Team SuperStarz

Introduction:

Engineering professionals have observed that there are many current and global engineering challenges that impact much of the world. These challenges have been consolidated into fourteen Engineering Grand Challenges. These fourteen Grand Challenges include tasks such as restoring urban infrastructure, providing reliable energy from fusion, and engineering better medicines. Each of these Challenges was determined by assessing the current state of global development and then re-imagining the possibility of a better future with improved technologies. This particular demonstration will help 4th and 5th grade students better understand the Grand Challenge of securing cyberspace.

Securing cyberspace is of vital importance for corporations, governments, and essentially any individual who uses the internet. One aspect of securing cyberspace involves keeping a network secure. A network is a group of computers which share files of information. When the methods of protecting a network are compromised, many unfavorable consequences arise, such as confidential information being stolen, the invasion of privacy, and identity theft. Sony is one example of a large company that was recently the victim of a cyber attack. After hackers gained access into Sony's network, they acquired confidential information that Sony did not want to go public. This attack resulted in Sony's network being down for days, four unreleased movies being made available on file-sharing networks, and thousands of confidential files being leaked to the public [1]. The hacker's ability to infiltrate a network and obtain confidential information is one reason why cyber security is an important topic. This ability can lead to many disastrous consequences for both businesses and individuals [2].

Cyber security specialists have introduced a number of methods to attempt to detect and stop hackers. A firewall is one form of cyber security. It is in many ways similar to a wall in the physical world. A firewall's purpose is to inspect all traffic going into and out of its perimeter. While firewalls attempt to inspect all information that goes into and out of its ports, it cannot check everything thoroughly because there is so much data constantly being transferred. Because of this, malicious code can often slip past a firewall disguised as favorable code [3].

Honeypots are another entity designed to protect against cyber attacks. Honeypots operate under the assumption that a hacker has broken through the firewall that was protecting the network. A honeypot is meant to look like valuable information to a hacker, but it actually monitors the hacker's activities once accessed [4]. Honeypots are traps that lure hackers in and then track them.

Summary:

Students in teams of 2 will explore the challenge of securing cyberspace by attempting to secure their own network (a maze). The students will be able to use honeypots and firewalls of varying prices to help protect files placed throughout their network. After the students have placed firewalls and honeypots throughout their network, they will exchange networks with another team and attempt to "hack" the other team's files. Students will then return the mazes to the "defenders" and the hacking attempts will be scored. Students will then be encouraged to reflect on their performance and what changes they would make if they were to repeat the activity.

Time:

The entire presentation should take approximately 42 minutes. This includes: 7 minutes for an introduction, 15 minutes for activity description and design time, 5 minutes for hacking, 10 minutes for scoring, and 5 minutes for reflection.

The Challenge:

The challenge is to design the maze in the best possible way to cause other teams of hackers to spend more time to obtain files; a shorter time is indicative of a better score for the hacker. The challenge when hacking the maze is to try to make the most profit by obtaining as many files as possible in the least amount of time.

Materials:

The table below shows the items necessary for the demonstration assuming that 40 students are completing the activity. The total initial cost is estimated to be $50.72 after tax. Even so, the cost for repeating this demonstration is much less because the compasses and colored pencils are reusable and 500 sheets of paper is more than enough for one demonstration. It should also be noted that many of these items are most likely already available within the classroom.

Items Needed for Demonstration Start-Up			
Item	**Quantity**	**Individual Price**	**Price**
Printing Paper	500 sheets	$6.97 per package	$6.97
Compass	20 compasses	$0.97 per compass	$19.40
Colored Pencils	3 boxes of 50 colored pencils	$7.01 per package	$21.03
Total Without Tax			$47.40
Tax (7.00%)			$3.32
Total			**$50.72**

Prices were found using Wal-Mart's website

Procedure:

Preparation: *(Before Class)*

In order to properly implement this activity, some preparations must be made:

1. Designate an area where each team of two students will be able to complete the activity. Make sure to distribute the compasses and at least six colored pencils per group in these areas in order to save time.

2. Prepare enough copies of the Activity Handout (3 pages total) at the end of this guide for each group to have a copy.

3. Determine how you wish to present the visuals to the students and make sure that they are prepared ahead of time. We recommend using posters or other large tangible visuals, but if appropriate, a slideshow presentation using a projector could be made to suit your needs as well.

Introduction: *(7 minutes)*

In order to introduce the students to the Grand Challenge of securing cyberspace, we suggest using the following steps. Even so, this part may be adjusted to best suit your needs. Keep in mind that cyber-related topics are often extremely abstract, so be prepared to use plenty of analogies and metaphors to properly convey the right ideas. Also, be sure to make this part relatable to the students so that they understand the importance of securing cyberspace as well as current methods used to try to stop hackers. During this introduction, be sure to encourage your students to ask questions so that they can best understand the material.

1. Start by asking the students if any of them have a Playstation or Xbox. Then ask if any of them own a computer. These questions are geared towards making the students more interested in your discussion as well as making what you are about to say more personal.

2. Show the students Visual 1, which is Sony Corporation’s logo. Ask the students what they know about this company, such as what they make. Then, tell the students that Sony is a company that is worth over 18 billion dollars and that they make many different products including Playstations, electronics, and movies.

Visual 1 — Sony Corporation's logo [6].

3. Next, ask the students if they have heard about the recent cyber attack that Sony experienced. Tell the students about some of the consequences of this hack, such as Sony's network being down for days, four unreleased movies being released online, and thousands of confidential files being released to the public [1]. Tell them that it is estimated that this hack cost Sony over 100 million dollars [5]. More statistics about the consequences of this hack can be found in article "[1]".

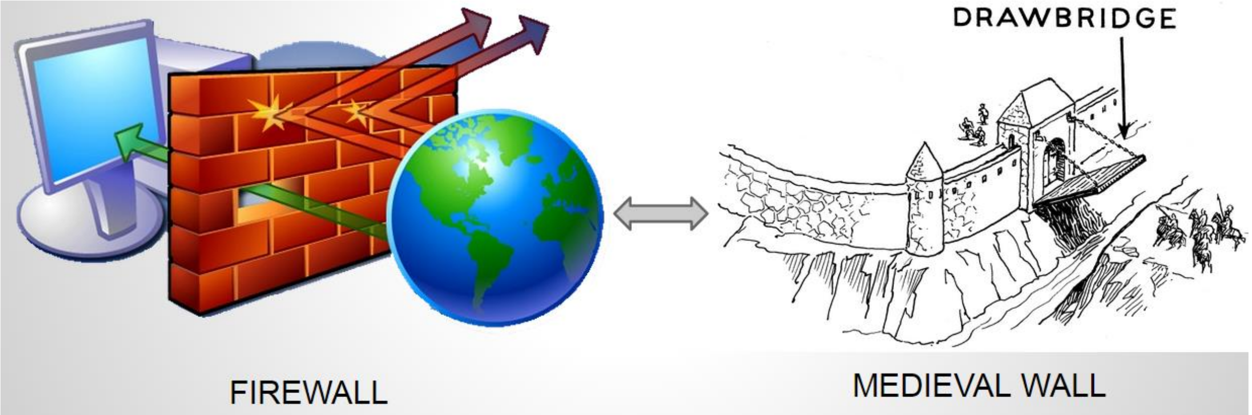
4. Relate the importance of stopping cyber attacks such as the one Sony experienced to the students' lives. Refer back to the personal devices that the students own and discuss the susceptibility of these devices considering that Sony, a multi-billion dollar company, was infiltrated.

5. Explain to the students that one aspect of securing cyberspace is to secure a network. You should define a network for the students, which is a group of computers that share files of information. Show the students Visual 2, which is a conceptual picture of a network, to help them understand what a network is.

Visual 2 — Conceptual picture representing a computer network [7].

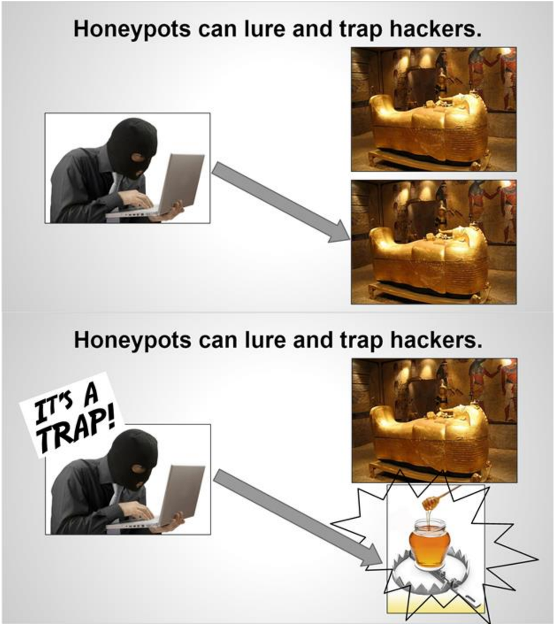
6. Tell the students that computer scientists have developed different methods to help secure cyberspace, such as firewalls and honeypots.

7. Show the students Visual 3, which is a visual analogy between computer firewalls and medieval walls. Inform the students that a firewall is in many ways similar to a medieval wall. Like a medieval wall, a firewall inspects all traffic going into and out of its perimeter. The drawbridge will only be opened for information that the firewall believes is good information. Discuss the difficulties that firewalls have with trying to inspect all incoming and outgoing information because so much data is constantly being transferred. Tell them that malicious code can often slip past a firewall disguised as favorable code for this reason. Make sure the students realize that firewalls are not always successful.



Visual 3 — Visual analogy between computer firewalls [8], and medieval walls [9].

8. Then tell the students about honeypots. Describe the function of a honeypot, which is to look like valuable information to a hacker, but actually monitors the hacker's activities once accessed. Explain that honeypots are traps that lure hackers in and then track them. While telling the students about the function of a honeypot, be sure to refer to Visual 4, which is a visual representation of a honeypot. You may choose to show the students the top half of Visual 4 before showing them the bottom half so that they can understand that the hacker cannot tell a honeypot apart from valuable information until it is too late.


Honeypots can lure and trap hackers.
Honeypots can lure and trap hackers.
IT'S A TRAP!

Visual 4 — Visual analogy of a hacker [10], choosing between the actual valuable information, i.e. the pharaoh's sarcophagus [11], and a fake piece of information, the honeypot [12].

Defense Phase: *(15 minutes)*

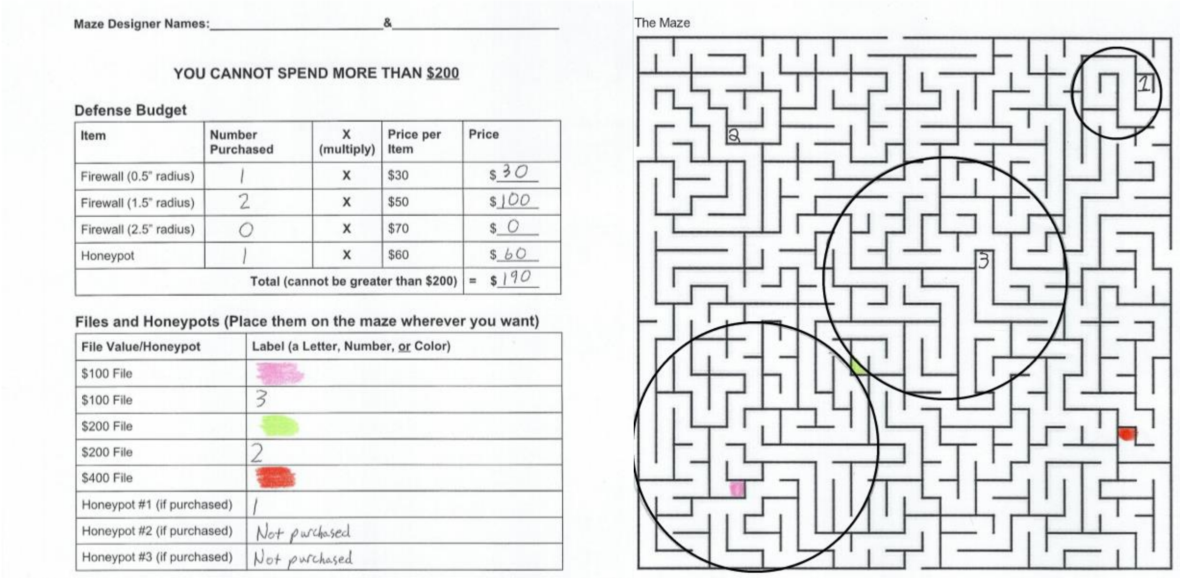
This part of the presentation will introduce the students to the engineering process and will encourage them to work in teams. Each group of students will have to balance their budget while determining how to best secure their network. It is important to note that the accompanying video for this activity begins at this point and ends at the completion of the activity.

1. You should now break the students into teams of two.

2. Once the students have been split into teams, the first two activity sheets, which include the **Defense Budget** table, the **Files and Honeypots** labeling table, and the maze, should be distributed to each team. Also, If you have not yet passed out six colored pencils and one compass to each group, now is the appropriate time to do so.

3. Introduce the activity to the students by explaining that the maze represents a network which they must place all of their valuable files inside. You should refer to the list of files in the **Files and Honeypots** labeling table (or answer key) and tell them that they must place all five of these files inside their maze. Show the students Visual 5 which depicts a completed maze along with its labeling table. Explain to the students that they have to label each file in the maze in a way which distinguishes it from any other file. They can label their files however they want to, using numbers, letters, or colors, as long as each file is distinguishable

from the other files. Also, make sure that the students know that they can place their files anywhere that they want to inside of the maze.



Maze Designer Names:______________________&______________________

YOU CANNOT SPEND MORE THAN $200

Defense Budget

Item	Number Purchased	X (multiply)	Price per Item	Price
Firewall (0.5" radius)	1	X	$30	$30
Firewall (1.5" radius)	2	X	$50	$100
Firewall (2.5" radius)	0	X	$70	$0
Honeypot	1	X	$60	$60
			Total (cannot be greater than $200) =	$190

Files and Honeypots (Place them on the maze wherever you want)

File Value/Honeypot	Label (a Letter, Number, or Color)
$100 File	🟪
$100 File	3
$200 File	🟩
$200 File	2
$400 File	🟥
Honeypot #1 (if purchased)	1
Honeypot #2 (if purchased)	Not purchased
Honeypot #3 (if purchased)	Not purchased

Visual 5 — Filled out defense budget, labeling table and maze.

4. Now, explain to the students how they are going to secure their placed files. Once again, show the students Visual 5 and explain that the circles represent firewalls placed throughout the network. Be sure to note that none of the firewalls cross and make sure that the students understand that firewalls cannot cross each other. Firewalls can be drawn outside of the maze if necessary, but there is no benefit to doing so. Also, show the students the honeypot located in the top right corner of the maze labeled “1”. Explain to the students that the hacker will not have the labeling table while hacking the maze and that this honeypot will look like an ordinary, valuable file to the hacker.

5. Now that the students can identify that the circles are firewalls and that honeypots are disguised as files, explain to the students how the budget works. While explaining this to the students, make sure to refer to the **Defense Budget** table on their handout. An example of a completed **Defense Budget** table can be seen in Visual 5. Make sure that the students understand that they only have $200 to spend on honeypots and firewalls. Also, ensure that the students know that the firewalls of varying size cost different amounts. You should explain to the students how to use this table in order to calculate the amount of money that they have spent. Make sure that they understand that they have to multiply the **Number Purchased** by the **Price per Item** and then add all of the prices together in order to find out how much they have spent. It may be beneficial to make an example secured maze in front of the students so that they understand how to stay under their budget.

6. Now, give the students some context for their design by explaining the time penalties given when hackers cross a firewall or access a honeypot. Each time the circle defining a firewall is crossed, 3 seconds is added to the hackers' final time. Accessing a honeypot adds 30 seconds to the hackers' final time.

7. Now that the students understand the time penalties associated with the defense mechanisms, explain to the students the objective of this activity: to place the files, honeypots and firewalls inside the maze in a way so that it is difficult for a hacker to retrieve the files in a timely fashion.

8. At this time, it may also be beneficial to spend a moment reminding the students how to properly use a compass.

9. Now that the students understand the concept of defending their network, the design period of defending their network can begin. During this 10 minute period, the student teams will decide where to place their files throughout the maze and which defense mechanism that they want to use. The students will then place these defense mechanisms throughout their maze in order to protect their files.

10. During this period, you should circulate the room and offer help to any of the groups who appear to be struggling. Also, make sure that each group remains under the $200 budget. You should also call out the time remaining every 2 minutes so that the students can be sure to complete the design phase in time.

11. Once this 10 minute period ends, it is time to enter the hacking phase.

Hacking Phase: *(5 minutes)*

During this phase of the activity, students will attempt to hack another group's maze by trying to reach all of the files in the maze as quickly as possible.

1. Now that each team of students has designed their own maze, have each team exchange their maze with another team. Explain to the students that they will now attempt to hack the other team's maze.

2. You should tell the students that they have to pick one of the four entrances and draw a continuous path throughout the maze. It is important that the students understand that they cannot pick up their pencil and move to another location.

3. Ensure that the students know that they may choose to leave the maze and end the hacking phase whenever they wish to, even if they are not near an exit or have not collected all of the files.

4. Tell the students that this is a timed event, and make sure that they know that the goal of this phase is to collect as many files as quickly as possible while attempting to avoid firewalls and honeypots. Tell the students that you will be calling out every 30 seconds that passes during this activity. Make sure that the students understand that they have to write down the most recent time that you called out when they are finished hacking.

5. Now that the students understand all of the rules, the hacking phase can begin.

6. Once the hacking phase begins, you should call out the time in 30 second intervals so that the students can keep track of their progress while they are completing the maze. Stop all students who have not stopped hacking after **4 minutes**.

7. Make sure that each team records the time that they spent inside of the maze, which should be some multiple of 30 seconds, below the maze.

Scoring: *(10 minutes)*

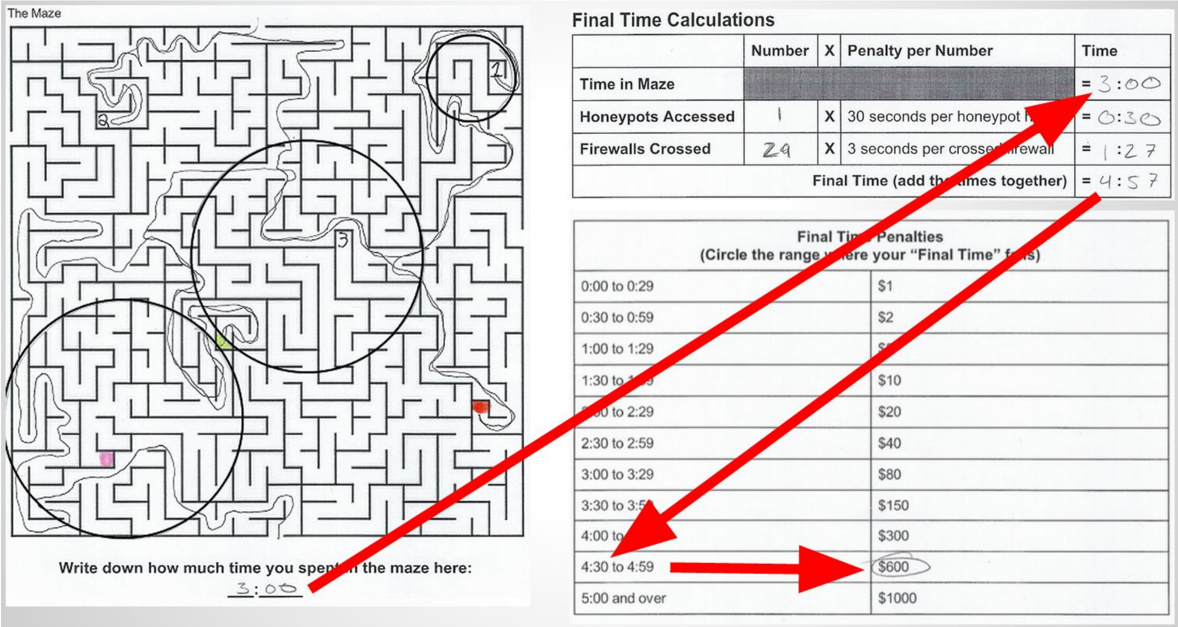
During this portion of the activity, students will determine how effectively they protected their files inside of the maze by using an activity sheet for scoring. For a walkthrough on how to score the team’s hacking attempt, please see the accompanying video.

1. Once the students have finished hacking, give each team a copy of the third activity sheet which includes the **Final Time Calculations** table, the **Final Time Penalties** table, and the **Calculating Hackers’ Final Score** table.

2. Meanwhile, have students return the hacked mazes to their original owners, who will then count up how many times their firewalls were crossed and how many honeypots were accessed by the hacker. Make sure the students record these values in the **Number** column of the **Final Time Calculations** table.

3. Tell the students that in order to obtain the total time penalties associated with firewalls and honeypots, they have to multiply the **Number** by the **Penalty per Number** and then record this time in the **Time** column.

4. Show the students that in order to get the **Final Time** for the hacker, they have to add all of the times in the **Time** column of the **Final Time Calculations** table.
5. This total time will be used to determine the hacking team’s money penalty, which can be found in the **Final Time Penalties** table. Have them circle the money penalty which corresponds to the time range where the hacking team’s **Final Time** falls. Visual 6 below helps indicate how to determine the time penalty for the hacking team.


The Maze
1
2
3

Write down how much time you spent in the maze here: 3:00

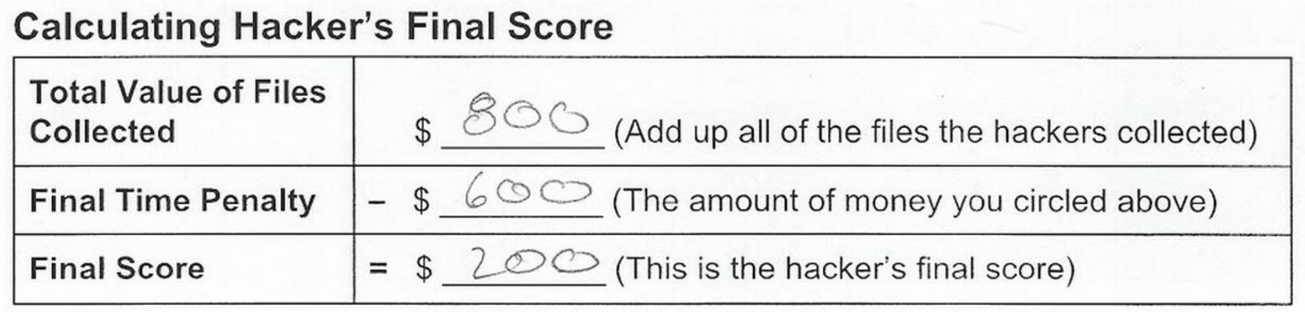
Final Time Calculations

	Number	X	Penalty per Number	Time
Time in Maze				= 3:00
Honeypots Accessed	1	X	30 seconds per honeypot h	= 0:30
Firewalls Crossed	29	X	3 seconds per crossed firewall	= 1:27
Final Time (add the times together)				= 4:57

Final Time Penalties (Circle the range where your "Final Time" falls)	
0:00 to 0:29	$1
0:30 to 0:59	$2
1:00 to 1:29	[illegible]
1:30 to 1:59	$10
2:00 to 2:29	$20
2:30 to 2:59	$40
3:00 to 3:29	$80
3:30 to 3:59	$150
4:00 to [illegible]	$300
4:30 to 4:59	[✓ $600]
5:00 and over	$1000

Visual 6 — Indication of how to determine time penalty.

6. The students will add up the the total amount of money that the hacking team obtained from files in the maze and record this value in the **Total Value of Files Collected** row of the **Calculating Hackers' Final Score** table. Then, the students will need to write the **Final Time Penalty** which they circled in the **Final Time Penalties** table in the **Final Time Penalty** row of the **Calculating Hacker's Final Score** table. Make sure the students subtract the **Final Time Penalty** from the **Total Value of Files Collected** in order to obtain the hacking team's **Final Score**. Visual 7 below shows a sample calculation of a hacker's final score.



Calculating Hacker's Final Score

Total Value of Files Collected	$ 800 (Add up all of the files the hackers collected)
Final Time Penalty	– $ 600 (The amount of money you circled above)
Final Score	= $ 200 (This is the hacker's final score)

Visual 7 — Sample calculation of hacker's final score.

7. You should make sure that the students understand that a lower score is better in determining the effectiveness of their maze. This is because a higher score reflects the hacking team's ability to more effectively infiltrate the maze in a timely fashion.

Reflection:

Now that the students have had the opportunity to see how well their maze performed, it would be a good opportunity to allow them to reflect on this performance. This part may be adjusted to best suit your needs.

1. Allow the students to share their scores amongst themselves to see how well they did compared to others.

2. Now that the students have had the opportunity to see how their maze did in comparison to others, you should ask them some reflection questions about the defense phase of this activity. Ask them questions such as: *What would you do differently if you were to repeat this activity? Would you change the placement of files? Would you spend your budget differently? Would you change the placement of your honeypots or firewalls?* You should also ask reflection questions about the hacking phase, such as: *How would you approach the same maze if you were to try to hack it again? Could you have improved your score by leaving earlier? Should you have taken a different path?* You can choose how you want students to answer these questions, such as through written response or just discussing with a neighbor. Also, you should ask any other questions that you think are appropriate. This reflection period is meant to emphasize the importance of communicating results within the engineering profession.

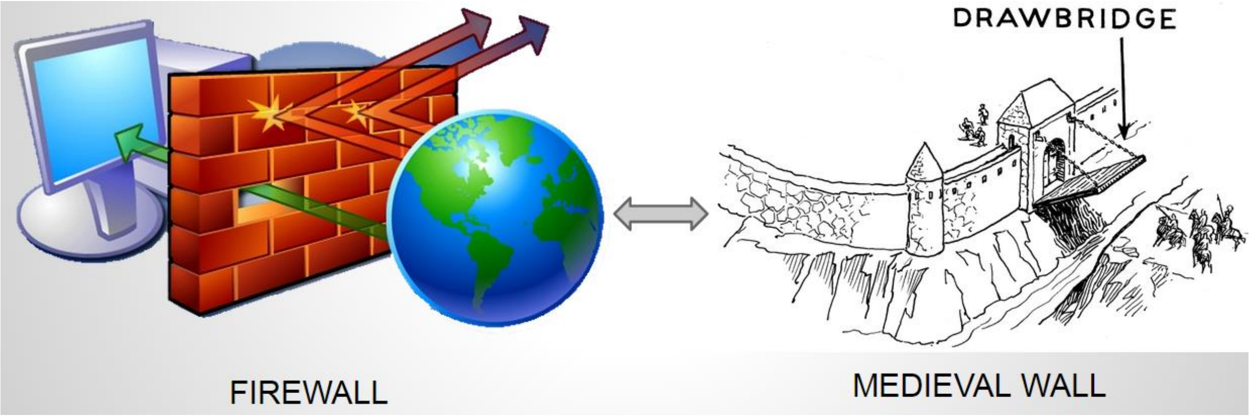
3. Now, you should make sure to ask the students if any of them have any questions related to securing cyberspace or the activity.

4. Once all of their question have been addressed, the activity is complete.

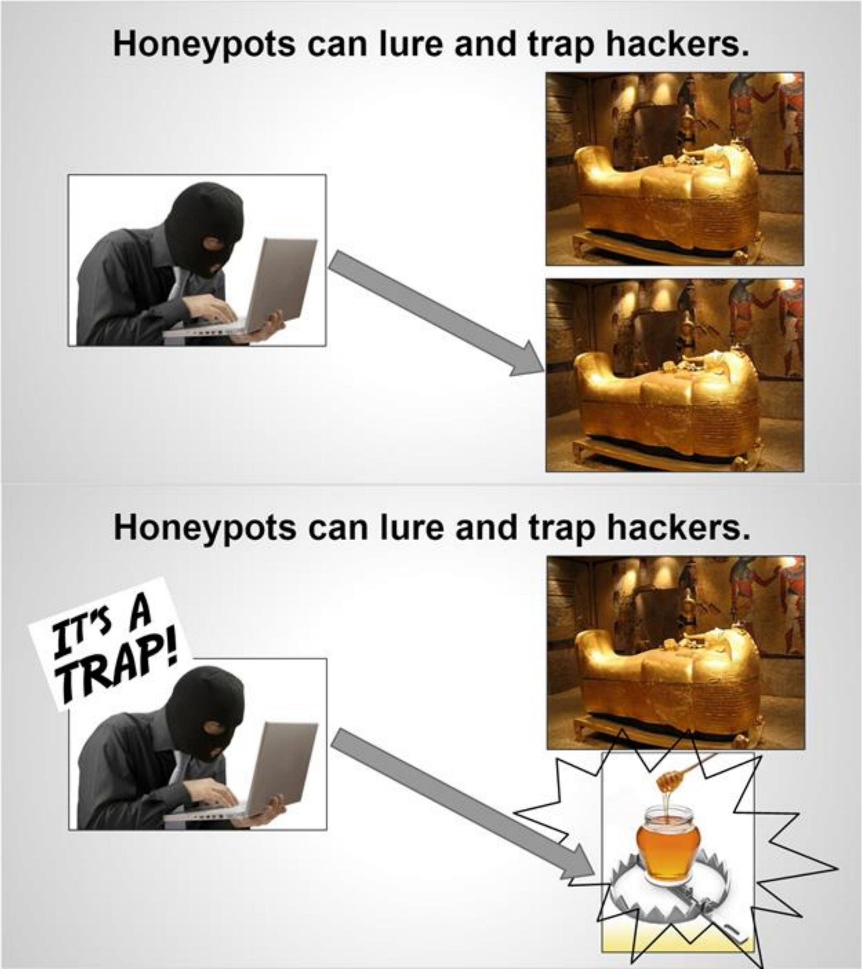
Visuals

Visual 1 — Sony Corporation’s logo [6].

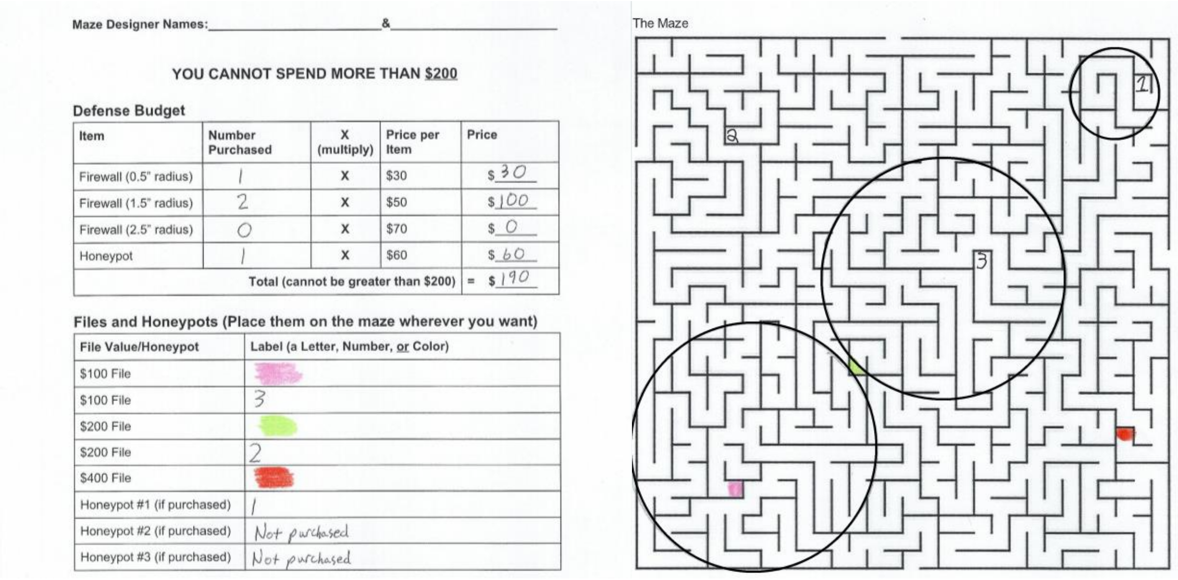
Visual 2 — Conceptual picture representing a computer network [7].



Visual 3 — Visual analogy between computer firewalls [8], and medieval walls [9].


Honeypots can lure and trap hackers.
Honeypots can lure and trap hackers.
IT'S A TRAP!

Visual 4 — Visual analogy of a hacker [10], choosing between the actual valuable information, i.e. the pharaoh's sarcophagus [11], and a fake piece of information, the honeypot [12].


Maze Designer Names:________________&________________

YOU CANNOT SPEND MORE THAN $200

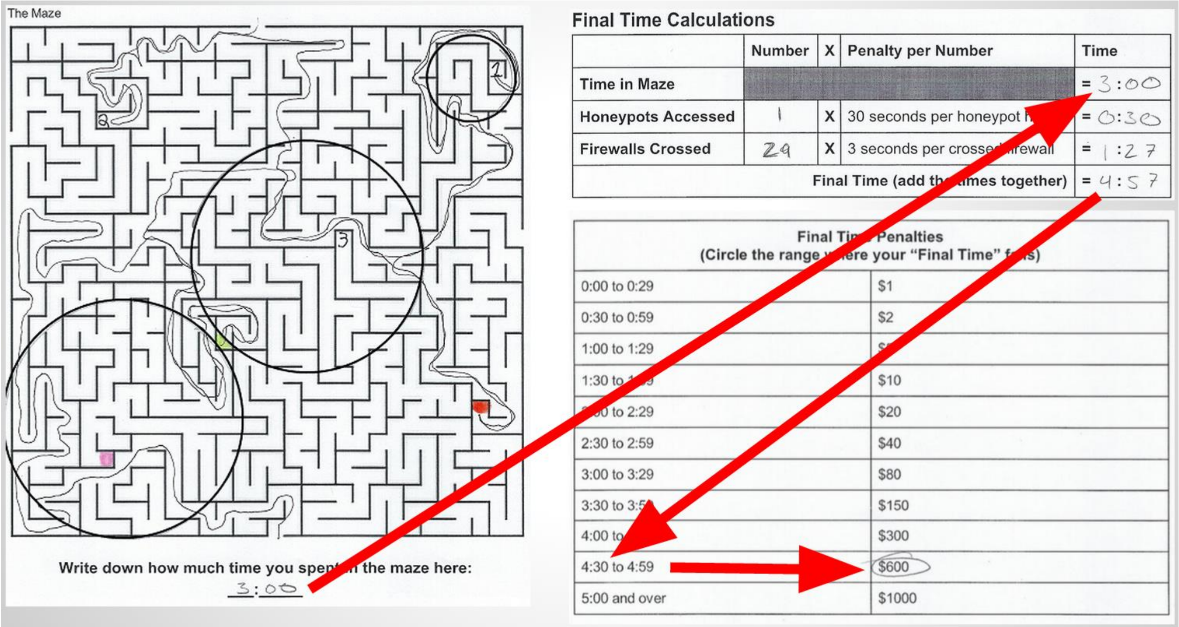
Defense Budget

Item	Number Purchased	X (multiply)	Price per Item	Price
Firewall (0.5" radius)	1	X	$30	$ 30
Firewall (1.5" radius)	2	X	$50	$ 100
Firewall (2.5" radius)	0	X	$70	$ 0
Honeypot	1	X	$60	$ 60
Total (cannot be greater than $200)			=	$ 190

Files and Honeypots (Place them on the maze wherever you want)

File Value/Honeypot	Label (a Letter, Number, or Color)
$100 File	🟪
$100 File	3
$200 File	🟩
$200 File	2
$400 File	🟥
Honeypot #1 (if purchased)	1
Honeypot #2 (if purchased)	Not purchased
Honeypot #3 (if purchased)	Not purchased

Visual 5 — Filled out defense budget, labeling table and maze.


The Maze
1
2
3

Write down how much time you spent in the maze here: 3:00

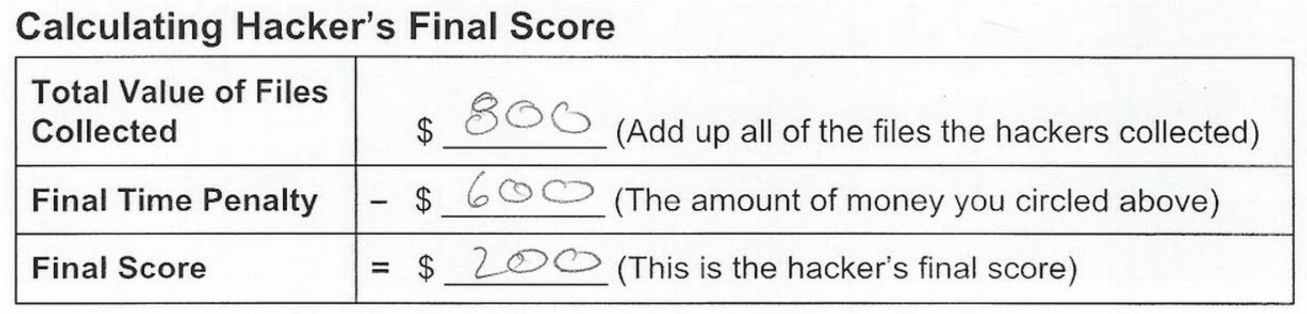
Final Time Calculations

	Number	X	Penalty per Number	Time
Time in Maze				= 3:00
Honeypots Accessed	1	X	30 seconds per honeypot hit	= 0:30
Firewalls Crossed	29	X	3 seconds per crossed firewall	= 1:27
Final Time (add the times together)				= 4:57

Final Time Penalties
(Circle the range where your "Final Time" falls)

0:00 to 0:29	$1
0:30 to 0:59	$2
1:00 to 1:29	$5
1:30 to 1:59	$10
2:00 to 2:29	$20
2:30 to 2:59	$40
3:00 to 3:29	$80
3:30 to 3:59	$150
4:00 to 4:29	$300
4:30 to 4:59	[✓ $600]
5:00 and over	$1000

Visual 6 — Demonstration of how to determine time penalty.



Calculating Hacker's Final Score

Total Value of Files Collected	$ 800 (Add up all of the files the hackers collected)
Final Time Penalty	– $ 600 (The amount of money you circled above)
Final Score	= $ 200 (This is the hacker's final score)

Visual 7 — Sample calculation of hackers' final score.

Teacher Resources

Documentation:

This website describes the Sony hack, how it happened, who may be responsible, and what information was taken. This is a great source for familiarizing yourself with the Sony hack and its consequences.

> [1] T. Lee. (2014, December 17). *The Sony hack: how it happened, who is responsible, and what we've learned*. [Online]. Available: http://www.vox.com/2014/12/14/7387945/sony-hack-explained

This article describes what cyberspace is, and why it is important to keep cyberspace secure. This article also illustrates different methods for securing cyberspace and how engineers are attempting to keep cyberspace secure.

> [2] National Academy of Engineering. (2012). *Secure cyberspace*. [Online]. Available: http://www.engineeringchallenges.org/cms/8996/9042.aspx

This article is an in-depth description of firewalls and how they function. This was the primary source we used to provide technical information for firewalls and how they work.

> [3] L. Majowicz. (2008, December 15). *Firewall Cracking and Security*. [Online]. Available: http://pages.csam.montclair.edu/~robila/SECURITY/2008/pp27.pdf

This journal article describes the functions of honeypots in great detail.

> [4] A. Prathapani, L. Santhanam, D. P. Agrawal. "Detection of blackhole attack in a Wireless Mesh Network using intelligent honeypot agents." *Journal of Supercomputing*, vol. 64, pp. 777–804, 2013.

This site was used to give an estimate as to how much the Sony hack will cost the Sony corporation.

> [5] S.Sanders. (2014, December 18). *How Much Will The Hack Cost Sony?* [Online]. Avaliable: http://www.npr.org/2014/12/18/371721061/how-much-will-the-hack-cost-sony

Visual 1: Sony Logo

[6] D. Poeter. (2014, December 16). *Employees Sue Sony Pictures Over Massive Hack*. [Online]. Available: http://www.pcmag.com/article2/0,2817,2473756,00.asp

Visual 2: Network

[7] (2014). *Computing network services.* [Online]. Available: http://www.teratechuganda.com/computer-networking-services/

Visual 3, Left Image: Firewall

[8] Admin. (2014, October). *Firewalld - How to dynamically manage firewall in RHL/CENTOS 7.0*. [Online]. Available: http://www.gocit.vn/bai-viet/firewalld-how-to-dynamically-manage-firewall-in-rhelcentos-7-0/

Visual 3, Right Image: Medieval Wall

[9] Tim Cool. (2014, October). *Lowering the Drawbridge*. [Online]. Available: http://coolconversationslive.com/lowering-the-drawbridge/

Visual 4: Hacker

[10] Clark Howard. (2015, January 9). *Is Your Password Easy To Hack?* [Online]. Available: http://www.clarkhoward.com/news/clark-howard/consumer-issues-id-theft/your-password-easy-hack/njkDq/

Visual 4: Pharaoh's Sarcophagus

[11] (2014). *Flight 37 Role Play*. [Online]. Available: http://www.wattpad.com/85525564-flight-37-role-play-role-play-the-pharaoh's-tomb#

Visual 4: Honeypot Picture

[12] (2015). *Early detect APT's via an internal honeypot network*. [Online]. Available: http://www.krinoscybersecurity.com/early-detect-apts-via-an-internal-honeypot-network/

This video shows president Obama talking about cybersecurity and national cybersecurity awareness month. Showing this video to your students can make them more aware of the seriousness of securing cyberspace.

[13] The White House, *National Cybersecurity Awareness Month*, [Online Video] Washington DC, The White House, 2009. https://www.youtube.com/watch?v=UIIY9AQSqbY&index=1&list=FLx9mpsq9kYATCOmRQZuZZ-A

Maze Designer Names:______________________________**&**_____________________________

YOU CANNOT SPEND MORE THAN <u>$200</u>

Defense Budget

Item	**Number Purchased**	**X (multiply)**	**Price per Item**	**Price**
Firewall (0.5" radius)		**X**	$30	$______
Firewall (1.5" radius)		**X**	$50	$______
Firewall (2.5" radius)		**X**	$70	$______
Honeypot		**X**	$60	$______
Total (cannot be greater than $200)				**= $______**

Files and Honeypots (Place them on the maze wherever you want)

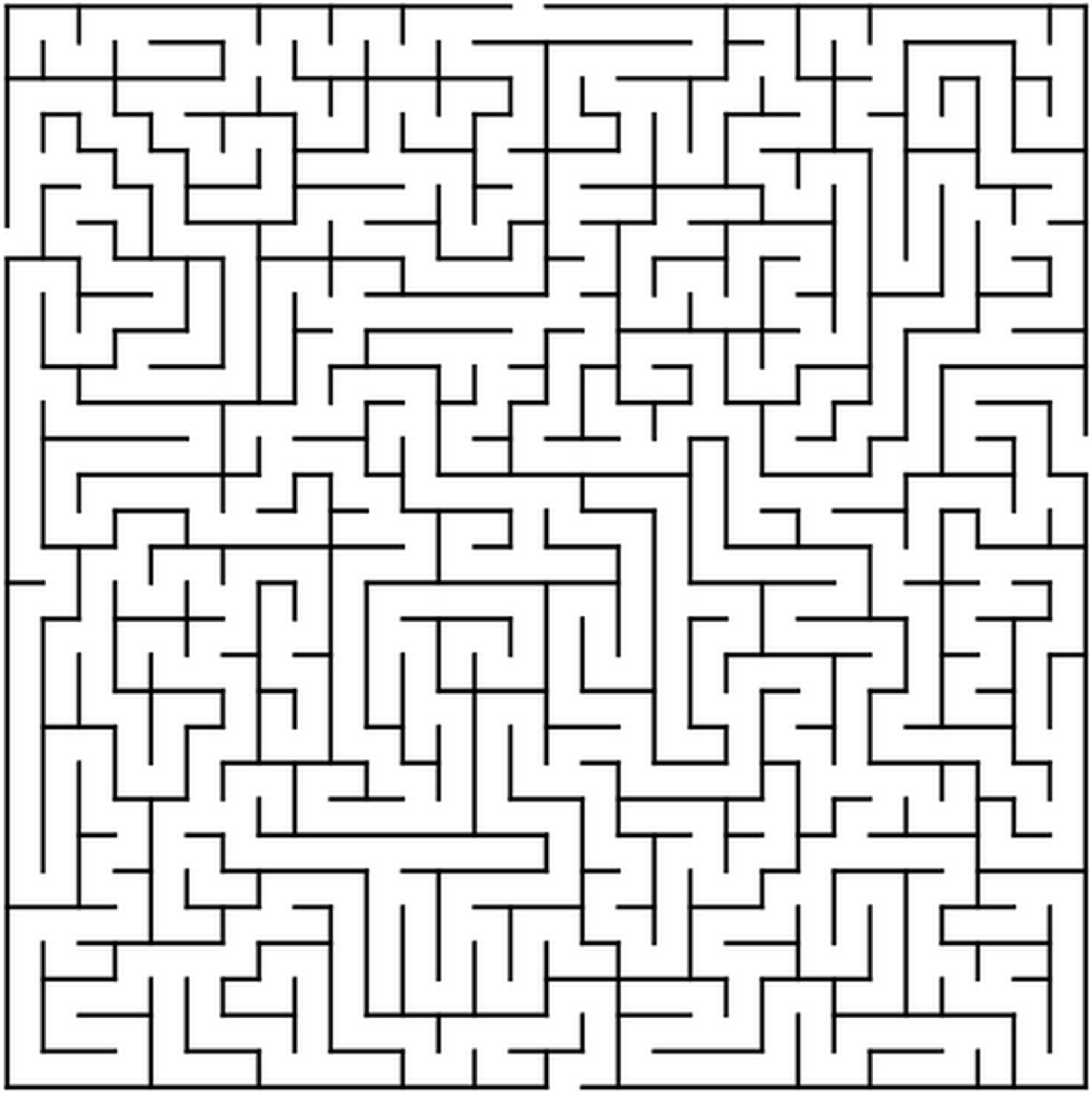
File Value/Honeypot	**Label (a Letter, Number, <u>or</u> Color)**
$100 File	
$100 File	
$200 File	
$200 File	
$400 File	
Honeypot #1 (if purchased)	
Honeypot #2 (if purchased)	
Honeypot #3 (if purchased)	

Team SuperStarz

Maze Designer Names:________________________&___________________________

Maze Hacker Names:__________________________&_________________________

The Maze



Write down how much time you spent in the maze here:

___:_____

Final Time Calculations

	Number	X	Penalty per Number	Time
Time in Maze				**= :**
Honeypots Accessed		**X**	30 seconds per honeypot hit	**= :**
Firewalls Crossed		**X**	3 seconds per crossed firewall	**= :**
			Final Time (add the times together)	**= :**

Final Time Penalties **(Circle the range where your "Final Time" falls)**	
0:00 to 0:29	$1
0:30 to 0:59	$2
1:00 to 1:29	$5
1:30 to 1:59	$10
2:00 to 2:29	$20
2:30 to 2:59	$40
3:00 to 3:29	$80
3:30 to 3:59	$150
4:00 to 4:29	$300
4:30 to 4:59	$600
5:00 and over	$1000

Calculating Hackers' Final Score

Total Value of Files Collected	$ __________ (Add up all of the files the hackers collected)
Final Time Penalty	**–** $ __________ (The amount of money you circled above)
Final Score	**=** $ __________ (This is the hackers' final score)