Engaging Middle and High School Students in Cybersecurity through Summer Camps

Joaquin Hernandez, Xiuli Qu, Xiaohong Yuan, Jingsheng Xu
North Carolina Agricultural and Technical State University

Abstract

The increasing shortage of cybersecurity workforce in the nation needs more talented students interested in studying cybersecurity and pursuing relevant careers. To promote the study of cybersecurity and build the cybersecurity talent pipeline, North Carolina Agricultural and Technical State University (NC A&T) has offered non-residential GenCyber summer camps for rising 8th to 12th grade students in 2018 and 2019. The camps enrolled diverse students who are interested in STEM areas as well as non-STEM areas. A highly engaging curriculum has been developed and continuously improved for the GenCyber summer camps at NC A&T. It covers cybersecurity concepts, computer networks and Internet, computer security, authentication and passwords, online safety and digital forensics. This paper presents our curriculum, teaching methods and experience of the camps. The experience and lessons learned from our GenCyber lectures and labs will benefit us and other educators for the improvement of GenCyber summer camps.

Keywords

Cybersecurity, GenCyber, K-12, outreach

Introduction

The shortage of cybersecurity workforce is increasing in the nation. According to CyberSeek, there were about 314,000 cybersecurity job openings in the nation during a one-year period (September 2017 – August 2018)[1]. The global workforce shortage in cybersecurity professionals has been projected at 1.8 million by 2022[2]. Therefore, it is important to attract more talented students to study cybersecurity and increase their interest in cybersecurity careers. To address the nation's shortage of cybersecurity professionals, the GenCyber program provides grants to universities and colleges to offer summer camps in which to teach K-12 students the cybersecurity fundamentals[3]. These summer camps can introduce computer programming concepts, provide engaging and enriching experiences, and have measurable effects on self-efficacy and career interests[4]. As one of the GenCyber grantees, the College of Engineering at North Carolina Agricultural and Technical State University (NC A&T) offered non-residential GenCyber summer camps for rising 8th to 12th grade students in July 2018 and 2019. In this paper, we present our GenCyber summer camp curriculum and discuss the experience and lessons learned from the GenCyber summer camps at NC A&T.

The GenCyber summer camps at NC A&T were hosted by the Center for Cyber Defense at NC A&T, which has been designated as a Center of Academic Excellence in Information Assurance Education (CAE/IAE) since 2010 and recently as a National Centers of Academic Excellence in

Cyber Defense Research (CAE-R) in 2019. The camps at NC A&T introduced GenCyber Cybersecurity Concepts and correct and safe online behavior, and provided hands-on experience to participants. Each camp ran for five days (Monday to Friday) and eight hours per day (9am to 5pm). The camps targeted at students from underrepresented populations in STEM fields such as African Americans. Being a Historically Black College or University (HBCU), NC A&T attracted more African American students to attend the GenCyber student camps, which will help increase diversity in the nation's cybersecurity workforce in the future.

The GenCyber team at NC A&T included three faculty members, one research associate, one high school teacher and several graduate and undergraduate student assistants. Based on the published examples[5], the team designed scaffolding activities to increase the retention of computational topics, which include cybersecurity related games and hands-on labs. The overall goals of the GenCyber camps at NC A&T are to provide a highly engaging and interactive camp with games, hands-on labs, simulations, videos, and invited speakers to increase interest in cybersecurity, and to provide a foundation of exploring the field of cybersecurity to fulfill the GenCyber program goal of supporting the growth of the next generation of cybersecurity experts in the nation[6].

Curriculum Overview

The GenCyber summer camps at NC A&T introduced GenCyber Cybersecurity Concepts and correct and safe online behavior, and exposed participants to the basic topics of computer networks, operating systems, and computer and information security. The camp curriculum is highly engaged and interactive, through a set of scaffolding activities which included games, hands-on labs, animation/simulations, videos, and invited speakers. Table 1 summarizes the topics and activities included in the camp curriculum. The camp activities provided plenty of opportunities for participants to collaborate with peers. They were engaged in cooperative learning. Small group discussions were used during the camp instruction. Participants worked as small groups to conduct hands-on labs and work on a final project.

At the camps, participants learned the Hand model of GenCyber Cybersecurity Concepts, which represents six principles: Confidentiality, Integrity, Availability, Defense in Depth, Think Like an Adversary and Keep it Simple[6]. All principles in the Hand model depend on each other and work together as a whole unit, just like each of your fingers and the palm. When one principle is compromised, the entire system is compromised[3]. The GenCyber Cybersecurity Concepts were taught through the exposures to the basics of computer networks, operating systems, and computer security concepts. On the first day of each camp, the Hand model of the GenCyber Cybersecurity Concepts was introduced to participants. At the end of the first day, the participants were given the requirements of a final project, in which they were asked to use the GenCyber Cybersecurity Concepts. The six principles of the GenCyber Cybersecurity Concepts were reinforced in the activities throughout the curriculum as shown in Table 2.

Curriculum Learning Outcomes

At the GenCyber summer camps offered at NC A&T, the participants learned (1) how to differentiate safe and spam URLs and identify phishing websites and emails, (2) cryptography and its applications, (3) the basics of cybersecurity, network security, digital forensics and

steganography, and (4) how to handle administrative tasks in a multiuser windows system. At the end of the camp, the participants should

1. be able to identify and prevent the risks and threats when using the Internet,
2. understand the basics of cryptography and be able to apply Caesar Cipher,
3. be able to explain the basics of cybersecurity and network security,
4. be able to explain the mechanisms of brute force attack and packet sniffing,

Topics	Activities
1. GenCyber Cybersecurity Concepts • Confidentiality • Integrity • Availability • Defense in Depth • Think Like an Adversary • Keep it Simple	• Presentation, invited talks • Student final projects • Case discussion on cyber ethics • Video clips, PBS[7] game, Kahoot[8] games • Internet of Strings • Brute force attack lab, packet sniffing visualization, MITM attack demo
2. Introduction to Computer Networks and Internet • LAN vs Internet • TCP/IP and Layered Model of Networks • Packets and Routing • Wireless Networks	• Presentation • Video clips • Internet of String (hands-on) • Setting up Wireless Access Point (WAP) with Raspberry Pi (hands-on)
3. Computer Security • Access control • System audit records • Password policy	• Presentation • Thunderbird Cup lab[9] (hands-on)
4. Authentication and Passwords • What is authentication? • Passwords and vulnerabilities of passwords • Dictionary attacks and brute force attacks • Multifactor authentication	• Presentation • Password cracking and protection using Raspberry Pi (hands-on) • PBS[7] game (hands-on)
5. Online Safety • Online Ethics • Privacy • Cyber bullying • Identify Theft • Phishing • Malware	• Presentation • Video • Invited talks • Google Interland[10] game (hands-on) • Anti-Phishing Phil[11] game (hands-on) • PBS[7] game (hands-on)
6. Introduction to Digital Forensics • The basic process of digital forensics • How to analyze images with forensics tools (Forensics Toolkit (FTK) and Autopsy)? • What is steganography? • What are the techniques used for steganography? • How to detect steganography?	• Using the IPAR[12] (Imaging, Preserving, analyzing and reporting) game to investigate the "Academic Dishonesty" case (hands-on) • Steganography and metadata lab[13] (hands-on)
7. Summer Camp Final Project • Identify a security problem and propose a solution	• Student presentation

Table 1. Camp Curriculum Overview

5. be able to explain the basics of digital forensics, and analyze simple cases using a digital forensics tool, and
6. be able to apply administrative tasks in multiuser windows systems.

Table 3 summarizes the games and hand-on activities that contribute to the learning outcomes.

GenCyber Concepts	Activities in which to implement the Principles
Defense in Depth	Presentation, PBS[7] game incorporated different layers of defense
Confidentiality	Presentation, Brute force attack using Raspberry Pi, Steganography lab, ARP cache poisoning attack demo
Integrity	Presentation, Caesar Cipher wheel game, Escape from the room
Availability	Presentation, Internet of strings. Demonstrated distributed denial of service
Think Like an Adversary	Presentation, video, discussion of ethics. The thinking of hackers, Steganography lab
Keep it Simple	Presentation, Project design
GenCyber Hand	Presentation, Final project

Table 2: Hand-on Activities Related to the GenCyber Cybersecurity Concepts

Learning Outcomes	Hand-on activities contributing to the learning outcomes
Outcome 1	Google Game Interland[10] game, Anti-Phishing Phil[11] game, PBS[7] game
Outcome 2	Caesar Cipher wheel lab, Escape from the room game
Outcome 3	PBS[7] game, Internet of Strings game, Lab of setting Raspberry Pi as wireless access point, Thunderbird Cup[9] lab
Outcome 4	SSH and brute force attack lab using Raspberry Pi
Outcome 5	Steganography lab[13], IPAR[12] lab
Outcome 6	Thunderbird Cup lab

Table 3: Hand-on Activities Contributing to Learning Outcomes

Example Activities

Internet of Strings

In this activity, students simulated how the Internet works by using strings to form a grid of interconnected nodes and routers. Each router has multiple links to other routers within the "network" as shown in Figure 1. This activity was designed to teach the concepts of router, network topology, network addresses, and denial of service. All of these concepts were introduced at the beginning of this activity with the introduction videos that teach the topics of network topology, IP addresses and Denial of Service attack[14-16]. These videos were followed by

a PowerPoint presentation on the network topology simulated in the activity. The learning objectives of this activity are that at the end of the activity, participants should be able to:

1. explain how routers make decisions when moving a packet through the Internet,
2. demonstrate data encapsulation, and
3. demonstrate distributed denial of service attack.

Availability, one principle of the GenCyber Cybersecurity Concepts, is applied to this activity since the denial of service attack made the network service unavailable.

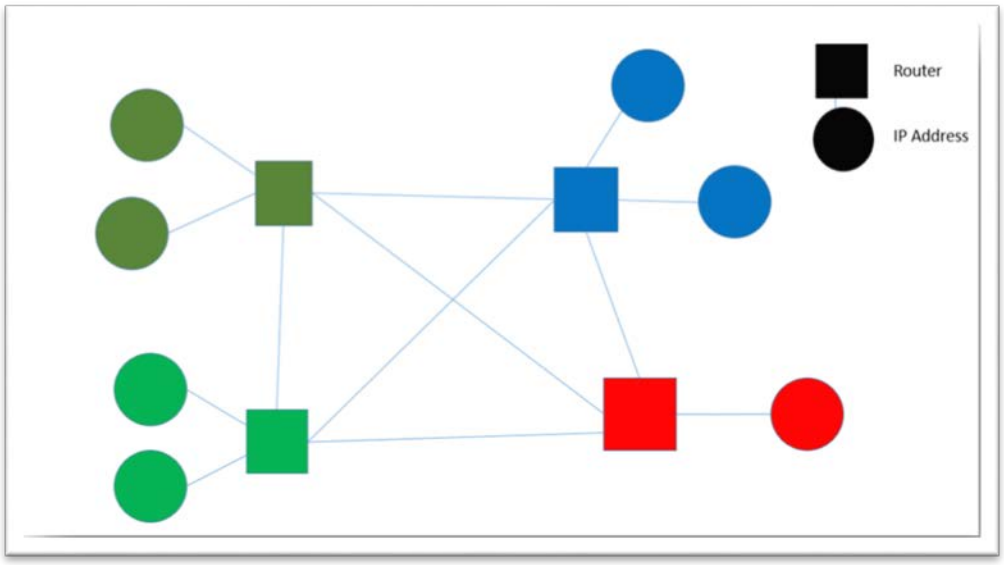

Figure 1. The Network Topology Simulated on the Internet of Strings Activity

In this activity, the instructor first discussed with the students the contents of the videos and the network topology for the activity. Then the instructor provided the students with pencils and guided them to form a mesh network. After the students learned the basic concepts, the instructor and teacher assistants guided them to form the network as shown in Figure 1. After the network was formed, the first task was to demonstrate how packets are routed from the source to the destination.

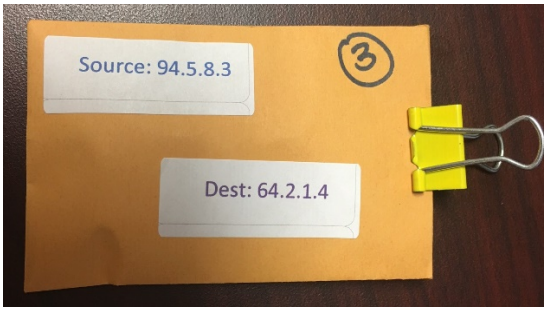

Figure 2. A Packet for the Internet of Strings Activity

The activity also demonstrated how data encapsulation works, and a distributed denial of service attack. During the activity students put a candy in an envelope and wrote the source and destination addresses of the packet on the envelope. Figure 2 shows the envelope representing the packet. Then the students sent the packet through the network to the destination. After the students successfully sent a few packets through the network to different destinations (i.e., students representing computers), they performed a denial of service attack by having all the source computers send multiple packets to the same destination.

Steganography Lab

The learning objectives of this activity are that at the end of the activity, participants should be able to:

1. explain the concept of Steganography,
2. use Exiftool17 on Ubuntu to get the location where a picture was taken, and
3. demonstrate how to extract messages from pictures.

The lab uses a made-up scenario to ask students to find passwords from keywords, which are extracted from location names based on GPS coordinates from image metadata, to crack a hidden message. The game combines aspects of problem solving, team building and digital forensics. In this activity students also learned the basic knowledge of encryption and decryption.

Scenario for the steganography lab

The infamous Frank William Abagnale, Jr. has struck again! He has stolen a crown jewel worth of $50 million from the recent royal wedding and went into hiding. In order to contact him, one must use the password. He has left some clues for his accomplices to follow his trail and make contact with him. Once the clues are assembled, it will reveal a quote. The author of the quote will be the password. Luckily, the CIA has intercepted this message. But the bad news is, only 2 hours remain and Frank will never be found after then. You and your team have been tasked with cracking the hidden message from clues left behind by Frank. If you find the message before it's too late, Prince Harry is determined to award you with a grand prize. Good luck!

Lab activities

The lab started with watching two short videos to introduce digital forensics and metadata concepts. After watching the videos, the instructor discussed the content with the students. Then a lab manual was given to the students, and the instructor explained the task (scenario) to the students and showed them how to use the tools. Following the lab manual, the students need:

- to find locations from 8 images using ExifTool[17] on Ubuntu, and
- to decrypt images to find the hidden messages by using keywords extracted from the names of the locations.

When the students worked on the task, the instructor and the teaching assistants walked around to check the progress of the students and assist the students.

The main steps of the lab are as follows:

1. Open virtual machine on VirtualBox
2. Open Terminal, use commands such as ‘cd’ to get to the “Steganography/Original Pictures” directory, use the web if unsure how, and use ‘ls’ to find out what’s in the current directory.
3. Open Terminal, go to the “Steganography/Pictures with Secrets” directory
4. Use the command(s) from the ExifTool to get the GPS location of each picture. For example, Figure 3.2 shows the metadata extracted from Figure 3.1 using ExifTool. From this data we can use the coordinates: 41 deg 53′ 55.64” N 12 deg 28′ 23.39” E - (This is interpreted as: “30 degrees, 39 minutes, 46.63 seconds North and 104 degrees, 1 minute, 30.32 seconds East.”) to find the location where the picture was taken.
5. Find the name of the location or the name of a landmark nearby (could be the name of a landmark, restaurant, store, city, state, etc.). By putting the coordinates found in step 4 on google maps the location will be displayed as seen in Figure 4. The location is “Rione VI Parione, 00186 Rome, Metropolitan City of Rome, Italy”. From this information possible keywords can be deduced such as “Rome”, “Plazza Navona” or “Italy”.

Following the above steps students were able to decrypt all the messages embedded in the 8 Images. Then the messages were written in pieces of cardboard, and given to students to hold while the rest of the students move them around to assemble the quote. After the quote was put together, the students figured out the author name of the quote, which was the password to contact the thief Frank William Abagnale, J.

The GenCyber Cybersecurity Concepts applied in this lab were Confidentiality. This activity also reinforces the GenCyber concept Think Like an Adversary because the students had to think like an adversary when they play the role of detectives.

Figure 3.1. Original Photo to Be Analyzed

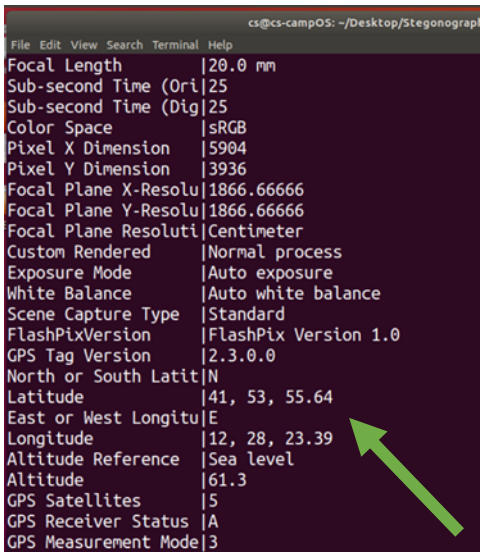

Figure 3.2. Photo Metadata

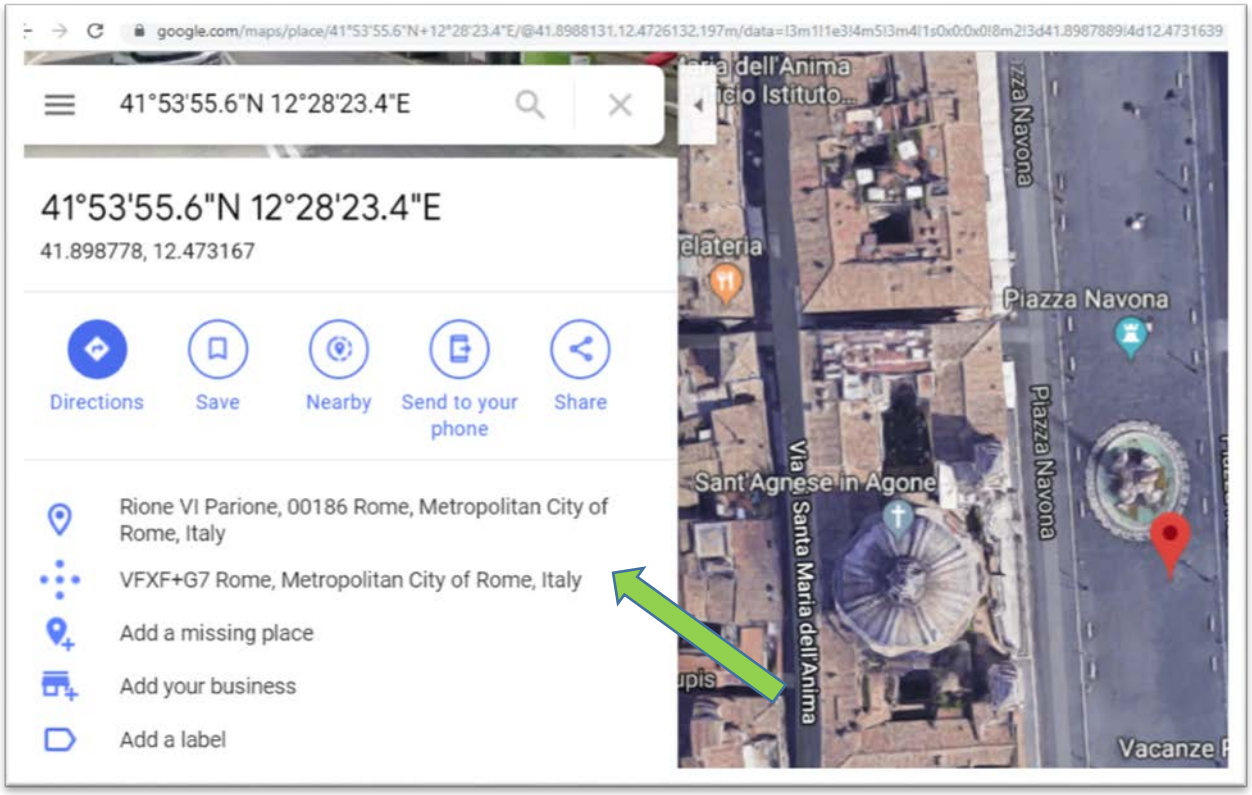

Figure 4. Location Where the Picture Was Taken

Lessons Learned

Our camps attracted more students of rising 8th to 10th grade than students of rising 11th and 12th grades. Providing younger students the opportunity to explore the cybersecurity career can significantly affect their choice in their college majors and future careers. For 11th and 12th grade students who are interested in Computer Science or Cybersecurity, our GenCyber summer camps can prepare them better for their college study. Moreover, more than half of our camp participants are African American students, which supports the GenCyber program goal of increasing diversity in the cybersecurity workforce in the nation.

The games and hand-on activities in our camp curriculum helped attract students' interests in cybersecurity. For each game or hands-on lab, our GenCyber team first developed, tested and revised the course materials. After that, the games and hands-on labs were put in the curriculum in the order of difficulty levels (easy to difficult), and then generated the camp schedule based on the estimated time of each activity. Based on our experience, back-up plans are always needed for hands-on labs of high difficulty levels due to the diversity of participants' experience and computer skills. In addition, more teaching assistants are needed to help participants during a challenging hands-on lab. Our experience showed that the ratio of teaching assistants to participants should be higher than 1:5 in order to run a challenging hands-on lab smoothly.

The social games played a very important role in establishing a friendly learning environment. Our curriculum includes two 15-minutes social games on each day, one in the morning and the other in the afternoon. As a result, after the first two days of a camp, all participants knew each other well and felt comfortable to ask help from other participants and work on hands-on labs and their final project. Some participants became friends and shared their information, knowledge and ideas with each other.

A challenge faced at our camp is disruptive behaviors of camp participants. The high-school teacher in our team is very experienced in handling student disruptive behaviors. However, we still discussed strategies and policies to reduce disruptive behaviors in our short daily review meetings. After trying different strategies and policies, we found that it is very important to emphasize detailed behavior expectations at the beginning of a camp. Meanwhile, instructors and teaching assistants should repeat the behavior policies and expectations to all participants when a disruptive behavior occurs.

Conclusion

In the past two summers, the GenCyber team at NC A&T developed and implemented a highly engaging curriculum for 5-day, non-residential GenCyber camps that enrolled rising 8^{th} to 12^{th} grade students. The camp curriculum includes games, hand-on labs, invited speakers, demos of robot, drone and Internet of Things, and a group project. The GenCyber Cybersecurity Concepts were taught and reinforced throughout the curriculum. All hands-on activities have been tested and revised for high-school students in our GenCyber camps. Some hands-on activities such as the two activities presented in this paper can be used in relevant high-school courses. In addition, Kahoot games and minute-question sheets have been used to assess and strengthen students' understanding on the concepts, knowledge and skills taught at the camps. To track participants' interests in Computer Science and cbersecurity, the team organized follow-up events in the past two Novembers, which were security-focused competitions. All camp students of 8^{th} to 12^{th} grade were invited to attend both follow-up events and about 30% invited students attended the follow-up events.

Our GenCyber camps enrolled more students from underrepresented populations in STEM fields, especially African Americans (AA). At all GenCyber summer camps offered at NC A&T, more than half of participants were AA students. As a result, our GenCyber camps helped improve cybersecurity awareness in the AA communities, and increase diversity in the nation's cybersecurity workforce in the future. In addition, our GenCyber camps also enrolled students who are interested in non-STEM areas such as nursing and business. Exposing them to the basic concepts of Computer Science and cybersecurity may inspire them to direct their talent in cybersecurity-related careers.

Acknowledgments

The camps at NC A&T were funded by GenCyber (DOD/NSA #98230-19-0170 and #98230-18-0083) projects and partially funded Consortium Enabling Cybersecurity Opportunities and Research (NNSA #F1040061-18-17-08 and #F1040061-18-08) CECOR project.

References

1 CyberSeek (2018) "Cybersecurity Supply/Demand Heat Map." Retrieved November 14, 2019, from https://www.cyberseek.org/heatmap.html

2 A Frost & Sullivan Executive Briefing. Global Information Security Workforce Study. 2017. [online] https://www.isc2.org/-/media/B7E003F79E1D4043A0E74A57D5B6F33E.ashx

3 GenCyber PNW website. Retrieved October 29, 2019, from https://www.gen-cyber.com/about/.

4 Chulakorn Aritajati, "A Socio-Cognitive Analysis of Summer Camp Outcomes and Experiences," SIGCSE '15 Proceedings of the 46th ACM Technical Symposium on Computer Science Education Pages 581-586

5 Webb, H. and Rosson, M.B. 2013. Using Scaffolded Examples to Teach Computational Thinking Concepts. Proceeding of the 44th ACM Technical Symposium on Computer Science Education (New York, NY, USA, 2013), 95–100.

6 GenCyber website, Retrieved October 29, 2019, from https://sites.google.com/site/gencyberpnw/cybersecurity-first-principles

7 PBS game. Available from http://www.pbs.org/wgbh/nova/labs/lab/cyber/

8 Kahoot Game. Available from https://kahoot.it/

9 Thunderbird Cup. Available from http://thunderbirdcup.com/

10 Google Interland Game. Available from https://beinternetawesome.withgoogle.com

11 Anti-Phishing Phil. Available from http://www.ucl.ac.uk/cert/antiphishing/

12 Digital Forensics "Academic Dishonesty Case" Tools and instructions to follow the IPAR game. Available from http://forensic-games.csec.rit.edu/ipar/game/

13 Steganography, Class modules, tools and direction to the hands-on exercises. Available from https://cyfor.engineering.nyu.edu/

14 What is the Internet? Available from https://youtu.be/Dxcc6ycZ73M

15 The Internet: IP Addresses & DNS. Available from https://youtu.be/5o8CwafCxnU

16 The Internet: Packets, Routing & Reliability. Available from https://youtu.be/AYdF7b3nMto

17 ExifTool by Phil Harvey. Available from https://sno.phy.queensu.ca/~phil/exiftool/index.html

Biographical Information

Joaquin Hernandez

Mr. Hernandez is a research associate in the Department of Computer Science at North Carolina A&T State University. He received his BSCS and MSCS from North Carolina A&T State University. Before that he received his ASCE from Davidson County Community College. Mr. Hernandez successfully co-led the application for National Center of Academic Excellence in Cyber Defense Research (CAE-R). His research interest is in Machine Learning and The Internet of Things.

Xiuli Qu

Dr. Qu is an associate professor in the Department of Industrial and Systems Engineering at North Carolina A&T State University. She received her MS and Ph.D. in Industrial Engineering from Purdue University. Before that, she received her BSEE and MSEE from the University of Science and Technology Beijing. Her research interests focus on the applications of optimization and systems engineering tools in complex systems such as transportation systems and health care systems. Her teaching interests include Operations Research, Quality Improvement, and Information System Security. Dr. Qu is a member of IIE, INFORMS, and SHS.

Xiaohong Yuan

Dr. Yuan is a Professor and the Chair of the Computer Science Department at North Carolina A&T State University. She is the director of the Center for Cyber Defense, and a Center of Academic Excellence in Cyber Defense Education and Research. She has more than 18 years of teaching and research experience in cybersecurity education, software security, machine learning, intrusion detection, and human aspects of security. She has led the creation of the Interdisciplinary Undergraduate Certificate in Cybersecurity. She has developed many case studies/hands-on labs for teaching cybersecurity, and has used these case studies/labs in her courses.

Jinsheng Xu

Dr. Xu is currently an associate professor in the Department of Computer Science at NCAT. Dr. Xu received his Ph.D. from Michigan State University. He implemented several interactive and animated IA educational tools for students and used them in IA courses to enhance the learning experience. Dr. Xu participated in several funded projects in IA education and research. Dr. Xu successfully led NCAT in application for National Center of Academic Excellence in Information Assurance Education (CAE/IAE). Dr. Xu teaches Data Structures, Advanced Algorithms, Network Security, and other courses.