Kyle Kodani

CS35L

Assignment 10

Google Declares War on the Password

The article I read was titled “Google Declares War on the Password.” It was authored by Robert McMillan and posted on www.wired.com on 1/18/13. The article focused on Google’s efforts to improve cyber security, specifically through alternatives to passwords.

The article argues that passwords are gradually becoming a less and less secure option when it comes to protecting personal information. While there is much effort put into server side security, client side security has much room for improvement and expansion. An example of this is Google’s two-step login process, which was introduced as an option for Google accounts in 2011. In this process, a user logs in using their password, but then receives a text message with a one-time code that must also be entered to login. While slightly inconveniencing the user, this extra step does add another layer of security to one’s information, and places more of the security burden on the user. This type of login is also known as two-factor authentication (McMillan).

Google’s next step is looking into other techniques for two-factor authentication, or even replacing the password entirely. They are currently experimenting with the YubiKey, by Yubico. The YubiKey is a small chip that plugs into a USB port and is used to log a user into various accounts. The YubiKey doesn’t require the user to have any extra hardware or software (besides the key itself), but it does require some modification of code on the part of the server/website. The key will only work if the site you are

trying to log on to supports it. Ideally, now that Google is backing this technology, more and more websites will make their login systems compatible with devices like YubiKey. In some cases, the YubiKey completely replaces the password as a login tool, but other websites allow for the YubiKey to be used in conjunction with a password for a secure two-step login (McMIllan).

Here's how it works: when plugged into a USB port, the user can tap the button on the YubiKey and it will generate a one time, 44-character, encrypted code. The first 12 characters represent the ID of the physical YubiKey itself, it is manufactured into the key. The remaining 32 characters make up the always-unique part of the one time password. The whole code is sent to a Yubico server to be validated. The validation is then passed to whatever server the user is trying to log on to. This 32-character set includes a counter that increments each time the key is used. If the number of uses counted on the key doesn't match the number of uses counted on the server, the code will be rejected (www.yubico.com).

The YubiKey is very small: it can easily fit in a wallet or on a keychain. It also does not have any moving parts or battery, so it is resistant to various types of damage. Currently, it only functions through a USB port, but Yubico is working on making the technology wireless, possibly similar to Bluetooth. In this way, the YubiKey could easily work with mobile devices. The shape of the key could also change. One idea is to have the key be a ring that one wears and activates when they want to log in (www.yubico.com).

Personally, I think the YubiKey is a great idea. I've always been a bit paranoid about internet security and privacy, so anything to help soothe me is welcome. I have

tons of different accounts for various websites and services, and it is very difficult trying to manage passwords for each one, so I am all for anything that would make that process easier.

However, my inner cynic already sees some problems with this technology. Ideally, users would be forced to have a two-step login, say for instance a password and a YubiKey. However, I don't see this being forced on people. Two-step authentication will likely remain an optional feature for the more popular websites. Users will have the option of password only, YubiKey only, or both. I feel like most people would stick with password only, since a two-step login is slightly more inconvenient. There's also the problem with what happens when you lose the key. Will you be locked out of your accounts? Can the key be deactivated? How does the replacement process work? I'm also cynical enough to believe that this system can be cracked, regardless of how secure it seems. There's always a way.

Of course, someone felt this way too and decided to look into it. The paper by Künnemann and Steel was written about their exploration of YubiKey security protocol. In their paper, they concluded that the YubiKey does its job effectively, but there are still several possible vulnerabilities. For example, if the validation server goes down, users will not be able to log in. Even worse, if the key generation server is compromised, users might still be able to log in, but their codes can be tracked and manipulated. To prevent against these server exploits, Yubico has another product called the YubiHSM, where the HSM stands for "Hardware Security Module." This device stores the several future codes for your YubiKey. It can be used in conjunction with the YubiKey to validate your code in the event that the servers go down or are compromised. However, it seems that

even these devices have the potential to be exploited (or physically stolen), mainly due to how it syncs with the server to store future codes (Künnemann and Steel).

## Works Cited

McMillan, Robert. "Google Declares War on the Password." Wired.com. Conde Nast Digital, 18 Jan. 0013. Web. 15 Mar. 2013.

Künnemann, Robert, and Graham Steel. "YubiSecure? Formal Security Analysis Results for the Yubikey and YubiHSM." <http://www.lsv.enscachan.fr/Publis/PAPERS/PDF/KS-stm12.pdf>.

"Yubico." *Yubico*. N.p., n.d. Web. 15 Mar. 2013. <http://www.yubico.com/>.

Also see presentation for additional sources and media.