Slide 26

Last time we talked about ,and mechanism ,if you remember, the most important security services were, authentication, integrity, confidentiality, non repudial, access control ,traffic flow confidentiality, and we use on major mechanism to implement security services. That was encryption definitely ,cryptography in other words, And the other techniques are going to be based on cryptography. Lets discuss the security model of the computer networks, but before going into security model, lets discuss, what type of technology we need to have in today's technology. We have to talk about the advantages of the computer networks. You guys are familiar with it, computer networks ,when you guys have it ,you guys have to share the resources or you are going to increase the reliability , or you are going to distribute the workload ,and you are going to make it expandable. If you want to add something ,you can add easily ,if you want to remove something, you can remove it easily. But while sharing resources you are going to have one major resources, what is that stuff. That is security, if you are sharing something with someone, you are going to protect that thing basically. When you share the resources ,you are going to share the security. So, you are going to find the way to share your resources in a secured way. They say computer networks helps in reliability, do you know when computer networks are more reliable or less reliable. What is your opinion??.. people think computer network is more reliable, but it depends on network configuration. If one server is down and if there is another server, then you might not talk about reliability. But if the first one is down and second one is up ,then you will say that these networks increases the reliability. So it depends on the configuration of your networks. But we know that we are distributing the work load, distributing is the major thing in the computer networks.

Slide 27

For network security problems ,sharing will be the major part , when you are using the complexity, you need to do sharing, I don't like, complex stuffs in security, because complex stuffs increases the weaknesses in security. You may not see that because of complexity. And the other thing is unknown parameter, I don't know the limits of my system now, does it starts from this point and ends at that point. I don't know the limits of my system, if you don't the limit of your system, then how you are going to provide a parameter protection ,its not going to be easy. Also if you don't know the parameter. There are many point of attacks that are possible. You don't have control over your network , you don't know the limits of your network ,so those points will become the attack points of network security and for unknown path, you don't know the path basically that you are taking and you have no control over those paths anyways, for example you are sending email to your friend and how are you going to control the communication ,you cannot, they will not allow you to control those kind of networks basically ad how are you going to do, you are going to rely on there network which they will not allow.

Slide 28

Another thing is the exposure that you are going to get exposed is different, the number one is privacy, privacy is with many unknown users on a network, concealing sensitive data becomes more difficult. This is one of the major thing in today's world basically, the identity and certain kind of stuffs, they are

all attacks on privacy and everytime I ask these questions to my students, I jus ask this, if your identity is stolen what are you going to do, or what steps that you are going to take in today's world. Report to these three major credit companies ,and names of those companies are ,trans union, Experian and the other one ,I am not remembering, anyways three major credit based companies. Report that your identity has been stolen and your identity will be valid only for three months. For every three months you are going to report it ,and you will give your cell phone number ,so whenever someone or even you apply for something or the other ,they are going to call u and look for the authorization from your side, that is the only protection mechanism that you have . There is a company now identitytheft.com, if you arepaying $10 ,then they are going to protect your identity. So for every three months, they are going to report your details to these three major companies. That will say this is my SSN number, this my ph number and I am going to disclose all my details to all the people all over US. If somebody stoles my identity ,then iam going to give them million dollars, but somebody stole his identity, by the way, but they didn't use it in anyways, they said this one million dollar was just a mistake and it wouldn't happen anymore. You are reporting to those companies, that means that you are placing a effort on the alert,so who ever uses your credit by your identity then they are going to call you. That the protection mechanism. That is not good enough ,that is very dangerous basically. And it will pt lot of burden on user side, which is you. They are keeping lot of information about you and they are selling it back to you which is not free by the way ,and then they are selling the same information to the other companies, and they have no idea of the data that they are finally keeping. Now the privacy prices will come low with the new president as discussed in congress. So the companies will be made more responsible and they will be handled more duties, so that you don't have to go for everything to the company. And you never gave permission to give some kind of report about you . So why should I do that stuff myself. So this is the privacy technique and data integrity because more nodes and users have potential access to a computing system ,the risk of data corruption is higher. So we need a integrity mechanism ,in authenticity, it is difficult to assure the identity of a user on a remote system. It is really a difficult job especially if the user is in the remote system. It is difficult to identify the user ,if the user is on the same system ,it is easy , but if it is the remote one then we will have some problems. So these are the exposure in the network security world, while we use the computers three major things , piracy, data integrity and authenticity.

Slide 29

The network security model that we are going to use in today's world is this , there are two guys trying to exchange data, this message is going to get transferred from this guy to the other guy ,but this message will encrypted by using the secret info, known by this guy and there is security related transformation which is actually encryption algorithm ,so what we are going to do is, we are going to encrypt the message by using the secret info , by using the encryption algorithm and then we are going to and we are going to transmit the data towards the destination and when the transmitters receives the data. It has dicpher it and for that decipherment, it has to use the same algorithm at the destination. It is the key for the algorithm, secret key I should say. You see the idea is very simple, I need to have the secret info key, I have to have the encryption, I will not say that encryption algorithm should be secret. Generally in today's world we are not going to work by any secret algorithm, that is called secret by

obscurity. They are in other words, obscuring the algorithm In this crypto course what we are going to see is all the algorithm publicly encrypted in the secret course. The used algorithms that are used here and there will be publicly available algorithms nothing will be secret about the algorithm, everything will be known about the algorithm. So, we are going to work only on using open algorithm . So we have the algorithms we have the secret info and everything. As you see in this model ,there is an intruder, so this intruder will monitor the communication and try to get the message back or try to see the content of the message that you are seeing and to do that , intruder knows the algorithm and nothing is secret about the algorithm ,without the secret information intruder cannot decipher this message and cannot see the content of this message security relies on the secrecy of your key, as long as the key is secret ,the key is secured, if the key is not secret, then key is not secured. You may use such an algorithm, lets say the algorithm is unbroken and it is impossible to break the algorithm and you see that it takes million years to break that algorithm ,but if you cannot keep the key secret then there is not meaning of all those algorithm details basically. Actual security will come from the secrecy of the security key basically. Without the knowledge of the secret info intruder cannot , decipher the message, the question will be this, how destination will come to know the secret info ,here we say that secret info that we used should be known by the destination ,but how this destination will know this secret info?...certificates are not for these kinds of info ,they are used for public info and not for the secret info. Third party ,like this judge, the functionality of this judge is this , the judge is going to create the secret info and it is going to transfer the source to the destination .So by this way, source and destination will have the same secret info. So that they can exchange the secret messages right now. But if these secret info is not secured enough ,then there is no secret in your key basically. So this distribution must be secured enough to provide security to your network basically. And this distribution is the biggest deal in this security ,unfortunately, or I should say fortunately, that is going to solve these key distribution problem , but trusted third party is not a good idea. And in security we are trying to eliminate these trusted third party. We do find it very difficult to find the trusted third party. Who am I going to trust??.. Is this thing is government then forget it, private company ,then forget it. Because they are going to sell these things if they pay some money or some other independent establishments. I don't know ,you have to check them in details basically, in other words. We are having difficulties in finding ,trusted third parties .Because look at the transmitter, he knows your secret, your secret is your security. And sharing this secret ,especially with some one else. In today's technology we are eliminating this third party. We are not going to use any third party ,instead we are going to use a good encryption algorithm ,lets say RSA algorithm to distribute our secret info, and that's going to solve our problems, if you see, this is the model of today's security and these model is also having lot of problems, our job to focus on those problems, In this course we are going to focus on security related issues. Distribution of secret info and integrity and authentication . So those are going to be the main focus in this course. So are you guys clear about this.

Slide 30

Lets move on, components of the techniques for providing security. These as I said, security information related transformation to be sent which is going to be encryption algorithms. Some secret information shared by two entities and its unknown to the intruder .

Slide 31

So trusted third party is responsible for distributing the secret information to the entities and responsible for settling disputes between two entities concerning authentication of messages. If somebody say, hey this wasn't my key and some body stole my key , and send this message to me, then e are going to go to the third party and that third party will decide ,whether that message belongs to me or not.

Slide 32

So these are the elements that we have in the network security model. Let me ask a question to you guys, if you want to design a particular security service what steps you should take ??.. the first step is you are going to design or choose a security algorithm ,design part is a little bit tricky part, I don't recommend to design, the security algorithms if you are not competent in math or in cryptography. Because it is not easy to design, and we don't have million of cryptographic algorithms ,we have only hundreds of encryption algorithms and with the public key cryptography even that 100 will become 10. We don't have many algorithms, what we do basically is we choose a security algorithms . There might be some unknown algorithms choosed by the secret agencies ,but we are not dealing with those kinds of algorithms what we are working on is publicly known. So we are going to choose the algorithm, lets say I choose DES algorithm and if I choose des algorithm then we have to choose secret info for that des algorithm ,secret information is the key that I am going to use for that kind of information ,in some algorithm, key or key generation ,may become important for those kind of information . let say in RSA algorithm to generate a key u need have finding very large, finding very large number itself is a (…..)..So you need an algorithm to find those prime numbers basically. So you need to do some calculations to find some inverse or some modular or some transformation so you will be able to generate the keys. So, in some cases you need some algorithms to generate a key, but in some cases you are going to randomly select the algorithm. 64bit for example and that 64 bit will be your secret key for your des algorithm. And you need to develop strategies for the distribution and sharing of the secret information that is one of your crucial part. Your security depends on the security on this key. Or security of these strategies. If you are not using. If you are not using proper security distribution stuffs, you are going to be in trouble. Thus you are going to specify a protocol to be used by the communicating entities. Either tcp or udp .So these are the basic tasks in designing a particular security service.

Slide 33

As you remember encryption is going to be the most important thing for everything and we are going to have two types of encryption ,the first one is link encryption ,it is going to provide physical protection and the other one is end to end encryption ,we are going to provide confidentiality. But what Is the difference between link and end to end encryption

Slide 34

So lets have a look at that ,in link encryption these two communicating entities are going to use link encryption algorithms there should be router somewhere here and for some reason, router doesnot show up on my powerpoint presentation. There is a router right here and this guy will transmit the information to this physical device and the data will be encrypted and will be transmitted to the communicating link to the router as there is a router right here. So everything in this communication link is encrypted, so think about protocol errors. Lets start from the application layer till the physical layer. All the protocol layers are encrypted including the data. When the message comes through router, router needs what, ip address to transfer the packet. But ip address has been encrypted, what we are going to do is we are going to decrypt everything and send the content of the ip header and based on that ip header, it force the packet to this site and it encrypts it, everything is encrypted to the physical layer and transmitted to the destination. Destination has physical encryption devices,these are physical devices, (hotwire..) devices.so it deciphers the message and recives the message back. So everything that we use in the communication link will be encrypted, so it is a pretty good, encrypting method, but only trouble is this router here. In this router we have to decipher everything so that security becomes security of the router basically. If the router is not working then everything will be closed , so that is the drawback of the link encryption ,what are the advantages of these link encryption is everything will be encrypted and you will not see a thing basically. This is generally used in military basically, in military we are going to use these kind of stuffs basically. And the other disadvantage is these are hardware devices and they are expensive. Other thing is each device has to have a secret key to encrypt and decrypt the data. And imagine you have 100’s of routers and 100’s of these kind of communication link and you need to have 1000’s of devices and you need to have secret keys for all the devices for which you are going to share. So the key management will be going to be very big deal . It is not going to be easy

Slide 35

But with end to end encryption communicating parties will be communicating as it is and this time its going to be server side and decryption will be taking place on the destination side. I am not going to encrypt everything, iam going to encrypt only my software data, on the other side within the computer,it is not a physical device. It is just going to encrypt your data, all the data will be on the clear form. Sothat all the other packets are sent to the destination side. So only on the destination it is going to decipher the message. Right now in the end to end encryption inside the router, the message is in clear form or in encrypted form??.So that router security is not big deal for me, so the message will be in the encrypted form inside the routers . So that you cannot see the message inside the router in this form. But in link encryption data is in clear form inside the data basically.