Teacher’s Guide

Rolling Thunder:

Justin Hohl, Justin Willoughby, Ryan Coffman,
Morgan Escalera and Quinn Schaffer

Learning Objective:

The objective of this module is to educate and shed light on the Engineering Grand Challenge of Securing Cyberspace. Cyberspace is an ever expanding section of our world and the need for security rises every day. Huge amounts of information and work is done and or stored in computers and accessible via the internet. In order to make sure this work and information does not fall into the wrong hands, measures have to be put in place so that all sense of privacy can be upheld. As a result of completing this module, the students should have a firmer understanding of how cyber attacks work in the virtual world around us. They will also be exposed to the engineering method of identifying a problem, planning a solution, then testing and reflecting on it, honing their problem solving skills.

Technical Background:

The original design of the internet assumed that all users would play nice, since only an elite few would be on it. However, the internet’s rapid growth proved this assumption wrong. [12] Today, it is becoming even harder to keep up with the sheer number of attacks happening every second. The Norse Attack map shows just a glimpse of the quantity of attacks made. It only takes a single attack to completely render a security system useless. The consequences to these defenses being broken down can be drastic considering some of our most confidential information is now stored on the internet. One example of this was the Adobe security breach in October of 2013. In this breach, almost 3 million credit cards were stolen along with over 38 million users’ passwords. [10]

To defend from attacks like this again, developers and security specialists must design diverse systems to encompass the different types of security attacks, including distributed denial of service attacks, keyloggers, malware, and trojan horses. The way these developers go about this is to first limit the number of locations that are vulnerable. Since this does not cover all areas, layered protection is usually the best second step. [11] These are the two ideas we are portraying in our module.

Materials and Budget (12 teams of 2-4):

Tupperware Containers	$40 for 36
Ping Pong Balls	$3 for 6
Masking Tape	$10 for 2
Popsicle Sticks	$6 for 200
Plastic Solo Cups	$3 for 50
Candy	$10
Total	**$72**

Module Instructions:

The purpose of the introduction is to get the students to start thinking about computer security and what is happened in real time with these security attacks. The introduction has a little bit of technical things to discuss in order for students to get a basic idea of the computer attacks. This entire module leads to a game which a metaphor, it is absolutely necessary to show the connection between the game and cyber security every chance you can.

Phase 1: Introduction of the Activity

Split the students into teams of 2,3 or 4 depending on amount of students

1. Go to map.norsecrop.com (5 min)
    a. Explain to the students in a little more detail what is happening on the site.
    b. Explanation: Norse is a security company that defends many companies and uses its defenses to also track attacks. Each line is a cyber security attack with different colors representing different types. Another way they track these attack is by setting up honeypots all over so they can see where attacks are going.
    c. Explain the concept of 'honeypot' security. Honeypots are unsecured servers that a cyberattack will go to and not have any data, Norse uses them to track attacks, other companies use them like a mousetrap.
2. Pass out the Worksheet to each student
3. Turn off the map to not distract the students

Phase 2: Defense Design and Building

It is important for the instructor in this section to help the students make mental connection between what they are designing and what is required of them. It is also there so the students can begin to grasp the optimal strategies for both offense and defense within the rules of the activity

1. Read the rules from the worksheet outloud to the students and if needed give demonstrations
2. Show the building supplies to the students, so that they have an idea of what the materials look like.
3. Tell the students to begin the design of the defense. This should take no more than a few minutes
4. Instructors should walk around and get the students thinking about the right things: who do they want to defend from?Do they want the containers clustered or spread out?
5. If students finish faster than others have them answer the next parts of their worksheet
6. Once all teams have finished designing their defenses hand out the materials to each team.
7. The students must have a drawn out design before they get their materials, this teaches them about the Engineering Design process.
8. Allow the students to begin building their defense (10 – 15 min).
    - Carefully monitor that everyone is evenly contributing to the building
9. As students are building, walk around to each team and ask questions. Some suggestions may be:
    - Why do you think taller defenses are better than shorter defenses?
    - If students are running low on supplies ask them about:
        - Is this a problem?
        - What material could be moved to better defend your data?

    - o How does this affect your attacks
  - Encourage students to use the designs of the other teams to create the best possible structure
  - Later when the students are close to finishing, prompt them to evaluate their design.
    - o Did they have any pieces left over?
    - o What pieces do they think are the best for defenses?
    - o What defense strategies did they use?

10. Announce when there is one minute of building time left and prompt students to finish up.
11. When time has elapsed prepare for the attack phase.

Phase 3: Attacking

The basic idea of the attacking phase is that students stand behind their defenses and attempt to throw a ping pong ball into another team's bowl. If they make it inside the opposing bowl everyone from the team takes a piece of candy from the bowl that their ball landed in. Each teammate gets 2 attacks per round. Once all teammates have thrown their ping pong balls the instructor hands the Ping-Pong balls to the group to the left of them. The group to the left of them then become the attackers and the attack phase starts again. This continues till the Ping-Pong balls reach the starting positions and that signifies the end of the round. Any number of rounds can be played depending on time and number of groups. This part may get a little hectic for a large groups of students. Make sure to inform students to use light tosses when throwing the Ping-Pong ball. During this time make sure to ask the attackers who they are aiming at and why they chose that target.

1. Place approximately equal amounts of varied candy into each bowl.
2. While doing this, explain the how the game is to be played to the students. (The basic idea is in the paragraph above)
3. When all the candy/data is placed in each bowl designate a team to be the attackers.
4. Before handing the attackers the ball explain to the students to lightly toss the ball into bowls.
5. Have the students stand a couple steps behind their defense before making an attack.
6. Once the students are behind their defenses and understand what they are to do hand them the ping pong balls.
7. Each student on the team will get two ping pong balls to throw and will take turns throwing the ping pong ball.
8. If a student makes the ball into the bowl, then each person on their team takes a piece of candy from the bowl.
9. Once all the ping pong ball have been thrown the teacher will collect the balls and hand them to the team to the left.
10. The students will continue to throw the ping pong balls and pass them to the left until they reach the team that was the first attacker. This signifies the end of the round.
11. Multiple rounds can be played if there is time or you have a small group.
12. At the start of successive rounds, random benefits or problems can be introduced to spice the game up
    a. One example if giving one group a large amount of candy(as a data center) and say if you make it there each team member gets more candy than just one piece.
    b. Throw in the element of human error, maybe an employee lets his password out, then maybe take away a piece of a defense away from a group.
13. After all the rounds are played students will answer some questions on their worksheets.

Phase 4: Reflection

This is the time where students are to make connections about computer security and the activity. The instructor is in charge of framing questions that lead into discussion such as what does each piece represent in computer security. These questions are to help students gain a better understanding of computer security and why it's important.

14. Have the students circle up and discuss what they thought of the game. Discussion points can come from the worksheet
15. Talk about what strategies and designs seemed to work the best and what things didn't.
16. Have the students discuss what they think each piece represented.
17. Ask the students how they think the game related to computer security
    a. If one is having difficulty with this question ask how it made them feel when someone took candy from their bowl or remind them about the norsecorp map
    b. Tell them how losing candy is like losing valuable information.

References:

[1] Apple, *IPhone6*. 2016. [Online]. Available: http://images.mobilefun.com/graphics/productgalleries/41166/b.jpg.

[2] Pepperfry, *Tupperware Mini Rectangular*. 2016. [Online]. Available: http://i2.pepperfry.com/media/catalog/product/t/u/800x880/tupperware-mini-rectangular-white-container---850ml-tupperware-mini-rectangular-white-container---85-oydt4v.jpg.

[3] Walmart, *Ping Pong Balls*. 2016. [Online]. Available:

[4] Slate, *Red Solo Cup*. 2016. [Online]. Available: http://www.slate.com/content/dam/slate/articles/business/adreportcard/solocupmodern.jpg.CROP.article250-medium.jpg.

[5] Factory Direct Craft, *small wood popsicle sticks*. 2016. [Online]. Available: http://factorydirectcraft.com/pimages/20050927122837-028791/small_wood_popsicle_sticks.jpg.

[6] KBear, *Jolly Rancher*. 2016. [Online]. Available: http://www.kbear.fm/wp-content/uploads/2013/10/jolly-rancher.jpg.

[7] GRTCorp, *Balanced Defence*. 2016. [Online]. Available: http://www.grtcorp.com/sites/grtcorp.com/files/balanced_defence.jpg.

[8] Twirlit, *Lock Your Phone*. 2016. [Online]. Available:

[9] Datanami, *Fast Data Brain Tree*. 2016. [Online]. Available: http://2s7gjr373w3x22jf92z99mgm5w.wpengine.netdna-cdn.com/wp-content/uploads/2014/04/fast_data_brain_tree.png.

[10]B. Arkin, "Adobe Breach Impacted At Least 38 Million Users — Krebs on Security",*Krebsonsecurity.com*, 2016. [Online]. Available: http://krebsonsecurity.com/2013/10/adobe-breach-impacted-at-least-38-million-users/. [Accessed: 26- Jan- 2016].

[11] C. Perrin, “Understanding layered security and defense in depth”, techrepublic.com, 2016, [Online]. Available:

http://www.techrepublic.com/blog/it-security/understanding-layered-security-and-defense-in-depth/. [Accessed: 26- Jan- 2016].

[12] M. Zalewski, Silence on the Wire. San Francisco, CA: no starch press, 2005.

Appendix A: Student Handout

Name:_________________ **Team Name:_________________** **Date:____________**

Materials:
2 Index Cards
10 Popsicle Sticks
3 Red Cups
3 Bowls
1 Yard of Tape

Design Constraints:
Defenses must be build straight up
Bowls must be flat on the table
Nothing in the bowls besides candy

1. Sketch out a design for the defense you want to use (use back of sheet if needed).

2. What strategies did you use for your defense?

3. What strategies did you use for your attacks?

4. What defense strategies seemed to work the best?

5. What do you think each of these pieces represent in regards to computer security?

Appendix B: Additional Resources

The Grand Challenge of Securing Cyberspace

http://www.engineeringchallenges.org/challenges/cyberspace.aspx

Visual comparisons to help better relate our module materials to real life items/scenarios

[2]

Devices

[1]

[3]

Attacks

[7]

[4]

[5]

Defenses

[8]

[6]

Data

[9]