Advantages and limitations of CTR

If you look at the advantages and limitation of counter mode efficiency we can do parallel encryption we can do in advance of need and good bursty high speed links ,wireless links are not in high speeds, its kind of variable bit rate traffic that means you are transforming images, images are actually very good example of bursty high images, you are watching television news and anchor women are not moving there is not much to describe but if you are watching a movie, cars are moving, cars are bursting then you are generating more data for one scheme you want to transfer the same thing with low level, you are not going to watch those movies you are going to see lot of freezing on your screen basically and at the same time I have to increase the capacity of communication for bursting traffic and imagine I am encrypting those things then you are transmitting ,then it is going to be good candidate which is good technology anyways ,you are watching videos, download movies from Netflix and you can watch it, how that is possible because of those communication links and of capacity and those can be easily indicated for the requirements of the application and that's for the computer networks, so random access of the access to encrypted blocks provides good security , and there is another rule for this kind of mode which is must ensure never reuse the key or the counter values or the counter pair , you are going to use one key one time and not using it again and that is the requirement of these guys and this wireless security ,IEEE. A or b or c they are using these kind of ciphers and they are generating algorithms which is RC4 algorithm ,this algorithm generates the key for vernam cipher in the in the implementation for algorithm to reuse the keys for this encryption if you use these guys an attacker can break the algorithm and that happened for the wireless security ,in 5 yrs ago ,some people in Berkeley managed to break this algorithm because of poor implementation everything sounds good ,and I m generating it randomly if you are not obeying or if you are ignoring this kind of rules then you are having problems ,right now it is pretty secure but in future it is pretty standard IEEE 802 .e they are completely changing it and its going to be AES. They are going to use AES for encryption.

Confidentiality using symmetric encryption

To avoid those kind of stuffs we are going to have these things workstations on LANS to access other because LAN kind of networks are broadcast networks .it means when you transfer anything to local area network everybody on it will receive the information . lets say if one them is receiving the email then each one of them will receive the email . okk?..because that thing will be going around the segment and you are going to see those segments basically . we have ciphers and we can use that software to cineph the broadcast network of the network , going to internet and if you see ciphers there are lot of them and you can download them, and you can actually see the network information who is sending what kind of information ,but you should have some rights to install those programs actually, what else LAN is interconnected with switching and routers ,so switching and routers become very important and external lines, these are the radio or satellite links will be the problem ,if you consider attacks ,it will be snooping from another workstation ,then use of dial in to LAN or server to snoop ,we don't use this kind of stuffs anymore, because right now for remote excess to lans we are using what?... in the past we were using dial up servers , you were logging on to campus network to get the campus services ,but now we don't do all those dial in things, we are using something else what is that something else, and we are using VPN's that is the most secure on at the moment so for the general

purpose we have the VPN's to access the local area network and we may also monitor the external links and these are the possible things thatcan happen in that scenario.

Slide70

one is called link encryption ,in link encryption what we are doing is this guys circles I should say we are putting the input and the output of the router of the switches ,you see every input part and every output has these kind of devices and these are physical encryption devices. Because encryption should be fast as these are fast links and the only option we are having is hardware implementation of the encryption algorithm , and it is another science actually and lot of people are working on that side to implement RSA, APJ implementation and many more and it is very hard in today's technology. So anyways we are having those kind of physical devices that provides encryption on the communication links, so who ever taps on the communication links will see nothing except the encryption things and the other things that we are going to see is the these black darks over here, or black circle it is called end to end encryption and I don't care about these guys and what I do care is providing security between source and destination, I am going to encrypt the message and encrypted message is going to trail in the message , so what I am saying is this and lets have a look in detail and lets say link encryption ,in ink encryption what will happen is as you see these two guys will be connected to each other through wires or switches or something like that, and each one of them will have a hardware encryption device. Imagine hardware AES and hardware DES. So anything that is going to be transferred to this guy will be encrypted, at the physical layer and when you encrypt the message in the physical layer, you are doing what, you are encrypting everything including protocol headers like, IP header ,tcp and datalink like that and if you are encrypting the headers ,you are dis functioning the routers and without IP knowledge, routers cannot route the packets ,so before going into routers I am going to decrypt the message ,so that router can see the headers and they can see TCP and IP anyway, so based on that one its going to route the packet in this data and when it puts the data in communication link, its going to encrypt it again ,so if you are tapping this communication link ,you are going to see only encrypted data and you don't know, you don't know , source or destination or port or information itself basically ,I am hiding everything and this is a standard In all military application ,it should have these application ,these are fast, and communication is faster and you need these kind of hardware encryption. And also it is hiding everything and traffic analysis is possible anymore ,because I don't see the destination IP address and these are the major advantage point of link encryption and what is the disadvantage, router , why the router is disadvantage ,because inside the router including the data is in clear form. Any security bridge to this router will jeopardize the whole system , in other words the whole security becomes security of the router, if you look at the router the major thing is the password protection in other words they are controlling the password and if you break the password then you are going to be in, so in that sense this is not goingto hep too much ,as far as traffic analysis is concerned this is in perfect shape as I am hiding everything. And the second disadvantage point that I should say is the key management, this guy will share a secret key, and the other guy will share a secret key , so every user or port of the router, and multirouters you will have secret keys and how many secret keys you have,and square they say, square type of relation ship ,if n is thousand then these things become very big deal, key management thing is not easy for big networks ,but it is still manageable, and it is not that easy and second thing is money,

this security devices are expensive and you are going to put it every node in the network. And if the network is the big network ,imagine bank of america using link encryption and all these networks ,every crypto device will have these kind of device and so imagine the money and facilities that have to provide to have this kind of security .ok?.so its not going to be practical actually, but these guys are having it for some limited networks, of there own , like bank of America, as you see this not going to help us to solve the problem but it will help to solve the problem of confidentiality, in end to end encryption iam going to do same kind of encryption and this time its not a hardware device. This is a software implemented on the computer, it will be data link layer, transport layer , application layer, so what I am doing here is I am encrypting the data and I am living the headers, in clear form ,so over here you are tapping the information what you are seeing is clear protocol header and encrypted data, so you are not going to get information on the data that you are transferring but you are getting information of the data, about its destination and its port, like email or port you can atleast understand the application, from the protocol header, so it doesn't provide any protection against the traffic flow analysis , but it does for confidentiality ,right now you can look at the router and switches ,inside the router and switches, switch data is in encrypted ,its not in any clear form anymore and it will provide good security to the routers and the only drawback is this is not good against traffic flow analysis kind of things and it is cheaper than, physical encryption and link encryption, I don't need hardware devices anymore and I don't need hardware devices in the network all I need is the software implementation of the crypto algorithms in each, computer that's it, it is much more cheaper and the other thing is the key management and it is only, source and destination it doesn't include any intermediate nodes and it is much more simpler than,the key management in the link encryption, ok??..{question from a student}..it is a little bit slower ,but software implementations are getting little bit faster so you may not get, to feel too much, if the communication then you may think that you don't not need this software. Because it is slow and you need to have hardware, most of the algorithms and software's are pretty much faster except the public key algorithm ,look at the AES algorithm ,or any other, they are fast and have only 4 look up tables, and nothing else basically , in link encryption occurs independently on every link but in end to end encryption occurs between original source and destination.

Key distribution

Major problem of the encryption algorithm is the key distribution , if you don't solve the key distribution problems then there is problem ,that why symmetric encryption is the secure key distribution ,if you don't have the secure key distribution then often failure due to break in the key distribution scheme and this going to be very important especially in PGP smime Kerberos and SSL all of those major protocols will come up with there own key distribution problem and most of them public key cryptography except Kerberos ,it doesn't use any public key cryptography and everything based on symmetric encryption so you don't have options to distribute the keys for the Kerberos environment and we are going to have solution for that and that solution is the needam shroder key distribution algorithm and when we go into Kerberos we can understand the how Kerberos is distributing the key and when we go into other protocols we are going to discuss the key distribution of that protocols