Rule based intrusion detection

What we doing is they are going to observer the system and apply rules if the activity is suspicious or not , so the are going to apply the rules one methods Is rule based anomaly system, they are going to analyze historical audit records to indentify usage patterns and auto generate rules of them , for exam pl the rule for the the email application and my analogy is 8 if you exceed 8 ,in 4hrs then im going to assume that it is a intrusion and this rules is generated not because for past audit , but they may also see what type of things is doing so it may require some time to check with this , most of intrusion detection are like this in the industry its rules and the other one is observe current behavior and match against rules and see it conforms like statistical anomaly detection does not have prior knowledge of security flaws. nothing is based on known security flaws up to this point 20 or 50 yrs in computer lot of security attacks happened and we have good data base on all those attacks we have a institute called SERT , these guy have the binge database every time security attacks happened they inform it to set and in other word we have very good knowledge of security attack to find the intruders. Most probably some of the intruders have this old technique its going t o be very easy for me to detect it , in rule based penetration identification what we are doing is we are using expert system and this is expert on known penetration ,they are going to look on known pattern ,suspicious behavior and based on that on they are going to develop rule and intrusion system, rules usually machine and OS specific why is that because attacks are going to be machine and OS specific the security attacks you are getting I n windows is different than what you are getting in mac, only a fewer attacks like mac , but lot of them will be for windows ,if you have intrusion detection system for mac the rules that you are going to apply is different than windows, and we are going to use expert system technology , do you have any idea on expert system ?.. it is something like this I saw that one in Oregon it's a security company and they develop a product for OS security , you have no knowledge if you dint take this course or curious about this course but you guys are educated you can learn yourself but vast majority of people they are talking like authentication must be important ,use hash function they will say what is this they are going to configure OS ,one thing is they have to get educated about this system and what they are doing is this company they developed a expert system which specialized on xp ,its guiding the user by asking equation ,like do you need password to access a file ,if the user says yes then it will selects the password and encrypts the file sort the file ,and encryption option this is and it checks all the weaknesses about the xp as it knows more about the xp than user so it will ask there is this danger and this danger what you are going to do, so any guiding the user like this eventually that system is going to configuration ,and it is different thing for different application and that application specifically knows the xp and it guides the user for configuration so most of the intrusion that is in the rule based or rule based penetration system one is in silicon valley that is called arch site ,there main job is to develop intrusion detection system they are selling intrusion detection system ,but I know that they dong statistical anomaly and user pattern but what they do is they are having this and checking the ports and everything and if they say some silly request comes from there they say this is intrusion detection kind of stuff .its limited and not an easy job,

Base rate fallacy

Practically intrusion detection should detect substantial percentage of intrusion with few false alarms I do expect little false alarms if too intrusion detected this is not good false security if too m any false alarms its not good either you will ignore or waste of time because of user behavior and intruder behavior , we will be having lot of problem we are trying to keep it small as possible that part is not easy but this is hard and existing system seem not to have good base rate fallacy because they don't implement intrusion detection based on this ,the intrusion detection developing is quite limited, one of the application of intrusion detection we are going to detect intrusion detection and we are going to block then the second part was. ?..detecting intrusion block it to improve the security and what was the second one, act as deterrent that means that you are using intrusion detection then I will be like change on a minute this is a dangerous area im going to get caught or something, you may say those kind of stuffs ,collect info to improve security if I have better knowledge about the behavior of the intruder this base rate fallacy will be improved but how will I improve my knowledge ,and these guys are special guys and they are having own festivals and I have been to one in Europe, where everyone comes with there own laptop and they teach each other how to hack the other system and they are having in lasvegas also, its black hat conference couple f years ago ,my students went there where they teach each other and one of my student explained in conference room wireless system and one guy used his computer as router and travelling within t he room and all the other trying to hack each other and they are explain and learning the technique and these are very well known conference, and when you see them you will see them you will know how different they are ,so knowing there behavior it will help to develop better intrusion detection system that is the reason why there is another new subject and that new subject is called honey pods, these are steps ,detection deterrent and learn the intrusion but we are leaving in a distributed environment so how are you going to live distributed environment from intrusion thats the another question before local networker is easy for distributed environment so we will have agent based models like mobile agents or fixed agents ,agents are intelligent software and you install that software to get every other info like network management operation some of them could be mobile , for example you will go one the internet and see a 56 chevy blue car 100000 mile on it you are going to pay $10000 for it ,but are you going to check every chevy dealer for that ,you are going to put the mobile agent on the system and you a re going to give detail and that mobile agent will look all around internet to check for your specific car. And its going to find something and its going to negotiate price and this going to show that dealer has said $11000 and not $10000 and its going to share , im here and im the agent and you are either going to buy a car or authorize the agent to buy the car, these are mobile agent technology and you are using not mobile but fixed agent technology for distributed intrusion detection in every lan and WAN and everyone will have agent model its going to look at all the codes and based on that intrusion detection you have its going to detect intrusion on the host if it is detected then its going to inform the central manager. And then central manager will act on intrusion it depends on how intelligent that agent is , and there is actually implementation of this one , we have in UC davis, they are very famous in intrusion detection, they are the one who came actually, and they implement d this one and they used in on campus and the have distributed and they a have the info they filter out that one they create there own data and the rules and then agent protocol machine and they are going to use this kind of info to detect the intrusion ,if they want to change the logic to rules , thye can cahgne thelogicto thesystme this way they provide distributed intrusion system it Is agent basaed, as I said for the third level its honey pod

Honey pod,

Here we are going to look at the behavior of the intruder these are the decoy system to lure attacks, I have a network and I know it is quite popular for attackers an d its very important to protect from these attackers im going to prepare a dummy network from lot of silly info form it that info that is into private or that is not required for me when you look at outside ,this look s like actual network, and im going to put weaknesses over here and and intruder going to provide the weaknesses and attack them back in other were im inviting them to attack m y network ,I will not worry because everything that I got over here is dummy but what I got over here is some monitoring device which monitor behavior intruders and I will keep some alarms so that they can monitor and one hour later they are going to catch up the guy but most important this is to learnt the behavior of this guy and to improve the security of the network it is actually difficult as actual network , you have to spend money for that, some big companies are using this honey pod technology , and the other thing is I draw some kind of network and this could also be this kind of network outside of your actual network , security is going to be low and monitoring will be high ,if I detect anything of here im not going to let this guy into the system im going to raise the alarms and everything this system is much secure than that one and im going to cal them honey its another important new technology this way we completed intrusion detection system and you know it right now . you k now honey pod. , another thing we said was the intruders first approach the system to hack the system is to find the password either to guess or capture the password ,to avoid those password attacks what kind of stuff I can do to manage the password that's going to be very important this is first lien of defense if you don't have proper password then you will be in problem

Password management

Most of the time you are using login name and password to gain access password are not stored in clear in OS, generally they stored encrypted so any password file stored in os will to disclose the password still we have proper access control for that passwords for example in unix ,what they are doing is crypt 3 algorithm it is similar to des and they are using this to limit it to 2 keys one key is 8 character password and the other is salt it is the date and time info for the creation of password, and the input to the crypto 3 is 64 n bit 0, so that 64 bit 0 is going to encrypted with salt and password and that's going to be the cipher text and im going to do another encryption with same salt and password and im going to do 25 encryption and the result Is going to be stored here encryption with the password and then input is salt and 64 bit 0 , this is the login name and salt value and 25 times encrypted 0 with the password is going to be right there and if you login and it wll go and find the user id and salt while you enter your password and immediately goers to salt and 64 bit 0 and 25 encryptions its going to get a resultant hast result must be equal to this result if the comparison fails they will say this is not correct password or user id and if its some you reload to access the system , these guys are not keeping in clear form , they are going to hash or encrypt it, we have extra protection, even the administrator cannot see your password , and this excess is also tough so its not easy for intruder to get access and try 25 encryption for guest password and software, its not going to be easy ,as I said user id will help in selecting a password and by using this salt and the password you enter this one and im going to encrypt 64 bit 25 times and you are going to enter compare with the stored result and if its same you are allowed to login to the system , salt is like IV, what I know is crypto tree is a des algorithm and it allows this one

kind of key and its not a input to the des its going to go with the password and if you call it iv then they are using counter mode or something like that ,I don’t know which mode, the algorithm is crypto tree and its des based , so in other words OS will have this kind of mechanism to store the password on the system but this is not related to manage system ,this is not related to managing password.