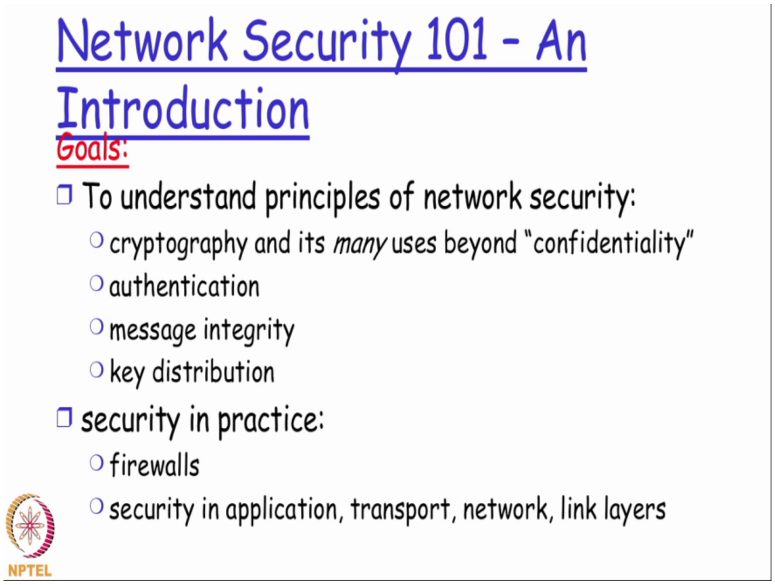
Information Security 3
Sri M J Shankar Raman,
Consultant Department of Computer Science and Engineering,
Indian Institute of Technology Madras
Module 60
Review - ll

So in this module we are basically going to do a very quick review of what are all the different concepts that we actually talked about in network security right, so network security it's basically a a set of principles which will help to put in place certain kind of confidentiality to the type of to the traffic that is actually being sent across on the network.

(Refer Slide Time: 00:44)



Network Security 101 - An Introduction

Goals:

- To understand principles of network security:
  - cryptography and its *many* uses beyond "confidentiality"
  - authentication
  - message integrity
  - key distribution
- security in practice:
  - firewalls
  - security in application, transport, network, link layers

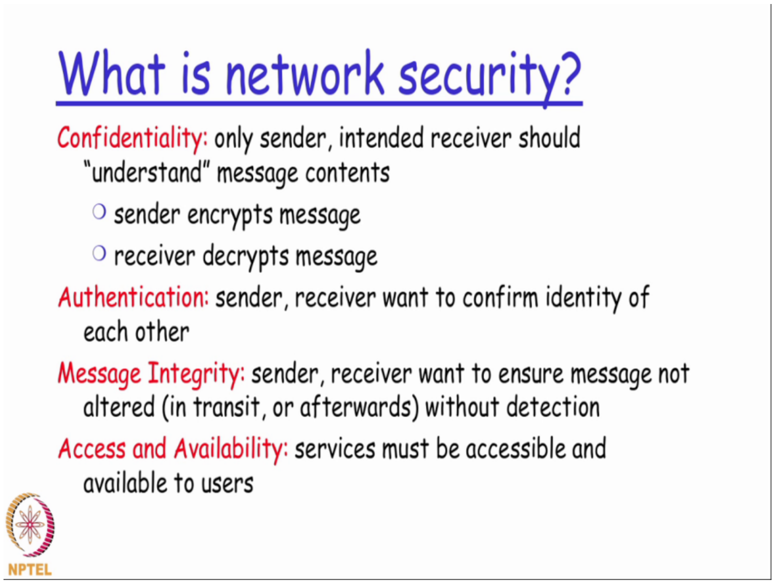
It is a set of principles that will provide us a set of authentication mechanisms for either the devices or the users which are trying to participate.

In a conversation, so conversation here means a the exchange of any kind of data, it's the set of principles that will provide me a message integrity service that we discussed in detail of trying to ensure that the the message that is finally received by the destination node or the user is really the one that has been actually sent by the original source and then it also talks about the different kinds of the key distribution mechanisms that we had discussed right.

So whether we are actually using a a private key or a public key, how is it that it is actually going to be exchanged especially the the public key which has to be exchanged to the other side and intimated to the rest of the users right, so then we also had discussed very briefly about the different types of technologies in practice as well as tools so we've talked about firewalls and the tools like a wire shark and a intrusion detection tool like snort, so we will try to do a quick review of them right now.

So what exactly is confidentiality we talked about it, so confidentiality is basically a mechanism that my network security should provide, wherein the sender and the internal receiver alone should understand the content that is actually flowing from a sender to the receiver right, so how is this achieved, so sender will encrypt the message and the receiver will be expected to decrypt the message.

(Refer Slide Time: 02:26)



What is network security?

Confidentiality: only sender, intended receiver should "understand" message contents

- ○ sender encrypts message
- ○ receiver decrypts message

Authentication: sender, receiver want to confirm identity of each other

Message Integrity: sender, receiver want to ensure message not altered (in transit, or afterwards) without detection

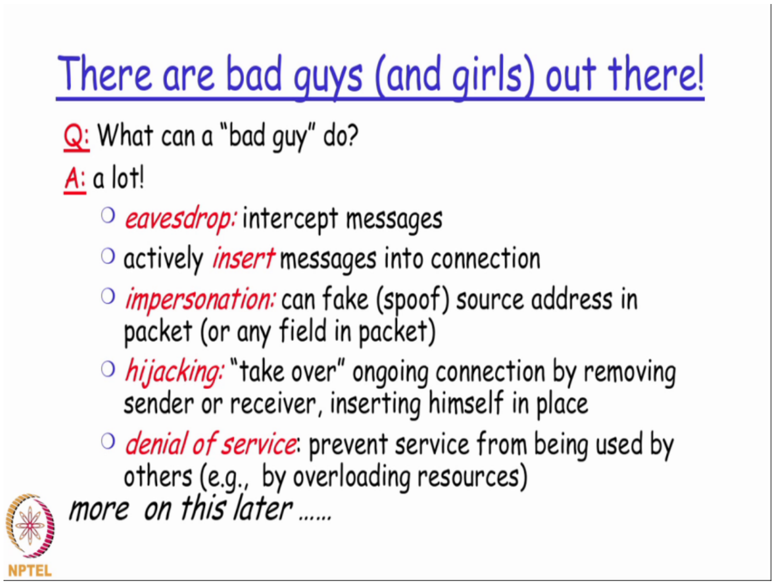
Access and Availability: services must be accessible and available to users

So authentication is a mechanism by which the network security should provide me. By which the sender and the receiver should be able to confirm the identity of each other right, so the message integrity is basically by a a mechanism by which the receiver can be sure that whatever it has received is really the message as the sender has actually try to send, along with it the network security also should provide a way by which the access and availability is guaranteed either to the set of users or to the set of devices as required for my security policy right.

So far as the sender and the receiver here we discussed in detail about how they could be really, any kind of an users, so user here could be an application like a web browser or web server or a email client or the email server, it could be a banking application on your mobile that is running for example with your banking web server it could be a dns client and the dns server and so on and so forth right, so it could be typically any kind of an application that is used, now what kind of different things that as part of network security we need to be very aware of,

So we will need to have mechanisms in place to protect against somebody just doing a plain eves dropping, somebody might try to actively insert messages the, giving an impression that they are really authentic users somebody my try to impersonate as they are maybe portraying a picture as if they are some other user,

(Refer Slide Time: 03:53)



There are bad guys (and girls) out there!

Q: What can a "bad guy" do?

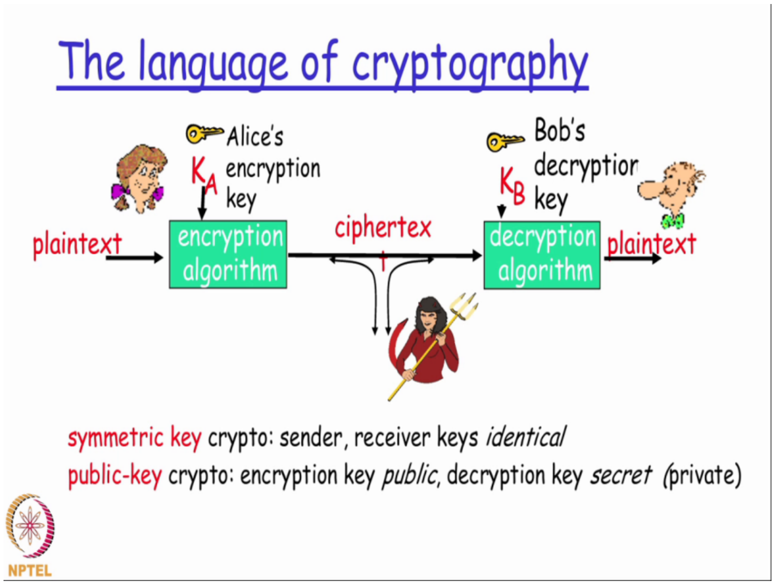
A: a lot!

- *eavesdrop:* intercept messages
- actively *insert* messages into connection
- *impersonation:* can fake (spoof) source address in packet (or any field in packet)
- *hijacking:* "take over" ongoing connection by removing sender or receiver, inserting himself in place
- *denial of service*: prevent service from being used by others (e.g., by overloading resources)

more on this later ……

Somebody might try to hijack an existing connection session and somebody might play a dirty trick of trying to do a denial of service attack or do a a distributed denial of service attacks, these kind of things we actually discussed in detail.

(Refer Slide Time: 04:05)



The language of cryptography

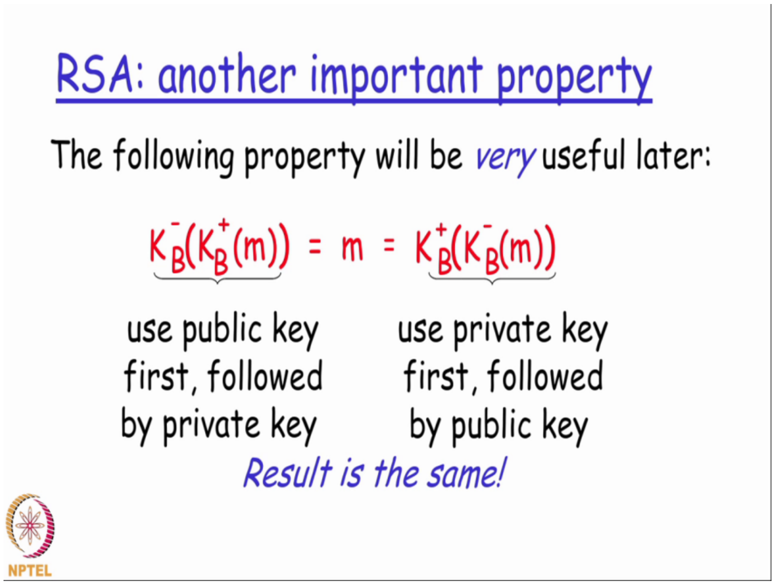
symmetric key crypto: sender, receiver keys *identical*

public-key crypto: encryption key *public*, decryption key *secret* (private)

So coming into the confidentiality part we talked about a symmetric key cryptography or a public key cryptography, a symmetric key cryptography means that both side, the sender and the receiver is going to be actually using the same key for encrypting and decrypting whereas the public key cryptography essentially means that the sender and the receiver.

Will be using two different keys, the sender will be using what is called as a public key of the receiver, the receiver is expected to use a private key of his own self which nobody else is expected to know other than him right, so thereby the since the decryption is protected the requirement and the confidentiality part of it is also taking care of, so from a symmetric key cryptography we talked about the different kinds of common cryptographic algorithms like desk, aes and triple desk that are actually available.

(Refer Slide Time: 04:55)



RSA: another important property

The following property will be *very* useful later:

$$\underbrace{K_B^{-}(K_B^{+}(m))}_{\substack{\text{use public key} \\ \text{first, followed} \\ \text{by private key}}} = m = \underbrace{K_B^{+}(K_B^{-}(m))}_{\substack{\text{use private key} \\ \text{first, followed} \\ \text{by public key}}}$$

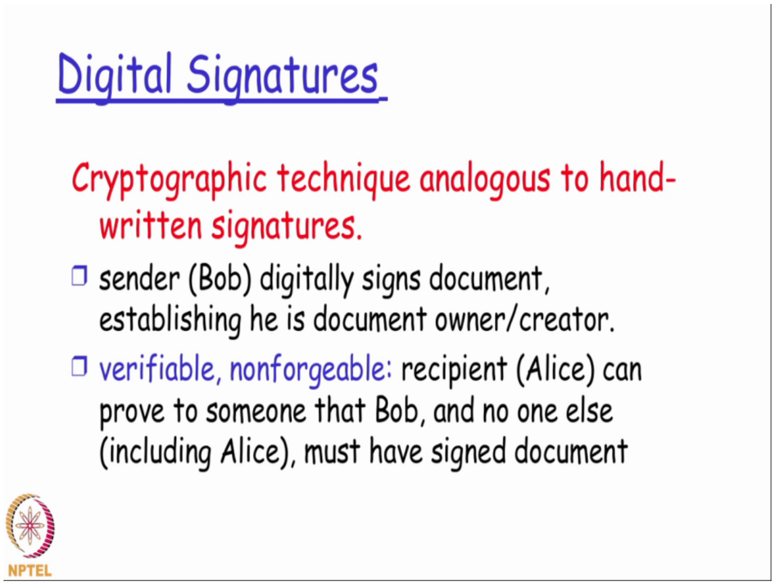
Result is the same!

And in the public key cryptography we talked about a mechanism called as an rsa mechanism where I will basically be able to use either the private key or the public key on on the sending side and the corresponding key on the receiving side to get back the original message right, so that was basically an important property of the rsa protocol, rsa protocol mechanism that we discussed in detail is basically an important the crux of am public key cryptographic mechanism.

Then we talked about about the different levels of authentication evolutions right from what kind of limitations are there if a person just says that I am so and so and then we actually evolved into subsequent versions and then finally interviews a concept of a norms value and the norms value getting encrypted to finally prove that this kind of a mechanism could be typically made use of for having the other party authenticated before the exchange of data could really happen.

So through this mechanism the authentication requirement of the network security principle could actually be met, so this was actually discussed in detail and then we introduced a concept of a digital signature.

(Refer Slide Time: 06:17)



Digital Signatures

Cryptographic technique analogous to hand-written signatures.

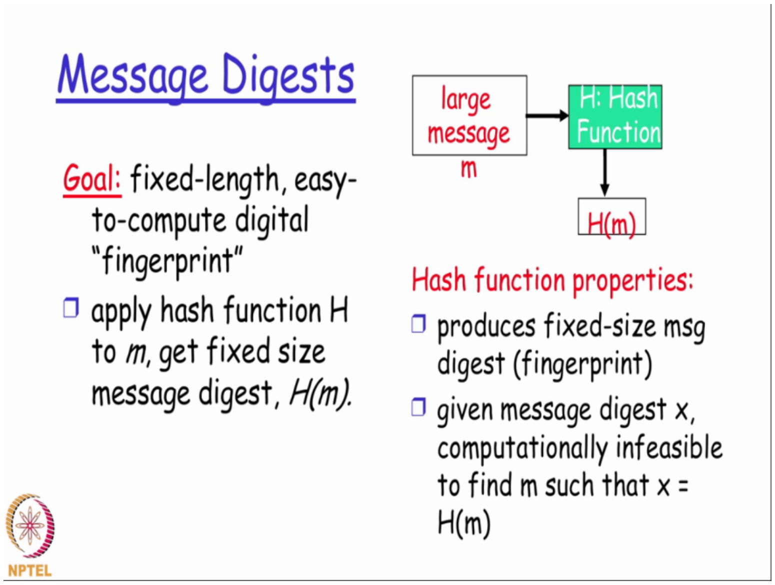
- □ sender (Bob) digitally signs document, establishing he is document owner/creator.
- □ verifiable, nonforgeable: recipient (Alice) can prove to someone that Bob, and no one else (including Alice), must have signed document

And compared it with how the digital signature could really be compared with a normal handwritten signature and then sort of make it as part of a verifiable requirement as well as non forgeable requirement right, so the digital signature be explained the the working.

Of how a digital signature is implemented at the sending side, how the digital signature is implemented on the receiving side, and how is this concept of a non reproduction is possible to be demonstrated as part of digital signature, so non reprodiation we discussed in detail wherein the person after sending the message does not claiming that he has not send the message at all in future right,

So the using the digital signature, we will be able to prove that it was indeed this person who had actually originally send the message if required even in a court of law right, so essentially the the mechanism by which even a third party could verify by the digital signature concept right,

(Refer Slide Time: 07:17)


large message
m
H: Hash Function
H(m)

Message Digests

Goal: fixed-length, easy-to-compute digital "fingerprint"

- apply hash function H to *m*, get fixed size message digest, *H(m)*.

Hash function properties:

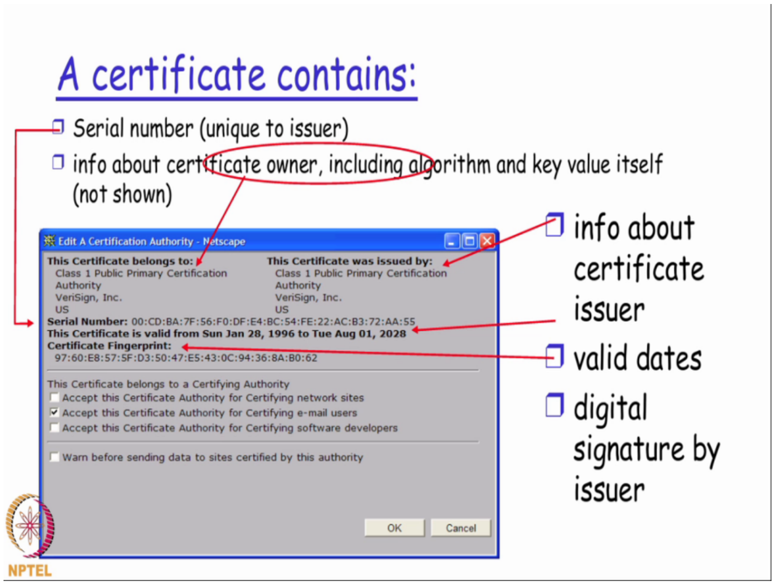
- produces fixed-size msg digest (fingerprint)
- given message digest x, computationally infeasible to find m such that x = H(m)

Then we introduced a concept of a message digest, where we talked about how different message digest algorithms like md5, sha algorithms are available for providing me the data integrity part of it, wherein with the hash function that I generate a fingerprint I will conclusively prove at the receiving end.

That the receiver has actually received the message intact without any of corruption happening either intentionally or unintentionally as part of the message transit as part and also as part of the message storage if the message is getting stored on the receiver end right, so message digest is basically to generate a fixed length, easy to compute, a fingerprint signature that I could effectively generate on the sending side and then sort of transport it to the receiver and have the receiver run the same algorithm.

To the sending side as sent on the data that has been received and the comparison of this fingerprint that has been received on the receiver side should, would be compared with whatever the sender has also generate it and sent, if these two match that essentially means that there has been no modification of the data if there is a mismatch that means essentially there has been some modification of the data in transit and then we discussed because of this the the receiver might just discard the data completely right,

(Refer Slide Time: 08:41)



A certificate contains:

- Serial number (unique to issuer)
- info about certificate owner, including algorithm and key value itself (not shown)
- info about certificate issuer
- valid dates
- digital signature by issuer

Edit A Certification Authority - Netscape

This Certificate belongs to:
Class 1 Public Primary Certification
Authority
VeriSign, Inc.
US

This Certificate was issued by:
Class 1 Public Primary Certification
Authority
VeriSign, Inc.
US

Serial Number: 00:CD:BA:7F:56:F0:DF:E4:BC:54:FE:22:AC:B3:72:AA:55
This Certificate is valid from Sun Jan 28, 1996 to Tue Aug 01, 2028
Certificate Fingerprint:
97:60:E8:57:5F:D3:50:47:E5:43:0C:94:36:8A:B0:62

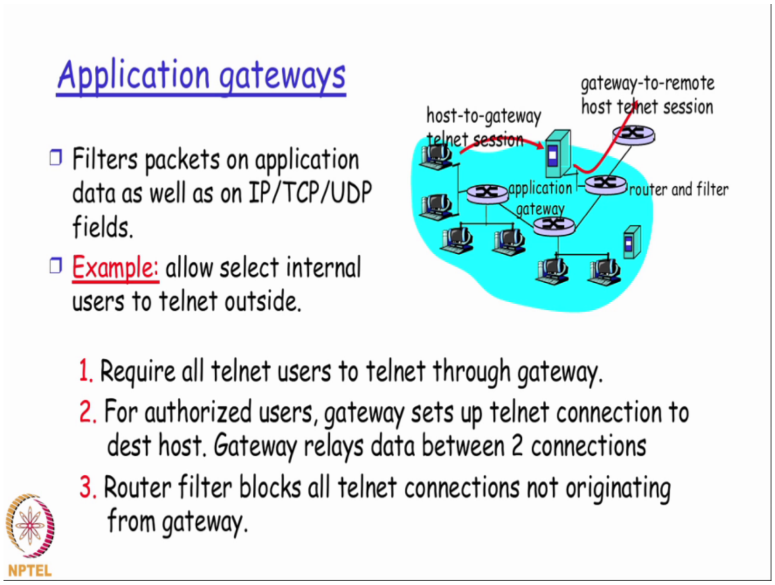
This Certificate belongs to a Certifying Authority
☐ Accept this Certificate Authority for Certifying network sites
☑ Accept this Certificate Authority for Certifying e-mail users
☐ Accept this Certificate Authority for Certifying software developers

☐ Warn before sending data to sites certified by this authority

So then we talked about how a digital certificate is actually useful for extracting the public key which is actually used for the asymmetric key or the public key cryptography encryption right, the digital certificate will actually have lot of other details in which the public key will also be part of it and that is basically what will be use with the client side to generate of the receiver and then used that public key for encrypting the data before sending it to the receiver,

Then we started looking at the different kinds of technologies like firewalls, what are the different types of firewalls that are there, what could of attacks that the firewall device typically tries to protect us form like dos attack any kind of an active attack of illegal modification or any kind of a spoofing attack, we talked about different types of firewalls like a packet filtering, we we discussed in detail about how with a packet symmetric kind of a firewall, I could actually try to filter packets based on the metadata or a packet header.

(Refer Slide Time: 09:45)



Application gateways

- Filters packets on application data as well as on IP/TCP/UDP fields.
- Example: allow select internal users to telnet outside.

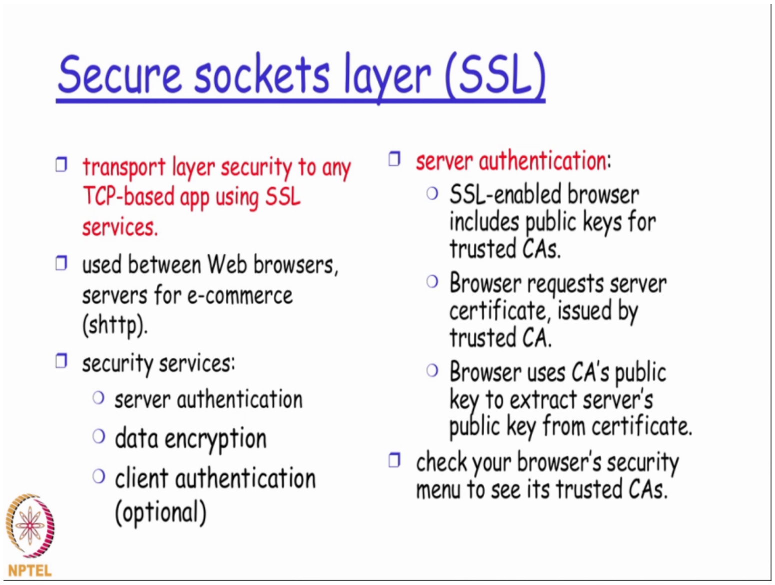
1. Require all telnet users to telnet through gateway.
2. For authorized users, gateway sets up telnet connection to dest host. Gateway relays data between 2 connections
3. Router filter blocks all telnet connections not originating from gateway.

host-to-gateway telnet session
gateway-to-remote host telnet session
application gateway
router and filter
NPTEL

Then we looked at application gateway type of a firewall where I could actually have a gateway firewall which is running for each of the applications that I want to protect my network against right then we talked about the different limitations that a firewall and a gateway kind of a a device could have and what could be deployed to overcome that limitations as as different types of rules right.

So we discussed about the ip spoofing what kind of rules and counter missions that are typically there for preventing that, kind of a ip spoofing what, kind of an attack and similar other attacks right, so once we looked at the differ types of attacks we had a very brief discussion on the secure sockets layer.

(Refer Slide Time: 10:27)



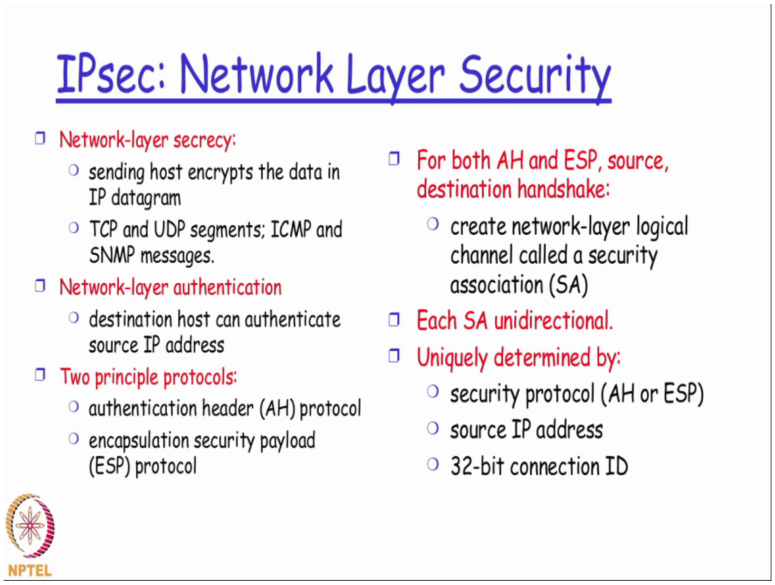
Secure sockets layer (SSL)

- transport layer security to any TCP-based app using SSL services.
- used between Web browsers, servers for e-commerce (shttp).
- security services:
  - server authentication
  - data encryption
  - client authentication (optional)
- server authentication:
  - SSL-enabled browser includes public keys for trusted CAs.
  - Browser requests server certificate, issued by trusted CA.
  - Browser uses CA's public key to extract server's public key from certificate.
- check your browser's security menu to see its trusted CAs.

The ssl part of it which is actually available as part of my transport layer security and discussed the kind of services that my ssl provides in terms of doing a encryption and decryption at the at the data level doing a type of an authentication and if necessary doing the authentication of the client also.

In certain specific application requirements, then we looked at the network level security of the ip sec protocol and how having ip sec protocol implementation,

(Refer Slide Time: 11:02)



IPsec: Network Layer Security

- Network-layer secrecy:
  - sending host encrypts the data in IP datagram
  - TCP and UDP segments; ICMP and SNMP messages.
- Network-layer authentication
  - destination host can authenticate source IP address
- Two principle protocols:
  - authentication header (AH) protocol
  - encapsulation security payload (ESP) protocol
- For both AH and ESP, source, destination handshake:
  - create network-layer logical channel called a security association (SA)
- Each SA unidirectional.
- Uniquely determined by:
  - security protocol (AH or ESP)
  - source IP address
  - 32-bit connection ID

Two different protocols in ip sec one which is the authentication header, another which is encapsulation security payload protocol, with these two things how different network security services, are typically deployable at my network layer right, so based on these discussions we had a very brief look at a couple of network security products.

Starting with a wire shark we looked at very briefly on what kind of features are available in that how I can make use of in what kind of requirements and also we looked at network intrusion software like snort, which could be used for trying to identify possible network intrusion detections on my network, so these are software's that network administrator would typically try to make use of at a very basic level to understand what kind of attacks are possibly could happen.

And also to do some kind of a basic auditing on the network in terms of what kind of traffic is flowing though that whether originating from outside or originating from inside into the outside network, so with those two sample applications we just wanted to give you an idea of what are the different type of network security products that are there but that is actually just an example, set of products that we have introduced and just to give you an idea and apart from this there are more sophisticated products.

That are actually also available, so with these basic foundation level discussion on network security in our subsequent information security courses when we talk about in detail about the different network security products and tools and configurations, this basically foundation should help you to understand the different kinds of jargons that we will need to discuss and make use of those discussions, we hope you find this module and this level security course very useful for you.

Thanks to all of you for attending this particular information security course,

Thank you.