Slide 35

In end to end encryption we don't have to deal with security of the routers basically. Before we go into key distribution let us discuss a little bit more. In link encryption ,as we remember the key distribution is the only problem. But here only we need to manage key between source and destination.

Slide 36

But if we can use it both of them together, because in key end to end encryption and end to end encryption you are having one problem and that problem is the traffic flow confidentiality. You are not able to provide communication between the users in traffic flow confidentiality, because the ip header is not encrypted and can check the flow of message to that particular destination. But in link encryption it does provide the good encryption as everyone can see the destination address information. That is the drawback of the end to end encryption {question from a student}.. that's why the security depends on the security of the router in the link encryption but in end to end encryption you don't need it because everything will be inside the router basically. But if you combine both the techniques ,first do the end to end encryption and then do the link encryption that is the perfect solution that you are going to provide. Because when you decipher the message this time you are only going to decide where the protocol header and data is going to be still in encrypted, because ,data is encrypted in end to end form basically in the end to end encryption, lets have a look this way, key distribution, key distribution is the important thing that we are going to deal with. We are going to have secure key distribution and key distribution centers. We will see the details anyways in this course.

Slide 37

When we look at the access control ,we are going to have port protection, access rights and node authentication. These things are going to provide access control for us.

Slide 38

For user authentication we are going to use passwords, passphrases, token or smart cards, personal characteristics. First we are going to look at the passwords, you guys are using it everyday, that is the first line of defense in the network security we are going to use . first line of defense is always the username and password pair. If you want to have still strong defense then you are going to use passphrases. This going to be one paragraph, so you can use it as a password or , may be the login requires two people to be there to login to the system ,so that one passphrase will be yours and the other will be mine, it requires two passphrases. We are going to enter both passphrases, in other words two paragraphs to login to the system. This is going to give greater access control, you can see it in the science friction movies. You can also use token or the smart cards. Smart cards are like credit cards that you can swipe it inside the computer. Computer might have the card reader or some kind of pin from which you are going to be in your computer .and the last one is personal characteristics ,which is a very good technology which we call it biometrics. Biometrics technology for access control, it is gaining enormous popularity ,and it is one of the oldest technology that we are using for user authentication. The first one is the finger prints, we also get finger print mouse, which are 10 dollars in the market. Its

not a big deal anymore, if you touch your mouse it will read your finger and it will allow you to access the system with or without the password basically. It is better protection that we are using. {question from a student}.. because everytime you try to login to your system it will check your fingerprint, first of all the system will check your finger and put in the system and everytime you have to use that stuff. Itseems a very useful technology and I have used that technology for very large clients and we had the most important or major problem in our system. And that was those mouse, because everytime I try to use it , gets dirty and it doesnt read your finger print after it gets dirt ,so you need to clean always before using it. And clients kept calling us saying that your information is not coming as they dint know that here we have to clean the mouse always, n we dint know they had the same problem. Because you don't think in that way when you are an engineer, as you are so locked up with your details ,you don't see those small things which may be the major thing as it was for us. Now we have replaced with smart cards, it doesn't work, may with the new technology or new mouse it could be better, iam talking 4 or 5 years from now. Another type of personal characteristics is cut the finger and place it near the mouse and it will read. Its not a good technique unless you have the finger of the other person. But those guys are also very clever that they are coming with the new technology , right now,these finger readers also checks blood pressure and also body temperature, so that you just cannot cut your finger and place it. Still it is not a proper solution, the other one is voice, voice recognition all the recent cars comes with the voice recognition system, when you say call my home then that thing will call you place ,Microsoft sink is the tool that they use for that I guess. So Microsoft provides you with that tool in your car to call or to play any songs. And for finger prints in cars , lexus has the finger prints when you touch the door,its reads your finger and automates the car. So that you can go inside the car, they say the car which listens to humans. This is a very good technology, where you can automate or activate you car without a key, by your voice, but if you are drunk ,your voice changes and you cannot activate using your voice command and you will be very angry. Or even if you are sick, voice characteristics change again so its not a perfect solution, but if you combine both then it can become the perfect solution, then comes the retina readers, retina from the eyes these are all unique things, but finger prints are not unique technology actually, retina is much more complex than finger prints as we can see around 2 in one million people having the same finger prints. So finger prints are not that unique. But retina is unique, they use laser scanner to scan your retina and it scans your retina and based on the retina the system will allow you to login and people are scared of this technology because it might damage there eyes and its not safer. The last technology that is coming up is detecting through DNA, so you are going to spit on your computer and computer will detect, so that no body will ever use your computer ,if it dint detect your spit then spit again. These are not perfect solutions but they are some new technologies. Another things in personal characteristics is the face recognistion, as there are terrorist activities going on ,especially in airports, they will automatically recognize out face through their database ,we will not be aware of that ,you are just walking ,but there are some cameras that will take your picture without your knowledge ,and they are going to match your face with the face that they are looking for .if its matches then somebody will come and take you immediately. These things are very good technology and lot of people are working on it basically . plastic surgery will not completely help to change the face as they show it in movies. They can change the shape of the nose or eye shape some thing like that. But I don't know those systems, whether or not we can cheat those systems. Right now we have to change the US passports , within five years or something its going to change all over the world .now the passport will

carry the biometrics of yours inside a chip and so when you be in the custom and if the password of yours matches with custom officers system and then you come officer, your files will be with him in his system and your finger print will also be there with him . I hope in Missouri there was some kind of proposal in parliament, that some people have to put (rf…) chips inside the skins of the workers who are working in that company. To check the details and the confirmation of the workers in that company. And the government rejected due to privacy law and said this is the invasion of privacy. My point is people are going to push those things in future and people will carry (rf..) chips like dogs and cats I think. Because dogs are already having ,them, basically if they get lost then we can detect them where they are and we are going to pay a lot of money for that. So we are going to be the only one with (rf..) chips .we don't need anymore fast tracks, when we walk towards the gate, both will communicate with those chips and you can pass through the bridge basically. So those things are coming in the future,they are going to push to that direction. So this personal characteristics in authentication will be all around us in near future basically. But we are going to see more in the future.

Slide 39

Next of traffic control, we are going to pad the traffic or we will do routing control.

Slide 40

In data integrity, we are going to use parity, checksums, cryptographic checksums, digital signatures. But in cryptography we are not going to use parity, and checksums. We are going to use cryptographic checksums and digital signature and we are going to look at the details of those guys anyways. Because these parity and checksums in computer networks are not good enough for security . they will not detect all the errors but some errors, but with cryptographic checksums we can detect all possible errors, that is the difference between checksums and cryptographic checksums.

Slide 41

The other one was network security model, this is the other one system access model. In this model we are going to identify and authenticate with these three things something you know ,something you have and something you are. What are things that you know ??..passwords, passphrases, username, pin numbers all those stuffs. Something you have is keys ,tokens, smart cards, all those kind of stuffs. In companies they do create one time passwords .so when you press that thing its going to create a password on the destination thing ,so that password is matched and you can login to the system. So those kind of stuffs are also comes under something you have. That's going to generate something but you cant predict that thing. Something you are biometrics, personal characteristics basically . something you know ,something you have and something you have is going to be the major thing for us

Next slide

For the access policies we are going to work on these models, and its going to give the major access policies.