Kerberos version 5 key exchange

As we saw the major things about version 5, the major difference between version 4 and version 5 is ,environmental and technical deficiency and one of the technical deficiencies is double encryption ,des encryption in version 4 and right now you can use any encryption and environmental usage ,life time in tickets and we have the authenticators to authenticate the ticket and in 5 and 6 message we are exchanging the session key that is going to be used to encrypt data after the access ,including sequence number ad session key, It cannot be, it may not, so there is no clear definition that you have to use the same algorithm over here there could be some other algorithm just for the confidentiality services ,there could be some changes in the Kerberos, tickets have different functionalities and were defined in flags and this flags were, response to options and what were those flags and what were different tickets used in version 5, let's have look at it.

Kerberos v.5 flags

The initial flag will be up in the ticket if the ticket is initial ticket , so if the ticket is issued using AS protocol and not based on TGT and pre authentication before issuing the ticket ,you may authenticate the ticket ,if that Is the case you are going to use pre authentication and hardware authentication and this is pre authentication could be different ,in other words authentication technique may not be password based , by using that you are going to authenticate it ,now you are going to authentication server asking ticket , hardware authentication will allow you to use hardware authentication technique like smart cards or one time passwords like buying it in 10$ or 15$ and you will get a new password and everytime you will be entering new password, and new password is your password and system will recognize that one as system is running the same password at the same time most of the time you are going to use one time password in the bank account and they are going to give you are password and they are going to set there login and everytime when you login your account ,the access password will be different ,this way Kerberos are password dependent so the security Is dependent on the password security only as password is not that secure , as it is first line defense and it is going to secure your password and to do that you need to have hardware authentication for example or pro authentication so by using this pro authentication or hardware authentication you can improve the security of the Kerberos , in other words Kerberos Is going to provide means to come up with better authentication ,renewable is tells tgs that this ticket can be used to obtain a replacement that expires at a later date, we discuss that one, we have a simulation too late and running for 2 days or 4 days and you have a simulation that works only for 2 days at that time you have to go back and get the ticket again for another two days and this not the way we are working and if you don't know the running time of the simulation we are going to get the ticket so the simulation day the ticket system will renew the ticket , like credit card, before the expiration you will get the new card , it is the same thing so hat you can get the renew able ticket how can i know that this is a renewable ticket , as there will be renewable flag at the top of the ticket, may postdate , you have a ticket and you are going to use it in may, that means you have ticket and you have to use it in a later date and if you use those stuffs, you a]may have may post date and post date and if the ticket is not invalid and at that time the ticket must be validated by kdc before use. and if the ticket is going to be validated in may but you start you are planning in april so this ticket is going to be invalid ticket that means that we have to go back to tgs and validate the ticket and if

tgs validates the ticket ,that ticket is going t be valid and this ticket is to be validated if it is done then its okk, if it is not then it is going to stay invalid ,it cannot use it , proxy able and proxy tells the tgs with the different network address ,may be issued based on presented ticket , in the ticket we have id_c and address of c this way we can identify that this ticket is coming from this workstation in other words this ticket is coming from this workstation only , if it comes from other im not going to accept it as the address of workstation will be different than the address of the ticket so if this is different im not going to be accepting it , im having the ticket with the different network address, remember this definition , in proxy server they are dummy proxy who don't have standard address, so they don't have implementation of telnet and If there authentication is successful they are going to forward you to telnet server and that's why they are called telnet servers and remember we are going to use the same thing here ,remember the example that I gave you that print server has to go to file server to get the files and print server as to go to file server and this time the ticket address in the network will be address, print server and that's why it is outing a different network address and print server is putting his access on behalf of mee, to access address .but the fileserver will get the ticket from the server if he doesn't change the address in the ticket, file server into accept that ticket and it is not coming from the ticket server ,proxy able ticket we are using user credentials in the place of tickets in other words we are transferring user credential to someother entity like print server and flag is going to be up and that flag is proxy flags and if the ticket is proxy able then the ticket will be up and if the ticket is forward able it is almost the same with the proxy able , one major difference is if you have forward able ticket then you can go to another Kerberos realm directly sot he Kerberos realm don't have to share any secrets anymore you can directly got o another realm to gain access and with the proxy you can go there as proxy is valid in your realm you can go to realm but you have to follow al the steps , in the forward able you can directly go to others realm. And the flags going to be forwarded flag in the ticket and that flag will be out and in other words forward able has more power than proxy able and forward able is going o be valid for inter realm communication and proxy able is not valid for that ,you cannot just directly go to other realm if you ticket is proxy and you need forward able if you have to go to other ticket , so every authentication ticket must save with another AS , but if we have forward able ticket we are actually eliminating this management problem that we are facing in Kerberos and if you have n domains show many keys related that you have to manage that is share between AS and it is approximately n^2 and it is a symmetric encryption algorithm and that's why it is approximately n square relation ship requires and if n is quiet large then we are going to have problems , remember physical layer encryption ,the physical layer encryption, how many hardware key you have to manage it wa n^2 keys and this forward able we are going to forward these tickets basically and it is going to help us a lot basically. That's my point this way version 5 is much more flexible than version 4 ,in other words version 5 will address the needs of todays security world more than version 4, so this is the end of Kerberos version 4 and 5 and there are some other details as that we dint mention ,like packet structure and format and if you are interested there are lot of books available for Kerberos

X509 authentication service

Now we are going to go another AS, which is x509AS,which is certificates , when we look at the email security we are going to look at it and when we look at digital security we will see this guys and

certificates are very important for todays world that is CCITT X500 directory service standards and what is directory service standards x500 , generally when we look at the address of other people in the network we are using a server and what is the name of the server?. .DNS , imagine that do you guys remember yellow books and imagine dns is something like that all the name hoe address location city country and it is going to be placed in the server and if you are looking for you friend in china you will be able to see home address, office address and phone number all those kind of thins and this is electronic yellow book and for example if you look at my email ertaul@yahoo.com , this is my yahoo address, and this defines what, this is a company and yahoo is the domain name and this is the account owner name and we have three major information and mainly whose this guy ,he is a professor and if he is a professor in which university ,cal state university and in which department like that , csueastbay.edu this shows that this guy is staff or faculty or student in this university so that I can understand that this is university and imagine I write like this, name levent ,organization CSUEASTBAY and org unit is math and comp science and country usa and defining this of email with this kind of attribute and this is called x400 , in email we have two protocols one is smtp and the other is x400, generally valid for unix and x400 is more compatible to x500 than smtp and x500 defines these attributes for smtp and imagine the database like this org ,org unit ,name country unit and number all those kind of information is going o be placed in x500 and it is kind of icon I n the shape of word, and it is going to go and connect to the local network and if you are going and asking somebody name or somebody ph number the return is going to be your request and this x500 is supposed to replace dns serve and everybody and every machine will be replaced in this x500 , it didn't happen and there was big expectation it did not happen if you look at the application ,you are not going to see this structure, you are going to see also this structure if you look at the details of the address you are going to see these things and these are x500 standards and in the certificates we are going to define the guys like this one of the major entries is certificates and why they put this entry because in Public key cryptograph we are going r have public key information of the user and here it will give a place to put the public key info of the users in the domain in this place or in this application {question from a student}. I don't know very much microsoft active directory ,mit is pretty complied with x500 if you look the structure of this and when you look at the definition of x500 they are thousand of attribute ready and I developed one of them 4 or 5 years ago and it was very popular , I was a project manager of project which was x500 project for nato countries this is for military application and the biggest trouble that we had , the definition of this attributes which attribute we have to define each and every different attribute for different country and with in the army it was really difficult to define these guys but anyway why im telling x509 is part of x500 because of this certificate entry so that you can place the certificate entry to x500 users so that every one all around the world if they want to find your public key they are going to find that public key from that entry , so that I the idea, defines the frame work for AS, directory may store public key certificates as I said, and with the publickey of the user and signed by the CA, this CA are big companies like verisign or Microsoft ,the main jobs of these companies are to create certificates , and also defines some authentication protocols , uses public key crypto and digital signatures algorithms not standardized and RSA is the main algorithm that we are using .

X509 certificates

First of all we are going to have 1 to 3 versions and todays world we are using versign 3, we are going to have serial number and signature algo identifier and we are going to have issuer x500 name ,which is different name than justice name and so they are going to use this kind of attributes to define the name ,period of validity and subject x500 name this is the owner name x500 format and subject algorithm ,RSA,diffehellman or elliptic curve and if it is RSA what kind of parameters required , its going tobe public key and modulus ,in other words parameters is going to be modulus and public key itself and we are going to issue version two and above and extension fields in version 3 and one of the major thing that we are going to see is digital signature and in digital signature are hashing all the fields and we are encrypting the fields by using key of CA, when I do that I show it something like this A is signed by CA so this is the signature part and remember we are creating certificates for what??. for authentication , but not exactly it was for distribution of the public keys and public keys require no secrecy, but distribution was easy as it was just distribution anyways but this time there was another problem how do I know that this key belongs to this user , then the CA will give us the keys but those public keys is going to be bind to the owner in a way the it is unforgable and that s why we are having these signature so no one replace these keys unless they have the private key information of the CA and if it is secret no one can generate the key and when it is secret we know that no one can generate the key ok.