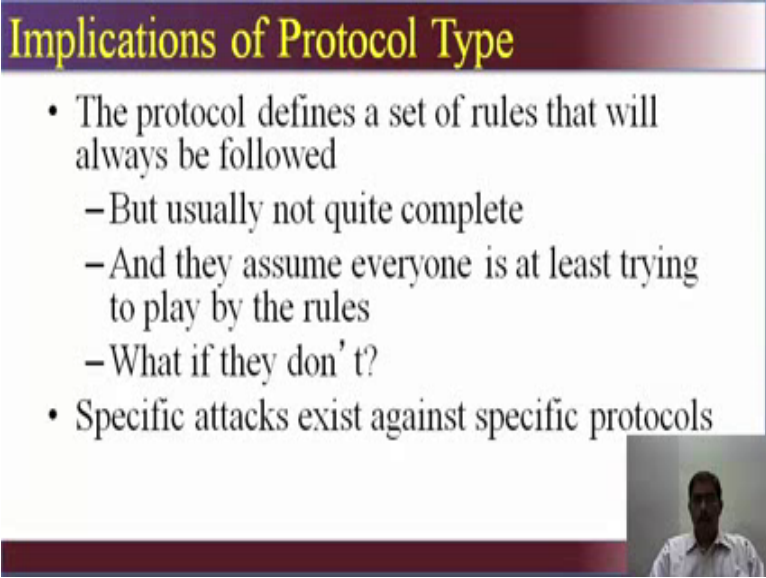


Introduction to Information Security
Prof. Dilip. Ayyar
Department of Computer Science and Engineering
Indian Institute of Technology, Madras

Lecture – 44

(Refer Slide Time: 00:10)



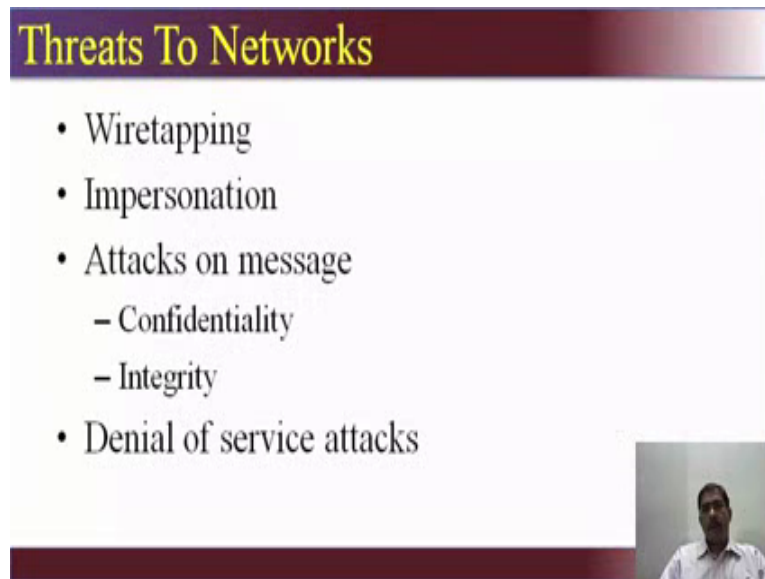
Implications of Protocol Type

- The protocol defines a set of rules that will always be followed
 - But usually not quite complete
 - And they assume everyone is at least trying to play by the rules
 - What if they don't?
- Specific attacks exist against specific protocols

Video inset of Prof. Dilip. Ayyar


Let see what are the implications of the protocol type. The protocol has a basic set of rules as that should be followed and that will always be followed, but it is usually not complete and the protocol assume that everyone trying to play by the rule. What if they don't play by the rules? There are specific attacks against specific protocols; vulnerability in HTTP protocol, in ssl, in ssh. So, there are vulnerabilities or specific attacks against specific protocols.

(Refer Slide Time: 00:46)



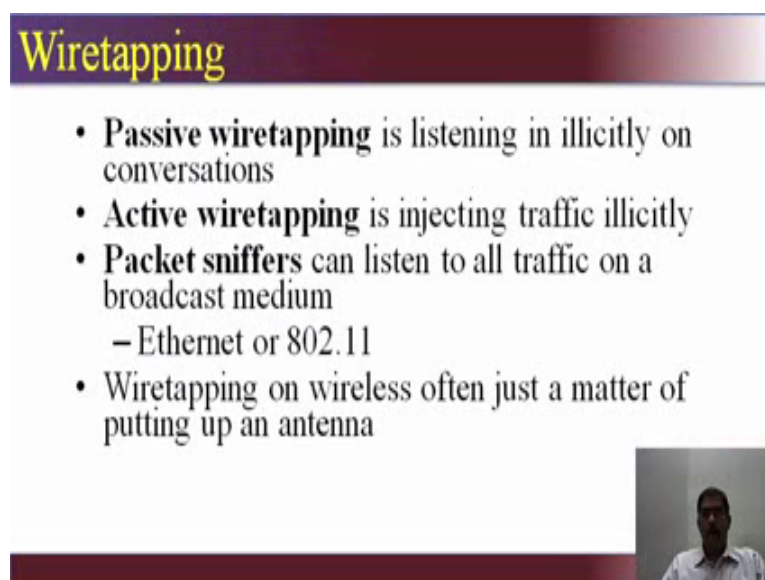
Threats To Networks

- Wiretapping
- Impersonation
- Attacks on message
 - Confidentiality
 - Integrity
- Denial of service attacks




There are several threats to networks some them have been discussed wiretapping is one, impersonation, attacks on the messages which is confidentiality and integrity and a denial of service. If you see here, all of confidentiality, integrity and availability or loss a confidentiality, integrity and availability affect the network.

(Refer Slide Time: 01:13)



Wiretapping

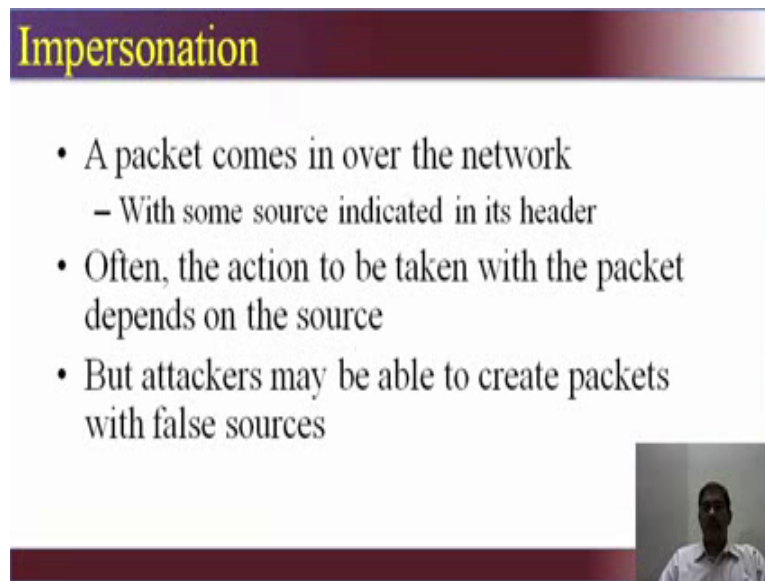
- **Passive wiretapping** is listening in illicitly on conversations
- **Active wiretapping** is injecting traffic illicitly
- **Packet sniffers** can listen to all traffic on a broadcast medium
 - Ethernet or 802.11
- Wiretapping on wireless often just a matter of putting up an antenna



In wiretapping, there are two types, passive and active. What is passive, passive is listening in illicitly on conversation; like your traditional wiretapping on the telephone lines. And active wiretapping is injecting traffic illegally and illicitly within the network.

Packet sniffers can listen to all traffic on a broadcast medium on a internet or an 802.11, which is a wireless one ; an example packet sniffers is wireshark, which is the most popular. Then wiretapping on wireless also to the just a matter of putting up an antenna what happens there have been several instances where people with powerful antenna connected to the laptop, drive around places where wireless network is available, try to hack into the network using the tools like thi one and then try to getting to the network.

(Refer Slide Time: 02:24)



Impersonation

- A packet comes in over the network
 - With some source indicated in its header
- Often, the action to be taken with the packet depends on the source
- But attackers may be able to create packets with false sources


Video inset showing a man speaking.

A simple explanation of the impersonation is a packet comes in over the network with some kind of source indicated in the header. Now the action to be taken with the packet depends on the source what is to be done with the packets. But attackers may be able to create packets with false sources. Now packet is nothing but your data this broken down into pieces with adding certain information. In the packet that reach the designation are reassembled to give the actual message. So, attackers may be able to create packets with a false sources indicating that it is not coming from the original in the intended or original location.

(Refer Slide Time: 03:14)

Violations of Message Confidentiality

- Other problems can cause messages to be inappropriately divulged
- Mis-delivery can send a message to the wrong place
 - Clever attackers can make it happen
- Message can be read at an intermediate gateway or a router
- Sometimes an intruder can get useful information just by traffic analysis




How is the confidentiality of the message validated? There are problem can cause message to be inappropriately divulged. Mis-delivery or non delivery both can be and issue. Here, mis-delivery can send the message to the wrong place. So, clever attackers can make it happen. Message can be read at an intermediate gateway or a router sometimes an intruder can get useful information just by traffic analysis by using tools like wireshark; he may be able to know the pattern of traffic that is going there, what kind of messages are going there, what actually is going back and forth on the network.

(Refer Slide Time: 03:55)

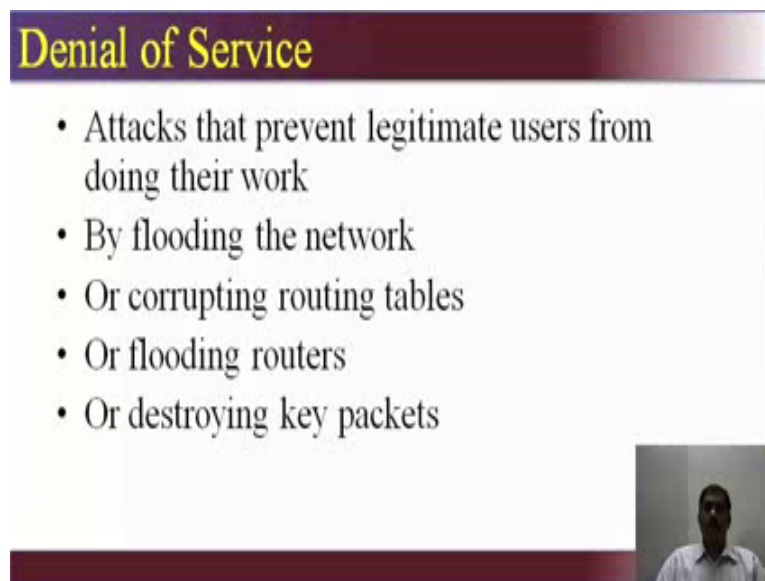
Message Integrity

- Even if the attacker can't create the packets he wants, sometimes he can alter proper packets
- To change the effect of what they will do
- Typically requires access to part of the path message takes



How is integrity effected; even when the attacker cannot create the packets that he wants, sometimes he can alter the proper packets that means, velocity of the data being transmitted is effected. Why?To change the effect of what the packet will do and also it requires access to the part of the path of the message takes. So, the attacker will require part of the path that the message takes to affect the integrity of messages being transmitted.

(Refer Slide Time: 04:30)



Denial of Service

- Attacks that prevent legitimate users from doing their work
- By flooding the network
- Or corrupting routing tables
- Or flooding routers
- Or destroying key packets

A small video inset in the bottom right corner shows a man in a light-colored shirt speaking.

Perhaps has the most common attacks on the network is the denial of service. They are attacks that prevent the authorized users from doing their work. It can be flooding the network by sending in a lot of request to the server so that they cannot handle it any more or corrupting routing tables or flooding router itself by sending in a large number of packets or even destroying key packets on the way to its destination. So, all this can cause denial of service attack.

(Refer Slide Time: 05:05)

How Do Denial of Service Attacks Occur?

- Basically, the attacker injects some form of traffic
- Most current networks aren't built to throttle uncooperative parties very well
- All-inclusive nature of the Internet makes basic access trivial
- Universality of IP makes reaching most of the network easy



How does denial of service attack happens? Basically the attacker injects some form of traffic. Nowadays the networks aren't built to throttle uncooperative parties very well. So, and the all-inclusive nature of internet makes basic access trivial because we know that the common protocol used is TCP IP. So, the first step is already there. And then universality of IP makes reaching of the network easy and again like I said and since the IP is the most common or preferred mode of communication, reaching most network is pretty simple.

(Refer Slide Time: 05:44)

An Example: SYN Flood

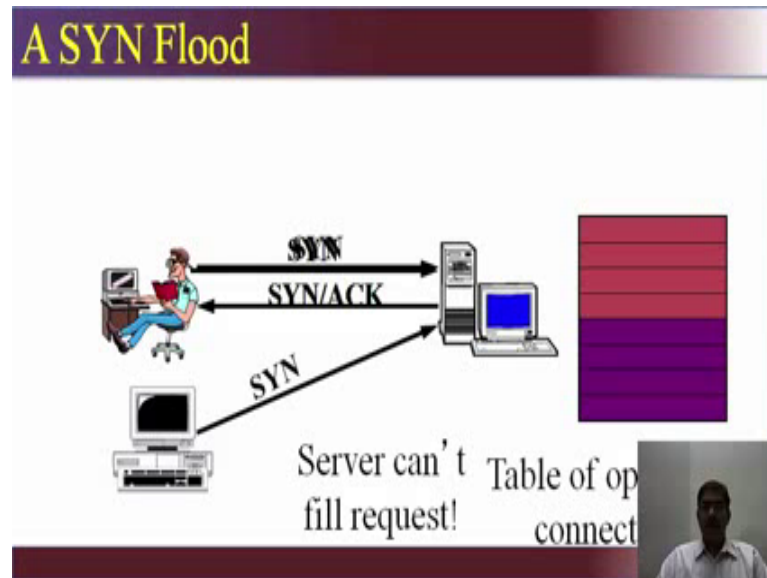
- Based on vulnerability in TCP
- Attacker uses initial request/response to start TCP session to fill a table at the server
- Preventing new real TCP sessions
- SYN cookies and firewalls with massive tables are possible defenses



Now, let us see an example of SYN flood. It is based on vulnerability in TCP that is transmission control protocol. The attacker uses initial request response to start TCP

session to fill a table at the server. What it basically does it prevent new real TCP session. SYN cookies and firewalls with massive tables are the possible defenses.

(Refer Slide Time: 06:14)




Let see graphically what exactly happens in a SYN flood. In a normal SYN behaviour the client on the left sends SYN packet to the server the server acknowledges with the SYN ACK packet and the client responds to ACK packet. So, SYN SYN ACK and ACK this is basically the TCP prevail hand sheets, so this is normal SYN behaviour. Now let see how a SYN flood will happen. . The attacker sends a SYN, server responds with a SYN ACK, the attacker again responds to the SYN, that is the double one on top and then somewhere else the attacker sends another SYN . So, the server cannot actually fill that request. So, what basically happens is the server gets flooded with the requests, a SYN flood happens.

(Refer Slide Time: 07:08)

General Network Denial of Service Attacks

- Need not tickle any particular vulnerability
- Can achieve success by mere volume of packets
- If more packets sent than can be handled by target, service is denied
- A hard problem to solve




So, people general network denial of service attacks; it need not tickle any particular vulnerability I mean denial of service attacks need not tickle any particular vulnerability. It can happen to any system. . It can achieve success by mere volume of packets if more packets are sent than that can be handled by the target, then the service is denied. It is hard problem to solve.

(Refer Slide Time: 07:35)

Distributed Denial of Service Attacks

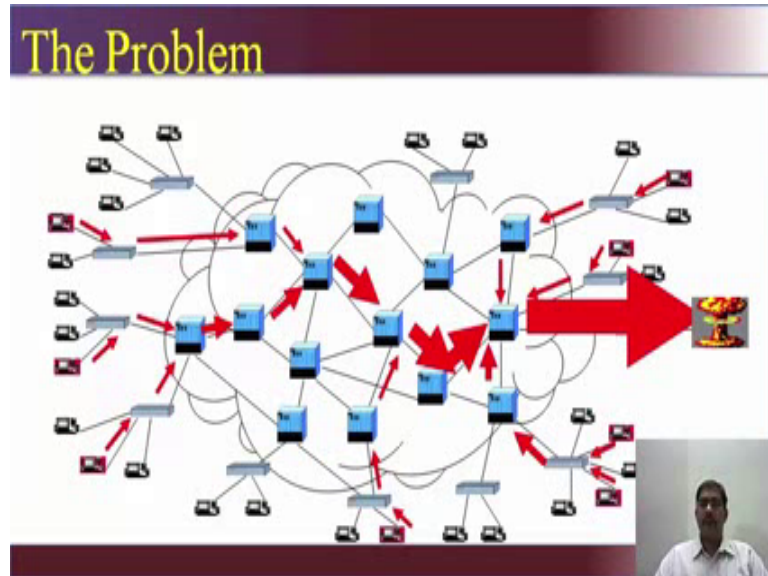
- Goal: Prevent a network site from doing its normal business
- Method: overwhelm the site with attack traffic
- Response: ?



Then, DDOS or the distributed denial of service attack. The main goals to prevent a network site from doing its normal business; the method is overwhelm the attack traffic

from different sources, from distributed sources. While the response I mean the server will not be able to process that information and denial service attack will happen.

(Refer Slide Time: 07:57)



This is an example of denial of service attack. The problem is there are several computers coming in or attacking the server on several sources, different geographical locations, not necessarily within the network, the inundates the network of the server with so much of traffics that the server cannot respond, and the denial of service or distributed and denial of service condition occurs.

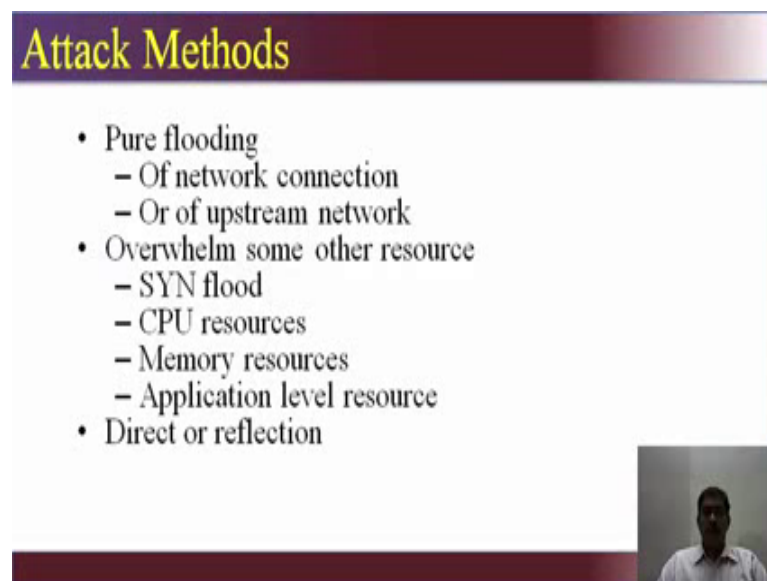
(Refer Slide Time: 08:26)

Why Are These Attacks Made?

- Generally to annoy
- Sometimes for extortion
- Sometimes to prevent adversary from doing something important
- If directed at infrastructure, might cripple parts of Internet

So, why do people do these attacks, why are the attacks made. Generally, to annoy. It sounds rather silly, but that is a thought for this. Sometimes for extortion, sometimes to prevent adversary from doing something important. If it is directed you can infrastructure might cripple parts of internet also. Say foreexample it is directed at an e-commerce site, a popular e-commerce site like ebay or amazon or flipkart, then it might cripple parts of internet of if it is a banking site it my again cripple parts of the internet. So, the attacks of made for generally to annoy, just to bring down the network, fun of it or ego then for extortion. So, if you don't pay the money, I will bring a network then it something to prevent adversary from doing something important may be two parties different parties are trying for a tender which is very important. And one of them capability of doing the DOS attack and he tries to prevent the other person from competing the tender by creating a DOS attack on his network; that could be an example.

(Refer Slide Time: 09:42)



Attack Methods

- Pure flooding
 - Of network connection
 - Or of upstream network
- Overwhelm some other resource
 - SYN flood
 - CPU resources
 - Memory resources
 - Application level resource
- Direct or reflection

The slide features a dark red header with the title 'Attack Methods' in yellow. The content is a bulleted list of attack methods. A small video inset in the bottom right corner shows a man in a white shirt.

There are different methods of attacks, one is pure flooding of the network connection. We have flooding of upstream network or overwhelm some of their resources. Eat up their CPU resources eat up the memory, cause an inflect to happen or ieat is up or application level resources, it could be any of the method they can be used. It can be a direct DOS as the reflected DOS.

(Refer Slide Time: 10:10)

Why “Distributed”?

- Targets are often highly provisioned servers
- A single machine usually cannot overwhelm such a server
- So harness multiple machines to do so
- Also makes defenses harder



But why distributed attack because targets are often highly provisioned sources. So, now a days the computers of the servers which handle the sites are highly efficient were tremendous processing powers, tremendous memory and a large storage space. So, you need to have aa distributed attack because one or two systems on the internet will not cause the server to come down. So, that covers the next sentence, a single machine usually cannot overwhelm such a server. So, unit multiple machine to do so, so it could be that each of the computer identified by the hacker could be a zombie or it could be a part of the botnet.

(Refer Slide Time: 11:12)

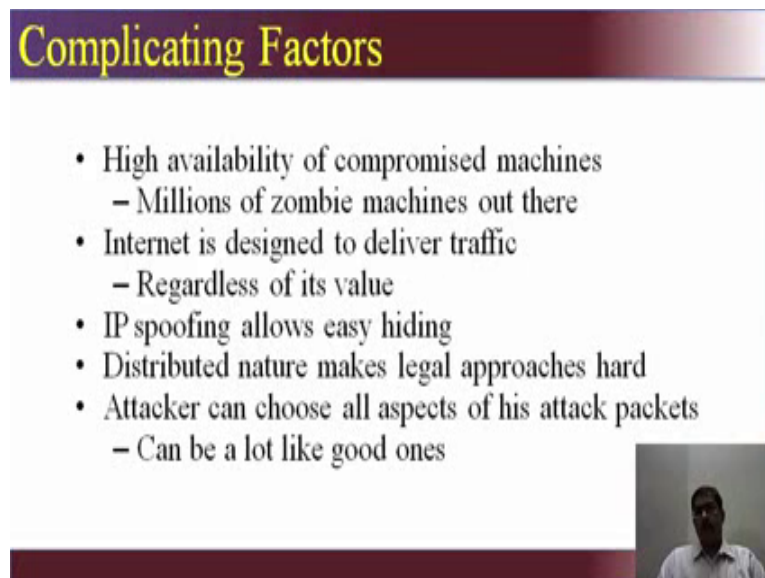
How to Defend?

- A vital characteristic:
 - Don' t just stop a flood
 - ENSURE SERVICE TO LEGITIMATE CLIENTS!!!
- If you deliver a manageable amount of garbage, you haven' t solved the problem
- Nor have you if you prevent a flood by dropping all packets



So, then all of these do of concerted attack on the server then it makes a defence also harder because you don't know where actually the traffic is coming from becomes from everywhere. So, how you defend this kind of incidents. One is you can't just stop of a flood; you have to just ensure that if services to legitimate authorised clients are given. If you deliver a manageable amount of garbage you have not solved the problem that means, you can't give an information in piece meals. The information that is available to the authorised users should be legitimate. It should be in full, in toto. Nor have you if you prevent a flood by dropping all packets. So, the drop all packets then more even the authorised packets will be dropped.

(Refer Slide Time: 11:58)



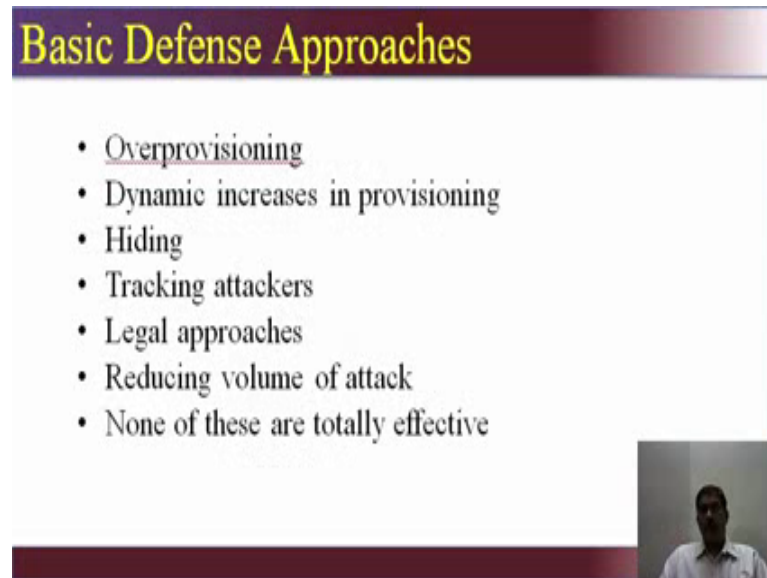
Complicating Factors

- High availability of compromised machines
 - Millions of zombie machines out there
- Internet is designed to deliver traffic
 - Regardless of its value
- IP spoofing allows easy hiding
- Distributed nature makes legal approaches hard
- Attacker can choose all aspects of his attack packets
 - Can be a lot like good ones

It is a no use for the authorised users. There are complicating factors; it is the high availability of the compromised machines that is there are millions of zombie machine out there. Its a part of your botnet. internet is designed to deliver traffic regardless of its value. So, take first small informative site to site hosted for bank to an internet banking site to e- commerce site. So, everything goes through the internet regardless of value internet banking will be valued much higher because financial transactions are happening. A static site will be value lower because of the static contents or the informative content which is any way meant for the general public and so forth. Then IP spoofing allows easy hiding spoofing is you are actually the IP spoofing is you tender a source address in a pop in a header for the purpose of masquerading or hiding or real IP, so that source of packet will not be found. Then the distributed nature makes legal

approaches hard; now if there is a pack coming from a foreign country how do you take action against the perpetrators. It becomes a legal issue also unless there is a co-operative agreement between the two countries, it can't be done. . Then attackers can choose all aspects of his attack packets; that means, a lot of packets can be like the good packets with no receivable differences.

(Refer Slide Time: 13:47)



Basic Defense Approaches

- Overprovisioning
- Dynamic increases in provisioning
- Hiding
- Tracking attackers
- Legal approaches
- Reducing volume of attack
- None of these are totally effective

so that it become very difficult identify which is the packet, and which is true packet. Some of the basic defence approaches are over provisioning which is not actually a good idea, dynamic increase in provisioning moderately. It is the resources. Then hiding tracking the attackers taking legal approaches reduce volume of attack by putting some kind of filters.

(Refer Slide Time: 14:14)

Traffic Control Mechanisms

- Filtering
 - Source address filtering
 - Other forms of filtering
- Rate limits
- Protection against traffic analysis
 - Padding
 - Routing control



But none of these are totally effective, but there are traffic control mechanisms, like the filtering where the source address filtering can happen. So, if my packet is not from sources, drop it. Other forms of filtering are there, that limits some rates of transmission that can happen. Protection against traffic analysis of traffic padding you will discuss of traffic padding then routing control is the. So, padding actually involves having of sending a lot of packets, encrypted packets along with your genuine traffic. So, because difficult for anyone to identify whether traffic is coming in. So if there are a lot of encrypted traffic going by the during traffic padding, a continuous stream of encrypted padding also goes with network. So, if that is an attacker sitting somewhere in AP, is trying to beat out the traffic analysis or he is trying to get the analysis or pattern, it becomes difficult to find out because of a lot of useless encrypted data is also sent it in the network.

(Refer Slide Time: 15:34)

Source Address Filtering

- Filtering out some packets because of their source address value
 - Usually because you believe their source address is spoofed
- Often called ingress filtering
 - Or egress filtering . . .



So, analysis of the traffic itself becomes very difficult. Then there is source address filtering, it is basically filtering of some packets because of their source address value like I said before. So, if you say that the network should not accept packets from this range to this range, drop the packets. . Usually because you believe their source address spoofed, it is often called ingress filtering there is also egress filtering, where you can prevent the destination address filtering from your network. (Refer Slide Time: 16:06)

Source Address Filtering for Address Assurance

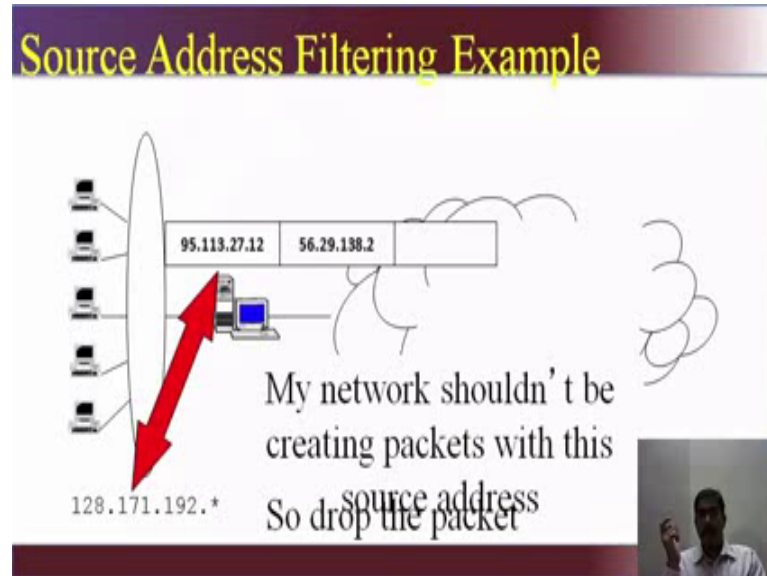
- Router “knows” what network it sits in front of
 - In particular, knows IP addresses of machines there
- Filter outgoing packets with source addresses not in that range
- Prevents your users from spoofing other nodes’ addresses
 - But not from spoofing each other’s



Source address filtering is basically used for address assurance that is router knows what network it sits in front of in particular it knows IP addresses of machines that it is interacting with. It filters outgoing packets with source addresses not in that range. So, it

filters outgoing packets; the filters which is not in that range set in a router and it prevents your users from spoofing other nodes addresses.

(Refer Slide Time: 16:45)




But within the network the clients can spoof each other addresses that is possible. This is the simple example of source address filtering. Now my network should not be creating packets with this source address the source is the address like 128.12.., which is not there in the address filtering.

(Refer Slide Time: 17:04)

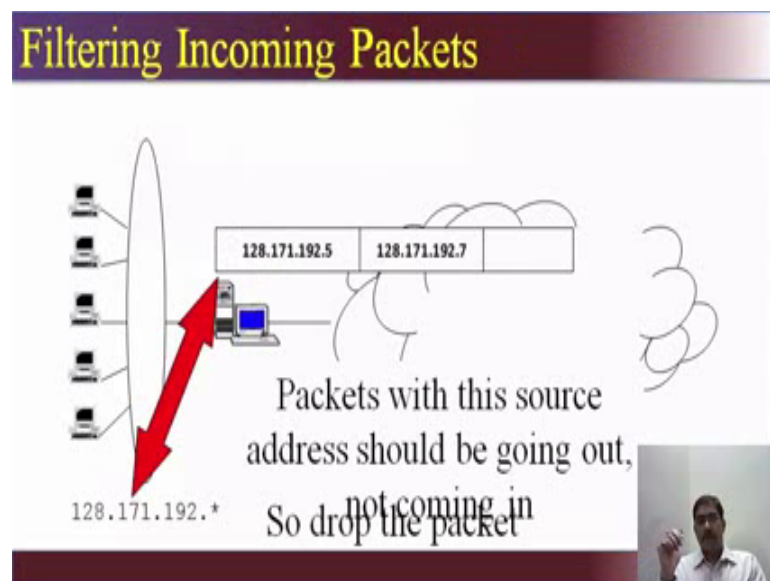
Source Address Filtering in the Other Direction

- Often called egress filtering
 - Or ingress filtering . . .
- Occurs as packets leave the Internet and enter a border router
 - On way to that router's network
- What addresses shouldn't be coming into your local network?



So, drop the packet; it is a very simple example of how source address filtering happens. The outbound is called egress or ingress is that comes in. So, it occurs as packets leave the internet and enter a border router. So we are looking at both sides. One is egress, the packets going out of the network and going into other network. Now it occurs as packets leave the internet and enter a border edge router on the way to that router's network. Now, it determines what addresses should not be coming into your local network. So, egress is you sent a packets out; the router at other end does the ingress filtering, determines whether this packets can come in, if it is not in the list, it drops the packets.

(Refer Slide Time: 17:53)



An example of this the filter incoming packets, packet with this address should be going out, it should not coming in so your drop the packet. So, the simple example of how the incoming packets of filter, so a particular source occurrence is there. So, in the network it is configured that these packets should be going out and not coming in; since, it is coming in, it drops the packets.

(Refer Slide Time: 18:30)

Other Forms of Filtering

- One can filter on things other than source address
 - Such as worm signatures, unknown protocol identifiers, etc.
- Also, there are unallocated IP addresses in IPv4 space
 - Can filter for packets going to or coming from those addresses
- Some source addresses for local use only
 - Internet routers can drop packets to/from them



There are other forms of filtering, that is you can filter out things other than source address such as worm signatures unknown protocol identifiers and so many other things. So, if there is a worm that is coming in you can filter based on the type of this worm come in. So, you can say basically, the rules will say, anything in the database which resembles in the worm database which we have, if there is any packet resembles that of a worm signature drop it. Also there are unallocated IP addresses in IP v 4 space which is now this I P v 6is coming to. So, it can filter for packets going to or coming from these addresses where unallocated addresses then some source addresses for local use only. So, internet routers can drop packets to them or from them now when you talk about network also we need to understand what a class A network class B network class C network what is the loop bag address, if you can write it down go to the internet, it is the part of your CCNE basics. So, you can actually go to Google find out what is the class A, class B, Class C network, look bag address what is ARP, what is RARP.

(Refer Slide Time: 19:56)

Realistic Limits on Filtering

- Little filtering possible in Internet core
 - Packets being handled too fast
 - Backbone providers don't want to filter
 - Damage great if you mess it up
- Filtering near edges has its own limits
 - In what's possible
 - In what's affordable
 - In what the router owners will do



What are the different protocols used in the network. You can learn about that. But we have realistic limits on filtering also. Little filtering is possible in internet;so internet is meant to be a repository of information sharing. So, you can't filter out everything with that. And packets go packets go very fast and your backbone providers may be a service provider do not want to filter for obviously reasons, unless there is a regulatory requirement that this, this sites should be blocked, they dont generally block. Now if filtering is not done properly damage will be great. So, that is another issue and filtering near the edges that is the border or the perimter of a network has its own limits, in what is possible what is observable and what the router owners also will do. You can put abundance of protection in the network or the perimeter of the network which is highly unaffordable to you.