Intro to Cybersecurity

Foundations and Threats

1.1.2 Authentication

How do authentication and strong passwords help secure data?

Overview

The student will be able to:

- Identify primary methods of authentication
- Apply best practices for creating a safe password

Grade Level(s)

6, 7, 8, 9, 10, 11, 12

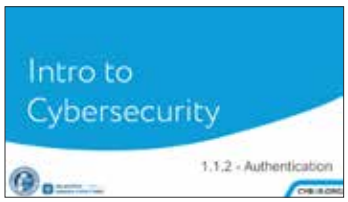
Cyber Connections

- CIA Triad
- Data Security

This content is based upon work supported by the US Department of Homeland Security's Cybersecurity & Infrastructure Security Agency under the Cybersecurity Education Training and Assistance Program (CETAP).

GALANTECH with GARDEN STATE CYBER
CYBER.ORG

Teacher Notes:



Authentication

Slide 1 - Intro Slide

Slide 2 – AAA Tools used to acheive CIA

CIA defines the goals of cybersecurity. To achieve those goals our primary tools are AAA. You can put these steps into context by using an exclusive party as an example.

1. *Authentication* – methods of proving that you are who you say you are. For the exclusive party, this would be showing the screener your ID to prove you are John Smith.

2. *Access Control* – okay, just because you are John Smith doesn't mean you get into the party. The screener now has to check to see if you are on the invited list – i.e. are you allowed access?

   Be careful – one of the synonyms, "Authorization" is often confused with "Authentication". In fact, they are completely different security steps. The most understood term for Access Control is permission.

3. *Accounting* – this isn't the financial type of accounting. This is the keeping track kind of accounting. If we want to know which of the invitees has already arrived at the party, we can review the list to see if their name is checked off. In computing we use log files to keep a record of what has happened on the system.

Slide 3 – Authentication

We will start our in-depth learning with the Authentication tool. Here's a cute cartoon to get us started on thinking about the simplest type of authentication – the password.

Slide 4 – Authentication

Most people don't realize that Authentication is about trust. In fact, we are developing authentication "fatigue" because our digital systems are constantly challenging us for passwords and PINs. But as we mentioned before, I can't let you touch the valuable data until I know exactly who you are.

Teacher Notes:

FIRST ask students for some ideas about this question. Can be online OR offline. They will likely come up with answers like driver's license, passport, fingerprints, school id swipe card – and of course passwords.

THEN Click to start the formal answer of 3 ways that we authenticate

- Click - Something you know – password or pin
- Click - Something you have – school ID swipe card or see if anyone has thought of the digital version of this = the code from Google 2-factor authentication
- Click - Something you are – did anyone come up with something besides fingerprint? We will look at other forms when we discuss biometrics.

Slide 5 – Passwords

Something you know is the form of authentication that we rely on most, usually as a password – which is defined here as "a combination of characters and numbers". The video clip is from Spaceballs and it's just a quick take on the silliness of some passwords.

Video is 1:04 min. Embedded from Vimeo: https://vimeo.com/521239024

Slide 6 – Password attacks

In attacking "what you know" the first method will be to try to steal your password – that's the easiest way to get it!

The next method is through trial and error – the hacker keeps guessing until it works or until the hacker gives up.

- A Brute force attack doesn't try to make any sense of your password, it just tries every combination of characters. If your 3-letter password uses only the 26 lower case letters, then there are just 17,756 possible combinations and that will take a computer about 3 seconds to try all of those. Here is a fun website to calculate the total combinations based on whether you use lowercase, uppercase, numbers and characters. I suggest showing this on the screen to give the students perspective on how changing your password length can make a big difference in resisting a brute force attack. https://cyber.org/find-curricula/test-strength-your-passwords

Slide 7 – Brute Force

Let's look at how password length makes a difference in hacking a password. If the attacker is going to try guessing a password, either by hand or by using cracking software, then here is how long that brute force guessing attack will take.

Teacher Notes:

Notice the major difference between using only lower-case letters for the password versus using all the characters on the keyboard. With only lower case it takes all the way up to 11 characters to slow the hacker down to a day. With all the keyboard characters it takes only 8 characters (8 hours). AND it would take a brute force 400 YEARS to crack an 11-character password using all keyboard characters.

So this illustrates an important part of security. You want to make yourself more trouble than it's worth to attack. Hackers will only put days or even years into hacking a password IF there is a lot of guaranteed payoff at the end. So if you have the formula for making gold out of dirt, they will hack you for years. But otherwise they will give up after a few hours and go try someone easier. Make yourself too much trouble to hack!

Slide 8 – What Hackers Know About Passwords

We know that length and complexity will strengthen a password. It should have a mix of lower case and upper-case characters, numbers and symbols and should be at least 8 characters. The slide shows how even when people follow these guidelines they are still very predictable! Talk through each one of these points

1. 50% of all passwords have at least one VOWEL
2. Capital letters are usually at the BEGINNING and then are followed by a vowel
3. Numbers used are usually 1 OR 2 and they are usually placed at the end.
4. Family often use PERSONAL NAMES for passwords frequently - kids, partners and, pets.
5. People use their HOBBIES for passwords frequently - team names especially!
6. These are the SYMBOLS used most often - ~ ! @ # $ % & ? Point out that here are other symbols NOT used very often: ^ * ( ) + | { } =

So, if a malicious actor starts with these basics - but users make it even easier for them!

Teacher Notes:

Slide 9 – Activity: Testing Password Strength

This is a fun activity but WARN the students not to ever use their real password on one of these testing sites. While we believe this one is run by a reputable firm, you don't really know who is behind a website and they could be collecting real passwords to be used for future hack attempts.

This activity is more fun if the students can come up to the instructor's computer to put in their password so that the results can be displayed on the projector screen.