“Computer Talk”- A Middle School Cyber Security Unit

Terin Kirk, MAT Secondary Science

UNR Cyber Security Initiative for Nevada Teachers (CSINT)

University of Nevada, Reno

INTRODUCTION

This unit introduces middle school students to three crucial computer science concepts: networking, cryptography, and cyber security. This unit was created in response to 8th grade NGSS standards that require students examine encoding and decoding data (encryption) and how data is transferred through electrical systems (networks). The unit scaffolds critical cyber security concepts for the middle school population. The unit addresses basic concepts that may be expanded upon in higher education. Constraints leading to cyber security not being taught previously are as follows: nonexistent teacher knowledge, classroom time constraints, content standards taking precedence in classroom instruction, lacking materials and resources to teach cyber security lessons, limited access to technology in the classroom, no computer science/cyber security standards are required, etc. This unit involves multi-modal instruction for diverse learners and allows for student voice and choice.

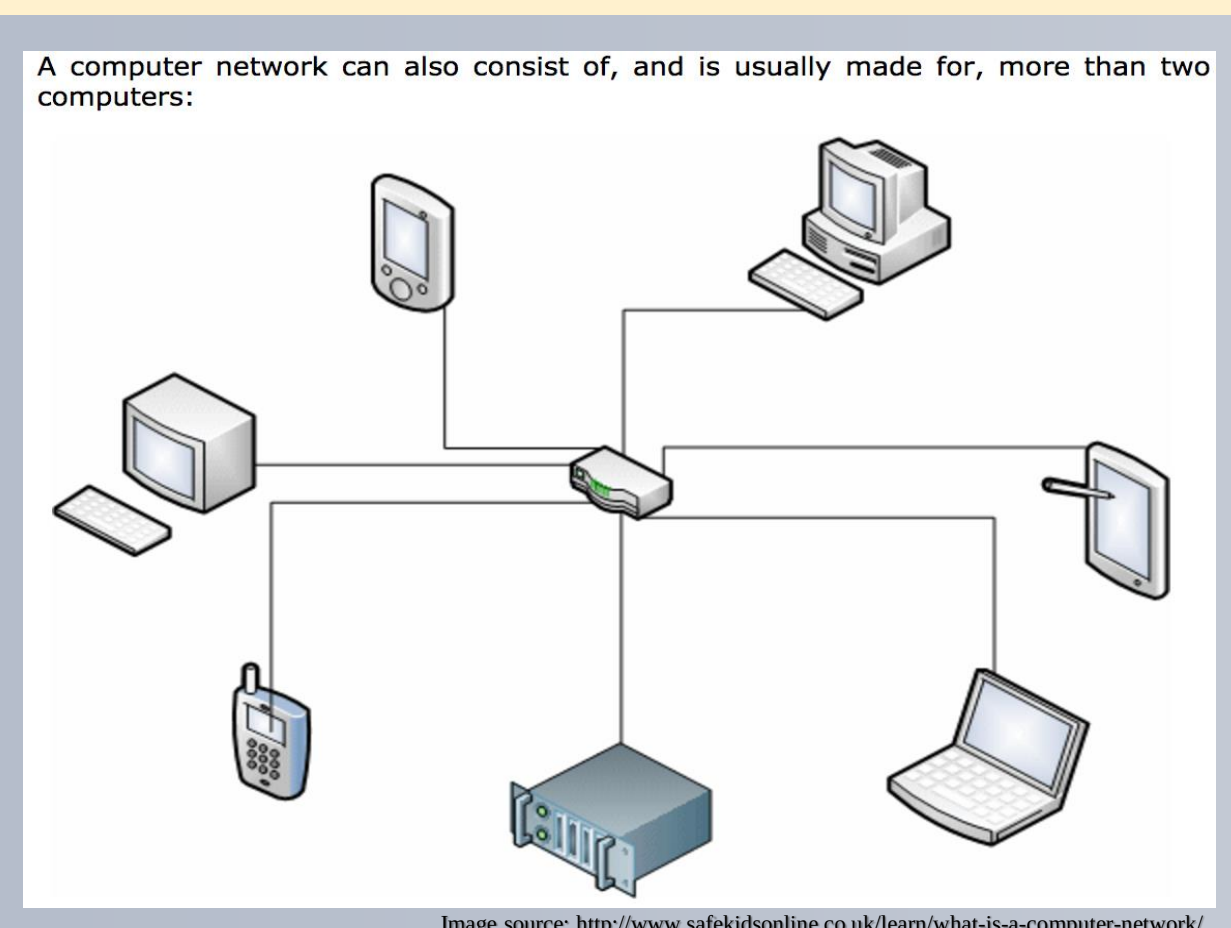

A computer network can also consist of, and is usually made for, more than two computers:

Image source: http://www.safekidsonline.co.uk/learn/what-is-a-computer-network/

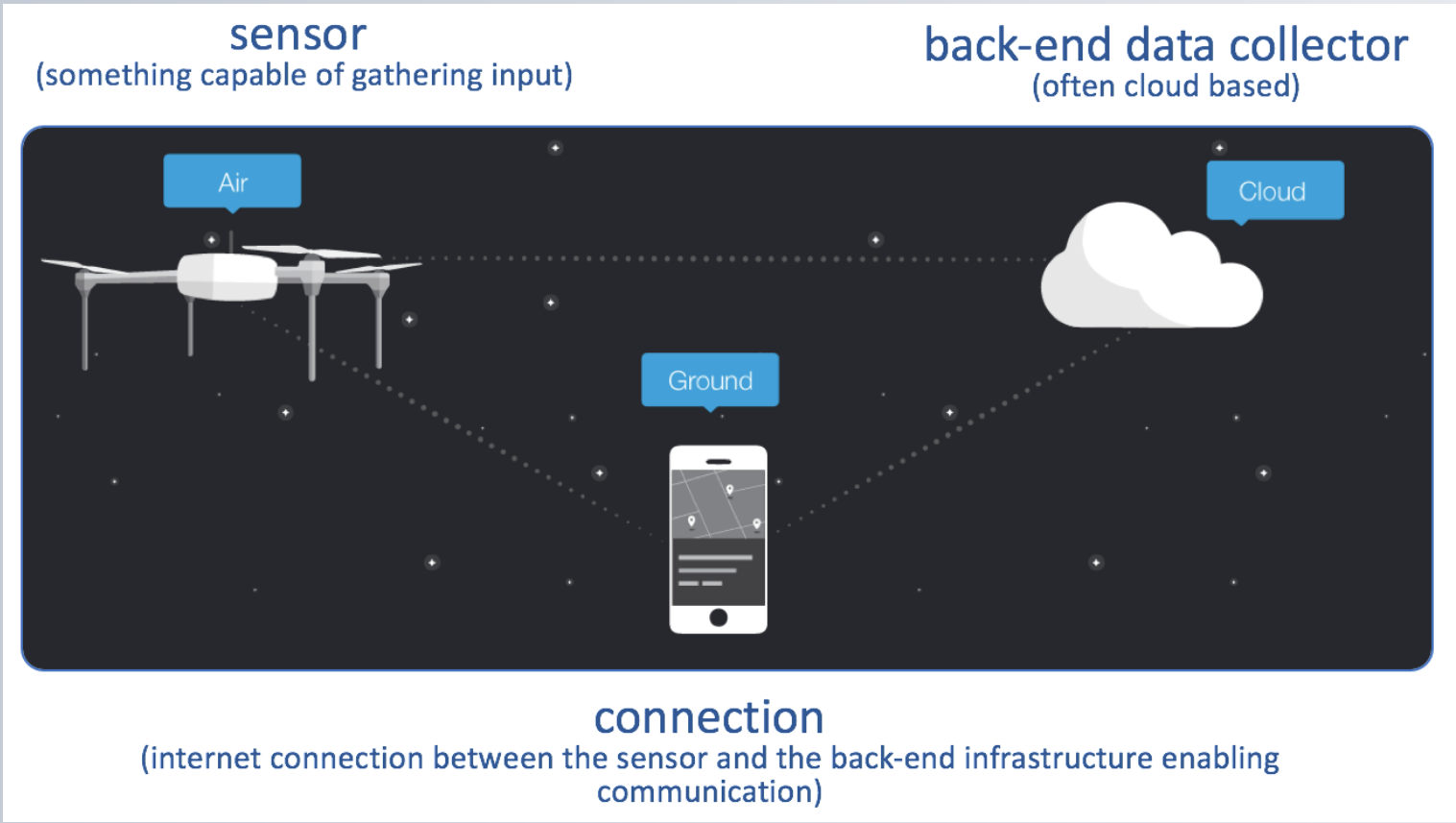

sensor
(something capable of gathering input)
back-end data collector
(often cloud based)
Air
Cloud
Ground
connection
(internet connection between the sensor and the back-end infrastructure enabling communication)

Image source: http://techgenix.com/drones-another-threat-security/

LESSON 1: NETWORKING

ENGAGE:

The teacher will present the essential question: “How do computers ‘talk’ to each other?” Students will make predictions in their notebooks. The teacher will then play the YouTube clip of Siri and Cortana ‘talking’ to one another. The teacher will ask students to share their predictions and create a list on the board.

EXPLORE:

The teacher will define network and give an example of the US Road Network. Students will fill in vocabulary on student handout. The teacher will introduce the “Is This a Network?” game. Students will give a thumbs up for each image that depicts a network and a thumbs down if it does not exemplify a network. Examples range from a cottage in the woods (no sewer, Wi-Fi, etc.) to multiple computers and devices connected (depicting a ‘computer’ network).

EXPLAIN:

The teacher will give descriptions of why each image from the “Is This a Network?” game is or is not an example of a network. The teacher will give two explicit examples of how computer networks may be connected/what devices networks consist of (or the “Internet of Things”). The teacher will ask students to yell out examples of items that are part of the Internet of Things, which make up these networks. Students will share out and fill in vocabulary on their note takers when prompted by the teacher.

EVALUATE:

The teacher will introduce the reading, “Now That’s a Long Distance Phone Call,” which explains how NASA’s Mission Control communicates with astronauts in space via a network. Students will:

1. Read the article. Highlight every thing in the article that would be a part of NASA’s Network.
2. Then, draw a picture of the astronauts in space communicating with Mission Control on Earth. Add each of NASA’s network components identified in the article. Make certain to label each item drawn and provide a brief description of its function.
3. Write a 5-sentence summary answering the following questions:
   - “What kind of data may be sent through this network?”
   - “How is data sent through this network?”
   - “How do astronauts in space use a network to communicate with Mission Control on Earth?”

The teacher will circulate, asking strategic questions as students work through the assignment. Students will present their final poster to three other students in 30-second-insta-summary format. The teacher will ask students to find a new partner to present to every 30 seconds.

EXTEND:

The teacher will ask students to log onto the following site to simulate the creation of a network from a local and worldwide scale: http://www.teach-ict.com/gcse_new/networks/hardware/resources/NWB_SIM.swf

UNIT PROGRESSION

Lesson	Essential Question	Objective	Activity	Timescale
Lesson 1	How do computers “talk” to one another?	Students will be able to explain that a computer network is 2 or more computers joined together.	- Is this a Network? - “Now That’s a Long Distance Phone Call” - Build a Network Simulation	120 min + 60 min Extend (Three 60-min class periods)
Lesson 2	How do we make sure that data sent through computer networks are safely received?	Students will be able to explain that data sent through computers can be encrypted and give one example of an encryption method.	- Trapped on Mars- Hexidecimal Cipher - Secret Emoji Cipher - Dumbledore’s Army- The Enchanted Galleon	120 min (Two 60-min class periods)
Lesson 3	How do UAVs communicate with computers and are these communications secure?	Students will be able to describe a UAV system and list at least 3 vulnerabilities within a UAV system.	- UAV System Vulnerabilities Game - Inform the Public! PSA	240 min (Four 60-min class periods) (Additional 60-100 minutes for final presentations)

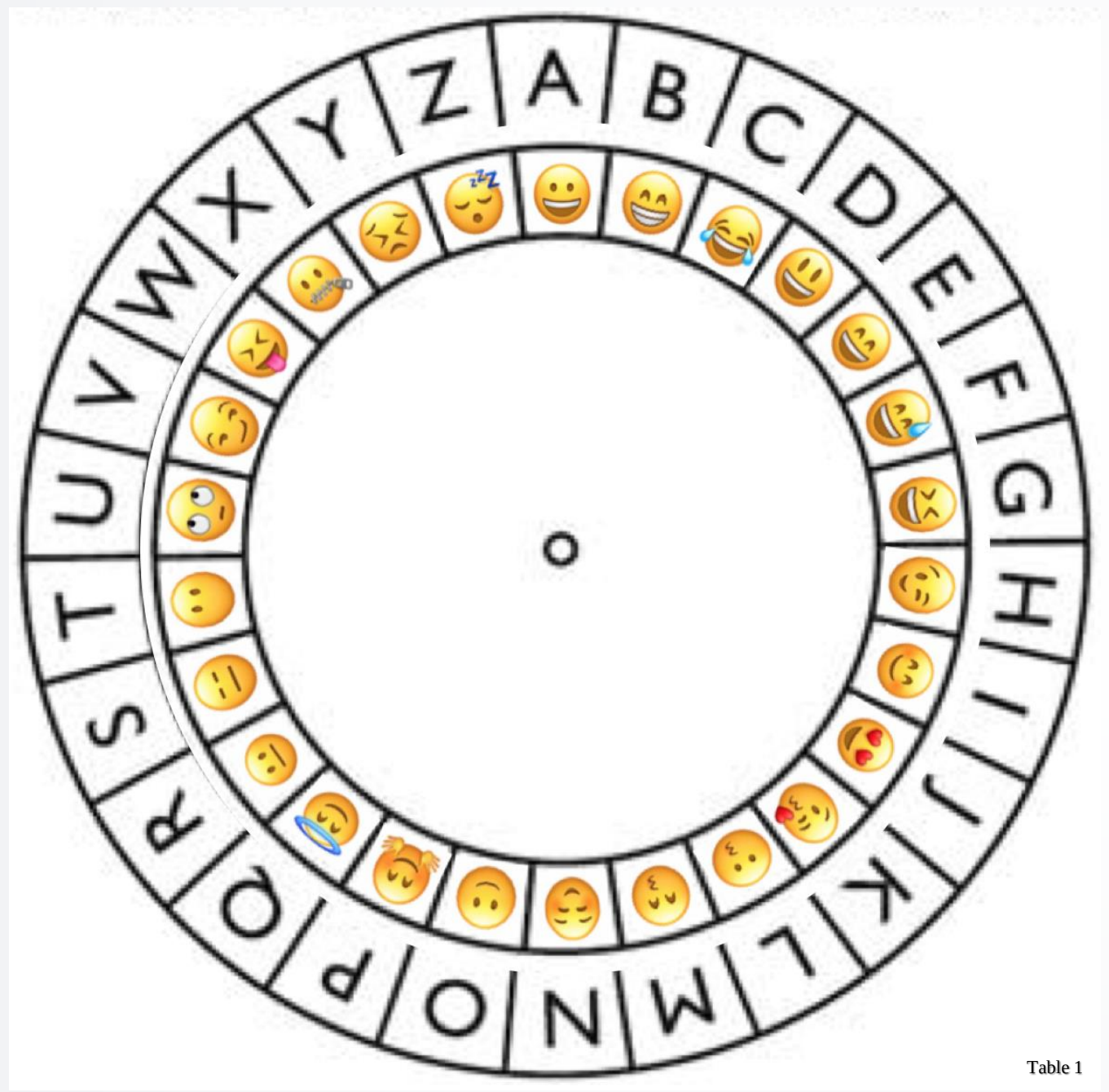


Table 1

Image source: http://makezine.com/projects/build-wi-fi-drone-disabler-with-raspberry-pi/

LESSON 2: CRYPTOGRAPHY

ENGAGE:

The teacher will pose the question, “What if you were trapped on Mars and all you had to communicate with Earth was a swiveling camera?” The teacher will give students three minutes to share verbal answers. The teacher will show “The Martian” clip of hexadecimal cipher.

EXPLAIN:

The teacher will revisit previous lessons takeaways to build on background knowledge. The teacher will present the essential question for lesson 2: “How do we make sure that data sent through computer networks are securely received?” The teacher will show “What is hacking?” YouTube clip. Students will brainstorm, “How can we hide data from hackers as it travels across networks?” The teacher will show the Cryptography clip, if time permits (8 min video). The teacher will introduce key terms: encryption, cipher, key, decrypt Students will answer the question, “Why use a cipher and a key?” (Without a cipher and a key, the message would be the same every time and would be easy to decipher.) The teacher will introduce the example “a key of 1” and show “Historical Use of Ciphers” clip. The teacher will explain encryption and decryption with a Caesar cipher example.

EXPLORE:

The teacher will introduce the Secret Emoji Cipher (see Table 1). Students will: cut out the circle with the emojis on it, place the emoji circle inside the alphabet circle, push a brad through the center of both circles, attaching them and follow the instructions on their handout to complete each activity. Students will encrypt or decrypt each problem and then post their results on the classroom Padlet.com message board.

EXTEND:

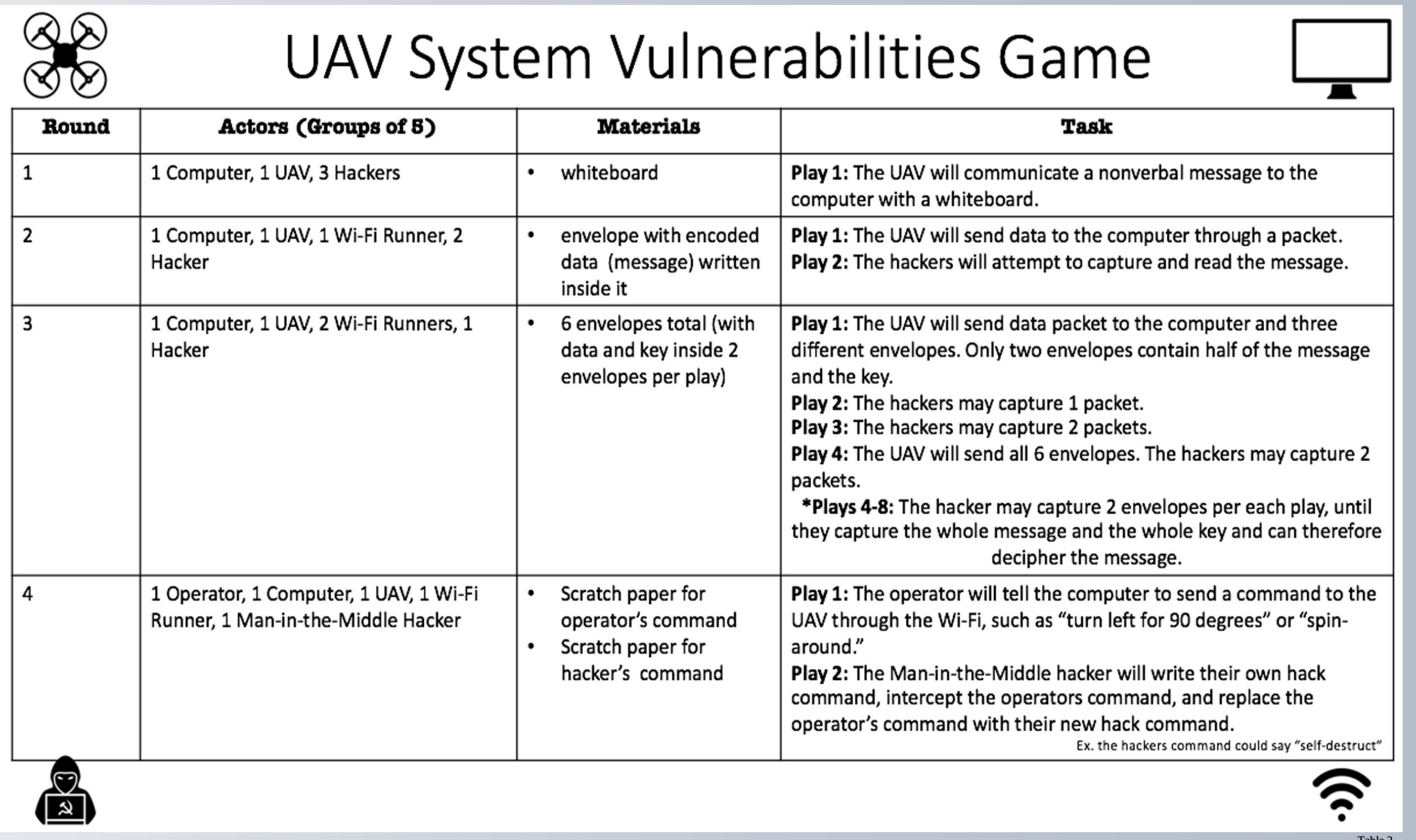
The teacher will extend this lesson with a ‘magical’ example: Dumbledore’s Army- Enchanted Galleons.

EVALUATE:

The teacher will use student responses from the secret emoji cipher to evaluate student mastery.

PURPOSE & OVERVIEW

The purpose of this unit of instruction is to provide students with a basic understanding of how computers communicate, how data is secured as it travels through a network, and how these concepts are applicable, observable, and vulnerable in a UAV system. The main parts of this lesson are as follows: (1) networking, (2) cryptography, and (3) cyber security per UAV system vulnerabilities.



UAV System Vulnerabilities Game

Round	Actors (Groups of 5)	Materials	Task
1	1 Computer, 1 UAV, 3 Hackers	• whiteboard	**Play 1:** The UAV will communicate a nonverbal message to the computer with a whiteboard.
2	1 Computer, 1 UAV, 1 Wi-Fi Runner, 2 Hacker	• envelope with encoded data (message) written inside it	**Play 1:** The UAV will send data to the computer through a packet. **Play 2:** The hackers will attempt to capture and read the message.
3	1 Computer, 1 UAV, 2 Wi-Fi Runners, 1 Hacker	• 6 envelopes total (with data and key inside 2 envelopes per play)	**Play 1:** The UAV will send data packet to the computer and three different envelopes. Only two envelopes contain half of the message and the key. **Play 2:** The hackers may capture 1 packet. **Play 3:** The hackers may capture 2 packets. **Play 4:** The UAV will send all 6 envelopes. The hackers may capture 2 packets. ***Plays 4-8:** The hacker may capture 2 envelopes per each play, until they capture the whole message and the whole key and can therefore decipher the message.
4	1 Operator, 1 Computer, 1 UAV, 1 Wi-Fi Runner, 1 Man-in-the-Middle Hacker	• Scratch paper for operator’s command • Scratch paper for hacker’s command	**Play 1:** The operator will tell the computer to send a command to the UAV through the Wi-Fi, such as “turn left for 90 degrees” or “spin-around.” **Play 2:** The Man-in-the-Middle hacker will write their own hack command, intercept the operators command, and replace the operator’s command with their new hack command. Ex. the hackers command could say “self-destruct”

Table 2

LESSON 3: UAVs & CYBER SECURITY

ENGAGE:

The teacher will review Lesson 2’s learning goal: “data sent through computers can be encrypted to keep information safe and confidential.” The teacher will present Lesson 3’s essential question: “How do UAVs communicate with computers and are these communications safe?” The teacher will show the “Packets of Music” code.org clip showing how Spotify brings students ‘lit jams’. Students will take notes on how packets ‘travel’ through a network. Students will share out with shoulder partners. Shoulder partners will share their agreed upon answer to the question with the whole class.

EXPLAIN:

The teacher will frontload vocabulary terms and differentiate between the UAV and the UAV System: UAV, sensor, connection, back-end-data collector, UAV System. (Students may have background knowledge from previously having handled classroom parrot mini drones). Students will fill in the diagram of the UAV system on their guided note taker.

EXPLORE:

Students will complete all rounds of the “UAV System Vulnerabilities Game” (see Table 2).

1. Round 1 exemplifies data transfer without encryption.
2. Round 2 exemplifies data transfer with the use of encryption.
3. Round 3 exemplifies data transfer through packet switching.
4. Round 4 exemplifies data transfer where a “Man-in-the-Middle” attack occurs.

EXTEND:

The teacher will demonstrate how a raspberry pi with a cantenna can disable a UAV that operates through Wi-Fi.

EVALUATE:

Students will:

1. Choose Round 1, Round 2, Round 3, or Round 4 of the UAV system vulnerabilities game.
2. Create a PSA that answers the following questions for the Round chosen: What data can be transferred through the UAV system? What was the vulnerability in the network for this round? What steps can the operator take to fix this vulnerability? (Research this!) Why is it important to keep this data safe and secure when it is transferred through the UAV system?
3. The PSA may be in the form of a PowerPoint, VoiceThread, video, PowToon, Prezi, Skit, FaceBook post, radio announcement, song, rap, comic strip, or poster.
4. Students will present their final projects to the class or an public audience..

This research supported by the National Science Foundation under grant #1542465 & the University of Nevada Reno Cyber Security Initiative for Nevada Teachers (CSINT).