Information Security: Level #4

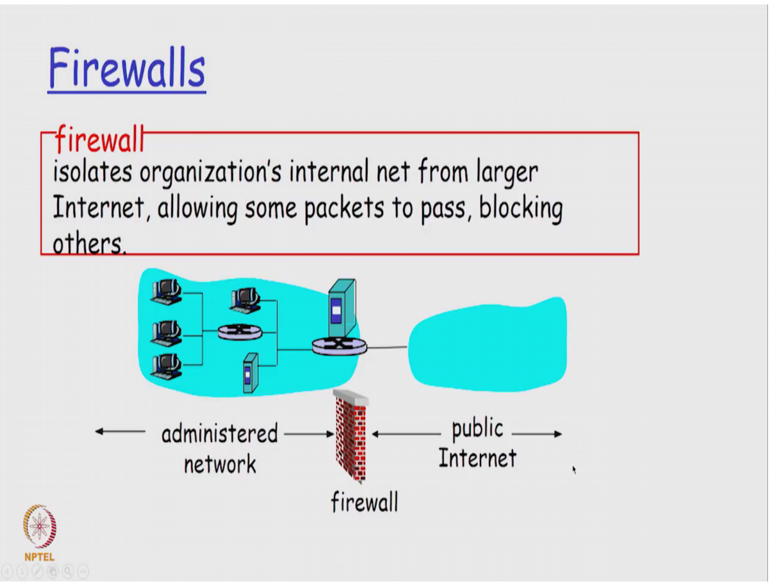
Prof. V. Kamakoti
Department of Computer Science and Engineering
Indian Institute of Technology, Madras

Lecture - 06
Basic Network Security Components

So, welcome to the next session. And last time we talked about different things that we could do on the messages that are passed on the network, so that there can be proof that somebody has sent the message that there is there is that four things that we have talked of namely confidentiality, authentication, integrity and of course, accessibility and availability can we ensured. Now, what we will now discuss in the com this session in the next session is about basically the components that are part of this network which basically can help you achieve these digital signature hash, it can also help you achieve this crypto like public key and private key cryptography.

So, what are the components that are available on the network? We will give you a very basic introduction to all these components. We have covered this in good detail in the information security three course, but we just start that some of the basics we will revise for people who have not done that course or who have done that course and forgotten something about it ok.

(Refer Slide Time: 01:25)



Firewalls

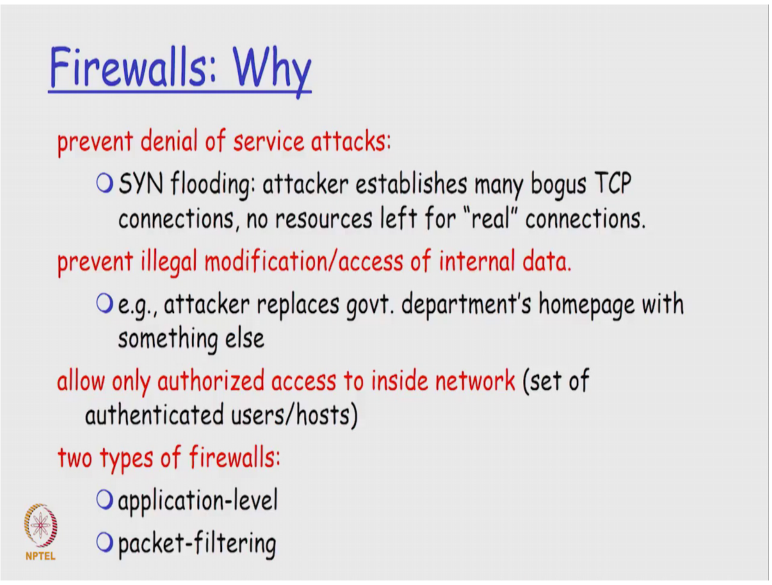
firewall
isolates organization's internal net from larger Internet, allowing some packets to pass, blocking others.

Now, first thing is the firewall. What is the firewall? Firewall as we see as the name suggest is something which will isolate an organisations internal network from the larger internet. And you can put rules on the firewall by which it can say it will allow you to pass certain packets and it will ask you to stop certain packets right. So, as you see on the screen that there is a public internet, and then there is this firewall that you are seen, and there is an administrator network. And what the role of the firewall is to allow certain packets from the public internet flow out flow into the administrator network and something about the administered network to go back to the public internet. So, I can control both ways you using puting rules on this firewall.

The challenge is firewall is like a dam you can very easy to purchase and put it, but the most important thing is how do you configure it right that is how you pour water into the dam. So, you have to pour it with correct good water know how do you how do you configure the rules right that is the major challenge today. So, today purchasing a firewall installing the firewall saying that I have a firewall all these are all easy, but how somebody arrived at the rules for this firewall which basically regulates the traffic from the public internet to the ah internal organisation and back from.

So, how what are the rational behind those rules these are some things that need to be audited. So, somebody that is a vulnerability assessment are penetration testing of your ah IT infrastructure, the thing is that he should not just say oh if there is a firewall, yes firewall is present is tick one. And then some patches of these are all install, they have the latest operating system etcetera tick two these are all does not make any sense. He should actually go and audit the rules that are part of this firewall and that makes the audit more effective and that is what we call as audit right. So, so that is something which if you are a (Refer Time: 03:30) the undergoing this course and somebody comes and that is a v a p t for you please ensure that this is done.

(Refer Slide Time: 03:39)



Firewalls: Why

prevent denial of service attacks:

- SYN flooding: attacker establishes many bogus TCP connections, no resources left for "real" connections.

prevent illegal modification/access of internal data.

- e.g., attacker replaces govt. department's homepage with something else

allow only authorized access to inside network (set of authenticated users/hosts)

two types of firewalls:

- application-level
- packet-filtering

Why do you need firewalls, lot of reasons, so at least four reasons that we will come out here one is denial of service. What is denial of service? Again going back to that four principles of confidentiality, authentication, integrity, availability. So, this is something like that there is one techniques was SYN flooding what SYN flooding basically does is that an attacker will start creating lot of TCP connections to the firewall I took to the network so that your router and. So, the router will be and they will just open the session and do nothing or maybe send some garbage in garbage out.

So, your router will become extremely loaded that nobody else can connect or a genuine user cannot connect. So, by this they deny the service for a genuine user. The genuine user can be a Bob who is sending, and you are the Alice and to and they want to communicate. But you have sent so many extra messages have inserted so many messages so that the genuine user cannot communicate. This is called denial of service. SYN flooding is a technique that can be this not a technique as a it is it is basically a method by which ah denial of service could be actually affected on a system.

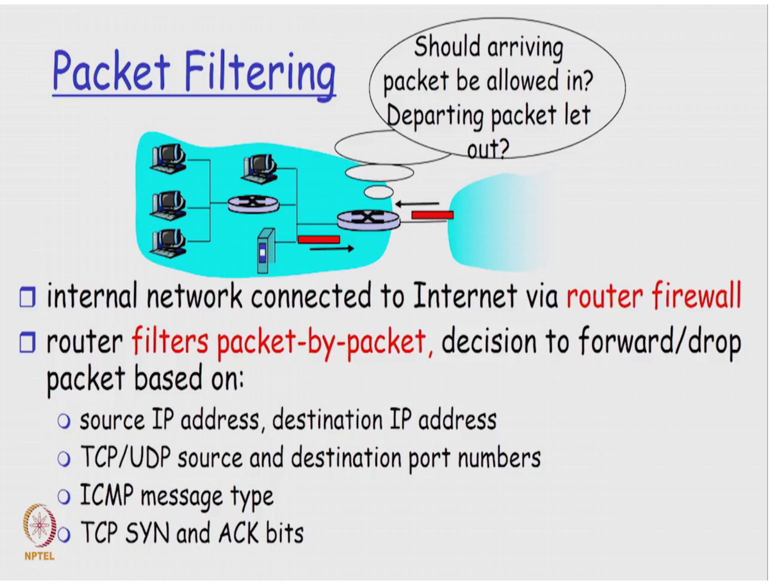
And the next thing is that a firewall can stop this type of things. So, if it sees is many TCP connections coming then it can cut certain things, it can see the threat that your router which is beyond that firewall is not affected by this unwarranted unknown unwarranted connections. The second thing is that the firewall can also prevent illegal modifications slash access of internal data. For example, somebody the attacker comes and say for example, replaces the government departments homepage, it is something else is this is really very bad thing to happen. So, a firewall can actually stop that from happening.

The third thing is it can allow only authorised access to inside network. So, nobody else can come just like that you can put a firewall saying only these people can come to the network others cannot come. So, I could authenticate at a user level. So, can a single firewall achieve all these things not necessarily. So, there are so we have talked about some connections being dropped that is at the communication level. We have also said the next thing is that some web application could not be up modified or right, so this the and some user person can be allowed to login somebody else. So, we may try to safeguard, we may try to attack, we may try to in monitor the traffic at the network level or we can also try to monitor the traffic at an application level right and both are necessary we have seen even within the slide we are seeing the necessity for both.

So, this basically ensures that the firewall is classified into two parts; one part is the application level firewall which will take care of all the application related access controls that you want to put. Application related means this particular web application this particular you know application inside that your hosting it, these application should be touched only way these, these, these people. So, like that type of things that you can use, so that is application level firewall. Other thing is that network level basically packet filtering right, so many these packets comes, these are not necessary these are unwarranted, this they are trying to attack the system, stop that right.

So, so the firewall can be used for can be of two types; one is to handle a networking level and that basically packet filtering; and another is to handle at a application level. So, application firewalls exist, network level firewalls also exist and both are different.

(Refer Slide Time: 07:43)



Packet Filtering

Should arriving packet be allowed in? Departing packet let out?

- internal network connected to Internet via router firewall
- router filters packet-by-packet, decision to forward/drop packet based on:
  - source IP address, destination IP address
  - TCP/UDP source and destination port numbers
  - ICMP message type
  - TCP SYN and ACK bits

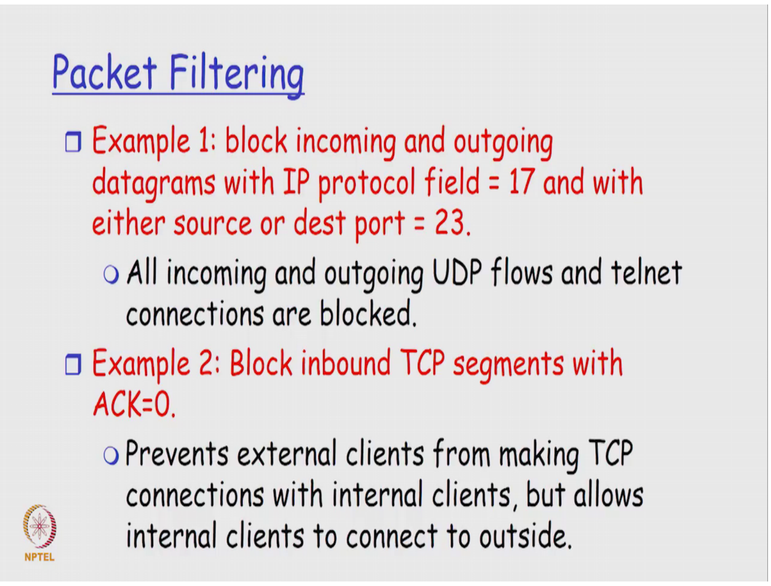
Now, let us see what do you mean by packet filtering. I need to make a decision such that the arriving packet be allowed in or not, and the dip allowed in means arriving packet is coming from the external internet, it is going to try to go into my internal system should allow it or not. And the other way is that can departing packet that is going out should I allow it to go or not right, both are important. Say from an external packet I could get the Trojan or a worm or a virus or a malware inside; on the other side, I can also allow somebody as a company secret they can send that company secret outside. So, both ways have to monitor somebody internally does not do some mischief and try to send confidential information outside. Somebody from external do not try and inject a malware into the system to basically start ah you know malfunctioning my system. So, both ways if I may have to do a packet filtering.

So, the router actually filters packet by packet and decision to forward slash drop the packet can be based on this thing. So, if put a firewall then if I do packet I can basically filter. And what I can wha wha what are the conditions based on which I can filter I can say source IP, destination IP. So, if I say source IP for example, I am I am in a bank, some attack from say some foreign country those IPs will have some number. So, anything coming from that IP stop; that means, nobody in that country can come and access my. So, this is what we say as source IP address or destination IP address base filtering.

So, when friends in network packet comes, please note that there are some sources source address destination address then payload, payload is actually the message. When I start accessing the payload it becomes much complex because payload is large in size, it can be encrypted can come through VPN and etcetera. But other than that there are the source address destination address and other thing which we call as metadata. Typically, a router actually access the metadata a network based firewall actually looks at this metadata and try to make some decisions whether to allow a packet to go in and similarly some packets to wants to go should allow it to go out or not. So, the packet filtering can happen either by the source IP address or the destination IP address it can be through TCP slash udp source and destination port numbers right from this port do not allow rather than the address there can be a port.

A port is nothing but one that gives you a particular service I do not want to give telnet service or something. So, block telnet. So, if somebody irrespective of which source address or destination IP address, if you want to access that port stop it and it can be ICMP message type all it can be a TCP SYN. And acknowledge with based on these things the router can basically stop a packet from going in or stop a packet from going out. And this is what we call as packet filtering. So, these are all some examples of packet filtering.

(Refer Slide Time: 11:08)



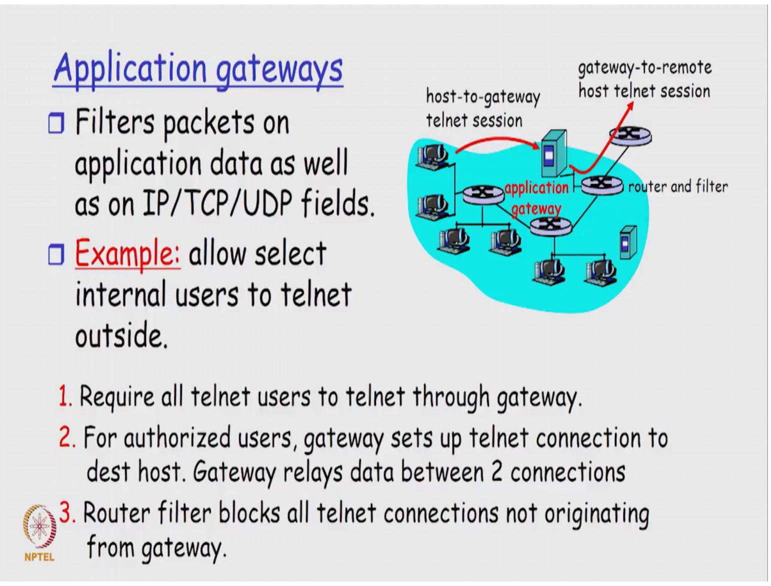
Packet Filtering

- Example 1: block incoming and outgoing datagrams with IP protocol field = 17 and with either source or dest port = 23.
  - All incoming and outgoing UDP flows and telnet connections are blocked.
- Example 2: Block inbound TCP segments with ACK=0.
  - Prevents external clients from making TCP connections with internal clients, but allows internal clients to connect to outside.

Example one block incoming and outgoing datagram with IP protocols field equal to 17, and with either source or destination field port equal to 23, so that means, all incoming and outgoing UDP flows and telnet connection are blocked. The IP protocol field 17 essentially means UDP; and source or destination port equal 23 means telnet. So, these are blocked otherwise (Refer Time: 11:20).

The example two is block inbound TCP segment with ACK equal to 0 this what it will prevent external clients from making TCP connections with internal clients, but allows internal clients to connect to go; from external I cannot make a TCP connection to internal clients. So, these are some simple rules that you can put and basically protect your network from. These things you do not want whatever I put in red I do not want tell the way by which I can capture it at the crux at the at the edge of my organisation with the internet; at that edge I put this firewall put these rules and see that this does not.

(Refer Slide Time: 11:57)



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.

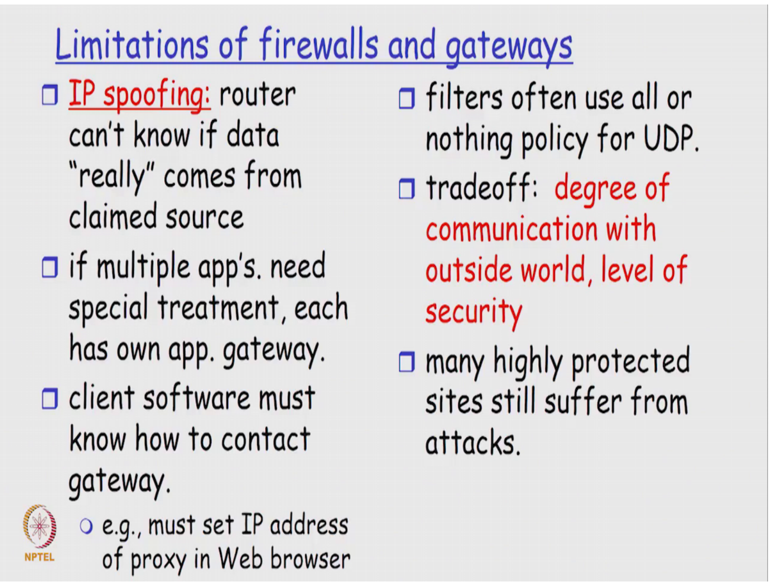
host-to-gateway telnet session
gateway-to-remote host telnet session
application gateway
router and filter
NPTEL

Now let us look at application gateway. What are application gateways they actually filter packets on application data as well as they can do on IP TCP UDP fields application gateway or firewall at application level can also serve as a packet-filtering thing. So, let us look at the setup here. So, as I allow select internal users to telnet outside. In the previous case, I said no telnet outside or no telnet inside right. So, suppose I say if I do a packet base filtering as a no telnet outside. But now I can say it is no telnet outside except for some of these how do I achieve this is how so require.

So, these are the three steps that we need ensure. First I need an application gateway application gateway realises that this is a telnet application. And it will require all the telnet users to telnet through that gateway only. So, if I want to telnet to outside have to use that gateway only. And for all authorised users the gateway sets up telnet connections to destination host, the gateway relates data of between these two connections. So, this becomes like a postmaster with postman with basically takes data from here and give it there and vice versa.

And the router filter the filter in that router blocks all telnet connections not originating from. So, this is a set up here as you see here. So, you have an application gateway there, you have a host to gateway telnet session, and the gateway to remote host telnet session and you basically have a router and filter. So, so the router filter blocks all telnet connections not originating from the gateway. So, by this what happens is the gateway basically disables at an application basically at a telnet level telnet as an application is basically stops any user who is not who is not auth authorised by your rules from telneting outside right. So, so this is what we call as an application gateway and that is different from a packet filtering gateway.

(Refer Slide Time: 14:04)



Limitations of firewalls and gateways

- IP spoofing: router can't know if data "really" comes from claimed source
- if multiple app's. need special treatment, each has own app. gateway.
- client software must know how to contact gateway.
  - e.g., must set IP address of proxy in Web browser
- filters often use all or nothing policy for UDP.
- tradeoff: degree of communication with outside world, level of security
- many highly protected sites still suffer from attacks.

So, let us very quickly look at the limitations of firewalls and gateways. First thing is that it relies on what you get on a metadata. For at times it cannot stop you from say IP spoofing, spoofing means somebody says somebody makes that destination address or sorry the source address or something and sends me right, somebody is attacking the institution or say some country that some that country has some IP address. This firewall cannot ensure whether that IP address correct or not. Somebody can put some other IP address and still send me, I believe on what that IP addresses. So, if I want to stop something from say some country x that, but people in that country x can himself send and that that I do based on the IP address. People in that same country x can send with some IP address y and your firewall will think it is not from x it is from y, so that is one thing. So, the router cannot really know if data is actually coming from the client source that is a limitation of firewalls and gateways.

The second thing we call it as the gateways application gateway if multiple apps applications need special treatment each has to have its own application gateway right that is another thing. And if the client software must know how to contact the gateway that is must set IP address of proxy in web browser right. So, I have to go through that gateway; otherwise I cannot even go out like what we saw in this telnet thing right. So, I have to have to go through that gateway and the gateway has the authenticate. If something does not from that gateway I cannot basically move forward ok.

And then this filters often use all or nothing policy for UDP. I cannot have selected things especially the UDP protocol. So, I there I will say either at shave my head completely or full grow, I do not have an hair cut right. So, this is does the same thing here. So, use all or nothing. And the trade off is the biggest trade of is degree of communication with outside world with level of security. If I put more and more rules it becomes complex that same way I become more and more (Refer Time: 16:15) ah. So, many highly protected sites still suffer from attacks because of these limitations because I cannot put very tight rules. So, I relax the rules and that relaxation basically is exploited right. So, there needs to be something more than this firewall. Firewall is very important application gateways are very important, but beyond this firewall and the gateway, we need something much more also to handle these limitations. We will see about that in the next session on what we claim as internet security tricks.