Passwords and their alternatives: How we 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: physical password keys (such as smart cards), biometrics, multi-factor authentication. 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 accounts 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 passwords 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 characters 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 and better 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 pro-

tected. 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 could require 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 enforce 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.

Password Alternatives

Physical Password Keys. This tool is being implemented with growing popularity: the idea is to only let a user access their account when a physical key, whether in the form of a usb drive or a smart card, is attached to the computer. One of the more recent companies to try using this method of authentication is Google. They have announced a simple usb key that fits on your keychain; when logging in to any Google account, the user is prompted to press the button, and is automatically authenticated (Simonite, 2014). They're not the first to try something like this, but given the reach of Google's services, they're likely the organization with the broadest reach, not to mention very strong tech credentials.

The upside to a physical key is, of course, that an attacker can't get to the key without access to your local machine, or to the key itself. This is an ideal protection from scanning attacks, and it saves the user from dealing with yet another complicated password. The downside, of course, is that stealing the key is tantamount to stealing the password, and much easier for a thief with close access to the victim. If they could steal a key to your house, or your wallet, they could steal the password key as well.

To supplement this paper, I've implemented the software that (should) create a simple usb key for encrypting and decrypting files. After the scripts are up and running, whenever the usb drive is inserted, the encrypted files will be decrypted into their readable counterparts. Upon the ejection of the drive, the same files should be removed

from the designated folder, leaving only unreadable files encrypted with what's known as a one-time pad. The scripts and code are a proof-of-concept, to be sure, but serve to demonstrate the method behind password key technology. The files are included in my Security Github account, at https://github.com/tuftsdev/comp116-ccasey/tree/master/finalproject/pad-crypt.

Biometrics. The concept of biometrics is simple - use measurements of the user's body to verify their identity. The obvious example is fingerprint scanning: everyone has a unique fingerprints, so if another person picks up your device and tries to unlock it, they shouldn't be able to. What's more, fingerprints come pre-packeged. We all have them (barring unfortunate accidents and the like), so there's nothing to think about and remember - just swipe and go. The more recent versions of Apple and Samsung mobile devices even have built-in fingerprint scanners, so we know that it can be implemented on a wide scale. So far, the idea doesn't sound like a bad one.

Unfortunately, there's more to the story. Fingerprints aren't a "secret" - passwords are (generally) kept hidden from the outside world, whereas anyone can pick up a person's fingerprint with a couple of low tech tools. This would be an issue if a thief stole your fingerprint-locked phone as well as something with a surface prone to collecting fingerprints; with certain phone screens, those are one and the same. After getting your fingerprint, there are methods in place that can fool biometric scans - researchers in Germany have already shown that one of Samsung's phones can be fooled. (Eadicicco, 2014)

So there's a trade-off. Relying on biometrics - at least fingerprints - to protect physical devices does have some downsides. They aren't foolproof, and their use is somewhat limited. Perhaps the place for biometrics is to supplement other protection tools. A semi-strong password and a fingerprint may not amount to a whole lot on their own, but together, couldn't they provide more protection? This is actually the premise of multi-factor authentication.

Multi-Factor Authentication. If passwords aren't going to cut it, why don't we add something? Reinforce the passwords with an extra check, to make doubly sure the user is actually who they say they are. In two-factor authentication, this is typically done by having users enter their password, then refer to another device or site to get a passcode that must be entered into the login screen. This could easily be further supplemented by, as I mentioned before, biometrics, giving us what could be a very secure three-factor authentication. There are even alternative schemes out there; PassFaces asks users to remember a series of faces, which they then have to pick out of a group of pictures when they log in to their accounts (Tanaka, 2012).

While any one of these methods might not be very powerful on their own, multiple tools give users strong redundancy. Even if your password is cracked, if the attacker doesn't have your phone or access to the passcode server, they can't get into your account. Likewise, stealing a phone doesn't give the attacker much without a password, which takes time to get. It's clearly possible to get break multi-factor authentication, since we know how to break all the pieces, but the goal isn't impervious defenses. The goal is making the defenses hard enough to breach that an attacker will need so much time and energy they won't find it worthwhile.

There is one potential downside to multi-factor authen-

tication, though not from a security perspective. It's just more cumbersome to use. Perhaps a person who is educated in the field of security, or one who has been the victim of a digital attack (such as identity theft), wouldn't find the effort too much. However, many people find the simple act of typing in one password to be annoying, let alone typing in a password, waiting for a text, then typing that in. Multi-factor authentication has great potential to improve general security, but only if people actually use it. While we've convinced most people to use passwords, it may take some effort to get those same people to take the next, more secure step.

Conclusion

There isn't one, cure-all solution to the problem of password security, but we probably knew that to start with. In our current position, password protection simply isn't enough to protect us from the threats facing our data. This doesn't mean passwords are useless, but people have to learn how to use passwords properly. On top of that, there are tools that could help replace, or even shore up our current password security. It's the job of major organizations and account managers to put these in place, to help users more effectively tackle the problem of security.

It's important to remember that, as Adams and Sasse pointed out 15 years ago, "users are not the enemy" (Adams & Sasse, 1999). They pointed out that it's the job of security experts to keep people safe, and that doesn't just mean providing them with tools. It also means teaching users how to use them, why they should use them, and what's at stake. More than anything else, we face a lack of communication between people trying to protect, and those who want to be protected. Before anything else, we have to remove the debilitating confusion behind account security - only then can we move forward, creating better tools and transparent policies that users will actually use to keep themselves safe.

References

Adams, A. & Sasse, M. A. (1999, December). Users are not the enemy. *Communications of the ACM*, *42*(12).

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.

Eadicicco, L. (2014, May 11). Passwords are a horrible way to keep us safe. *The Business Insider*.

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.

Simonite, T. (2014, October 21). A physical key to your google account.

Tanaka, E. T. (2012, March 22). Replacing the password: more secure high-tech alternatives to traditional alphanumerics.