Managing passwords

Is the one of the most important thing for the user side because life is getting complex everyday and everything based in ip technology and we are going t o calculate for you level how many password you are going to remember I will give you my example , I have my yahoo account, I have Gmail I have email ,and one another email university ,this is the email side and I have two bank accounts and I have pin number from card and I have 7 cards I have and I have web access to each card so not 7 but 4 of them same bank and its going to be 4 or 3 bank info and for this bank I have 3 passwords and web app cards and I have travelocity , expedia and hotel.com , one or the other time you have to create account with these guys and you are going to use it, and then book companies, as a professor this very important, macronial edision Wesley I have crc and presentation, and I have my personal things , I have account with American scientist it's a magazine and teaching.com and my insurance companies , just see the list, and this is the just the line, for each one of them I have to use different log in and password name, so how many password, 29 passwords , more than that , and I have to keep track of , im not going to remember all those , as most probably will for get password of Travelocity I do daily check the bank account , but for these guys I do forget , n to forget I have to write it down and if you look at your personal at your level you have to know at least 20 different passwords, and how are you to manage those stuffs, you are selecting one big master password and using it everywhere you don't even know how secure these guys are how they are storing there password and may be bank is ok way ,you will get your money back but for your book companies and all you don't know you are just disclosing your important password which is not good, this is becoming big deal for everyone its not easy as a security professor you have to use different password for everything ,for selecting its not going to be easy to remember if you remember easily then this readable then its going to write it down and its another security problem what they are doing and you have to pay $10 or something and they are giving you only one password this called single sign on by using only one password for that company ,that company arranges access to other companies means you entering password once for the bank and everything and they have the list and if you want to go to the bank then you entering only that companies password you don't have to enter any other password ,you see these type of companies .,even for telephones don't forget the pin number for phones as pin numbers are also kind of passwords ,they are storing password in a way that they cannot read it ,if there is a need they are going to disclose it over there the automatic way the machine are seeing it, in yahoo and gmail the email things are not very important, they are not in your machine and it will be on the third parties machine but may it not in the clear form ,the company doesn't know the password and they have to transfer to the bank when they are transferring it the password must be in clear form, but I know that there is that kind of company ,banks and stuffs basically I think , this is becoming very important thing and you are paying and they are managing these things for you identity protection , how are you going to solve these things you have to select a proper password , that means goo d password ,user education , you will select a good password , or again you are tech guy and you will buy on time password and it's a device like a credit card kind of thing, to use that one the other side must provide , they are going to send the password and set the password and then this guy is based on time every time you turn on the card so whatever you see you will enter into bank account , bank account same machine create same password , but you can have that kind of stuff for your local work station not for bank station for those bank must provide technology ,

user education and proactive password selection and we have some techniques. Are called markov chain and bloom filters with these two you can create very good password in the past we had compute generated password ,and it was setting such a strong password that it wasn't easy to remember and people tend not to use those password and it became reactive checking password, you are selecting the password and computer is telling 6 character ,number or unreadable characters and something like that , you are entering a password and computer is checking how strong it is if it is strong then its going to comeback saying this password is not allowed, these are the major technologies and I know in some companies they are running password crackers, the manager is running password cracker for the employees when they discovered the password they have told them to change he password its not a strong password and some companies have that kind of policy or some companies enforce periodic changing of passwords so your password will expire in 3 months , if you enter the same password system will not a low as it will have it in this history of password, and it will say its in system and you cannot use ti some of them will keep the history and some of them will make sure that they have good password depending on security requirements so then we have to find some kind fo balance to select ,most reactively run guessing tools user can select own password and system will verify , verification is going to be done and it will cause dictionary attacks in other words it cannot find anything from dictionary then it will say that its not able to find it , so password should have some silly things then its going to be strong gif you don't find hat kind of method then we are going to sue markov method im going to show this in three letters abc, its could be 27 or multidimensional

Markov model

If the first letter is a and the probability of second letter to be a is 0 this is a random definition but after a the probability is 50% of the second letter is b if im in the b again 40% the third letter could be b or 20% it could be c or40% its could be a or 0% it could be c or b or if you are in the state c then Its going to be a and lets say that w e are going to start from one state you guys tell me which state you want to start, lets start from c , and if it is c the most probably the next letter is a and im in a now and what is the biggest possibility it could be b or c lets say c as its 50% now i m creating another sequence and i can go to a now if im in b I could go to b or c, or a, lets have look at highest possibility so if im in b then it could be b , c or a, so you are going to generate ,lets say im looking for 4 later password and im going or see all the sequence that can be generated from this model , and I m going to use my password out of , im not going to use nay sequence form password, what that is generated will not be used as password and whatever you cannot generate from this model will be used as password and this is very good password generations scheme but t here it is very limited we have only three letters put 27 letters and this is one single dimensional for example this is b and you can go to d and it could be multiple dimensional including character including character and number and huge number and if you are having a good. Computer programming skill its going to be very easy for you generate a good password , just model the computer like this and generate the password based on the rule , but don't forget we are going to generate password not from the secret that we generated it will from a sequence which cannot be generated and its called markov model , so this is very neat stuff, one another called bloom filetr

Bloom filter

What im going to do with bloom filter is im going to have a huge table what is the output of sha1 ,160 bits, im going to have a table with the entries 2 to 160 , something like this, im selecting a password lets say m y password Is k ,but I don't how secure this k is , and I have bunch of hash algorithm and I have md5 , ripem , hamc, so I have all the hash algorithm and md2 ,md4, im calculate the hash of the k with sha1, lets say my sha is 4, im going to go to the 4th cell and im going to look at the content of the cell, if its 0 then the k is quite secure to select as the password as there is no hash output for the k to select as the password then im going to make it 1, if some other people select k then the hash of the k is anyway 4 so they will say this k is not secure , because the corresponding shell algorithm is having k and im going to calculate k for all the hash algorithm and im going to put the ones to different places if I hit 0 all the time then this k is quite strong password to be used, if we use more hash algorithm we are going to select better stronger password, if you use only one algorithm it will be strong but not as strong as all the hash algorithm , so this is really nice way to select a password and it can be used along with the markov model and this is going to be best of creating a password ,if you have any problems in password then in internet you will get hash algorithm and put those stuffs just check the hash and all you have to do is you have to create a big table and this way you can create a strong password.