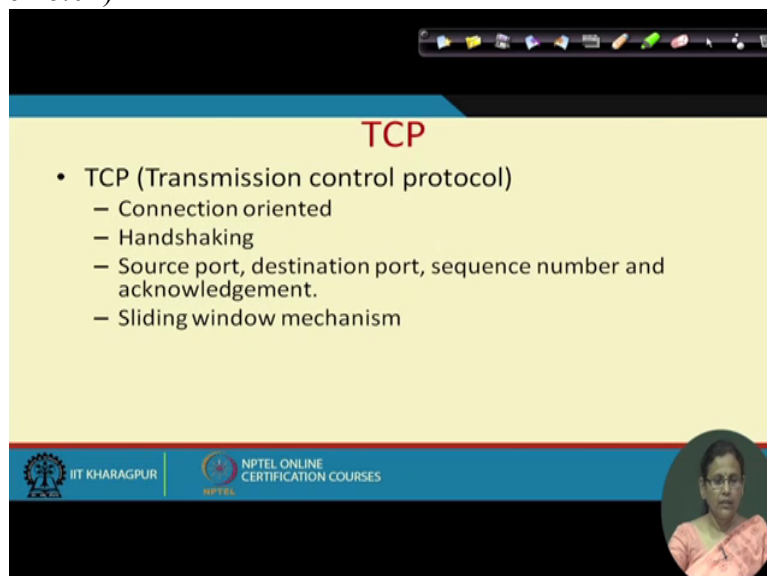
A screenshot of a presentation slide titled "Availability" in red text. The slide has a yellow background. It lists "Denial of Service Attacks" with two sub-points: "Creating extra legitimate workload that the server cannot handle" and "Ex. Partially opened TCP Connection". At the bottom, there are logos for IIT KHARAGPUR and NPTEL ONLINE CERTIFICATION COURSES. A small circular inset in the bottom right corner shows a woman in a pink sari.

- Denial of Service Attacks
 - Creating extra legitimate workload that the server cannot handle
 - Ex. Partially opened TCP Connection

Then next is the availability. By availability we mean the system should be made available, the client at, at any point of time should be able to connect to the system when the system is up. But there are certain attacks because of which it is not possible. It is about creating extra legitimate workload that the server cannot handle. This is because of partially open T C P connection.

To understand it further,

(Refer Slide Time 16:02)

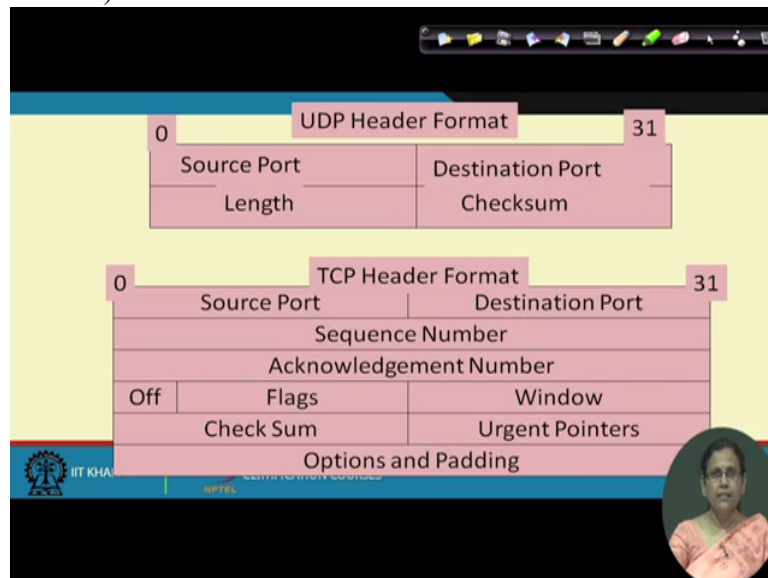
A screenshot of a presentation slide titled "TCP" in red text. The slide has a yellow background. It lists "TCP (Transmission control protocol)" with four sub-points: "Connection oriented", "Handshaking", "Source port, destination port, sequence number and acknowledgement.", and "Sliding window mechanism". At the bottom, there are logos for IIT KHARAGPUR and NPTEL ONLINE CERTIFICATION COURSES. A small circular inset in the bottom right corner shows a woman in a pink sari.

- TCP (Transmission control protocol)
 - Connection oriented
 - Handshaking
 - Source port, destination port, sequence number and acknowledgement.
 - Sliding window mechanism

let us look, let us try reviewing what we learnt during T C P. T C P that is a transmission control protocol is a connection-oriented protocol and in order to send the data and maintain,

to send the data it first the server and performs some kind of handshaking. This, during this handshaking, couple of things

(Refer Slide Time 16:30)



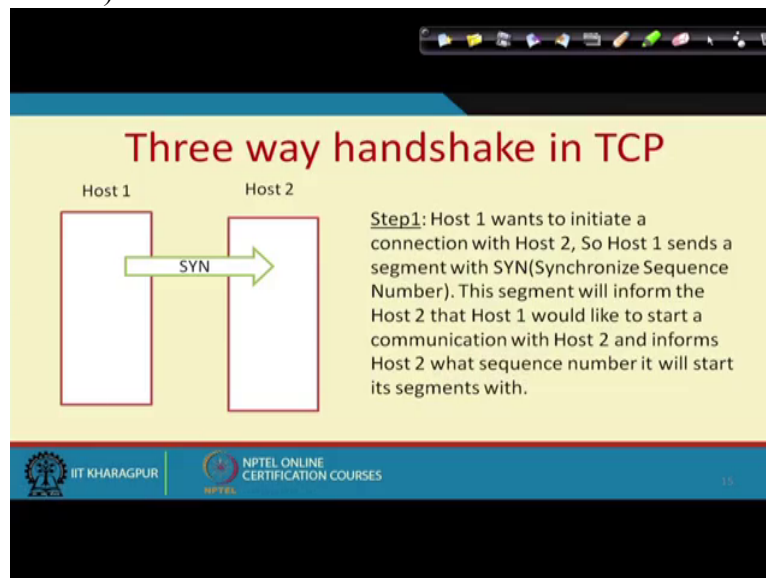
happen. You send your sequence number and receive acknowledgement number. This sequence number and acknowledgment number are very much part of your T C P header, so therefore just like I P header somebody was reading and removing your I P addresses, somebody can also

(Refer Slide Time 16:47)



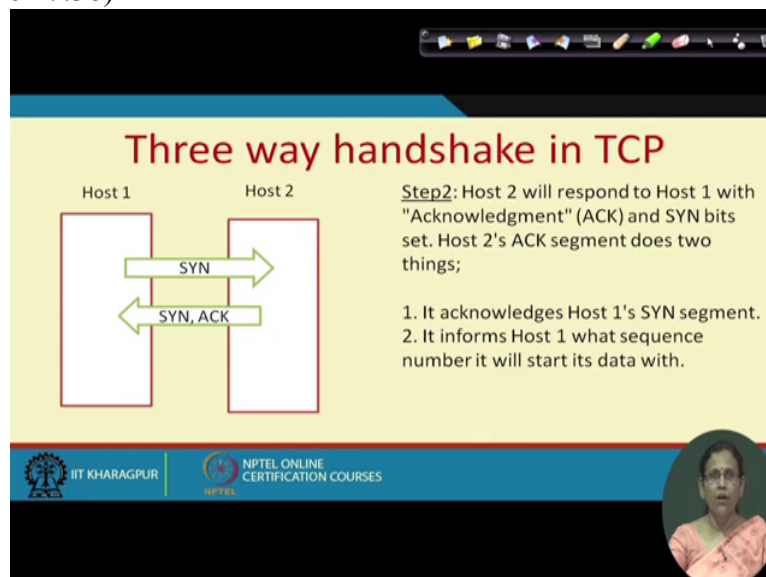
read, attacker can also read your sequence number and acknowledgement number.

(Refer Slide Time 16:54)



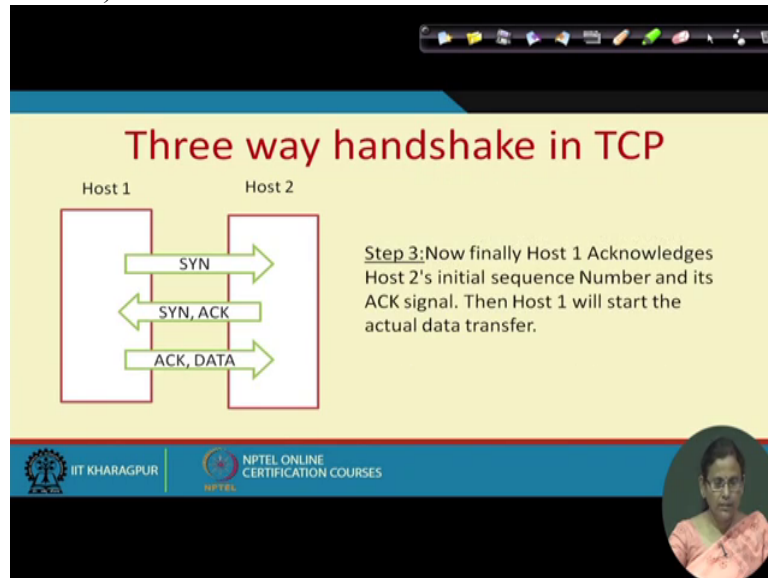
So during the three way handshake process, if the host 1 wants to connect to host 2, first it will be sending some kind of message where it will be letting the host to know the synchronization sequence number. So now this particular data segment that will be sent to the host 2 has to now acknowledge that it has received this synchronization number so in step two

(Refer Slide Time 17:38)



of this handshaking procedure the host 2 now responds to host 1 with an acknowledgement and some kind of, some kind of sequence bit set. This host 2's acknowledgement segment does two work. It acknowledges host 1's synchronization number segment, then it informs host 1 that the sequence number, informs the host 1 from which sequence number it will start taking the data. So in the

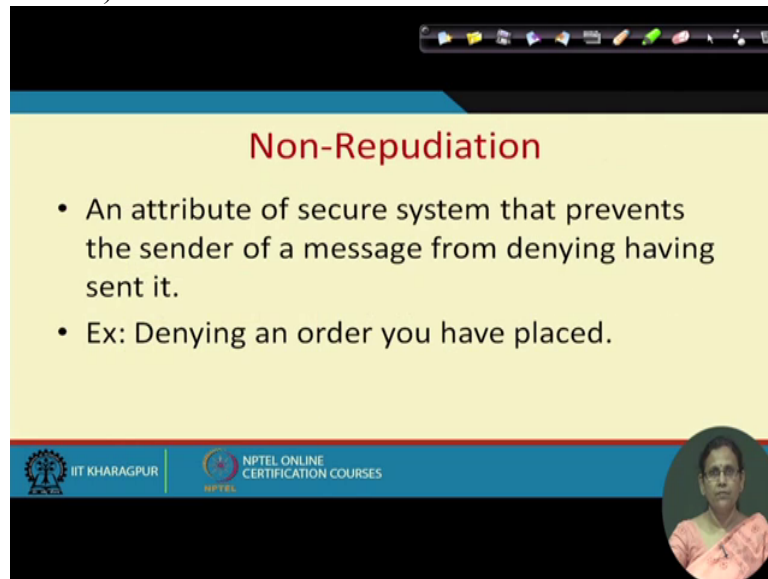
(Refer Slide Time 18:18)



third step, your T C P, what your T C P will be doing, the host 1 who is supposed to send the data will send the acknowledgment as well as the data.

So which means before the data is actually sent two more steps happen. First some synchronization number is sent to host 2. Then host 2 acknowledges that it has received a number and it tells that from which sequence number it will now start getting the data. So at the end of this, the second step the host 2 actually waits for the host 1 to receive this acknowledgement as well as the data. So now the question is, if the host 1 which is supposed to send the data does not do it, then what happens? The host 2 will be, will keep waiting at least for some time and the resources at host 2 which is server here and host 1 is possibly is a client or another server who is trying to send the data, the resources of host 2 are limited. By resources we mean here the number of connections that it can parallelly handle at a time. So therefore if somebody at host 1 writes a program so that it simply sends this, it simply performs these first 2 steps of T C P and not the third step then all the connections available at host 2 will be exhausted and all the connections will be waiting for the data and this process will, if the program continuously runs, as soon as one of the, one of the points is available at host 2, it is again, it is again attacked by, it is again used by the, the connection is again used by the attacker and the attacker continues not sending with the data. So it continues in a loop so all the connections at the host 2 are keeps getting exhausted. So this particular attack is called Denial of Service

(Refer Slide Time 20:59)



Non-Repudiation

- An attribute of secure system that prevents the sender of a message from denying having sent it.
- Ex: Denying an order you have placed.

IIT KHARAGPUR NPTEL ONLINE CERTIFICATION COURSES

attack.

Then the next category is your non-repudiation. So it is an attribute of a secure system that prevents the sender of a message from denying having sent it. For example suppose you place an order, you just

(Refer Slide Time 21:25)



send through from your internet based, internet account, internet banking account, you give some order to the bank to transfer some fund to somebody else's account. What if you say that you have not given this instruction? Can you do it? No. Because banks have made sufficient provisions so that the moment you say that you have not given this instruction, they can provide you evidence that it is not the case. You have actually given. So, so it is

extremely important in case of e-commerce transactions and payment transactions that this non-repudiation is practiced. So with this we finish our lecture on various security categories, thank you very much.