Passwords and their alternatives: How we should (and do) try to secure our data, and why it isn't working. Yet.

Carter Casey
Mentor: Ming Chow
Tufts University Department of Computer Science

Password security, which may be the most common security tool a person interacts with on a daily basis, is flawed. In this paper I discuss some of their flaws - while some of the problems come from how passwords work in the first place, a majority arise because humans aren't good at using passwords securely and effectively. I then approach some of the alternatives to passwords that have gained popularity over the past couple years: biometrics, multi-factor authentication, and smart cards. The advantages of using these techniques are again tempered by a mix of software and human flaws. I also provide software that can create a (very basic) usb key to encrypt and decrypt sensitive files on a user's machine. It seems that while we should use better and stronger techniques of protecting our data, we also need to improve people's understanding and appreciation of security.

With technology deeply engrained in human life, the way we secure our digital property has risen to a level of importance comparable to protecting our physical property. A break-in can be less devastating than identity theft; bank robberies don't have to happen with a gun and mask anymore, and often a keyboard, internet connection, and technical know-how are plenty to pull a major heist. To keep ourselves safe, many people and digital systems use password protection. The vast use of passwords makes them arguably the most common security tool used by anyone on the internet.

However, password protection techniques haven't kept up with advancing technology. Despite being used so frequently, passwords are an old idea. The MIT manual makes reference to a "six character secret password" used on the ac-

counts of their Compatible Time-Sharing System back in the 60s (Crisman, 1965). Since then we've started encrypting our passwords for internal storage with stronger and stronger algorithms, but not much else has changed. On the other hand, our understanding of how to crack passwords has grown phenomenally in that time. There need to be better ways to combat attackers who would gladly take advantage of those vulnerabilities.

This problem is well recognized in the tech and security communities, and consequently there are many attempts at creating secure alternatives to using passwords. These include biometric verification, typically in the form of fingerprint scanners, as well as multi-factor authentication and smart card verification. The proponents of these methods claim that each one is stronger than password protection schemes used today. There are, indeed, advantages to these password alternatives, one of the more obvious being that they *aren't passwords*, and attackers don't have the depth of tools with which to crack them.

To demonstrate how a simple password alternative might work, I've put together a proof-of-concept smart "card." Given the right software and a big enough usb drive, it should lock and unlock certain files when attached to and ejected from a computer.

There are, of course, disadvantages to using password alternatives, not the least of which being their usability. People are often uninterested in proper data security. In fact, that may be the core problem we face when trying to secure data. Even though more people claim to be aware of the risks and best practices to use when using the internet and computer systems, a much smaller proportion actually put these practices to use (*McAfee Internet Home Users Survey*, 2011). This, to my mind, is the real danger to our security.

To the Community: Why passwords matter

Passwords are everywhere. If you have any presence at all in the digital world, you can't escape having at least password. Most people have more passwords than they can keep track of - literally. People often deal with the overwhelming number of passwords they're asked to use in very insecure ways. The typical example is your grandmother, or your coworker, who keeps post-it notes one the edge of their computer screen, squinting at that neon scrap of paper whenever they need to log in to their email or work account.

Writing down your passwords is dangerous, and a huge security risk at workplaces where pass-

words are the key to proprietary information. But even for proficient internet-users, who may scoff at the idea of leaving their passwords out on a bright pink invitation to steal it, aren't immune. Password reuse is hugely common, and very dangerous. A large-scale (500,000 users) study by Microsoft into password strength and reuse found that an average user's password is used at around 6 different sites (Florencio & Herley, 2007). This means that an attacker only needs to get the password for one site to break into 6 others - you might not care if your Facebook password is stolen, but if it's the same as your Amazon or banking password, you could be in deep trouble. Cases like this have already occurred, from the thief who stole 450 passwords from a Kinko's facility and used them to defraud banks, to an attacker who managed to use password reuse among several websites to crack 47,642 accounts (Blake Ives & Schneider, 2004).

On top of everything else, a password is only useful if it's strong and can stop an attacker from getting into your account. The original password length of 6 characers just won't cut it anymore, and neither will passwords that are easy to guess. Unfortunately, "easy to guess" covers a lot more passwords now that tools like John the Ripper let you use your computer and lists of known passwords to brute-force password cracking. This has led many companies and organizations to require users have long and perhaps more complicated passwords - which are harder to remember, spurring users to do exactly what is detailed above: writing them down and re-using them. And so we find ourselves with a classic problem: how do we balance usability and security? There are two ways that seem evident right now: better education, policies, and tools.

Action Items

Users want to be secure. People like to be safe in general - it's not as though people would rather they not be protected. If you know there's a thief in the neighborhood, you'd probably prefer to have a lock on your door than leaving it wide open. The same is true for people who realize that attackers are constantly after personal information; we'd prefer to have that password locking our data up so only we can get it. There are two caveats to this: awareness, which we can tackle with education, and convenience, which requires smarter security policies and better tools.

User Education

Notice that I said ïf you *know* there's a thiefänd p̈eople who *realize* that attackers ...F̈or a

user to appreciate the protection they're given, they have to be aware of the threat in the first place. People might not have a strong enough sense of what threats they're presented with on a daily basis. People in "safe neighborhoods" probably don't lock their doors as frequently as those living in places where robberies are common place. Think of leaving a spare key somewhere obvious (say, under your doormat), and compare that to writing down your password in a notebook next to your desk. If you're not too worried about a break-in, or maybe if you just don't realize how obvious your backup plans are, you won't think twice about giving a thief all the tools they need.

A study found that 21% of users "don't think it's necessary to change account passwords regularly," and 25% "never change their passwords unless prompted" (*McAfee Internet Home Users Survey*, 2011). The security community knows that changing passwords is very important, because eventually they do get broken, but a particular user might not. Part of the problem seems to be that, although organizations enfore security policies, they often don't do much to convince their users why they're needed. I would argue that people will care more about password protection if they knew about the risks they face when online, and the benefits of stronger passwords.

Policies

Password Alternatives

References

Blake Ives, K. R. W. & Schneider, H. (2004, April). The domino effect of password reuse. *Communications of the ACM*, *47*(4).

Crisman, P. A. (Ed.). (1965). *The compatible time-sharing system: a programmer's guide*. The M.I.T. Press.

Florencio, D. & Herley, C. (2007). A large-scale study of web password habits. *Microsoft Research*.

Mcafee internet home users survey. (2011, October). National Cyber Cecurity Alliance / McAfee / Zogby Int'l.