SECURE NETWORKING LESSON

Mark Emry – McNeil High School, Round Rock ISD, Austin, TX

This material is based upon work supported by
the **National Science Foundation** under Grant No.1548315.

Additional materials may be found at www.ncyte.net

SECURE NETWORKING

This module has two main themes: 1) introducing students to basic network functions, specifically regarding the Internet, and 2)the ethical concerns that come with storing & transmitting data within and amongst networks. Students will complete the "Muddy City" exercise and design a network of their own. Next, students will complete an OSI model lesson in which they identify the model's Internet layers. Participants will then research various network attacks, including man-in-the-middle attacks such as network sniffing and DNS Spoofing or Poisoning. As an option, students will play an online simulation in which they play the part of a spy seeking to gather information. Additionally, ethical issues and legal matters are discussed and researched. Students will research consequences for unethical behavior within the cyber, or online, realm.

OVERVIEW

Prerequisite Knowledge: Although not required, it is suggested that students complete CCL 1: Personal Data Vulnerabilities.

Length of Completion: This Cybersecurity Concept Lesson will take approximately 200-250 minutes to complete. Research could be done as homework. Other activities could be removed to complete the CCL in a shorter time period.

Learning Setting: This CCL is intended to be taught in a classroom with access to computers connected to the Internet.

Lab Environment: Any configuration of lab or classroom will be appropriate. Students will work together to complete the first activity and will need to be seated in an adjacent manner. The "Muddy City" activity works well using small candies to represent pavers.

Activity/Lab Tasks: The first activity, *Muddy City*, engages students in an inquiry-based lesson to introduce real-world networking problems and solutions. Students are given a scenario and will try to find the path between houses with the fewest pavers needed. Following the activity, a thorough discussion of types of networks around them takes place. The final activity for the first lesson involves students creating their own *Muddy City* involving a fixed number of destinations (houses).

This material is based upon work supported by the **National Science Foundation** under Grant No.1548315.

The second activity uses the OSI Model activities and a PowerPoint presentation which covers the OSI model of the Internet. Students will complete an activity which models the layers of the Internet through a planning activity of moving across the country. The OSI Model PowerPoint presentation and graphic organizer synthesizes the activity.

Upon completion of the graphic organizer, students research the types of network attacks. This rapid-fire activity leads to students choosing one of the types of attacks and researching it in more detail.

One requirement of the research is to recognize the ethical implications of the attack. Students should identify consequences (penalties, both monetary and criminal) of performing such an attack. Students should identify actual occurrences of the attack and the penalties suffered by the perpetrator. Students will then synthesize their research into a presentation (i.e. PowToon, Google Slides, video).

The final activity before the assessment is a “$100,000 Pyramid” game.

- 01.SecureNetworking_Overview.docx
- 02.SecureNetworking_Presentation.pptx
- 03.SecureNetworking_OSIModel_Activity.docx
- 04.SecureNetworking_OSIModel_ActivityManipulatives.pdf
- 05.SecureNetworking_OSIModel_LessonPlan.docx
- 06.SecureNetworking_OSIModel_Organizer.pdf
- unplugged-09-minimal_spanning_trees.pdf

Assessment: The Pyramid Game Review can be used as an assessment as well as a review for a multiple-choice question quiz. The presentation is a summative assessment of the student’s grasp of this CCL’s content.

LEARNING OBJECTIVES AND AP CSP ALIGNMENT

Lesson Learning Objectives

Students will:

1. Identify the OSI Network layers and their functions.
2. Research and recognize common network attacks.
3. Explain one of the network attacks and analyze the ethical considerations and consequences dealt to attackers.

ASSOCIATED AP CSP SUB LEARNING OBJECTIVES

This material is based upon work supported by the **National Science Foundation** under Grant No.1548315.

AP COMPUTER SCIENCE PRINCIPLES COURSE, BIG IDEA 3: ALGORITHMS AND PROGRAMMING

- LO AAP-4.AFor determining the efficiency of an algorithm:
    - (a) Explain the difference between algorithms that run in reasonable time and those that do not.
    - (b) Identify situations where a heuristic solution may be more appropriate.
    - AAP-4.A.2: A decision problem is a problem with a yes-no answer. An optimization problem is a problem with the goal of finding the "best" solution among many. For example, is there a path from A to B? What is the shortest path from A to B?

AP COMPUTER SCIENCE PRINCIPLES COURSE, BIG IDEA 4: COMPUTING SYSTEMS AND NETWORKS

- LO CSN-1.A Explain how computing devices work together in a network.
    - CSN-1.A.3: A computer network is a group of interconnected computing devices capable of sending or receiving data.
    - CSN-1.A.4: A computer network is a type of a computing system.
    - CSN-1.A.5: A path between two computing devices on a computer network (a sender or a receiver) is a sequence of directly-connected computing devices
    - CSN-1.A.6: Routing is the process of finding a path from sender to receiver.
- LO CSN-1.E For fault-tolerant systems, like the Internet:
        - Describe the benefits of fault tolerance.
        - Explain how a given system is fault-tolerant.
        - Identify vulnerabilities to failure in a system.
    - CSN-1.E.3: One way redundancy is accomplished in networks is by having more than one path between two devices.

AP COMPUTER SCIENCE PRINCIPLES COURSE, BIG IDEA 5: IMPACT OF COMPUTING

- LO IOC-1.F Explain how the use of computing could raise legal and ethical concerns.
    - IOC-1.F.8: Using computing to harm individuals or groups of people raise legal and ethical concerns.
    - IOC-1.F.11: Computing innovations can raise legal and ethical concerns.

This material is based upon work supported by the **National Science Foundation** under Grant No.1548315.

- LO IOC-2.A Describe the risks to privacy from collecting and storing personal data on a computer system
  - IOC-2.A.1 Personally identifiable information (PII) is information about an individual that identifies, links, relates, or describes them. Examples of PII include: social security number, age, race, phone number(s), medical information, financial information, biometric data.
  - IOC-2.A.2 Search engines can record and maintain a history of searches made by users.
  - IOC-2.A.3 Websites can record and maintain a history of individuals who have viewed their pages.
  - IOC-2.A.4 Devices, websites, and networks can collect information about a user’s location.
  - IOC-2.A.5 Technology enables the collection, use, and exploitation of information about, by, and for individuals, groups, and institutions.
  - IOC-2.A.7: Disparate personal data, such as geolocation, cookies, and browsing history, can be aggregated to create knowledge about an individual.
  - IOC-2.A.11: Information placed online can be used in ways that were not intended and in ways that may have a harmful impact. For example, an email message may be forwarded, tweets can be retweeted, social media posts can be viewed by potential employers.
  - IOC-2.A.12: PII can be used to stalk or steal the identity of a person or to aid in the planning of other criminal acts.
  - IOC-2.A.13: It is difficult to delete information once it has been placed online.
  - IOC-2.A.14: Applications can collect your location and record where you have been, how you got there, and how long you have been at a given location.
- LO IOC-2.C Explain how unauthorized access to computing resources is gained
  - IOC-2.C.1 Phishing is a technique that attempts to trick a user into providing personal information. That personal information can then be used to access sensitive online resources, such as bank accounts and emails.
  - IOC-2.C.3:Data sent over public networks can be intercepted, analyzed and modified. One way that this can happen is through a rogue access point.

This material is based upon work supported by the **National Science Foundation** under Grant No.1548315.

LESSON DETAILS

LESSON 1

Upon completion of this lesson:

- Students will devise steps to solve a minimal spanning tree.
- Students will create their own spanning tree and describe the solution.
- Students will understand that the internet is a network of networks.

Cyber Ethics Activity: Direct students to read, "Equifax data breach FAQ: What happened, who was affected, what was the impact?" Discuss cyber ethics, and who is involved and responsible when a breach occurs. The discussion questions (slide 3) can be done as a whole group, small group, think/pair/share, or journaling activity.

Warm Up: Direct students to write two sets of directions from their home to school. Students should identify which way is usually a quicker journey. Students should then identify obstacles that may influence the speed of the commute. A brief (5 minutes maximum) group discussion leading to the creation of roads/networks should follow. Questions could include: Is the fastest path always the best? Why or why not? What things influence your decision to get to school one way or another?

Lesson:
unplugged-09-minimal_spanning_trees.pdf

Follow the directions in the *Muddy City* activity from csunplugged.org. Each student should get a copy of the activity on page 78. Additionally, students should be given candy/cardboard/paper to use as pavers.

You should do the activity ahead of your students - the best way to picture how this activity works is that you try it!

Students should be given approximately ten minutes to find the path using the fewest pavers. Students should then discuss their path with an elbow partner. The instructor distributes pages 79 and 80 to students and discuss the topics of networks, including computer networks. Explain that this minimal spanning tree activity is an introduction to a network of networks we call the Internet.

Students create their own minimal spanning activity using the lines and nodes, like the model on page 79. Students identify which path is most efficient. As an exit ticket, students identify 3 networks (i.e. telephone networks, utility supply networks, computer networks, and road networks) in existence today.

Active Learning Activity: This inquiry-based lesson involves students identifying an optimal route of data in a network. Students are actively searching for the

This material is based upon work supported by the **National Science Foundation** under Grant No.1548315.

fewest number of pavers to be used and then discussing with a partner the routes they have chosen.

Students are also active when creating their own network model.

LESSON 2

Warm Up: Students will share their own minimal spanning trees with a partner and try to complete their partner's tree. Students discuss the process they used for creating their tree. (5 minutes)

Lesson: Explain to students that the Internet is a network of networks and communication between those networks needed to be standardized for communication to occur. Remind students that their fastest route to the school wasn't always the best (ex. If they had to pick up a friend, traffic jams). The OSI model explains the standardization and how data is transmitted on the Internet.

Begin the OSI Model lesson:

- 02.SecureNetworking_Presentation.pptx
- 03.SecureNetworking_OSIModel_Activity.docx
- 04.SecureNetworking_OSIModel_ActivityManipulatives.pdf
- 05.SecureNetworking_OSIModel_LessonPlan.docx
- 06.SecureNetworking_OSIModel_Organizer.pdf

The teacher should review the "OSI Model Lesson Plan" document for detailed plans and create the manipulatives previously.

1. Students should be given the "OSIModel_Activity" document and the whole group should preview the activity.

2. Teacher should follow the timeline in the "OSI Model Lesson Plan" document. Follow the lesson as presented in the document.

3. As the class finishes the "OSI Model_Activity", they should be given a copy of the "OSI Model Organizer" to use during the presentation. Explain the heading and the top titles as the presentation is given.

4. OSI Model PowerPoint will then be presented and students complete their organizer during and after the presentation. Whole group discussion should occur with each slide.

5. At the conclusion of the slide presentation, students should discuss the graphic organizer with a partner, and then with a group of 4 or 5. Did they

This material is based upon work supported by the **National Science Foundation** under Grant No.1548315.

fill in their table with the same information as their group? Why or why not? How many extra notes were taken on the worksheet?

(Optional activity. Students should be directed to the Interactive Role Playing Game)

Students play the game, noting the decisions they made for each step. At completion of the simulation, students discuss with a partner which, if any, layers from the model were attacked.

Students exit the room with a list of the seven layers and what they do.

Active Learning Activity: Students are engaged while searching their partner's tree and the discussion that follows. Students are active during the OSI Model lesson. They work together and create a plan. Students are also active during the presentation as they complete the graphic organizer. Lastly, students have an active discussion about their notes.

LESSON 3

Warm Up: Using the students' plan from the OSI Model activity & organizer, students write one potential test question they might see on a test about the OSI model. Students should then share their question with an elbow partner giving the partner a chance to answer the question.

Lesson: Ask students to write down what risks there may be to using networks to create, store and transmit data. Give students time to write and then conduct a short discussion of their ideas.

Tell students they are to "race research" the topic of network attacks. Give students sticky notes and when they find a type, they are to write it down and put the sticky note on the board. If the specific type of network is already on the board, then they run back to the computer and try again. A list of 8-10 network attacks is quickly accumulated and the teacher stops the race. The class discusses each of the attacks and any prior knowledge they have of them. As each attack is discussed, the instructor should write them on the board.

Common attacks are:

- Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks
- Man-in-the-middle (MitM) attack
- Phishing and spear phishing attacks
- Drive-by attack

- Password attack
- SQL injection attack
- Cross-site scripting (XSS) attack
- Eavesdropping attack
- Birthday attack
- Malware attack

A whole-group discussion regarding the ethical considerations of attacking networks should take place before the research continues:

- Ask students why these attacks can hurt people and organizations.
- Is it right to access data that is not yours?
- Should you do something just because you can?
- What happens to people when they commit these attacks?

After the discussion, students should be given instructions to research one of the following types of network attacks:

- How is the attack performed? What layers of the OSI Model are attacked?
- What are the ethical concerns of the attacker? What are they gaining and who can it affect?
- What are the consequences of this attack? Personal, organizations, criminal consequences

Students take the results of their research and create a presentation of their findings, i.e. infographic, PowToon, Google Slides.

Students should present their findings and artifact to the class.

The Pyramid Review Game is used as a culminating activity for either the entire CCL, or immediately after the OSI Model presentation.

Students are placed in pairs, one student describing the topic on the pyramid and the other guessing. One example is included in the CCL.

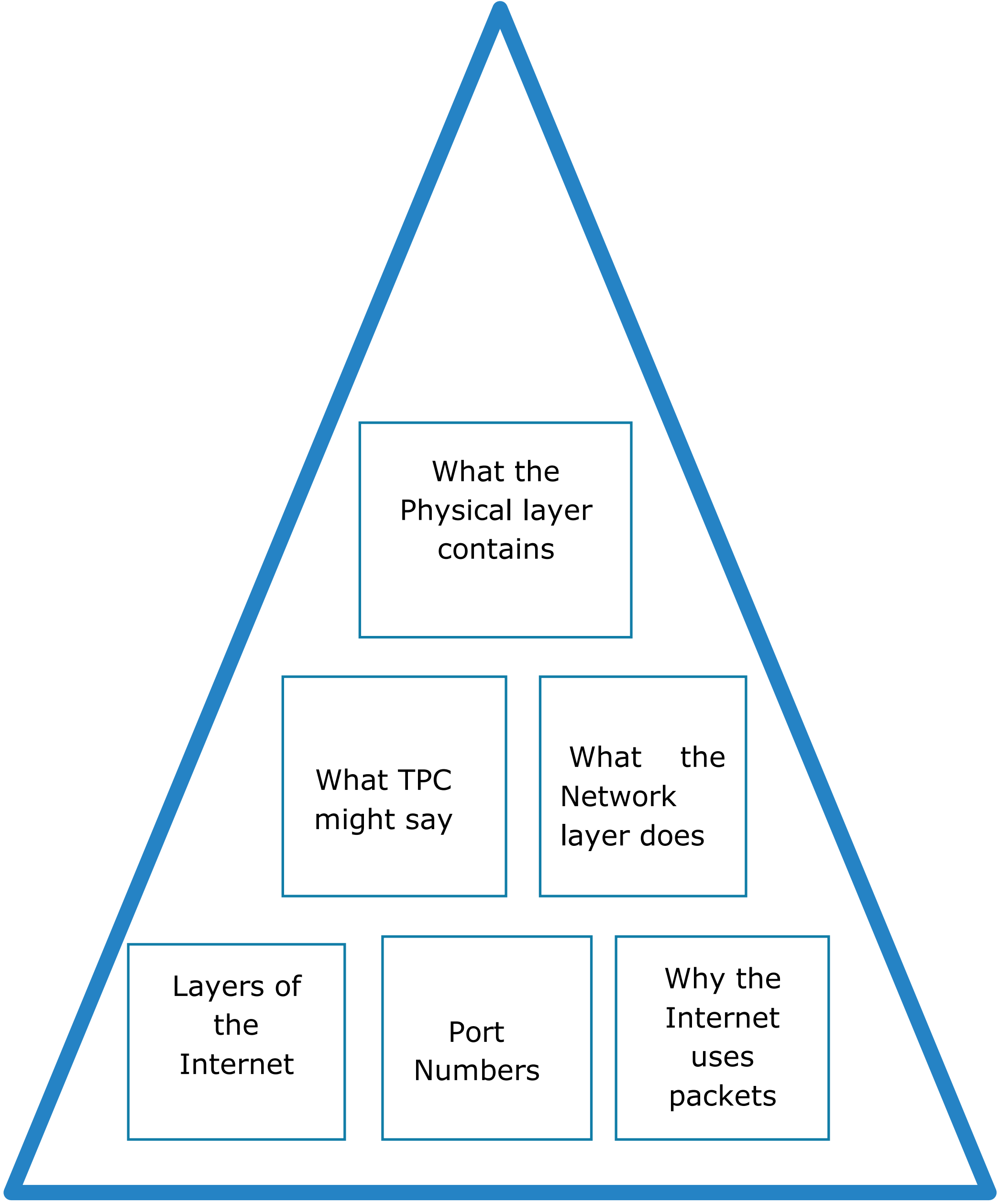
- Student pairs keep track of how many correct responses were given in 60 seconds.
- Students then trade places and another pyramid game is played. (Teachers can make another pyramid, or have students create their own.)

This material is based upon work supported by the **National Science Foundation** under Grant No.1548315.

Active Learning Activity: Students are engaged in the “research race”, using the Internet, writing on sticky notes, and racing to the board. Students are actively searching an attack topic of their own choice. Students are active while presenting their findings. The Pyramid Review Game is an active review strategy (example below).

This material is based upon work supported by the **National Science Foundation** under Grant No.1548315.

PYRAMID


What the Physical layer contains
What TPC might say
What the Network layer does
Layers of the Internet
Port Numbers
Why the Internet uses packets

This material is based upon work supported by the **National Science Foundation** under Grant No.1548315.

ACKNOWLEDGEMENTS

Resources:

CS Unplugged @ csunplugged.org for the Muddy City activity

Pacific Northwest National Library for the online simulation

SMAC Entertainment in association with Sony Pictures Television for the concept of the Pyramid Review Game.

Jacqueline Corricelli, Conard High School, West Hartford CT for the OSI Model Lesson activities and materials.

Fruhlinger J. October 14,2019 Equifax data breach FAQ: What happened, who was affected, what was the impact?