SSL master key generation

Let s start with is new setting , in the last class as I set there is video recording sound mpec format and also enhance sound and video , you can download this video using iPod or you can watch it using the enhanced version ,lets start with the last part of SSL protocol what we are seeing is the generation of cryptographic parameters and cryptographic generation so far you understood SSL has more than 1 protocol one is handshake protocol and the other one is record protocol and the other one is alert protocol but the major part of the whole thing was handshake protocol we exchanged 10 message with that protocol and with that one we exchanged certificates we decide about the keys that we use, what were the major keys that we have to decide, client write Mac key and server write Mac key ,client write key and server write key and server and client keys sp these are the generation of keys basically , we are going to see master secret generation in this generation as you see ,we are going to use a premaster secret and his premaster secret is generated by the client and the size of the premaster secret is 48 byte, generated by the client, but the question is this , this premaster secret is going to be calculated in both ends on the server side and also in the client side how the server know premaster secret?..we have an option and that is RSA encryption of parameter secret ,what we are going to do is we are going to encrypt the premaster secret ,and then we are going to send it to sever and that serer is going to recover that one ,and that is the way to distribute premaster secret, let me go and have a look and the other alternative is we going to use differ Hellman so both ends will al the secret, so we are going to come with 2 options one is RSA for key distribution and diffehellman for premaster calculations ,now both ends have premaster secret ,and by using that one we are going to generate the master secret and generation of master secret is depended on this algorithm t hat is client hello random number and server hello random numbers are going to be appended ,remember those random numbers ,exchanged with that messages with the hand shake protocols ,and that is going to be appended to premaster secret and that is appended to SHA CCC and everything is going to be SHA and output is appended to premaster secret and its input is MD5 and out put of md5 is input to client hello and server hello and appended to premaster secret and append to BB and appended to premaster secret and input is MD5and output of md5 is appended to client hello ,server hello, and premaster secret and it will be appended to A which is sha and output will go to md5 and the result is master secret the master secret is the function of premaster secret idea behind the SSL master secret generation ,what we are going to d with master secret ,we are going to use this master secret for necessary secret generated using HMAC calculation and also for encryption,

SSL cryptographic parameter generation

So client random server random appended to master secret appended to CCC and that is going to be input to sha1 algorithm and output of sha is going to be append and output of that is going to go to md5 and output is going to do go to client hello master secret appended to SHA BB, which is the input to SHA and output is going to go to md5 and that Is appended to client hello ,server hello ,master secret appended to SHA A, which is the input to SHA and output is going to go to md5 but there is no ending for the algorithm why is that with this what im doing is this , im generating server write Mac key and client write mac key and server write key and client write key an d necessary iv and what is the result of this key block what is the size ,output of md5, 128 bits, you are going to use 128 for all those keys , every

output of md5 is going to give one block of key, one block is used as client write Mac and second is used as server write Mac and third is used as client write and fourth server write , and that's why there is no ending here ,based on the size this could go like this with DDDD, but it's the same random number the only things that going to change is characters here by using the premaster secret I can use the master secret based on the algorithm in previous slide , right now both ends have the same master secret and based on cipher suite remember cipher suite all the algorithm we define cipher suite, based on all the requirements ,they are going to cary the key block for the required key length and all the necessary keys that's the idea.

TLS (Transport layer security)

It is defined in RFC 2246 and it is similar to SSLv3 with minor differences what are those record format version numbers ,remember Mac calculation in SSL ,it was like HMAC and we didn't xor the key instead we attacked , so HMAC is used directly and a pseudo random function expands but the key generation depends on this pseudo random generation ,some additional alert codes ,some changes in supported changes most of the cipher supported by SSL is supported by TLS ,except 1 that is fortezza it is the hardware based on cryptographic algorithm ,but its not supported by TLS ,changes in certificate negotiation and changes in padding . The most important part is this part that is pseudo random function in tls is defined like this there is HMAC there is a seed and there is a secret seed is going to be the input and secret is the key what is the seed for hamc ?..its IV , output is going to go and get A1 and the other part is appended to seed again then go to hamc and I will have one block of key from this output ,but the first output is going to go to another HMAC and it will be appended and it will go to another HMAC and it is the second block and second output go to third HMAC and appended to the seed and again appended to the secret and the seed and im generating the third block ,so how many secrets I need depends on key size and how many parameter I generate , this is better than the previous one, you can directly go and until forever and you can generate enormous amount of processes, how are going to apply to TLS we are going to see ,this is the definition of the function and im going to represent like this ,the input to pseudo function is going to be secret and seed and seed is going to be appended to A3 and that is also input to secret and that is input to HMAC and that is appended ot A2 ,seed and secret and these are all block definition , lets go back what im saying is this A3,went to this secret and seed and the result appended to a2 to this one and im trying to explain this one, lets start from this one may be its going to make more sense I have this sees and secret and that is secret and seed and this is A1 and this is HMAC and that is going to go , seed and secret and A2 and that is going to go to secret and seed and A3 appended to seed to other hamc ,I m trying to explain the figure with the functions, A0 is the seed A1 is the hash secret HMAC hash secret A(i-1)., I will use this and I wil have three parameters one is secret the other one is seed and im going tp put the label and if im saying that it's a master secret then it's a master secret that's just a label and im going to do that pdf calculation using md5 and sha algorithm im going to split the secret into two , first part is the sha 1 algorithm and im going to do this table thing with the secret but but the hamc is using sha1 and im going to do the same thing with the second part of the secret but HMAC this time is SHA1, in other words HMAC is using sha1 so then the both results are going to be appended to create the key blocks so what im doing is im splitting it and naming it as it doesn't mater and im going t o do that alogorithm with md5 and sha1 and

im going to xor both of them to get the whole block so this way im increasing the randomness of the output one from sha1 and one from md5 ,you got one big block so number of block that im generating should be equal to number of block generated in sha1 md5 output is different and sha1 output is different ,system is doing it anyways ,by using this concept im going to change the finish message as they say in the TLS message ,again the master secret and the label is finish label this is could be finish client and finish all the handshake messages and al the handshake messages and the output and this time all the handshake messages this time its going to go to md5 so this way im modifying the finish message and it is different thn version 3 and for the cryptographic calculation this master secret is calculated by PRF, how am I going to calculate the label is master secret this type seed value ,you can ask what i s the seed value but in the definition of random number in the TLS again its going to be random number and its going to be client and server hello random , so those number are appended to form a seed so the seed is those random and premaster secret is the secret for those algorithm and those secret master they are going to calculate the master secret 48 bytes., there is going to be 2 sha1 in hmac it is pretty random .other difference between this tls version of SSL and the SSL is the key exchange in tls doesn't support fortezza ,tls support all the algorithm except fortezza and one more thing client certificate type there wer e ephemeral difeehelman what was that?..we are sighting the parameter ,when we are exchanging it but that one is not supported by tls instead tls has these type of certificate RSA signed DSS signed , RSA fixed dife helam and dss fixed difehelman and it will not have ephemeral as its not required for any other signing ,RSA and dss is enough for the signing of the differ Hellman these are the new types supported by TLS these are the major difference between tls and SSL so this is the end of SSL when I say this that means that the other chapters that we are going to cover we cover almost 60 or 70% of the network and other are going to be system security and it will have only definition we are not going to see this kind of protocol except set , just show you the one major technology we are using , now you guys know the IPSec, SSL , email security I know you guys are struggling with pgp that is the idea this is another protocol and you may not use this one in day today life .

SET (secure electronic transactions)

This is developed for ecommerce industry and this is developed for visa and mater cards in to words by the big guys and they developed this one and no one started implementing it and no one started using it except big guys, when they exchange ,money they might use it ,but this comes with a very good concept and technology it provides security and also formats it supports X509 version 3 ad privacy for restricted info for those who need it and this item major part for this set and this guy has decided this im buying something on internet and this guy on the other side is charging me for getting my money from my bank when I look at my bank statement in other words bank does see what you bought ,but why should bank people know my info ,they have to know only that payment info that is one problem the other Is when you give your credit card how are you going to know that those guys are not going to double credit your card because you disclose everything to those guys ,only 1 mechanism and that is trust mechanism as there is no other mechanism those guys if they are malicious they can end up buying anything and you will end up paying debt. ,im buying something from this guy is there any necessity for that guy to know my whole credit card info credit card info only important to bank only to know how

much it is charged , they are going to hide the information of the order that we are going to buy and they are hiding the info of your credit card from the merchant ,so the merchant will be knowing what you are buying but bank will know how much you have spent for it. ,im going to hide that kind of info and that info is going to get from the bank without knowing m y credit card , set is going t o solve the problem its going to hide your info to merchant and merchant info to bank so that way we are going to have pretty good security , these guys are doing it by Dual signature it is the process where order information is encrypted to bank payment info is going to be merchant it will be like certificate and no one can forge that link payment and order info that is the basic info we use .