End User Security

Ben Tribelhorn '07
Harvey Mudd College
Computer Security
btribelh@cs.hmc.edu

Abstract

This paper details security risks, compromises, and options available to the average computer user. It includes specific discussions of encryption and password security. Analysis of a survey of Harvey Mudd students is also presented.

1. Introduction

This paper seeks to address the relevant security concerns that a typical end user should be aware of. The average end user is defined as someone who turns one their computer and expects it to work and to be secure to some extent. To address security concerns one must be aware of risk which includes using the internet and email, location, and the user's actions. This will lead to a discussion of passwords which is likely the most important thing to consider for an average user because it is the simplest bottleneck in security to attack and to fortify. In the end, utilizing security for computing is akin to locking the doors to your house; it is *only* a deterrent! Unfortunately many users find themselves too lazy or too disinterested to take advantage of security precautions.

For the purpose of this paper, Mac OS X was chosen as the operating system to focus on because of its accessibility. Comparisons are made with Windows, however implementing certain security measures under Windows can be prohibitively difficult.

2. Expectation

The belief of privacy and security when at home in front of a computer is easy. So easy in fact that everyone finds solace in this privacy to some extent. The expectation of a user is that the information travels unread and uninterrupted from end to end, and that it's perfectly secure when SSL is used. The problem is that using the internet is like walking out the front door into public, every moment spent outside is inherently insecure. You can be tailed, you can be watched, your conversations can be heard. You have to talk in code while at the coffee shop to be sure of the safety of your communication. And yet, almost no one encrypts their email. There is an obvious lack of thought associated with computer use. Even when ignoring outgoing traffic on the internet, simpler security concerns are prevalent everywhere.

3. Risk

Risk is apparent in every facet of computing. Basic awareness of risk can significantly increase user security. The two typical environments of most users are home and office. Although businesses usually manage and enforce protection, assuming the same security at home is potentially disastrous. Alternately, trusting physical security at the office to be as secure as your home is also fallacious. Possibly the largest security risk day to day is user fallibility, spanning from password choice to wanton clicking.

3.1. Internet

The internet is vast and most people think of internet browsing when the word internet is said. It really is a lot more than that, but browsing alone is riddled with insecurity. Once a computer is connected to the internet, it is accessible in certain ways from any other connection to the internet. Firewalls are designed to protect the computer from undesired entries and are discussed more below. Other security holes from just browsing are plentiful enough. Here is a sampling.

In basic browsing many people buy stuff online from places like Amazon.com and want to ensure that their private data is secure and securely transfered. Users must be wary of fraud and the validity of web sites. When a certificate is unknown to the browser, an effort needs to be made on the part of the user to check the validity of that certificate and the certificate authority.

An easy exploit, that your kid's friend could commit, is to take advantage of the auto-logon and auto-fill/cookies services that your computer offers. In some cases you can

trick auto-fill to fill in enough information (*e.g.* forgotten password 'secret' question) to hack your accounts. A computer will auto-logon to an administrator account leaves all sort of openings in the system and user data.

The Mac operating system will ask if you really want to run an application the first time it is being opening on the system. This feature is particularly helpful in preventing accidental downloads from running on the system. It is a clear warning that often times, downloaded software is buggy and can be some form of malware that is designed to subvert your system. Anti-virus software will attempt to protect the user from these sorts of applications but can be wrong or unable in many cases, so your security is relative to how much you trust and how effect that software is. This will be discussed in more detail below.

3.2. Email

Often the vulnerability of a user is increased when using email. Fraudulent email easily ensnares unwary users. With the currently increasing volume of junk mail, most users are inundated with email. Eventually, one slip opens you or your computer to a phishing probe. A quick way to protect yourself from these scams, you can avoid clicking on links in email. For example, if you receive an message that claims to be from ebay and you're not sure, type `www.ebay.com` into your web browser rather than trusting the provided link. Links are very easy to falsify. A lot of times users don't check the exact address that an email comes from. If it says from "`Ebay Support and Customer Service <customer-reply18234@ebaz.com>`" then it's obvious that it is not from ebay.

Unlike conversations behind closed doors and on the telephone or letters in sealed envelopes, email is not private. "Managers can legally intercept, monitor, and read employees' email."[11] It is clear that email is significantly different from older methods of communication and with it comes a myriad of subtleties. The most well defined of these is the fact that email is an insecure and virtually public method of communication. There is a simple fix to this though: encryption.

3.2.1 Encryption

Although very few people use encryption with their email, it is an easy addition to make. A standard encryption method is PGP[10] which relies on a public/private key set. The public key for someone is freely available from a public server and the private key is held by only the user. This guarantees that only someone with the private key can decrypt something encrypted with the public key. This method of encryption is fully secure given a few reasonable assumptions: the private key is only held by its owner which means that physical security is an issue, and the public key server is not compromised, and you trust your software which is always a concern. Trusting software is a requirement of computing and software is basically guaranteed to be buggy at best. Since the user can't do anything about the second two assumptions, the primary weakness of PGP is access to your private key. Since your private key is password protected, it is imperative that you employ a secure password. Ultimately PGP is as strong as your password and access to your computer.

To be able to claim that setting up encrypted email is an accessible process for the average user, I set up PGP email, validated my key's fingerprint with my sister over the phone, and then sent and received encrypted email. To make the study reasonable I chose a different setup from my sister's. My sister installed a trial of the PGP Desktop 9.0[10] and also set up a web-based email account that does encryption automatically.[6] My method was to download and install Mac GNU Privacy Guard[7] and then to download and install Sen:te's PGP[3] for Apple Mail. I also took advantage of Mac OS X's unix base and checked the MD5 checksums of everything that I downloaded. To do this I opened Terminal and typed: "md5 <filename>" which returns a string that I dutifully compared to the one on the site with the download link. Of course, the packages are also signed with the provider's PGP key, but at this point the effort becomes too great for the lack of benefit. At this point a PGP key can be generated by the installed software and then encryption of emails merely requires typing in a password to encrypt or decrypt a message. The great thing about this set up is that I can search the public key server for someone's key and download it easily. I think that after 15-30 minutes of basic setup, this method is the most convenient but the web-mail method is equally valid and possibly more useful for people who travel or use public computers.

3.3. Home

Many homes today utilize the wonderful Wi-Fi technology designated 802.11 by purchasing a wireless router at the store. They are easy to configure, some automatically configure themselves. Very few homes bother to secure these networks or to change the password for the unit. A number of security flaws present themselves with this technology. An unprotected wireless network allows your neighbors to access the internet and the inside of your home network. This means that anyone in close proximity to your home (a parked car in the street by your house) can get inside any hardware firewall you or your ISP has. They can start interacting with your computer and probably gain full access to your files given enough time. The other problem is that because you're serving the internet you end up in a tight legal position. Often you are violating the terms of agreement with your ISP, but you could even be responsible for the actions of your neighbors over your home network. Even

home networks that use WEP encryption to protect their wireless traffic are at risk. It has been shown that the WEP encryption can be broken in a short amount of time.[1] Once again it is evident that security is only a deterrent. However, it is still worthwhile to add access control and encryption to home wireless networks, especially access control to limit your neighbors.

In the case that someone does manage to gain access to your home network, the question of protection is still relevant. Software firewalls are easy to enable and run with virtually no footprint. So on a computer one might expect that the OS provides this by default. Under Windows this is not true, but with Mac OS X "[a]ll the communication ports are closed and all native services — personal file sharing, Windows file sharing, personal web sharing, remote login, FTP access, remote Apple events and printer sharing — are turned off by default."[5] Minimization of services is the best way to protect your computer. Often anti-virus software will attempt to do this for the user.

Anti-virus software typically does a number of different things. McAffee and Norton will block ports (a software firewall), scan downloads and drives, among other things. For users of Windows it is necessary to run anti-virus software to prevent infection and to recover from infection. The concern with anti-virus software is that you have to trust it. How much do you trust your software? You shouldn't. A case of this would be the Sony root kit fiasco, where Sony CDs would install a cloaked piracy protection program that opened the system to several hacks from internet sources. For a significant amount of time the anti-virus programs wouldn't even notice it. Eventually they updated to remove the cloaking, but leaving the software left the systems open to attack. The Sony root kit actually modified system files so that forcible removal would irrevocably damage the system itself. Finally, Microsoft released software to remove the intruding software because the anti-virus companies didn't believe the threat.

3.4. Business

Computing at the office can depend greatly on policy. Do you know the policies that effect you and by how much. Very often policies aren't enforced or even enforceable. Of course violation of policy will matter in a legal arena, but before that it's important to set some of your own policies to protect yourself.

In a business situation, physical security is a larger risk than it is at home. Written passwords on sticky notes under the mouse pad or on the monitor are five-second-easy. Locking screen savers are native in most operating systems and usually part of that computing policy you signed at hire. Mac OS X provides an on-the-fly file encryption service called FileVault[5] that is very useful for laptop users, especially in the case of theft. Much to the chagrin of users, they often choose not to use these services due to the performance hit or inconvenience of enabling them.

4. Passwords

As we've seen, passwords are the most influential and dynamic component of computer security. Since passwords are clearly so important it's worth considering what makes a good password on two counts: security and usability. The average person must choose their password weighing these tradeoffs which comes down to complexity versus memorability. Following these points are results from a password survey informally conducted at Havery Mudd College.

4.1. Security

Secure passwords:

1. Contain no words.
2. Are at least 8 characters.
3. Contain at least one character of each: upper case, lower case, numeric, non-alphanumeric.
4. Are changed often.

A secure password maximizes entropy, so the most secure password's length is the longest the system allows and consists of a random selection of all possible characters. Realistically, a password should meet the aforementioned requirements. Additionally, passwords that contain native language words are prone to dictionary attacks. However, this typically isn't enough of a worry to users because in a survey of 3,289 passwords on a unix system, 86% were easily broken and about one third of all the passwords succumbed to a dictionary attack in under five minutes.[8] Evidently, many passwords are poorly chosen. Many times software will enforce password policy to avoid easy to hack passwords.[9] Unfortunately, enforced rules can force users to choose easy passwords or to change passwords rapidly to be able to go back to a favorite password. This type of user actions compromises security.

4.2. Memorability

Human memory is the limiting factor in secure passwords. "[H]uman memory for a sequence of items is temporally limited," and when remembering "a sequence of items, those items [...] must be familiar 'chunks' such as words or familiar symbols."[12] What this means is that an arbitrary sequence of characters is virtually impossible for human memory to easily remember. Specifically, the neocortex is the part of the brain that is associated with memory and it can be though of as a pattern-matcher.[4] Since the neocortex matches associatively, passwords need to have components that have meaning. This limiting factor reduces

the entropy of passwords significantly. Often difficult passwords that are either provided or required to include certain non-alphanumeric characters encourage users to write down their passwords. In some cases, this can compromise security completely.

4.3. Survey of Passwords

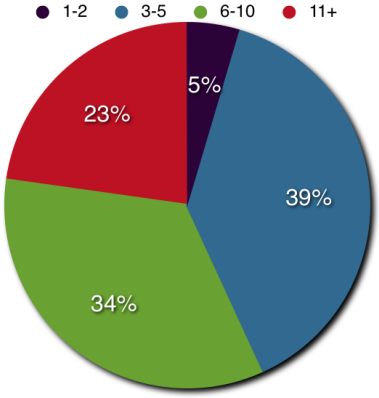

Figure 1. "How many passwords do you have?" A majority, 57%, of users have more than five passwords. Given that human short-term memory has a capacity of seven plus or minus 2 items[12], roughly a quarter of responders have too many passwords to remember for concurrent use. This can be seen in Figure 2 as 28% of responders write down their passwords.

In regard to the list of secure password qualities above, I constructed an online survey and emailed a link out to the east-dorm-chat list and friends of mine in order to have some relevant and current statistics on password security. The survey size was $n = 45$. Since the population surveyed was primarily Mudders and over half were CS majors, one would expect their passwords to be more secure than the average soccer mom's passwords. My questions attempted to address the salient statistics of passwords. Unfortunately my question on the prevalence of words, names, dates in passwords was misunderstood by enough of the responders that I felt its result needed be thrown out.

We see in Figures 1 and 2 that the number of passwords that users have is variable and based on memory studies, it seems that roughly a quarter of users write down their passwords because they have so many. To support this claim, roughly 85%[1] of responders should follow this trend. For an overlap of $n = 43$, I created a table of theoretical values as shown in Table 1. The survey data is presented in Table 2. Statistical inference yields a $\chi^2 = 1.6$ which gives confidence level at $p = 0.05$ for my claim. So, the key here is to keep your number of passwords to a small enough set that you aren't forced to write them down. This will increase your security.

[1]85% is standard for primary explanatory variables. The remainder is explained by uncontrolled variables and random variance.

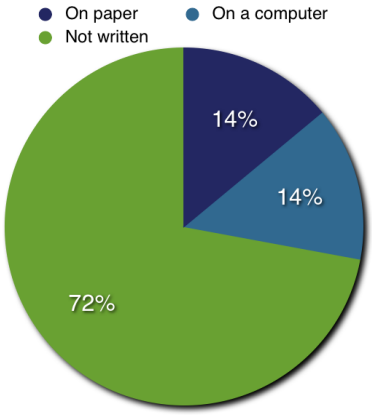

Figure 2. "Do you write some or all of your passwords down?" One quarter of users write down their passwords.

Passwords	Written	Not written
1-10	3	27
11+	10	3

Table 1. These are theoretical values assuming an 85% correlation between number of passwords and whether or not passwords are written down.

Passwords	Written	Not written
1-10	5	27
11+	7	4

Table 2. Compiled survey responses to the questions "How many passwords do you have?" and "Do you write some or all of your passwords down?"

I asked a set of three similar questions on the complexity of a person's set of passwords. Figure 3 depicts the results from one of the questions, the other two asked about subsets of user passwords. As one would expect, most people have at least one password that is relatively secure. The importance of the question shown is that it was phrased in such a way that if someone has one 'dummy' password for things that aren't important then we can still see that even people who should be aware of password security don't use non-alphanumerics all the time. It is clear that password security can always be improved by a conscious effort on the part of the user.

Finally, changing passwords is a good security measure when users voluntarily follow this policy. Unfortunately, many people dislike changing their passwords due to its inconvenience. I asked a simple question of frequency offering a range of choices as can be seen in Figure 4. No responders claimed to change their passwords often and at least 65% change their password far too infrequently. Clearly, rotating or changing passwords is too much of a pain in the user's mind to merit doing it.

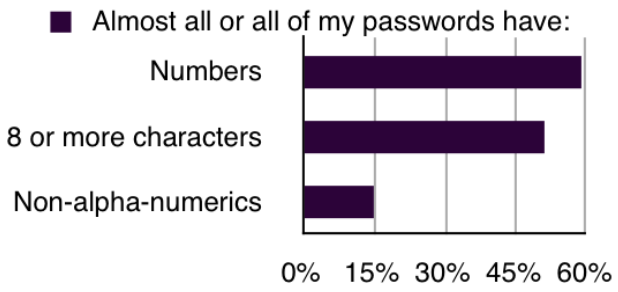

Figure 3. This chart shows the security of people's entire set of passwords. We can see that non-alphanumeric characters, often considered the key to a secure password, rarely permeate all of a set of passwords. This means that most people have at least one high risk password.

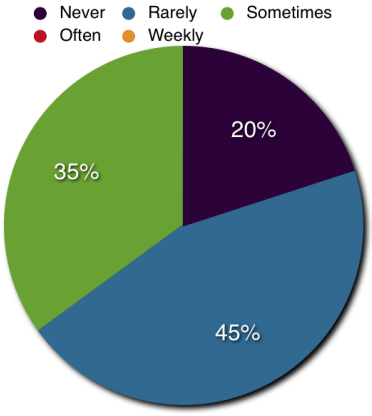

Figure 4. Frequency of password rotation or changing. No one willingly changes their passwords often.

4.4. Limitations and Reality

Passwords comprise the *key* variable in security and are easily enhanced by user volition. However, in the end, the value of the property being protected will weigh with convenience. It may be worth the user's while to run intrusion detection[2] over securing their passwords. Often a reactive policy is most popular.

5. Conclusion

Security is and never will be complete protection, nevertheless, it *can* be an effective deterrent to all but the most serious adversaries. Trust is a key component to good security and yet it is very situational to the extent that no system or user can choose the correct set to trust. What makes the biggest impact in security is the set of choices that the user makes, including choice of software from downloaded applications to operating system, choice of daily practices from using encryption to secure file systems, and of course, choice of passwords.

[2] *e.g.* Tripwire, Little Snitch, CheckMate.

5.1. Where do you go from here?

A multitude of security enhancements are available and constantly evolving. These include RSA's SecurID which uses a physical random number generator to confirm identity, and bio-informatic technology that scans various unique physical traits such as fingerprint or the eye's iris.

Passphrases were not mentioned in this paper, but they are significantly longer than a password, so they can offer heightened security if well chosen. A site for random generation is Diceware[2] which might be helpful for using the encrypted webmail service[6] mentioned earlier or tighter security for login. Most operating systems now support passphrases.

For the user to gain security they must be aware of the risks presented in this paper *and* be willing to make the effort to address these risks by making smart decisions. Security should no longer be neglected in fear of it interrupting work flow, it needs to be accepted as the best way of computing.

References

[1] N. Borisov, I. Goldberg, and D. Wagner. Intercepting mobile communications: The insecurity of 802.11. http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html, 2001.

[2] Diceware. http://world.std.com/ reinhold/diceware.html.

[3] GPG Mail. http://www.sente.ch/software/GPGMail/.

[4] J. Hawkins and S. Blakeslee. *On Intelligence*. Times Books. Henry Holt and Company, LLC, 2004.

[5] http://www.apple.com/macosx/features/security/.

[6] http://www.hushmail.com.

[7] Mac GNU Privacy Guard. http://macgpg.sourceforge.net.

[8] R. Morris and K. Thompson. Password security: A case history. *CACM*, 22(11):594–597, 1979.

[9] PassfiltPro Eliminate weak passwords. http://www.altusnet.com.

[10] http://www.pgp.com.

[11] S. P. Weisband and B. A. Reinig. Managing user perceptions of email privacy. *Commun. ACM*, 38(12):40–47, 1995.

[12] J. Yan, A. Blackwell, R. Anderson, and A. Grant. The memorability and security of passwords – some empirical results, 2000.