

Information Security: Level #4
Prof. V. Kamakoti
Department of Computer Science and Engineering
Indian Institute of Technology, Madras


Lecture - 07
Internet Security Threats

So, welcome to the session. So, in the last session, we just stopped with understanding some of the limitations of firewalls and gateways.

(Refer Slide Time: 00:22)

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.
- 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.

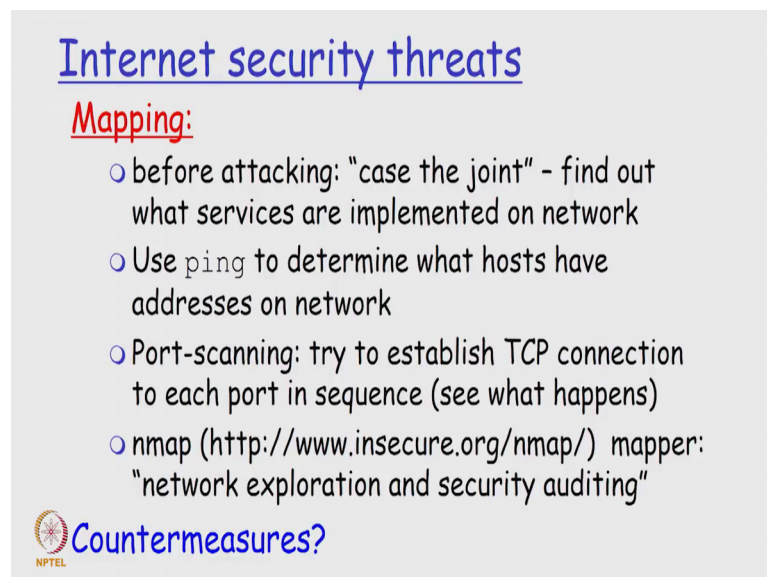
 ○ e.g., must set IP address of proxy in Web browser

Just quickly recap the limitations are that number one IP spoofing. The router actually cannot know if the data really comes from the claim source. And if multiple applications need each one of them need a special treatment, like for this, for application one some IP should not be there for application two some other IP should not be there right. So, there is some special treatment, each will have its own application gateway. So, you will have multiple application gateway one each for each.

And the client software must know how to contact gateway that is must set IP address of proxy in web server web browser. So, even when we have a restricted access for say within a particular organisation then whenever I open a browser I need to be authenticated by the web gateway, so that you know all my traffic with respect to browsing goes to. So, this is essentially means that you will have lot of web application proc[proxy]-proxies or gateway.

And many times the filters that we use or either you completely block or completely allow. So, it is not that is cannot be something middle how send this do not send this. Ultimately, when we start looking at firewall and gateway the trade off is now between the amount of communication that I want to have with external world verses the amount of rules I am going to do here for security reasons to stop this communication. So, the tradeoff is between how much should I communicate, if you want to communicate more freely, if you want many people to communicate at the same time I want security I start putting rules. So, this tradeoff essentially is seen quite big by just having firewalls and gateways. So, with this as a background, in this session, we will talk more about what is security in the internet.


(Refer Slide Time: 02:13)



Internet security threats

Mapping:

- before attacking: "case the joint" - find out what services are implemented on network
- Use ping to determine what hosts have addresses on network
- Port-scanning: try to establish TCP connection to each port in sequence (see what happens)
- nmap (<http://www.insecure.org/nmap/>) mapper: "network exploration and security auditing"

 Countermeasures?

So, let us see how an attack actually happens. The attack actually happens in a very systematic fashion. So, first the attacker actually would go and find out what are the services that are implemented on your network on your system. For that we can first you need to find out whether a system exist for that we can use things like ping to determine what hosts have addresses on network. So, they can ping and find out the existence of the system whether system is alive or not etcetera, so that is why many times ping is disabled. If you do not, so at the point if you go and disable ping and really when the system is not working, you cannot really go and find out whether system is not working or there is a some other failure.

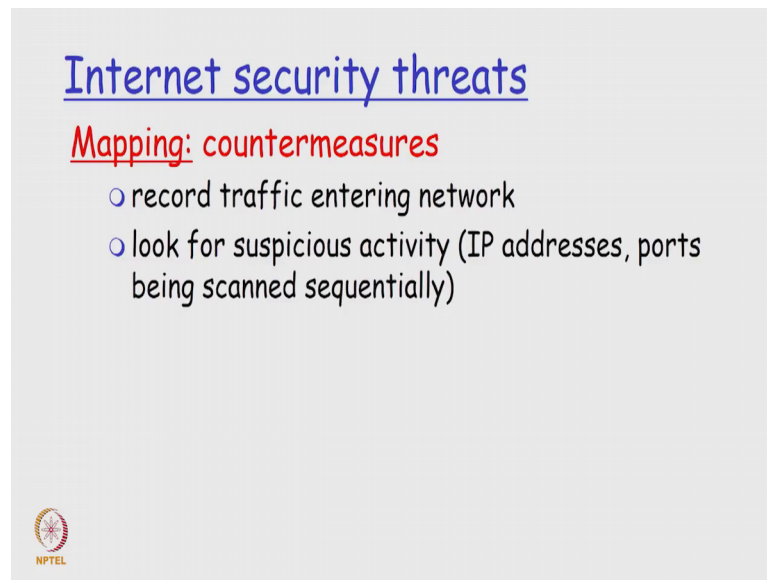
So, by disabling ping nobody can basically go and find out what is happening with the system is alive or dead. By enabling ping an a person who need not know about the network will start knowing more about the network. So, this is this is basically slowly a type of tra[deoff] tradeoff. I hope all of you know what ping is if you do not know please go and Google it for this.

Then once I know that a system exist then I can do something call port scanning. So, for every service, there is a port. So, you are only one Ethernet interface, but you have multiple ports every service is a port. So, what are the services that are open. So, we can actually try to establish say a TCP connection to each port in some sequence and find out which are the ports that are open. So, I will know as a hacker by using ping I know that you exist, and then by trying to establish connections I will find out which are the ports that are open. So, many of the ports are standard ports, and you can basically go to these ports and open them.

Then there is something called nmap mapper, please visit these sites gives you much more about nmap which is actually a network exploration and security auditing type of tool. So, I strongly suggest that you have a look at this nmap. Down the line, we will give you some fe[edback]-feedback about some more insights into the nmap. Now, basically this is the over all modus operandi. So, someone wants to attack a system, they will try to know where the system exi[st] whether a system is exist or not by using ping then they get hold of your IP address then they start doing some port scanning to find out which are all the service that are open.

Then if you have a service which has a vulnerability people then attack through that vulnerability right. So, this is the modus operandi. And now we will see in very very you know very big view on what are the counter measures for these type of threats. These type of what we call as an organised threat. So, there is a procedure involved to basically attack the system.


(Refer Slide Time: 05:18)



Internet security threats

Mapping: countermeasures

- record traffic entering network
- look for suspicious activity (IP addresses, ports being scanned sequentially)



The first thing is that we have to record traffic entering your network and always look for suspicious activities like some IP addresses, some port being scanned sequentially right, so that is one fellow. So, so the main important thing is monitoring. Today I cannot integrate security, I cannot put the security here. So, what I mean is that instead of putting some gate and then lot of locks inside which you should do or you can do, one of the preliminary thing is to put a surveillance camera and see what is happening going inside. So, when you want to secure your house of course, you go and put lock gate so many things, but more importantly if say a very important solution is to put a secure camera outside and always keep watching it, so that is a more you know full proof way of doing it.

So, one of the important countermeasure you need to do is to actually record all the traffic that is entering your network, whether it is certain a simple small LAN level or it is a multi major you know institution or multi major institution distributed geographically or it is a nation itself. So, everywhere we need to have a record of traffic that is entering a network. Once I have that record basically even looking at the metadata, metadata basically is the header etcetera information, we can do quite a bit of significant analysis right is going to be big data, and we can do lot of analysis. And based on that analysis we can do some very quick things as you see in the slide, we can look for suspicious activities like there is an IP address and that IP addresses scanning all the ports one by one why is it doing right.

So, obviously, it is trying to do something with the system. So, these type of analytics real time analytics we can perform on this large data, and basically understand the internet security threat. So, to sum up the internet security threat that is coming from the internet basically has a two step procedure. First, it identifies the existence of your system, it finds the IP, then it scans all your ports and find out what all the services that are open. And if there is some service that is open and then there is a vulnerability there the train attack into the vulnerability.

So, one of the important things the first countermeasure to stop such type of internet security violation is to go and start recording your traffic entering the network and start analysing the traffic. It is not just it is some this disk company being benefited by this, you keep storing say n tera bytes of data without doing anything. Actually have to do something with the data on a real time basis to find out something is going wrong or not. So, this is the first countermeasure. And if you do this at least 90 percent of the problem will get solved, but you have to do it sensibly with direction and focus.

(Refer Slide Time: 08:18)

Internet security threats

Packet sniffing:

- broadcast media
- promiscuous NIC reads all packets passing by
- can read all unencrypted data (e.g. passwords)
- e.g.: C sniffs B's packets

Countermeasures?

NPTTEL

Now, this is basically in some sense it is also called as packet sniffing. What do you mean by packet sniffing like every packet that enters into your network you sniff and take it out. So, this you can it ethical legally you can basically get it out. And if you do it illegally that is what we call it as packet sniff packet sniffing. So, what happens is when I send a packet, it is basically it is on a broadcast media everybody will get it right. And so

when your CPU is in promiscuous mode or in your system is promiscuous mode sorry then what happens see if your system is not in a promiscuous mode right then when I get so let me say my IP addresses p if I get a packet which is not p then basically the network interface card itself will in you know throw it off will reject it. It will not enter the system itself right if the destination address is not p, those packets will not come in. But if I am working in a promiscuous mode, every packet irrespective of my IP address whether it is for me or not will come and fall into the system.

So, so packet sniffing is basically done by having your NIC and your CPU hosts in a promiscuous mode. So, that all the packets none of them will get rejected all will be recorded. Once it is recorded, people can start looking at by software can start looking at the IP address, source address, who is sending all these things. This is good in one way in the sense that if I want to capture all the incoming traffic B analysis for that nothing wrong gets it that is ethical that is legal that is also in the sense this packet sniffing. But then some intruder can also do the same thing without your knowledge and that is illegal right.

So, as you see in this diagram C actually sniffs B's packet. So, B is actually sending something to A through the network, so C actually sits in between and C actually sniffs the B's packet. So, there is something like a man in the middle who is trying to get all the activity that is happening between a B and A. So, how can we stop this packet sniffing. So, let us talk about the internal LAN right and I do not want, so there can be something internally who sniffing all the packets and sending it out, let us assume such a scenario.

So, what we need to do is there should be a software which goes into every system and find out if the system is in promiscuous mode, if the host interface is in promiscuous mode. If it is promiscuous mode then that system will basically act as a sniffer, and then people can hack into that system and take back the values that are going out.

(Refer Slide Time: 11:20)

Internet security threats

Packet sniffing: countermeasures

- all hosts in organization run software that checks periodically if host interface in promiscuous mode.
- one host per segment of broadcast media (switched Ethernet at hub)

The diagram shows a network topology with three hosts: A (server), B (client), and C (sniffer). Host B is sending a packet to Host A. The packet structure is shown as 'src: B | dest: A | payload'. Host C is connected to the same network segment and is sniffing the traffic. An NPTEL logo is visible in the bottom left corner.

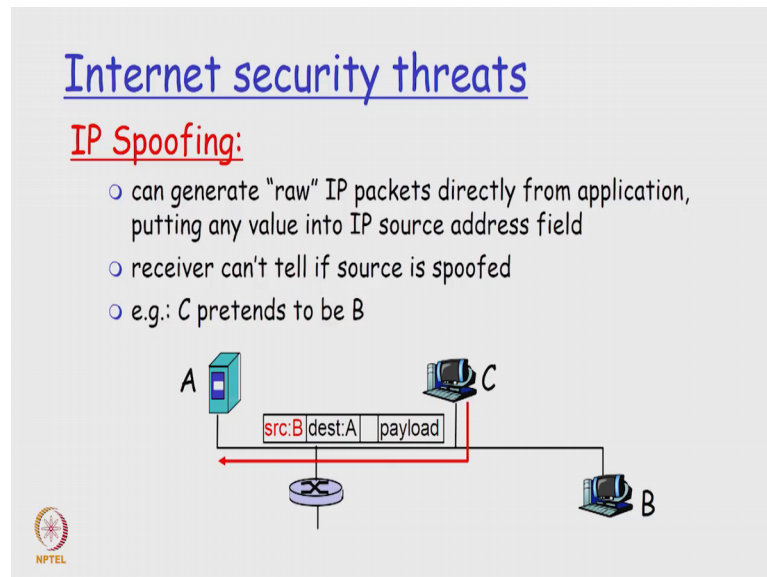
So, all hosts in organisation should run software that periodically check if the host interfaces in pro promiscuous mode. If the ho host interface who will make it promiscuous mode, some third party will come into the system and make it promiscuous mode or any internal person also can make it into promiscuous mode just for sniffing purpose. So, we should have a software that automatically every two to three hours, it should keep checking whether the system has gone into a promiscuous mode if it as gone into promiscuous mode. Immediately we need to stop and change it because it does the potential that it can act as a packet sniffer.

And whenever we are trying to broadcast, we can have something called is switched Ethernet. What is switched Ethernet then one percent can send to all and then when the next fellow wants then it is again next. So, it is not that several fellows try to send to several other fellows at the same point rather than we will have one host per segment of bros broadcast media. So, if you want to send there will be only one fellow who will send, he will finish and then the next fellow will send. So, if multiple fellow will start sending at the same time then there can be issue right. We do not know who is sniffing who we do not know who in the correct one.

The first one is sniffing of course, sniffing is done for even monitoring purposes. Sniffing is also done to basically see that that some level of authenticity in the transactions that are happening. The second important threat that we see here is IP

spoofing. What is IP spoofing? I can generate an IP address which is belongs to somebody else. So, whenever I send a packet I will generate that IP address and put it as a source. So, the so the destination address will think that I am not sending somebody else is sending.

(Refer Slide Time: 13:06)



So, here in case here as you see in the figure C is the intruder B is communicating to A, now, initially it was source B as you see here. But actually C is sending the packet to A B should not send the packet A. Now C is sending the packet to A when the network is free. And then C is sends the packet to A, it makes the source as B as you see here that red colour, it makes the source as B and not as C right, because C is actually sending it, but then it is putting the source as B.

So, as far as A is concerned you will think that the message is coming from B, but the message need not necessarily come from B, it can come from something else and that is what you call as spoofing. Here C has spoofed on behalf of B, C has spoofed as B. So, whatever package C is sending it will tell A I am not sending, B is sending by make making that source has been. So, this is basically called IP spoofing.

(Refer Slide Time: 14:12)

Internet security threats

IP Spoofing: ingress filtering

- routers should not forward outgoing packets with invalid source addresses (e.g., datagram source address not in router's network)

The diagram shows a network topology with a central router. To the left is device A (server), to the right is device B (server), and above the router is device C (laptop). A packet is shown with three fields: 'src: B', 'dest: A', and 'payload'. A red arrow points from device C, through the router, towards device A. The router has a red 'X' over it, indicating it is filtering the packet because the source address (B) is not in its network.

NPTEL

So, how do you address is IP spoofing again I do what we call as ingress filtering. ingress or outgress also. So, whatever comes in have to filter it. What do you mean by filtering? Many times when I want to filter things of course, in the case of IP spoofing have to go filter the top two network. But in general if I want to go and filter a packet especially the payload as you see here, I have to decrypt that payload go and find out if there is same signature inside that somewhere else is there or not. I will to encrypt that the payload and send it back right. So, it involves the decryption of payload also to find out to do ingress filtering specifically when I am looking at application level worms that are injected through emails. So, I need to completely decrypt it, completely analyze it, and that is what I mean by ingress filtering.

So, ingress filtering if I put that filter that means, that this particular system is behaving erratically, so put filter nothing from that communication will reach. If that is the case then the router should not forwarded outgoing packets with invalid source addresses right, so that is what happens when we start doing the ingress filtering and the aftermath of data.

(Refer Slide Time: 15:28)

Internet security threats

Denial of service (DOS):

- flood of maliciously generated packets "swamp" receiver
- Distributed DOS (DDOS): multiple coordinated sources swamp receiver
- e.g., C and remote host SYN-attack A

Countermeasures?

NPTEL

Finished is of course, we have been talking about which we call as denial of service where you know multiple the SYN is a package. So, if multiple SYN packets are generated that go and flood the network and flood it and reach. For example, I want to do distributed denial of service at a denial of service attack on A, so C actually sends lot of packets which actually is originated towards A.

And, so when B wants access A as you see in the figure B is the genuine you know system which wants access to A, when B wants to access A, then what happens B cannot access A because C is taken up all the resources by pumping useless packet to A. And a had to accommodate it for some time till it completely you know understands that C has done it, and it has to block C. Till it block C this SYN packet should be less going to A and B will not get access to A. So, this is another very interesting important way of attack call dos denial of service. I am denying the service of A to the network by blocking it by pumping it with useless packet.

(Refer Slide Time: 16:48)

Internet security threats

Denial of service (DOS): countermeasures

- filter out flooded packets (e.g., SYN) before reaching host: throw out good with bad
- traceback to source of floods (most likely an innocent, compromised machine)

NPTEL

So, again even for this the way is to filter out flooded packets it is SYN before reaching host and trace back to source of flood that is also very important. One is first detecting and stopping; and thus the second think one thing is to detect and you know safeguard your system, safeguard your router from getting all this junk packages. The next thing is of course, tracing back and going to the original source where that guy is originating the packet. So, both are very very important when we are trying to handle denial of service.

(Refer Slide Time: 17:21)

Secure sockets layer (SSL)

- transport layer security to any TCP-based app using SSL services.
- used between Web browsers, servers for e-commerce (https).
- 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.

NPTEL

And many times today between any two points in the communication in the in many of the infrastructure IT infrastructure communication goes to something called a secure socket layer SSL. So, these are all the features of this is SSL. So, let me just go through one by one. On these five features the first feature is that the transport layer security to any TCP based app using SSL services ok. So, the mom moment I have this secure sockets layer, I have the certification for that then `my transport layer essentially become secure. The second thing is there this SSL is used to between web browser, service for e commerce lot of use of SSL is that and what SSL gives you is basically the authenticity that this is the fellow this is against IP spoofing.

So, what are the security services reaches SSL gives you it gives you server authentication, it gives you data encryption, it also gives you client authentication. What do you mean by server authentication SSL enabled browser in includes public keys for trusted CAs. browser request server certificate and is issued by a trusted CA, and browser uses CA's public key to extract service public key from certificate. So, all these thinks are basically ensures that a server is a indeed authenticated by using this SSL.

Now, you can actually check your browser security level by clicking on this trusted CAs website. So, the sum up SSL actually becomes a very very nice platform for ensuring security specifically on the home ground network. And this SSL is basically commonly used between applica[application] different web servers and ecommerce. And it gives you the server authentication it gives you data encryption, and also gives you client authentication if needed.

So, that are SSL enable browser that include public keys as I mentioned just earlier. And then the browser also uses CA's public key to extract sever public key from certificate. So, these are some of the very interesting things that we would like to basically cover in the session. So, what you have seen so far is the type of attacks that could happen, and one such as such type of attacks happen, what is the forensic type we need do, and we got some very good deep inside in this lecture. We will we will meet in the next session.

Thank you.