ADVERSARIAL TELEPHONE GAME

Lesson Description: During this lesson we describe the CIA triad. The students conduct a telephone game that takes into account all three principles.

Prerequisite Knowledge: Knowledge of Cyber hand principles.

Length of Completion: 50 minutes

Level of Instruction: This activity is intended for middle and high school students at all levels of expertise.

Applicable First Principles &/or Concepts:

- Confidentiality
- Integrity
- Availability

GenCyber Cybersecurity Concepts

Defense in Depth	**Availability**
Confidentiality	Think Like an Adversary
Integrity	Keep it Simple

Resources that are Needed:

- White board
- Participants

Accommodations Needed: N/A
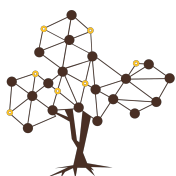
- Students will be able to explain the three CIA principles.
- Students will be able to identify each principle when using it in the telephone game.
- Students will be able to describe how a principle has come into play.
- Students will be able to contrast each principle from each-other.

LESSON DETAILS

Interconnection: This lesson prepares students to think about the CIA principles when working on the Beacon lab.

Assessment: Formative assessment - Instructors ask students to explain what they have learned about CIA during this lesson. In addition, students make a 2 minute video at the end of the day summarizing what they have learned during the day.

Extension Activities:

Example of CIA video for students to discuss:
https://www.youtube.com/watch?v=B5-JKK3ItUs

Differentiated Learning Opportunities:

Advanced students are asked to connect the CIA triad to real life situations. They can create a list of real life situations where these principles apply, applications that have tried to mitigate the issues that these principles bring, how they feel that these principles affect their everyday life, and the limitations that these principles may have.
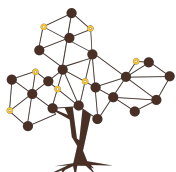
Warm Up: Play a normal game of Telephone - make sure learners operate using the same rule set:

- Stand/Sit in a circle - goal is to transmit a message to every player
- The word or phrase can only be whispered once, so players must pay close attention.
- The word or phrase should never be too familiar; you want to make sure it changes as it is whispered.
- Only one player – the first – should know what the word or phrase is. The facilitator of the game may wish to have the original phrase or word written down.

Lesson:

Throughout this lesson, the lead instructor acts as a facilitator while another instructor (near-peer) or planted student/learner acts as an adversary. Learners engage in multiple rounds of the common "telephone game." Prior to the start of each round another constraint or a proposed additional rule is included. Constraints are typically added by the lead instructor while additional rules are added (after consensus) by the learners in order to mitigate issues within the game.

Round 1:

Students play a traditional game of telephone with no extra constraints applied. The games rules stipulate that a message may only be communicated once from any one sender to a receiver. Issues that may arise include poor transmission of the message (**loss of integrity**).

Learners should 1) identify that message corruption is a loss of integrity, 2) a discussion should occur on how they can solve this problem. [A potential solution is receivers can now repeat the message to the sender, who can then confirm or repeat the message;]
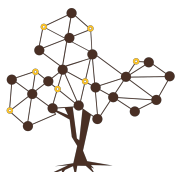
Round 2:

Learners should implement their new version and compare the results.

The lead instructor should prompt "did this new version come at a cost?" or some similar guiding question "what are the pros/cons to this new version." The learners should play again - this time however the planted adversary (who has been playing in the prior rounds) will intentionally change the message.

Learners should 1) identify that message corruption is a loss of confidentiality (an adversary made it into the secure communication channel), 2) a discussion should occur on how they can solve this problem. [A potential solution is all participants must be on an approved list]

Round 3:

Learners should implement their new version and compare the results.

The lead instructor should prompt "did this new version come at a cost?" or some similar guiding question "what are the pros/cons to this new version." The learners should play again - this time however the planted adversary (who has been playing in the prior rounds, and while now has made their way back in- with approval) will intentionally not share any message they receive.

Learners should 1) identify that message corruption is a loss of availability (again an adversary made it into the secure communication channel), 2) a discussion should occur on how they can solve this problem. [A potential solution is all participants must be on an approved list(repeat), the sender can also seek out a new receiver should they get a message from the other side of the "telephone line" that a message never got to them.]

Based on time - continue the activity - adding more constraints and rules to try to secure the message transmission as efficiently as possible.
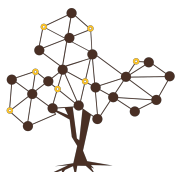
After the game - show the video (https://www.youtube.com/watch?v=B5-JKK3ItUs) - reference that this two minute video should be what they strive for in the creation of their flipgrid videos (clearly not that level of production, but that the video communicates a concept in a clear and effective manner for many to understand).