The Password Conundrum by XXXXX
April 3, 2014

INTRODUCTION

The world is increasingly moving towards computer based verification, a venue where personal recognition cannot confirm an individual's identity or their right to access assets or information. Instead user name and password combinations are employed. Individuals are required to obtain account credentials and remember user names and associated passwords, often for simple transactions. The average user has multiple accounts but generally has only a few unique passwords. Account security is greatly reduced by a lack of password diversity as one compromised account can put many others in peril. Individuals are often unaware, uniformed or misguided by what constitutes strong passwords and of the various risks they face.

IMPORTANT IDEAS

Morris and Thompson [1] examine what constitutes a strong password and what users are actually using. The concept of attacker and defender (bad guy and good guy) are used to analyze the security of UNIX passwords. Master password files are vulnerable when stored as plain text on a mainframe but gain a measure of protection when encrypted. The strongest passwords draw from a pool of all 128 ASCII characters and gain strength as they increase in length. However, many seemingly strong passwords remain vulnerable to brute force attacks that cycle through a list of common words, called a dictionary attack. In practice, users do not make sufficiently strong passwords as a vast majority are vulnerable. Having the mainframe check for password strength when it is initially set by a user and requesting stronger passwords be used can improve the situation. Appending 12 random bits to an input password and encrypting the entire string, also called salted passwords, adds little overhead to a system but dramatically increases the potential pool of passwords for an attacker to try and solve by brute force. Logging user access to a system can help illuminate potential malicious behavior and implementing encryption can reduce the overall vulnerability.

Adams and Sasse [2] found that users have little concept of what made a password secure and fault administrators for keeping security risks from users. Many users have multiple passwords, either due to using different applications or being required to change passwords due to expiration. Many users admit to writing passwords down or choosing very simple passwords in an effort to remember them. Some techniques users feel assist them in remembering passwords, such as related passwords (pass1, pass2, pass3) actually cause worse retention due to their similarity. Users misunderstand that secret style passwords like using a mother's maiden name are vulnerable to dictionary attacks. Motivating users to choose better passwords is often viewed as punitive and may cause users to minimally comply with regulations but still choose poor passwords. A better solution is to modify systems to combine credentials where possible as there is mounting evidence that five passwords are the maximum users can realistically recall. Administrators need to begin educating users to the threats that exist and the best practices to avoid them. The use of physical security mechanisms such as smart cards are a better solution that greatly reduces the necessity to recall passwords but can be expensive.

Ives, Walsh and Schneider [3] demonstrate the tremendous risks users face by having multiple accounts that use the same or similar passwords. Data breaches are occurring with regularity and passwords get stolen. “Users who reuse passwords often fail to realize their most well-defended account is no more secure than the most poorly defended account for which they use that same password.” Users continue to exhibit poor choices in choosing and maintaining passwords despite many of them comprehending some of the best practices for password security. Despite the high costs, physical security mechanisms are the best solution for e-commerce sites but they are not being implemented in appreciable numbers. Public-key infrastructure utilizes public-key encryption to verify a user's identity without passwords. By storing a large public key on a client computer or smart card, security is simplified and increased in theory, but there have been difficulties in it's implementation. Education of users and additional auditing of passwords are the current best measures to achieve the greatest security without dramatically changing the status quo such as with smart cards or public key encryption.

Gaw and Felten [4] show users have a limited number of passwords for online accounts and these passwords tend to be reused. One problem is passwords are required on sites that only identify users and have little to nothing of value to protect. Users realize they are receiving minimal benefit and this reduces their overall view of password importance. Users justify password reuse due to the large number of accounts they have and their difficulty in remembering password combinations. As a user gains more accounts, they tend to reuse passwords instead of make new ones. Over time, this causes more accounts to share the same or a related password which increases overall risk.

Users mistakenly view those closest to them as the greatest security risk for accessing their accounts and orient their passwords to protect against human attackers. Users recognize strong passwords when they are shown guidelines for password strength but most don't follow those guidelines in practice. They generally don't recognize the risks of automated dictionary attacks nor the threat posed by stolen passwords regardless of their level of technical prowess.

Egleman et al [5] shows users choose stronger passwords when exposed to meters displaying the strength of their password. This effect is more evident during password changes than during account creation. The increase in password strength is significant with both traditional password strength meters that rate passwords from weak to strong as well as with comparative strength meters that displayed the strength of a user's password versus their peers. However meters don't influence users to make stronger passwords when they perceive they are for an unimportant resource. Nor do meters address the security concern users face when reusing passwords from other locations.

One of the newest threats to password security comes from issues unrelated to actual password strength. Fink [6] reports strong passwords don't protect against recording devices that have special software installed to track finger movements. Xinwen Fu developed software which illustrates the systematic vulnerability of pin based passwords. The software can determine a password with incredible accuracy after watching it be entered several times from as far away as 140 feet, with little regard to viewing angle. The only protection users can achieve involves installing tools that randomize the placement of the virtual keys on a screen. However, few users know of the risks let alone the solution.

Wiedenbeck et al. tested a graphical password system [7] to attempt to minimize the deficiencies associated with recall of random text passwords. Human memory is shown to be better suited at recalling images rather than words. Utilizing a password system that relies on users selecting multiple points within a photograph in a sequence holds promise. Images with more discernible complexity such as a photograph of a multicolored group of marbles seem more suited to creating and retaining valid passwords. Passwords increase in security when the level of precision used to consider a point valid during password entry is higher, but memorability suffers. A big question posed by graphical passwords is how users would fare if they had multiple such passwords as the gains in security and performance might be attributable more to the uniqueness of the situation than the methodology.

CONCLUSION

The methods to increase conventional password security are often understood by a great number of people. Character diversity and password length have long stood as hallmarks of password strength. While many understand these principles, most are unaware that dictionary attacks and data breaches are omnipresent dangers. Few individuals take proper steps to properly protect themselves. Instead they choose simple passwords, reuse them and rarely change them.

Some of this carelessness is conditioned apathy from users being forced to create passwords for obviously unimportant resources. Some of it is a lack of education or clear understanding of the threats they face. And a final measure is the mental limitation due to the sheer number of combinations they are forced to try and remember. This causes users to create passwords they view as secure such as secret type words but are still vulnerable to dictionary attacks. Users often resort to writing down and reusing passwords they create because they feel they have no other good choices.

Technology brings problems and solutions to the table. The most effective solutions are based on physical measures and are the most costly. As smart card technology matures and becomes cheaper, it holds great promise. Within the current world of user names and passwords, administrators can assist users by giving them feedback on password strength and generally educating them to the risks of insecure passwords. New methods of generating passwords, such as relying on photographic recall hold promise but are a niche solution for now. New methods for maliciously accessing accounts continue to come to light, from advanced attacks based on brute force methods, data breaches that expose tens of thousands of accounts, to surveillance that can steal a password while it is entered while sitting in a restaurant or market.

The solution that occurs again and again is education. The best tools can be on the market but if one is unaware of them they confer no benefit. Administrators and advanced users need to encourage better password security in a way that does not alienate but clearly fosters a understanding of the risks and instills a desire to ameliorate them.

REFERENCES.

[1] Morris, R,. and Thompson, K. Password security: a case history. *Commun. ACM* 22, 11 (November 1979), 594-597.

[2] Adams, A. and Sasse, M.A. Users are not the enemy. *Commun. ACM* 42, 12 (December 1999), 40-46.

[3] Ives, B., et al. The domino effect of password reuse. *Commun. ACM* 47, 4 (April 2004), 75-78.

[4] Gaw, S. and Felten, E.W. Password management strategies for online accounts. In *Proceedings of the second symposium on Usable privacy and security* (SOUPS '06). ACM, New York, NY, USA, 2006, 44-55.

[5] Egelman, S., et al. Does my password go up to eleven?: the impact of password meters on password selection. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '13). ACM, New York, NY, USA, 2379-2388.

[6] Fink, E., (July 7, 2014) Google Glass wearers can steal your password [Online] Available: http://money.cnn.com/2014/07/07/technology/security/google-glass-password-hack/

[7] Wiedenbeck, S., et al.Authentication using graphical passwords: effects of tolerance and image choice. In *Proceedings of the 2005 symposium on Usable privacy and security* (SOUPS '05). ACM, New York, NY, USA, 2005, 1-12.