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. 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. most 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://bit.ly/pdx-yubi, 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 can 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 to demonstrate to them the problem of using such passwords for protection.

**Lesson:** The lesson alternates exposition and inquiry following a logical progression in which students continually practice adversarial thinking. The exercises include student prompts and labs for engagement.

* Instructor describes a collection of news headlines detailing security breaches
  + Prompt: What do they have in common?
* Instructor explains phishing (attack the integrity of authentication)
  + Lab: Identify phishing attempts (Google/Jigsaw site)
  + Instructor goes through attempts explaining them
* Instructor shows how phishing is a result of password authentication
  + Prompt: Guess top 25 passwords being used today
* Instructor reveals how many were guessed
  + Prompt: What strategies can you use to guess passwords?
* Instructor reveals common strategies
  + Prompt: Devise a mechanism that is better
* Instructor shows xkcd cartoon on passphrases
  + Lab: Test password/passphrase strength using an on-line site
* Instructor describes the prevalence of password re-use
  + Prompt: What would an adversary do knowing this?
* Instructor describes password spraying, stuffing, and harvesting
* Instructor gives statistics on the number of compromised passwords
  + Lab: Find if your account has been part of a compromise.
  + Lab: Find how many times a password you no longer use has shown up in compromises
  + Lab: Find the top 3 passwords that show up in compromises
* Instructor describes how password managers can help
  + Lab: Set up and learn to use a password manager (LastPass)
  + Prompt: Think of ways to authenticate without a password
* Instructor describes 2-factor authentication and the issues they have
* Instructor then describes Yubikeys and their use (via analogy)
  + Optional module on cryptography behind Yubikeys can be given
* Instructor describes why Yubikeys are so effective and the statistics that show it
  + Lab: Set up and use a Yubikey on a Google account
  + Lab: Simulate account recovery in case Yubikey is lost