Bastion host

As I said the bastion host is the highly secured host system lets look at the firewall configuration

Firewall configuration

One is called screen hose firewall system ,this is internet connection and my system is connected by packet filtering router and with that im going to check the incoming ip address and it will go to bastion address and it will do the stuff whatever we need and its going to all to the traffic to go to private host and there is info server and connection will go to info server which are other wise web servers , ok this is called single round bastion stating what is wrong with this, the thing is that if something has spend over here and it is highly secure and this is not protecting too much the network any security compromise will open the whole network you don't have to go to through bastion host and you can directly go to this guy and you can physically separate this guy to this bastion connection and we say that bastion host may have more than 1 network connection and right here there is not physical connection and I separated the whole network and security compromise over here is not going to cause problem over here, as whoever compromises packet filtering router must go to bastion host and we said that its a highly secure environment and this the actual firewall, but look at the info server, It is still, not behind ,with the base station host but its inside the host so any security compromise ,whoever wants to attack may gain access to this server while im going to call it web server and it must be open to public and you have to check whether someone is changing you r contents or denial or service or something like that , you must control those stuffs that why bation host is going to come up another security network and any security compromise with that networks will not jeopardize the other network as there is not physical connection between the two networks its called DMZ zone of the firewall most of the public things will go there, and so you are not going to keep in the hostile environments or talkt to the open but you will keep in control and its called DMZ zone, so this way we have different physical connection and whose going to connect those physical connection that Is the bastion host its going to check the connection and based on that one its going to allow the incoming packet to server so this is called dual home bastion host ,most of the time network will be protecting that configuration but if you need more configuration then im going to come up with another one that is this one I have 2 router one is inside and the other is outside I don't have physical security connection or bastion host so if there is any security problem this is going to protect me so the private network is not totally open to internet and I will have some protection and sometimes in big companies they may want to access there comp from outside for that these guys must by pass the firewall ,but if you allow them to by pass easily the someone may use that facility to use system so that's why inside router is very important as this is going to control this dial in type of things along with the network its going to go with two level o f security bastion host and inside router and this is going to provide a dial in type of service , I don't see anyone now use modem to gain access or to login to other accounts what kind of technology we are using , so whoever comes , will go and by pass the network and bastion host will by pass the network with the vpn and its going to d other stuff with the vpn, remember the vpn model the destination address will be the address of the bastion host when the bastion host decrypts this going to sees the host in one of the private networks and its going to send it there, now as I said every major company is using dial in not

wireless, so vpn is used using ssl protocol remember ,it deals with security association and that's why all around internet we can have vpn access so these are firewalls,

Access control

We know that there are two type ,dictionary and mandatory , as you guys know about the discretionary which is read write , ,executable kind of things, important thing is mandatory and we are going to see the bell lapadula model lets have a look we have the subject and we the object and the relationship between subject and objects access file and this has read access write for this particular object an that kind of stuff and wear going to have access control and we will be having access control to all the segments where segment a can read and write so and so forth this is going to b e access list and this is the most commonly used access control in today's technology , but this is going to case some problem which will be Trojan horse and I will explaining how to control , so we are going to have many comp system and it will be evaluated and it will be having c1c2c3 kind of this and its called transport system and we will be having subject object kind of levels, for example subject will have max security level and object will have object s that have security level and you may say this is public and the other is sensitive depends on application and important thing is we are going to have security levels and we are going to define it for subject and objects, and one method is this bell lapadulla , it has two rules no read up a subject can only read an object if the current security level of the subject dominates the classification of the object I m the subject and I have the secret level clearance the data is top secret I cannot read, but the data is ordinary secret , I can read , no read up, and no write down. Its called start problem a subject can only be append or write to an object if current security level of the subject is dominated by the classification of object. In other words im top secret but the object is secret I want to write something can I ,no I cant it should be less than my security ,you cannot write those , so why we need those kind of stuffs, generally this is used in military im going to show you that one , that is Trojan horse attacks we are going to avoid that one by using the blp attack ,that is the core reason for something new and that is called reference model in that we will have subject and object data base where will replace this access control list with this data base and there will be subject security clearance and object specific clearance over here and if the subject wants to aces the object this subject will check the policy ,no read up or write down based on the this clearance this classification and there its going to allow the subject to allow the object so it is different than the actual thing that we are using and then there is going to be audit file which will say this subject at this particular time access this object and something like that so this is a secure access control and its better than read write access control this is the secure part of that one how we are going to use this one, lets say that Alice wants to gain access to whole system ,an outsider came to my comp and plug-in my comp and it became a part of the computer and in the past it was easy now we have to register ourselves in the network the reason was the lot of people were coming and they were accessing our network to attack other networks so to avoid that kind of stuff we had simple admin stream ,but lets say that you will find a laptop unattended and you will go and sit there bob is a legitimate student and her created a file and its read write on that file and he is the owner of the file and Alice is a intruder it gives Alice access to both read and write and bob write rights,and this is a program and lets say that this a comp and Alice say s this Is a very nice comp game why not we paly it , so bob starts playing it ,when bob starts playing then bob becomes the owner of the

game and he gets the write access to this file and lets say that in that file there is a password and program will read the password and writ that password in the back of the file and this way as you se e Alice will be able to get the password and important string of the file to her own file, so this is the with the access control on your workstation now lets have a look at reference monitor, first of all im going to have two sensitivity level over here sensitive and public ,bob is sensitive and alcie is public and she creates the same thing and bob starts playing the game this is public and alcie is program will be able to add the bob file because of no read up condition because when bob reads the Alice program it becomes the owner so the bob has the right to aces to this sensitivity level and bob can read this one the level is the same ,but the program will read this and write it down to the back pocket file ,but the back pocket file is public and no write down and the application monitor will not allow it to write down this string to the back pocket file so this way as you see reference monitor avoids Trojan horse attacks and that s why it is important in military and financial application because security levels are so high hand with reference monitor and it is vulnerable attacks , so this way we going to have pretty secure access control mechanism