Yubikeys as an instrument for security education: combating apathy and the lack of computer security/science curriculums in high schools

Leslie Choi
Department of Computer Science
Portland State University
lchoi@pdx.edu

Rebecca Sexton-Lee
Department of Computer Science
Portland State University
resexton@pdx.edu

1. Introduction

Data breaches aren't unusual occurrences anymore and 2018 has been an eventful year for a sector that is vastly popular with the younger generation: social media. Facebook faced an attack that left 50 million users' personal data exposed and similarly, Quora had a breach that exposed user data such as encrypted passwords and links to other social media accounts [6]. Even Google announced that a bug in the system exposed users' data on their Google+ network and will be shutting down [8]. Despite all of this, there doesn't seem to be an imminent boycott of social media sites, as it has become so integrated in our daily lives in both personal and business matters. Since social networks are here to stay, the best step of action to mitigate these security breaches is to educate users. However, many high schools don't have computer security curriculums that would help increase access to computer science as a career or adequately equip high school students with the skills to protect their own personal information online. Poorly designed passwords and two-factor authentication schemes perpetuate this disconnect by making security difficult or costly to use. To address this, we aim to teach high school students how to use Yubikeys, which are inexpensive physical USB devices, as a way to literally put security back into their hands and potentially bring back a personal responsibility in protecting users' virtual data that has been missing with the constant integration of technology.

2. Two Factor Authentication – Hardly a Foolproof Security Feature

Yubikeys are a specific form of two-factor authentication (2FA), which aims to add another layer of security in addition to the username and password combination for online applications. Instead of just having “something you know”, two-factor authentication requires “something you have” or “something you are” [5]. Examples of 2FA include sending a unique code to the user to verify their identity, often via text or email or using biometrics such as a fingerprint scanners to confirm identity. To combat account hijacking, many social media platforms and applications incorporate 2FA into their services.

Unfortunately, recent attacks have shown that passcodes sent through texts or apps are easily phishable by hackers [2]. Adversaries can prompt users for their credentials and redirect the user to another page to enter their verification codes all within a matter of seconds. The result is the seamless theft of tokens, unbeknownst to the user. The user in this scenario is tricked into verifying the auto-generated code that is then intercepted by the hacker and replayed. Another weakness of 2FA is that adoption of this feature is often low due to usability, user sentiments, and perceptions. In a study conducted by Carnegie Mellon University with their mandatory adaptation of Duo Mobile, researchers found that the largest number of users only implemented it when they were required to [1]. Furthermore, the study found that users who had negative experiences with Duo were less likely to use it again for future applications, with one user specifically stating that it “handcuffs us to our smartphones even more than we already are” [1]. That sentiment is telling of the lifestyle we’ve come to rely on today. If a user is locked out of his or her room where they left their smartphone, there is no way to access Duo and access email or other accounts that require 2FA. This isn’t even considering those who may not own a smartphone at all or know how to use one – a huge disadvantage to the elderly or individuals from low-income backgrounds.

Most users cannot remember a different password for every website, yet they are encouraged not to reuse passwords. When told to enable 22FA, they inevitably must own a smartphone and are then confronted by a multitude of ways to do it including via SMS, a custom per-site smartphone application, or a third-party smartphone application like Duo. Moreover, such schemes are now being bypassed by clever adversaries. While two-factor authentication using passcodes may add extra security, vulnerabilities against them and usability issues have now made it something that no longer works as well as intended.

3. Yubikeys - An Alternative

Yubikeys are physical hardware devices that make it impossible to steal or trigger authentication without tangible interaction from the actual device [10]. Using a physical key provides the

advantage of isolating hardware from malicious software that can intercept the authentication process. The mechanism of verification used in the most basic Yubikeys is the Universal 2nd Factor (U2F) protocol to provide a serial number to a web page without software or drivers, allowing for 2FA with only the touch of the key. Upgraded versions of Yubikeys implement the latest open authentication standard, FIDO2, which now supports password-less authentication, making it even easier for users [4]. Yubikeys may also help improve the user experience of authentication by making 2FA uniform across all sites. Both FIDO2 and WebAuthn allow a browser to prompt for the physical key and bypasses the need for passwords altogether. Standards like these combined with the fact that Yubikeys do not require smartphones will potentially offer a simple, password-less way to log into websites securely. Such a mechanism is the heart of Google's approach that completely eliminated phishing against its employees [7]. Due to their ease of use and effectiveness, we are currently undertaking an effort to teach underrepresented high school students about computer security and to train them how to use Yubikeys to protect their accounts. The goal is to not only help them develop secure online habits, but also engage them in a topic that they might be interested in pursuing as a career choice.

4. Case Study: Yubikeys at CyberPDX

Security breaches are easily performed in part because people aren't properly educated on the basics of web security and how to keep personal information safe when interacting with applications online. Low-income individuals, people of color, and women are especially susceptible to this void of knowledge. In underprivileged communities, schools rarely incorporate computer science or security curriculums in their programs due to reasons such as a lack of funding, absence of qualified teachers who can teach the material, or gender disparities in STEM classes. CyberPDX aims to address all of these issues and provide computer science education to students who don't traditionally have access to the exposure.

CyberPDX is a week-long camp hosted by Portland State University and supported in funding by the NSF and National Security Agency via GenCyber under Grant No. 206965 [9]. Each year, the cohort of students consists of roughly 60% females and 40% ethnic minorities. Camp surveys conducted at the end of the week have demonstrated that interest in security and computer science as a career choice increased and attendees had an overly positive experience overall [9].

We are interested in conducting a longitudinal study to track long-term outcomes of the camp, including how many of these students are victims of phishing after they've gone through CyberPDX. Currently, we are undertaking the development, deployment, and analysis of introducing a 2FA curriculum and training based on Yubikeys in the camp curriculum. Our hope is that by appropriating parts of the CyberPDX funds to invest in Yubikeys for camp attendees, we can increase students' interest in computer science and security and bring awareness to the individual responsibility necessary to be safe with personal information online. The Yubikey will serve as a tool to provide an example of how authentication is implemented and how its usage

differs from traditional 2FA through text messages or email. As most of the camp attendees come from underprivileged backgrounds, we believe that providing Yubikeys will empower them to see security as something they have control over, since many would have no knowledge of how it works or the means to obtain one in the first place. Additionally, we believe that the motivation has to be there in order to stimulate interest in security and promote best security practices. The basic Yubikey is cross platform and supports common applications such as Google, Facebook, Twitter, Dropbox, and more [3]. Integration with social media and common communication applications will serve to further incentivize the use of Yubikeys in addition to teaching high schoolers about the importance and intricacies of secure authentication.

We believe that Yubikeys will be simple enough to use and present an added value to the security issues users face, overcoming any preconceived notions that the devices will be a hassle or ineffective in preventing security breaches. In improving both user experience and training of security in students, we also theorize that it will contribute to students' self-identity as someone who is knowledgeable and capable enough to pursue a career in security. The long-term effects we aim to monitor are the quantity of account compromises and phishing victimization of those introduced to Yubikeys as well as the general interest in pursuing a career in cybersecurity.

5. Measuring outcomes

Our approach seeks to address two issues: improving individual user security of those receiving Yubikeys and increasing the participation of underrepresented groups in the field of computing. With the first issue, we seek to address apathy when it comes to security best-practices, both inside and outside the technology circles. Part of the issue is that the motivation isn't there to incentivize people to care. By introducing a tangible and potentially easy-to-use mechanism early on with high-school students, we hypothesize that they will become less apathetic in securing their accounts online and can use the knowledge and skills gained to protect themselves against phishing attacks and account compromises long-term. Regarding the second issue, high schoolers who are just starting to venture into what careers to pursue may strongly benefit from early access to security education, helping them improve their feelings of self-efficacy which in turn may improve their likelihood of pursuing computer security as a discipline to study. Our goal is to examine the long-term effects of both issues using a long-term study of those who go through the program. With CyberPDX's targeting of underrepresented minorities and specific curriculum, we hope a positive experience with the camp will improve the inclusiveness of the field of computer science and ultimately, STEM education as a whole.

6. References

[1] Colnago, J., Devlin, S., Oates, M., Swoopes, C., Bauer, L., Cranor, L., & Christin, N. (2018). "It's not actually that horrible": Exploring Adoption of Two-Factor Authentication at a University. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI 18*. doi:10.1145/3173574.3174030

[2] Cox, J. (2018, December 19). How Hackers Bypass Gmail 2FA at Scale. Retrieved from https://motherboard.vice.com/en_us/article/bje3kw/how-hackers-bypass-gmail-two-factor-authentication-2fa-yahoo

[3] Discover YubiKeys | Strong Two-Factor Authentication for Secure Login. (n.d.). Retrieved from https://www.yubico.com/products/yubikey-hardware/

[4] FIDO2. (n.d.). Retrieved from https://www.yubico.com/solutions/fido2/

[5] Hunt, T. (2018, November 15). Beyond Passwords: 2FA, U2F and Google Advanced Protection. Retrieved from https://www.troyhunt.com/beyond-passwords-2fa-u2f-and-google-advanced-protection/

[6] Isaac, M., & Frenkel, S. (2018, September 28). Facebook Security Breach Exposes Accounts of 50 Million Users. Retrieved from https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html

[7] Krebs, B. (2018, July 23). Krebs on Security. Retrieved from https://krebsonsecurity.com/2018/07/google-security-keys-neutralized-employee-phishing/

[8] O'Flaherty, K. (2018, December 19). Breaking Down Five 2018 Breaches -- And What They Mean For Security In 2019. Retrieved from https://www.forbes.com/sites/kateoflahertyuk/2018/12/19/breaking-down-five-2018-breaches-and-what-they-mean-for-security-in-2019/#563ae65141c4

[9] Sexton-Lee, R., & Harmon, E. (n.d.). *Bringing computer science to high school students and teachers: Assessing the impact of CyberPDX* [Scholarly project].

[10] Stellabelle. (2017, June 05). What The Heck is U2F? – Hacker Noon. Retrieved from https://hackernoon.com/what-the-heck-is-u2f-35cb68082dbe