Introducing Security using Authentication and YubiKeys

**Lesson Description:** Poor authentication processes using usernames and passwords has led to phishing attacks and account compromises that have cost hundreds of millions of dollars in damage. In this lesson, students will learn the scope of the problem and ways for addressing it. In particular, they will learn about passphrases, password managers, and hardware security tokens (e.g. Yubikeys) and be able to apply them on their own on-line accounts in order to secure them against attacks.

**Prerequisite Knowledge:** None. A sub-module within the curriculum that describes the underlying cryptography that makes Yubikeys work is optional. Students would need the associated cryptography curriculum if those slides are covered.

**Length of Completion**: For the entire curriculum, 2-2.5 hours. Some of the hands-on labs can be removed for a shorter lesson.

**Level of Instruction:** Intended for students who are just beginning to create on-line accounts of their own. Typically, older than 13 years of age based on most terms of service for most social media sites. Appropriate for anyone who does not know about or actively use 2-factor authentication for on-line account access (e.g. the vast majority of students).

**Applicable First Principles &/or Concepts:** Lesson plan covers and applies all 6 GenCyber Cybersecurity Concepts:

Defense in Depth Availability

Confidentiality Think Like an Adversary

Integrity Keep it Simple

**Resources that are Needed:** Slides from https://crypto.cyberpdx.org, a web browser that users can install extensions in (if one does the LastPass activity), and a Yubikey per student (if one does the Yubikey activity).

**Accommodations Needed:** Sites used should be accessible already. Video shown is close-captioned. Some images in slide presentation must be described for the blind by the teacher presenting the lesson.

# learning outcomes

LEsson learning oUTCOMES

* Describe problems with passwords that people are using for their on-line accounts
* Identify phishing attacks sent via e-mail
* Explain different methods for authenticating users over the Internet
* Use a hardware security token (e.g. a Yubikey) to protect their on-line accounts from attack

# Lesson Details

**Interconnection:** The lesson optionally interconnects with a 3-part cryptography curriculum, but can also be offered as a standalone lesson that omits the cryptography content.

**Assessment:** A demonstration that a student has both setup and can use a password manager. A demonstration that a student has both set up and can use a hardware security token to login to an on-line account from a new laptop or desktop computer.

**Extension Activities:** None

**Differentiated Learning Opportunities:** It is expected that all students are able to complete all exercises in this curriculum. Advanced students are encouraged to help less advanced students set up their accounts and browsers.

# lesson

**Lesson 1 Details:** For lesson 1, please describe:

**Warm Up:** Real-life examples of attacks are given at the beginning of the module. Students are asked to identify what they all have in common. Students also collaborate in groups to brainstorm common passwords and password strategies they think are being used by people for their on-line accounts in order to demonstrate to them the problem of using such passwords for protection.

**Lesson:** The lesson is part expository and part inquiry. The lesson presentation has exercises in which students try to derive subsequent material that follows in order to practice adversarial thinking. Specifically, the outline of the path they take is:

* Instructor describes a collection of news headlines detailing security breaches
* Students are asked what they have in common
* Instructor reveals they all use phishing (an attack on the integrity of authentication). Instructor explains what phishing is.
* Students do a lab to test their ability to identify phishing attempts
* Instructor describes how phishing is made possible by using passwords for authentication that are easy to guess
* Students are asked to come up with common passwords being used today and what strategies they might use to guess someone else’s password.
* Instructor reveals how accurate the student’s guesses are
* Students are asked if they might know a password mechanism that users can easily remember, yet are still resistant to attacks
* Instructor reveals passphrases
* Instructor describes the rampant re-use of passwords and how password managers can help
* Students set up and learn to use a password manager such as LastPass
* Instructor reveals how many compromised credentials are publicly available
* Students are asked to see if their accounts show up in a data breach using an on-line site
* Students are then asked what ways one can be authenticated other than a password
* Instructor reveals all of the types of ways to perform 2-factor authentication and the issues they have
* Instructor then describes Yubikeys and their use (via analogy)
* Optional module on the cryptography behind Yubikeys can be given
* Instructor describes why Yubikeys are so effective and the statistics that show it, along with its use in a popular program to protect highly targeted professionals
* Students set up and use a Yubikey in conjunction with a Google account