Slide 18

Okay lets continue, I will live you guys, little bit early. As I said there is no software mechanism to check the software mechanism. But their can be something for the hardware errors. Do you guys remember any hardware errors in computer networks or in computers. There are some of them which are mechanisms and are not errors. Like you have the CPU and CPU does not work properly. Or you have the network card and it does not work properly. So those kind of stuffs I am talking about. So, if it does not work, you care going to crazy and you are going to loose your CPU. So, basically that is not the hardware error, what I am talking is while I am manufacturing the CPU. May be during the manufacturing process something happens to your CPU and may be your CPU, may not work properly, for example, lets say you say 2+2, then It might say 3 and not 4. Can you check those kind of stuffs, no ways. There might be error with one floating point modification. With two floating point, it was giving wrong answers. So, the answer was wrong, so lets say Pentium 2 manufacturing, they corrected the error was wrong. For users from our prospective we have this. So, if you have malicious stuffs, basically its going to run, there will be some kind of suggestion ,for these hackers ,they said ,why don't you put such kind of stuffs, in CPU, its not user accessible. You are not aware of that one, that computer will identify with that secret code. Hardwire within the CPU, so that way we are going to follow the hackers. So you can find computer much more easier ,so that way when you see the secret things, you cannot support other kind of secret things which will cause more error, who is going to control those errors. If there is not control mechanism you may have problems. That's a very simple questions, do you trust corporations in this country. Most probably not. If that is the case, its going to be dangerous. {question from a student}. As far as I know, nothing is secret at this moment. I cannot talk at this moment. With the privacy kind of this in this country, it is difficult to manage those secrets. If you get caught, you have to pay lot of amount in respond. So, it is difficult to keep those secrets, with companies like Microsoft to handle those kind of secret which people are not aware off. { Question from a student}. They are checking the signature of each employer and if they don't have the signature on the operating system, they say that this is not your signature. So, they have caught like that. { question from a student}. If you don't have agreement with Microsoft, you cannot manufacture , Microsoft compatible products. They have to be approved by Microsoft, they have to pay money. I was working with those guys on some system, and I had to pay half million dollar for the server software's and we tried to get something for that software, they said you cannot do that, you have sign a partnership contract. When you sign partnership then they do opening of (faces…) , for the developers , so you are going to use those interfaces, and you are going to make those application for windows. And then Microsoft will say that it is a valid application. So hardware errors as I said will not be easy for us to detect. The other is poor management of resources, the other way and important one, poor management of resources, because most of the times, you are going to have problems with this one. If your administrator of your network is not aware of your security, then you will get this problem. What is this problem, you are firing a guy from your company, and you are not closing the account of that guy, and this guy will be a very dangerous guy, believe me, because, he will already pissed that he is removed and he can do any kind of damage, to your company and also to its resources. And people are selecting some passwords for example and they are not checking the passwords, am I right??.. Is it a good example for poor management of resources.. No one is checking your passwords, if someone is checking your passwords

,then you are in big trouble, no one sees your passwords, sites do ask to update your passwords, without the knowledge of your passwords ,they do ask you to update, in case your passwords, compromised, but they don't see your password. Even if you want to recover your password, they are again going to say to enter your new password. They will say to enter your old password and you are going to enter your new password. In Linux system, they are actually, encrypting the password, 25 times ..I don't know why they say 25 times. In other words, no one is going to recover that password. But they can say you to select from some passwords, which have 4 characters, two letter, and two numbers, it should be minimum six characters, or 10 characters, so they may say, password crackers in their system. If you say, can I change the password, they immediately say the user to change the password. We are not going to see these techniques in network security. And these are the techniques that are possible for the password management. And that is why if you cannot manage your password in your system, then that is a very good example of poor management. So poor management is a very good technique, for the administrators and also for the company people, for security level and also for security understanding must be improved basically. So, these are accidental things, we cant control them too much. Intentional thing, they might be passive and active attacks. In passive attacks, there are release of message content ,that we have already discussed, and there is another one which is called traffic analysis. What the attackers do in this traffic analysis is , it is momentarily meant for traffic. If there is any ups and downs in network traffic. They may think that ,something is going on in the network. Or nothing is going on in the network. They don't see the traffic going on or messages that are being exchanged or the content of the messages that are being exchanged , but they can see how many packets, they are exchanging among the nodes basically. Doing this kind of stuff may be a valuable information, depending on the taste basically. So these are some kind of intentional network. Lets take military network. And one country is going to attack another country and that country is very well advanced country. All the movements are going from the network and the network is exchanging lets say 12 million packets per second. But one day, lets say its exchanging billions of packets, and politically I know that they are going to attack that country and I am expecting, an attack with an amount or something like that. But when I see the strike like this , to traffic flow, then I can say that this country is ready and they are going, there is very well planned information basically. So we have to avoid those kind of things. And it is very easy to avoid those kind of things, so what we are going to do, we are going to keep the network traffic constant. We have to generate (dumb…) traffic ,if I need to, so we are going to have someone to look at the network traffic. They are going to see (…….) , but they are going to see little bit stable traffic all the time. They can be any real information. If you look at the active attacks, data modification is the most important one, in the intentional active attacks, so someone is trying to capture the packets and when they are trying to change, the content of you packets, so lets say you are the attacker and you are trying to capture the packet, or someone is trying to capture your packet , and you are depositing 1000$ from your account, to someone else account, what you call it, FT, or EFT and you are transferring files from one account to another account, and another guy is your analysis guy and he is going to capture your transfer data, your transferring $1000 from one account to another account. But he just adds, two zero's with this modification, and it becomes immediately a million dollar. When this modification ,you have to be very careful in the financial world ,to avoid those kind of modification, we have to be able to detect these kind of modification very easily. And we have to thank, that we have all these kind of techniques to find the types of attacks. Another thing is data delay, in data delay

capturing the packet is not forwarding the packet for a while, why is that, security of the information is very sensitive and is very crucial for a while. Because after sometime , it might not have any meaning. {question from a student}.. With live telecast, for real time traffic kind of stuffs. But what I am saying is little bit different kind of things. Lets say the stock market, lets say you are trying to buy, Microsoft stocks, and you know that they are going to go up today, you are transferring information through stock block. And this guy is not buying it. The following days the stocks are up and you are going to buy the stocks. Because the blocker did not block and some attacker block the message, and the next day the stock buyer is going to buy the stock, and its going to go high and when it is going to go high, and its going to go down after that, the next day the stock buyer buys the stock which is actually low and not high. And at that time you sue a stock broker, As you are loosing money. Another thing is lets say some (……) through FBI, so they see some (……), lets go and arrest this guy, and if there is a malicious guy between them, may delay the message and inform the other guy and the other guy might delay the message. {question from a student}. Depending on the cases as I said, if could practically could damage, this guy for example , taking the information and informing the other guy these information is not damaging anyone . Keeping FBI out of reach of that guy basically, those kind of problematic things basically, but most of the times the important thing is time dependence. Because of the time delay, their might be some problem with the security. After that time the security may be no longer valid, for that particular case. In those case these delays are very important. Data blocking is another form of delay instead of forwarding the packet, it will block the message and broker will never get the message. {question from a student}. They may depending on the cases as I said. If FBI is going to arrest my friend and I know the information about it and I tell my friend about it, they will go and disappear for one day and they will be enough space for him to go out of the country, in other words, I will find the time and I will find the information about the case. Data blocking is the extending block of the delay. We are not signing anything on the other side. Data copy looks like little bit harmless, they might ask what is the security problem with the copying. If you are message Is secured, then copying, then copying is the big deal, but what they are doing is copying of the data to see the content of the data, if it is protected it takes time. So by that way they will have time to work on the data and the others will not be aware of the copying. They will be receive those messages anyways. So over here these guy, intruder's role is to(…….) , copy of the data. He needs more time to work on those data basically. So that's why they can do these data copying thing. Data replay, this is the big (…….)..of this security , big (….) replaying the big, we have good protecting mechanism for the replaying. Replay is the recording the packets that you are exchanging and later time you are replaying it .For example, money from the ATM machine, someone is recording your information of your transaction, so when you are left ,they are just replaying the transaction. And they are getting money from the ATM machine without your ATM card. That thing is not possible as we have protection mechanisms, we have timestamps and everything, so it is not easy to, these kind of data replay attacks through ATM machines ,for some data replay is very big deal, so we have to the proper protection mechanism for that. One of the major thing is the timestamp basically. Good timestamp will help in secure data transaction ,so that they cannot modify the timestamp basically. And you are protect the replay attack basically. Data destruction, we cannot do anything for this basically, if they have to destroy your data they are going to destroy your data. But for these things we can do a lot of things, we are having mechanism to avoid those guys, if the destruction continues, I don't know any mechanisms for that. I don't know anything that is going to harm destruction. So these

are the attacks, so based on these attacks I am going to develop the security services. And for those security services ,I am going to use the security mechanism.

Slide 19

OSI system architecture. What does OSI stands for , Operand system interconnection. What is ISO, its international standard organization developed open system interface and that operating system interface, will stand for seven layer model for, seven layer reference model for computer networks. ITU is the communication part of the same organization. This guy which is for the security architecture is called X800 and this defines the systematic way of defining and providing the security requirements. It also provides the overview of the useful concepts. It doesn't say the it must be like this, instead it says it should be like this. So it is a should type of architecture, instead of must type of architecture. Which I follow sometimes and security is a flexible mechanism and you as an engineer decide on what to do.

Slide 20

So X.800 defines the security services like this, a service provided by a protocol layer of communicating open systems that ensure, adequate security of the system or of data transfers. It is a simple stuffs, it says RFC 2828, RFC stands for requests for comments, so before anything becomes standard, people are preparing these RFC documents and they are posting it on the internet and they are looking for the inputs from everybody all around the world. After that things becomes standard. So this guy defines security services as, a processing or communication services provided by a system to give a specific kind of protection to system resources.

Security services X.800

In security services , there are 5 kinds of services. They are, Authentication, Access control, Data Confidentiality, Data Integrity, Non repudiation. If you look at the authentication , by definition it is the assurance that the communicating entity is the one claimed. So that is the identity, Lets put it this way, identity, and authentication different things. Identification depends on something u know, something you have and something you are. But authentication is a cryptographic function. To identify the application users or some other things. In other words , I should say most of the identification .So that's the difference between authentication and identification, alright. So access control is nothing but the prevention of unauthorized resources , and data confidentiality is the protection of data from unauthorized disclosure and data integrity is the assurance that data received it as send by an authorized entity. That is also as I said very important security service. One more thing is the non repudiation defined by these X 800 guys . It is the protection against the denial by one of the parties in a communication. If you are sending mail to a stocker to the broker, and he claims that he dint receive the money and he dint receive the mail, what are you going to do at that time. So it means that there is not protection mechanism to protect your mail. I am talking about cryptographic protection, But if you are using, (…)… email client ,there are two options about it. Delivery confirmation and The flow confirmation and rate confirmation, its cryptographic stuff and it cant be used all the time. So email supports that kind of stuff. At least you are going to get the information that your mail has been reached to the mail server of that person. From that to the client you don't know, In cryptography, you are going

to do something that ,that guy cannot say that he hasn't seen the mail. Or he did receive the mail and he went and he worked the stocks, but stocks went low like yesterday or today, the stocks went down ,you lost money and you at this time say that you haven't sent that money. Why you are going to go and buy those stocks. You see there are coins and two flip sides of the coins basically, it could be either, we have to protect that guy as well. If you send that email with all your cryptographic functions ,you cannot deny that you didn't send that email. I will be able to prove that you sent that email . So that's called non repudiation, its generally used in financial industries, and military industries basically, they love these kind of stuffs, in military its very important, you are going to kill that guy and you say that I didn't receive anything, I am enjoying myself here ,right here right now ,so I don't know when did it come, so it could be a big trouble at that time at that basically.

Slide 22

OSI security services. What about services?.. they are Authentication, Access control, Data confidentiality, Traffic flow Confidentiality, Data integrity, Non repudiation this time its two types which is both origin and delivery of data ,These are the major security services for the (…) bases security services, in today's world we are going to have these services basically, they are going to be the major services. Alright are you clear, ok, so what are the different mechanisms we have.

Slide 23

What type of mechanisms we have, so far we identified the different kind of attacks, we saw the consequences of everything ,then to alert those things, which is passive and active attacks, we designed the security services, or we decided the security services. Now if I want to implement those security services, I have to use security mechanisms, that what are going to be the security mechanisms. What type of mechanisms I have for security services. So ,lets See all of those mechanisms , The first mechanism is encipherment, we are going to spend 3 chapters just for this encipherment and we are to see the substitution cipher, transposition cipher and when I see this substitution cipher and transposition cipher, we are going to see actual, encryption algorithms, why these are substitution ciphers and which are substitution ciphers. Like Ceaser cipher and we are going to see those kind of ciphers basically alright, then we are going to move into modern symmetric ciphers ,that's another kind of ciphers like RC4,RC5 ,these are some of the encryption algorithms. Then we are going to move into public key cryptography, we are going to look at the (…….), ECC cryptography and then and also encipherment algorithms. If you see the encipherment, it is the core of the mechanisms. Digital signatures ,it looks like a different mechanism, but actually it is an encryption as well. What we are going to do with digital signature as we discuss. There Is a message right here like this, what I am going to do is, I am going to calculate the hash of the message or digest or fingerprint of the message. So there is a hash algorithm ,message digest algorithm in other words. This algorithm is going to generate a fixed length something. That fixed length something will be going to be the edges of the messages. In other words this is going to be totally dependent on the messages. Change over here will change the entire fixed length algorithm. So, when I create this one, this is a digest of the messages as I said, I am going to encipher these messages, with some algorithms then encryption and then this is the digital signature .So this is the generation of the digital signatures. How am I going to verify it, if you see this , I am going to

calculate this hash and I am going to decipher this encrypted part, because these encrypted part will come with that message. And if the content of this encrypted part ,is equal to recalculated hash, then I would say this signature is called and verified ,so this signature belongs to the guy who sent those signatures. So that is the digital signature mechanism. But you see Digital signature mechanism itself is an encryption. So encipherment as I said, we are not going to go away from this encipherment. And there are some access control mechanisms. We are going to see two types of access control mechanisms (datch…), match. Mandatory access control and (……) excess control. (dis……..) excess control will be useful for security point of view for us. Because it is much more secure than match. It can avoid (……..) attacks. Data integrity mechanisms totally depends on these hash functions. We have one chapter to look at the details of these hash functions . We are going to see sha1, MD5 , RIPHEM 160, HMAC in details, You may wonder why you are teaching this stuffs to me. SHA 1 has some security weakness , so the people who are interested in security decided to change this sha1 to 1010 ,I believe sha112 is going to be the stand after 2010 I believe and RIPHEM you are not going to see the much of these as these are European design ,but we have to see these things to understand the others, others are going to have the same structure as almost and if you are seeing HMAC. HMAC doesn't specify any hash algorithm but it does show us , how to use hash algorithms, then you are going to see the security protocols ,all the security protocols are going to depend on HMAC, we are going to do everything jus for the data integrity, what I am going to do is , I am going to calculate the hash algorithm ,but iam not going to encrypt this time ,after calculation the hash of the message will be appended to this message so both of them will be transferred to the other side, so the other side will recalculate the hash algorithm from the other side. And its going to compare this recalculated hash with the received hash. If you see the things are same then there is no change in the content of the message, so iam going to accept as it is. So this fixed bit message is same for all the algorithms ,even a one bit change totally change the algorithm. You may ask this question ,ok what is the integrity mechanism we are using in computer networks. Let me rephrase the question what Is the checksum mechanism, parity is not the word, its CRC, cyclic redundancy check. How many bits we are use for that??... 32 bits. The length of that CRC is 32 bit and we are calculating the length of each bit and message. If you remember it's a division method. If I divide that , the reminder which is polynomial will be my CRC. With 32 bit CRC's I can detect all the single bit errors. The odd numbers, even numbers, all less than 32 bits. But the number more than 32 bit may not be detected. In other words I am not able to detect all possible errors. Still I am using it and it works fine right, some or the other conviction is rubbish ,okay. But 99% of the time it works good. But that is not good for security and security point of view. We cannot use those kind of stuffs .I must to able to detect all possible errors and modifications. These are errors. Not jus 32 bits ,or jus another number modifications, or any other new modifications and I can do this only using these hash function. Because these hash function are going to generate a unique act for each messages. For example, act of hash ,are going to be unique for messages. We don't need time stamp for integrity, timestamp will be only for the replay. {question from a student}. If you are sending the message in a general form ,then you are correct, but generally in confidentiality services you are going to encrypt these things and then send it to other sides. In other words, may the message confidentiality is not the quiet or the other way. You are right then some one will capture this message changes the content of the message and combines everything and send it to other site and the other site can be fooled. That's true for hash algorithm ,but most of the time we are going to use the HMAC algorithm. And HMAC algorithm need the

secret for the these hash guys. If there is not secret key then they cannot calculate the integrity of the ,so its going to depend on secret key and the message. And the other one is authentication exchange mechanism are protocols and you can see those kinds of protocols. In traffic padding mechanism, I am going to generate dumb traffic for what, for the traffic flow confidentiality, it is the third party we will not see those third parties anyways. Notarization mechanism, we can force some packets to follow the paths. We can do it by some ip protocols. What is the name of the ip protocol that you force to fire packets on routers (……..) routing ,there is option where you can use (……..) routing . You can define , followed by blabla blocks basically. We are not using that one so much as I am providing security for the entire network. So we may need specific kind of security mechanism right now which might be much more secured than the others.

Slide 24

As we now discussed, we know security services, mechanisms. So what is the relationship between security services and mechanisms and the security services and the seven layer. So if I want to implement confidentiality services, which layer is the most good layer. To implement the confidentiality ,if you are experienced in this subject you may know ,if we define all the process, they said these . If you implementing authentication ,network layer , layer 3, transport layer, layer 4, and application layer ,layer 7 could be good candidates, these are should type of approach and not must type of approach. You cant say that you must implement this and all. But it is easy to implement authentication ,network layer , layer 3, transport layer, layer 4, and application layer ,layer 7 ,and even access control is the same, confidentiality you have physical, network, data link, transport session and application layer. Connection less service is 3,4,7 ,Data integrity is 3,4,7 ,Traffic flow confidentiality is 1,3,7 and non repudiation of both origin and delivery of data is only 7 ,so if you look at this table , application layer is the best. If you see something implementing on the application, you can implement lot of services on the application services. The upper layer protocol might have some problem for you. But if you implement something with the network layer, then this time, that authentication will be authenticated for every possible application. If you implemented on the application layer, those implementation will be specific for that layer. You are not providing applications for all possible applications basically, so that’s why lower layers might have some better option for you. So as I said, you have to decide how to implement these security services. So if you see the confidentiality it has the physical layer in it. You don’t see physical layers for others. We also use physical encryption or physical security I can say, for the hardwire connections and some links. For those kind of stuffs we use physical layer. You are going to see those kind of stuffs too. You are going to see two kinds of encryption, link encryptions and end to end encryption. Link encryption is generally, a physical layer encryption, we are going to provide security in the communication link. And non repudiation of both origin and data is only for the application layer. So only application layer can handle that one . Another thing we are going to see in this relation ship between security services and mechanisms. The authentication can be implemented using encipherment ,encipherment is a good way for authentication ,and also digital signatures and some authentication protocols, access control uses only access control and confidentiality, encipherment is important and routing protocol is not important. In traffic flow confidentiality, encipherment and traffic padding , in data integrity , encipherment and data integrity. In non repudiation its digital

signature and data integrity. And the other option is transmit to the third party, or the some one. And keep the transactions recorded like notary and that's why it is called notarization. If you look at these slide carefully every service needs encipherment and that's why encipherment is one of the most important and that's why we are going to focus on that one. So lets finish it today.