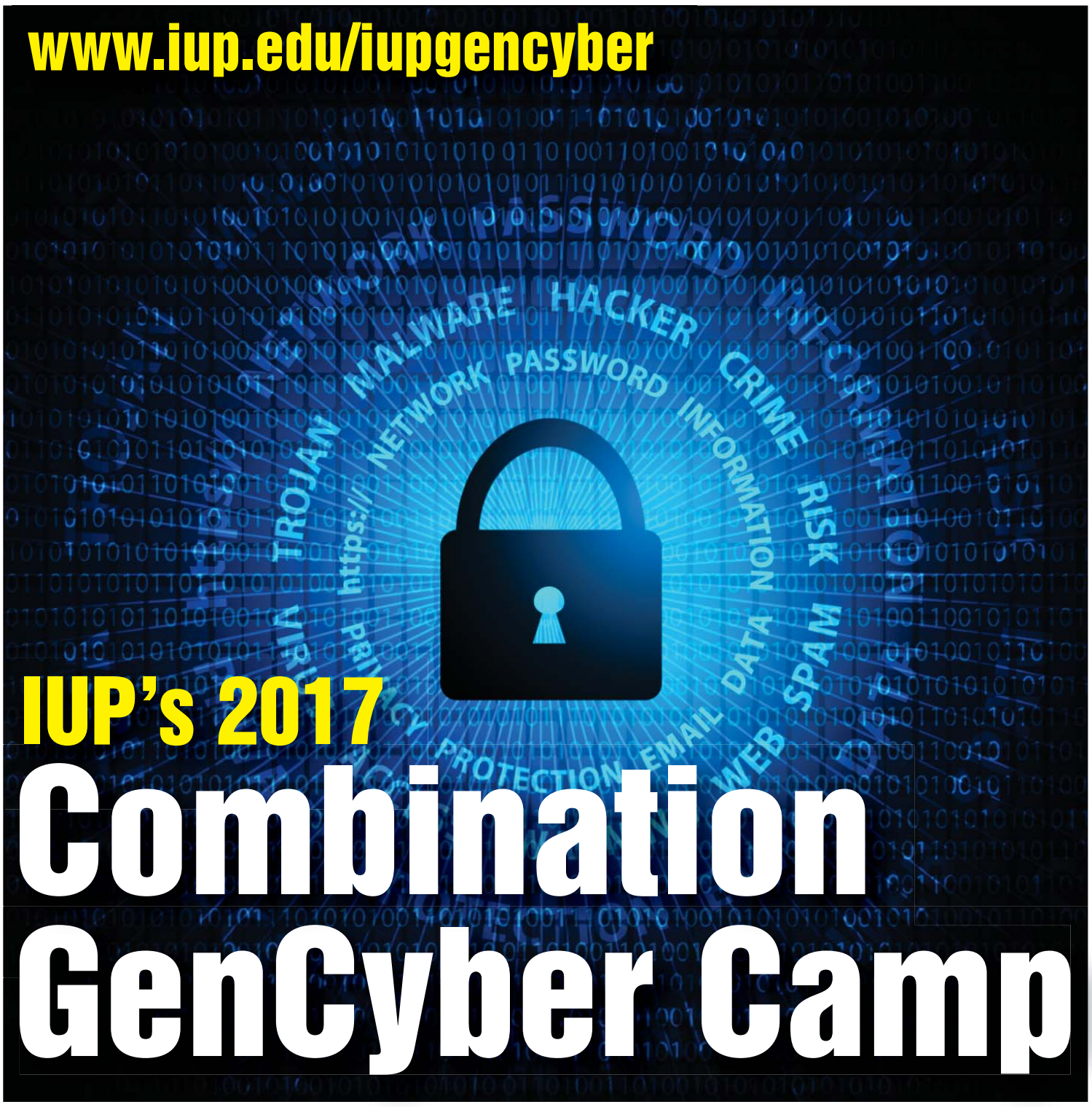
www.iup.edu/iupgencyber



IUP's 2017 Combination GenCyber Camp

JUNE 12 TO JUNE 16, 2017

IUP GENCYBER: CYBERSECURITY CAMP FOR MIDDLE AND HIGHSCHOOL STUDENTS

- Learn detailed information about cybersecurity basics
- Learn hacking defense techniques
- Acquire skills to land your dream job
- Do any of the topics interest you? Apply today!

Through this opportunity, you will learn safe online behavior, increase knowledge of cyberspace, and explore cybersecurity careers.

Advantages*

Offered at no cost!

Parrot Cargo Drone for each participant!

FREE lunch and afternoon snack!

Instruction and mentorship from IUP faculty and other experts!

Skills and knowledge for a growing career field!

Apply NOW space is limited!

Questions?

gen-cyber@iup.edu

Location:

IUP main Campus

Program Directors

Waleed Farag, Ph.D.
Computer Science

Mac Fiddner, Ph.D.
Political Science

*program is contingent on funding released by NSA

www.iup.edu/iupgencyber

IUP's 2017 Combination GenCyber Camp

JUNE 12 TO JUNE 16, 2017

IUP GENCYBER: CYBERSECURITY CAMP FOR MIDDLE AND HIGHSCHOOL TEACHERS

- Learn detailed information about cybersecurity
- Learn about promising careers for students
- Acquire skills to change the future of your students
- Do any of the topics interest you? Apply today!

Through this opportunity, you will learn safe online behavior, become part of the solution to the nation's shortage of skilled cybersecurity professionals, and help inspire young people to direct their talents to cybersecurity, a profession of critical importance to our nations future

Advantages*

Offered at no cost!

A Chrome Book for each participant!

Act 48 Credits

FREE lunch and afternoon snack!

Mileage reimbursement for those who qualify

Multidisciplinary cybersecurity teaching skills, and modules to be used in the classroom!

Apply NOW space is limited!

Questions?

gen-cyber@iup.edu

Location:

IUP main Campus

Program Directors

Waleed Farag, Ph.D.
Computer Science

Mac Fiddner, Ph.D.
Political Science

*program is contingent on funding released by NSA

IUP Proudly Presents:

Advanced GenCyber Camp

JUNE 27 TO JULY 3, 2017

ATTENTION: MIDDLE AND HIGH SCHOOL STUDENTS!

- Expand your cybersecurity and technical knowledge
- Explore techniques for securing networked systems
- Learn more about advanced programming, cryptography and digital forensics
- Do any of these topics interest you? **Apply today!**

Location

IUP Main Campus

Questions?

gen-cyber@iup.edu

Program Directors

Waleed Farag, Ph.D.
Computer Science

Mac Fiddner, Ph.D.
Political Science

Advantages*

- Offered at no cost!
- Arduino Circuit Board for each participant!
- FREE lunch and afternoon snack!
- Instruction and mentorship from IUP faculty and other experts!
- Skills and knowledge for a growing career field!

Apply NOW space is limited!

GenCyber NSF National Security Agency United States of America

www.iup.edu/iupgencyber

*program is contingent on funding released by NSA

ADVANTAGES FOR STUDENTS

- Offered at no cost!
- Mini Drone or Arduino for each participant!*
- FREE lunch and afternoon snack!
- Instruction and mentorship from IUP faculty and other experts!
- Skills and knowledge for a growing career field!

ADVANTAGES FOR TEACHERS

- Offered at no cost!
- A Chromebook to take home for each participant!*
- FREE lunch and afternoon snack!
- ACT 48 Credits
- Mileage reimbursement for those who
- qualify!
- Multidisciplinary cybersecurity teaching skills, and modules to be used in class!

*Program contingent on funds released by NSA!

HOW TO APPLY

Applications are accepted online only. To apply or view other important information, please visit:

www.iup.edu/iupgencyber

CAMP DATES

Combination Camp
June 12 to June 16, 2017

Advanced Camp
June 27 to July 3, 2017

PROGRAM DIRECTORS

Dr. Waleed Farag
Professor of Computer Science

Dr. Mac Fiddner
Associate Professor of Political Science

PROUDLY AFFILIATED WITH

NSF NSA GenCyber IUP

SUMMER 2017 GENCYBER CAMPS

PRESENTED BY IUP AND NSA

IUP GENCYBER

SUMMER 2017 PROGRAM

Gen Cyber is a new national initiative that is supported by the National Science Foundation and the National Security Foundation. This program has the following objectives:

- Increase interest in cybersecurity careers and diversity in the cybersecurity workforce of the nation
- Help all students understand correct and safe on-line behavior.
- Improve teaching methods for delivering cybersecurity content for K-12 curricula

THE FUNDED GRANT

Under the leadership of Dr. Waleed Farag, grant PI, and Dr. Mac Fiddner, grant co-PI, IUP, along with a selected group of national universities, has been awarded funding to hold a combination summer camp for middle and high school students and teachers, and an advanced camp for middle and high school students.

These funded projects will focus on fostering and sustaining a strong cybersecurity culture in high and middle school students and teachers in western PA through a holistic multidisciplinary approach. The combined camp will present a general introduction to cybersecurity fundamentals. The advanced camp will be technically oriented and geared toward students with previous programming and/or cybersecurity experience and knowledge.

CAMP PROGRAM SUMMARY

This project will host two FREE (no cost to participants), five-weekday day-camps in summer 2017. Instruction will be delivered by a team of professors and high/middle school teachers with numerous backgrounds but established expertise in cybersecurity teaching, research, and K-12 education. Camp will include:

- Upon completion of camps, participants will have a strong understanding of cybersecurity in addition to mastering basic skills that help them be safer online.
- 85 projected participants. 55 in the combination camp and 30 in the advanced camp.
- 150 teaching hours proposed (30 for each group at a rate of six hours per day).
- An engaging content delivery approach that includes direct instruction, group activites, structured discover, and hands-on laboratory.

CYBERSECURITY CAMP DAILY SCHEDULE — DAY 1 - JUNE 12, 2017

	Middle School Students	High School Students	Teachers
9:00 a.m. to 9:50 a.m.	Welcome, Introduction to team members, orientation and logistics HSS Building, Room 126		
9:50 a.m. to 10:00 a.m.	BREAK		
10:00 a.m. to 10:50 a.m.	Cybersecurity First Principles - Dr. Farag/ Dr. Fiddner HSS Building, Room 126		
10:50 a.m. to 11:00 a.m.	BREAK		
11:00 a.m. to 11:50 a.m.	Session 1 - Facility tour, computer account access, equipment activation Stright Hall, Rooms 112 A, 112 B, 107 A		
11:50 a.m. to 1:00 p.m.	LUNCH - Stright 112B		
1:00 p.m. to 1:50 p.m.	Session 2 - Facility tour, computer account access, equipment activation Stright Hall, Rooms 112 A, 112 B, 107 A		
1:50 p.m. to 2:00 p.m.	BREAK		
2:00 p.m. to 2:50 p.m.	Session 1 - Block Coding w/ Scratch Mrs. Gentile — Stright Room 112A	Session 1 - Robots Dr. Rodger — Stright Room 320/301	Session 1 - Transforming Your Curriculum: A Toolbox of Resources Dr. Machado — Stright Room 112B/107A
2:50 p.m. to 3:10 p.m.	BREAK - Stright 112B		
3:10 p.m. to 4:00 p.m.	Session 2 - Block Coding w/ Scratch Mrs. Gentile — Stright Room 112A	Session 2 - Robots Dr. Rodger — Stright Room 320/301	Session 2 - Transforming Your Curriculum: A Toolbox of Resources Dr. Machado — Stright Room 112B/107A

CYBERSECURITY CAMP DAILY SCHEDULE — DAY 2 - JUNE 13, 2017

	Middle School Students	High School Students	Teachers
9:00 a.m. to 9:50 a.m.	Session 1 - Robots Dr. Rodger Stright Room 320/301	Session 1 - Programming in JavaScript on Khanacademy Mrs. Gentile Stright Room 112A	Session 1 - Using Social Media for Teaching and Reputation Management Dr. Machado Stright Room 112B/107A
9:50 a.m. to 10:00 a.m.	BREAK		
10:00 a.m. to 10:50 a.m.	Session 2 - Robots Dr. Rodger Stright Room 320/301	Session 2 - Programming in JavaScript on Khanacademy Mrs. Gentile Stright Room 112A	Session 2 - Using Social Media for Teaching and Reputation Management Dr. Machado Stright Room 112B/107A
10:50 a.m. to 11:00 a.m.	BREAK		
11:00 a.m. to 11:50 a.m.	Session 1 - Intro to Networking Dr. Pankaj Stright Room 320	Session 1 - Drone Technology Dr. Farag Stright Room 107A	Session 1 - Implementing First Principles into Subject Area Mr. Tozer Stright Room 112A
11:50 a.m. to 1:00 p.m.	LUNCH - HSS 225		
1:00 p.m. to 1:50 p.m.	Session 2 - Intro to Networking Dr. Pankaj Stright Room 320	Session 2 - Drone Technology Dr. Farag HSS Room 225	Session 2 - Implementing First Principles into Subject Area Mr. Tozer Stright Room 112A
1:50 p.m. to 2:00 p.m.	BREAK		
2:00 p.m. to 2:50 p.m.	Session 1 - Separating the Domains of Factual and Fake News Mr. Tozer Stright Room 112A	Session 1 - Intro to Networking Dr. Pankaj Stright Room 320	Session 1 - Learning Through Teacher-Made Games and Activities (incl GenCyber Cards) Mrs. Gentile Stright Room 112B/107A
2:50 p.m. to 3:10 p.m.	BREAK - Stright 112B		
3:10 p.m. to 4:00 p.m.	Session 2 - Separating the Domains of Factual and Fake News Mr. Tozer Stright Room 112A	Session 2 - Intro to Networking Dr. Pankaj Stright Room 320	Session 2 - Learning Through Teacher-Made Games and Activities (incl GenCyber Cards) Mrs. Gentile Stright Room 112B/107A

CYBERSECURITY CAMP DAILY SCHEDULE — DAY 3 - JUNE 14, 2017

	Middle School Students	High School Students	Teachers
9:00 a.m. to 9:50 a.m.	Session 1 - Putting GenCyber Principles into Practice - Mrs. Gentile/Mr. Tozer Stright Hall, Rooms 112 A, 112 B		
9:50 a.m. to 10:00 a.m.	BREAK		
10:00 a.m. to 10:50 a.m.	Session 2 - Putting GenCyber Principles into Practice - Mrs. Gentile/Mr. Tozer Stright Hall, Rooms 112 A, 112 B		
10:50 a.m. to 11:00 a.m.	BREAK		
11:00 a.m. to 11:50 a.m.	Session 1 - Drone Technology Dr. Farag — Stright Room 112B/107A	Session 1 - Physical Security Dr. Giever — HSS Room 114	Session 1 - Cyberbullying Tactics: Empowering Students to Take Charge Dr. Machado — Stright Room 112A
11:50 a.m. to 1:00 p.m.	LUNCH - HSS 126		
1:00 p.m. to 1:50 p.m.	Session 2 - Drone Technology Dr. Farag — HSS Room 126	Session 2 - Physical Security Dr. Giever — HSS Room 114	Session 2 - Cyberbullying Tactics: Empowering Students to Take Charge Dr. Machado — Stright Room 112A
1:50 p.m. to 2:00 p.m.	BREAK		
2:00 p.m. to 2:50 p.m.	Session 1 - Physical Security Dr. Giever — HSS Room 114	Session 1 - Separating the Domains of Factual and Fake News Mr. Tozer — Stright Room 112A	Session 1 - On-line/Tech-Based Engagement and Assessment Mrs. Gentile — Stright Room 112B/107A
2:50 p.m. to 3:10 p.m.	BREAK - Stright 112B		
3:10 p.m. to 4:00 p.m.	Session 2 - Physical Security Dr. Giever — HSS Room 114	Session 2 - Separating the Domains of Factual and Fake News Mr. Tozer — Stright Room 112A	Session 2 - On-line/Tech-Based Engagement and Assessment Mrs. Gentile — Stright Room 112B/107A

CYBERSECURITY CAMP DAILY SCHEDULE — DAY 4 - JUNE 15, 2017

	Middle School Students	High School Students	Teachers
9:00 a.m. to 9:50 a.m.	Session 1 - Games Dr. Smith — Stright Room 320	Session 1 - Network Security Dr. Farag — Stright Room 112B/107A	Session 1 - Summarizing First Principles Relation to Subject Area Mr. Tozer — Stright Room 112A
9:50 a.m. to 10:00 a.m.	BREAK		
10:00 a.m. to 10:50 a.m.	Session 2 - Games Dr. Smith — Stright Room 320	Session 2 - Network Security Dr. Farag — Stright Room 112B/107A	Session 2 - Summarizing First Principles Relation to Subject Area Mr. Tozer — Stright Room 112A
10:50 a.m. to 11:00 a.m.	BREAK		
11:00 a.m. to 11:50 a.m.	Session 1 - Network Security Dr. Farag — Stright Room 112B/107A	Session 1 - Games Dr. Smith — Stright Room 320	Session 1 - Using Google Apps to Share Ideas Mrs. Gentile — Stright Room 112A
11:50 a.m. to 1:00 p.m.	LUNCH - Stright 112B		
1:00 p.m. to 1:50 p.m.	Session 2 - Network Security Dr. Farag — Stright Room 112B/107A	Session 2 - Games Dr. Smith — Stright Room 320	Session 2 - Using Google Apps to Share Ideas Mrs. Gentile — Stright Room 112A
1:50 p.m. to 2:00 p.m.	BREAK		
2:00 p.m. to 2:50 p.m.	Session 1 - Networked Society - Mrs. Gentile/Mr. Tozer Stright Hall, Room 112A, 112B		
2:50 p.m. to 3:10 p.m.	BREAK - Stright 112B		
3:10 p.m. to 4:00 p.m.	Session 2 - Networked Society - Mrs. Gentile/Mr. Tozer Stright Hall, Room 112A, 112B		

CYBERSECURITY CAMP DAILY SCHEDULE — DAY 5 - JUNE 16, 2017

	Middle School Students	High School Students	Teachers
9:00 a.m. to 9:50 a.m.	Session 1 - Connected and Protected: Protect Your Privacy When Sharing Information Online - Dr. McDevitt Stright Hall, Rooms 112 A, 112 B		
9:50 a.m. to 10:00 a.m.	BREAK		
10:00 a.m. to 10:50 a.m.	Session 2 - Connected and Protected: Protect Your Privacy When Sharing Information Online - Dr. McDevitt Stright Hall, Rooms 112 A, 112 B		
10:50 a.m. to 11:00 a.m.	BREAK		
11:00 a.m. to 11:50 a.m.	Session 1 - Decision Making Simulation - Dr. Fiddner HSS Building, Rooms 103,104,113,125		
11:50 a.m. to 1:00 p.m.	LUNCH - HSS 126		
1:00 p.m. to 1:50 p.m.	Session 2 - Decision Making Simulation - Dr. Fiddner HSS Building, Rooms 103,104,113,125		
1:50 p.m. to 2:00 p.m.	BREAK		
2:00 p.m. to 2:50 p.m.	Final Camp Competition Stright Hall, Rooms 112 A, 112 B		
2:50 p.m. to 3:10 p.m.	BREAK - Stright 112B		
3:10 p.m. to 4:00 p.m.	Post Camp Surveys, Award Certificate Ceremony Stright Hall, Rooms 112 A, 112 B		

ADVANCED CYBERSECURITY CAMP DAILY SCHEDULE

DAY 1 - JUNE 27, 2017

	Middle School Students	High School Students
9:00 a.m. to 9:50 a.m.	Welcome, Introduction to team members, orientation and logistics Stright Room 112 A/B	
9:50 a.m. to 10:00 a.m.	BREAK	
10:00 a.m. to 10:50 a.m.	Cybersecurity First Principles, accessing accounts, Arduino set up Stright Room 112 A/B and 107 A	
10:50 a.m. to 11:00 a.m.	BREAK	
11:00 a.m. to 11:50 a.m.	First Principles Outdoor Activity Outside Stright	
11:50 a.m. to 1:00 p.m.	LUNCH - STRIGHT 112 B	
1:00 p.m. to 1:50 p.m.	Networking Basics - Dr. Farag Stright Room 112 A/B	
1:50 p.m. to 2:00 p.m.	BREAK	
2:00 p.m. to 2:50 p.m.	Session 1 - Cybersecurity Movie - Intro and Planning Ms. Mishler Stright Room 112A	Session 1 - Drone Programming Dr. Farag Stright Room 327/329
2:50 p.m. to 3:10 p.m.	BREAK - STRIGHT 112 B	
3:10 p.m. to 4:00 p.m.	Session 2 - Cybersecurity Movie - Intro and Planning Ms. Mishler Stright Room 112A	Session 2 - Drone Programming Dr. Farag Stright Room 327/329

ADVANCED CYBERSECURITY CAMP DAILY SCHEDULE — DAY 2 - JUNE 28, 2017

	Middle School Students	High School Students
9:00 a.m. to 9:50 a.m.	Session 1 - Java Programming Dr. Farag — Stright Room 320	Session 1 - Cybersecurity Movie - Intro and Planning Ms. Mishler — Stright Room 112A
9:50 a.m. to 10:00 a.m.	BREAK	
10:00 a.m. to 10:50 a.m.	Session 2 - Java Programming Dr. Farag — Stright Room 320	Session 2 - Cybersecurity Movie - Intro and Planning Ms. Mishler — Stright Room 112A
10:50 a.m. to 11:00 a.m.	BREAK	
11:00 a.m. to 11:50 a.m.	Session 1 - Arduino Projects Dr. Smith — Stright Room 112A	Session 1 - Java Programming Dr. Farag — Stright Room 320
11:50 a.m. to 1:00 p.m.	LUNCH - STRIGHT 112 B	
1:00 p.m. to 1:50 p.m.	Session 2 - Arduino Projects Dr. Smith — Stright Room 112A	Session 2 - Java Programming Dr. Farag — Stright Room 320
1:50 p.m. to 2:00 p.m.	BREAK	
2:00 p.m. to 2:50 p.m.	Session 1 - Digital Forensics and Encryption Dr. Ezekiel/Dr. Farag — Stright Room 107A/112B	Session 1 - Robots Programming Dr. Rodger — Stright Room 320
2:50 p.m. to 3:10 p.m.	BREAK - STRIGHT 112 B	
3:10 p.m. to 4:00 p.m.	Session 2 - Digital Forensics and Encryption Dr. Ezekiel/Dr. Farag — Stright Room 107A/112B	Session 2 - Robots Programming Dr. Rodger — Stright Room 320

ADVANCED CYBERSECURITY CAMP DAILY SCHEDULE — DAY 3 - JUNE 29, 2017

	Middle School Students	High School Students
9:00 a.m. to 9:50 a.m.	Session 1 - Cybersecurity Movie Creation Ms. Mishler Stright Room 112A	Session 1 - Digital Forensics and Encryption Dr. Ezekiel/Dr. Farag Stright Room 107A/112B
9:50 a.m. to 10:00 a.m.	BREAK	
10:00 a.m. to 10:50 a.m.	Session 2 - Cybersecurity Movie Creation Ms. Mishler Stright Room 112A	Session 2 - Digital Forensics and Encryption Dr. Ezekiel/Dr. Farag Stright Room 107A/112B
10:50 a.m. to 11:00 a.m.	BREAK	
11:00 a.m. to 11:50 a.m.	Session 1 - Drone Programming Dr. Farag Stright Room 327/329	Session 1 - Arduino Projects Dr. Smith Stright Room 112A
11:50 a.m. to 1:00 p.m.	LUNCH - STRIGHT 112 A/B - Guest Speaker Dr. Lee - Watching the watchers: How information flows impact privacy in social computing	
1:00 p.m. to 1:50 p.m.	Session 2 - First Principles Outdoor Activity Dr. Farag Outside Stright	Session 2 - Arduino Projects Dr. Smith Stright Room 112A
1:50 p.m. to 2:00 p.m.	BREAK	
2:00 p.m. to 2:50 p.m.	Session 1 - Robots Programming Dr. Rodger Stright Room 320	Session 1 - Cybersecurity Movie Creation Ms. Mishler Stright Room 112A
2:50 p.m. to 3:10 p.m.	BREAK - STRIGHT 112 B	
3:10 p.m. to 4:00 p.m.	Session 2 - Robots Programming Dr. Rodger Stright Room 320	Session 2 - Cybersecurity Movie Creation Ms. Mishler Stright Room 112A

ADVANCED CYBERSECURITY CAMP DAILY SCHEDULE — DAY 4 - JUNE 30, 2017

	Middle School Students	High School Students
9:00 a.m. to 9:50 a.m.	Session 1 - Cybersecurity Movie Premier/Cybersecurity Board Game Development - Ms. Mishler Stright Room 112 A/B	
9:50 a.m. to 10:00 a.m.	BREAK	
10:00 a.m. to 10:50 a.m.	Session 2 - Cybersecurity Movie Premier/Cybersecurity Board Game Development - Ms. Mishler Stright Room 112 A/B	
10:50 a.m. to 11:00 a.m.	BREAK	
11:00 a.m. to 11:50 a.m.	Session 1 - Secure Coding Dr. Farag Stright Room 112A	Session 1 - Databases and Security Dr. Smith Stright Room 320
11:50 a.m. to 1:00 p.m.	LUNCH - STRIGHT 112 B	
1:00 p.m. to 1:50 p.m.	Session 2 - Secure Coding Dr. Farag Stright Room 112A	Session 2 - Databases and Security Dr. Smith Stright Room 320
1:50 p.m. to 2:00 p.m.	BREAK	
2:00 p.m. to 2:50 p.m.	Session 1 - Databases and Security Dr. Smith Stright Room 320	Session 1 - Secure Coding Dr. Farag Stright Room 112A
2:50 p.m. to 3:10 p.m.	BREAK - STRIGHT 112 B	
3:10 p.m. to 4:00 p.m.	Session 2 - Databases and Security Dr. Smith Stright Room 320	Session 2 - Secure Coding Dr. Farag Stright Room 112A

ADVANCED CYBERSECURITY CAMP DAILY SCHEDULE — DAY 5 - JULY 3, 2017

	Middle School Students	High School Students
9:00 a.m. to 9:50 a.m.	Session 1 - Cybersecurity Board Game Development/Play Ms. Mishler Stright Room 112A	Session 1 - NSA Day of Cyber Dr. Farag Stright Room 320
9:50 a.m. to 10:00 a.m.	BREAK	
10:00 a.m. to 10:50 a.m.	Session 2 - Cybersecurity Board Game Development/Play Ms. Mishler Stright Room 112A	Session 2 - NSA Day of Cyber Dr. Farag Stright Room 320
10:50 a.m. to 11:00 a.m.	BREAK	
11:00 a.m. to 11:50 a.m.	Session 1 - NSA Day of Cyber Dr. Farag Stright Room 320	Session 1 - Cybersecurity Board Game Development/Play Ms. Mishler Stright Room 112A
11:50 a.m. to 1:00 p.m.	LUNCH - STRIGHT 112 B	
1:00 p.m. to 1:50 p.m.	Session 2 - NSA Day of Cyber Dr. Farag Stright Room 320	Session 2 - Cybersecurity Board Game Development/Play Ms. Mishler Stright Room 112A
1:50 p.m. to 2:00 p.m.	BREAK	
2:00 p.m. to 2:50 p.m.	Session 1 - Final Camp Competition Stright Room 112 A/B	
2:50 p.m. to 3:10 p.m.	BREAK - STRIGHT 112 B	
3:10 p.m. to 4:00 p.m.	Session 2 - Post Camp Surveys/Certificates Stright Room 112 A/B	

Mrs. Gentile's Lesson Plan
I.U.P. June 13, 2017 9:00 –11:00am

Lesson Title: Introduction to Programming for High School Students

Summary: Through the use of www.Khanacademy.org, young people will explore the use of variables and conditionals to animate objects. Logical, sequential and critical thinking drive their mastery of efficient coding strategies. Basic examples of Cyber Security First Principles are applied throughout their learning.

Grade Band:	**Time Required:**
9-12	2 50-minute sessions

Lesson Learning Objectives/Outcomes

Upon completion of this lesson, students will be able to:
Evaluate algebraic expressions for given values, evaluate algebraic expressions for user-defined values, draw simple characters, create simple animations, set necessary parameters for functions, perform operations involving loops and conditional statements

Materials List:

Computers with Internet connection Classroom Board w/marker , eraser
Directions for which Khanacademy lessons to complete

How will you facilitate the Learning?

Sessions 1 and 2:

1) Students will log-in or create an account in Khanacademy. I will discuss the importance of never allowing a program to "save your password."
2) On Khanacademy, we will view a video from Pixar animation about how mathematics and coding are used to make computer-generated characters "come to life." (Welcome to Rigging + Math meets Artistry)
3) I will present students with the task: Create an animation of your first initial which translates, expands and changes color as if on a neon sign in Hollywood.
4) Students will brainstorm what it takes to carry out the task on a real sign, and we will record these thoughts on the board for reference throughout the session.
5) Students will go to www.khanacademy.org to watch videos and complete corresponding projects to work towards their "Name in Lights" task.
6) After some exploration time, it would be appropriate to discuss *Simplicity*, as it relates to the real javascript behind some of the predefined commands we are using, such as draw, fill, mouse x, mouse y, which the narrator says are "autocompleted."
7) As students complete each project at their own paces, I will check them off on my roster, as a means of informal assessment.

8) As the coding becomes more complicated with "Logic and If Statements" being the ultimate video lesson/topic.
9) Students will show off their "Name in Lights" projects so far, and assist one another with helpful suggestions.
10) Given time, we will conclude the session with a Quizizz to review the aspects of coding learned today as well as Cyber Security First Principles.

11) **Mapping to Cyber Security First Principles (in bold):**
Students will identify applications of the Cyber Security First Principles within Khanacademy's Javascript instruction:
Simplicity – addressed by the use of predefined commands where we users do not know the Javascript creating the function.
Domain Separation – addressed with advanced learners who know how to incorporate their own files into Khanacademy programs
Process Isolation - addressed when I proposed the possibility of working on Khanacademy and javascript programming while having one's grades open in one tab and listening to music on You-tube

Assessment of Learning:

TYPE	**Name/Description**
Project	Create a program w/specified requirements
Quizizz (on-line assessment)	On-line coding vocabulary practice, quiz, game

Accommodations:
Khanacademy's video lessons provide self-paced instruction and extra review materials at the end of each section.

Description of Extension Activities:
Students will be encouraged to pursue the lengthy list of javascript tutorials available on Khanacademy and to share their creations during camp breaks.

Acknowledgements:
GenCyber Security First Principles concepts
www.Khanacademy.org

Mrs. Gentile's Lesson Plan
I.U.P. June 12, 2017 2:00 – 4:00pm

Lesson Title: Introduction to Programming for Middle School Students

Summary: Through the use of object-oriented (block) coding, young people explore the use of variables and conditionals to animate objects. Logical, sequential and critical thinking drive their mastery of efficient coding strategies. Basic examples of Cyber Security First Principles are applied throughout their learning.

Grade Band:	**Time Required:**
6-8	2 50-minute sessions

Lesson Learning Objectives/Outcomes
Upon completion of this lesson, students will be able to:
Evaluate algebraic expressions, create animation, perform operations involving loops and conditional statements

Materials List:
Computers with Internet connection Classroom Board w/marker , eraser

How will you facilitate the Learning?
Session 1:
1) Students will join my Google Classroom, if possible on IUP's server.
2) I will present students with the task: Make a simple soccer shoot out animation that keeps track of goals and makes the "sprite" do a funny dance when it gets 10 goals.
3) Students will brainstorm what it takes to carry out the task in real soccer games, and this will be recorded for reference on the classroom board.
4) Students will go to www.scratch.mit.edu to create an account or login, with the strong reminder to never agree for a computer to "save password."
5) Initially, I will guide inexperienced students to observe the functions of various blocks that are available for our task. More experienced learners can create at their own paces. This is a good time to discuss *Simplicity*, as it relates to the real javascript behind the blocks we are using.
6) Students will be grouped by ability/experience with Scratch and then given time to explore the coding needed to complete the task. More experienced students will be challenged to use their best skills to impress us all.

Session 2:

1) Student will show their programs from Session 1 so that more advanced students can make suggestions to help everyone learn.
2) In session 2, depending upon time and the rate of acquisition in Session 1, students will play and "see inside" other programs made by people in the Scratch community.
3) For informal assessment, conduct a type of scavenger hunt with oral questions such as: Look for a loop that creates motion, one that tests boundaries, one that asks for user input, etc. Additionally, they will be asked to identify the use of variables in computational algorithms and other conditionals and to explain the function of those parameters.

4) **Mapping to Cyber Security First Principles:**
   Finally, given a written matching "quiz," students will pair up, using their GenCyber cards to identify applications of the Cyber Security First Principles within Scratch, with special emphasis placed upon these three:
   Simplicity – addressed by the use of Javascript applied in object-oriented programming
   Domain Separation – addressed with advanced learners who know how to incorporate their own files into Scratch programs
   Process Isolation - addressed when I proposed the possibility of working on Scratch while having one's grades open in one tab and listening to music on You-tube

Assessment of Learning:

TYPE	**Name/Description**
Project (Session 1)	Create a program w/specified requirements
Oral Questioning (Session2)	Identifying the use of parameters in programs
Writing Assignment (Session 2)	Given matching sheet, students will identify applications of Cyber Security First Principles in Scratch

Accommodations:

Grouping by ability for program creation
Grouping in mixed ability groups for Oral Questioning and Matching Sheet

Description of Extension Activities:

Students will be encouraged to create an additional Scratch program to share during camp breaks: Make a bouncing ball which when it touches a sprite, the sprite changes size and color. Then when the sprite is 4 times the original sprite, it will do some kind of silly dance.

Acknowledgements: GenCyber Security First Principles concepts

Introduction to Robotic AI Security Module

Module Learning Outcomes: (Please include explicit references to the submitted Grant Learning Outcomes – Appendix 3)

Camp Learning Outcomes

1. Demonstrate substantial understanding of the cybersecurity First Principles.

Numbers four, five, six and seven

2. Explore the use of basic operating systems commands on different platforms.

All robot OS can be compromised to alter what they were originally intended for

3. Explain different types of attacks on computing systems.

Robots can be attacked both physically and through cyber

4. Experiment with basic tools and techniques used to attack and/or defend systems.

Firewalls on robots defend them from vulnerabilities

5. Realize the importance of password and username management and apply effective approaches to increase their security.

iPhone and Android both control robots so their passwords can b compromised

6. Understand the basics of computer programming and experiment with simple programs.

Computer programming runs robots

7. Realize the importance of secure coding and apply effective techniques to improve security.

If trap doors or backdoors left in code than can be used maliciously

8. Engage in scenario-based learning that allows them to make educated decisions and take deliberate action online to prevent things from going wrong in the first place.

Use black tape versus white tape on Cublets robots to show wrong and right code

9. Uncover their own digital footprint and learn how to give themselves an “online make-over.”

See what other robots are available and what else these robots can do

10. Exemplify the ability to identify the authenticity and credibility of access requests.

Ask robots to play games

11. Develop skills needed to defeat various mal- and social engineering attacks.

Try to run robot without my phone. Will it work on theirs if download the app?

12. Apply the knowledge gained in solving real-world, scenario-based problems.

Interactive physical security with robots (diffuse a bomb)

13. Realize the important role humans play in the digital world and understand how to minimize accidental and intentional human errors.

Robots are not charged or app is not available

The Module addresses the following First Principles: (Please include explicit references to the First Principles - Appendix 1)

- #4: Domain Separation area of control of robots
- #5: Layering of computer security in both the robot and the control mechanism
- #7: Modularity or separation of the functionality of the robot into modules
- #6: Abstraction of the toy robot into a full scale physical security model

Description:

This module presents an easy-to-understand introduction to fundamentals of robotics, AI and security. The participants will be introduced to Cozmo, Cublets and the DJI drone. The robots will provide input, process and output examples of cybersecurity such as disarming a potential bomb, distinguishing between right and wrong security paths and aerial surveillance. Cybersecurity threats to both the control mechanisms and the actual robots will be explained, explored and demonstrated. Pattern recognition will be utilized to find a potential terrorist among a mountain of surveillance data.

Learner-centered classroom:

This module is designed to be taught in a highly interactive environment in which all attendees will be active participants in the learning process. To achieve that, one approach is to use a series of lab-based activities to enable students to "do it yourself" in order to enhance their comprehension of taught contents. Such lab activities include basics of AI, robotics and security applications. Participants will be encouraged to take the learning with them and apply the principles to their home networks and daily life. They will be encouraged to troubleshoot and secure their robotics for optimal performance.

Assessment:

This component of the module is designed to use a variety of formative assessment strategies in order to ensure that the students has acceptably achieved the Intended Learning Outcomes

(ILOs) of the module. Examples of the proposed techniques are use of discussion, questioning, peer-assessment, and constructive quizzes. For example, a carefully chosen set of questions on the covered topics can form a quiz given at the end of this module. After the students finish the quiz, all quiz questions will be reviewed and proper answers will be identified. This positively contribute to productive discussions in the classroom and increase the chances of students achieving higher degrees of learning.

Suitability to various groups:

The contents the module will be adapted to better fit the level of each of the proposed three groups. For the teachers group, topics covered will stress how the AI security concepts and techniques can be integrated into the K-12 curriculum in addition to covering advanced concepts such as robotic co-existence with the human world. The contents will also advance in the level of detail when being presented to the Middle school group compared to when being presented to the High school students.

Introduction to Networking Module

Module Learning Outcomes: (Please include explicit references to the submitted Grant Learning Outcomes – Appendix 3)

- #2: Explore the use of basic operation systems commands on different platforms.
- #4: Experiment with basic tools and techniques used to attack and/or defend systems.
- #8: Engage in scenario-based learning that allows students to make an educated decisions and take deliberate action online to prevent things from going wrong in first place.
- #12: Apply the knowledge gained in solving real-world, scenario-based problems.

The Module addresses the following First Principles: (Please include explicit references to the First Principles - Appendix 1)

- #4: Domain Separation
- #5: Layering
- #7: Modularity

Description:

This module presents an easy-to-understand introduction to fundamentals of networking. The participants will be introduced to the networking stack including both the OSI and Internet stack and the functionality of each layer and its importance. This will be used to illustrate the concepts of layering and modularity. Discussion of the DNS and ARP will be included to address the concepts of logical and physical. Various networking commands using the command line, windows based applications, and web applications will be used to illustrate the concepts and demonstrate the principles of networking. From a security perspective concept of how a firewall works (including both port based firewalls and application based firewalls) will be introduced. Other security concepts like proxy and whitelisting will also be introduced. Concepts related to encryption during network connections will be introduced. The importance of encrypting your wireless connection and use of VPNs will also be discussed. The module will adopt different pedagogies for middle and high school students. The Middle school students will have more emphasis on hands on learning while for high school students conceptual basis for what is being done will be stressed.

Learner-centered classroom:

This module is designed to be taught in a highly interactive environment in which all attendees will be active participants in the learning process. To achieve that, one approach is to use a series of lab-based activities to enable students to "do it yourself" in order to enhance their comprehension of taught contents. Such lab activities include basics of windows commands, use of windows built-in utilities, and some web based applications. Participants will be encouraged to take the learning with them and apply the principles to their home networks and daily life. They will be encouraged to troubleshoot and secure their networks for optimal performance.

Assessment:

This component of the module is designed to use a variety of formative assessment strategies in order to ensure that the students has acceptably achieved the Intended Learning Outcomes (ILOs) of the module. Examples of the proposed techniques are use of discussion, questioning, peer-assessment, and constructive quizzes. For example, a carefully chosen set of questions on the covered topics can form a quiz given at the end of this module. After the students finish the quiz, all quiz questions will be reviewed and proper answers will be identified. This positively contribute to productive discussions in the classroom and increase the chances of students achieving higher degrees of learning.

Suitability to various groups:

The contents the module will be adapted to better fit the level of each of the proposed student groups. The contents will advance in the level of detail when being presented to the High School group as compared to when being presented to the Middle school students. The Middle school students will have more emphasis on hands on learning while for High school students conceptual basis for what is being done will be stressed.

Lesson Plan

LESSON TITLE: Fake News

SUMMARY:

The instructor will give brief introduction to examples of fake news and how people can be influenced by false reports. The instructor will show how there are links built into text of media stories to track sources. The instructor will facilitate a discussion using the discussion questions. The instructor will show how there are links built into text of media stories to track sources. The instructor will create groups of students. One group will produce a fake news story about a candidate or celebrity or create a real news story about a candidate or celebrity based on material from an established news site. Groups will work independently, then share their stories with the class. The class will then vote which is the real story and

GRADE BAND:

- ☐ K-2
- ☐ 3-5
- ☑ 6-8
- ☐ High School

Time Required:

100 minutes

Lesson Learning Objective/Outcomes: Upon completion of this lesson, students will be able to:

-Learn what inspires fake news stories and how these stories rely on the nature of the internet for their success.
-Determine the effectiveness of fake news with reference to several issues (environment, national defense, etc).
-Discuss ways in which fake news can be mitigated without infringing on free speech.

Materials List:

Rose Eveleth, BBC, "How fake images change our memory and behavior":
http://www.bbc.com/future/story/20121213-fake-pictures-make-real-memories
Scott Shane, e New York Times, “From Headline to Photograph, a Fake News Masterpiece”:
https://www.nytimes.com/2017/01/18/us/fake-news-hillary-clinton- cameron-harris.html?

How will you facilitate the learning?

- Describe the Warm-up Activity/Focused Activity/Closure and/or Reflection
- Decribe the Teacher Instruction

- Discussion of playing the "telephone" game.
- Instructor Presentation
- Examination of links in news stories
- Discussion Questions
- Students Create Fake/Real News
- Student Presentation of Fake/Real News

This lesson includes:

- ☑ Mapping to Cyber Security First Principles
- ☑ Assessments
- ☑ Learning Objectives

Mapping to Cyber Security First Principles:

- [x] **Domain Separation**
- [ ] **Process Isolation**
- [ ] **Resource Encapsulation**
- [ ] **Modularity**
- [ ] **Least Privilege**
- [ ] **Abstraction**
- [ ] **Data Hiding**
- [ ] **Layering**
- [ ] **Simplicity**
- [ ] **Minimization**

Assessment of Learning:

TYPE (Examples Listed Below)	NAME/DESCRIPTION
Presentation	Fake/Real News Story Presentation
Project	Create a Fake/Real News Story
Writing Assignment	Write a Fake/Real News Story
Observation	Instructor observation during group work.
Walk Around	Instructor walk around during group work.
Oral Questioning	Discussion Questions
Assessment Quiz	Fake News Summary Quiz

Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)

Differentiation will be used to meet the needs of specific students.

Description of Extension Activity(ies):

Acknowledgements:

Cyber Politics: Politics and Fake News NICERC.org

Lesson Plan

LESSON TITLE: Fake News

SUMMARY:

The instructor will give brief introduction to examples of fake news and how people can be influenced by false reports. The instructor will show how there are links built into text of media stories to track sources. The instructor will facilitate a discussion using the discussion questions. The instructor will show how there are links built into text of media stories to track sources. The instructor will create groups of students. One group will produce a fake news story about a candidate or celebrity or create a real news story about a candidate or celebrity based on material from an established news site. Groups will work independently, then share their stories with the class. The class will then vote which is the real story and

GRADE BAND:

- ☐ K-2
- ☐ 6-8
- ☐ 3-5
- ☑ High School

Time Required:

100 minutes

Lesson Learning Objective/Outcomes: Upon completion of this lesson, students will be able to:

-Learn what inspires fake news stories and how these stories rely on the nature of the internet for their success.
-Determine the effectiveness of fake news with reference to several issues (environment, national defense, etc).
-Discuss ways in which fake news can be mitigated without infringing on free speech.

Materials List:

Rose Eveleth, BBC, "How fake images change our memory and behavior":
http://www.bbc.com/future/story/20121213-fake-pictures-make-real-memories
Scott Shane, e New York Times, “From Headline to Photograph, a Fake News Masterpiece”:
https://www.nytimes.com/2017/01/18/us/fake-news-hillary-clinton- cameron-harris.html?

How will you facilitate the learning?

- Describe the Warm-up Activity/Focused Activity/Closure and/or Reflection
- Decribe the Teacher Instruction

- Discussion of playing the "telephone" game.
- Instructor Presentation
- Examination of links in news stories
- Discussion Questions
- Students Create Fake/Real News
- Student Presentation of Fake/Real News

This lesson includes:

- ☑ Mapping to Cyber Security First Principles
- ☑ Learning Objectives
- ☑ Assessments

Mapping to Cyber Security First Principles:

- [x] **Domain Separation**
- [ ] **Process Isolation**
- [ ] **Resource Encapsulation**
- [ ] **Modularity**
- [ ] **Least Privilege**
- [ ] **Abstraction**
- [ ] **Data Hiding**
- [ ] **Layering**
- [ ] **Simplicity**
- [ ] **Minimization**

Assessment of Learning:

TYPE (Examples Listed Below)	NAME/DESCRIPTION
Presentation	Fake/Real News Story Presentation
Project	Create a Fake/Real News Story
Writing Assignment	Write a Fake/Real News Story
Observation	Instructor observation during group work.
Walk Around	Instructor walk around during group work.
Oral Questioning	Discussion Questions
Assessment Quiz	Fake News Summary Quiz

Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)

Differentiation will be used to meet the needs of specific students.

Description of Extension Activity(ies):

Acknowledgements:

Cyber Politics: Politics and Fake News NICERC.org

Physical Security Module

Module Learning Outcomes:

- #3: Explain different types of attacks on computing systems.
- #5: Realize the importance of password and username management and apply effective approaches to increase their security.
- #11: Develop skills needed to defeat various mal- and social engineering attacks.
- #12: Apply the knowledge gained in solving real-world, scenario-based problems.
- #13: Realize the important role humans play in the digital world and understand how to minimize accidental and intentional human errors.

The Module addresses the following First Principles:

- #4: Least Privilege
- #5: Layering
- #7: Information Hiding

Description:

This module on physical security will allow students the opportunity to develop an upgrade to the physical security system of an office building. These upgrades will included changes to policy, procedures and personnel actions within the organization. The upgrades suggested will be performance tested (validated numeric characteristics through computer simulation) to assess the impact that those upgrades have to the overall security posture of the organization. Students will be given an overview of the Design and Evaluation Process Outline (DEPO) as developed by the Department of Energy and how it applies to the protection of computer hardware and storage devices. Students will be challenged to recognize and understand security concerns from multiple perspectives, ranging from the insider threat, outsider threat, to threats involving the actual physical components. Exposure to a design methodology, associated system components modules, and basic security principles are featured in this module. Students will learn the importance of integrating people, procedures, and equipment for the protection of assets or facilities against theft, sabotage, or other malevolent human attacks. Students will be challenged to provide an upgrade of the security system for a simulated data storage facility. The importance of a sound security policy in the overall management of any organization is addressed.

Upon completion of the module students will:

- ❖ Possess an understanding of physical security system design and evaluation and how they apply to cybersecurity.
- ❖ Gain an understanding of the process of evaluating existing or proposed physical protection systems.
- ❖ Understand the policies and procedures needed to protect an organization and its computer resources from insiders who might do harm.

- ❖ Be able to develop a sound security policy that addresses the overall physical threat to an organization's computer resources.

Learner-Centered Classroom:

In this module students will work in teams to test and design an upgrade to an existing physical security system. Students will be challenged to upgrade a facility to increase its security posture. As part of this team building exercise, students will test their upgrade using computer modeling software. A major component of this module will be the introduction of the design and evaluation process as developed by the Department of Energy. Students will be instructed on how to apply this process for their own protection and also the protection of personal assets such as a laptop or computer system. Students will be introduced to the three types of adversaries: outsiders, insiders, and outsiders in collusion with insiders, and the unique challenges each brings. They will also be exposed to the three basic tactics that adversaries might utilize: force, stealth, and deceit.

Assessment:

This module will be assessed by the following criteria - how realistic, budget and cost, probability of interruption from the modeling software, and upgraded policies and procedures. Each group will be challenged to develop an upgrade to a scenario and each group's upgrade will be assessed using a modeling program which assesses its ability to defeat an adversary. Students will also critique the other groups' upgrades and offer suggestions on how improvements could have been made.

Suitability to various groups:

The principles introduced in this module are applicable for all three groups. The development of sound protection policies and procedures are important for all individuals. Understanding how to model this process and gaining insight into the impact of changes to these policies and procedures will help both students and teachers alike in safeguarding themselves, not just in the cyber world, but in their day-to-day activities.

Object Oriented Programming Game Module

Module Learning Outcomes:

Primary:

- #1: Demonstrate substantial understanding of the Cybersecurity First Principles.
- #2: Understand the basics of computer programming and experiment with simple programs.

Secondary:

- #5: Realize the importance of password and username management and apply effective approaches to increase their security.
- #12: Apply the knowledge gained in solving real-world, scenario-based problems.
- #13: Realize the important role humans play in the digital world and understand how to minimize accidental and intentional human errors.

The Module Addresses the following Cybersecurity First Principles:

- Encapsulation
- Abstraction
- Information Hiding
- Modularization
- Least Privilege
- Domain Separation
- Process Isolation

Description:

This module will exploit student's interest in computer games while laying a rudimentary understanding of Object Oriented Programing. Students will experiment with several games implemented in the Java programming language and make small modifications in logic and the instantiation of objects within each game. Emphasis will be placed on principles of abstraction, encapsulation, modularization, information hiding as applied to object oriented programming. In addition to the basics of object oriented programming, the danger of installing games from unknown sources will be made evident in a demonstration of covert interrogation of a computer and stealing of digital content. Through this demonstration students will recognize the importance of least privilege, domain separation, and process isolation.

Upon completion of the module students will:

- ❖ Gain further understanding of programming basics including variables, assignments, operators, loops, conditionals, and functions.

- ❖ Gain a cursory understanding of object oriented principles including class, encapsulation, inheritance, polymorphism, instance variables, methods and instantiation.

- ❖ Gain understanding of the risks of installing games and improve judgement on what and what not to install.

- ❖ Gain understanding of techniques to minimize risk in executing games.

Hands-On Classroom:

In this module students have hands on access to several games written in the Java programming language through the use of the Eclipse development environment. Following a short presentation on object oriented programming in relation to game design, instructor will lead examination and execution of several games. Students will modify constructor parameters of objects within each game and observe the results. Other instructor led modifications include instantiation of further objects within games and small changes to logic involving loops and conditionals. To minimize errors, most changes will be performed by uncommenting pre-supplied lines of code within each game. Students may perform their own experimental changes. While leading the students through the modifications, cybersecurity first concepts of abstraction, modularization, information hiding and encapsulation will be referenced and discussed.

Included in the module is a demonstration of covert interrogation and stealing of digital media. The demonstration involve having students create a few files on their computer's desktop folder prior to the presentation on object oriented games. One of the games when executed will in the background steal the files the student created and send them to a server. This action will only be revealed at the end of the object oriented programming presentation. While this demonstration is benign, the point will be made that games could behind the scenes perform malicious activities that could have drastic consequences. Students will then be asked for steps they could take to minimize the risk. In the course of this discussion cybersecurity first principles of least privilege, domain separation, and process isolation will be injected into the discussion.

Assessment:

This module will be assessed by the pre/post test for the camp. In addition reaction to the covert interrogation and digital stealing demonstration will be noted in the instructor's post camp report which will include a list of actions suggested by the students to reduce the risk in executing games.

Suitability to various groups:

The principles introduced in this module are applicable for both the middle school and high school as the modifications to the programs will primarily be accomplished through uncommenting lines, copy/paste, and change of very limited text. It is anticipated that high school students may proceed at a quicker pace. In the event the primary content is complete, secondary examples may be used. Both groups will experience the covert interrogation and digital stealing.

How the Teachers and Students groups will be interacting:

This module is targeted for the student groups. Teachers may be invited to observe the presentation. The content will be available to teachers following the camp to use in their own demonstrations.

Introduction to Network Security Module

Module Learning Outcomes: (Please include explicit references to the submitted Grant Learning Outcomes – Appendix 3)

- #1: Demonstrate substantial understanding of the cybersecurity first principles.
- #3: Explain different types of attacks on computing systems.
- #4: Experiment with different tools and techniques used to attack and/or defend systems.
- #13: Remember the important role humans play in the digital world and understand how to minimize accidental and intentional human errors.

The Module addresses the following First Principles: (Please include explicit references to the First Principles - Appendix 1)

- #1: Domain Separation
- #4: Least Privilege
- #5: Layering
- #7: Information Hiding
- #10: Minimization

Description:

This module starts by a brief overview of the fundamental working principles of computer networks then introduces various types of attacks (malicious software, password guessing, man-in-the-middle, replay, session hijacking, and Denial of Service (DoS)), effective countermeasures (firewalls and intrusion prevention systems, encryption and the role it plays in securing information while in transit or in storage), attackers and their varying motivations. . Application of several cybersecurity First Principles will be incorporated, e.g., layering in design of secure network environments and least privilege to help minimize the possibilities of attacking various network components. While discussing attackers and their motivations, ethical concepts will be discussed to include the controversies associated with hacktivism.

Learner-centered classroom:

This module is designed to be taught in a highly interactive environment in which all attendees will be active participants in the learning process. To achieve that, one approach is to use a series of lab-based activities to enable students to "do it yourself" in order to enhance their comprehension of taught contents. Such lab activities include network reconnaissance, password cracking tools, and traffic analysis. In addition, we are using a number of simulating activities that highly promote participants' engagement and make them positive contributors to the learning process. Another approach is to use mobile technology to maximize participant involvement through the use of their own smart phones (BYOD) and/or the provided mobile devices. Services such as, Kahoot, tophat and Poll Everywhere will be used to achieve this.

Assessment:

This component of the module is designed to use a variety of formative assessment strategies in order to ensure that the students has acceptably achieved the Intended Learning Outcomes (ILOs) of the module. Examples of the proposed techniques are use of discussion, questioning, and constructive quizzes. For example, a carefully chosen set of questions on the covered topics can form an interactive quiz administered via online tool such as Kahoot and given towards the end of this module. Such environment promote competitiveness and encourage students to be involved. After the students finish the quiz, all quiz questions will be reviewed and proper answers will be identified. This positively contribute to productive discussions in the classroom and increase the chances of students achieving higher degrees of learning.

Suitability to various groups:

In this module, the examples used and scenarios presented will have difficulty levels suitable for each of the groups. Topics covered will stress how these fundamentals of network security can be applicable to K-12 environments. Moreover, the contents presented and hands-on used will advance in the level of difficulty when being presented to the Middle school group compared to when being presented to the High school students.

Lesson Plan

LESSON TITLE: Networked Society

SUMMARY:

For this lesson the teacher will need to introduce the term networked society to the students and give them an opportunity to discuss how the networked society can be used. The main goal for the lesson is for the students to discuss and define the networked society. This goal will be accomplished by looking at the history of technology advancements with focus on a specific example, phones, and how these advancements have led to the creation and development of the networked society.

GRADE BAND:

- ☐ K-2
- ☐ 6-8
- ☐ 3-5
- ☑ High School

Time Required:

100 minutes

Lesson Learning Objective/Outcomes: Upon completion of this lesson, students will be able to:

Discuss the networked society in order to understand the purpose of the networked society.

Materials List:

Video

? Now I get the Networked Society found at http://www.youtube.com/watch?v=L5Pxenw7UFA

Presentation

?Networked Society

How will you facilitate the learning?

- Describe the Warm-up Activity/Focused Activity/Closure and/or Reflection
- Decribe the Teacher Instruction

To get students motivated for the lesson they will be asked a few questions related to cell phones and smart phones. The students will be introduced to the history of the phone, starting with Morse code & the telegram and the development up to the modern smart phone. The teacher will spend some time focusing on the major inventions and providing some history. Once the history of the smart phone is finished the teacher should refocus the students on the unique features of smart phones. After going over smart phones the teacher will have students define the networked society in their own words. After students have defined the networked society they will be shown the Ericsson video that gives a definition

This lesson includes:

- ☑ Mapping to Cyber Security First Principles
- ☑ Learning Objectives
- ☑ Assessments

Mapping to Cyber Security First Principles:

☐ **Domain Separation**	☑ **Abstraction**
☐ **Process Isolation**	☐ **Data Hiding**
☐ **Resource Encapsulation**	☐ **Layering**
☐ **Modularity**	☑ **Simplicity**
☐ **Least Privilege**	☐ **Minimization**

Assessment of Learning:

TYPE (Examples Listed Below)	NAME/DESCRIPTION
Presentation	Networked Society Solution Presentation
Project	Networked Society Solution Project
Observation	Instructor Observation Durring Group Work
Walk Around	Instructor Walk Around Durring Group Work
Oral Questioning	Disucssion Questions
Assessment Quiz	Networked Society Summary Quiz

Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)

Differentiation will be used to meet the needs of specific students

Description of Extension Activity(ies):

Cyber Communities: Hisotry of The Networked Society www.NICERC.org

Acknowledgements:

Connected and Protected: Protect Your Privacy When Sharing Information Online

Module Learning Outcomes:

Participants will:

- Consider the ways that online activity involves the intentional and unintentional exchange of information.
- Discuss a practices that put you at risk and keep you safe
- Demonstrate knowledge of correct and safe online behaviors through successful completion of games and simulations
- Engage in scenario based learning that allows them to make educated decisions and take deliberate action online to prevent things from going wrong in the first place
- Consider current online sharing practices and consider how they might be revised to improve privacy
- Realize the importance humans play in the digital world and understand how to minimize accidental and unintentional human errors
- Apply knowledge gained to the development of documents/activities designed to share online privacy preservation and safe computing practices

The Module addresses the following First Principles:

- Layering
- Domain separation
- Least privilege
- Simplicity

Description

These days people get most of their information online. That can be easy, fast, and inexpensive. Accessing it can also be a threat to user privacy. When you gather information, you are almost always sharing information about yourself in the process. Third parties including scammers, hackers, and identity thieves can in turn use that information. They may use it to trick you into sharing passwords, bank account numbers, and other information that you want to keep private.

Are you doing all you can do to protect your information when you gather and share information online? What can you do to increase security of your personal information? How might information protection best practices be shared with others so they can be secure online as well?

In this module we will invite participants to explore the many ways that people share personal information every day online, both intentionally, and unintentionally. We will consider the negative impacts of such information sharing on both individuals and groups. We will work in small groups to create a list of recommendations for staying private and safe when sharing information online, and techniques for sharing these recommendations with friends and family.

Learner Centered Classroom

High school students and teachers will be briefly introduced to principles through active learning techniques including pre-and post-session surveys, short engaging videos, and share and compare activities.

Assessment

Participants will be asked to engage with the material and each other frequently during the session. They will then work in groups to practice principles presented. High school students will be asked to develop recommendations for safe online information sharing and techniques for sharing such information effectively with family and friends. Teachers will be asked to develop recommendations for safe online information sharing and techniques for sharing such information effectively with their students.

Suitability to Various Groups

Modules will include material accessible to all groups on some level and be offered simultaneously for all groups. The culminating activities will be similar, but adapted to the interests of the different levels of learners.

Teacher Student Interaction

Students and teachers will participate in similar learning activities during the information exploration section of the module. Students and teachers will participate in a discussion of recommendations and best techniques for sharing information during culminating session.

Decision Making Simulation

Module Learning Outcomes.

Participants will:

1. Apply the knowledge gained throughout the week's instruction to understand better the cause and effect of cybersecurity practice by reacting to and solving real-world, scenario-based unexpected inimical events
2. Recognize different types of attacks on computing systems and the ensuing "real world" problems these attacks can produce
3. Hypothesize the connectivity between the various unexpected events and develop courses of action to respond to the larger connected implication.
4. Develop educated skills needed for decision making to prevent and defeat various mal- and social engineering attacks activity in the first place
5. Connect the important role humans play in the digital world to what might happen and understand how to minimize accidental and intentional human errors

The Module addresses the following First Principles:

- least privilege,
- process isolation,
- domain separation
- modularity, and
- abstraction

Description

This module is a decision making simulation that addresses the least privilege, modularity, process isolation, and abstraction cybersecurity First Principles by illustrating the essential role and fallibility of the human user in cybersecurity, the interconnectivity and aggregation of activity globally, and the "real world" implications of the lack of cybersecurity practice. The exercise demonstrates the ambiguity of the origin and intention of interruption to and/or corruption of digital media using "real world" situations.

Participants as an entire group will be informed of various cyberactivities occurring globally over a period of time with the international security situation becoming increasingly more perilous. A brief description of the interconnectivity of critical infrastructure will be provided to inform novices of the critical synthesis of aggregated activities occurring in one infrastructure.

The will then be divided into teams to assess the situation and prepare recommendations to a "decision maker" on how to respond to the aggregated activities and which Cybersecurity First Principles are violated and how. The recommendations will be presented to the assembled entire group to provide all participants the opportunity to observe and evaluate and respond to each group's different assessment and analysis of and recommendations for responding to the individual and aggregated activities.

Learner Centered Classroom

All participants will be actively learning as part of the different groups' assessing the situation and preparing the group's recommendation and Cybersecurity First Principles involved. Since this is a combination camp, the middle and high school students will be integrated into groups incorporating both. After an initial short introduction of the global situation, the different teams will be provided group work space to assess and analyze the situation and prepare their recommendations to the decision maker. Teachers will serve as an "informational resource" and provide supervision (as needed) for the student groups.

The first task for each group will be to organize to solve the problem provided them. Then each participant not only will be participating as part of the group's efforts to assess and analysis the situation and prepare recommendations for addressing the identified activities, but completing different tasks as assigned by the leadership core of the group. Not only does each group have to assess the situation and develop responses to what is happening and the cybersecurity First Principles involved, but each group also must prepare an oral briefing of their recommendations to the decision maker and the other groups.

Assessment

Assessment will be continuously conducted by both the teachers with each group and by the instructor and the instructor's knowledgeable assistant instructors. The instructor and the assistant instructors will continuously move between the groups assessing the groups' progress and providing knowledgeable guidance, advice, and recommendations. Each group's recommendation and oral presentation will be provided "feedback" by the instructor and other student and teacher participants at the end of the oral presentation.

Suitability to Various Groups

This activity is designed to occur at the end of the camp's instruction so all participants should have some knowledge of the cybersecurity First Principles and the different types of attacks of the information network. The middle school students should have at least a summary knowledge of cybersecurity's First Principles if not the implications of the global situation being assessed and analyzed. The middle school students should also be able to contribute to preparation of the oral briefing to be delivered at the end of the assessment and analysis at the very least.

The high school students should have better than summary knowledge not only of cybersecurity's First Principles but also the implications of the scenario's aggregated cyberactivities from the camp's instruction and greater learning from an additional 3-5 years of education. High school students will be able to exercise this greater knowledge to organize, assess, analyze, synthesize, and develop responses to the cyberactivities and their implications.

Teachers have the experience of supervising middle and high school students, monitoring classroom activity, and guiding students in searches for solutions from data given.

Teacher Student Interaction

All participants will have interaction with the primary and assistant instructors during the entire simulation. All will receive the data about the global situation and the cyberactivity happening and their instructions. Middle and high school students will have the opportunity to interact with the instructor and assistants as they circulate between working groups assessing progress and providing advice and guidance. Teachers will further have access to the instructor and assistants for additional expertise on the situation depicted and advice on what is expected of the students at the end of the work session.

Students will have access to their assigned teacher "experts" during the group work session for advice, guidance, and recommendations on what to do and how to do it.

Transforming your Curriculum: A Cyber Security Toolbox for Teachers

Developed by Crystal Machado

Module Learning Outcomes:

#8: Engage in scenario-based learning that allows them to make educated decisions and take deliberate action online to prevent things from going wrong in the first place.
#12: Apply the knowledge gained in solving real-world, scenario-based problems.
#13: Remember the important role humans play in the digital world and understand how to minimize accidental and intentional human errors.

The Module addresses the following First Principles:

#4: Least Privilege
#5: Layering
#6: Abstraction
#7: Information Hiding
#9: Simplicity of Design
#10: Minimization

Description:

As digital devices like iPads and cell phones gain popularity with teens and young adults' educators need to become better informed about how they can teach students how to use these devices as learning tools. This module will provide middle and high school teachers with essential content related to digital citizenship. They will be provided with access curricular developed by three different groups, provided with an opportunity to examine and test out the material, and create a Google Site that includes grade and subject specific content that they can use with their students.

Upon completion of the teachers will:

- Describe Ribble's nine elements of digital citizenship.
- Describe the benefits of using interactive digital games to enhance students' cyber security skills.
- Locate free resources (interactive games, articles, videos etc.) developed by cybersecurity experts and educators that they can use in their classrooms.
- Describe how they will use these resources in their classroom.

Learner-Centered Classroom:

The instructor will create a highly interactive environment that provides middle and high school teachers with an opportunity to interact with the content and each other. She will use direct

instruction, structured discovery and informal instruction to deliver the content. She will include whole group activities as well as small group activities structured within and across instructional levels (middle and high).

During the first hour the instructor will use an interactive web-based software to (a) engage teachers in a self-evaluation of access to and use of digital tool (b) facilitate a discussion of Ribble's essential elements of digital citizenship. She will then use a modified version of the jigsaw approach to provide teachers with an opportunity to (a) individually test out an interactive digital game that involves decision making (b) discuss the outcomes of the different games and how these games can be integrated into the curriculum. During the second hour the instructor will engage students in a Digital Scavenger Hunt for cyber security curriculum resources. This will require teachers to (a) visit the websites provided by the instructor (b) identify resources that they can use with their respective classes (c) create a Google Site page that includes grade specific resources they plan to use with their students. They will be invited to share their Google Site page with peers during the last ten minutes of the session.

Assessment:

She will formatively assess teachers in a number of ways during the first hour. First, with the help of the interactive web-based software the instructor will evaluate the ways in which teachers integrate digital citizenship into the curriculum. She will then informally observe teachers' engagement in the digital game and the discussion that follows. She will use a whole group format to elicit teachers' reactions to the different games and the ways in which they plan to integrate them into the curriculum. During the second hour the instructor will informally observe teachers' as they engage in the Digital Scavenger Hunt. She will formally assess the Google Site pages that teachers create and present during the last ten minutes.

Suitability to various groups:

This module includes a wide range of cyber security resources relevant to the needs of middle and high school students. The Google Site page that each teacher creates will target the level that he/she teaches. Teachers will benefit from viewing the different Google Site pages created by their peers.

How the Teachers and Students Groups will be Interacting:

Not applicable. This session does not include students.

a.

Using Social Media for Teaching, Learning and Reputation Management

Developed by Crystal Machado

Module Learning Outcomes:

#1: Demonstrate substantial understanding of the cybersecurity first principles.
#5: Realize the importance of password and username management and apply effective approaches to increase their security.
#8: Engage in scenario-based learning that allows them to make educated decisions and take deliberate action online to prevent things from going wrong in the first place.
#9: Uncover their own digital footprint and learn how to give themselves an "online make-over."
#10: Exemplify the ability to identify the authenticity and credibility of access requests.
#12: Apply the knowledge gained in solving real-world, scenario-based problems.
#13: Remember the important role humans play in the digital world and understand how to minimize accidental and intentional human errors.

The Module addresses the following First Principles:

#4: Least Privilege
#5: Layering
#6: Abstraction
#7: Information Hiding
#9: Simplicity of Design
#10: Minimization

Description:

Social media has gained considerable popularity with teens, young adults and professionals. While students have limited access to social media like Twitter, Facebook, Snapchat and Instagram at school, they often use social media to interact with peers and family members outside of the classroom. Students' and teachers' safety needs will be better served if they are informed about the ways in which these tools can be used in a safe and secure manner to provide opportunities for professional growth, enhanced home-school communication, and conversations that allow learning to continue beyond allotted class times.

This module will provide middle and high school teachers with an opportunity to engage in meaningful activities and discussions regarding the appropriate use of social media to build a strong positive online reputation. The instructor will:

a. Use photographs from Facebook, twitter and Instagram to engage teachers in a dialogue about the consequences of appropriate and inappropriate posts.
b. Engage teachers in an "Online Reputation Assessment and Management" activity.
c. Provide teachers with an opportunity to work in small groups to develop and post 5 developmentally appropriate instructional activities (across grade levels) that include the use of a social media tools on their assigned Google Site page.
d. Present and critique each other's strategies.

Upon completion of the teachers will:

- ❖ Describe the positive and negative circumstances that can impact online reputations.
- ❖ Describe the changes they will make to the personal information they currently have online.
- ❖ Have access to developmentally appropriate instructional activities that employ social media tools across grade levels and content areas.

Learner-Centered Classroom:

The instructor will create a highly interactive environment that provides middle and high school teachers with an opportunity to interact with the content and each other. She will use direct instruction, structured discovery and informal instruction to deliver content. Instruction will include whole group activities as well as small group activities structured within and across instructional levels (middle and high).

During the first-hour the instructor will use photographs from new reports, Facebook, Instagram and Twitter and informational handouts to stimulate a discussion about the consequences of appropriate and inappropriate posts on the web. She will then engage teachers in a Reputation Assessment and Management activity that allows them to uncover their own digital footprint. They will discuss several methods that can be used to modify and/or safeguard their digital footprint and that of their students. After the break, teachers will work in instructional level groups. They will pick one of the six social media tool, browse the web to learn more about how other teachers use the tool, and then list five developmentally appropriate instructional strategies that involve use of the tool (across grade levels and content areas) on their assigned Google Site page. Groups will present their Google Site page to the larger group for peer critique.

Assessment:

A series of formative and summative assessments will be used during the module. First, the instructor will use probing questions to evaluate teachers' interpretation of photographs that depict positive and negative use of social media. Next, the instructor will informally interact with teachers while they are engaging in the Reputation Assessment and Management Activity and the small group activity. During their oral presentation, the instructor will formally evaluate their Google Site page which includes instructional strategies related to different social media tools. .

Suitability to various groups:

This module introduce middle and high school teachers to a wide range of social media tools. The strategies that teachers design in instructional level groups will target both middle school and high school students.

How the Teachers and Students Groups will be Interacting:

Not applicable. This session does not include students.

Mrs. Gentile's Lesson Plan
I.U.P. June 13, 2017 2:00 - 4:00 pm

Lesson Title: Learning Through Teacher-Made Games and Activities

Summary:
Teachers will be given time to explore and develop engaging strategies for embedding Cyber Security First Principles into their classrooms, to be tested tomorrow when combined with students and then culminating on Day 4 with the creation of on-line sharing tools to share their well-developed plans with others.

Grade Band:
PK – 12 Teachers

Time Required:
2 50-minute sessions

Lesson Learning Objectives/Outcomes
Upon completion of this lesson, teachers will be able to:

- Develop at least one GenCyber card game beyond the given suggestions
- Create an active game to practice the Cyber Security Principles
- Apply Webb' Depth of Knowledge levels to all activities and assessments
- List ways teachers can briefly apply the Cyber Security Principles when using technology in front of students in their classrooms

Materials List:
GenCyber Cards
Webb's DOK reference charts
Guided Notes for class ideas (on a Google Slide)
Pens
Marzano's 6-step Vocab handout
Bloom/Marzano Taxonomy

How will you facilitate the Learning?
Session 1:

1) Begin with a "Word Wall" where key ideas/connections can be accumulated as our discussions progress, encouraging teachers to keep such an active reminder in their classrooms and to employ Marzano's 6-step process to vocabulary teaching, shared and modeled here today.
2) Briefly discuss how the complex Cyber Security Principles terms could be made simpler for younger learners through physical classroom analogies.
3) If not already done earlier in the week, play the originally suggested GenCyber card game. Provide teachers with the answers for their answer card in the deck.
4) Then ask the teachers to think of common card games that we could play with the GenCyber deck (e.g. Rummy w/3 of a kind, GoFish w/8-card hand, War, Poker, Crazy 8s, Solitaire)
5) Demonstrate 1 way to play an active game, Red Rover, with the Cyber Security Principles (layering, modularity, domain separation, least privilege)
6) Then ask the teachers to think of common active games that we could adapt to practice the Principles (e.g. Capture the Flag, Duck, Duck , Goose; Mother May

I, 7 UP, Freeze Tag, Scavenger Hunt, Egg Hunt, Nerf Wars, Obstacle Courses, Trashketball)

7) While going to break, invite teachers to offer key words or concepts we can add to our Word Wall.

Session 2:

1) Briefly discuss Piaget's contribution to our understanding of differentiating for students and encouraging higher order thinking. Refer to the Bloom-Marzano Hybrid Taxonomy, already distributed. Transition into the more currently used phrase "DOK levels," coined by Dr. Norman Webb, and distribute that handout.
2) With DOK prompts, make the following suggestions for classroom activities:
   DOK 1 – play Win, Lose, Draw with the Principles
   DOK 2 – Categorize which Principles are related to hardware, software or processes
   DOK 3 – Critique the use of Cyber Security Principles in our school OR Investigate other Cyber Security Principles on the Internet
   DOK4 – Apply Cyber Security Principles to the creation of an on-line game like Kahoot (already seen this week)
3) Given time, allow the teachers to share how other DOK prompts can use Cyber Security Principles
4) Finally, discuss how our own use of technology in the classroom can lead to impromptu lessons about Cyber Security Principles, without having to make complete lessons about the topic.

Mapping to ALL Cyber Security First Principles:

Domain Separation	**Abstraction**
Process Isolation	**Data Hiding**
Resource Encapsulation	**Layering**
Modularity	**Simplicity**
Least Privilege	**Minimization**

Assessment of Learning:

TYPE	**Name/Description**
Writing Assignment	Word Wall of Cyber Security ideas and concepts
Oral Questioning	Teachers offer additional examples of each topic Demonstrated
Guided Notes	Completed as we discuss each activity

On-line Writing Assignment (Google Slide) To be completed on Day 4

Accommodations:

N/A

Description of Extension Activities:

N/A

Acknowledgements:

Dr. Norman Webb for DOK chart
Ms. Myra Collins for DOK chart
NSA – Gen Cyber cards

Mrs. Gentile's Lesson Plan
I.U.P. June 14, 2017 2:00 - 4:00 pm

Lesson Title: On-Line/Tech-Based Engagement and Assessment

Summary:
Based upon pre-camp survey data, teachers will be given time to explore and develop engaging on-line strategies for teaching and assessing Cyber Security First Principles, culminating on Day 4 with the creation of an on-line sharing tool. Kahoot, Quizlet, Quizizz, Edpuzzle, Google Forms and possibly Hyperdocs will be explored as effective assessment methods with immediate feedback for students.

Grade Band:
PK – 12 Teachers

Time Required:
2 50-minute sessions

Lesson Learning Objectives/Outcomes
Upon completion of this lesson, teachers will be able to:

- Create an active, on-line game to practice the Cyber Security Principles
- Search and critique popular on-line learning games for resources already made
- Create a video lesson for review, assessment or to flip the classroom
- Observe how I use Google Classroom to organize work/activities, retention – building materials, videos, games, assignments
- Apply Webb's Depth of Knowledge levels to all activities and assessments
- List ways teachers can briefly apply the Cyber Security Principles when using technology in front of students in their classrooms

Materials List:
Chromebooks
Webb's DOK reference charts
Google Accounts/Knowledge of Drive
Guided Notes about On-Line Games

How will you facilitate the Learning?
Session 1:

1) Review Kahoot (previously played in week) for variations, ways to customize
2) Play Quizizz to see its individual assessment records and ways to customize
3) Play Quizlet and Quizlet.live on the Chromebooks, both vocabulary-building and communication/collaboration tools

Session 2:

4) Demonstrate Edpuzzle; Discuss the benefits of Assessment, Retention-building, Flipping the Classroom
5) Demonstrate Google Forms by showing my GenCyber teacher or student survey data, my Friday review forms, how to make quizzes from forms
6) Given time, further develop hyperdocs from earlier session (Includes question, links for discovery, create authentic assessment) using Kidsdiscover.com

Mapping to ALL Cyber Security First Principles:

Domain Separation	**Abstraction**
Process Isolation	**Data Hiding**
Resource Encapsulation	**Layering**
Modularity	**Simplicity**
Least Privilege	**Minimization**

Assessment of Learning:

TYPE	**Name/Description**
Oral Questioning	Teachers offer additional examples of each topic demonstrated
Guided Notes	Completed as we discuss each activity

On-line Writing Assignment (Google Slide) To be completed on Day 4

Accommodations:

N/A, except that some teachers' districts do not have a contract for GAFE, but still have access to Google Docs

Description of Extension Activities:

It would be wonderful if we could work as a team to make a GenCyber Hyperdoc to share on Day 4.

Acknowledgements:

Lisa Highfill, Kelly Hitton, Sarah Landis for Hyperdoc information

Mrs. Gentile's Lesson Plan
I.U.P. June 15, 2017 11:00 – 11:50 am, 1:00-1:50 pm

Lesson Title: Using Google Apps to Share Ideas

Summary:
After a full week of learning concepts about the GenCyber Security Principles, teachers will be given this time to more fully develop their Google Site from Dr. Machado's session, create shared documents with other participants through Google Docs, contribute to a Team Drive Folder (if possible on IUP's server) and possibly create/revise a hyperdoc for students to explore at their respective grade levels or in specific subject areas.

Grade Band:
PK – 12 Teachers

Time Required:
2 50-minute sessions

Lesson Learning Objectives/Outcomes
Upon completion of this lesson, teachers will be able to:

- Create an on-line resource of ways to organize practice methods for mastering the Cyber Security Principles, including Google Sites and Google Docs and Slides, and to compile the week's big ideas
- Collaborate with other teachers by commenting with one another on their slides
- Observe how I use Google Classroom to organize work/activities, retention – building materials
- In grade level teams or subject-specific teams, create a Hyperdoc to be used with students studying the Cyber Security Principles
- Review ways teachers can briefly apply the Cyber Security Principles when using technology in front of students in their classrooms

Materials List:
Chromebooks
Hyperdoc How-To's
Google Accounts/TEAM DRIVE/Google Site
Notes from all sessions from the camp

How will you facilitate the Learning?
Session 1:

1) Introduce the concept of a Team Folder, as one Google possibility for sharing information with one's colleagues
2) Introduce the Google Slide I made with preset heading (previously shared w/participants). Discuss how the principle of *least privilege* is involved here, but again, is another method for sharing the Cyber Security Principles with everyone on one's school team.
3) Ask for contributions to each slide, and show how the commenting feature can be applied to provide immediate feedback to students

Session 2:

1) Demonstrate hyperdocs (Includes question, links for discovery, create authentic assessment) using Kidsdiscover.com and other resources (TBD).
2) Have teachers assemble into grade-level or subject area groups.
3) Begin the process of creating one Hyperdoc to help students actively discover various depths of knowledge about Cyber Security Principles. Hyperdocs can include teacher-made games, vocabulary building through Marzano's 6 step process, on-line explorations for acquiring new information or on-line games for building retention. Hyperdocs can be designed to accommodate different types of learners, as well. The use of Hyperdocs practices the Cyber Security Principles of *Minimization,* where students are guided to explore only certain areas of the Internet.
4) Finally, given time, we will brainstorm ways we can share the week's learning with our colleagues at our home schools.

Mapping to ALL Cyber Security First Principles:

Domain Separation	**Abstraction**
Process Isolation	**Data Hiding**
Resource Encapsulation	**Layering**
Modularity	**Simplicity**
Least Privilege	**Minimization**

Assessment of Learning:

TYPE	**Name/Description**
On-line Writing Assignment (Google Slide)	Compiled Concepts from the GenCyber Camp, to be shared
Hyperdoc Creation in Small Groups	Discovery activity for students at various levels in various subjects

Accommodations:

N/A

Some teachers' districts do not have a contract for GAFE, but still have access to Google Docs. These teachers can just plan on email attachments and making copies to share their knowledge gained from the camp.

Description of Extension Activities:

On-going encouragement to contribute to our Google Slide resource compilation

Acknowledgements:

Lisa Highfill, Kelly Hitton, Sarah Landis for Hyperdoc information

Lesson Plan

LESSON TITLE: Networked Society

SUMMARY:

For this lesson the teacher will need to introduce the term networked society to the students and give them an opportunity to discuss how the networked society can be used. The main goal for the lesson is for the students to discuss and define the networked society. This goal will be accomplished by looking at the history of technology advancements with focus on a specific example, phones, and how these advancements have led to the creation and development of the networked society.

GRADE BAND:

- ☐ K-2
- ☐ 6-8
- ☐ 3-5
- ☑ High School

Time Required:

100 minutes

Lesson Learning Objective/Outcomes: Upon completion of this lesson, students will be able to:

Discuss the networked society in order to understand the purpose of the networked society.

Materials List:

Video

? Now I get the Networked Society found at http://www.youtube.com/watch?v=L5Pxenw7UFA

Presentation

?Networked Society

How will you facilitate the learning?

- Describe the Warm-up Activity/Focused Activity/Closure and/or Reflection
- Decribe the Teacher Instruction

To get students motivated for the lesson they will be asked a few questions related to cell phones and smart phones. The students will be introduced to the history of the phone, starting with Morse code & the telegram and the development up to the modern smart phone. The teacher will spend some time focusing on the major inventions and providing some history. Once the history of the smart phone is finished the teacher should refocus the students on the unique features of smart phones. After going over smart phones the teacher will have students define the networked society in their own words. After students have defined the networked society they will be shown the Ericsson video that gives a definition

This lesson includes:

- ☑ Mapping to Cyber Security First Principles
- ☑ Learning Objectives
- ☑ Assessments

Mapping to Cyber Security First Principles:

☐ **Domain Separation**	☑ **Abstraction**
☐ **Process Isolation**	☐ **Data Hiding**
☐ **Resource Encapsulation**	☐ **Layering**
☐ **Modularity**	☑ **Simplicity**
☐ **Least Privilege**	☐ **Minimization**

Assessment of Learning:

TYPE (Examples Listed Below)	NAME/DESCRIPTION
Presentation	Networked Society Solution Presentation
Project	Networked Society Solution Project
Observation	Instructor Observation Durring Group Work
Walk Around	Instructor Walk Around Durring Group Work
Oral Questioning	Disucssion Questions
Assessment Quiz	Networked Society Summary Quiz

Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)

Differentiation will be used to meet the needs of specific students

Description of Extension Activity(ies):

Cyber Communities: Hisotry of The Networked Society www.NICERC.org

Acknowledgements:

Connected and Protected: Protect Your Privacy When Sharing Information Online

Module Learning Outcomes:

Participants will:

- Consider the ways that online activity involves the intentional and unintentional exchange of information.
- Discuss a practices that put you at risk and keep you safe
- Demonstrate knowledge of correct and safe online behaviors through successful completion of games and simulations
- Engage in scenario based learning that allows them to make educated decisions and take deliberate action online to prevent things from going wrong in the first place
- Consider current online sharing practices and consider how they might be revised to improve privacy
- Realize the importance humans play in the digital world and understand how to minimize accidental and unintentional human errors
- Apply knowledge gained to the development of documents/activities designed to share online privacy preservation and safe computing practices

The Module addresses the following First Principles:

- Layering
- Domain separation
- Least privilege
- Simplicity

Description

These days people get most of their information online. That can be easy, fast, and inexpensive. Accessing it can also be a threat to user privacy. When you gather information, you are almost always sharing information about yourself in the process. Third parties including scammers, hackers, and identity thieves can in turn use that information. They may use it to trick you into sharing passwords, bank account numbers, and other information that you want to keep private.

Are you doing all you can do to protect your information when you gather and share information online? What can you do to increase security of your personal information? How might information protection best practices be shared with others so they can be secure online as well?

In this module we will invite participants to explore the many ways that people share personal information every day online, both intentionally, and unintentionally. We will consider the negative impacts of such information sharing on both individuals and groups. We will work in small groups to create a list of recommendations for staying private and safe when sharing information online, and techniques for sharing these recommendations with friends and family.

Learner Centered Classroom

High school students and teachers will be briefly introduced to principles through active learning techniques including pre-and post-session surveys, short engaging videos, and share and compare activities.

Assessment

Participants will be asked to engage with the material and each other frequently during the session. They will then work in groups to practice principles presented. High school students will be asked to develop recommendations for safe online information sharing and techniques for sharing such information effectively with family and friends. Teachers will be asked to develop recommendations for safe online information sharing and techniques for sharing such information effectively with their students.

Suitability to Various Groups

Modules will include material accessible to all groups on some level and be offered simultaneously for all groups. The culminating activities will be similar, but adapted to the interests of the different levels of learners.

Teacher Student Interaction

Students and teachers will participate in similar learning activities during the information exploration section of the module. Students and teachers will participate in a discussion of recommendations and best techniques for sharing information during culminating session.

Decision Making Simulation

Module Learning Outcomes.

Participants will:

1. Apply the knowledge gained throughout the week's instruction to understand better the cause and effect of cybersecurity practice by reacting to and solving real-world, scenario-based unexpected inimical events
2. Recognize different types of attacks on computing systems and the ensuing "real world" problems these attacks can produce
3. Hypothesize the connectivity between the various unexpected events and develop courses of action to respond to the larger connected implication.
4. Develop educated skills needed for decision making to prevent and defeat various mal- and social engineering attacks activity in the first place
5. Connect the important role humans play in the digital world to what might happen and understand how to minimize accidental and intentional human errors

The Module addresses the following First Principles:

- least privilege,
- process isolation,
- domain separation
- modularity, and
- abstraction

Description

This module is a decision making simulation that addresses the least privilege, modularity, process isolation, and abstraction cybersecurity First Principles by illustrating the essential role and fallibility of the human user in cybersecurity, the interconnectivity and aggregation of activity globally, and the "real world" implications of the lack of cybersecurity practice. The exercise demonstrates the ambiguity of the origin and intention of interruption to and/or corruption of digital media using "real world" situations.

Participants as an entire group will be informed of various cyberactivities occurring globally over a period of time with the international security situation becoming increasingly more perilous. A brief description of the interconnectivity of critical infrastructure will be provided to inform novices of the critical synthesis of aggregated activities occurring in one infrastructure.

The will then be divided into teams to assess the situation and prepare recommendations to a "decision maker" on how to respond to the aggregated activities and which Cybersecurity First Principles are violated and how. The recommendations will be presented to the assembled entire group to provide all participants the opportunity to observe and evaluate and respond to each group's different assessment and analysis of and recommendations for responding to the individual and aggregated activities.

Learner Centered Classroom

All participants will be actively learning as part of the different groups' assessing the situation and preparing the group's recommendation and Cybersecurity First Principles involved. Since this is a combination camp, the middle and high school students will be integrated into groups incorporating both. After an initial short introduction of the global situation, the different teams will be provided group work space to assess and analyze the situation and prepare their recommendations to the decision maker. Teachers will serve as an "informational resource" and provide supervision (as needed) for the student groups.

The first task for each group will be to organize to solve the problem provided them. Then each participant not only will be participating as part of the group's efforts to assess and analysis the situation and prepare recommendations for addressing the identified activities, but completing different tasks as assigned by the leadership core of the group. Not only does each group have to assess the situation and develop responses to what is happening and the cybersecurity First Principles involved, but each group also must prepare an oral briefing of their recommendations to the decision maker and the other groups.

Assessment

Assessment will be continuously conducted by both the teachers with each group and by the instructor and the instructor's knowledgeable assistant instructors. The instructor and the assistant instructors will continuously move between the groups assessing the groups' progress and providing knowledgeable guidance, advice, and recommendations. Each group's recommendation and oral presentation will be provided "feedback" by the instructor and other student and teacher participants at the end of the oral presentation.

Suitability to Various Groups

This activity is designed to occur at the end of the camp's instruction so all participants should have some knowledge of the cybersecurity First Principles and the different types of attacks of the information network. The middle school students should have at least a summary knowledge of cybersecurity's First Principles if not the implications of the global situation being assessed and analyzed. The middle school students should also be able to contribute to preparation of the oral briefing to be delivered at the end of the assessment and analysis at the very least.

The high school students should have better than summary knowledge not only of cybersecurity's First Principles but also the implications of the scenario's aggregated cyberactivities from the camp's instruction and greater learning from an additional 3-5 years of education. High school students will be able to exercise this greater knowledge to organize, assess, analyze, synthesize, and develop responses to the cyberactivities and their implications.

Teachers have the experience of supervising middle and high school students, monitoring classroom activity, and guiding students in searches for solutions from data given.

Teacher Student Interaction

All participants will have interaction with the primary and assistant instructors during the entire simulation. All will receive the data about the global situation and the cyberactivity happening and their instructions. Middle and high school students will have the opportunity to interact with the instructor and assistants as they circulate between working groups assessing progress and providing advice and guidance. Teachers will further have access to the instructor and assistants for additional expertise on the situation depicted and advice on what is expected of the students at the end of the work session.

Students will have access to their assigned teacher "experts" during the group work session for advice, guidance, and recommendations on what to do and how to do it.

Lesson Plan

LESSON TITLE: Teaching the 1 First 10 Principles-Deb Mishler-S1-MS-6/27/17

SUMMARY:

GenCyber Camp students will use the First 10 Principles to create a movie, game and participate in online simulations. The differences between the middle school and high school movie situations, grade level variety in online simulations, and variety in ways to make a board game provide evidence of differentiation. The middle school movie is called "Cyber Chaos in Bradbury Middle School." The high school's movie is called "How to Control Your New Cyber House." Examples of online simulation differentiation include "Targeted Attacks - The Fugle" for high school students and "CyberAcademy for middle school students

GRADE BAND:

- [ ] K-2
- [x] 6-8
- [ ] 3-5
- [ ] High School

Time Required: 120 minutes

Lesson Learning Objective/Outcomes: Upon completion of this lesson, students will be able to:

1. Recognize the 10 First Principles
2. State the definition of each of the 10 First Principles
3. Apply each of the 10 First Principles to a real-life situation
4. Create a movie using the 10 Principles

Materials List:

Middle School Movie Scenes Document
camera
WeVideo

How will you facilitate the learning?

- Describe the Warm-up Activity/Focused Activity/Closure and/or Reflection
- Decribe the Teacher Instruction

1. Welcome group and distribute the learning packet (Warm Up)
2. Discuss the 10 Principles of Cyber Security (Warm Up)
3. Discuss the procedure for making the movie. Using the 10 First Principles real-life scenes, students will develop skits demonstrating the use of the 10 First Principles in real life. (Focused Activity)
4. Divide students into groups (Focused Activity)
5. Assign one Principle to each group (Focused Activity)

This lesson includes:

- [x] Mapping to Cyber Security First Principles
- [x] Learning Objectives
- [x] Assessments

Mapping to Cyber Security First Principles:

- [x] **Domain Separation**
- [x] **Process Isolation**
- [x] **Resource Encapsulation**
- [x] **Modularity**
- [x] **Least Privilege**
- [x] **Abstraction**
- [x] **Data Hiding**
- [x] **Layering**
- [x] **Simplicity**
- [x] **Minimization**

Assessment of Learning:

TYPE (Examples Listed Below)	NAME/DESCRIPTION
Quiz/Test Presentation Project Writing Assignment Observation Walk Around Oral Questioning Other	Presentation - Using the 10 First Principle real life scenes, students will develop skits that demonstrate the use of the principles in real life. Student skits must demonstrate understanding and correct use of the assigned principle. Observation Walk Around

Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)

Students who are hearing impaired will be able to read all materials, closed captioning is available for all videos.
Students who are visually impaired will be able to have all materials read to them.

Description of Extension Activity(ies):

Students may explore the cyber-security simulations on Mrs. Mishler's Website

Acknowledgements:

Dan Mishler - co-creator of Lessons and Materials

Lesson Plan

LESSON TITLE: Teaching the 10 First Principles-Deb Mishler-MS-6/29/17

SUMMARY:

GenCyber Camp students will use the First 10 Principles to create a movie, game and participate in online simulations. The differences between the middle school and high school movie situations, grade level variety in online simulations, and variety in ways to make a board game provide evidence of differentiation. The middle school movie is called "Cyber Chaos in Bradbury Middle School." The high school's movie is called "How to Control Your New Cyber House." Examples of online simulation differentiation include "Targeted Attacks - The Fugle" for high school students and "CyberAcademy for middle school students

GRADE BAND:

- [ ] K-2
- [x] 6-8
- [ ] 3-5
- [ ] High School

Time Required:

120 minutes

Lesson Learning Objective/Outcomes: Upon completion of this lesson, students will be able to:

1. Recognize the 10 First Principles
2. State the definition of each of the 10 First Principles
3. Apply each of the 10 First Principles to a real-life situation

Materials List:

WeVideo - https://www.wevideo.com/
Digital cameras
Poster Board
Markers/rulers/pencils

How will you facilitate the learning?

- Describe the Warm-up Activity/Focused Activity/Closure and/or Reflection
- Decribe the Teacher Instruction

1. Welcome students. (Warm-up Activity)
2. Distribute learning packets. (Warm-up Activity)
3. Discuss how to create board games. (Warm-up Activity)
4. Complete student skits (Focused Activity)
5. Final practice – skits (Focused Activity)
6. Film student skits (Focused Activity)

This lesson includes:

- [x] Mapping to Cyber Security First Principles
- [x] Learning Objectives
- [x] Assessments

Mapping to Cyber Security First Principles:

- [x] **Domain Separation**
- [x] **Process Isolation**
- [x] **Resource Encapsulation**
- [x] **Modularity**
- [x] **Least Privilege**
- [x] **Abstraction**
- [x] **Data Hiding**
- [x] **Layering**
- [x] **Simplicity**
- [x] **Minimization**

Assessment of Learning:

TYPE (Examples Listed Below)	NAME/DESCRIPTION
Quiz/Test Presentation Project Writing Assignment Observation Walk Around Oral Questioning Other	Project - Student skits will be review to make sure that the skits present the assigned principle correctly. Observation Walk Around

Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)

Visually impaired students will have all material content read to them.
Hearing impaired students will have all material content presented in a visual form.

Description of Extension Activity(ies):

Students who finish early may work on the simulations on Mrs. Mishler's website.

Acknowledgements:

Dan Mishler - Co-creator of Lessons and Materials

Lesson Plan

LESSON TITLE: Teaching the First 10 Principles-Deb Mishler-MS-S6-7/3/17

SUMMARY:

GenCyber Camp students will use the First 10 Principles to create a movie, game and participate in online simulations. The differences between the middle school and high school movie situations, grade level variety in online simulations, and variety in ways to make a board game provide evidence of differentiation. The middle school movie is called "Cyber Chaos in Bradbury Middle School." The high school's movie is called "How to Control Your New Cyber House." Examples of online simulation differentiation include "Targeted Attacks - The Fugle" for high school students and "CyberAcademy for middle school students

GRADE BAND:

- [ ] K-2
- [x] 6-8
- [ ] 3-5
- [ ] High School

Time Required:

[ ] minutes

Lesson Learning Objective/Outcomes: Upon completion of this lesson, students will be able to:

1. Recognize and define First 10 Principles.
2. Demonstrate knowledge of First 10 Principles.

Materials List:

Kahoot-It
Mrs. Mishler's website

How will you facilitate the learning?

- Describe the Warm-up Activity/Focused Activity/Closure and/or Reflection
- Decribe the Teacher Instruction

1. Welcome class (Warm Up)
2. Administer a Kahoot-It quiz to assess understanding of 10 Principles (Focused Activity)
3. During the time remaining, students may explore cyber security simulations on Mrs. Mishler's website (Focused Activity)
4. Discuss previous lessons and activities. Discuss student suggestions for improving Mrs. Mishler's activities. (Closure/Reflection)

This lesson includes:

- [x] Mapping to Cyber Security First Principles
- [x] Learning Objectives
- [x] Assessments

Mapping to Cyber Security First Principles:

- [x] **Domain Separation**
- [x] **Process Isolation**
- [x] **Resource Encapsulation**
- [x] **Modularity**
- [x] **Least Privilege**
- [x] **Abstraction**
- [x] **Data Hiding**
- [x] **Layering**
- [x] **Simplicity**
- [x] **Minimization**

Assessment of Learning:

TYPE (Examples Listed Below)	NAME/DESCRIPTION
Quiz/Test Presentation Project Writing Assignment Observation Walk Around Oral Questioning Other	Quiz - Kahoot-It Quiz

Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)

Visually impaired students will have all materials/content read to them.
Hearing impaired students will have all materials/content read to them.

Description of Extension Activity(ies):

Students will be able to explore the cyber-security simulations on Mrs. Mishler's website.

Acknowledgements:

Dan Mishler - Co-Creator of Lessons and Materials

Lesson Plan

LESSON TITLE: Teaching The 10 First Principles-Deb Mishler-Session 2-HS-6/28/17

SUMMARY:

GenCyber Camp students will use the First 10 Principles to create a movie, game and participate in online simulations. The differences between the middle school and high school movie situations, grade level variety in online simulations, and variety in ways to make a board game provide evidence of differentiation. The middle school movie is called "Cyber Chaos in Bradbury Middle School." The high school's movie is called "How to Control Your New Cyber House." Examples of online simulation differentiation include "Targeted Attacks - The Fugle" for high school students and "CyberAcademy for middle school students

GRADE BAND:

- ☐ K-2
- ☐ 6-8
- ☐ 3-5
- ☑ High School

Time Required: 120 minutes

Lesson Learning Objective/Outcomes: Upon completion of this lesson, students will be able to:

Upon completion of this lesson, students will be able to:
1. Recognize the 10 First Principles
2. State the definition of each of the 10 First Principles
3. Apply each of the 10 First Principles to a real-life situation

Materials List:

High School Movie Scenes Document
camera
WeVideo

How will you facilitate the learning?

- Describe the Warm-up Activity/Focused Activity/Closure and/or Reflection
- Decribe the Teacher Instruction

1. Welcome group and distribute the learning packet (Warm-up Activity)
2. Discuss the 10 Principles of Cyber Security (Warm-up Activity)
3. Discuss the procedure for making the movie (Focused Activity)
4. Divide students into groups (Focused Activity)
5. Assign one Principle to each group (Focused Activity)
6. Help high school students to develop skits (Focused Activity)

This lesson includes:

- ☑ Mapping to Cyber Security First Principles
- ☑ Learning Objectives
- ☑ Assessments

Mapping to Cyber Security First Principles:

- [x] **Domain Separation**
- [x] **Process Isolation**
- [x] **Resource Encapsulation**
- [x] **Modularity**
- [x] **Least Privilege**
- [x] **Abstraction**
- [x] **Data Hiding**
- [x] **Layering**
- [x] **Simplicity**
- [x] **Minimization**

Assessment of Learning:

TYPE (Examples Listed Below)	NAME/DESCRIPTION
Quiz/Test Presentation Project Writing Assignment Observation Walk Around Oral Questioning Other	Project/Presentation - Student skits should correctly use the assigned principle in the real-life scenario which was assigned. Observation Walk Around

Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)

Hearing impaired students will have all materials/content presented as a visual.
Visually impaired students will have all materials/content presented auditorily.

Description of Extension Activity(ies):

Simulations on Mrs. Mishler's Website

Acknowledgements:

Dan Mishler - Co-Creator of Lessons and Materials

Lesson Plan

LESSON TITLE: Teaching the 10 First Principles-Deb Mishler-HS-6/29

SUMMARY:

GenCyber Camp students will use the First 10 Principles to create a movie, game and participate in online simulations. The differences between the middle school and high school movie situations, grade level variety in online simulations, and variety in ways to make a board game provide evidence of differentiation. The middle school movie is called "Cyber Chaos in Bradbury Middle School." The high school's movie is called "How to Control Your New Cyber House." Examples of online simulation differentiation include "Targeted Attacks - The Fugle" for high school students and "CyberAcademy for middle school students

GRADE BAND:

- [ ] K-2
- [ ] 6-8
- [ ] 3-5
- [x] High School

Time Required: 120 minutes

Lesson Learning Objective/Outcomes: Upon completion of this lesson, students will be able to:

1. Recognize the 10 First Principles
2. State the definition of each of the 10 First Principles
3. Apply each of the 10 First Principles to a real-life situation

Materials List:

WeVideo - https://www.wevideo.com/
Digital cameras
Poster Board
Markers/rulers/pencils

How will you facilitate the learning?

- Describe the Warm-up Activity/Focused Activity/Closure and/or Reflection
- Decribe the Teacher Instruction

1. Welcome students. (Warm-up Activity)
2. Distribute learning packets. (Warm-up Activity)
3. Discuss how to create board games. (Warm-up Activity)
4. Complete student skits (Focused Activity)
5. Final practice – skits (Focused Activity)
6. Film student skits (Focused Activity)

This lesson includes:

- [x] Mapping to Cyber Security First Principles
- [x] Learning Objectives
- [x] Assessments

Mapping to Cyber Security First Principles:

- [x] **Domain Separation**
- [x] **Process Isolation**
- [x] **Resource Encapsulation**
- [x] **Modularity**
- [x] **Least Privilege**
- [x] **Abstraction**
- [x] **Data Hiding**
- [x] **Layering**
- [x] **Simplicity**
- [x] **Minimization**

Assessment of Learning:

TYPE (Examples Listed Below)	NAME/DESCRIPTION
Quiz/Test Presentation Project Writing Assignment Observation Walk Around Oral Questioning Other	Project - Student skits will be review to make sure that the skits present the assigned principle correctly. Observation Walk Around

Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)

Visually impaired students will have all material content read to them.
Hearing impaired students will have all material content presented in a visual form.

Description of Extension Activity(ies):

Students who finish early may work on the simulations on Mrs. Mishler's website.

Acknowledgements:

Dan Mishler - Co-creator of Lessons and Materials

Lesson Plan

LESSON TITLE: Teaching the First 10 Principles-Deb Mishler-HS-S6-7/3/17

SUMMARY:

GenCyber Camp students will use the First 10 Principles to create a movie, game and participate in online simulations. The differences between the middle school and high school movie situations, grade level variety in online simulations, and variety in ways to make a board game provide evidence of differentiation. The middle school movie is called "Cyber Chaos in Bradbury Middle School." The high school's movie is called "How to Control Your New Cyber House." Examples of online simulation differentiation include "Targeted Attacks - The Fugle" for high school students and "CyberAcademy for middle school students

GRADE BAND:

- [ ] K-2
- [ ] 6-8
- [ ] 3-5
- [x] High School

Time Required:

120 minutes

Lesson Learning Objective/Outcomes: Upon completion of this lesson, students will be able to:

1. Recognize and define First 10 Principles.
2. Demonstrate knowledge of First 10 Principles.

Materials List:

Kahoot-It
Mrs. Mishler's website

How will you facilitate the learning?

- Describe the Warm-up Activity/Focused Activity/Closure and/or Reflection
- Decribe the Teacher Instruction

1. Welcome class (Warm Up)
2. Administer a Kahoot-It quiz to assess understanding of 10 Principles (Focused Activity)
3. During the time remaining, students may explore cyber security simulations on Mrs. Mishler's website (Focused Activity)
4. Discuss previous lessons and activities. Discuss student suggestions for improving Mrs. Mishler's activities. (Closure/Reflection)

This lesson includes:

- [x] Mapping to Cyber Security First Principles
- [x] Learning Objectives
- [x] Assessments

Mapping to Cyber Security First Principles:

- [x] **Domain Separation**
- [x] **Process Isolation**
- [x] **Resource Encapsulation**
- [x] **Modularity**
- [x] **Least Privilege**
- [x] **Abstraction**
- [x] **Data Hiding**
- [x] **Layering**
- [x] **Simplicity**
- [x] **Minimization**

Assessment of Learning:

TYPE (Examples Listed Below)	NAME/DESCRIPTION
Quiz/Test Presentation Project Writing Assignment Observation Walk Around Oral Questioning Other	Quiz - Kahoot-It Quiz

Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)

Visually impaired students will have all materials/content read to them.
Hearing impaired students will have all materials/content read to them.

Description of Extension Activity(ies):

Students will be able to explore the cyber-security simulations on Mrs. Mishler's website.

Acknowledgements:

Dan Mishler - Co-Creator of Lessons and Materials

Lesson Plan

LESSON TITLE: Teaching the 10 First Principles-Deb Mishler-MS,HS Combined-6/30/17

SUMMARY:

GenCyber Camp students will use the First 10 Principles to create a movie, game and participate in online simulations. The differences between the middle school and high school movie situations, grade level variety in online simulations, and variety in ways to make a board game provide evidence of differentiation. The middle school movie is called "Cyber Chaos in Bradbury Middle School." The high school's movie is called "How to Control Your New Cyber House." Examples of online simulation differentiation include "Targeted Attacks - The Fugle" for high school students and "CyberAcademy for middle school students

GRADE BAND:

- [ ] K-2
- [x] 6-8
- [ ] 3-5
- [x] High School

Time Required: 120 minutes

Lesson Learning Objective/Outcomes: Upon completion of this lesson, students will be able to:

1. Recognize the 10 First Principles
2. State the definition of each of the 10 First Principles
3. Apply each of the 10 First Principles to a real-life situation

Materials List:

WeVideo Movie
markers
poster board

How will you facilitate the learning?

- Describe the Warm-up Activity/Focused Activity/Closure and/or Reflection
- Decribe the Teacher Instruction

1. Welcome students (Warm-Up)
2. Watch WeVideo Movie and discuss (Focused Activity)
3. Complete board games (Focused Activity)
4. If time remains, students may play the board games that they created with other students (Focused Activity)
5. Discuss the board games and movie, ask students for suggestions to make the activities better,answer

This lesson includes:

- [x] Mapping to Cyber Security First Principles
- [x] Learning Objectives
- [x] Assessments

Mapping to Cyber Security First Principles:

- [x] **Domain Separation**
- [x] **Process Isolation**
- [x] **Resource Encapsulation**
- [x] **Modularity**
- [x] **Least Privilege**
- [x] **Abstraction**
- [x] **Data Hiding**
- [x] **Layering**
- [x] **Simplicity**
- [x] **Minimization**

Assessment of Learning:

TYPE (Examples Listed Below)	NAME/DESCRIPTION
Quiz/Test Presentation Project Writing Assignment Observation Walk Around Oral Questioning Other	First 10 Principles Movie - Teacher will review the movie to make sure that the skits accurately demonstrate the assigned principle in real life. Observation Walk Around

Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)

Visually impaired students will be able to have all material content read to them.
Hearing impaired students will be able to have all material content presented visually.

Description of Extension Activity(ies):

Students may use Mrs. Mishler's website to do the online cyber security simulations.

Acknowledgements:

Dan Mishler - Co-creator of lessons and materials

Lesson Plan

LESSON TITLE: Drone Programming

SUMMARY:

The instructor will give a brief introduction to drone technology, highlighting the First Principles that are missing or employed. Students will then be tasked with using "Tynker," an app available on both iOS and Android to program the drone to accomplish various tasks with increasing difficulty, including dropping items on a target, and navigating a small obstacle course.

GRADE BAND:

- ☐ K-2
- ☐ 3-5
- ☑ 6-8
- ☑ High School

Time Required:

100.000 minutes

Lesson Learning Objective/Outcomes: Upon completion of this lesson, students will be able to:

Activities in this module map directly to the following two outcomes proposed in our grant proposal:

1. Demonstrate in-depth understanding of the cybersecurity First Principles.
4. Have a better understanding of essential problem solving and programming concepts.

In addition, the following objectives are also addressed:

-Identify the First Principles that are used and not used in drone technology

-Create simple programs using drag and drop procedures to control the drone

Materials List:

Tynker App

Parrot Mambo Drone - provided to students who attended the IUP GenCyber Combination Camp

How will you facilitate the learning?

- Describe the Warm-up Activity/Focused Activity/Closure and/or Reflection
- Decribe the Teacher Instruction

-Discussion of First Principles

-Explanation and tutorial of Tynker App

-Discussion of safety procedures for drone operation

-Students attempt various tasks using Tynker to program drone

-Kahoot Quiz on drone technology

This lesson includes:

- ☑ Mapping to Cyber Security First Principles
- ☑ Assessments
- ☑ Learning Objectives

Mapping to Cyber Security First Principles:

- [ ] **Domain Separation**
- [x] **Process Isolation**
- [ ] **Resource Encapsulation**
- [ ] **Modularity**
- [ ] **Least Privilege**
- [ ] **Abstraction**
- [ ] **Data Hiding**
- [ ] **Layering**
- [x] **Simplicity**
- [x] **Minimization**

Assessment of Learning:

TYPE (Examples Listed Below)	NAME/DESCRIPTION
Quiz/Test Presentation Project Writing Assignment Observation Walk Around Oral Questioning Other	Drone technology presentation Drone safety presentation Instructor observation during group programming tasks Kahoot quiz

Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)

Description of Extension Activity(ies):

Acknowledgements:

Lesson Plan

LESSON TITLE: Java Programming

SUMMARY:

This module reviews the basics of problem solving (building blocks, simple design, etc.) and computer programming (variables, expressions, decision making, etc.) in an approachable and catching way. Throughout this review, relevant cybersecurity First Principles will be fully explained and links to the discussed topics will be clearly established. For example, the building blocks problem solving approach will be discussed as a direct implementation of the design modularity FP. The module then focusses on familiarizing participants with essential programming concepts and constructs needed to develop software solutions to real-world application. Details of decision making constructs, various looping

GRADE BAND:

- [ ] K-2
- [ ] 3-5
- [x] 6-8
- [x] High School

Time Required:

100.000 minutes

Lesson Learning Objective/Outcomes: Upon completion of this lesson, students will be able to:

Activities in this module map directly to the following three outcomes proposed in our grant proposal:

1. Demonstrate in-depth understanding of the cybersecurity First Principles.
2. Explore the use of various operating systems commands on different platforms.
4. Have a better understanding of essential problem solving and programming concepts.

Materials List:

Lab Computers
Eclipse IDE
Lab Handouts
Flash memory

How will you facilitate the learning?

- Describe the Warm-up Activity/Focused Activity/Closure and/or Reflection
- Decribe the Teacher Instruction

-Discussion of programming basics
-Explanation and tutorial of a typical IDE such as Eclipse
-Students will be involved in editing and running a number of Java programs
-Simulation exercise on software programming
-Kahoot Quiz on programming basics
- Delivering customized modules to each group (more challenging labs will be given to high school

This lesson includes:

- [x] Mapping to Cyber Security First Principles
- [x] Learning Objectives
- [x] Assessments

Mapping to Cyber Security First Principles:

- [x] **Domain Separation**
- [ ] **Process Isolation**
- [x] **Resource Encapsulation**
- [x] **Modularity**
- [ ] **Least Privilege**
- [x] **Abstraction**
- [x] **Data Hiding**
- [ ] **Layering**
- [x] **Simplicity**
- [ ] **Minimization**

Assessment of Learning:

TYPE (Examples Listed Below)	NAME/DESCRIPTION
Quiz/Test Presentation Project Writing Assignment Observation Walk Around Oral Questioning Other	Intro to programming presentation Instructor observation during group programming tasks Kahoot quiz Simulation exercise.

Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)

Description of Extension Activity(ies):

Acknowledgements:

Lesson Plan

LESSON TITLE: Arduino, Embedded Systems, and the Internet of Things

SUMMARY:

Embedded systems are becoming prevalent in today's connected "Smart" world. For example many homes have internet cameras, smart TVs, smart security systems, and connected climate controls systems. This module provides a hands on introduction to embedded systems using the Arduino Starter Kit. Students will wire circuits and program the Arduino embedded board to read switches, potentiometers, photocells, and temperature sensors; and send signals to LEDs, speakers, motors, servos, and LCD displays. Students will wire a circuit that when triggered by switch, potentiometer threshold, interruption of light source, or excess heat will sound an alarm, rotate a servo, flash the LED

GRADE BAND:

- ☐ K-2
- ☐ 3-5
- ☑ 6-8
- ☑ High School

Time Required: 100.000 minutes

Lesson Learning Objective/Outcomes: Upon completion of this lesson, students will be able to:

1. Demonstrate in-depth understanding of the Cybersecurity First Principles.
2. Explore the use of various operating systems commands on different platforms.
4. Have a better understanding of essential problem solving and programming concepts.
5. Apply programming knowledge and skills to design and implement reliable software systems that takes into account software assurance concepts.

Materials List:

Arduino Starter Kit

How will you facilitate the learning?

- Describe the Warm-up Activity/Focused Activity/Closure and/or Reflection
- Decribe the Teacher Instruction

Students will be provided a summary sheet of input and output controls/devices provided in the Arduino Starter Kit. Students will be led through set up of the Arduino board, connection to a computer, an programming in the Arduino development environment. The presentation will incrementally add a control or device to the circuit along with programming. A pre-built set of programs will be used.

This lesson includes:

- ☑ Mapping to Cyber Security First Principles
- ☑ Assessments
- ☑ Learning Objectives

Mapping to Cyber Security First Principles:

- [x] **Domain Separation**
- [x] **Process Isolation**
- [x] **Resource Encapsulation**
- [x] **Modularity**
- [ ] **Least Privilege**
- [x] **Abstraction**
- [ ] **Data Hiding**
- [x] **Layering**
- [ ] **Simplicity**
- [ ] **Minimization**

Assessment of Learning:

TYPE (Examples Listed Below)	NAME/DESCRIPTION
Quiz/Test Presentation Project Writing Assignment Observation Walk Around Oral Questioning Other	Formal assessment of cyber security first principles together with select embedded systems concepts will be part of the pre/post camp tests. Informal assessment will be made by completion of in classroom project and by oral discussion/questioning.

Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)

Description of Extension Activity(ies):

Subsequent to this module, students can proceed through all projects provided in the guide book accompanying the Arduino Starter Kit. Students will be directed on where to find the example programs for the circuits given in the book.

Beyond the guide book, students will be shown on-line sources for Arduino add-ons.

Acknowledgements:

Arduino.cc

Lesson Plan

LESSON TITLE: Encryption

SUMMARY:

The instructor will begin with a brief introduction into encryption and its importance. Students will then be able to see a visual representation of how encryption works by utilizing projects available on code.org. The first project allows students to view how a Caeser Cipher encryption is implemented, and can then manipulate it themselves. The second project allows students to view how a random substitution encryption is implemented, and then can try and decipher multiple examples. This lesson will coincide with the NSA Day of Cyber projects later in the week.

GRADE BAND:

- ☐ K-2
- ☐ 3-5
- ☑ 6-8
- ☑ High School

Time Required:

100.000 minutes

Lesson Learning Objective/Outcomes: Upon completion of this lesson, students will be able to:

Activities in this module map directly to the following two outcomes proposed in our grant proposal:
1. Demonstrate in-depth understanding of the cybersecurity First Principles.
9. Understand cryptographic basics and its role in securing data communications.

In addition, the following objectives are also addressed:
-Identify various types of encryption technique
-Recognize the importance of encryption and it's role in their daily lives
-Be able to decrypt simple encryptions, including Caesar Cipher and random substitution

Materials List:

-software provided by code.org

How will you facilitate the learning?

- Describe the Warm-up Activity/Focused Activity/Closure and/or Reflection
- Decribe the Teacher Instruction

-Discussion of how encryption is used in current technology
-Discussion of how encryption works and the various types of encryption
-Discussion of how encryption types vary in strength and security
-Students attempt to break simple encryptions using online software
-Kahoot quiz on general encryption knowledge

This lesson includes:

- ☑ Mapping to Cyber Security First Principles
- ☑ Assessments
- ☑ Learning Objectives

Mapping to Cyber Security First Principles:

- [ ] **Domain Separation**
- [ ] **Process Isolation**
- [ ] **Resource Encapsulation**
- [ ] **Modularity**
- [ ] **Least Privilege**
- [ ] **Abstraction**
- [x] **Data Hiding**
- [ ] **Layering**
- [ ] **Simplicity**
- [ ] **Minimization**

Assessment of Learning:

TYPE (Examples Listed Below)	NAME/DESCRIPTION
Quiz/Test Presentation Project Writing Assignment Observation Walk Around Oral Questioning Other	-Kahoot quiz -Instructor observation of attemps to break encryption

Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)

Description of Extension Activity(ies):

Acknowledgements:

www.code.org

Lesson Plan

LESSON TITLE: Advanced Programming Robotic Security Module Using Cubelets and MOSS

SUMMARY:

This module presents an easy-to-understand introduction to fundamentals of robotic programming and security. The participants will be introduced to learn to code with Cubelets! Cubelets Blockly is the perfect platform to learn how to program your own robots. It's a simple and powerful visual programming tool gives you full control over your Cubelets® robot blocks. Create countless new robots and behaviors with the parallel programming.

GRADE BAND:

- ☐ K-2
- ☐ 3-5
- ☑ 6-8
- ☑ High School

Time Required:

240.000 minutes

Lesson Learning Objective/Outcomes: Upon completion of this lesson, students will be able to:

Camp Learning Outcomes

1. Demonstrate substantial understanding of the cybersecurity First Principles.
Numbers one, six, seven and eight

2. Explore the use of basic operating systems commands on different platforms.
All robot OS can be compromised to alter what they were originally intended for in both MOSS and Cubelets

Materials List:

Cubelets
MOSS
Scratch Pad
Cubelets Blocky

How will you facilitate the learning?

- Describe the Warm-up Activity/Focused Activity/Closure and/or Reflection
- Decribe the Teacher Instruction

MOSS Scratch is an extension for Scratch that enables programming support for the MOSS Brain. It adds Scratch blocks which can programmatically read inputs from sensors (like the knob, proximity or microphone) and send outputs to actuators (like the spin, pivot, or light). Use your MOSS to draw pictures in Scratch with knobs or proximity blocks, drive your MOSS car around with your keyboard, or build an autonomous exploring robot! This module is designed to be taught in a highly interactive environment in which all attendees will be active participants in the learning process. To achieve that, one approach is to

This lesson includes:

- ☑ Mapping to Cyber Security First Principles
- ☑ Assessments
- ☑ Learning Objectives

Mapping to Cyber Security First Principles:

- [x] **Domain Separation**
- [ ] **Process Isolation**
- [ ] **Resource Encapsulation**
- [x] **Modularity**
- [ ] **Least Privilege**
- [x] **Abstraction**
- [x] **Data Hiding**
- [ ] **Layering**
- [ ] **Simplicity**
- [ ] **Minimization**

Assessment of Learning:

TYPE (Examples Listed Below)	NAME/DESCRIPTION
Quiz/Test Presentation Project Writing Assignment Observation Walk Around Oral Questioning Other	Four questions to be used in the Pre/Post assessment survey. 1. The artificial intelligence of the robot has gone “out of control” and the Bluetooth “brain” is not controlling the Cublets. The robot needs to be reprogrammed and it is experiencing which cybersecurity first principle?

Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)

The contents the module will be adapted to better fit the level of each of the proposed three groups. For the teachers group, topics covered will stress how the AI security concepts and techniques can be integrated into the K-12 curriculum in addition to covering advanced concepts such as robotic co-existence with the human world. The contents will also advance in the level of detail when being presented to the Middle school group compared to when being presented to the High school students.

Description of Extension Activity(ies):

This component of the module is designed to use a variety of formative assessment strategies in order to ensure that the students has acceptably achieved the Intended Learning Outcomes (ILOs) of the module. Examples of the proposed techniques are use of discussion, questioning, peer-assessment, and constructive quizzes. For example, a carefully chosen set of questions on the covered topics can form a quiz given at the end of this module. After the students finish the quiz, all quiz questions will be reviewed and proper answers will be identified. This positively contribute to productive discussions in the classroom and increase the chances of students achieving higher degrees of learning.

Acknowledgements:

Lesson Plan

LESSON TITLE: Secure Coding

SUMMARY:

This module will build on the knowledge and skills gained via introducing participants to the "Java programming" module. In this module, participants will learn about the importance of secure programming and how they can apply simple, but effective techniques to make sure that their programs are more secure. For example, the concept of buffer overflow will be fully explained and used as an example of a very common security vulnerability that can be avoided by simply checking boundary conditions. Moreover, the concepts of input validation and black-box implementation will be introduced as other important approaches to ensure and improve the security of the coding process. One example

GRADE BAND:

- [ ] K-2
- [x] 6-8
- [ ] 3-5
- [x] High School

Time Required:

100.000 minutes

Lesson Learning Objective/Outcomes: Upon completion of this lesson, students will be able to:

Activities in this module map directly to the following two outcomes proposed in our grant proposal:
1. Demonstrate in-depth understanding of the cybersecurity First Principles.
4. Have a better understanding of essential problem solving and programming concepts.
5. Apply programming knowledge and skills to design and implement reliable software systems that takes into account software assurance concepts.

Materials List:

Lab Computers
Eclipse IDE
.NET Visual Studio IDE
Lab Handouts

How will you facilitate the learning?

- Describe the Warm-up Activity/Focused Activity/Closure and/or Reflection
- Decribe the Teacher Instruction

-Discussion of secure coding basics
-Students will be involved in editing and running a number of Java and C++ programs
-Kahoot Quiz on programming basics
-Delivering customized modules to each group (more challenging labs will be given to high school students).

This lesson includes:

- [x] Mapping to Cyber Security First Principles
- [x] Learning Objectives
- [x] Assessments

Mapping to Cyber Security First Principles:

- [ ] **Domain Separation**
- [ ] **Process Isolation**
- [x] **Resource Encapsulation**
- [x] **Modularity**
- [x] **Least Privilege**
- [x] **Abstraction**
- [x] **Data Hiding**
- [x] **Layering**
- [x] **Simplicity**
- [ ] **Minimization**

Assessment of Learning:

TYPE (Examples Listed Below)	NAME/DESCRIPTION
Quiz/Test Presentation Project Writing Assignment Observation Walk Around Oral Questioning Other	Intro to secure coding presentation Instructor observation during group programming tasks Kahoot quiz

Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)

Description of Extension Activity(ies):

Acknowledgements: