Portland State University

PDXScholar

University Studies Faculty Publications and
Presentations

University Studies

3-2020

Securing the Next Generation

Wu-chang Feng

Portland State University, wuchang@pdx.edu

Robert Liebman

Portland State University

Ellie Harmon

Portland State University

Veronica Hotton

Portland State University, hotton@pdx.edu

Michael Mooradian Lupro

Portland State University, lupro@pdx.edu

See next page for additional authors

Follow this and additional works at: https://pdxscholar.library.pdx.edu/studies_fac

Part of the [Curriculum and Instruction Commons](#), and the [Curriculum and Social Inquiry Commons](#)

Let us know how access to this document benefits you.

Citation Details

Feng, W., Liebman, R., Harmon, E., Hotton, V., Lupro, M., Delcambre, L., & Pouliot, D. (2020, March). Securing the next generation. Poster presentation at Special Interest Group on Computer Science Education (SIGCSE) Technical Symposium, Portland, OR.

This Conference Proceeding is brought to you for free and open access. It has been accepted for inclusion in University Studies Faculty Publications and Presentations by an authorized administrator of PDXScholar. Please contact us if we can make this document more accessible: pdxscholar@pdx.edu.

Authors

Wu-chang Feng, Robert Liebman, Ellie Harmon, Veronica Hotton, Michael Mooradian Lupro, and Lois Delcambre

Securing the Next Generation

Wu-chang Feng, Bob Liebman, Ellie Harmon
Veronica Hotton, Michael Lupro, Lois Delcambre
Portland State University
Portland, Oregon

ABSTRACT

Weak authentication practices that rely on passwords for security have led to widespread data breaches and successful phishing attacks. Recent advances in the cost and usability of hardware security tokens have made the prospect of effectively augmenting password-based authentication or removing it altogether a possibility. To actualize this, a paradigm change in how people learn to authenticate accounts on-line must occur. Towards this end, we describe a curriculum to teach high-school students the perils of passwords and a program to distribute hardware security tokens to them as they are first setting up their on-line presence in order to improve the security of the next generation.

1 INTRODUCTION

Hardware security tokens [2] are a specific form of two-factor authentication (2FA) which augments the username and password method for online authentication with secondary methods. Instead of just having “something you know”, two-factor authentication often requires you to supply “something you have” or “something you are” to authenticate. There are many options for performing two-factor authentication including codes sent via text messages, phone calls, e-mails, and security questions. Unfortunately, many of these methods suffer from usability issues and are cumbersome for users to employ regularly [3]. In addition, such methods have been targeted by attackers effectively, leading to account compromises for those who employ them. Hardware security tokens, of which Yubikeys are an example, have been shown to completely eliminate account compromises due to phishing [4]. As a result, training the next generation of Internet users how to use such tokens as they are coming on-line has the potential to eliminate phishing in the future.

To actualize this, we have developed a curriculum for high-school teachers to on-board students in the use of hardware security tokens [1]. The curriculum starts by describing the high costs of phishing and of easily-guessed passwords to motivate students to consider alternative ways including two-factor authentication. From this point, students examine the security, usability, and cost-effectiveness of different

approaches for performing two-factor authentication, before being given a Yubikey and learning how it addresses many of the weaknesses in how authentication is currently being performed. A guided walkthrough for setting up and using a Yubikey is then done to train students on their use.

After undergoing training with this curriculum, teachers are given a classroom supply of Yubikeys so that they can offer it to their students. This poster describes our current results in measuring the impact that our program has on students including 1) their long-term security habits on-line, 2) their ability to avoid account compromise, 3) their ability to bring awareness of the problem to others as a result of owning a Yubikey, and 4) their interest in pursuing computer science and security as a career. Initial deployment at a public school in Olympia, Washington has shown promise in improving students' awareness of password security issues, account compromise, and phishing and has demonstrated that Yubikeys can be readily deployed into high schools. We plan follow-up surveys and a longitudinal study to assess the impact that our curriculum and program has on students.

2 ACKNOWLEDGMENTS

This material is supported NSF under Grant No. 1821841 and NSA under Award No. H98230-19-1-0027. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the National Science Foundation or the National Security Agency.

REFERENCES

- [1] CyberPDX. [n.d.]. CyberPDX Yubikey Curriculum and Program. <https://bit.ly/pdx-yubi>.
- [2] FIDO2 Alliance. [n.d.]. FIDO2. <https://fidoalliance.org>.
- [3] Google Security Blog. 2019. How Effective is Basic Account Hygiene at Preventing Hijacking. <https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html>.
- [4] B. Krebs. 2018. Security Keys Neutralized Employee Phishing. <https://krebsonsecurity.com>.

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).
SIGCSE '20, March 11–14, 2020, Portland, OR, USA
© 2020 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-6793-6/20/03.
<https://doi.org/10.1145/3328778.3372665>