Slide 42

Ok lets have a look at this excess policies. Information model will be different that security model, there are differences in the model, data and software kind of stuffs. This is connected the outside of the access channel ,that is your communication link basically. Everyone from the internet like human, intruder, software are trying to access this information system. That thing will control internal resources from outside. What is the gate keeper function, in today's world we are using firewall. Firewall will protect this internal information system from outside by regulating the access. That is the important thing, by controlling the access. This is the model we use in today's world for the access policies, and every network that we use so far, definitely they have firewall services, firewalls not so used ,but if you connect to the router to your firewall, router comes with firewall nowadays. Jus configure the router basically and you can configure the firewall basically. So this is very widely used access policies.

Slide 43

This model requires us to select appropriate gatekeeper functions to identify users ,it is the firewall functionality basically. And implement security controls to ensure only authorized users access designated information or resources .And trusted computer system can be used to implement this model. Ok this is one extra stuff. What is trusted computer system??.. not really, when we say trusted computer system in real word, it doesn't mean anything different ,it doesn't have a trousure, that is not a identity of a trusted computer .C1, C2, like that different levels, if your computer is configured in the different levels. If your computer is in C3 level, then you cannot install anything, not any software anything at all. Lets say you have installed Microsoft outlook, outlook is the only thing lets say that you have installed ,if the server is web server then only contents related to web server will be there. And to install things you have to go to the system and you cannot just go and install the things. You have to rebuild the system with C3 ,but with C2, you can still see some other things ,with C1 you can do anything you want. There are some organization that evaluate your system, which gives approve that this is a trusted system and they have a (…..)…they have a (…..) based on those (…..) definitions they define whether this is a trusted system or not, with this kind of trusted system , like an operating system, does it support support C3 system, OS like XP?.. I don't know but if it does, you will have huge specification of how to configure XP at the C3 level. These are different manuals basically, you are not going to switch something and that doesn't will become C3 level system. If it is C3 or if it does support C3, and there are some guys, it takes years and years but still operating system comes up with that system basically. So these are the transfer system, just know that there are C1, C2, C3 level of security system basically.

Slide 44

What about data access??. And we going to have two types of data access basically, one is called discretionary access control (DAC), and the other is called mandatory access control (MAC). You guys are familiar with the DAC, you are having read write and executable rights. Remember change rights 77766 something like that ,so that you can give rights to all the systems basically.

Slide 45

There is alice, there is bob and these is file ,there will be a payroll file, in this payroll file, alice and bob ,where alice has read and write right, but bob has only read rights. That means alice can only read the file and can write the files. But bob can only read the file, but cannot write the file. Sam cannot read nor write to the file, the data access control list, who creates this data control list, the administrators of the file, generally create the permission of the file basically. This is called discretionary access control, there is one drawback actually, that is (tro….) attacks. You cannot attack or detect the attack by these discretionary access control basically.

Slide 46

In our day to day world ,they came up with the new model and I call this model as the mandatory access control model. These model had the lot (…….) I cannot pronounce that name. that is actually this stuff. Reference monitor remember it, the reference monitor will be the major thing ,what we are going to do in this kind of situation is alice and bob are working in secret place. You need security clearances if you are working in a secret place. Those things can be secret ,top secret ,or (……..) secret. And lot stuffs basically, the secret is the number one. What they are doing is they are looking at your background, your school, your information of the past ,whether you are not involved in any political activities or you dint get any political conviction or something like that. And generally they do give these kind of secret clearances and who gives those kind of secret clearances or security clearances. Whoever is your employee they do give security clearances. In US they do apply for FBI or some secret agencies, depending on which level of security clearance they need. They will work one or two months, once that is done then you can work ,but if you don't have that clearance then you cannot work with that secret projects . top secret clearance ,you need to clear top secret information. So here alice has secret clearance and bob has top secret clearance. Alice has less level of clearance than bob. Basically these kind of things are used in military, most of the general will be having these kinds of top secret things. Or somebody like lieutenant, or some higher level personals will be having top secret clearance { question from a student}..thats the point we are going to discuss. So we have secret and top secret level of information. Also we have sensitive level of data, which can be secret or it could be top secret. Data itself it could be secret or top secret. We will also will be having branches like this, alfa, venus alfa data. So venus alfa, so by this way the logistic file will be having secret sensitivity level. To that level if alice has secret level and bob has super secret level and if the sub secret level alfa and alfa, then rule says alice can write the file but cannot read the file, if the security level, security clearance is equal to or less than the sensitivity level of the logistic file. You cannot see the whole content of the file ,but you can only add somethings to the file. Imagine this scenario, we are in the war, and general have to see only the whole thing and not only the front lines. So they will be inputting data from the front line and the data will be like all the generals can see. That's why the data will be same low level, can only add something in other words ,write somethings to file. If your secret level is greater than the sensitivity of your data. You can see the whole contents. But the general doesn't have to clear all the data coming from the front line, but it has to see the entire thing, tactics, strategies so and so forth basically. If the clearance level is greater than sensitivity level of the file, then you cannot write the file, but you can read the file, if It is less than or equal to the sensitivity level,at this time ,you cannot read the file ,but you can write the file. And that's called mandatory access control ,and with this mandatory access

control you can actually avoid (tro..) attacks. And the actual access control model we call it reference model. With those kind of things you are avoiding (tro…) attacks and you are developing mandatory access control basically. Are you clear??.