Cloud Computing
Prof. Soumya Kanti Ghosh
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

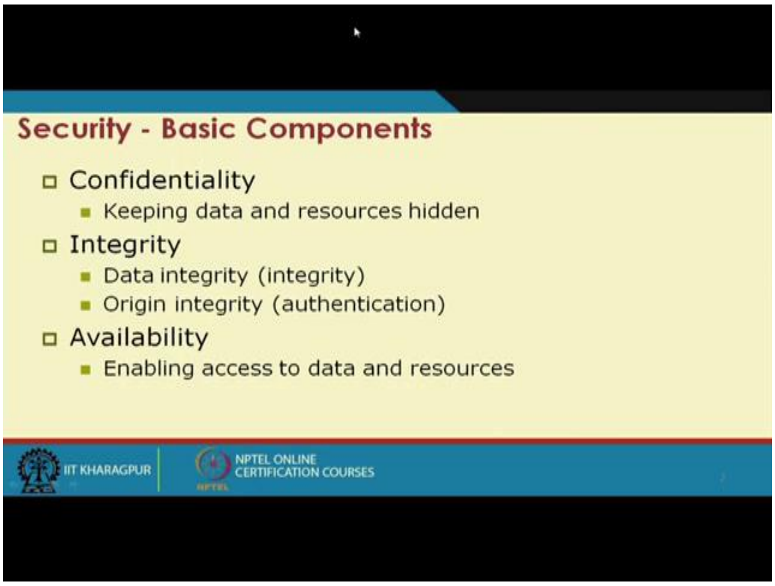
Lecture - 26
Cloud Security – I

Hi. We will be continuing our discussion on Cloud Computing. Today we will be discussing on another major aspect of this cloud computing which is which we can say Cloud Security. So, we will talk we will try to have a brief overview of the security parts say, and how this security affects cloud computing. As we all understand that when we go for cloud computing whether it is the infrastructure as a service a platform as a service or software as a service or anything as a service, what we are relying on a third party service provider.

So, our application data processes are running on some third party. So, whenever it is running on third party the security becomes a issue specially that what is the availability, where my data is stored whether it is been seen or intercepted by my some other parties, and those concerns will be there and specially if this is a mission critical operations or mission critical data or some critical data like banking data, defense data even academic data related to students results and other things. This needs to be looked into in a in a various serious person.

We will see in the course of the things that one of the one of the major hindrance towards going towards this cloud is more than technology, rather more this concern about security what will be the policies what data policy etcetera and so on and so forth. So, with this we will start our thing, but before going to that I thought that it will be quick brush up of what do you mean by security, in terms of when we talk about computer security or information security or network security. So, what are the different aspects are, there it is likely that all those aspect in some form of other will be also reflected in the cloud, but the concern may be different. So, before going to the cloud security part say we will see security in general for any computing service computing and networking service ok.

(Refer Slide Time: 02:36)



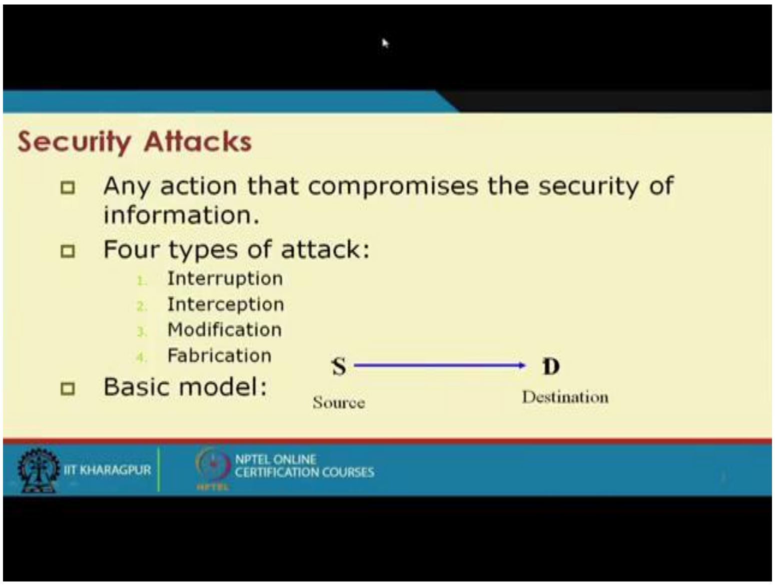
Security - Basic Components

- Confidentiality
  - Keeping data and resources hidden
- Integrity
  - Data integrity (integrity)
  - Origin integrity (authentication)
- Availability
  - Enabling access to data and resources

So, if we look at security what are the 3 basic components one is the confidentiality integrity and availability right. This is what we say CIA components right. Confidentiality deals with keep keeping the data and resources hidden that you do not know that where the data is that it is confidential, integrity is that data integrity is maintained like or origin or the source integrity is mentioned, may maintained right. Like So that whatever I sent from a to b; b receives the same thing or that integrity or authentication of the source that, I am getting from the itself it is there and availability in happening access to the data and resources there is another important component right.

So, that is what we see that most of the attacks are going as denial of services where the availability is compromised. So, everything is fine, but finally, you do not have the resource at your hand. So, it is some sort of a dos or sometimes the ddos type of attacks.

(Refer Slide Time: 03:43)



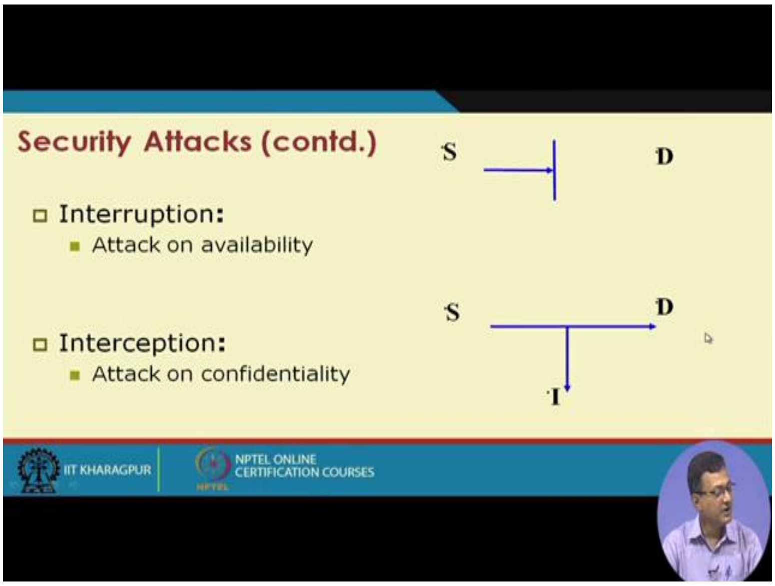
Security Attacks

- Any action that compromises the security of information.
- Four types of attack:
  1. Interruption
  2. Interception
  3. Modification
  4. Fabrication
- Basic model:

So, any security attack on the other say that any action that compromises the security of the information, or any action which violates the CIA type of things there is basic premise right. There are lot of other components we will see.

So, if we look at there are immediately it will come up that there are typically 4 type of things maybe there, one is inter interruption, one is interception, modification, fabrication. So, this 4 components more or less encompasses or combination of this more or less or it encompasses all type of things, which are which are compromised during a attack. So, our basic model is a source sending a data to a destination, and when we talk a talk about interruptions.

(Refer Slide Time: 04:31)

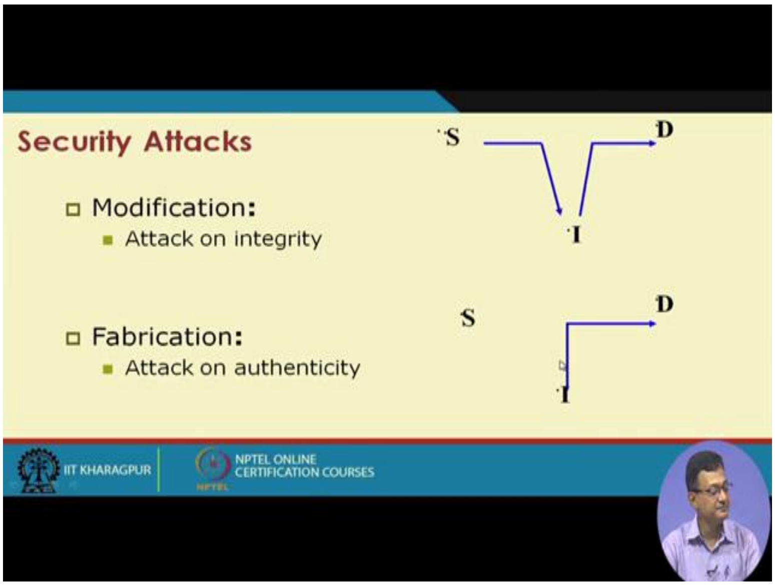


Security Attacks (contd.)

- □ Interruption:
  - Attack on availability
- □ Interception:
  - Attack on confidentiality

So, that a the message or the communication path is interrupted. It can be interception that the goes from source to destination, but somebody else also intercept and listening to the thing.

(Refer Slide Time: 04:47)



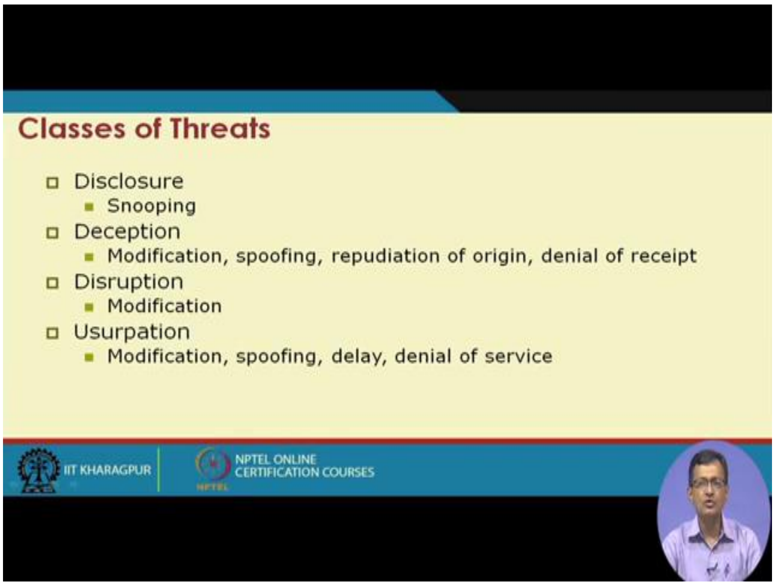
Security Attacks

- □ Modification:
  - Attack on integrity
- □ Fabrication:
  - Attack on authenticity

So, this is attack on availability this availability is block this is attack on confidentiality like you are sending from a to b or s to d and somebody else, that intruder I is listening to that it can be attack on modification, that this attack on integrity of that data right; so or even the origin right. Source is sending to d, but in between there is a intruder I which intercept the message changes the message and send it to d. So, d for d it is a message coming from s and the message am has been changed to am dash, but still the for d it is it is the message which is send which has been send or which has been forwarded by sources.

So, that is a attack on integrity. So, there can be attack on authenticity right. I pretend or intrude are pretend to be the sources right. And; so it is attack on authenticity. So, I need to authenticate who is my source. So, before receiving a message I need to know that I am supposed to receive from a authenticated source is, and I am receiving those message. So, that is a attack on authenticity or what we say fabrication.

(Refer Slide Time: 06:04)



Classes of Threats

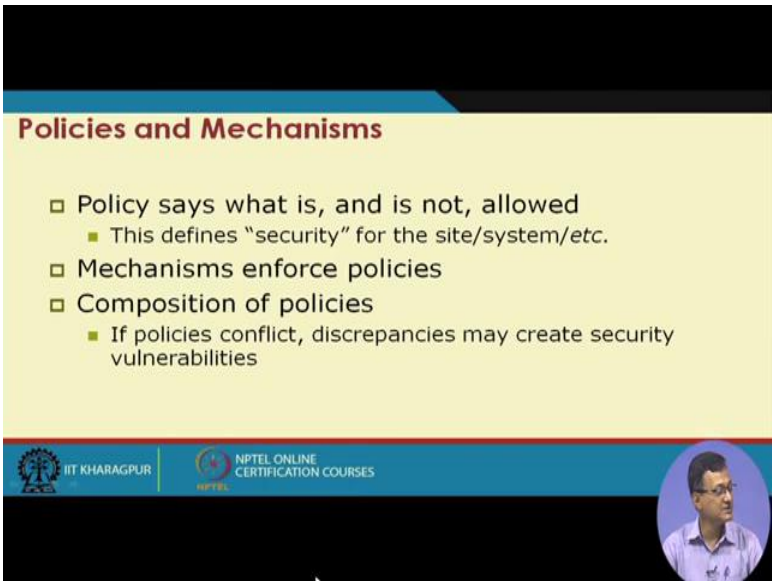
- Disclosure
  - Snooping
- Deception
  - Modification, spoofing, repudiation of origin, denial of receipt
- Disruption
  - Modification
- Usurpation
  - Modification, spoofing, delay, denial of service

Now so, one side we see that the major security components other side that the type of attacks which can be there what a and if you look at these are this can this is true for whether it is a computer security. Or a information security or network security or cloud security right. They it may have different type of characteristics and manifestation nevertheless it has the same type of what we say same type of problems, or same type of security issues realizes.

Now, if you look at that what are the threats right. So, threats does not mean it is attacked right. So, it is like vulnerability does not mean that it is compromised, but these are the possible threats. So, classes of threats one is a threat of disclosure right. So, I have a threat of disclosure like what which is type of in the attack what we say snooping. So, threats of deception like modifications spoofing repudiation of origin denial of receipt and type of things. So, this is a threat of deception.

So, there can be a threat of disruption that is if it is a modified in the threats of disruption service, and another is a threat of usurpation, that is modification spoofing delay denial of services.

(Refer Slide Time: 07:38)



Policies and Mechanisms

- Policy says what is, and is not, allowed
  - This defines "security" for the site/system/*etc.*
- Mechanisms enforce policies
- Composition of policies
  - If policies conflict, discrepancies may create security vulnerabilities

So, these are these are different category of threats which are there. So, we have attacks which have security concerns and threats these are different components. Overall whenever a whenever a it systems or any information system whether it is organizational or it is personal or it is inter organization intra organization, whatever there are guided by policies and mechanisms very tricky issues. So, policy says what is what is not allowed right.

So, the policy says that what is allowed what is that not allowed right. So, it is it tries to do it in a fashion that which of the things can be allowed and things there can be hierarchical to a way of defining policies. There can be different way of things we are not going to that. So, this defines the security of the site systems overall information structure, a overall network access protocol and individual to group to distributed anything right. So, there is policies usually in organizations policies are made somewhat centralized. In the sense it has been formulated across the for all components of the organizations and it is something a sort of a policy making body does it.

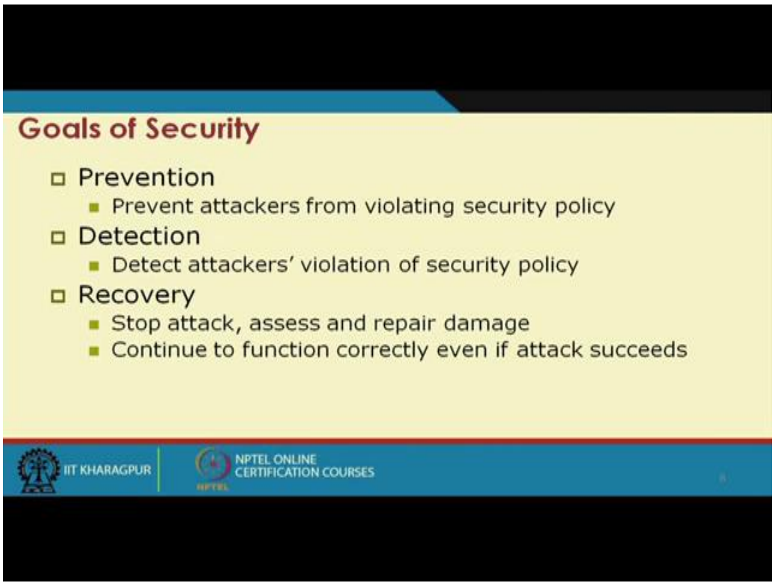
Now, incidentally the implementation is most of the time distributed. Like I say that I have a I have this IIT Kharagpur network. So, there are several departments there as a several sub networks there are several layer 3 plus layer 3 and layer 3 plus type of switches. So, it says they policy that this way the traffic will go and etcetera etcetera, and not only that they are additionally there are also presidents etcetera. At the same time this policy need to be implemented across this different category of devices. So, the implementation is often in a distributed fashion or in different devices and type of things where the. So now, there is a big challenge the how to guarantee this implementation conform to the policy one to one right. It is nothing more or less what the policy defines.

So, there is a these are some open not exactly open problem these are very strong research problem across the world that how to how to formally say that your implementation and policy match with each other and so forth. Now so, policies says what is and what is not allowed, where I on the other hand mechanisms enforce policies right. So, I have mechanism to enforce policies. So, composition of policies if the policy is conflict discrepancies may create security vulnerabilities.

So, there is another things, if it is if when we compose policies. So, if I have several policy and composition of the policies if there are conflicts, discrepancies may arise and then the there can be security vulnerabilities. Like I can say that one policy says that this traffic can be allowed or another policy said that this category of traffic should be denied, and you see there is a overlap that which can be either allowed or denied you need to decide right. This mainly happens because number of cases this implement is in a distributed way. And if sometimes there are there are class in the local versus global policies etcetera.

So, these need to be addressed. These need to be first of all I defined and this need to be a address and this becomes a very critical thing when there is a organization is pretty large to look at An individual policies and verify and all those things.

(Refer Slide Time: 11:08)



Goals of Security

- Prevention
  - Prevent attackers from violating security policy
- Detection
  - Detect attackers' violation of security policy
- Recovery
  - Stop attack, assess and repair damage
  - Continue to function correctly even if attack succeeds

So, looking all those things, so what we have seems there are security models or security objectives. There are attack models there are threats, and I there are policies and mechanisms. So, these are a different component which looks at a different way of the things right.

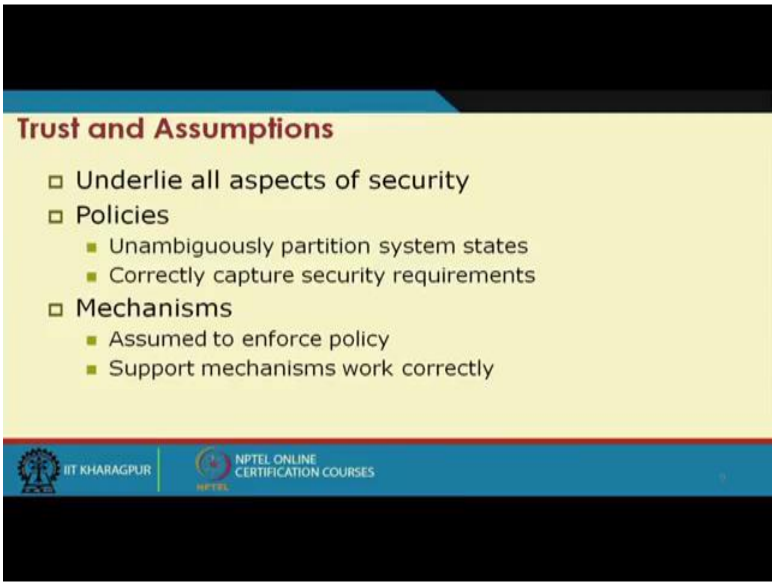
Now, I need to bring them together, and have what is my security goal. So, one of the major security goal is prevention, prevent attackers from violating security policies. So, that should be there. So, attacker if I have the security policies if it is restricts that thing, attackers should be should not be able to violate the security policies. Detection detect attackers violation of the security policy. So, detection that the when the security policies are being violated by the attackers need to be detected right.

So, detection I can have we then we will try to the earlier the detection is, more strong your security perimeter right. So, we need to detect as early as possible. Because if the attack has gone on go on into the place then what we what we are left with is more of the post mortem of the what had happened. And basically learn to look at the other things. There are a issues of another issue is recovering. If attack and if compromised if down to some extent or fully or partially, then how to recover from this thing, right?

So, what will be my recovery mechanisms mechanism from these types of things, like stop attack, assess and repair damage, continue to function correctly even if the attack succeeds. And there are different type of things people that there are in best practices.

We have in critical system as redundancy system, there are logging mechanisms to recover and other things never the less, we need to recover from the thing to a stage where we where like pre attack stays type of things you know on all doing. So, we incurred cost right. All this comes with a cost.

(Refer Slide Time: 13:21)



Trust and Assumptions

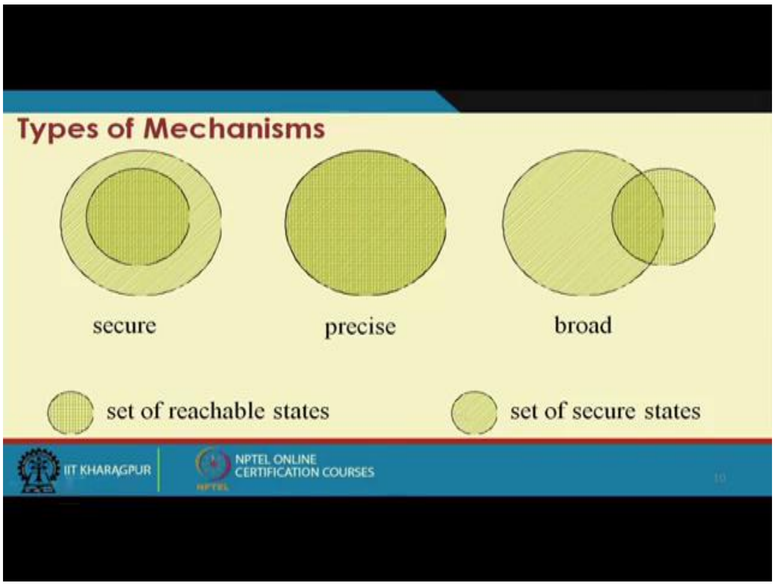
- Underlie all aspects of security
- Policies
  - Unambiguously partition system states
  - Correctly capture security requirements
- Mechanisms
  - Assumed to enforce policy
  - Support mechanisms work correctly

Trust and assumptions that is another aspects. So, underlie all aspects of security right. So, I have some trust and assumption, I trust this system I assume that system will work fine or this or this particular application and so on and so forth things are there. So, it all stress and if you if you look at our day to day life also for security mechanisms we have some sort of a test trust, and assumption like I say I understand what we trust that the security person who is guarding that particular installation or particular premise is can be trusted right.

So, I assume that this can be trusted to this extent and so on and so forth and type of things. So, this also is important thing. So, policies unambiguously partition system states right. So, that is if you look at the system state system goes on different state because first of all it is a dynamic thing right. It is not that it is statically one defined things are there. So, it is it should unambiguously partition the system state; that means, I am in this state or this state which state I am there. So, it should be ambiguous partition correctly capture the security requirement of every stage right.

So, it will not only partition it should also security requirements of every stage. Mechanisms assume to enforce policies. So, mechanisms are there to enforce policies. Supports mechanisms support mechanisms work correctly. So, that the mechanism is basically a implementation or realization of the policies and that should be they are in place.

(Refer Slide Time: 15:03)



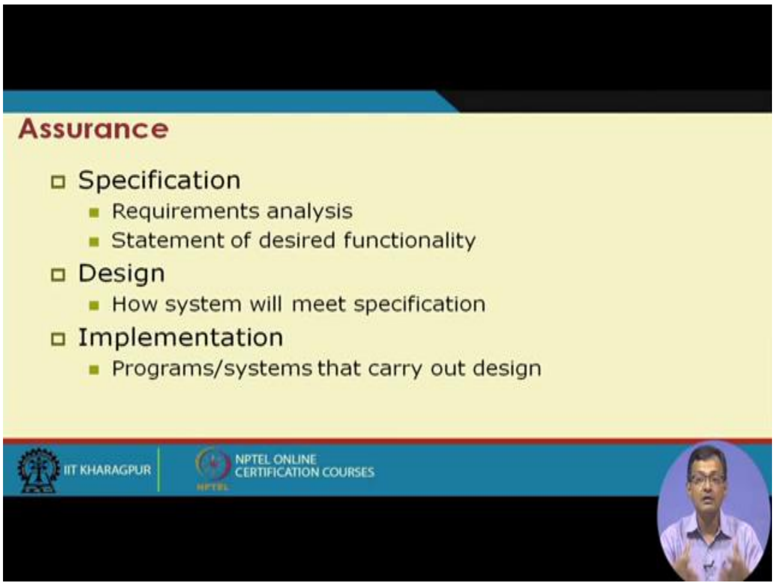
Types of Mechanisms

Now, if we look at a little bit holistically. So, if I have like set of reachable states of a system right.

So, if the set of reachable state is in this type of mess, and if I have a set of secured stages like this type of hash line right. So, one we say that if the set of reachable state is within the overall set of secured state then I say it is fully secure right. So, what I am trying to say that the system goes over different state all are within the security state. So, I have say I have security state security state at s1 to s20 as secure my system basically hover between s5 to s16.

So that means, it is always in the security state. It can be precise that the it totally matches with this the set of security and set of reachability is matches. Other can be broad; that means, all are not in the security zone or the in the secure state, but a, but there are some state which is there right. The one thing we should be we should know that how my security policy mechanisms visa-vies work. So, that I can say that how much secured I am.

(Refer Slide Time: 16:38)

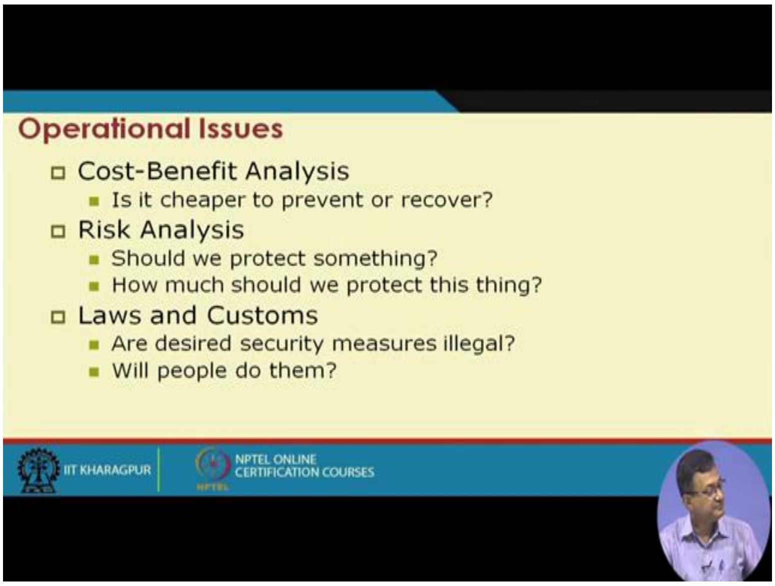


Assurance

- Specification
  - Requirements analysis
  - Statement of desired functionality
- Design
  - How system will meet specification
- Implementation
  - Programs/systems that carry out design

So, there is a issue of assurance, like which consists of specifications right. Like requirement analysis statement of desired functionalities designs; how the system will meet the specification and implementation, program systems that carry out design right. So, what it tries to do that in order to have properly design the thing, I can assure that this much security has been can be assured based on my design specification etcetera right.

(Refer Slide Time: 17:25)



Operational Issues

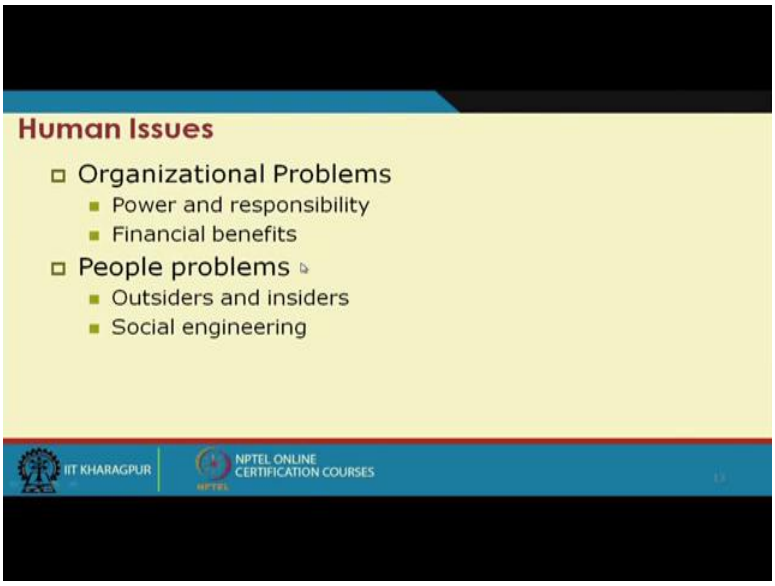
- Cost-Benefit Analysis
  - Is it cheaper to prevent or recover?
- Risk Analysis
  - Should we protect something?
  - How much should we protect this thing?
- Laws and Customs
  - Are desired security measures illegal?
  - Will people do them?

So, this is these are the best practices which need to be put into place. So, that my security level goes up. Now there are issues of operational issues, or sometimes there are economical issues right. Cost benefit analysis is it typical it is cheaper to prevent or recover right. So, so whether which is costly like, it is it is recovering is costly or things like I say that I have a lap which has some Linux installation, or windows installation or combined both of them. And we run the lap on day to day basis, but as such I we do not store anything in the system, right.

So, a in that case that is students are supposed to bring their documents or download their codes etcetera run, and then release the thing right, but end of the day there is no question of storing any data. Or there is no responsibility from the authority, so that the data will be saved etcetera. For that I may not look for much interested for preventing the attack right. Even some attack is there if I can recognize I can always reinstall that I can have a already a image of the whole system and I can reinstall the image, right.

But on the other hand if there is a data intensive or say research data etcetera, then I am more interested in preventing the attack right. Or a system which is online running on things I want to prevent the data hum. So, that is cost analysis benefit other is the risk analysis right; should we protect something how much should we protect this thing, right. How much risk is there are laws and customs right. Let are desired security measures illegal will people do them etcetera. So, we have different operational issues which are there.

(Refer Slide Time: 19:21)

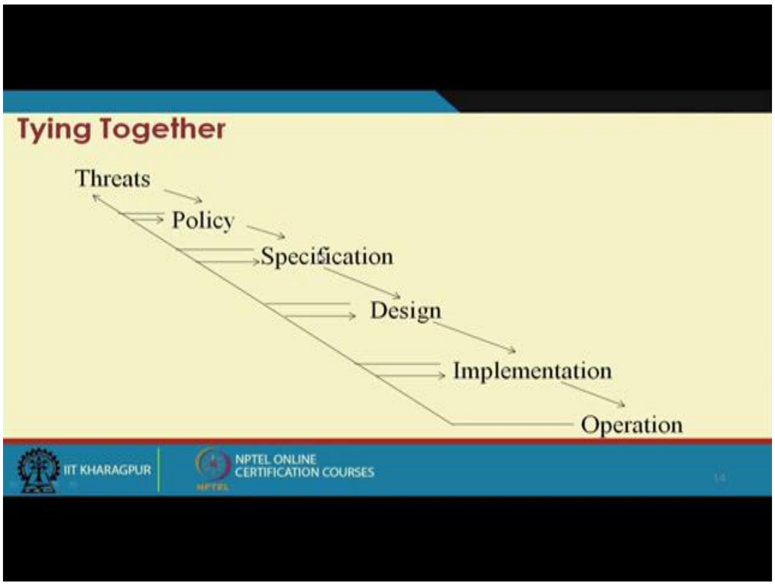


Human Issues

- □ Organizational Problems
  - Power and responsibility
  - Financial benefits
- □ People problems
  - Outsiders and insiders
  - Social engineering

There are of course, some of the human issues rights; organizational problems or people problems. So, there are always human in the loop, and there are human issues of responsibility per says authority And so on and so forth.

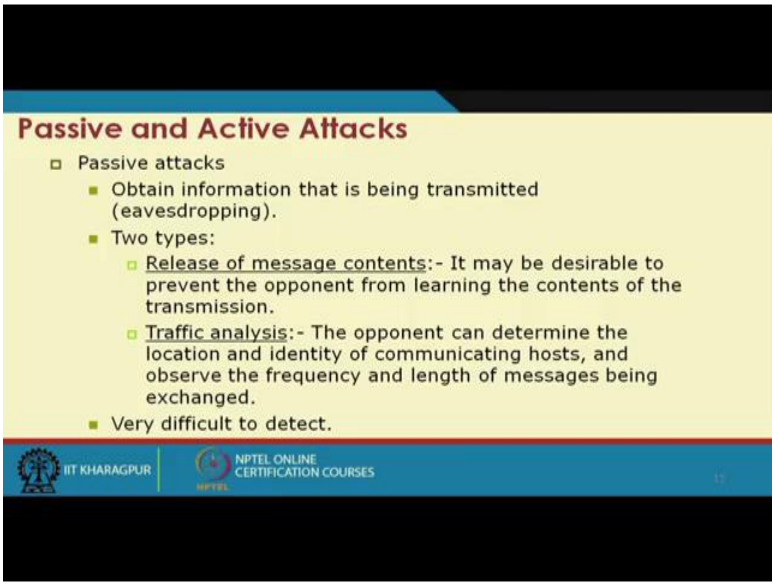
(Refer Slide Time: 19:39)



Tying Together

So, if we tie them together. So, threats are there policies are a based on the threats policies are made based on the specification based on the things policy specification the design is there based on design that implementation and then operation. These operational issues are feedback either to the implementation or design specification and things or operational issues comes as a threat.

(Refer Slide Time: 20:13)



Passive and Active Attacks

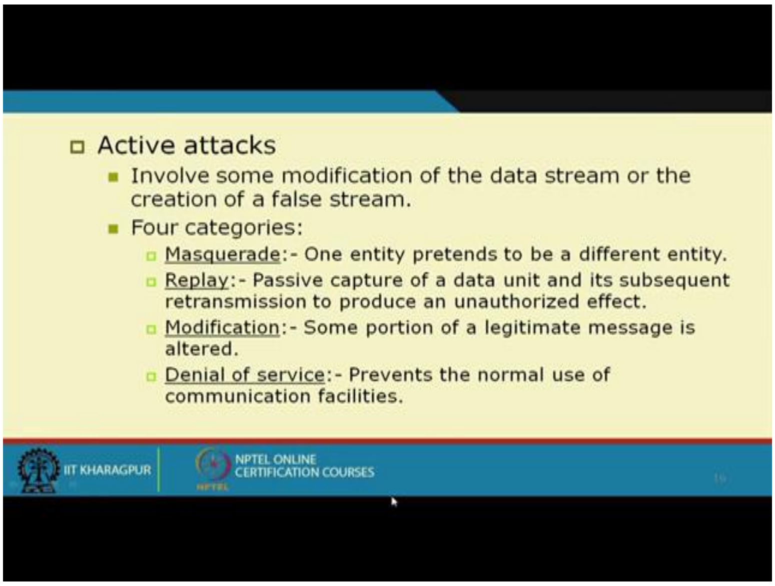
- Passive attacks
  - Obtain information that is being transmitted (eavesdropping).
  - Two types:
    - Release of message contents:- It may be desirable to prevent the opponent from learning the contents of the transmission.
    - Traffic analysis:- The opponent can determine the location and identity of communicating hosts, and observe the frequency and length of messages being exchanged.
  - Very difficult to detect.

So, this is if we try to make them together bring them together it is like sort of it. Now what we are looking as of now is more from the point of view of like from the providers or the from the system point of view. Like what are the what could be the possible threats what could be important possible policies, how to implement what is the mechanisms and so on and so forth, right. But if we try to look at that what are the different type of attacks like one is passive attack right. Obtain information that is being transmitted eavesdropping. So, it is not the attacks, but these are more eavesdropping.

So, 2 types release of message content it may be desirable to prevent the opponent from learning the contents of the transmission. So, release of the message content may be one of the attack traffic analysis. Like I do not look at the message, but say, but I want to look at the traffic right. If the traffic is highly volatile or heavy or low I try to predict that what could be the effect of the effect of the type of mechanisms going on right. I can say that if there is a very high traffic that may be some sort of a video conferencing or video chat is going on.

And it may be something need to be looked attached to me something if is a low traffic or medium traffic I can say that this is the type of things. And based on not only the traffic persist time it said also plays different important role.

(Refer Slide Time: 21:55)

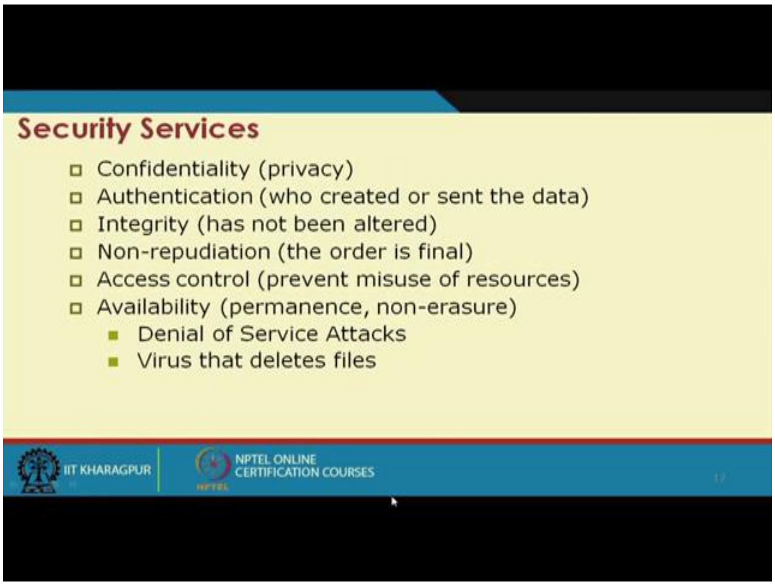


- Active attacks
  - Involve some modification of the data stream or the creation of a false stream.
  - Four categories:
    - Masquerade:- One entity pretends to be a different entity.
    - Replay:- Passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.
    - Modification:- Some portion of a legitimate message is altered.
    - Denial of service:- Prevents the normal use of communication facilities.

Usually passive attackers are difficult to detect because they do not do direct harm and very difficult to detect, whereas on the other hand I we have active attackers. Like involve some modification of the data stream or creation of false streams. So, that is these are all active attackers right, So 4 categories. So, one is masquerade one entity pretends to be different entity. So, that is the one attacker replay. Passive capture of the data unit and it is subsequent retransmission to produce unauthorized effect right. So, this is a replay attack right.

So, contained passive capture of the data units and it is subsequent retransmission huge amount of retransmission of the date modification. Some portion of the legitimate message is altered. So, that is the attack of modification denial of service prevents the normal use of communication facilities. So, this is a dos type of attack or denial of services attack. So, all these attacks actually create problem in our in the operation of the active system.

(Refer Slide Time: 23:04)



Security Services

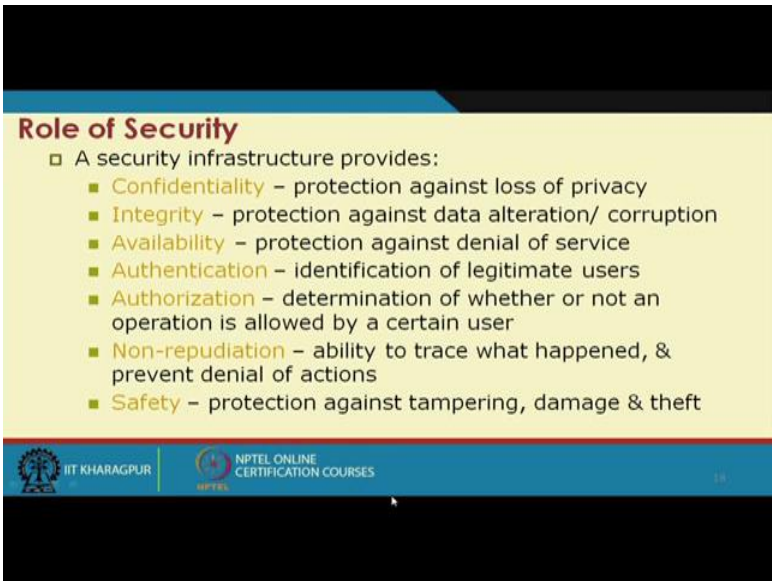
- Confidentiality (privacy)
- Authentication (who created or sent the data)
- Integrity (has not been altered)
- Non-repudiation (the order is final)
- Access control (prevent misuse of resources)
- Availability (permanence, non-erasure)
  - Denial of Service Attacks
  - Virus that deletes files

Now, in the security services as those things we have seen that the these are the security threats security services try to give provide this sort of services, right. Like confidentiality, authenticity, integrity, non repudiation, access control, accessibility, a availability. So, this first thing we had discussed non repudiation what we say the order is final right. It is like that you say you order something like you say that the bank you instruct your bank that you transfer over online that you transfer x amount from my account to somebody else’s account and next day I go to the bank that I never gave this right.

So, there is a there is a there should be a way of handling this. So, there is non repudiation is why is such things is basically says the order is better. Access control is a big field that how this access control will be there are works on role based access control mechanisms and so on and so forth. It is basically say the prevent misuse of resources. So, you should have that particular resource particular access to a particular resource center So That you can use that resources

Availability performance and non erasure type of services. So, that is denial of services service attack and there can be virus that deletes files.

(Refer Slide Time: 24:39)



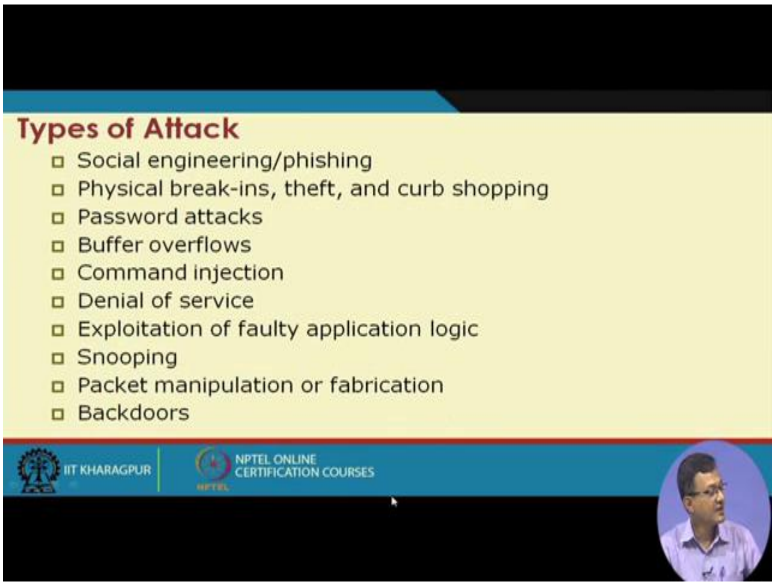
Role of Security

- A security infrastructure provides:
  - Confidentiality – protection against loss of privacy
  - Integrity – protection against data alteration/ corruption
  - Availability – protection against denial of service
  - Authentication – identification of legitimate users
  - Authorization – determination of whether or not an operation is allowed by a certain user
  - Non-repudiation – ability to trace what happened, & prevent denial of actions
  - Safety – protection against tampering, damage & theft

So, that is your that is the also case of non availability, so, role of security. So, if when you when you talk about computer security network security information security cloud security and so on and so forth. What are the role of thing? The security infrastructure should provide first of all confidentiality. That means protect against loss of privacy the integrity protection against data altered data alteration or corruption.

So, that is the protection of this the integrity, because as you have seen integrity that during the message transfer the data is being altered. Availability protection against denial of service authentication identification of legitimate users so that how to identify an authenticated legitimate user. Authorization is determination of whether or not operation is allowed by a certain user. Non repudiation as we have discussed the order is final, safety protection against tampering damage theft etcetera right.

(Refer Slide Time: 25:44)

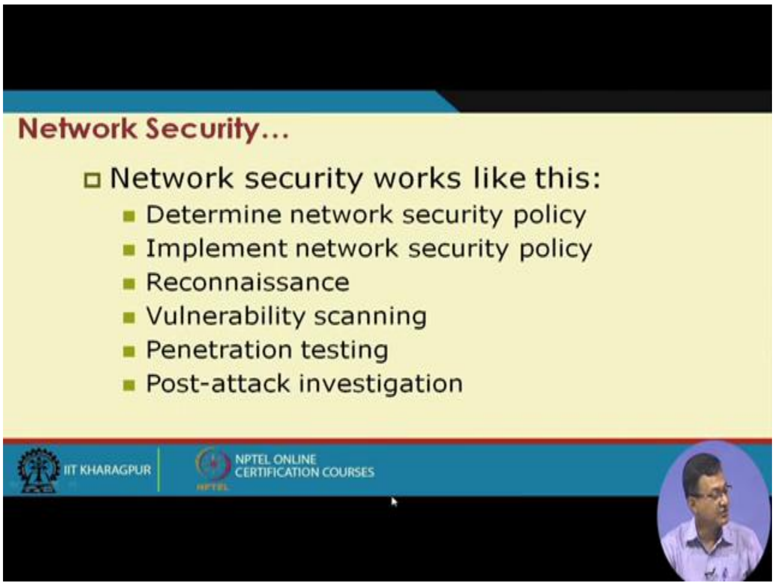


Types of Attack

- Social engineering/phishing
- Physical break-ins, theft, and curb shopping
- Password attacks
- Buffer overflows
- Command injection
- Denial of service
- Exploitation of faulty application logic
- Snooping
- Packet manipulation or fabrication
- Backdoors

And we have a series of attacks based on that different type of vulnerabilities and so on and so forth, from social engineering to phishing, password attacks, buffer overflow, command injection and etcetera etcetera. So, these are different type of attacks which are there in the information system, which are true in some sense for the cloud infrastructure also.

(Refer Slide Time: 26:05)



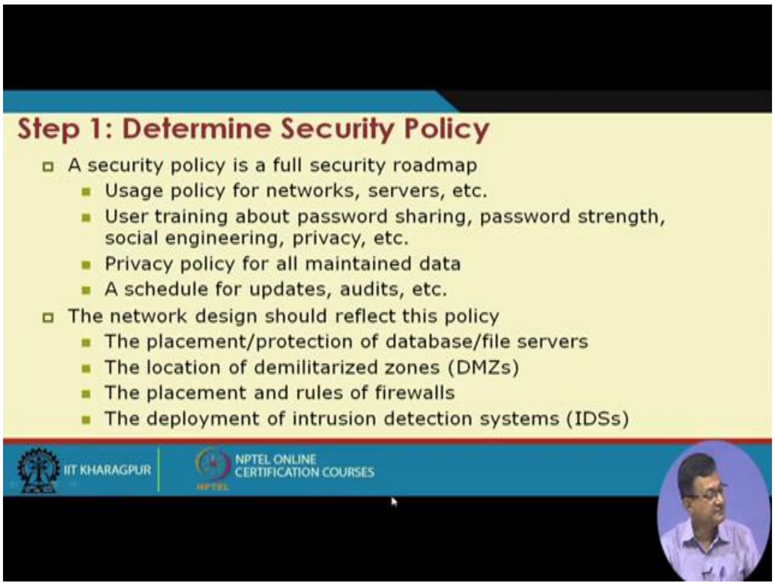
Network Security…

- Network security works like this:
  - Determine network security policy
  - Implement network security policy
  - Reconnaissance
  - Vulnerability scanning
  - Penetration testing
  - Post-attack investigation

Now, if we look at a typical scenario like say network security which is very prominent because the cloud is based on a this term is basically build on the distributed systems which are leverage or network and so, it is important that the basic network level security is high. So, network security works like this determination of the network security policies that what should be the security policy, implementing those policy then reconnaissance. So, that should this to see that whether the security things are in place or not vulnerability scanning like how vulnerable I am.

So, that look at the vulnerability scanning, there is a concept of penetration testing; that means, or what we say self attacking sort of scenario is a self and safe attacking scenario, that how much I can predict it to the system. So, it is a penetration testing and there is a need of post attack in investigation, if there is a attack then post attack investigation.

(Refer Slide Time: 27:05)

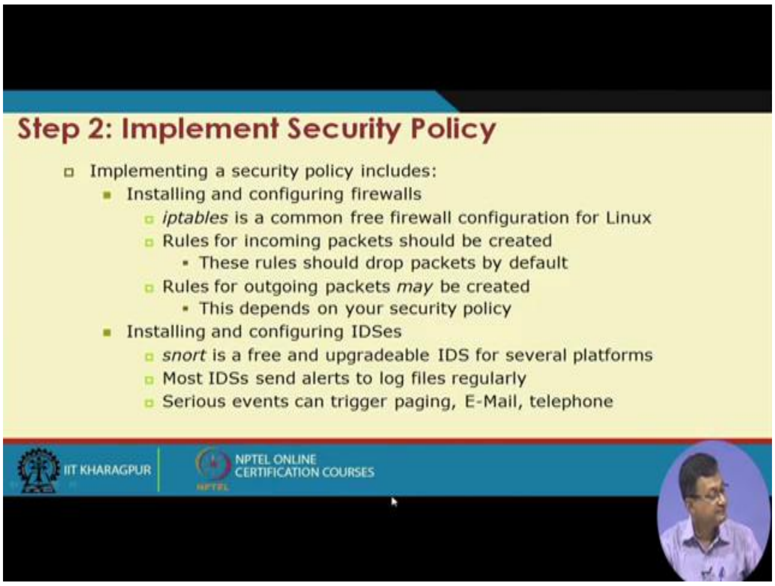


Step 1: Determine Security Policy

- A security policy is a full security roadmap
  - Usage policy for networks, servers, etc.
  - User training about password sharing, password strength, social engineering, privacy, etc.
  - Privacy policy for all maintained data
  - A schedule for updates, audits, etc.
- The network design should reflect this policy
  - The placement/protection of database/file servers
  - The location of demilitarized zones (DMZs)
  - The placement and rules of firewalls
  - The deployment of intrusion detection systems (IDSs)

So, determination of security policy, that the security policy is a full security roadmap and for any organization. So, smaller things if it is a inter organization. So, that what will be the security policies need to be placed right? It is a full road map have to be there. The network design should reflect these policies. So, if it is a network thing.

(Refer Slide Time: 27:35)

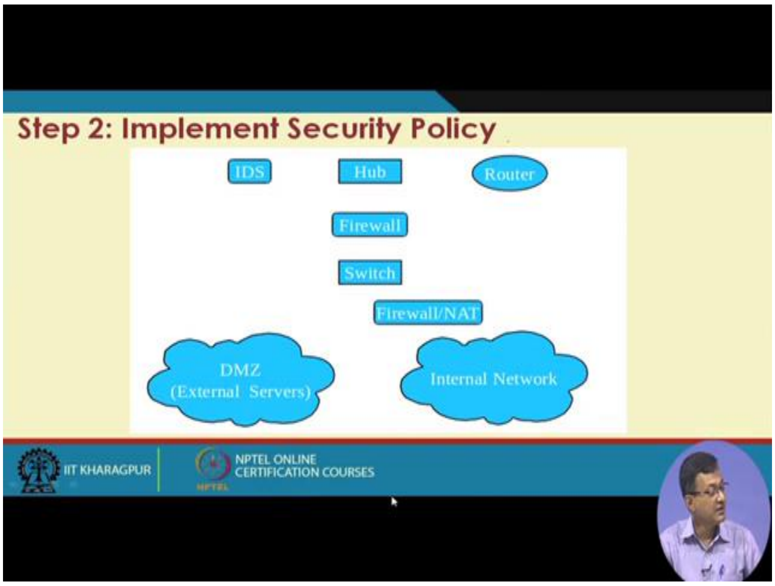


Step 2: Implement Security Policy

- Implementing a security policy includes:
  - Installing and configuring firewalls
    - *iptables* is a common free firewall configuration for Linux
    - Rules for incoming packets should be created
      - These rules should drop packets by default
    - Rules for outgoing packets *may* be created
      - This depends on your security policy
  - Installing and configuring IDSes
    - *snort* is a free and upgradeable IDS for several platforms
    - Most IDSs send alerts to log files regularly
    - Serious events can trigger paging, E-Mail, telephone

So, whenever you are designing. It should confirm these security policies. So, implementing the security policies implementing policies include installation and configuration of security measures like firewalls, installation of configuration of ID’s and there are several other type of things which need to be there.

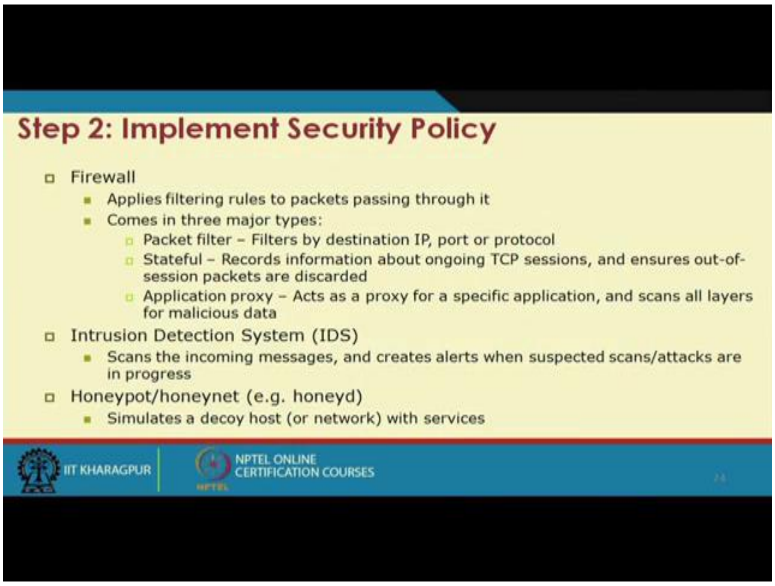
(Refer Slide Time: 27:53)



Step 2: Implement Security Policy

So, if we look at it is a big picture like this, where you have different there is demilitarized zone internal network. And that firewall or network address translator nat, switch, firewall and type of things right. So, it is it is dual homing or 2 firewalls are there.

(Refer Slide Time: 28:11)

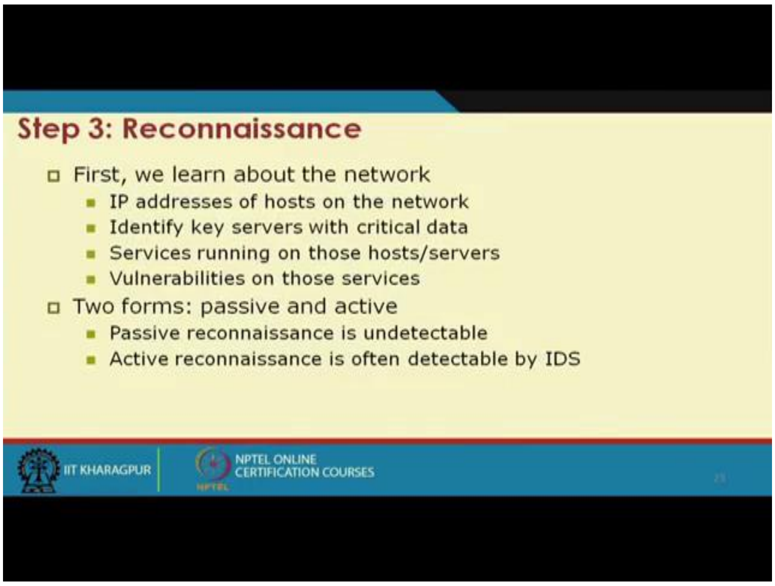


Step 2: Implement Security Policy

- Firewall
  - Applies filtering rules to packets passing through it
  - Comes in three major types:
    - Packet filter – Filters by destination IP, port or protocol
    - Stateful – Records information about ongoing TCP sessions, and ensures out-of-session packets are discarded
    - Application proxy – Acts as a proxy for a specific application, and scans all layers for malicious data
- Intrusion Detection System (IDS)
  - Scans the incoming messages, and creates alerts when suspected scans/attacks are in progress
- Honeypot/honeynet (e.g. honeyd)
  - Simulates a decoy host (or network) with services

So, implement security policies either the policies or the excess rules in the firewall or ID's or there is a concept of honeypot or honeynet where vulnerable things are there so, that lot of attacks will be there and the security means security personnels understand that what sort of attacks is there. Based on that signatures they basically do they basically fine tune there are RDA ID's or firewall policies.

(Refer Slide Time: 28:45)

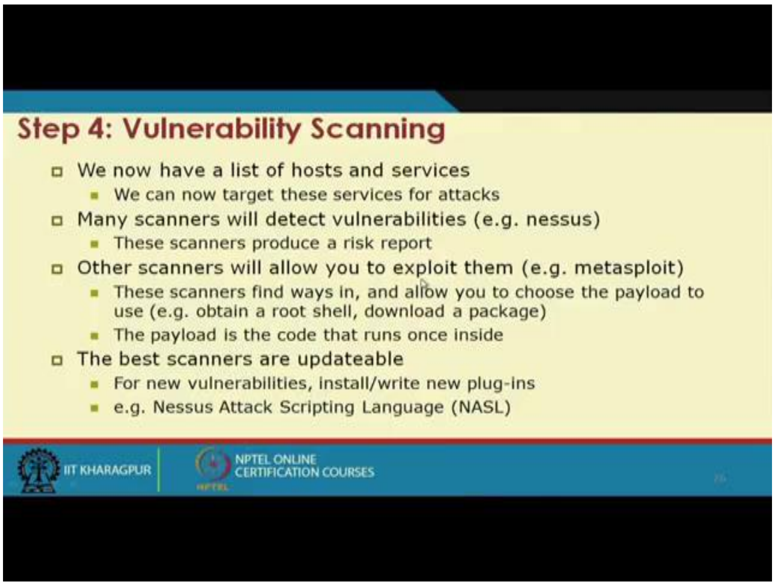


Step 3: Reconnaissance

- First, we learn about the network
  - IP addresses of hosts on the network
  - Identify key servers with critical data
  - Services running on those hosts/servers
  - Vulnerabilities on those services
- Two forms: passive and active
  - Passive reconnaissance is undetectable
  - Active reconnaissance is often detectable by IDS

So, the next thing is that need to learn about the network right. So, in order to whether to attack or prevent you need to none of the network. So, IP address of the host identify key servers with critical data and so on and so forth. So, there are 2 forms are there one is passive which is undetectable, one is active it is not often detected by the ID's right.

(Refer Slide Time: 29:12)



Step 4: Vulnerability Scanning

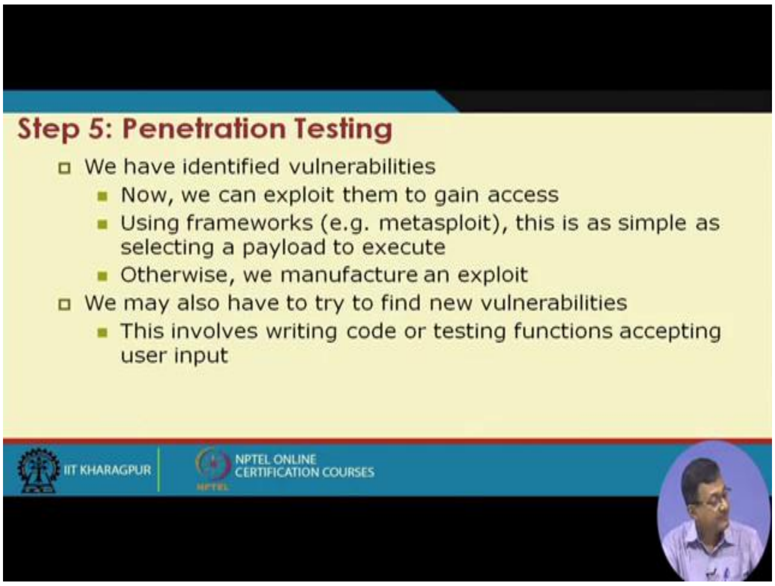
- We now have a list of hosts and services
  - We can now target these services for attacks
- Many scanners will detect vulnerabilities (e.g. nessus)
  - These scanners produce a risk report
- Other scanners will allow you to exploit them (e.g. metasploit)
  - These scanners find ways in, and allow you to choose the payload to use (e.g. obtain a root shell, download a package)
  - The payload is the code that runs once inside
- The best scanners are updateable
  - For new vulnerabilities, install/write new plug-ins
  - e.g. Nessus Attack Scripting Language (NASL)

So, there are this is a need. There is a vulnerability scanning that as we are discussing as we are discussing couple of minutes back that I need to basically scan my vulnerabilities right, so that how vulnerable I am in the other system wise.

So, there are different scanner there are in case of a network there are different like there is a open source thicknesses in map and so and so forth. So, that you can basically scan that which are the ports open, what are the possible vulnerabilities and type of things right. So, this is important that you scan and see that; what is the security quote unquote security health of your installation.

So, other scanner will allow to exploit then they are they are called metasploit and type of things which has is security database, there are difference security vulnerability database like one such is that in NVD national vulnerability database where which basically says that what are the different vulnerabilities. So, scanners are need to be updatable. So, that it goes on as in case of antivirus etcetera, which are primarily scanner. So, need to update with the signatures.

(Refer Slide Time: 30:21)

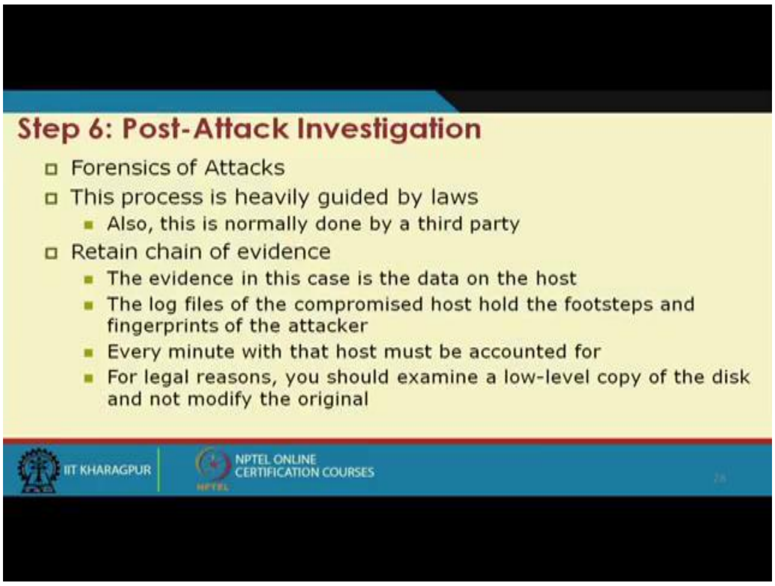


Step 5: Penetration Testing

- We have identified vulnerabilities
  - Now, we can exploit them to gain access
  - Using frameworks (e.g. metasploit), this is as simple as selecting a payload to execute
  - Otherwise, we manufacture an exploit
- We may also have to try to find new vulnerabilities
  - This involves writing code or testing functions accepting user input

And then we have the penetration testing, like one we do a vulnerability analysis of a say a network and then looking at the vulnerabilities, we do a penetration testing of the system that how much I can penetrate into the systems and type of things. These are safe attacks and late as late as means a organization or the security personnel can know that what are the different vulnerability points and put appropriate patches.

(Refer Slide Time: 30:53)



Step 6: Post-Attack Investigation

- Forensics of Attacks
- This process is heavily guided by laws
  - Also, this is normally done by a third party
- Retain chain of evidence
  - The evidence in this case is the data on the host
  - The log files of the compromised host hold the footsteps and fingerprints of the attacker
  - Every minute with that host must be accounted for
  - For legal reasons, you should examine a low-level copy of the disk and not modify the original

And finally, we have a post attack investigation. The forensics of the attacks the process is heavily guided by the laws that how this post attack or post mortem scenarios screaming there then retain chain of evidences that how things happens etcetera.

So, these are post mortem or post attack scenarios. Now if you look at in our in case of a cloud all these things also come in different in same or different forms right. Because these are more generic though we discussed at the end little bit of network related, but these are primarily more generating attacks. And then we have this post attack investigations to look at that what are the different attack pattern etcetera. And we will try to look at in our next lecture or so, that how what are the implications or what are the specialty of this security in case of cloud computing. So, will stop here today.

Thank you.