Computer Networks and Internet Protocol
Prof. Soumya Kanti Ghosh
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture – 58
Network Security – Overview

Hi. So, we will be continuing our discussion on Computer Networks and Internet Protocol. Today we will be discussing on a topic of called Network Security; or per se rather initially we will be discussing as a security of the Computing System per se what we mean, and then we will look at the Network Security. So, to say we as per as the course is concerned, it may not be within the very core of the overall course of computer networks and internet protocol, and but what we thought that without talking or discussing something on network security, the overall phenomenon may not be complete, alright.

So, we thought that we will add one if possible 2 lectures on computer per se this network security, right. And but for your convenience that will be most likely not including these in your exam per se. So, that is more of a thing what we like to say that to see the security aspects and what are the approaches things, but do not bother about the exams.

So, what why this is becoming important? Because see today's world or today's enterprises or today's day to day interaction are all becoming dependent on not only the computers, but more dependent on the network level activities or computer networks, right whether you are booking a ticket, or even paying your different your utility bills like electricity bills and water bills and type of things.

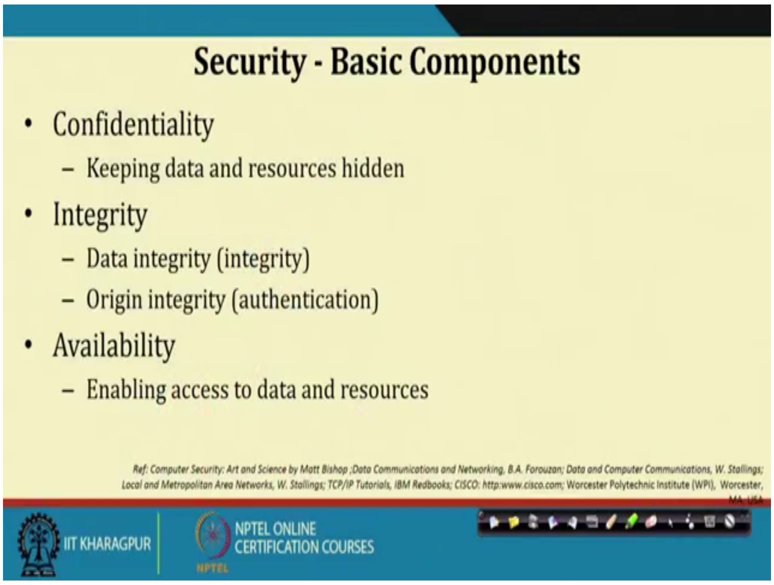
Even sending messages or looking for things, looking from information for some aspects and everywhere what we see this is a omnipresent; like, if you even look at the banking sectors. So, a more or less we are going to a scenario where you do not have to visit bank at any point of time, everything you are doing on the system. So, in other sense that becomes a this become a becoming one of part and per sell of our not only the enterprise network or organisation. It is also a becoming part and per sell of our day to day life right whether it is requirement or infotainment, where we see the security become the this network become a important aspects.

And in several as several activities, they are there is some sort of financial transaction is involved, right. And whenever there is a financial transaction involve, that becomes important to make it secured, right, or weather at all loopholes are there. I can say that the network is per se is secured network. Then there is no loophole right. So, whether there is a loop hole is there, where is a chance of loop hole is there, or what sort of quote unquote attacks can be there on the overall our network infrastructure; whether it is only affect the network or also the systems things, and different aspects of the things.

So, security is becoming a necessity rather than a yet another subject type of things, right. If you look at the overall academic courses, this network security, computer security, information security, these are becoming a not only a subject a line of vertical quotes altogether.

So, it is not possible to cover everything, but we will try to open up or look at the thing that different aspects of the security aspect. So, in this lecture we will initially will try to look at that what are the different aspects of security, which is related to computer and information security, and network security also and then what specifically we need to look at the, how what are the mechanisms and way we can make our infrastructure or the network secured.

(Refer Slide Time: 04:35)



Security - Basic Components

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

Ref: Computer Security: Art and Science by Matt Bishop ;Data Communications and Networking, B.A. Forouzan; Data and Computer Communications, W. Stallings; Local and Metropolitan Area Networks, W. Stallings; TCP/IP Tutorials, IBM Redbooks; CISCO: http:www.cisco.com; Worcester Polytechnic Institute (WPI), Worcester, MA, USA

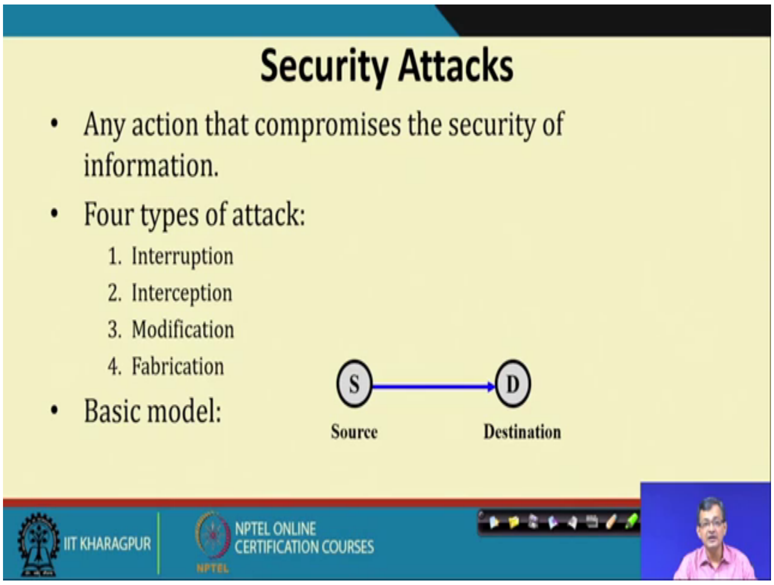
So, what we see that, when we look at the security per se, then what we are trying to look at? Primarily 3 aspects we want to look at confidentiality, integrity and availability, alright. So, these are the things if these are bridged we say that the security is bridged right. So, confidentially deals with keeping the data and the resource hidden alright, so that is confidential. So, if you are if I am sending a message to you, or your sending a message to me, so if it is mean for me only so it should be kept confidential. There should not be anybody who is listening to this message or reading this message, right.

So, confidentiality keeping the data and resources hidden or confidential integrity, what we say that data level integrity is that the message what I am sending should be reaching to the destination the same fashion. So, that the data is not being tampered right. If I am sending a message, so the data level integrity is there. There is another issue of origin integrity or what we say authentication; like, how do I know that who is sending is a correct person, alright. So, if I am say getting a message that today there will be a something say power cut and shut down the system, or something, then I how do I know that it is from the correct authenticate that thing, right.

So, this is also a question of integrity and then availability, enabling access to the data and resources right. I say that there is nobody looking at the data, no body tempering the data, no there is a message is coming on the same thing, but what I do there is a huge amount there is some way or other I not make the thing available to you, right. Like what I mean to say that, I if there is a attack like this by which you cannot access the internet. Otherwise everything is working fine. There is no question of integrity or confidentiality, but the internet is not accessible due to some problem, right. There may be physical problem of disrupting the things or there can be some other problem of say lot of traffic increases congestion etcetera.

So, there is what we say a attack on availability the resource is not available, enabling access to the data and resources this is the availablity. So, if you see this CIA, primarily rules the all above things whether it is network related, whether it is computer related, for that matter any type of document related.

(Refer Slide Time: 07:18)

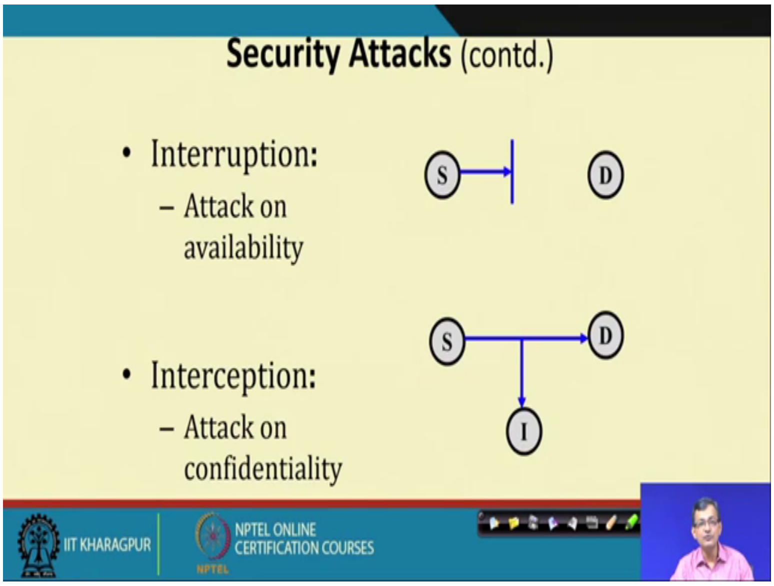


Security Attacks

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

Now, what are the different types of security attacks can be there? So, if you see there can be typically 4 category of the things. One is interruption like, so if I interruption, interception, modification, fabrication, right.

(Refer Slide Time: 07:36)



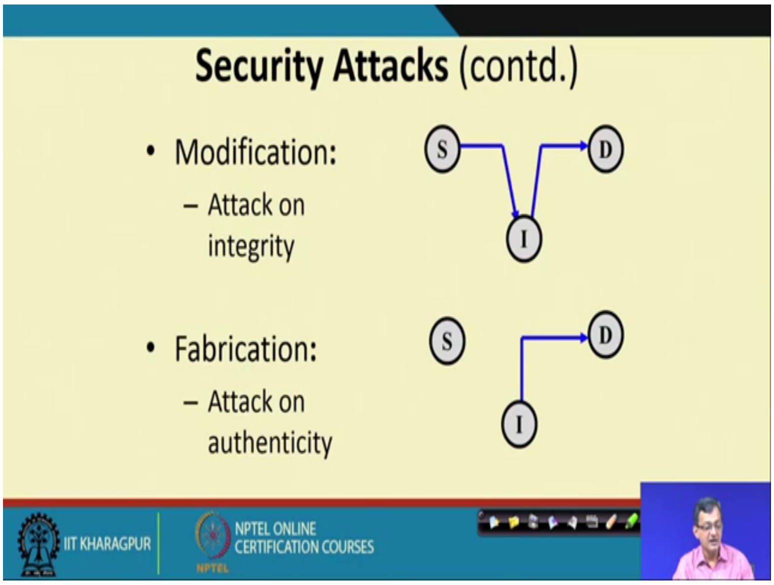
Security Attacks (contd.)

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

So, these are the 4 type basic model is that a message is being sent to source to destination. So, interruption is the attack on availability right; so it is blocked some way or other, either physically or through congestion or something that so that message cannot reach to the destination.

So, sometimes we can say that this is a type of denial of service. So, if you cannot this to the things. There is a attack on another kind what is interception right. So, attack on confidentiality A C sending to D, but that intercepted and it is also I is listening, or a attacker is listening to the things, so it is a attack on confidentiality.

(Refer Slide Time: 08:19)

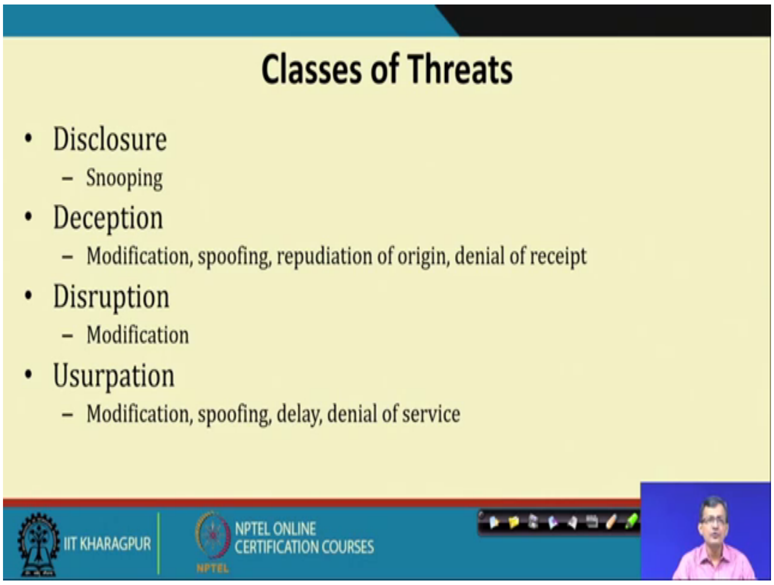


Security Attacks (contd.)

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

There can be a attack on modification. S is sending something do D, it is being intercepted and modified by I and send to D. So, it is a attack on integrity, integrity of data is there. And there can be a fabrication, I is sending to D pretending to be S right. So, I is sending to D pretending to be S; that means, there is a attack on authenticity of that particular origin. So, I cannot somebody else is pretending to be somebody else. So, these are the type of attacks which can be there.

(Refer Slide Time: 09:06)



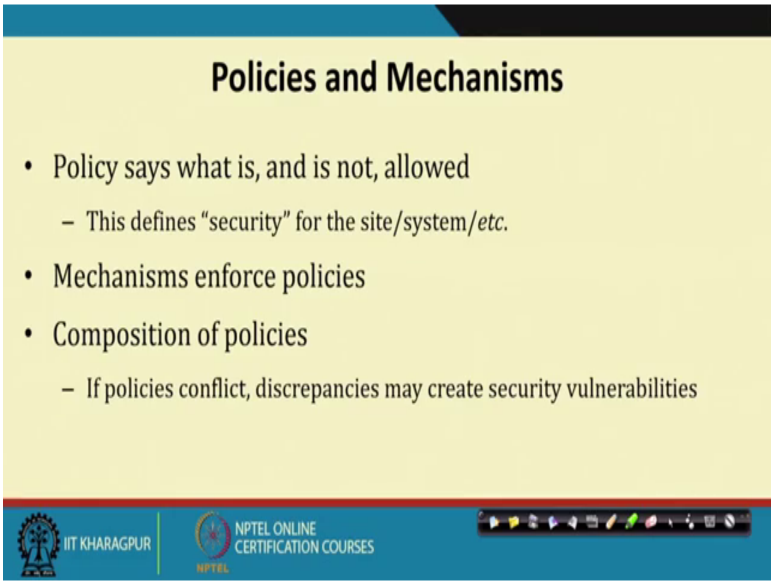
Classes of Threats

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

And if you look at the type of disclosures, so one is disclosure is a type of threats, one is disclosure that is snooping. Deception, modification, spoofing, repudiation of origin, denial of receipt and type of things are deception, right.

So, this can be deception. There is a threat of disruption of services; that can be a threat of disruption. And there can be a threat of usurpation, that modification spoofing delay denial of service. So, these are the different category of threat. So, what you are trying to see? What are the different types of attack, what are the different types of security attack, what are the different types of security concerns, and what are the different types of security threats, right.

(Refer Slide Time: 09:57)



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

IIT KHARAGPUR
NPTEL ONLINE CERTIFICATION COURSES
NPTEL

And then what we try to do? We try to make some policies and mechanisms which will enforce my mechanism which will enforce my policy. Like, so I have some security policy, this may happen this may not happen etcetera, etcetera and there should be a mechanism to enforce. So, policy says what is not allowed. So, what is allowed and what is not allowed. This defines the security of the site system etcetera right. Mechanism is enforce on the policy enforcement of the policies is by through mechanism, and there can be composition of policies, policy conflicts, discrepancies may create security vulnerabilities right.

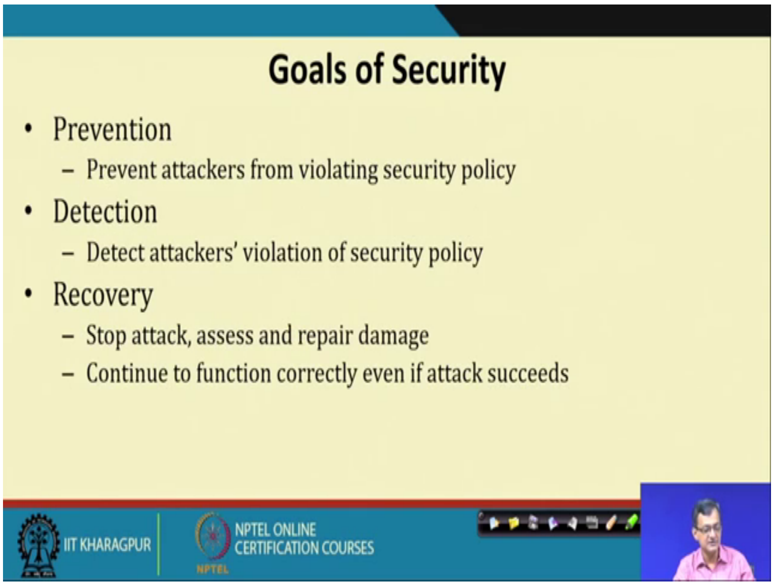
So, there can be if there are I have a policy and there is a mechanism to implement the things, if there is a conflicting policies, then there may be a security vulnerabilities may arise right. So, it becomes system becomes vulnerable right. So, why policy may conflict? Because sometimes the in a large organisation or large system, the policies may not be all globally decided, this is piecewise decided. But when you peace wise decide, when you integrate the things, there may be a problem in the conflict of the policy.

There can be other way the policy may not be a conflicting, but while implemented in a distributed manner that can be conflicting the things. Like I will give you one example, suppose IIT Kharagpur policy says that during a time period say, class hours or at mid night, there should not be any internet connection from the hall to internet, right.

However, this is a policy however the same in the same policy document that is there; however, that connects in from labs to the internet it is not restricted, because that is allowed. So, from the hall of residences or students hostilities may be restricted say this is the; now policy wise this is documented by when implementing implemented the policy in the hall particular security server or your switch which is say security enabled. And another thing we implement at in the departmental switch or departmental say they are 4 plus switch.

Now, see I can way this does not restrict the hall to access the departmental server, and make a hope from the departmental server to the internet. So, in a sense I have violated the policy. But as such the overall implementing mechanism may not be that tough to do that, right. Now it is may not be that straight forward to do in that, but there is a way to create this what we say it is a vulnerability, right. Vulnerability may also cope up if there is a something where policies are conflicting. We will see some of the things.

(Refer Slide Time: 13:00)



Goals of Security

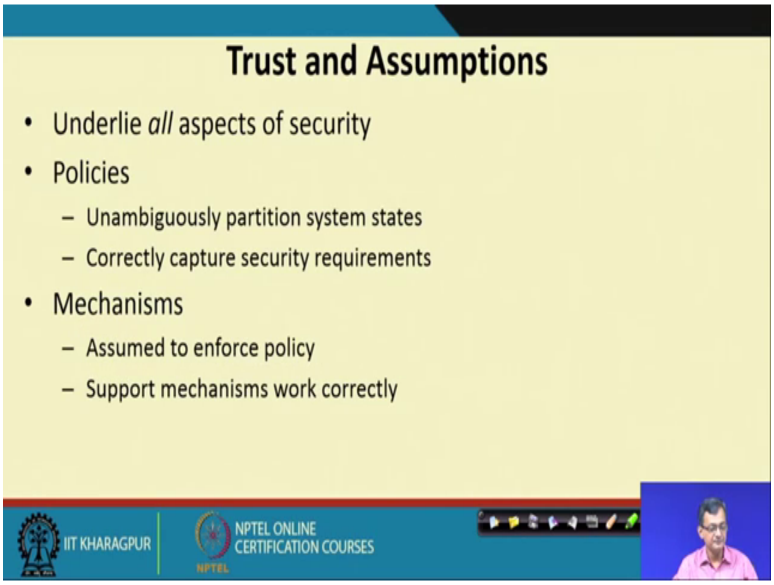
- Prevention
  - Prevent attackers from violating security policy
- Detection
  - Detect attackers' violation of security policy
- Recovery
  - Stop attack, assess and repair damage
  - Continue to function correctly even if attack succeeds

Now, well what goal of security, what we do we want first of all we want to prevent, right prevent attackers from violating security policies. If I have a security policies, prevent.

So, it is even if we look at our normal say what we say security of our particular building, particular campus, etcetera forget about the network that is also things are there. So, it is a prevention to prevent the violating security policy, if there is a another thing is that, it is a detection, if there is a attack the detect attacker violation of the security policy, I should be able to find out that where that attacker things are there. And then another aspect is the recovery, stop attack, access and repair the damage, continue to function correctly, even if the attack has success.

So, that is a case of continuing with the function even there is a attack on the thing, so this is a called a recovery. So, prevention, detection, recovery are 3 components of a typical security goal.

(Refer Slide Time: 14:05)



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

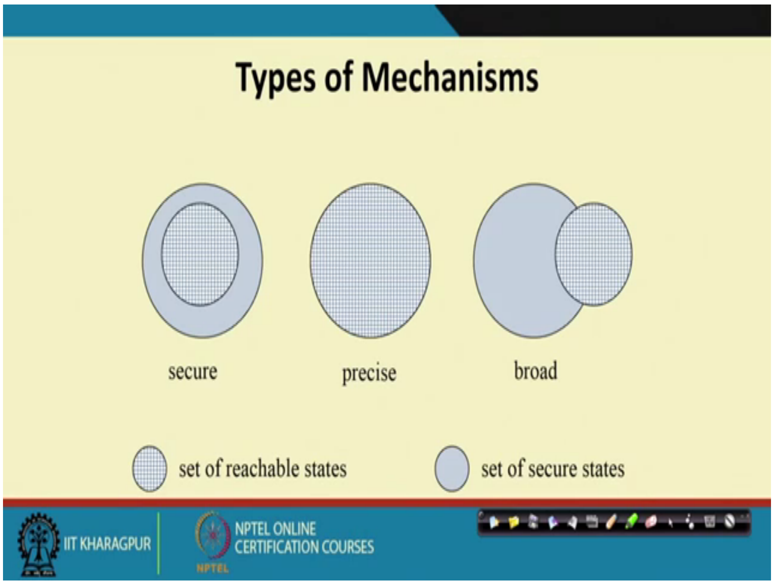
Now there is other co things comes up. There is a concept of there is a concept of trust and assumption. Underlie all aspects of security. So, say in our normal thing if I am having a security guard at the entrance of the building, I trust that guard, alright. And also I assume some of the things right. Like the attacker is likely to enter through this, I think that the attacker will be this category, this category of guard or mechanism able to solve it and type of things.

So, there are underlying any security things, whether it is network security or computer security or any other security, I have some sort of a trust on some of the things. And also I assume that this is the overall environment where the things are need to work, right. So, the based on that we want to formulate policies unambiguously partitioning, the system state right. So, I say this is the security state, this is non security state, correctly capturing the security requirements right. So, if I want to see that the a particular building or say

IIT Kharagpur what are the security requirement network infrastructure of IIT Kharagpur, first of all I need to know that what are the requirement.

And then if I want to implement divide or partition them into particular system state, that if this system is going to this system, and this state to the state and type of things, then it is; what are the security consequences. And finally, I should be have some mechanisms which assume to enforce this policy. Support mechanism work correctly. So, I have policies and mechanisms and there based on the trust and assumption.

(Refer Slide Time: 15:49)



Types of Mechanisms

So, types of mechanisms. Suppose these are set of reachable states. So, what you see? That any system or network is a dynamic and active system, right.

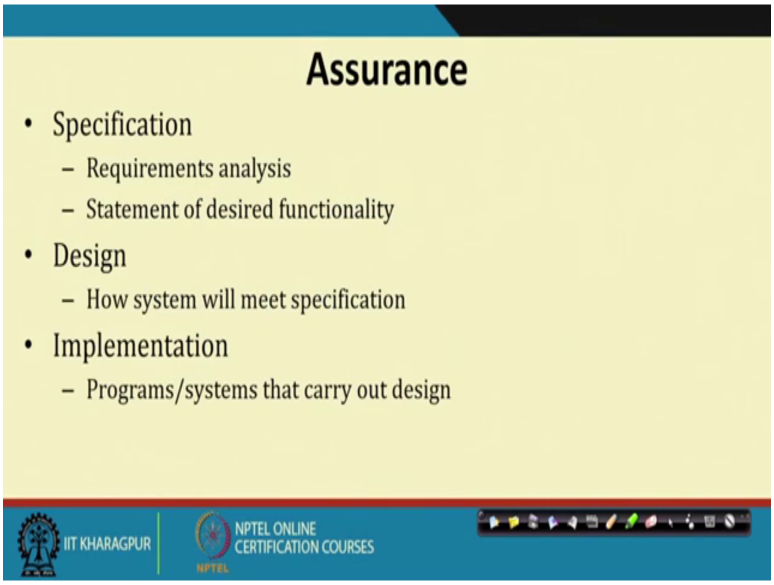
So, in the sense that, every activities it is going on the things we can think of the system is going from one state to another right, say for example, for simplicity I have a laptop. So, I install say particular operating system, then I put the security patches. So, while I install the operating system, it is in some state S 1, when I do a patch the security patches, it goes to some status 2, then I put another application over on the same system, so it may bring some vulnerability, may not bring some vulnerability, but goes to some S 3. And so that means, and I go on working with the things put pen drive etcetera, etcetera it go on what we say at different level of or different type of security states, right.

Same is true for the network right, you have different modules add devices, add network level devices, change the network level operating system, enhance those things, patch with new type of things, and it goes on going to the state. So, if I look at the IIT Kharagpur overall network, so it is a, what we say? Lively thing, right it is goes on the different state. So, I say state S 1 S 2 and S 3. So, our goal is that that if it is it should be within the secure state. So, I say that set of reachable state is identified by this diagram, and set of secured state is this. So, these are set of reachable state, so if I say whatever I do I am always within the secured state.

So, if the secured state is a super set of the reachable state, then I am secure. It can be directly precise like, whatever is it is on the directly mapping on the things or one to one making (Refer Time: 18:09) precise state. It can be brought like some of the some of the reachable state outside the security perimeter then what we say? It is some broad level security, but there are some security things which are beyond this type of things. So, this is true for definitely for network security it is true for any type of security aspects right; so our basic thing that it should be hovering around this 2; if it is always good if I can put it like this right. But as we understand, security is a costly affair right. So, whenever you want to put security, you are first of all putting more cost on it.

Secondly, you are basically making it more what we say time consuming things. So, it perform a degradation may be there like, I say that if I can enter a building or a particular campus straight away. So, I go on a particular level of flow is there, but everything is being checked with ID card scanning etcetera, it goes on a of obstructions ways things are there right. So, that means, not only it did not cause cost in terms of monitory it also have lot of mechanism into place which may affect the overall performance.

(Refer Slide Time: 19:23)



Assurance

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

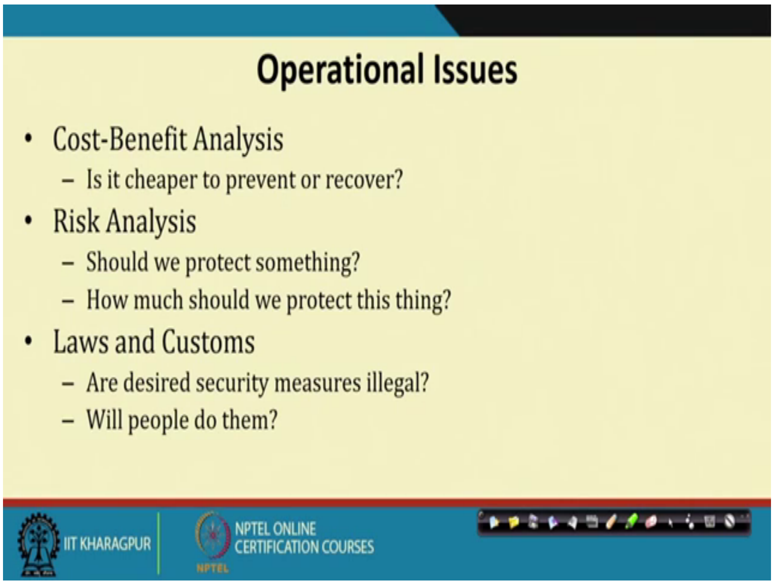
IIT KHARAGPUR

NPTEL ONLINE CERTIFICATION COURSES

Then above all doing said all those things, what I want to guarantee is the assurance. So, specification though assurance has a specification, requirement, analysis, statement of desire, functionality, design and implementation. So, given, so when I implement a security infrastructure say, particular this building or IIT Kharagpur by somebody, it maybe is whole team of IIT Kharagpur or from external third party, what I want to look at, that after doing this after investing this much of amount and this type of thing what is the assurance that I should get that it will not be breached, or in up to what level it is secured right. So, I can need to know say 1 to 10 scale or there are different security standards upto on that basis of that out level I have secured right.

So, what I require a set of specification right; so design constant how system will meet the specification; so requirement analysis statement of desired functionality and implementation; programs systems that carry out the design. So, there is a thing of this implementation.

(Refer Slide Time: 20:32)



Operational Issues

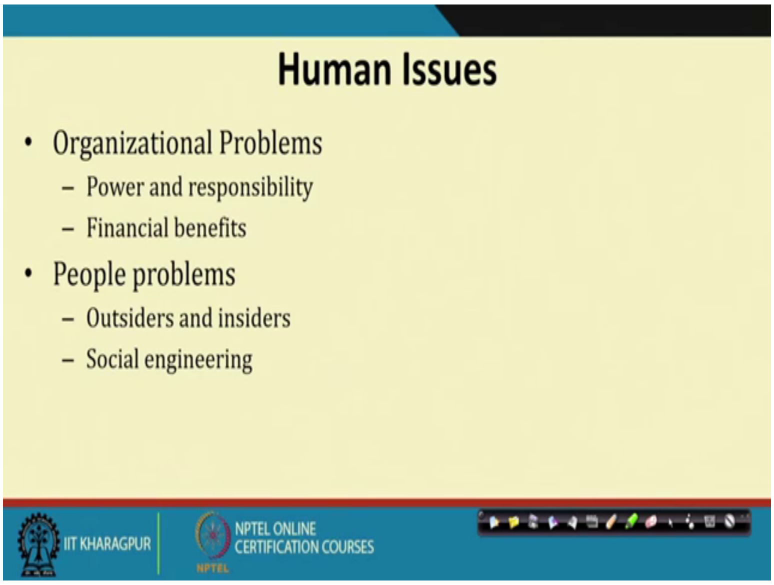
- Cost-Benefit Analysis
  - Is it cheaper to prevent or recover?
- Risk Analysis
  - Should we protect something?
  - How much should we protect this thing?
- Laws and Customs
  - Are desired security measures illegal?
  - Will people do them?

IIT KHARAGPUR
NPTEL ONLINE CERTIFICATION COURSES

And of course, there are operation issues, cost benefit analysis, whether investing so much whether it is becoming a cost benefit there is a return on investment. There issues of risk analysis should we protect something how much should we protect the thing etcetera. Like we can say that protecting instead of there are say 20,000 or system in the IIT Kharagpur campus or within the academic campus or even all the campus.

But those all are not important to the authority for the IIT Kharagpur authority or smooth functioning, maybe 100 out systems are more critical. So, whether to protect everything or I have different level of security for the things, I have a very cool level security or very strong security for those things which are which matters, and which are maybe some other thought of security. And above and all we should have low customs. And also standardization guidelines, which has to go into or desired security measure illegal will people do with them or something whether those are things which are legality there.

(Refer Slide Time: 21:36)



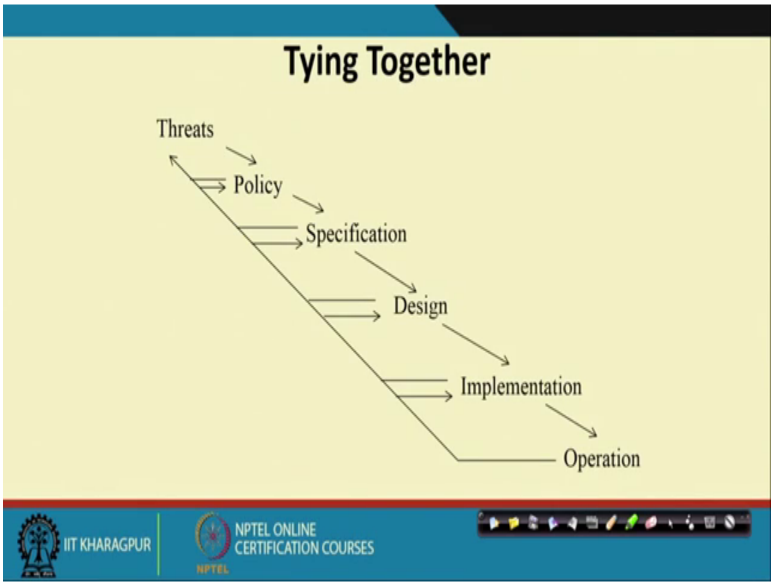
Human Issues

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

IIT KHARAGPUR
NPTEL ONLINE CERTIFICATION COURSES

And of course, there are human issues organisation problems, people related issues those are there.

(Refer Slide Time: 21:42)



Tying Together

Threats

Policy

Specification

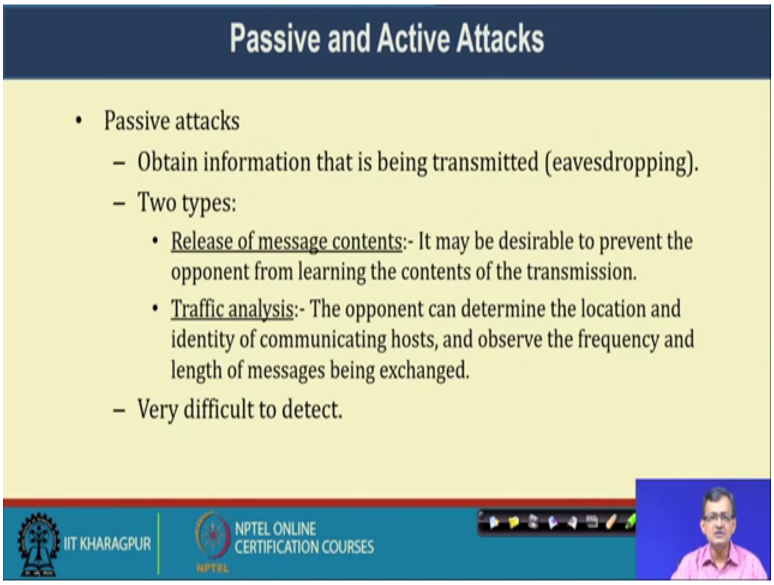
Design

Implementation

Operation

So, putting them together; so what we have we have threats based on the threats we frame policies. To implement policies, we design specification. Specification are with the help of specification we design the overall security scheme or mechanisms, and implement those mechanism and then I operationalise right. And then if there is and it goes on in different loop. So, from there it goes on implementation or design change or specification change or policy change, or while operating it may generate new threats right. So, this is a very dynamic and some sort of a lively thing. I should not say fully real time, or some sort of in your real time or a lively thing which is very dynamic and mutable things right type of things.

(Refer Slide Time: 02:35)



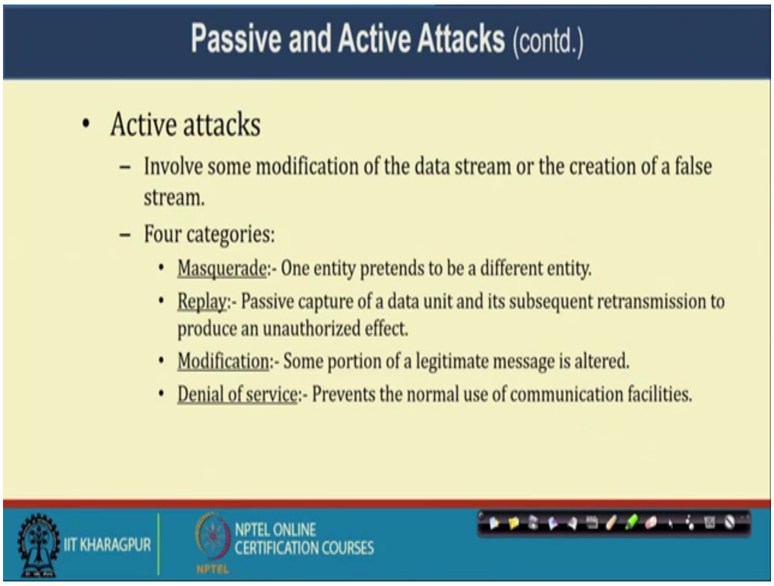
Passive and Active Attacks

- 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.

Setting all set is means giving all those things. So, if we look at the attacks, so there are broadly 2 category of attack. One is passive attack; another is active attack. So, passive attack obtain information that is transmitted, so some of a eavesdropping. So, there are there about we say that it is snipping and doing and information gathering, but it is not involving activator. They are more information gathering type of information. So, that can be a some software which is residing and carrying information about network which is etcetera, etcetera and go on transmitting to the somebody, so that it can launch a activator.

So, 2 type of release of message content, it may be desirable to prevent the opponent from land landing the content of a transmission system. So, that it is clamped on the things traffic analysis. Opponent can determine the location and identity of the communicating host, observe the frequency and length of the messages etcetera. So, it can analyse the traffic and try to see that what sort of things are there. So, it can be 2 things very difficult to attack detect this type of passive attacks, because they are not per se, so any manifests on the system. So, they has to gather on gather information and pass it to somebody else and that goes for a activator. So, they are not immediately involved in the thing. So, some sort of a spying and type of things on the network at the network level.

(Refer Slide Time: 24:10)



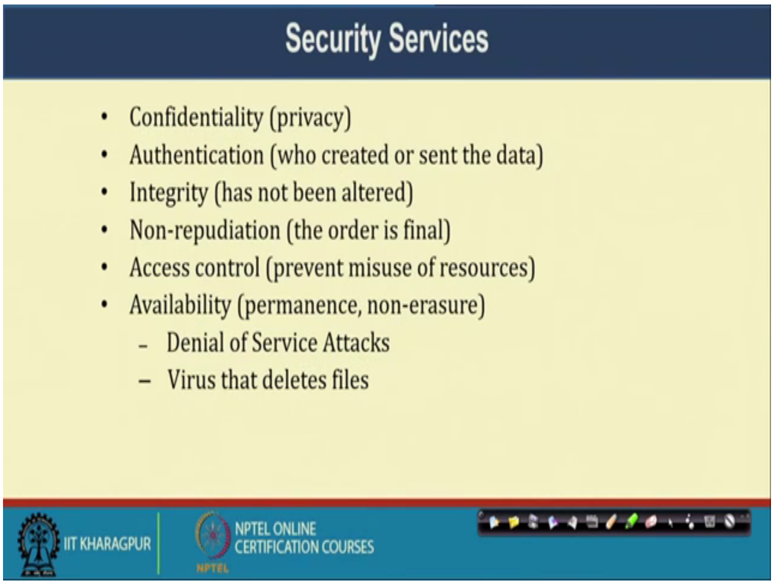
Passive and Active Attacks (contd.)

- 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.

So, activator on the other hand involves some modification of the data stream or creates any false stream and type of things. So, that is a activator 4 categories are replay may be there that is masquerade, one identity pretends to be a different identity, replay passive capture of the data units. And it is subsequent retransmission to produce an unauthorised effect. So, it is replay type of attack it can be modification, some portion of the legitimate message is altered. So, it is modified, it can be denial of service, prevents the normal use of the communication facilities.

So, there can be a denial of service right. So, dos attack very, what we say quote unquote popular attack so to say to create a denial of service everything is in place, but you cannot access the information. So, there is a denial of service attack.

(Refer Slide Time: 25:06)



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

IIT KHARAGPUR
NPTEL ONLINE CERTIFICATION COURSES
NPTEL

So, what are the based on this? If you look at the difference security services; so it is confidentiality. So, some sort of a service call privacy, authentication who created or send the data to find that authenticate? Integrity has the data has been not been message has not been altered, non-repudiation the order is final this is this is a typical thing like, like if I say instruction over the over the internet over a message to the bank.

And say transfer x amount of money from my account to some mister something, abc is the account alright. So, some (Refer Time: 25:49) the bank transfer based on the thing, then next I later I say I never told this, right I never told that to transfer the things. Right how do you created the things right. So, that requires a some sort of a non-repudiation. That is weather how can I guarantee the order is final. I buy a ticket, yet ticket or l ticket or bus ticket through some internet service, and then I say I never bought that right.

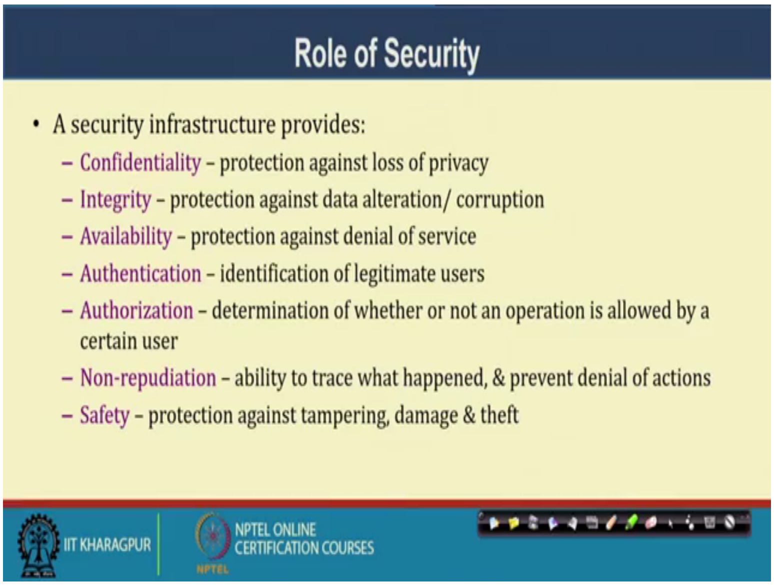
So, how do I say that I only did, somebody else has not this, whether the bank has itself not did right. So, then the bank there are different mechanisms like one is going to digital signature. If you recollect that now it is not that required otherwise we need to do some while purchasing something from is a departmental source swiping your credit card or debit card, they will give a paper where you sign and they will keep that sign thing and give the things.

So, why that is whether you think that they are it is not possible that thousands of sleeves are going to banks and type of things. It is basically if there is some allegation that it is not then they will show that see this is a sign thing right. So, this is a case of non-repudiation. So, what we use method of OTP, or sometimes that active the mean spin to enter the things. So, it is says that the order what I have given is final, you can go ahead with the things. There is another aspect what is we call access control mechanism right.

So, they are while you are accessing things over net internet it set that so that is what will be the access control mechanism right. So, there are different type of access control mechanism like mandatory access control, discretionary access control, very popular is a role based access control, based on my role what I can access is defined like based on the role I can access this type of data set or this part of the network and type of things right. So, this is access control also prevent misuse of the sources.

Then finally, we have the availability. So, permanence on non-erasure of the things like. So, if I am able to access something over the internet. So, and if I have a right to do that, then it should be available to me, right. So, if any attack on this availability there will be a denial of service attacks right. So, the you these services are some sort of a dos attacks right. So, there can be viruses which deletes a file right this is also attack on availability right. So, there are these are different security services which tries to prevent this type of attack, or give this type of things like availability ensured, confidentiality ensured, authenticity ensured, etcetera, etcetera. Access control is ensured and so and so forth.

(Refer Slide Time: 28:58)

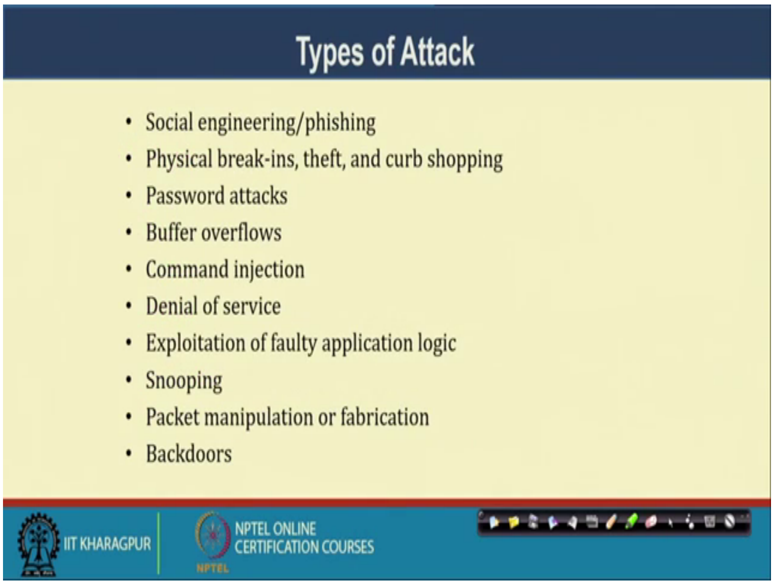


Role of Security

- 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, role of security: a security infrastructure provides confidentiality, protection against loss of privacy, integrity, availability, authenticity, authorisation, non-repudiation and safety protection against tempering damage and theft. So, these are the role of security features which is true for other computing system, also true for our network systems.

(Refer Slide Time: 29:19)



Types of Attack

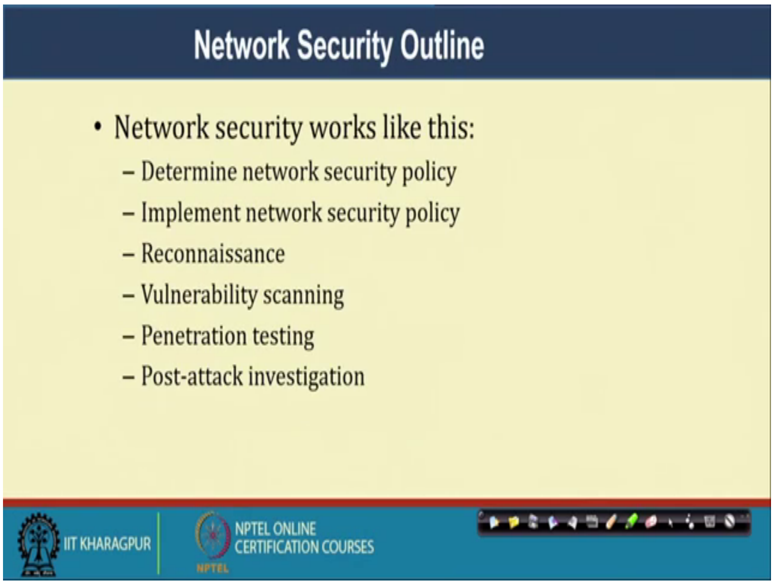
- Social engineering/phishing
- Physical break-ins, theft, and curb shopping
- Password attacks
- Buffer overflows
- Command injection
- Denial of service
- Exploitation of faulty application logic
- Snooping
- Packet manipulation or fabrication
- Backdoors

IIT KHARAGPUR
NPTEL ONLINE CERTIFICATION COURSES
NPTEL

And also we have seen type of attacks. A very popular one this days is a social engineering or phishing. Physical break ins theft curb etcetera is there physical attack password attack. Buffer overflow attack, right overflowing the buffer and going to the other segment and type of things.

Command injection type of things like a we or that SQL injection type of stuff. Denial of services, exploitation of faulty application logic, if there is a faulty application logic in the systems, if it is there then I can do a attack on the type of things. Snooping, packet manipulation and fabrication, backdoors and these are the different type of attacks what is possible.

(Refer Slide Time: 30:10)



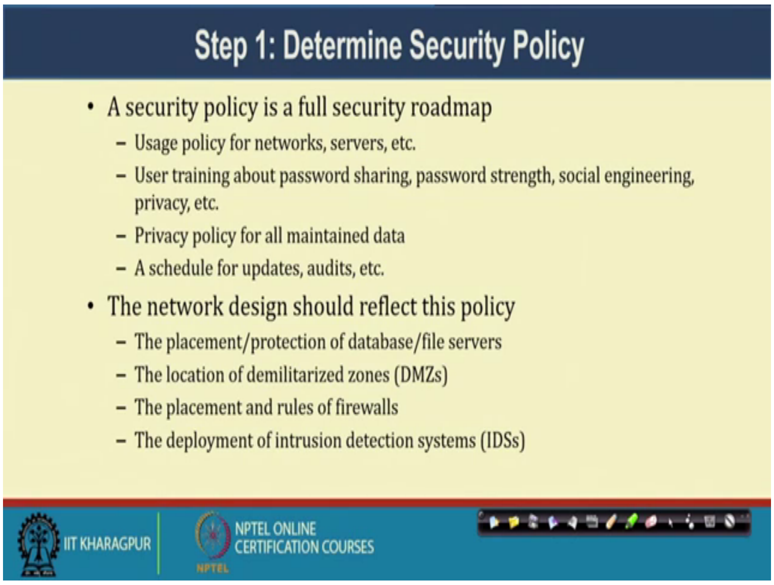
Network Security Outline

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

So, with this thing if we try to look at that what is our network security outline. So, it works like that determine the network security policy. Say, if I take a it infrastructure, what is the network security policies? Implement network security policy. So and there are other that, so one is determining then implementing, then other aspect is reconnaissance, then vulnerability scanning penetration testing post attack investigation.

So, these are the different; these are the different what we say steps towards securing a network. So, will look at step one by one that what are the different aspects of the network security right. So, how to go about it this network security aspects?

(Refer Slide Time: 31:12)



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, state step one is determine the security policy. So, security policy is a full security roadmap, right usage policy for networks servers etcetera, user training about password sharing etcetera. So, what we say making the user aware of these are the things. There can be privacy policy of maintain data.

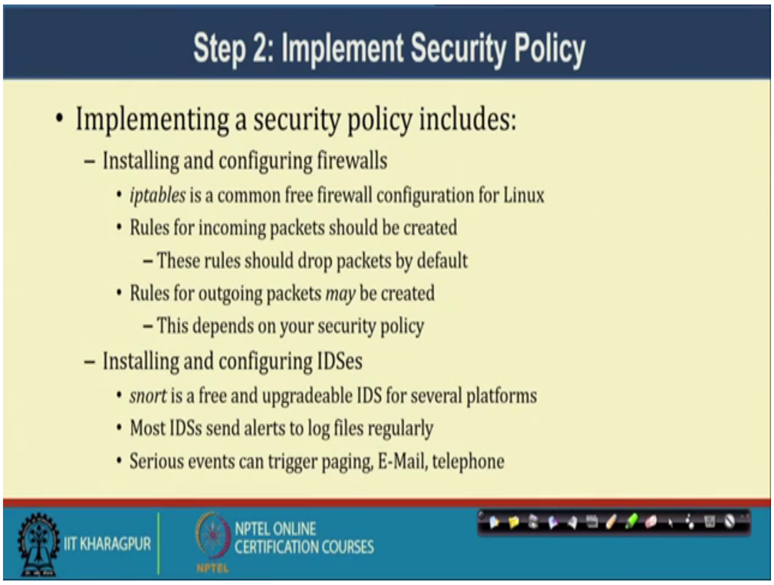
So, if I storing the data, what is the privacy policy a scheduled of updates audits etcetera that is also important. So, there is user's policy of the network server etcetera. So, user training about user making the user aware of the things; privacy policy of the data maintain data or the stored data, scheduling the updates laptops things will be there. So, it should be there the network design should reflect this policy. So, whenever we design should reflect, replacement production of database file servers. Placement and protection of the database, file servers why it will be placed, whether it will be in the DMZ zone or where location of the demilitarized zone.

So, there is a concept of demilitarized zone. We will see later. So, what we say that see if IIT Kharagpur is a secure network; if you want to make this IIT Kharagpur network secure. So, what are my exit point? Typically, the exit points are the routers by which things are connected at to the external world. So, what I mean what is my basic goal, I want to basically secure these exit things. Or and so, in other sense I want to make this militarized zone.

So, to say right so these are my militarized zone. So, but some of the things I want to expose right like my web server I want to expose, people should see that my webpage and other things. There can be different other some of the applications which people can want to work from the outside that is to be exposed. So, these are to be put into somewhere what we say demilitarized zone alright. So, this is important to look at that what are the different scenarios of this demilitarized zone. So, the network design should reflect this policy should this policy placement of rules and firewalls; the deployment of intrusion detection systems.

So, where do I put the firewall? What should be the fire wall rules? And there should be a deployment of intrusion detection system. So, if there is a intrusion is there how to detect that system; rather there is a another sort of systems called IPS intrusion protection system.

(Refer Slide Time: 34:02)



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, implementation of security policy; so implementing a security policy include installing and configuring fire walls. It may there are different way of handling this. So, we are not going to the details of the things. So, IP tables is a common free firewall configuration for Linux, some of you may be worked on it or knowing it. Rules for incoming traffic should be created. Rules for outgoing traffic should be created. Like, I can say that incoming traffic only http is allowed, where as outgoing I can allow we allow telnet ftp type of things.

So, both the rules should be should be there in the fire wall. We will try to see those things when we look at that little aspect some aspects of firewall configuration. Installing and configuring IDSes like so or that intrusion system detection systems. So, there are different tools some freewares are available, some are paid things are available, right. So, one is not is a free and upgradable ideas for several platforms. Most ideas are send alerts to the log files regularly. So, it is logged serious events anti guard paging email and telephone right.

So, by these 2 things what we are trying to look at is the one aspect is that determining the security policy. Say, what will be the different de security policies. Another aspect is how to implement the security policies right. So, these are 2 things are important, other than other miss will come to that other aspects of the things. So, when we frame a network right. So, when we try to trying to design a network. So, along with performance, efficiency, reachability, scalability, we need to also keeping to mind that what should be my security policy, while implementing, or deploying the network whether those security policies are implemented into the system or not that needs to be looked into right.

So, what we will do? We will continue our discussion on network security in our subsequent lecture, and with keeping in mind that our basic network infrastructure into thing. Also we will try to see some aspects of the things like whatever we have seen that, in the TCP IP layer, what we can do with those things with the security things, right. Now we see the TCP IP layer or OSI layer per se does not talk about the security aspects.

And security comes additionally in doing so we should be careful that intermediate devices which gives this packet with there should not be any problem with the standard right. If there is a problem or if there is a intervention or there is a interference with the standard that the packet may not be forwarded to the next hop right. So, in there are lot of consideration which need to be looked into. We will try to see some aspects and overview of the things which keep as a overall feel of the what are the network security aspects.

Thank you.