Authentication header

It provides support for integrity and authentication of ip packets integrity will be there and authentication will be there end user system can authenticate user or application and systems and routers and each router can provide authentication prevents address spoofing attacks by tracking sequence numbers , based on use of mac, but we using this HMAC md5 96 bit of HMAC sha 1 96 bits, and packets must share secret keys why is that ?.. because of HMAC, HMAC is secret key related why it is 96 bits because we are going to have 3 32 bits result for HMAC, because the header , right here auth data and each lien is 32 bit and 3 32 bits =96 bits we need 96 bits authentication data how we are going to calculate that one we are going to calculate that one, the next header is going to show which header is going to be used next and payload length , -2 how many fields I have 6 32 bits , 4 payload if there is auth data over here , this is reserved, this is important SPI security parameter index , this is the address of related security associations, other wise you are not going to use SA, other wise this SPI is going to be carried b y protocol in the header when I receive this im going to check the spy and do the calculation reacted to the SA, whatever is defined ,if its transport mode then im going to define like that if its tunnel mode ,because message format is going to be different if the message format is different then It depends on which algorithm that you are using , it might be md5, sha 1, 96 which key you are going to use?.. not al possible combinations not what ever combination lets say you need AH in transport mode you are going create related SA and then the address of SA is this, the address is going to created by system, but you are going to create SA depends on your requirements , this SA is going to be in the database and when it goes tot the other side you are negotiating it ,it is totally other side ,when you establish the client they are going to establish this SA, it depends on your requirements what ever application you want to have the security requirements then you want to require these SA, you are going to go and request SA for particular application ,we are going to have address for the SA ,we are going to have sequence numbers and it is going to solve the sequence number of the packet we are using and ht Auth data 96 , how am i calculate the data let me tell you , ip header fields do not change or immutable , will be included in the calculation of HMAC and the AH other than authentication data field not this one but this field is going to be included if that is the case then im going to fill this part with 0.this part is going to be full of 0 then I will have AH info and entire upper level protocol what im saying is this , some portions of ipv6 immutable fields , AH but not the authentication data field will be filled with 0 and the rest of the data, so its going to go to HMAC sha1 or md5 what is the result of sha1 , output , 160 and im not going to be able to use 160 bits im going to take only 96 bits and im going to place it here and lets discuss some portions what are the fields you think it is mutable and immutable ,in ipv4 and ipv6 , the first thing is time to live and hop by hop in ipv6 is mutable time to live will change the time depending on the field, and also hop limit its going to be reduce by packers that are visited, source is not going to change congestion and flow control may change depending on the algorithm and fragmentation is it going to change or not in ipv4 and ipv6 and we are fragmenting data based on what?.based on size and that size is dictating from where , first of all its going to be if you are using internet it will have max size and you are going to fragment that one , important thing is what is the storage capacity of the routers, so that may change ., router to router so what they are going to do is your packet size to move the packet size to store in there routers before they are forwarding the data to the other side ,so this is not that important , routers are not same in data anymore ,on the buffer before

routing it , when the ip sees it the destination will be forwarded to the port so then the major requirements for the size is going to be network protocol ,if every router is using the same protocol then no fragmentation if some routers are saving the data they may re fragmentation it could be changing can I predict t he result , you can use that predicted value and you are going to use it, if not you are going to add 0 , to that field that means that field is going to change or changing during transmission but immutable will be there in the calculation so you are going to put it here and then authentication will carry this information so when the destination receive this one ipv6 will look at this source and destination header and its going to go to AH it recalculate this HMAC and its going to fill 0 to proper field and it compares and recalculates the mac calculation that called ICV integrity check value ,if this is same authentication is successful and no spoofing attacks ,because mac calculation includes the source and destination address info, so how am I going to use this sequence numbers

Anti replay service

First of all ip sec dictates that you are going to have a window and size of window is 64 and lets say that you are going to have sequence numbers with this packet and lets call it n and he minimum number is n-w and these are acknowledge without any problem and white ones are waiting to be acknowledged that means they haven't received the packet yet, but this marked ones are acknowledged one and there is no problem with this in other words im having this sequence number and it is valid sequence number and im going to authenticate and everything is ok im just marking that if that received packet is closed to right edge and if authentication is successful it is going to slide to the right if the packet received it in the other end then the other end is going to slide if the packet hasn't received the packet or if it has but hasn't reached the other end in other words may there is repeated sequence number ,if you receiving there same packet with another sequence number I already make that packet and im going to reject hat packet and those rejection are called audible sounds in other words its going to give , some of the packets are going to say its duplicate or authentication may not be successful ,so this way im avoiding replay attacks it is not possible it is possible if the size of the sequence number is 32 bits , when you reach the limit if you start form 0 again then you are having trouble , because in network layer there is limit for the sequence number and if you exceed the sequence number , or AH, you are going to go and establish new SA, you cannot continue sending your data because this overflow data flag iin SA is going to stop when that flag is up then it means we have reached the limits of the sequence numbers, as you see it is pretty easy tot avoid IPSec integrity the IPSec is going to be calculated with HMAC, sha 96or HMAC sha1 96 which one is going to be used is defined where?, how the destination knows the sender is using HMAC sha1 96 or HMAC sha1 SA, we will see that detail right now its going to say HMAC sha1,where is the key ,it is going to be there only in SA , so when you iuse transport and tunnel mode we are going to have some scenarios and those scenarios are IPSec can be used in end to end authentication like this station to station within the network local and or external end to end authentication or end to intermediate authentication with the file ,iit will be with in the file and not with this guy and the other guy so the router that is firewall will authenticate the packets and will forward the packets to local address this is the most widely sued scenario for authentication the user directly connected to firewall but this is also possible without firewall like personal vpns which are possible without firewalls ,but with IPSec vpns we are having problems and discuss when we see ssl

protocols but with my experience what I saw is this thing in military if they are in the field you don't have any firewall within the network they are moving os the army is moving and the network is moving suddenly you are providing the network so you are providing the move along with the army these are really complex things but you are handling it using the security protocols so are you clear with this which scenario is going to be used in transport and tunnel mode , lets start with end to end authentication transport AH for this one ,as you don't have to hide the original Ip header ,this guy most probably you are going to go external mode so its tunnel mode ,what about this definitely tunnel mode, when you use external thing like internet the basic thing is tunnel mode between firewall router and device generally transport is enough because behind the firewall the network is secured so I don't need extra stuff, but when I go to external networks like internet then im having problem over there I have no control nor I have security so tunnel mode will provide security for me I need full authentication of my original ip header, you may think other way also but im not go into that, but you may take a risk if you think security is not a big deal for you guys then you can go and use it it's the choices you are going to make is depending one the security depending of the data, you can go and select either mode.