Passwords: Past, Present and Future

Abstract:

Passwords have been used for a long time now. According to an article in wired.com the first computer password came in the early 1960s. Later in the century other methods of breaking passwords were invented. The most widely used words or numbers and combinations of them were all added into what is called a “dictionary.” Password salts were invented later as a counter measure to dictionary attacks. As a result of password salts, brute force attacks were created. This led to passwords that are used today which are more complex. The reason for this complexity stems from the increasing propensity of security risks. The computer when stripped to its bare essentials is a device that connects people and information. The advantage associated with this machine is that information is now freely available and easily accessible. People from all over the world can access a computer and instantly be acquainted with knowledge and information. The downside is that the “goodness” and “prosperity” the computer can provide can be manipulated by the selfishness and evil of people. Security is thus an essential part of a computer system. Passwords were developed to help ensure this security. Passwords allow for many things to be kept safe and accessible to the computer user. Passwords have been increasing in complexity because people have been increasing their intrusive nature. Biometrics, Graphical Patterns, Passwords (normal) and Numerical Passwords are the “passwords” that are most used today. Password managers are used by several different Internet providers, which allow protection for users who set reminders for their passwords to be included by their providers. They entrust their providers with the utmost care concerning their personal and financial relations on the Internet.

Passwords in general have been used for a very long time now. Spartans and Romans have used them to assure safety around their camps and to ensure integrity of the incoming communications. However, in the modern times, when someone is trying a wrong password the perpetrator would probably not end up getting beheaded, but the penalties become much less life threatening to try and break passwords. According to an article in wired.com the first computer password came in the early 1960s. MIT built a massive computer called CTSS and allowed only a certain amount of time on it for those who were authorized to use it. It became an issue since some of them needed more time than they were allowed. Allan Scherr, a Ph.D. researcher at MIT in the early 1960's, admitted to what probably is the earliest case of password theft in computer history. He went and printed the password file, which included all the passwords stored on the system, and he used those passwords to get more time, as he needed it.

Later in the century other methods of cracking passwords were invented. After some thorough analysis it was found that most passwords picked up by users were predictable. The most widely used words or numbers and combinations of them were all add into what is called a “dictionary". A computer would run though the dictionaries and try all of the words until it found the right one. Password salts were invented later as a counter measure to dictionary attacks. Password salts are small random numbers generated by some programs. Salts would be added to the user’s password thus making dictionary attacks useless.

Brute force attacks became more effective after the introduction of salts. Brute force attacks are basically programs that would go through every possible combination until it succeeds in finding the right password. A counter measures to this was limiting the number of false passwords the user can try before he is introduced with another challenge. Visual recognition of some scrambled letters or numbers did a good job in that regard for a while. However it is not very difficult now a day to write some algorithms to identify these as well.

Biometrics is a type of password that deals with specific personal identification. These passwords are not made up but are basic parts of human uniqueness. Such programs as Fingerprint, Voice, and Facial Recognition are all examples of Biometric type passwords. These passwords are almost foolproof but not completely as they very hard to recreate and hack. Because nature (the most complex of all technologies) has engineered people with identifying characteristics that are unique to them and nobody else, these passwords are highly secure.

Graphical Patterns are a type of password that is usually seen on (but not always) touch screen systems. An iPhone for example is a system that uses a touch screen-graphical pattern as a password. Other cellphones services and providers have used similar types of passwords. Handheld computers and other forms of “tablet” technology also carry similar securities. The reason that graphical patterns are used is that like, Biometric passwords are unique to these individuals. Although one can say that most passwords are “unique,” to individuals, Graphical Patterns are especially unique because they're drawn by individuals using a set graphical pattern that are already in place. The weakness of such a password is that there is a “set” graphical pattern already in place. Although most of the population is not capable of cracking such a complex graphs. There are individuals (especially computer hackers and identity thieves) who are capable of solving complex codes and graphs created by such software providers.

Most normal Passwords are self-explanatory. We have at one time in our daily lives encountered this form of password. They are not highly complex and are used by many individuals around the world. Mostly these passwords are formulated on (or) by personal individual interest. The password could be as a simple as the users name, or what their favorite clothing brand, sports team, family member, pet etc. For the most part these passwords serve the purpose they were designed to for yet they are often simplistic and are extremely vulnerable to outside influence. Since many people (whether we know this or choose to accept this) have many of the same interests, family member names, names, and other characteristics. So it becomes quite easy for an intelligent individual to figure out these distinct (yet connective) attributes of password usage.

Numerical Passwords are again, like normal passwords, self-explanatory, and are also connected. Many technological services providers today have combined both these forms of passwords to help create a more distinct and secure password but even these passwords limitations. For some users a numerical password requirement is a blessing, but to others it is a confusing hassle. Some people have better memories associated with numbers while others are more concrete. This would mean that numbering as a universal system and a universal code for computing, a hacker could easily determine a passwords identity because of his/her familiarity with numbers in general.

After identifying several types of passwords, we have found significant variances in how passwords are distributed and made. Because of this we have improved the state of password usage and creation. However we as a society must be aware of an opposing force that is relentlessly in the search of maneuvering around these new techniques. The problems do not just stem from security But many other service providers have become engrossed in attacking and defeating this opposing force, and have lost sight of providing an adequate, timely "service" to their customers. I can say from my own experience that doing something as "simple" as forgetting your password can be a costly unnerving process to retrieve and reset. Especially when all you are looking for a simple solution to the problem something that service providers have pledged to provide. I have had a bad experience that has specific

requirements for passwords and how a user must use them. They also have specific requirements on how a user can gather their forgotten password. Because their requirements are so complex and unique they have bogged down the very thing they are suppose to do: adequate, timely, customer service. It is because of this the requirements of creating a password are not only frustrating they are almost unmemorable. Don't let me get started on how to acquire a forgotten password through this company; it might require you to pull out of your debit card or your eyeballs! Anyway, the point is that the dangers of password managing and creating have created a unique crisis amongst users and service providers. It has essentially (and ironically) created an identity crisis amongst users wishing to create a secure and easily accessible identity, while conversely disabling the competent service identity these providers have claimed.

There have been several papers published about different ways to help protect against the hacking of or password breaking. One paper in particular is a paper on Honey words (Ari Juels, 2013). The paper explains how honey words function. Basically there are 2 words one word is the right password and the other is incorrect and alerts the user that someone is trying to gain access to their account. This is great for people who have web-based email such as Gmail, Yahoo mail, and so on. Everyone at some point in time has had an issue when someone gets into your email and starts sending out random emails to all of their contacts on their email list.

The only problem is passwords aren't just used on the computers we use them when we make transaction at the checkout lane at grocery also known as our Personal Identification Number or PIN. This is also a password though it's at lower level of complexity it plays or has a major impact on our daily lives. PIN's are considered to be numerical passwords and even they can be stolen when you least expect it.

The question is how can we improve passwords of all types in the future? That really depends on what will be fastest and most secure at the same time. Currently passwords are the fastest and easiest to use because they don’t require a lot of bandwidth and they aren't overly complicated everyone can use them. But for the near future, we need to come up with ways to better protect our passwords from the opposing forces. There are several ways as a society we can improve the strength of passwords. One way is using the Honey words, since they wouldn’t require many changes to be made in order to implement them. Another way we could definitely help password protection is by having a multiple layers. We could accomplish this by several different methods. First, is have a double password setup so that when you enter one password correctly another password would popup requiring you to enter another password for the same website. This is a bit more time consuming but only by a few seconds. The second way we could implement a multi layer password is by linking websites. For example if you want to log in to your Gmail and you enter the Gmail password successfully Gmail would then redirect you to your Facebook where you would then enter your

Facebook password. Then it would redirect you back into your Gmail. This approach doesn’t necessarily have to redirect you to the Facebook website but just have another password box on the same web page labeled Facebook password. That way when you go to sign it would verify the password with Facebook and would allow you access. Something else everyone needs to think about is should everyone be required to change their password every six months or should there be a password policy for the everyday recreation user or just companies that have password policies.

The elements that will ultimately determine the fate of passwords are what we as a society do and time. If bandwidth becomes faster and Point Of Sale computers can use that bandwidth. Then who knows maybe our finger prints will be used at the point of sale computers. In the far future it might be possible to tie our bank accounts to our DNA this would be an issue if you had an identical twin though only time will tell that story.

Bibliography

Ari Juels, R. L. (2013 йил 2-May). Honeywords: Making Password-Cracking Detectable. Cambridge, MA.

Joseph Bonneau, C. H. (2012 йил 20-May). The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes.

Kippelman, S. (2013, September 30). *Passwords stink. Is there a replacement?* Retrieved November 24, 2013, from ComputerWorld: http://blogs.computerworld.com/cybercrime-and-hacking/22884/passwords-stink-there-replacement

McMillian, R. (2012, January 27). *The World's First Computer Password? It Was Useless Too*. Retrieved November 24, 2013, from Wired: http://www.wired.com/wiredenterprise/2012/01/computer-password/

Timothy. (2012, January 27). *How Allan Scherr Hacked Around the First Computer Password*. Retrieved November 24, 2013, from Slashdot: http://it.slashdot.org/story/12/01/28/024220/how-allan-scherr-hacked-around-the-first-computer-password

Watson, I. (2012, February 1). *The World's First Computer Password*. Retrieved November 24, 2013, from Universal Machine: http://universal-machine.blogspot.com/2012/02/worlds-first-computer-password.html