National Cybersecurity Institute Journal

Volume 2, No. 2

ISSN 2375-592X

National Cybersecurity Institute | 2000 M Street, Suite 500 | Washington, D.C. 20036
Excelsior College | 7 Columbia Circle | Albany, NY 12203-5159

National Cybersecurity Institute Journal

Volume 2, No. 2

NATIONAL CYBERSECURITY INSTITUTE JOURNAL

The National Cybersecurity Institute at Excelsior College is a research center based in Washington, DC, dedicated to increasing knowledge of the cybersecurity discipline and its workforce demands. Published three times a year, the peer-reviewed *National Cybersecurity Institute Journal* covers topics that appeal to a broad readership within the cybersecurity discipline, with a particular focus on education, training, and workforce development. The manuscripts submitted to the journal are reviewed for their contribution to the advancement of applied research in the area of cybersecurity.

Submission guidelines for authors can be found at www.nationalcybersecurityinstitute.org/journal/.

FROM THE EDITOR

Welcome to the fifth issue of the National Cybersecurity Institute Journal. This special edition of the journal focuses on the contribution of community colleges to cybersecurity and was produced with the cooperation of the National CyberWatch Center. This partnership allowed us to draw on the unique perspectives and resources that both organizations are well known for in the cyber community. As the cybersecurity community is fully aware, the mission at NCI is to increase awareness and knowledge of the cybersecurity discipline, and assist the government, industry, military, and academic sectors to better understand and meet challenges in cybersecurity policy, technology, and education. Much attention has been given lately to the role of community colleges in developing our cybersecurity workforce. This edition of the journal provides informative articles that relate to the development of our cyber workforce and are contributed by notable authors with a variety of perspectives. The National Cybersecurity Institute is proud to publish relevant and noteworthy articles three times a year that will serve to enlighten those with a vested interest in the cybersecurity field.

In this edition, Cheryl Calhoun and James Nichols provide an interesting review of the role of community colleges in developing the cybersecurity workforce. This is followed by an informative article on cybersecurity outreach for underrepresented minority students by Gonzalo Perez, John Monaco, Charles Tappert, and Li-Chiou Chen. Ronnie Saturno Jr. then offers his article Bridging the Gap: the role of America's community colleges in the future of America's cyber workforce. Portia Pusey, David Tobey, Diana Burley, Deanne Cranford-Wesley, and Jacob Frank present their article, Cybersecurity Competitions: Recommendations for Assessment, Evaluation and Research. This article is followed by one written by Jake Mihevc, Ronny Bull, Nick Merante, and Brandon Froberg in which they provide a detailed look at the Central New York Hackathon from design through implementation in case study format. Finally, we conclude the journal with the second installment in the NCI Symposium series, Security in Cyberspace, by Jane LeClair and Matthew Flynn.

This brings you the latest information relating to cybersecurity and the workforce, with specific ways community colleges are addressing national needs and deficits in these areas. These articles will provide you, the reader, with knowledgeable insight to bring to the workplace, and instill in everyone you speak with a desire for further thought on how our cyber workforce is, and should be, developed.

A publication such as this journal is never the work of one individual, but rather a collaboration of dedicated individuals at NCI whose hard work results in the quality product you have before you. Naturally my thanks go to all the contributors, administration, and staff for their extraordinary efforts in bringing the National Cybersecurity Institute Journal to you once again. In particular I would like to thank Diane Burley and Denise Pheils for their contributions in bringing this special edition of the journal to fruition. I hope that everyone in the cyber community will find this journal informative as you work within your respective cyber areas. As always, I look forward to your comments, suggestions, and future submissions to the NCI journal.

Jane A. LeClair, EdD

Editor in Chief

Developing a Comprehensive Cybersecurity Curriculum with a Collaborative Learning Environment

Cheryl D. Calhoun | James I. Nichols

ABSTRACT

The primary goal of this NSF-funded project is to develop a comprehensive cybersecurity curriculum to be more appealing to women and other under-represented groups. Based on previous research on effective engagement practices we redesigned our learning environments to be more inviting for students. We remodeled our classrooms to create collaborative learning spaces as warm, welcoming, and "non-techy" in appearance. We revised our curriculum, creating six new cybersecurity courses, which resulted in two new A.S. degree tracks and three college certificates. Finally, we included inquiry-based and collaborative learning in our face-to-face and online courses. Our curriculum now includes hands-on labs in a virtualized environment, collaborative wiki-style editing, gaming, ethics discussions, and competency-based, self-motivated learning modules. We will discuss the successes and challenges we encountered and how we addressed them. We conclude with recommendations for future study and practice.

INTRODUCTION

Research shows well-managed collaborative learning environments improve outcomes for all types of students (Barker & Cohoon, 2008b). For instance, collaborative learning environments improve retention for both men and women and make it easier for women to see how they compare to their peers (Eisenhart & Finkel, 1998). This comparison is especially important for women because they often misjudge their own abilities and opt-out of technology fields when they believe they are not as capable as others (Barker & Cohoon, 2008a).

Employers want to hire employees who have solid technical skills and good workplace skills. Industry research supports these recommendations. According to "Closing the IT Skills Gap" (McKendrick, 2011) employers are looking for critical thinking (70%), writing/communications (61%), interpersonal communications (59%), and project management (57%). Thirty-two percent (32%) of businesses surveyed said the business skills of new hires were unsatisfactory. Collaborative learning environments, which encourage students to work together on learning activities, contribute to the development of professional skills and help students learn practical work techniques, which are used in the Information Technology (IT) workforce (Cohoon, 2011).

The primary goal of the NSF funded "Cybersecurity Program Development at Santa Fe College" (Award #1304342) is to expand the cybersecurity curriculum, increase the recruitment and retention of female students, develop and strengthen

career pathways and provide professional development opportunities for faculty. Santa Fe College (SF) provided additional resources to support the classroom renovations. SF is located in Gainesville, Florida, and serves both Alachua County and rural Bradford County. SF is easily accessible with eight convenient campuses including the Northwest Campus, Blount Center, Center for Innovation and Economic Development, and Institute of Public Safety in Gainesville; the Perry Center for Emerging Technologies in the city of Alachua, and educational centers in the cities of Archer, Starke, and Keystone Heights. SF enrolls nearly 24,000 degree-seeking students annually from Florida, across the United States, and 54 countries. More than 40 percent of SF students come from outside of the two-county district. SF is a charter member of the League for Innovation in the Community College and the winner of the 2015 Aspen Prize for Community College Excellence.

After a brief overview of learning philosophies and collaborative learning, this article will provide details about the courses and learning components used in the cybersecurity curriculum. It will then discuss the classroom renovations and the addition of a NETLAB+ cloud-based learning environment. It concludes with the successes and challenges encountered along the way, and recommendations for future study and practice.

WHY COLLABORATIVE LEARNING?

The learning philosophy for this project is based on social cultural theory and collective cognition where two or more people working together can achieve insights neither could have reached on their own (Lund & Smørdal, 2006). Learning is developed through independent problem solving in collaboration with peers (Vygotsky, 1980). Collaborative learning is different from the more common "divide and conquer" style of group projects where students break up an assignment, individually complete their respective parts, and then compile their parts for group submission. Collaborative learning requires students to work together to accomplish a common goal, it encourages them to engage in intellectual talk with each other, thus improving critical thinking and increasing retention and the appreciation of diversity (Barker & Cohoon, 2008b).

Some of the collaborative assignments use collaborative writing using a wiki environment or Google Docs. Collaborative writing is an activity, which involves the production of a document by one or more authors (Meishar-Tal & Gorsky, 2010). Learning with wikis provides students with the opportunity to construct their own knowledge (Lund & Smørdal, 2006) and to engage in reflection (Forte & Bruckman, 2007).

According to Barker & Cahoon (2008b) collaborative learning should be introduced early in a program to avoid early socializing to perpetuate the stereotype computing is a career in which people work alone. This project provided the unique opportunity to conceptualize, from the ground up, how to include inquiry-based and collaborative learning in a comprehensive way across an entire curriculum.

PROJECT COMPONENTS

The project components include the development of a comprehensive cybersecurity curriculum, the renovation of our classroom labs and the addition of a NETLAB cloud-based learning environment. In designing the curriculum, we capitalized on work done by other community colleges, particularly those participating in the National Science Foundation (NSF) Advanced Technical Education (ATE) community of practice. Our goal was to learn from their experiences and expand upon that knowledge to further develop the practice of preparing information technology and cybersecurity technicians.

Curriculum Revision

The curriculum revision began by identifying six which, together with existing courses, created two new Associate of Science (AS) degree tracks

(Cybersecurity and Digital Forensics as seen in Figure 1) and three college credit certificates (Cybersecurity, Digital Forensics, and Database & e-Commerce Security as seen in Figure 2). Most of the courses align to industry certifications allowing students the option of completing an industry certification in lieu of the course's final exam. Students who have already completed industry certifications can apply for credit by experience for the courses aligned to those certifications. This structure provides students multiple entry and exit points allowing them to earn the degree or college credit certificate appropriate for their career goals.

Surveying the materials available meant obtaining curriculum from a variety of sources including textbooks, case studies, simulations, and hands-on assignments. Cyberwatch (http://www.nationalcyberwatch.org/) and CSSIA (http://cssia.org/) both provide NSF-funded repositories of cybersecurity curriculum. NDG (http://www.netdevgroup.com/products/) and Jones & Bartlett offer curriculum including cloud-based virtual hands-on labs. TestOut Software provides a Security Pro courseware, which includes video instruction, evaluation, and hands-on simulations. EngageCSEdu (https://www.engage-csedu.org/) provides a curriculum repository for computer science and information technology curriculum, which is peer-reviewed and designed to help faculty engage all of their students in computing.

All of the new courses use Instructure's Canvas Learning Management System (Canvas) to support both online and blended/flipped classroom implementation. Canvas provides a convenient way to assemble all course components for student access and provides an organizational framework for curriculum content. It provides synchronous and asynchronous collaborative learning tools where students can work together to complete coursework.

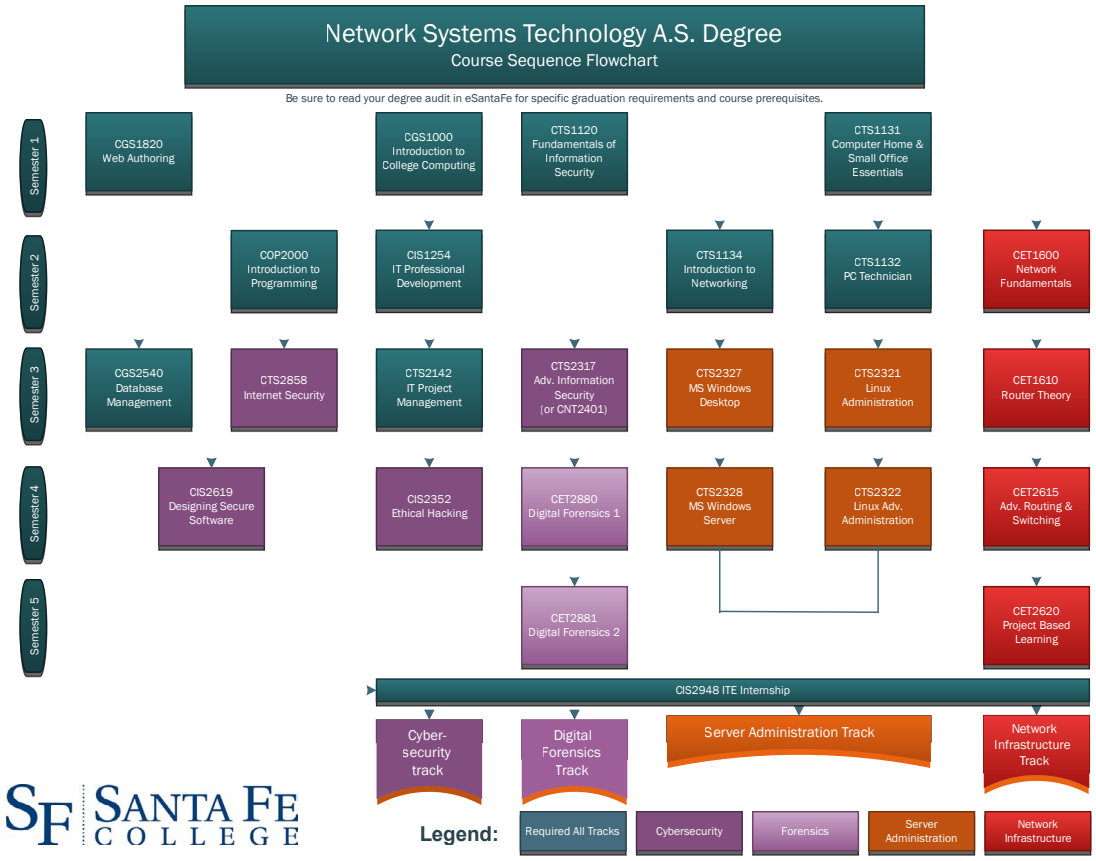

FIGURE 1: COURSE SEQUENCE FLOWCHART — A.S. DEGREES

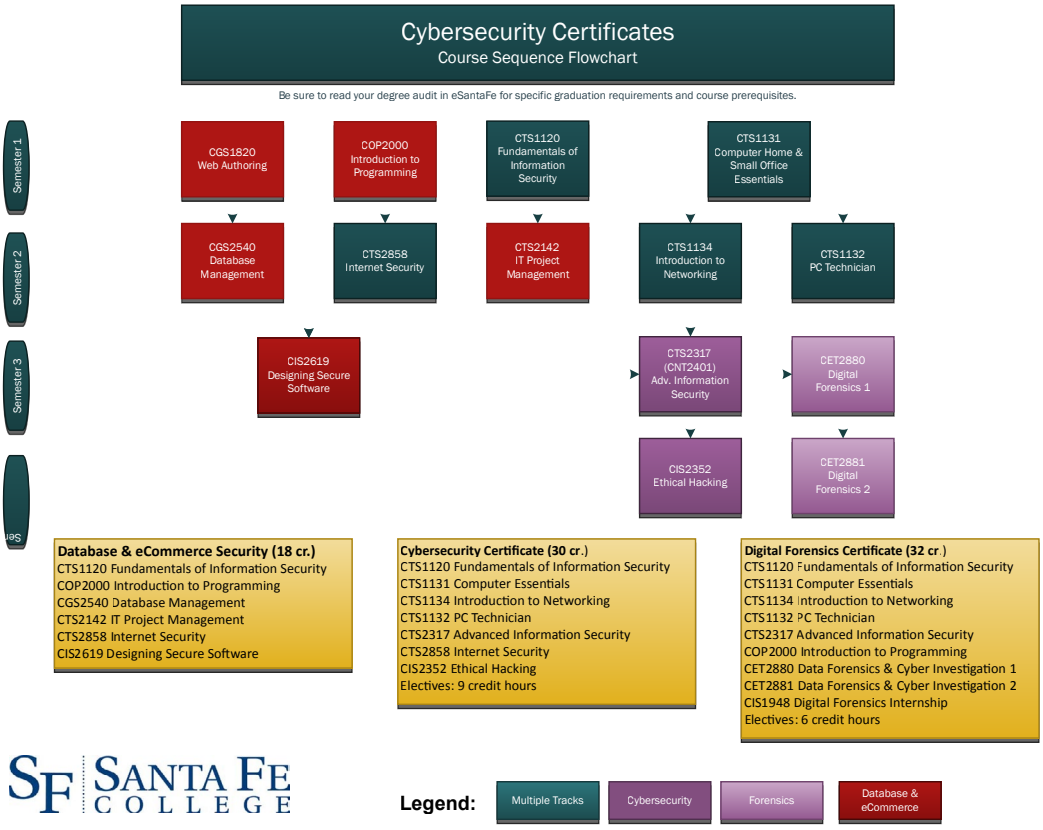

FIGURE 2: COURSE SEQUENCE FLOWCHART – CYBERSECURITY CERTIFICATES

The Courses

The six new courses are Fundamentals of Information Security (CTS1120), Advanced Information Security (CTS2317), Ethical Hacking (CIS2352), Internet Security (CTS2858), Designing Secure Software (CIS2619), and IT Project Management (CTS2142). Below, the goals, curriculum, and learning elements of each course are discussed.

Fundamentals of Information Security (CTS1120)

This course presents a comprehensive overview of the essential concepts of information security including information security standards, education, professional certifications, and compliance laws. It examines how business, government, and individuals operate in the digital world today. The course is designed to provide the beginning student with a comprehensive overview of information security. This course will be used in a variety of degree track programs including IT, Business, Health IT, and AA university transfer programs. The primary text for this class is *Fundamentals of Information Security* (Kim & Solomon, 2014), which comes with PowerPoint slides, test banks, and supplemental assignments. The course includes a Cybersecurity Canon book review, weekly quizzes, and collaborative case study. The content of this course aligns with ISC^2 SSCP certification, but since this is the student's first security course, it is not practical to assume they will be prepared for this exam after just this one course.

Advanced Information Security (CTS2317)

This course provides practical hands-on experience necessary to become proficient in the field of systems security. Students gain practice in implementing intrusion detection and prevention systems, access controls, and file system encryption. The focus is on protecting the confidentiality, integrity,

and accessibility of information systems (the triad of security). This course is competency-based and introduces the students to the process of preparing for industry certification exams. For study materials students can use the TestOut Security Pro curriculum, which includes instructional modules, quizzes and simulations, or they can use a variety of other materials such as certification study guides and Professor Messer's (Messer, 2015) online course. This course includes a Cybersecurity Canon book review and hands-on labs using the NDG NETLAB+ system. The content of this course aligns to CompTIA's Security+ and TestOut's Security Pro industry certifications.

Ethical Hacking (CIS2352)

This course provides the fundamental knowledge necessary for a student to become proficient in understanding the techniques of computer hacking and how to respond to hacking related incidents. Students are prepared to identify vulnerabilities and respond to attacks in an attempt to predict and prepare for tomorrow's exploits. This is an advanced level course designed for cybersecurity and digital forensics students. This primary text for this class is *Cyberethics: Morality and Law in Cyberspace* (Spinello, 2010), The course includes ethics discussions, a Cybersecurity Canon book review, hands-on labs using the NDG NETLAB+ system and the NCL (http://www.nationalcyberleague.org/) challenge.

Internet Security (CTS2858)

This course teaches how to secure a home network from unauthorized activity. Security principles, such as establishing an effective security policy and the different types of hacker activities a practitioner is most likely to encounter are topics of interest. The primary text used in the class is the CIW Web Security Associate course workbook. This course includes class discussions, a Cybersecurity Canon book review, module quizzes, and certification practice exams. This course aligns with the industry certification standards evaluated in the Certification Partners CIW Web Security Associate exam. Students take the CIW Web Security Associate exam in class as their final exam.

Designing Secure Software (CIS2619)

Students learn about security in the planning and delivery of software systems. This design of security in applications extends from the management of a project, to the implementation of projects primarily or partially comprised of software, from basic terminology to an understanding of the situation that security professionals and developers face in the current climate of cybercrime and rampant malicious. Students learn how to test code, perform code review, and identify weaknesses and threats to systems as well as inherent security flaws in programming languages. This course uses the *Secure Software Design* book (Richardson & Thies, 2012) and labs created by Debbie Reid, Professor, Information Technology Education, Santa Fe College. This course includes hands-on, written assignments, discussions, exams and a final exam.

Project Management (CTS2142)

The primary objective for this course is to introduce IT students from across the disciplines of networking, programming, and cybersecurity to the fundamentals of the Project Management Body of Knowledge (PMBOK). Although popular software tools for project management were a topic, mastery of project management tools was not the focus of laboratory assignments. The primary textbook used was *Information Technology Project Management* (Schwalbe, 2013) along with related test banks. Students were also required to read *How to Win Friends and Influence People in the Digital Age* (Carnegie, 2011). Students discuss people skills proposed by the supplemental reading within the context of realistic problem solving in the work place. This course includes weekly quizzes, online discussions, and weekly group collaborations.

Curriculum Components

Each of the new cybersecurity courses includes inquiry-based, collaborative, and hands-on learning. Inquiry-based assignments require students to go beyond what is included in their course textbooks or materials. They must seek out additional resources and information, share knowledge with peers, or co-create solutions. Collaborative assignments require them to work together with other students to develop or create a solution to a project, task, or case. Hands-on assignments allow students to practice doing the technical skills needed to be successful in cybersecurity. Below we will discuss some of the assignments incorporated in this curriculum including the Cybersecurity Canon book report; online collaborative group assignment; face-to-face collaborative assignment; ethics discussions; competency-based self-motivated learning modules; and the integration of the National Cyber League challenge.

Collaborative Online Group Assignments

The collaborative online weekly group assignments are designed to provide students with experience in working in a collaborative group project. This assignment was piloted in CTS1120 Fundamentals of Information Security. The assignment utilizes a threaded case study provided with *Foundations of Information Security* (Kim & Solomon, 2014). The case studies are modified slightly to work with a group approach. Students work together using the group tools provided in Canvas. Groups consisted of three students. Students were allowed to self-select groups up until the starting date of the assignment, when the instructor randomly assigned all remaining students to groups. Students then use discussion forums to discuss the questions in the case and plan out how they will respond to the case. They use the wiki-style pages editor in Canvas to co-create a single response to each weekly case. The project was designed based on collaborative learning as demonstrated by using a wiki editor to co-create the group's policy or procedure document. Students were graded individually on their group participation. The resulting group document was graded on the quality of the content.

Collaborative Face-to-face Assignments

Collaborative assignments in our face-to-face courses utilized the pod-based classroom setup. The IT Project Management (CTS2142) piloted this project. The weekly laboratory assignments were team oriented and specifically designed to demonstrate an important aspect of the weekly reading. On-line reading quizzes were taken prior to class to ensure students were familiar with the textbook material to be reinforced during the laboratory period. The laboratory was a 2.5-hour class period. At the beginning of each class session there was a brief overview of the leading topics along with an opportunity for discussion. Following discussion, students broke out into their assigned teams. Team composition was designated and rotated by the instructor to ensure diverse composition of the teams and to avoid clustering by IT discipline or degree. Each assignment was unique, requiring students to reach out for innovative views, strategies, and solutions. One joint laboratory report was prepared by each team and submitted at the end of every class period for assessment. Students not attending the laboratory class session did not receive credit for the laboratory report, which was a significant portion of their course grade. This laboratory report emphasized to students the importance of the collaborative team sessions. One laboratory assignment included a guest speaker who was an IT Project Manager from a local technology firm. After the speaker left, each team wrote a letter of appreciation to the speaker's CEO. At the end of all laboratory assignments, teams presented their work to the overall class.

Cybersecurity Canon

The Cybersecurity Canon assignment was designed using Rick Howard's Cybersecurity Canon blog post (Howard, 2014b). In this post, Rick Howard, Palo Alto Networks' Chief Security Officer, identifies a list of must-read books for all cybersecurity professionals. In addition, he challenges professionals in the field to identify and suggest additional titles that provide accurate information about the history of cybersecurity or provide important technical or background information about the field. The Cybersecurity Canon assignment is included in four

of the cybersecurity courses, allowing students to read and report on several of the books in the canon throughout their program.

This assignment will provide students with exposure to good professional development habits and encourage deeper dialog about the field of cybersecurity. Students choose a book from the Cybersecurity Canon to read. They then post a message on the assignment discussion board identifying their book and the rationale for why they have selected this book. This post helps the instructors to know the student is on track with the assignment, and creates a great interaction point among students as they share their book interests. After reading their book, students write a book review styled similar to those posted on the original "Books You Should Have Read By Now" post on Terebrate.blogspot.com (Howard, 2014a). Students share their book reviews with their classmates via a Canvas discussion. Many students comment about how they are interested in reading more of the books after they have read another student's review. They will often share tips about related movies or other titles they feel will be of interest to classmates.

Ethics Discussions

The CIS2352 Ethical Hacking course includes a series of six ethics discussions. These discussions, which are guided by readings from Spinello (2010), allow students to explore a variety of topics with regard to legal and security aspects of the Internet such as intellectual property, free speech vs. content controls, regulation vs. governance, and the differences between self-governance, and ethical vs. legal actions. Students initially post answers to four discussion questions based on the chapter readings and their perceptions on one of the cases presented at the end of the chapter.

The ethics discussion assignment uses the Canvas discussion forum, which allows the option of restricting a student's access to other students' posts until after they have submitted their own initial post. Once students have posted their individual answers and perceptions of the case, the discussion board will open up and reveal any posts previously submitted by other students. Students then read and discuss the merits of each other's perspectives on these issues. The grading rubric addresses both quality of content and discussion. Students who stimulate the most discussion about their original post can earn extra credit points.

National Cyber League Challenge (NCL)

This capture-the-flag style competition allows students to challenge themselves both individually and as a team. The NCL provides students both with a gymnasium-tutorial system where they can learn new cybersecurity skills as well as a multi-round competition in which they are challenged to use their skills to accomplish both individual and team related tasks. Currently the NCL is held annually in the Fall semester. It is a virtual competition, which allows students to compete using just a browser with Internet access. All tools and resources required are available within the virtual system. Eight students participated in the NCL challenge during the Fall 2014 event. All students who participated stated that their participation both challenged them and excited them about learning more about cybersecurity.

Classroom Renovation

The classroom renovation included four Networking Systems Technology (NST) classrooms, which house the cybersecurity program. The classroom design replicates a modern workspace for IT professionals and with the purpose of exposing students to problem solving in a team setting.

FIGURE 3: NETWORK SYSTEMS TECHNOLOGY CLASSROOM

The remodeled classroom labs include learning spaces, which are warm, welcoming, and "non-techy." These spaces allow students to work together on group projects or just support each other during hands-on learning labs.

Each of the four classrooms facilitates a different learning implementation that encourages student collaboration and hands-on learning. Three of the classrooms use laptop computers instead of desktop computers. When not in use, the laptops are stored in a lockable charging cabinet. This cabinet keeps the classrooms looking clean and inviting. One of the classrooms is outfitted with Node Chairs (Steelcase) and portable white boards, which allow students to work together in various configurations. A second classroom is outfitted with Techworks workbenches (Mayline, 2015) where students work in pairs in computer architecture and Cisco Certified Network Associate (CCNA) Routing & Switching classes. A third classroom uses collaborative pods. Each pod includes a wide desktop surface configured for five laptops, five swivel chairs, and a large screen monitor with an HDMI connection. All five students can connect to the large screen monitor, but only one student at a time has the capability to display their results on the team monitor. The fourth classroom is a more traditional style lab where students have access to dual-boot iMacs stationed around the perimeter of the room allowing for easy mobility throughout the room.

NETLAB+ Hands-on Learning Labs

The NETLAB+ system (Network Development Group, 2015) has allowed us to move our hands-on learning labs to a virtualized cloud based system. Using NETLAB+ students can schedule and complete hands-on assignments from a computer with a browser, Java, and internet access. The hands-on assignments provide real world experience in securing networked systems. This system utilizes a VMWare vSphere server configuration to manage device images in a learning pod. Each pod is isolated in a sandbox network so the devices can communicate to each other over a virtual network link, but they are not able to access the Internet directly. The NETLAB+ system serves as a proxy server, which manages the scheduling and loading of lab resources as needed for students to complete their lab assignments.

The National Information, Security & Geospatial Technologies Consortium (NISGTC) under the Department of Labor Trade Adjustment Assistance Community College and Career Training (TAACCT) grant has developed hands-on labs for the NETLAB+ system that support Ethical Hacking, Security+, Digital Forensics and a variety of other networking a security related curriculums. These labs are made available for use under the Creative Commons License and are available through CSSIA (http://cssia.org/; http://www.netdevgroup.com/products/). An additional side effect of using the NETLAB+ system was that it contributed to the goal of remodeling our classrooms. Because students can now access their learning labs through a cloud-based environment, we are able to streamline the technology located in the classroom. We have maintained one classroom that has rack-mounted servers, routers & switches so students gain familiarity with the look and feel of working with physical equipment.

SUCCESSES, CHALLENGES AND RECOMMENDATIONS

A challenging part of this curriculum revision was working with students in collaborative learning environments. At first students were resistant in both online and classroom collaborative environments. Many students would not engage, which created frustration among the students who did engage. Others were reluctant to edit each other's work, and wanted to divide work for individual completion. In the two courses focusing most heavily on collaborative work (CTS1120 and CTS2142), the faculty worked to refine the assignments by providing additional scaffolding to help students learn how to work together collaboratively. Some students expressed the opinion that collaborations skills were not needed for an IT or cybersecurity field. They were of the opinion, we should only be teaching them technical skills.

An additional challenge of instructing in a collaborative environment was the development of laboratory assignments, which were 1) team oriented by nature and 2) with technical issues, which were recognizable, by all IT disciplines represented. Informal student feedback indicated that changing activities and alternating the format of assignments was what kept the collaboration fresh and alive. Students indicated a preference for the collaborative learning style with one caveat: they would not want all IT courses presented in this style. As we continue to evaluate this curriculum, we will need to work to better refine the collaborative assignments and help students develop skills for collaborative work.

Hadjerrouit (2014) and Meishar-Tal and Gorsky's (2010) findings were very similar to those experienced at Santa Fe College. In both of these studies, students were resistance or reluctant to edit each other's work, late participation by students prevented real collaboration, and students exhibited a lack of collaborative writing skills. Both Hadjerrouit (2014) and Meishar-Tal and Gorsky's (2010) cite a need for more research, including inquiry into how to help students to develop collaborative editing skills.

Redesigning the classrooms to be neat as well as collaborative has already produced visible results. Previously, students would come into the first class and wait quietly until the instructor started the class and over the course of the semester, students would talk with other students. Now on the first day of class, students begin talking with each other because they are facing each other and likely feel a social responsibility to converse. One instructor even noted that she used to work hard to get students to interact. Now they are interacting naturally, sharing Facebook and social networking information, and connecting with each other outside of class. Additionally, having the shared monitors for collaboration has assisted in activities such as gamification or game-mechanics. For example, students are now able to pose questions for other groups as well as display their own answers. This creates a more of a game-like feel and invites students to be more immersed into the game zone.

The NETLAB+ system has been a wonderful success. Students have been able to improve their core technical skills through these labs. Current implementation includes ethical hacking labs and CompTIA Security+ aligned labs. For future expansion, it is desirable to use the NETLAB system to develop secure programming labs and digital forensics curriculum.

Future study should include expanding upon student participation evaluations to get a better sense of where students are struggling with the collaborative assignments. Additional scaffolding should be developed to help students learn how to work in collaborative environments and to tie student's perception of skills needed to be successful in an IT field and collaborative work. The collaborative learning assignments in CTS1120 Fundamentals of Information Security have only been offered in an online environment. That course will be offered in a face-to-face classroom in Fall 2016, which will afford the opportunity to evaluate and compare the results of the collaborative assignments in the classroom as compared to the results achieved in an online environment.

SPECIAL THANKS

Our special thanks to Debbie Reid, professor, Information Technology Education, and Susan Warshaw, adjunct professor, Information Technology Education, for their work on this project. Debbie Reid was the original developer for CIS2619 Secure Programming and Susan Warshaw was the original developer on CTS2142 IT Project Management. Debbie Reid provided detailed information on the Secure Programming course for this article. Susan Warshaw also provided documentation and input on the IT Project Management portion of this article.

Funding for this project was provided partially from the National Science Foundation's (NSF) Advanced Technical Education (ATE) program, Award #1304342. In addition, Santa Fe College (SF) provided resources for renovating the four primary classrooms utilized by the Networking Systems Technology (NST) program where the new cybersecurity curriculum will be offered.

REFERENCES CITED

Barker, L., & Cohoon, J. M. (2008a). How do you recruit or retain women through inclusive pedagogy? Boulder, CO: NCWIT.

Barker, L., & Cohoon, J. M. (2008b). How do you retain women through collaborative learning? In N. C. f. W. I. Technology (Ed.). Boulder, CO NCWIT.

Carnegie, D. (2011). *How to win friends and influence people in the digital age.* Simon and Schuster.

Cohoon, J. M. (2011). Design physical space that has broad appeal. In NCWIT (Ed.). Boulder, CO NCWIT.

Eisenhart, M. A., & Finkel, E. (1998). *Women's science: Learning and succeeding from the margins.* University of Chicago Press.

Forte, A., & Bruckman, A. (2007). *Constructing text: Wiki as a toolkit for (collaborative?) learning.* Paper presented at the Proceedings of the 2007 international symposium on Wikis.

Hadjerrouit, S. (2014). Wiki as a collaborative writing tool in teacher education: Evaluation and suggestions for effective use. *Computers in Human Behavior,* 32(0), 301-312. doi: http://dx.doi.org/10.1016/j.chb.2013.07.004

Howard, R. (2014a). Books You Should Have Read By Now. Retrieved from http://terebrate.blogspot.com/2014/02/books-you-should-have-read-by-now.html

Howard, R. (2014b). The Cybersecurity Cannon: Books every cybersecurity professional should read. Retrieved from https://paloaltonetworks.com/threat-research/cybercanon.html

The Center for Systems Security and Information Assurance. Retrieved from http://cssia.org/.

The National Cyber League. Retrieved from http://www.nationalcyberleague.org/.

National Cyberwatch Center. Retrieved from http://www.nationalcyberwatch.org/.

Network Development Group. Retrieved from http://www.netdevgroup.com/products/.

NCWIT EngageCSEdu. Retrieved from https://www.engage-csedu.org/.

Kim, D., & Solomon, M. G. (2014). *Fundamentals of Information Security.* Jones & Bartlett Learning.

Lund, A., & Smørdal, O. (2006). *Is there a space for the teacher in a WIKI?* Paper presented at the Proceedings of the 2006 international symposium on Wikis.

Mayline. (2015). Technology Furniture. Retrieved from http://www.mayline.com/product-detail.php?id=P1088

McKendrick, J. (2011). Closing the IT Skills Gap: 2011 SHARE Survey for guiding university and college IT agendas. Unisphere Research, a division of Information Today, Inc.

Meishar-Tal, H., & Gorsky, P. (2010). Wikis: what students do and do not do when writing collaboratively. *Open Learning: The Journal of Open, Distance and e-Learning,* 25(1), 25-35. doi: 10.1080/02680510903482074

Messer, P. (2015). Professer Messer Online Security+ Training. Retrieved from http://www.professormesser.com/

Richardson, T., & Thies, C. N. (2012). *Secure software design.* Burlington: Jones & Bartlett Learning.

Schwalbe, K. (2013). *Information technology project management.* Cengage Learning.

Spinello, R. (2010). *Cyberethics: Morality and law in cyberspace.* Jones & Bartlett Learning.

Steelcase. (2015). Node School Chairs. Retrieved from http://www.steelcase.com/products/collaborative-chairs/node/

Vygotsky, L. S. (1980). *Mind in society: The development of higher psychological processes.* Harvard university press.

AUTHORS

Cheryl Calhoun (cheryl.calhoun@sfcollege.edu) is the dean of Educational Centers and director, Blount Center, at Santa Fe College and a professor in the information technology education program. Her principle area of research is in increasing the student diversity in the information technology educational pipeline. She is the P.I. of the National Science Foundation, Advanced Technical Education, "Cybersecurity Program Development at Santa Fe College" grant. She serves on the community college leadership team for the National Center for Women in Technology (NCWIT) Academic Alliance and the Faculty Track Committee for the Grace Hopper Celebration. She served as a mentor for the Emerging Women in Technology Startups (eWITS) program at UF's Innovation Hub. She received her BS in Food and Resource Economics and an MBA from the University of Florida. She received a graduate certificate in Information Assurance for the University of Illinois Springfield and is currently pursuing a PhD in Educational Technology from the University of Florida. She holds Network+, IT Project+, Security+, CTT+, MCNE, MCNI, CIW Web Professional, and Web Foundations industry certifications

James Nichols (james.nichols@sfcollege.edu) is an assistant professor in the Information Technology Education program at Santa Fe College. His research interests are in using gamification techniques to engage students in the classroom. He is senior personnel on the National Science Foundation, Advanced Technical Education, "Cybersecurity Program Development at Santa Fe College" grant. He received his BS in Computer Science from UNC-Pembroke and a Master of Computer Engineering from the University of Florida where he served as teaching assistant for graduate courses in Software Engineering, Software Specification, Software Testing & Verification, and Human-Computer Interaction. He is currently pursuing a PhD in educational technology at the University of Florida. Previous experience includes serving as a consultant for Risk Analysis on a NASA project and as a Software Engineering lab instructor for Infosys in India. He is A+ and CCNA-Routing and Switching certified.

Partial funding for this project was provided by the National Science Foundation's Advanced Technical Education program, Award #1304342.

Cybersecurity Outreach for Underrepresented Minority Students

Gonzalo Perez, PhD | John V. Monaco, PhD | Charles C. Tappert, PhD | Li-Chiou Chen, PhD

The authors would like to acknowledge the support from the National Science Foundation under Grant No. 1241585. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation or the U.S. government.

ABSTRACT

Growing a cybersecurity workforce begins with generating student interest. One way for community colleges to develop a cybersecurity workforce is by exposing students to active research through academic partnerships with established cybersecurity research institutions. In 2012, Passaic County Community College and Pace University formed a partnership to better attract underrepresented minority community college students into the cybersecurity field of study. The purpose of the partnership was to expose underrepresented minority students to a four-year university in order to promote transfer, to engage the students in various hands-on experiments and activities, and to teach the students how to write a research paper from the results of their experiments. The result has been positive for our students and 82% have transferred to four-year institutions in an information technology or cybersecurity field.

INTRODUCTION

Cybersecurity has been identified as one of the most serious economic and national security challenges facing our nation today. Cyber-attacks are becoming more prevalent, and no organization or individual is immune from nefarious hackers. In order to strengthen the nation's security interests, significant effort is needed to recruit and build a 21st-century cybersecurity workforce. According to the Bureau of Labor and Statistics, the rate of growth for jobs in information security is projected at 37% from 2012–2022, which is higher than the average for all other occupations (Bureau of Labor Statistics, 2014). Hence, the demand for cybersecurity professionals is soaring, and leveraging an emerging underrepresented minority (URM) group of community college students is an ideal strategy to consider. According to a study by Cornell University ILR School, fewer women and minorities are receiving bachelor degrees in STEM disciplines (Griffith, 2010). The percentage of men entering STEM fields was higher than that of women (33% vs. 14%); Asian/Pacific Islander students experienced a 47% STEM entrance rate as opposed to other groups (19–23%) (Chen, 2009). Some reasons cited as to the lower entrance rates for these groups include lack of preparation throughout secondary education and a lack of positive role models in the same gender or race. (Griffith, 2010).

One approach to support cybersecurity adoption and retention is through an academic partnership formed between a community college and

established cybersecurity research institution. This provides URM community college students a clear pathway into a field that will afford a rewarding career, as well as directly benefit society.

The paper describes the cybersecurity outreach program that resulted from such an academic partnership. Using Passaic County Community College (PCCC) and Pace University as a case study, recommendations are made for other institutions interested in forming similar relationships. A background on behavioral biometrics is provided, including keystroke, mouse motion, and mobile touchscreen behavior, as a prelude to the biometric experiments that were cooperatively conducted between the community college and university students. Additionally, this article defines best practices that were developed to increase the impact on student success. Finally, some conclusions are drawn based on the feedback provided by the students through a reflection paper.

BACKGROUND

In 2012, Passaic County Community College and Pace University formed a partnership to better attract underrepresented minorities (URM) into the cybersecurity field of study. Pace has been a designated National Center of Academic Excellence in Information Assurance Education (CAEIAE) by the National Security Agency and the Department of Homeland Security since 2004. PCCC students traveled to Pace throughout the semester and also worked on various hands-on activities in between meetings as part of a cybersecurity outreach program. At the end of the research project, students had an opportunity to present their findings at Pace University's Annual Research Day Conference and publish their joint paper in the official conference Proc. (Farnon, et al., 2013) (Ciaurro, et al., 2014). Student research projects were in the area of behavioral biometrics, exposing the cohort of students to topics of growing interest in cybersecurity. The projects focused on behavioral biometrics, including keystroke, mouse motion, and touchscreen gestures on mobile devices. Additionally, Pace offered a cybersecurity day workshop to an alternative group of PCCC students in order to attract new groups of students to cybersecurity for the following academic year. The workshops introduced additional areas of cybersecurity to students such as Web security, mobile forensics, and keystroke biometrics. Information was made available to students regarding the CyberCorps scholarships supported by the National Science Foundation for students interested in pursuing a degree in cybersecurity at Pace University and working for the federal, state, or local government upon graduation.

Program Structure

The PCCC research team consisted of a total of 17 URM students in the spring semesters of 2013 and 2014. Students were made aware of the program by advertising on campus via posters, flyers, email blasts, and most importantly, faculty announcements in class. Students were interviewed and were selected by the following criteria:

- Computer Science, Engineering Science, Electrical Engineering Technology or Information Technology Major;
- Grade Level, (at least 3rd semester);
- GPA 2.5[1];
- Student schedule availability.

Students with a lower GPA were considered; however, motivation and commitment are important factors to consider when selecting students that are struggling academically. Once a cohort is recruited; all of the students meet each other via a kick-off meeting and expectations are made clear to all students.

The program was modeled similarly to an agile design approach that is utilized in the Doctor of Professional Studies program at Pace University (Alipui, et al., 2014). Students traveled to Pace from Paterson, New Jersey, four times during the

[1] GPA requirement was lowered in order to motivate the average students, which helps to increase retention, graduation, and ultimately transfer.

semester and worked on various problems onsite and in-between sessions that would ultimately result in a research paper submitted to Pace's Annual Research Day Conference. The four sessions are briefly described.

Session 1 included an introduction to Pace's Cybersecurity Program and the CyberCorps: Scholarship for Service Program. Students were exposed to active areas of research in biometrics and an overview of the research conducted at Pace University. Students also participated in data capture exercises to enroll them into a mobile biometric authentication system and later perform a live test of the system. A university tour with an admissions representative including information about transfer and scholarships was also given. Assignments for this session were to perform a literature review on keystroke and mobile biometrics in order to build context and learn best practices in writing a research paper. Data Capture exercises were conducted for the students to begin the enrollment phase of the biometric system.

Session 2 consisted of an introduction to data, analysis, and reporting. Elementary data analysis techniques were introduced, such as Euclidean distance and the nearest neighbor classifier. Biometric system analysis was described, including system evaluation in terms of empirical error rate. After this session, students began drafting their research paper and drawing conclusions based on several biometric experiments.

Session 3 prepared students to write a research paper for journal submission. Research methodology, specifically concerning biometrics and cybersecurity, was introduced. After this session, students collaborated in order to complete the paper and submitted it to the Research Day conference.

Session 4 was the final session where students presented their findings at Pace University's Research Day Conference.

Two or more weeks are needed in order for students to complete the assignments in between sessions. An advisor on the community college side must manage the program and follow up with students in order to ensure that work is being completed in a timely manner. Meetings are required at the community college sites in-between sessions where students can further collaborate on their projects and stay on track with their responsibilities. Online collaboration tools such as Google Docs/Hangouts and Microsoft One Drive were introduced to the students to encourage collaboration outside the classroom.

STUDENT PROJECTS

Students were afforded the opportunity to learn about general biometric topics, keystroke biometrics, mouse motion, and touchscreen gestures on mobile devices all via hands-on experiments. Behavioral biometrics is a growing area of research in cybersecurity, as suggested by recently issued RFPs by DARPA (DARPA, 2013) and the recent designation of the Defense Forensics & Biometrics Agency, established by the Secretary of the Army as an agency dedicated to biometric defense applications (McHugh, 2013). Several market reports indicated that biometrics will be about a $20 billion industry by 2020–2024 (TechSciResearch, 2015; Tactica, 2015).

Utilizing hands-on activities at a level that the individual student can understand and appreciate has proven to better engage, motivate, and increase student STEM proficiencies (Davis, et al., 2012). A biometrics project is ideal for this scenario as this field is itself extremely multidisciplinary, drawing from other fields such as human-computer interaction, machine learning, and hardware and software design.

BIOMETRICS BACKGROUND

Biometrics is the study of utilizing measurable human characteristics to identify, verify, and authenticate an individual. There are two major classes of biometrics: physical and behavioral. Physical biometrics consists of fingerprints, facial features, or scanning an individual's iris.

Behavioral biometrics includes analyzing a person's behavior, such as the manner in which a person walks (gait), eye movement, or keystroke input. There is not always a clear distinction between the two, as speech is considered both a physical and behavioral biometric since the way a person speaks depends on both physiology and behavior.

Behavioral biometrics, such as those that involve human-computer interaction, have become an increasingly popular solution for certain cybersecurity applications. It is believed that intrusion detection systems based on behavior may offer a robust solution to keeping networks and physical computers secure. Continuous authentication systems are designed to re-authenticate an individual continuously while an application is in use to offer greater security. Identity verification also bodes a solution, as a number of courses are now freely available online through massively open online (MOOC) course providers. Online course provider Coursera has begun offering certificates of course completion by verification of the student through keystroke dynamics, among other factors (Maas, et al., 2014).

A biometrics authentication system is typically evaluated based on empirical error rates from simulated authenticate scenarios. There are two types of errors that can occur during authentication: a false rejection occurs when a genuine user attempts to authenticate and is rejected by the system, and a false acceptance occurs when an imposter successfully authenticates as another user. These correspond to Type I and Type II errors in statistics, respectively.

In simulating many genuine and imposter authentication scenarios, the empirical false reject rate (FRR) and false acceptance rate (FAR) can be determined. There is a direct tradeoff between the FRR and FAR, which is controlled by a system parameter. The receiver operating characteristic (ROC) curve is a summary of the relationship between FRR and FAR, as a function of the system parameter. Typically, the performance of a system is summarized by the equal error rate (EER), the point on the ROC curve at which the FRR and FAR are equal.

KEYSTROKE BIOMETRICS PROJECT

In the spring of 2013, the students embarked on a keystroke biometric research project. The project focused on authentication of an individual user based on his/her various behavioral patterns on a desktop computer, such as typing and mouse movement.

The project was executed in four phases: first, the students collected data to simulate enrollment in a keystroke and mouse biometric authentication system. Next, students contemplated various behavioral traits that would be indicative of a user's identity. This was done with the help of experts from Pace, and ultimately a set of features were developed to capture user behavior. Experiments were then designed and carried out to simulate many genuine and imposter authentication scenarios. Finally, students reported their findings in a research paper.

DATA COLLECTION

The enrollment phase included performing three tasks: editing text, navigating a Web browser, and online gaming. The text and browser tasks consisted of six different scenarios each while the online gaming task consisted of two scenarios that were repeated six times each. For all three tasks, participants were asked to complete two scenarios for practice one time, and then complete all scenarios in each task one time. The students began collecting data during the sessions held at Pace and completed data collection independently as necessary.

During each task, all the user's interactions with the computer were recorded. The information obtained includes the timestamps of keys pressed and released on the keyboard, mouse pointer coordinates, and clicking and scrolling actions performed with the mouse. Events were logged by a cross-platform Java application developed at Pace University that utilizes the jnativehook library to register system-wide hooks (kwhat, n.d.). The data was transmitted by the logger to central server for processing. Figure 1 shows the Web interface students used to launch the logger (via Java Web Start) and begin each task.

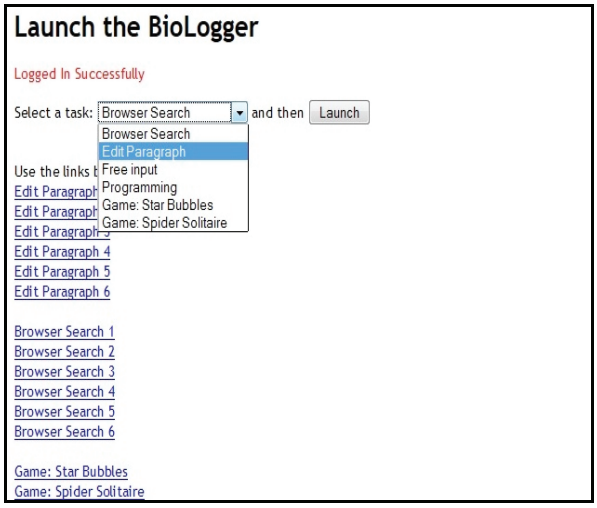

FIGURE 1: BIOLOGGER TASK SELECTION INTERFACE

Edit Tasks

Edit tasks are typical of activities performed by computer users. The tasks for this study were designed to induce a significant cognitive load and require hand-eye coordination and manipulation of the mouse and/or the keyboard. Six edit scenarios were prepared. Students were presented with a portion of text that they had to edit to match another non-editable portion of text on the screen. A typical sample edit scenario is listed below. The **given** text is what the student had to modify to make it match the **accepted** text, and the **edit** text highlights the changes that had to be made for the student to complete the task. In the edit text, insertions are underlined, and deletions are denoted by a strike through.

Given Koobface is a computer worm that spreads through social networking sites. Its name is an anagram for Facebook. The worm aims at Web users.

Edit Koobface is a multi-platform computer worm that spreads primarily through social networking sites. Its name is an anagram for Facebook. The worm ~~aims~~ targets at ~~w~~Web users.

Accepted Koobface is a multi-platform computer worm that spreads primarily through social networking sites. Its name is an anagram of Facebook. The worm targets Web users.

Each of the six edit tasks were designed to require either *minor edits* that do not alter the meaning of the text, such as the correction of typos, or *moderate edits,* such as structural reorganizations and word substitutions.

Browser Tasks

Browsing tasks were designed to induce a typical Web browsing session. There were six Web-browsing scenarios, each containing instructions similar to those below.

- Open a browser and go to Yahoo: http://www.yahoo.com/
- Click on Sports (left menu) MLB (top menu) Teams (top sub-menu) Boston Red Sox Team Report for the Boston Red Sox
- Go back two pages
- ...
- Exit tab or browser

Gaming Tasks

The students were required to complete 12 game-playing sessions, six sessions for each of two games: Spider Solitaire and Star Bubbles. The games were selected to require heavy interaction with the computer, in comparison with the edit and browse tasks. Both games are operated primarily by the mouse, with little or no keystroke information recorded during these sessions. They are both Web-based and run in a typical browser. After launching the logger, students were directed to read the rules for each game before the first session of that game. For each session, they were instructed to play one hand (Solitaire) or one round (Star Bubbles), attempting to finish the game.

Dataset Summary

The average number of events per sample for each type of event is shown in Table 1.

Number Events				
Task	Motion	Click	Scroll	Keystroke
Edit	4.5k	28	1	233
Browse	4.6k	33	108	107
Solitaire	12.6k	86	29	15
Star Bubbles	8.3k	110	46	5

TABLE 1: AVERAGE NUMBER OF EVENTS PER SAMPLE FOR EACH TASK

FEATURE EXTRACTION

As part of the second phase of the project, students worked with researchers from Pace to develop a set of features that capture user behavior. This involved introducing students to previous research in keystroke dynamics, which includes a well-established set of features (Tappert, et al., 2010).

Keystroke Dynamics

Keystroke biometrics has developed around the concept that each individual possesses distinctive, measurable typing characteristics and that any variation is improbable to duplicate by an imposter. Although keystroke biometrics has been one of the least studied behavioral biometrics, it is gaining in popularity due its low-cost and ubiquity. A keystroke event is generated when a key on the keyboard is pressed and released. The events occur in a sequence ordered by the timestamp of the press action, and each keystroke event contains the name of the key, the press time, and the release time.

The set of features used in this experiment were adapted from (McHugh, 2013). A total of 218 keystroke features are used, consisting of means and standard deviations of keystroke duration and latency times. The duration is the time that a key is held down for. There are four different types of latencies, and only two are used here: a release-press (RP) latency is the time from the release of a key to the time of the press of the next key. A press-press (PP) latency is the time between the presses of successive keystrokes. While a RP latency can be negative when the second key is pressed before the first one is released, and PP latency is always positive since the press timestamps in the sequence of keystrokes is monotonically increasing. The first 218 keystroke features in Appendix A of (McHugh, 2013) are used to obtain experimental results for the students.

Subsequent data pre-processing includes outlier removal and normalization as described in (McHugh, 2013). Since some tasks are dominated by interaction via the mouse and not the keyboard, a mechanism for dealing with missing data is needed. A linguistic fallback hierarchy, also described in (McHugh, 2013) is used to account for missing keystrokes. This ensures that keystroke features will not contain null values. Infrequently occurring keys are augmented with observations from other keys before computing the feature value.

MOUSE MOTION BIOMETRICS

The mouse input device is widely used today, and it is believed that mouse movement or touchpad behavior is unique to an individual and can be utilized as a method of authentication. While keystroke biometrics has seen an increase in research recently, mouse dynamics research remains largely untested (Betances, et al., 2014).

As part of the project, students worked with researchers from Pace to define a set of features to capture mouse behavior. The set of features includes measurements of motion, clicking, and scrolling.

Motion events are captured when a user moves the mouse. Each motion event contains a timestamp and the screen coordinates of the pointer. The distributions of three point-to-point measurements are considered: velocity, direction, and angular velocity.

Click events are generated when the user presses the left or right mouse buttons. Along with the button and the press and release timestamps, the event record contains the pointer coordinates at both the press and the release of the button. The event records in the sequence of click events from a sample are first labeled according to the "type of click" the user intended to perform. The three types of clicking actions that may occur are single clicks, double clicks, and drag-and-drops, corresponding to the three commonly occurring mouse-button interactions. Double clicks are characterized by the elapsed time between the press timestamps of consecutive click events. The default timing threshold between click events on Windows is 500ms (Microsoft, 2015), and click events which occur within 500ms of each other generate a double-click system event. Similar to keystroke, there are four different transition times that can occur between successive click events and only the RP and PP latencies are considered here.

Scroll events are generated when a user spins the wheel of a mouse in either direction to navigate quickly to off-screen elements in an application. Each scroll event contains a timestamp, the direction and amount of rotation, and the location of the pointer on the screen.

For a complete set of mouse features, see (Betances, et al., 2014).

EXPERIMENT DESIGN

After the data was collected and preprocessed, the authentication scenarios were simulated. The preprocessing and simulations were performed by Pace, on behalf of the PCCC students using an authentication system developed at Pace over several years (Monaco, et al., 2013).

To obtain authentication results, a leave-one-out cross-validation (LOOCV) procedure was used. LOOCV has low bias and high variance and is often used with small amounts of data as in this project. It simulates an authentication between every sample and enrolled user.

In total, there were 16 students who provided 6 samples from each task. This includes data collected from the PCCC students and several graduate students at Pace University. Thus, there are $1536 = n \times n \times m$ authentications, where n is the number of users and m is the number of samples per user. Out of these, there are $n \times m$ genuine authentications and $n \times (n-1) \times m$ imposter authentications. The number of false rejects and false acceptances are tallied to obtain the FRR and FAR in deriving the ROC curve. For more detail of the authentication system, see (Monaco, et al., 2013).

Using the classification system developed at Pace (Monaco, et al., 2013), experimental authentication results were obtained for each task and each modality, as well as combined modalities. The results are shown in Table 2, where task 1=edit, 2=browse, 3=Solitaire, and 4=Star Bubbles. It is clear that performance varies drastically between each task and modality, although it generally increases when various modalities are combined. This demonstrated to the PCCC students the importance of multi-factor authentication and multimodal biometric systems.

Task	Motion	Click	Scroll	Keystroke	Multi
1	8.3	22.3	50.0	10.1	4.2
2	9.4	34.5	26.5	21.4	6.3
3	4.2	22.9	8.3	22.2	4.2
4	5.2	21.8	11.2	33.3	5.5
Avg.	6.8	25.4	24.0	21.8	5.0

TABLE 2: KEYSTROKE AND MOUSE EXPERIMENTAL EER RESULTS

MOBILE DEVICE BIOMETRICS

In spring of 2014, PCCC students participated in a similar joint project with Pace University utilizing mobile touchscreen behavior. Based on the success of the project from previous year's students, the mobile project was structured similar to the keystroke and mouse biometrics project. The mobile biometrics project focused on user identification instead of authentication.

MOBILE BIOMETRICS BACKGROUND

Mobile or handheld devices are becoming increasingly important in our society as users are adopting the technology both for recreational and business purposes. According to a report by mobiForge in May 2014, there are nearly 7 billion mobile subscriptions worldwide. That translates into 95.5% of the global population (mobiThinking, 2014). Moreover, mobile phone sales worldwide have increased 8% since 2013, and tablets have experienced a whopping 79% increase in sales. Conversely, PC/laptop sales have experienced a precipitous decline over the past three years. Since 2013, worldwide sales of PC/Laptop sales have decreased by 11% (Rivera & Goasduff, 2014). The explosive growth and adoption of mobile and tablet devices warrants the need for a new biometric to emerge in order to better authenticate users across this growing medium. Very few studies have been conducted in this domain, one notable research effort occurred in 2012 in Hong Kong (Meng, et al., 2012). The researchers analyzed various gestures that are commonly used on a mobile device and derived a low EER rate of 3%.

Mobile biometrics applications generally consist of three major components. The first component is the touchscreen that is now widely considered the most adopted interactive panel for mobile devices. The second component that will assist in developing a mobile biometric system is the gesture recognition capability of the device. With regards to Android-based devices, the following are the core gestures supported as listed in the Android Developers Documentation (Google Inc., 2014): touch, long press, swipe or drag, long press drag, double touch, double touch drag, pinch open, pinch close.

The third component for a mobile biometric system consists of the device sensors. Sensors are typically grouped into three categories: motion sensors, position sensors, and environmental sensors. Motion sensors are used to measure acceleration and rotational forces along the axes (Google, 2014). Position sensors are used for capturing data about the physical position of the device (Google, 2014). Environmental sensors are used to measure environmental considerations.

DATA COLLECTION

During two sessions held at Pace, the PCCC students collected data on LG Nexus 5 devices using an application developed by Pace graduate students. The application prompted students to answer a series of questions that required navigating a Web page, reading text, and studying an image. During this time, the application sampled the screen and various sensors at a rate of about 1 kHz. An example of the data capture interface is shown in Figure 2. Each student recorded approximately 15,000 samples during each session, where a single sample consists of the touchscreen and device sensors values at an instant in time.

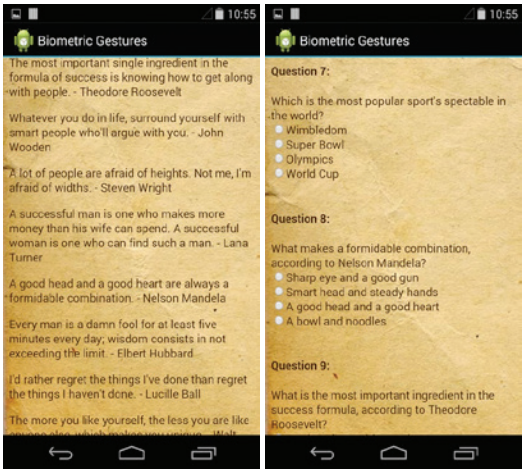

FIGURE 2: MOBILE DATA CAPTURE INTERFACE

The touchscreen data that was collected includes the location of each pointer (finger) on the screen, the pressure applied by each pointer, and major and minor axes of an ellipse approximating the pointer size. An example of the screen coordinates from a series of gestures from two users is shown in Figure 3.

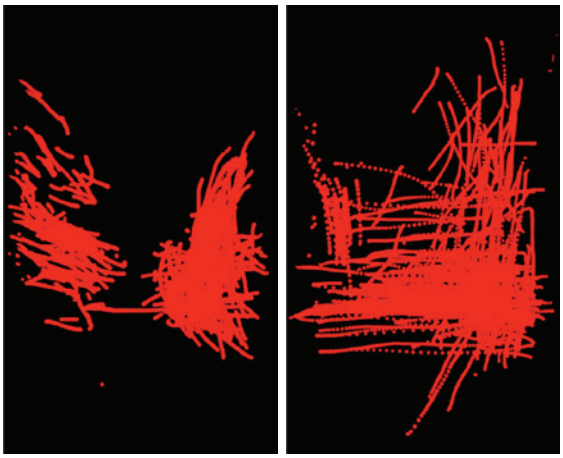

FIGURE 3: TOUCHSCREEN GESTURES RECORDED

In addition to touchscreen data, sensor-based data was recorded from the following device sensors.

Gyroscope: measures the rate or rotation around the device's axes and is used to maintain orientation of the device.

Accelerometer: measures the acceleration applied to the device, including the gravity force.

Linear Accelerometer: provides a three-dimensional vector representing acceleration along each device axis, excluding gravity.

Orientation: allows monitoring the position of a device relative to the earth's frame of reference, i.e. portrait vs. landscape orientation.

A feature vector was formed from the touchscreen and sensor values in each sample. For more details on feature extraction and data preprocessing, see (Alotaibi, et al., 2014).

EXPERIMENT DESIGN

Experimental results were obtained by Pace University graduate students and presented to PCCC in session three of the project. PCCC students were then able to include the results in their paper submitted to Pace's Research Day conference.

Results were obtained using a decision tree classifier generated by the C4.5 in Weka using a 10-fold cross-validation. Using data from both sessions yielded an identification accuracy of 98.4%, which is on par with other studies containing similar amounts of data. Since the data was collected in two different sessions, results were also obtained using the data from the first session as the training set and the second session as the testing set. In this case, identification accuracy dropped to 25%. This demonstrated to the PCCC students the problem of template aging, an issue that continues to arise in various biometric applications.

OUTCOME

Overall, 25 URM students participated in the partnership throughout 2013–2014. Seventeen students participated in the research project, and 8 participated in the outreach workshops. Out of the 25 students that participated, 22 (82%) graduated PCCC and are enrolled in a four-year STEM program. A few of the students in the cohort have not completed their degrees due to their part-time student status. It should be noted that a few students expressed interest in participating in the project during the recruitment phase; however, due to conflicts with their work schedules, they were unable to participate. Full-time employment can be a hindrance for students trying to achieve their degree in a timely fashion. According to the Chronicle of Higher Education, 71% of part-time students had not completed their associate degree within three years (Supiano, 2010). Many of these students must work a full-time job in order to support themselves and pay tuition. In order to help address this issue,

PCCC applied for and was awarded a $4.1M Title V STEM grant from the Department of Education, and a $1.5M Bridges to Baccalaureate grant from the National Science Foundation, which provides stipends to students participating in research projects and supports other STEM activities. These grants provide students with some financial assistance and support resources which allows students to focus more on their studies as opposed to work obligations and leverage resources to ensure STEM student success.

CONCLUSIONS

Students were asked to submit a reflection paper after the research project that summed up their experience with the project. We will summarize the key points mentioned by the students in this section to provide readers an idea of the key value gained from the experience. Many students mentioned how the biometrics research project expanded their current knowledge of technology. Students recognized the importance of security as they have read about the many data breaches that have occurred in the private and public sector. Many were not aware of biometrics as a study and career option, nor the high demand and growth potential for cybersecurity professionals. The project has increased their awareness and many are considering a career in cybersecurity. PCCC offers a networking option under the Information Technology degree that includes a computer forensics course. The cybersecurity research project will help expand the program and act as a recruiting tool with the goal of enrolling more students, offering more cybersecurity courses and, ultimately, an AS degree.

Pace University has emerged as a highly attractive option for transfer by offering bachelor's and master's degrees in cybersecurity. Information regarding transfer is made available throughout the research program and outreach workshops. Students particularly enjoyed the college tour offered by Pace during the project as well as the staff available to assist in the transfer process.

Students also noted the program design and development, mentioning in their reflection papers how they now have a better understanding of the agile project management process. The program coordinators introduced the method before the start of the program, provided examples throughout the sessions, and utilized the process during the development of the final paper.

Students found the final paper to be a rewarding experience due to the distributed nature of the assignment. The students enjoyed working collaboratively while using various online tools to complete the task before the deadline. Many students planned to use this newly acquired distributed model concept for future team projects.

Lastly, all of the students particularly enjoyed presenting their findings at Pace Research Day. The event afforded students an opportunity to meet Pace faculty and students focused on similar research areas. PCCC students had the opportunity also to learn about other research projects in biometrics as well as the emerging field of telehealth. They were extremely excited about taking home a copy of the official conference Proc. which included their paper in the publication. The research experience was highly successful and motivating for our students. Many of the students used this experience as a launchpad which would keep them working hard toward their goal and pursue their dreams. As one student best put it, "I am now aware of what is expected in order to complete a dissertation; I will now strive to complete my PhD."

REFERENCES

Alipui, G., Asamoah, C., & Barilla, R. (2014). An Agile Approach to Doctoral Research Dissertation. *Proceedings of Student-Faculty Research Day,* CSIS, Pace University (pp. D2.1–D2.8). White Plains: Pace University.

Alotaibi, N., Barilla, R., Betances, F., Chohan, A., Garcia, A., Gazarov, A., Monaco, J. V. (2014). Biometric System Design for Handheld Devices. *Student-Faculty Research Day.* Pace University.

Betances, F., Pine, A., Thompson, G., Zandikarimi, H., & Monaco, J. V. (2014). Mouse Biometric Authentication. *Proceedings of Student-Faculty Research Day,* CSIS, Pace University, May 2nd, 2014, (pp. B5.1–B5.8). White Plains.

Bureau of Labor Statistics. (2014, January 8). *Occupational Outlook Handbook.* Retrieved from Information Security Analysts: http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm.

Chen, X. (2009). *Students Who Study Science, Technology, Engineering and Mathematics (STEM) in Postsecondary Education.* Washington DC: National Center for Educational Statistics.

Ciaurro, W., & et al. (2014). Touch- Screen Mobile Device Data Collection for Biometric Studies. *Proceedings of Student-Faculty Research Day* (pp. B10.1–B10.3). White Plains: Pace University.

DARPA. (2013, February 11). Active Authentication (AA) Phase 2. *Broad Agency Announcement*. Arlington, VA, USA: Defense Advanced Research Projects Agency.

Davis, C. E., Yeary, M. B., & Sluss, J. J. (2012). Reversing the Trend of Engineering Enrollment Declines With Innovative Outreach, Recruiting and Retention Programs. *IEEE Transactions on Education*, 157–163.

Farnon, E. et al. (2013). A Keystroke Biometric Experiment on Edited Text. *Proceedings of Student/Faculty Research Day*, CSIS, Pace University (pp. B7.1–B7.6). White Plains: Pace University.

Google. (2014, March). *Sensors Overview*. Retrieved from Google Inc. Retrieved from http://developer.android.com/guide/topics/sensors/sensors_overview.html.

Google Inc. (2014, March). *Android Gestures*. Retrieved from Android API Guides: http://developer.android.com/design/patterns/gestures.html

Griffith, A. L. (2010). Persistence of women and minorities in STEM field majors: Is it the school that matters? *Economics of Education Review*, 911–922.

Kaminsky, M. E., & Anderson, E. (2008). *Identifying Game Players with Biometrics*. Retrieved from University of Seattle: http://homes.cs.washington.edu/~miro/docs/mouse_ID.pdf.

kwhat. (n.d.). *jnativehook: Global keyboard and mouse listeners for Java*. Retrieved 2013, from Github: https://github.com/kwhat/jnativehook.

Maas, A., Heather, C., Do, C., Brandman, R., Koller, D., & Ng, A. (2014). Offering Verified Credentials in Massive Open Online Courses: MOOCs and technology to advance learning and learning research. *Ubiquity symposium*. ACM.

McHugh, J. M. (2013). *Redesignation and Transfer of the Biometrics Identiy Management Agency as the Defense Forensics and Biometrics Agency*. Washington, DC, USA: Department of the Army.

Meng, Y., Wong, S. D., Schlegel, R., & Kwok, L. F. (2012). Touch gestures based biometric authentication scheme for touchscreen mobile phones. *Proceedings of the 8th China International Conference on Information Security and Cryptology*. Hong Kong.

Microsoft. (2015). *Microsoft Development Center*. Retrieved from Set Double Click Time Function: https://msdn.microsoft.com/en-us/library/windows/desktop/ms646263%28v=vs.85%29.aspx.

Mobithinking. (2014, June 13). *MobiForge*. Retrieved from Global mobile statistics 2014 Home: all the latest stats on mobile Web, apps, marketing, advertising, subscribers, and trends.... http://mobiforge.com/research-analysis/global-mobile-statistics-2014-home-all-latest-stats-mobile-web-apps-marketing-advertising-subscriber.

Monaco, J. V., Bakelman, N., Cha, S., & Tappert, C. C. (2013). Recent Advances in the Development of a Long-Text-Input Keystroke Biometric Authentication System for Arbitrary Text Input. *European Intelligence and Security Informatics Conference (EISIC)*. IEEE.

Moodle bioauth plugin. (n.d.). Retrieved 2014

Rivera, J., & Goasduff, L. (2014). *Gartner Says Worldwide Traditional PC, Tablet, Ultramobile and Mobile Phone Shipments Are On Pace to Grow 6.9 Percent in 2014*. Egham: Gartner.

Supiano, B. (2010, December 1). *Half of All First-Time Students Earn Credentials Within 6 Years*. Retrieved from The Chronicle Of Higher Education: http://chronicle.com/article/Half-of-All-First-Time/125585/.

Tactica. (2015, May). *Biometrics Market Forecasts*. Retrieved May 19, 2015, from Tactica: https://www.tractica.com/research/biometrics-market-forecasts/.

Tappert, C. C., Cha, S., Villani, M., & Zack, R. S. (2010). A Keystroke Biometric System for Long-Text Input. *Int. J. Info. Security and Privacy (IJISP)*, 32–60.

TechSciResearch. (2015, March). *Global Biometrics Market Forecast and Opportunities, 2020*. Retrieved May 19, 2015, from TechSciResearch. http://www.techsciresearch.com/3234.

AUTHORS

Gonzalo Perez (gperez@pccc.edu) is the executive assistant to the president/ assistant dean for academic affairs and a computer science adjunct professor at Passaic County Community College. Perez earned his doctorate in computing from Pace University in White Plains, New York. His role was to help develop the model for the cybersecurity research project, recruit the students, coordinate the activities, and help students collaborate on the final paper. He also held student meetings in between sessions in order to support the tasks that students were completing and, finally, conducted a closing meeting in order to reflect on the project outcome and assess student impact.

John V. Monaco (jmonaco@pace.edu) is an adjunct professor at Pace University, where he is also pursuing a PhD in Computer Science under the supervision of Dr. Charles Tappert. In 2013, Monacowas named one of Westchester's "Top Professionals under 30" for research in keystroke biometrics at Pace University. He has authored or coauthored over a dozen publications as a PhD student and placed 1st in an international competition on identifying users based on eye movements. Monaco currently attends school under a full scholarship provided by the Department of Defense. His role was to develop the applications used for data collection and obtain experimental results.

Charles C. Tappert (ctappert@paace.edu) has a PhD in Electrical Engineering from Cornell University and was a Fulbright Scholar. He worked on speech and handwriting recognition at IBM for 26 years, taught at the U.S. Military Academy at West Point for seven years, and has been a professor of computer science at Pace University since 2000. He has over 100 publications and his research interests include pattern recognition, biometrics, handwriting recognition/pen computing, speech recognition/voice applications, human-computer interaction, artificial intelligence, and Big Data.

Li-Chiou Chen (lchen@pace.edu) is a professor at Pace University. She has a PhD in Engineering and Public Policy from Carnegie Mellon University. Her publications and research interests have been focused on computational models for Internet-based attacks, user authentication, security usability, and computer security risk perception. She is the principal investigator of Pace's CyberCorps: Scholarship for Service program, supported by the National Science Foundation.

Bridging the Gap

Ronnie S. Saturno Jr.

The demand for qualified and competent cybersecurity professionals has become a dominant theme throughout the technology world. In recent years, increasing reports of malfeasance relating to connected systems have strayed from the exclusive domain of technology publications to the mainstream press. Every day, there is a new report of a retailer having customer records stolen or government systems being probed by foreign nation states as a supposed preemption toward a global cyber catastrophe. The collective eyes of America are squarely focused on cybersecurity like never before.

This has placed additional pressure on organizations from private companies to agencies of the federal government to address the subject of cybersecurity. Laws such as the Sarbanes-Oxley and Gramm-Leach-Bliley Acts that among other things demand a reasonable expenditure of effort toward the security of sensitive data and the increased emphasis on their enforcement have fueled the emergence of professionals devoted to the security of valuable information and the systems on which that information is stored, processed, and transported. There has emerged a comprehensive assortment of professional certifications and certifying organizations aiming to validate the skills and proficiency of those wishing to fill positions in the rapidly growing cybersecurity industry.

For years, the majority of professionals in cybersecurity positions have been products of university computer science departments. The intimate knowledge of computer systems, data networks, and programming required of the best cybersecurity professionals for many years could come from no other place. There are, however, a number of factors that diminish the relevance of this standard. There are many self-taught experts who are more than capable of performing in cybersecurity positions who for one reason or another have been unable to complete a rigorous program required to earn a baccalaureate degree in computer or information science. Further, many without a degree are more than capable of earning information security certifications required of cybersecurity professionals. Fittingly, the industry has recognized this trend. Beginning in 2005, the United States Department of Defense in its Information Assurance Training, Certification, and Workforce Management Directive 8570.1 *provided guidance and procedures for the training, certification, and management of the DoD workforce conducting Information Assurance (IA) functions in assigned duty positions.* (DoD, 2005). More recently, the United States House of Representatives passed HR 3017, the Homeland Security Cybersecurity Boots-on-the-Ground Act which *"develops a workforce strategy that enhances the readiness, capacity, training, recruitment, and retention of the DHS cybersecurity workforce, including a multi-phased recruitment plan, a 5-year implementation plan, and a 10-year projection of DHS workforce needs as well as a process to verify that employees of independent contractors who serve in DHS cybersecurity positions receive initial and recurrent information security and role-based security training commensurate with assigned responsibilities" by "developing occupation categories for individuals performing activities in furtherance of DHS's cybersecurity mission, ensuring that such categories may be used throughout DHS and are made available to other federal agencies, and conducting an annual assessment of the readiness and capacity of the DHS workforce to meet its cybersecurity mission"* (U.S. House, 2014).

There are many training centers that have capitalized on the growing number of professionals seeking to earn certifications that would allow them to compete for cybersecurity jobs, whether they are in private industry or in government positions that

are subject to DoD 8570. In the grand tradition of American tertiary education, traditionally known as *continuing* or *vocational* education, these training centers address the needs of those desiring to bring specific needs to the job market, much like the auto mechanics, medical assistants, and HVAC technicians trained in vocational training centers of years past. Despite the obvious value of these training centers, there is one big drawback. Certification programs which often consist of classroom training over a set period of time followed by a proctored certification exam neither result in a college degree or count as academic credit that can be later counted toward a degree. With a job market under increasing pressure from a weak economy and high unemployment that grows increasingly competitive by those seeking to work in a field that is increasing in public awareness, college degrees have increasing value.

This is where community colleges and their unique position in the American educational system distinguish themselves. For years, community colleges, junior colleges, and city colleges have occupied the sweet spot between four-year universities and vocational education training centers. Students have been afforded the option of earning valuable skills and credentials while working (or not) toward accredited associate degrees, many of which transfer whole or in part toward the lower-division educational requirements of baccalaureate degree-granting universities and colleges. While larger universities may have a harder time making adjustments to academic catalogs to accommodate instruction specific to cybersecurity, smaller community colleges are not as likely to be constrained by such difficulties. While many colleges and universities now offer cybersecurity-specific degrees or security-specific concentrations for their information and computer science degree programs, community colleges were well ahead of them, and community colleges are still capable of offering more. For example, a community college could offer a class such as "Advanced Penetration Testing and Ethical Hacking" in its computer or information science department that faithfully follows the objectives of the EC-Council Certified Ethical Hacker (C|EH) credential. Over the course of a semester, the class could review the material and perform the exercises of the program. At the end of the semester, the students would be prepared to sit for the C|EH exam, or perhaps the college could arrange for a discounted exam voucher through EC-Council or a local proctoring center. And of course, they would receive college credits for the course. The possibilities are endless, and are not limited to any one certifying body. Such arrangements could be made with organizations such as Cisco, ISC^2, PMI, or CompTIA. It is difficult to conceive the typical four-year university affecting such flexibility.

The ability to bridge the gap between four-year universities and vocational training centers while offering the added flexibility of online and evening classes defines the tremendous significance that community colleges have in today's cybersecurity environment, particularly for those who were not able to complete a four-year degree before entering the workforce. While the definitive value of an associate degree is constantly debated, such as in the 2013 report published by the American Institute for Research acknowledging that *"community colleges are commonly identified as the weak link in the higher education continuum, and their students identified as higher education's second-class citizens"* (de Alva & Schneider, 2013), the same report points out that *"a community college that works closely with the local labor market and promotes technical training (e.g., in health care, petrochemicals, high-end manufacturing, and engineering support) can significantly increase the likelihood that its graduates will enjoy strong income gains relative to high school graduates"* and emphasizes the value of transferring to a four-year institution. For many cybersecurity professionals, particularly those working in government positions aspiring for promotions to positions that require four-year degrees, the ability to earn a four-year degree has tremendous value in their career progression. There is nothing second-class about that.

REFERENCES CITED

de Alva, J. K., & Schneider, M. (2013, October). *What's The Value Of An Associate's Degree? The Return On Investment For Graduates And Taxpayers.* Retrieved from American Institute for Research. http://www.air.org/sites/default/files/Value_of_an_Associate_Degree_10.13.pdf.

DoD. (2005, December 19). *Information Assurance Workforce Improvement Program.* Retrieved from Defense Technical Information Center. http://dtic.mil/whs/directives/corres/pdf/857001m.pdf.

US House. (2014, July 29). *H.R.3107 — Homeland Security Cybersecurity Boots-on-the-Ground Act.* Retrieved from Congress.gov: https://www.congress.gov/bill/113th-congress/house-bill/3107.

AUTHOR

Ronnie S. Saturno (rsaturno@hush.com) is a graduate of the Excelsior College School of Business & Technology, having earned a Bachelor of Science in Information Technology with a concentration in Cybersecurity Technology in April 2014 and a Master of Science in Cybersecurity in February 2015. He is a 14-year veteran of the United States Coast Guard, serving as a maintenance technician on aviation electrical and electronics systems and aircrew instructor for patrol aircraft navigators and radio operators. In addition, he is an avid researcher of security in cyber, communications, and computer systems focusing on training and certification in meeting the needs of constantly evolving industrial needs and evaluating risk in interconnected communications systems. He is the organizer of Security B-Sides Honolulu and is a member of CyberPatriot, IEEE, ISSA, ACM, and InfraGard. He holds Certified Ethical Hacker and Computer Hacking Forensic Investigator certifications.

Cybersecurity Competitions: Recommendations for Assessment, Evaluation and Research

Portia Pusey | David Tobey, PhD | Diana Burley, PhD | Deanne Cranford-Wesley, PhD | Jacob Frank

ABSTRACT

There is a growing body of evidence that many colleges and universities are using cybersecurity competitions experiences with students to provide hands-on activities that simulate professional practice. However, the assessment and evaluation methods are often briefly described, if at all in the body of literature. The purpose of this paper is to report on methods of assessment that can be applied to measure gaps and growth in student competence when using cybersecurity competitions in formal learning environments. Furthermore, we describe evaluation techniques that can be used to improve instruction. Finally, we recommend two instruments which we use in our research to describe competition participants and the outcomes of competitions. The paper concludes with suggested debrief questions that can be used by educators to guide students to reflect on the application of cybersecurity course curriculum content during competition experiences.

INTRODUCTION

Cybersecurity competitions (or exercises) were described in a foundational overview conducted by Hoffman and Ragsdale: "To provide a venue for practical education in the implementation of all strategies, tools, techniques, and best practices employed to protect the confidentiality, integrity, authenticity, and availability of designated information and information services" (2005, p. 3). The body of literature now reflects that instructors are including competitions and competitive cyber exercises into formal classroom experiences (Chothia & Novakovic, in press; Mirkovic & Peterson, 2014; National Cyber League, 2015).

Competitions, when used in formal education, require rigorous evidence of student achievement. The educator is accountable both to the student and to their employer to justify that the competition is connected to the course outcomes, and that the grade the student earned is commensurate with a student's performance and can be defended with documentation. However, descriptions of specific methods of evaluation and assessment are not found in the literature. The purpose of this paper is to provide examples of ways to measure outcomes of competitions in order to improve both instruction and learning. Key definitions for assessment and evaluation terms will be presented followed by specific methods and techniques for assessment and evaluation. Finally, in order to address the paucity of research published on the use of competitions

in educational environments, recommendations for two instruments used by the National CyberWatch Center (NCC) Research team will be made.

REVIEW OF ASSESSMENT AND EVALUATION

In North America, assessment and evaluation are often used as synonyms (Sadler, 1989). For the purpose of this work we will operationally discriminate between the two terms. Assessment will be used to describe activities which support student learning such as quizzes, informal polls, checks for understanding, or final exams. Evaluation will be used to describe activities which support improved *instruction*. These include feedback from peers or supervisors, discussions with students, or course evaluation results.

Klinger et al. (2015) list the following uses for assessment:

- Inform instructional decisions and practice
- Provide feedback to students as they work to meet learning expectations
- Place students in learning groups or provide individualized instruction
- Engage students in self-assessment to reflect on their own learning
- Engage students in peer-assessment to deepen their own learning
- Provide feedback to students about the extent to which the learning expectations for a unit or term of instruction are being met

For evaluation, as well as assessment, the goal is to provide information that will "facilitate some specific course of action (Frechtling, 2010, p. 2)."

Assessments and evaluations can be further categorized in two ways: summative and formative. Summative assessment is a measure of student competency at the end of a course. It is a final snapshot of student achievement. "Formative assessment is concerned with how judgements about the quality of [instruction or] student responses (performances, pieces, or works) can be used to sample and improve [instruction or] student's competence by short-circuiting the randomness and inefficiency of trial-and-error learning. (Sadler, 1989, p. 121). Formative assessments occur from the first day and continue *throughout a course* or program to improve teaching and guide instruction to address gaps in student competencies.

In this work, we describe several formative and summative assessment / evaluation techniques that instructors can use to improve student competency or their own instruction. We also make recommendations for the use of two instruments that we have used to conduct research on the outcomes of cybersecurity competitions.

FORMATIVE EVALUATION

Angelo and Cross (1993) have developed a method of using classroom assessment to support classroom research which can improve an instructor's ability to facilitate learning. Angelo and Cross (1993) write that "the central purpose of Classroom Assessment is to empower both teachers and their students to improve the quality of learning in the classroom" (p. 4). This is because Classroom Assessment "provides faculty with feedback about their effectiveness as teachers, and it gives students a measure of their progress as learners" (p. xiv). The kind of Classroom Assessment Techniques (CATs) that Angelo and Cross recommend are not to assign grades. In fact, most of the CATs involve anonymous feedback from the students. CATs are short anonymous formative assessments that instructors review quickly to guide their instructional practice.

Angelo & Cross' (1993) research demonstrated that use of CATs can result in higher levels of student-faculty interactions, active classroom participation, and improved classroom learning. They also reported that there was a positive student response to the use of CATs. Further findings suggest that

students felt more involved in their learning, that students said they benefited from improved teaching, and that students described reflecting more on their own learning. In several independent studies of CATs at a community college Angelo and Cross' findings were replicated. In these studies students and instructors describe increased participation, more frequent student-faculty interactions, and improved teaching (Morris, 1994; Murphy, 1994; Samanta, 1994). Samanta (1994) also reported improved student retention.

However, Angelo and Cross (1993), as well as other studies, discuss a few drawbacks to using CATs. Negative feedback can be difficult to hear and formative assessments are time consuming (Murphy, 1994). It is not only time consuming to conduct and analyze the formative data but instructors reported that it is time consuming to re-teach content if the formative data indicates that students did not understand the content. Murphy (1994) and Angelo and Cross (1993) also warn that if the CAT is not carefully constructed, the data collected will not be useful to improve instruction. However, the studies agree that the benefits of improved instruction and enhanced metacognition for students outweigh the drawbacks (Angelo & Cross, 1993; Morris, 1994; Murphy, 1994; Samanta, 1994).

In order to use CATs to conduct classroom research to improve instruction, Angelo and Cross (1993) have provided several diagnostic tools — the Teaching Goals Inventory and the One Sentence Summary Tool. The instructor uses these diagnostic tools to focus the Classroom Research project and to align the research with their teaching goals. For example, Cluster V: Work and Career Preparation: Goal 43: Develop ability to perform skillfully can be measured using the Group Instructional Feedback Technique (GIFT). This is an anonymous, qualitative, three-question survey that instructors can use to determine the effectiveness of the instruction. It can be administered online or using pencil and paper. Richlin (1998) reported that the use of GIFT required the Teaching Assistants to reflect more on their teaching practice. Before the use of GIFT, the Teaching Assistants' primary focus was on the content of the instruction; the GIFT feedback caused the teaching assistants to shift their teaching to more student-centered practice. While this study did not look at student achievement, the study did report more positive course evaluations for the teaching assistants participating in the study.

It is recommended that the instructor customize each CAT to meet the needs of the individual context (Angelo & Cross, 1993; Morris, 1994; Murphy 1994). GIFT was designed to answer the following three questions:

1. What do students think is helping them learn? (Give one or two specific examples of ways that the competition facilitated your course learning.)

2. What is hindering the students' learning? (Give one or two specific ways that the competition made learning more difficult.)

3. What specific suggestions do the students have for improving learning? (Suggest one or two specific, practical changes that I can implement that would improve this learning activity to better help you learn to harden networks?)

Once the responses have been collected, present the responses in a survey that will allow students to rate the feedback. The responses with the highest ratings become the list of priorities to improve the learning activity. This list would only accurately reflect the priorities for the current group of students participating in the learning activity and could not be generalizable to reflect competition learning activities. This list should be compared against the list for subsequent semesters to assure that the changes that were made to the learning activity were effective in improving the perceived learning of the students.

FORMATIVE PEER ASSESSMENT

Formative feedback can make a valuable contribution to student learning. Good formative feedback focuses on learning and not grades (Bryand & Clegg, 2006). However, formative feedback can be a time-consuming process for the professor (Angelo

& Cross, 1993, Freeman & McKenzie, 2002). Irons (2006) recommend using peer feedback as a way to improve student learning and reduce the time commitment on the part of the instructor.

Formative feedback should provide specific information to the learner which will guide them as they improve their product or process. This means that formative feedback should be provided as the students are working on their learning activity so that they have time to incorporate the feedback into their final projects (Bryan & Clegg, 2006; Kvale, 2007; Carless, Joughin, & Liu, 2006; Irons, 2008). Improved motivation (Bloxham & West 2004; Pope, 2001), end products (Irons, 2008), learning (Pope, 2001), and participation in one's own learning are some of the benefits to formative peer feedback reported in the literature.

One benefit often studied in the literature is the development of metacognitive skills (Kvale, 2007; Sluijsmans, Brand-Gruwel, vanMerriënboer, & Bastiaens, 2003; Sluijsmans and Prins, 2006; Wen, Tsai, & Chang, 2006). One researcher, Kvale (2007), linked metacognitive development to improved learning. He writes that formative feedback enables a student to reflect on his learning to improve the quality of the performance/product that is being assessed. Kvale suggests that given multiple opportunities to practice this reflection process, learners will develop metacognitive skills that will facilitate learning.

Another connection that has been made in the literature is the relationship between peer formative feedback and improved quality of the end product. (Tsai, Liu, Lin, & Yuan 2001; Bloxham & West 2004). Several studies have been conducted in the field of preservice teacher education and have documented improvement in the lesson plans that were written (Bloxham & West 2004; Prins, Sluijsmans, Kirshner, Strijbos 2005; Sluijsmans, Brand-Gruwel, vanMerriënboer, & Bastiaens, 2003; Sluijsmans & Prins, 2006; Tsai, Liu, Lin, & Yuan 2001; Wen, Tsai, & Chang, 2006). In addition to improving preservice teachers' ability to write lesson plans, the use of peer assessment provides preservice teachers practice in performing assessment. (Ozogul, Olina, & Sullivan 2008; Sluijsmans, Brand-Gruwel, vanMerriënboer, & Bastiaens, 2003; Sluijsmans & Prins, 2006).

There are a strong recommendations found in the literature about the peer assessment process. Studies suggest that even students studying to become teachers may not be able to provide quality feedback without being trained to do so (Freeman, 1995; Sluijsmans, Brand-Gruwel, vanMerriënboer, & Bastiaens, 2003; Sluijsmans, Brand-Gruwel, vanMerriënboer, & Martens, 2004; Sluijsmans & Prins, 2006). One way for students to become aware of important assessment elements is for them to participate in creating the criteria for the assessment (Boud, Cohen & Sampson, 1999; Sluijsmans, Brand-Gruwel, vanMerriënboer, & Bastiaens, 2003; Sluijsmans, Brand-Gruwel, vanMerriënboer, & Martens, 2004; Sluijsmans & Prins, 2006; Sivan, 2000). Two studies suggested that the feedback should be anonymous (Li & Steckelberg, 2005; Wen, Tsai, & Chang, 2006). When researchers compared anonymous and non-anonymous feedback to instructor or expert feedback, the data suggested that anonymous peer feedback was more reliable than non-anonymous feedback. So while some studies suggest that peer feedback can provide useful information that will improve learning (Freeman, 1995; Magin, 2001; Tsai, Liu, Lin, & Yuan, 2001), these results can be assured by creating a peer feedback system that assures anonymity.

SUMMATIVE GROUP-WORK SURVEY ASSESSMENT

The literature on assessment for collaborative learning environments suggests that while students should work collaboratively, they should be assessed individually (Cubric, 2007). Research on the collaborative learning process reports that learner satisfaction in group learning activities increases when their individual contribution is assessed (Clark & Redmond, 1982; Hassaien, 2007; McGraw & Tidwell, 2001). Furthermore, there is evidence that students perceive the assessment process as fair when their individual contribution

to a group product is assessed (Bloxham & West 2004; Clark & Redmond, 1982; Elliott & Higgins, 2004; Gupta, 2004). This can be accomplished by assessing both the process and the product or by the use of a student survey that asks the student to rate himself and his team members (Tal-Elhasid & Meishar-Tal 2007).

Assessment of collaborative work has been the focus of many studies and has resulted in a formula that factors an individual's contribution to the final group product into his individual final grade (Conway & Kember, 1993; Goldfinch, 1994; Goldfinch & Raeside, 1990). There have been concerns that the rating system may not be a reliable source for individual assessment data. However, Li (2001) reported that if an individual rates their own contribution as well as his team members, the end rating is reliable. To complete the evaluation process students should be prompted to rate themselves and each team member in several different categories using a scale that ranges from 0 (no contribution to the task) to 3 (a major contributor). The following are general categories that can be used for cybersecurity competitions which are used in formal learning situations. Specific topics should be based on the instructor's goals and the competition tasks.

- **Techniques:** Provided ideas that were useful the tasks performed had few errors.
- **Communication:** Provided clear and timely instructions and requests for help.
- **Cooperation:** Helped the group to function well as a team.
- **Timeliness:** Attended all group meetings or met all deadlines set by group.

The individual's data is analyzed to create a weighting factor using a method adapted by Conway and Kember (1993) based on a formula developed by Goldfinch and Raeside (1990).

- **Individual Effort** = Total points given to a student by each team member
- **Team Average Effort** = Total points given to all team members ÷ Number of team members
- **Weighting Factor** = Individual Effort ÷ Team Average Effort

A team grade can be given based on the outcome of the competition or a rubric and the individual grade is the result of the weighting factor times the team grade.

Educator assigned grade
or rubric score **×** Weighting Factor
+ Total number of peer assessments completed up to 5
= Final Individual Grade

The data collection and analysis of this assessment was designed to facilitate the perception of fairness by the students and to minimize the workload of the instructor. Studies indicate that when an individual student's contribution to a group project is recognized, students perceive the grading system as fair (Hassaien, 2007; McGraw & Tidwell, 2001). By using the Conway and Kember (1993) formula to calculate each student's final grade, it is anticipated that students will feel that their individual contribution will be recognized and eliminate the need for instructors to mediate intra-group disputes.

SUMMATIVE RUBRIC ASSESSMENT

Competitions include tasks that cybersecurity professionals will perform during their professional careers. There is considerable evidence in the body of literature that suggests that rubrics be used for assessing authentic tasks (Bloxham & West, 2004; Prins, Sluijsmans, Kirshner & Strijbos, 2005; Sluijsmans, Brand-Gruwel, vanMerriënboer, & Bastiaens, 2003; Sluijsmans & Prins, 2006; Tsai, Liu, Lin, & Yuan 2001; Wen, Tsai, & Chang, 2006). Rubrics are summative assessments that students use to guide the completion of their coursework, in this case prepare to participate in a competition.

Best practice evidence found in studies for the use and construction of rubrics indicate that rubrics should be given to students when the learning activity is assigned, be specific rather than holistic, use consistent wording, and be connected to objectives (Anarde & Du, 2005; Castle & Arends, 2006).

When rubrics are given to students when learning activities are assigned, students are able to review their own work for errors prior to submission for feedback or grading (Andard & Du, 2005). However, instructors are cautioned that giving students the rubric in advance does not guarantee that students will be able to use the rubric to guide their work (Prins, Sluijsmans, Kirschner & Strijbos, 2005). Ozogul, Olina, and Sullivan (2008) reported that students who were trained to use a specific rubric produced superior end products to those students who did not receive the same training. Their finding was echoed by several studies with preservice teachers (Meier, Rich, & Cady, 2006; Li & Steckelberg, 2005). When students are trained to use a rubric that is aligned with the objectives of the course, the result is an improved final artifact (Meier, Rich, & Cady, 2006).

A rubric can also contribute to learning; Andarde & Du (2005) attribute this successful outcome to the ability of student to review his own work. In order for a rubric to contribute to learning, it must be specific rather than holistic (Castle & Arends, 2006). This means that the rubric should provide a detailed description of the subtasks necessary to complete the learning activity rather than a single general overall description. The detailed rubric provides precise feedback on the strengths and needs for the learning assignment which will allow the student to improve their future performance on similar activities. A rubric for competitions could be modeled on the following example for Security+.

	Good (1 Point)	Better (2 Points)	Excellent (3 Points)
NETWORK SECURITY	Describe three secure network principles	Implement three common secure network protocols	Prevent three common network attacks
COMPLIANCE AND OPERATIONAL SECURITY	Describe three risk mitigation strategies	Implement three incident response procedures	Execute three disaster recovery procedures

FIGURE 1: SAMPLE SECURITY + RUBRIC

The instructor can complete the assessment rubric him/herself or can have each team member complete the rubric for their project. Discrepancies between the instructor score and the students' scores can be discussed to provide a more thorough understanding of the outcomes of the competition or student understanding of the rubric. The literature indicates that if the quality of student work does not meet the expectation of the instructor, the rubric may not be clear or the students have not been adequately trained to use the rubric (Sluijsmans, Brand-Gurwel, vanMerriënboer, & Bastiaens, 2003; Sluijsmans, Brand-Gruwel, vanMerriënboer, & Martens, 2004; Sluijsmans & Prins, 2006). Angelo and Cross (1993) suggest looking for patterns in the errors in the students' work to guide improvements to the instruction or assessments that will lead to greater learning.

GRIT AND ENGAGEMENT INSTRUMENTS FOR RESEARCH

The National CyberWatch Center Research Team has been conducting mixed methods studies of cybersecurity competitions for three years (2012 – 2014) with players and coaches from two different competitions. For this work, cross-sectional data was categorized to study the descriptive engagement and grit traits of community and technical college participants and those who attend four-year and graduate institutions. Quantitative data was collected using two instruments. An engagement instrument based on to the UTRECHT Work Engagement Scale (Shaufeli & Bakker, 2003) was

given to National Cyber League (NCL) players prior to competitions in 2012, 2013, and 2014. The GRIT-S (Duckworth & Quinn, P. D. (2009) was administered to NCL and Collegiate Cyber Defense Competition participants in 2014.

We used the following recruitment methodology: Faculty of two- and four- year institutions of higher education, who serve as educators, coaches, and/or mentors for the CCDC or NCL teams were sent a link to the online consent document and survey instrument. The faculty coaches provided the link to the team members during practice sessions. In 2014, this process was changed for the NCL. A link to the survey was provided at the end of registration. Students were informed of research and those who consented to participate were directed to the survey instrument. None of the participants were compensated for their participation. The participants for these cross-sectional studies attended two- and four- year institutions of higher education and participated in either or both the NCL and CCDC competitions. The competitions and the instruments are described in this section.

THE NATIONAL CYBER LEAGUE (NCL)

The National Cyber League (NCL) is a network of five educational consortia: the Cyber Security Policy and Research Institute at George Washington University (CSPRI), the Center for Systems Security and Information Assurance (CSSIA) at Moraine Valley Community College, the National CyberWatch Center at Prince George's Community College, CyberWatch West at Mt. San Antonio College, and the Mid-Pacific Information and Communications Technologies Center (MPICT) at the City College of San Francisco. Collectively, the NCL partners include more than 580 higher education institutions nationwide and three state departments of education (California, Illinois, and Maryland). The NCL takes an education first approach to prepare individuals to compete in cybersecurity competitions and work in cybersecurity professions. NCL provides tools to support educators to integrate competitions into their curriculum including labs, tutorials, and individual and team competition activities aligned with the Security + and Certified Ethical Hacking exam.

COLLEGIATE CYBER DEFENSE COMPETITION (CCDC)

The CCDC is a series of tiered competitions that often provide two types of experiences for teams of competitors: online and face-to-face. Prior to the national competition, each of the 10 regions hosts an optional online qualifier and a face-to-face regional competition. During the face-to-face competitions, teams inherit the equivalent of the equipment and systems for a small business. The teams must manage and protect the network infrastructure while ensuring that the business needs are met. During the event, "teams are scored [PP1] based on their ability to detect and respond to threats, maintain availability of existing services, respond to business requests, such as the addition or removal of additional services, and balance security needs against business needs (CCDC, 2015)."

UTRECHT WORK ENGAGEMENT SCALE

The Utrecht Work Engagement Scale (UWES-9) to measure engagement was used in our exploratory studies because the UWES-9 has been established as a valid and reliable measure of engagement among individuals from diverse nations, racial, occupational backgrounds irrespective of gender. The nine questions, Likert-type scale items, ask participants to rate a statement about how they feel at work. The researchers edited each statement to read "while participating in the competition" rather than "at work" Participants could choose from a minimum rating of 0, "Never", to a maximum rating of 6 "Always/ Every Day." Participants rated three statements with indicators that relate to each of the three dimensions. For example, the dimension of vigor was assessed with the statement "While participating in the competition I feel bursting with energy." The nine indicators of career engagement

can be generally described by the way competing makes them feel. The dimension of dedicated indicators include 1) inspired, 2) enthusiastic, 3) proud. Absorbed indicators are 4) carried away, 5) immersed, 6) happy. And vigorous indicators are 7) bursting with energy, 8) strong and vigorous, and 9) feel like participating in the competition. Since leisure-time activities are good indicators of career choice, changes in the engagement measured after participating in a competition can suggest whether the competition activity builds or discourages an enthusiasm for the professional activity.

During the three years of our work the NCL has used analyses provided by their evaluator and the NCC research team to improve player satisfaction with the learning materials and play experience. Qualitative feedback from the 2012 season suggested that novice and community college players felt disadvantaged in the competition due to a lack of familiarity with the competition environment and lack of skill against experienced players with advanced skills (Tobey, Pusey & Burley, 2014). Two corrective actions were taken to improve the game experience for novice players. A competition environment walkthrough and example puzzles were provided. Furthermore, a bracketing system was designed and implemented so that novice players would compete against novice players.

In 2014, 77.03% of the players reported never participating a cybersecurity competition. Moreover, when we analyzed the UWES data from 534 NCL players between 2012–2014, players reported they experienced high levels of vigor, dedication, and vigor ("always" or "very often") when competing; this engaged group represented from 35.93% to 49.43% of the sample. The 2012 study suggested that engagement across all dimensions appears to improve as experience increases (Tobey, Pusey, & Burley, 2014). However, the 2012 study design precluded determining whether competitions lead to increases in professional engagement, or whether competitions are simply more effective at attracting students who already feel more engaged in pursuing a cybersecurity career. This is despite a high number of players reporting no experience with competition play. We recommend that research should be conducted that will compare preseason engagement with engagement among players later in the season. It would also be desirable to follow a cohort of players over a few years and competitions to observe changes in engagement over time. Finally, without studying students who elect to participate in competitions with those students who do not compete, we will not know if the self-selection bias has contributed to our findings.

GRIT

"Grit is the tendency to sustain interest in and effort toward very long-term goals. Self-control is the voluntary regulation of behavioral, emotional, and attentional impulses in the presence of momentarily gratifying temptations or diversions." Work by Duckworth (2007) suggests that grit can predict "objectively measured success outcomes." The grit construct consists of two factors: consistency of interest and perseverance of effort. It is interesting to note that Grit data collected from 230 CCDC 2014 competitors during the qualifying and regional rounds suggests that there may be differences in the competitors for each of the factors. More than two-thirds of the respondents answered "very much like me" and "mostly like me" to all of the subscales associated with perseverance of effort.

I HAVE OVERCOME SETBACKS TO CONQUER AN IMPORTANT CHALLENGE.	**80.86%**
SETBACKS DON'T DISCOURAGE ME.	**69.57%**
I AM A HARD WORKER.	**93.04%**
I FINISH WHATEVER I BEGIN	**73.04%**
I HAVE ACHIEVED A GOAL THAT TOOK YEARS OF WORK.	**72.17%**
I AM DILIGENT	**86.52%**

FIGURE 2: STUDENT RESPONSES

Without comparative data, it is unknown whether this is a trend we would see among all cybersecurity competitors. We therefore recommend that research be conducted to examine grit among and between:

- Competitors and non-competitors
- Competitors in a single competition
- Competitors from many competitions
- Competitors over time

CONCLUSION

When integrating competitions into a formal education environment, a team's final score is not an indication of what they have learned in the course. Furthermore, participating in competitions alone is neither learning nor instruction. Formal instruction requires understanding the gaps in knowledge, skills, and abilities of the learner and then providing interventions to address those gaps. Evidence that the intervention has been successful comes from the assessments conducted during and after the competition. We have provided several examples of assessment that can improve instruction, shape the students' learning, and provide a final grade. A final suggestion that can improve the development of professional cybersecurity skills among competitors even if competitions are used for informal learning is the "debrief." Reflecting on techniques and strategies applied during competitions is a critical process in improving practices that will be employed in professional settings. Many debrief questions were identified in the National Cyberwatch Center Resource Guide: Preparing for the Collegiate Cyber Defense Competition (CCDC): A Guide for New Teams and Recommendations for Experienced Players (Pusey, O'Brien & Lightner, 2015). While written for the CCDC, these are questions that can be implemented for any competition.

- What skills were you able to apply that you learned from your course work?
- What are some examples of skills needed but no team member possessed?
- Are there skills that were needed but not presently included in your program of study?
- Describe the communications processes (or lack thereof) that occurred within the team during the competition.
- In terms of team composition, in what area was the team lacking?
- Which team strategies worked and didn't work?
- Was the team effectively managed? What could have been done differently?
- Were there any obstacles that prevented the team from working together?
- Were the team member assignments relevant to the skills of those assigned?
- If you had it to do all over again, how would you prepare differently for the competition?
- Reflecting on the entire CCDC process, what are the most important things you learned from this experience?

Finally, information gathered during debrief or any assessment can be used as evidence for accreditation. Therefore, it is important to document and analyze the results of assessments to provide direct and indirect evidence of mastery of course objectives for the accreditation reviews. Measurements of engagement and grit can be used as evidence that your program is collecting data which will improve retention in the cybersecurity programs and engage students in the cybersecurity professions.

REFERENCES CITED

Hoffman, L. J., Rosenberg, T., Dodge, R. & Ragsdale, D. (2005). Exploring a National Cybersecurity Exercise for Universities. *IEEE Security and Privacy.* 3, (5), 27–33.

Sadler, D. R. (1989). Formative assessment and the design of instructional systems. Instructional Science, 18 (4), 119–144.

National Cyber League (2015). *About the NCL*. http://www.nationalcyberleague.org/about.shtml

Andrade, H., & Du, Y. (2005). Student perspectives on rubric-referenced assessment. *Practical Assessment Research & Evaluation*. 10(3), 159 –181.

Angelo, T. A., & Cross, K. P. (1993). *Classroom assessment techniques*. San Francisco, CA: Jossey-Bass Inc.

Bloxham, S. & West, A. (2004). Understanding the rules of the game: Marking peer assessment as a medium for developing students' conceptions of assessment. *Assessment & Evaluation in Higher Education.* 29 (6), 7221–7333.

Boud, D., Cohen, R., & Sampson, J. (1999). Peer learning & assessment. *Assessment & Evaluation in Higher Education*, 24(4), 413–426.

Bryan, C., & Clegg, K. (2006). Introduction. In C. Bryan & K. Clegg (Eds.), *Innovative Assessment in Higher Education* (1–8). New York: Routledge.

Carless, D., Joughin, G, & Liu, N. (2006). *How Assessment Supports Learning*. Aberdeen, Hong Kong: Hong Kong University Press.

Castle, S. & Arends, R. (2006). Developing credible performance assessments. In S. Castle and B. D. Shaklee (Eds.), *Assessing Teacher Performance.* (35–48). Lanham Maryland: Rowman and Littlefield Education.

Chothia, T., & Novakovic, C. (in press). Proceedings of the 2015 USENIX Summit on Gaming, Games and Gamification in Security Education. Washington: DC.

Clark, D. J., & Redmond, M. V. (1982). *Small group instructional diagnosis: Final report*. Seattle, WA: University of Washington Seattle. (ERIC Document Reproduction Service No. ED217954.)

Conway, R., & Kember, D. (1993). Peer assessment of an individual's contribution to a group project. *Assessment & Evaluation in Higher Education*. 18(1), (45–56).

Cubric, M. (2007). Wiki-based framework for blended learning. *Proceedings International Symposium on Wikis*. Canada.11–22

Duckworth, A. L., Peterson, C., Matthews, M. D., Kelly, D.R. (2007). Grit: Perseverance and Passion for Long-Term Goals. *Journal of Personality and Social Psychology*. 92 (6), 1087–1101.

Elliott, N. & Higgins, A. (2004) Self and peer assessment– does it make a difference to student group work? *Nurse Education in Practice*. 5, 40–48.

Freeman, M. (1995). Peer Assessment by groups of group work. *Assessment & Evaluation in Higher Education*. 20 (3), 289–299.

Freeman, M., & McKenzie, J. (2002) SPARK, a confidential web-based template for self and peer assessment of student teamwork: benefits of evaluating across different subjects, *British Journal of Educational Technology.* 33, 551–569.

Frechtling, J. (2010). *The 2010 user-friendly handbook for project evaluation* REC99-12175. National Science Foundation. Arlington, VA: NSF.

Goldfinch, J. (1994). Further development in peer assessment of group projects. *Assessment in Higher Education*. 19 (1), 29–35.

Goldfinch, J. M., & Raeside, R. (1990). Development of a peer assessment technique for obtaining individual marks on a group project. *Assessment & Evaluation in Higher Education*. 15 (3), 210-225.

Gupta, L. M. (2004). Enhancing student performance through cooperative learning in physical sciences. *Assessment & Evaluation in Higher Education*. 29 (1) 63–73.

Hassaien, A. (2007). A qualitative student evaluation of group learning in higher education. *Higher Education in Europe*, 31(2/3), 135–150.

Irons, A. (2008). *Enhancing learning through formative assessment and feedback*. New York: New York, Routledge.

i-SAFE Curriculum Effectiveness. (1998–2006). Retrieved April 2, 2008 from http://www.isafe.org/channels/sub.php?ch=op&sub_id=media_curriculum_effectiveness

Klinger, D. A., McDivitt, P. Howard, B.B., Munoz, M.A., Rogers, W.T., Wylie, E. C. (2015). *Classroom Assessment standards for Pre-K–12 Teachers*: Joint Committee on Standards for Educational Evaluation, Kindle Direct Press.

Kvale, S. (2007). Contradictions of assessment for learning in institutions of higher learning. In D. Boud, & N. Falchinkov (Eds.), *Rethinking Assessment in Higher Education: Learning for the longer term* (pp. 57–72). New York, NY: Routledge.

Li, L. K. Y (2001). Some refinements on peer assessment of group projects. *Assessment and Evaluation in Higher Education*. 26(1), 5–18.

Li, L., & Steckelberg, A. L. (2005). Peer assessment support system. *TechTrends*. 49(4), 80-84.

Magin, D. J. (2001). A novel technique for comparing the reliability of multiple peer assessments with that of single teacher assessments of group work process. *Assessment & Evaluation in Higher Education*. 26(2), 139–152.

McGraw, P., & Tidwell, A. (2001). Teaching group process skills to MBA students: A short workshop. *Education & Training*. 43(3), 162–170.

Meier, S. L., Rich, B. S., & Cady, J. (2006). Teachers' use of rubrics to score non-traditional tasks: factors related to discrepancies in scoring. *Assessment in Education*. 13(1), 69–95.

Mirkovic, J., & Peterson, P. (2014). Class Capture-the-Flag Exercises. Proceedings of the 2015 USENIX Summit on Gaming, Games and Gamification in Security Education. Washington: DC.

Morris, B. (1994). CATs project: Reinvigorating our classrooms: Positive results of using classroom assessment techniques. In Patricia A. Malinowski (Ed.), *Classroom implementation: Issues in assessment* (pp. 14–23), Canadaigua, NY: Fingerlakes Community College.

Murphy, B (1994). CATs project: Seeing problems, finding solutions. In Patricia A. Malinowski (Ed.), *Classroom implementation: Issues in assessment* (pp. 24–30), Canadaigua, NY: Fingerlakes Community College.

National Cyber Defense Competition (NCCDC) (2015). *About.* http://www.nationalccdc.org/index.php/competition/about-ccdc

Ozogul, G., Olina, Z., & Sullivan, H. (2008). Teacher, self and peer evaluation of lesson plans written by preservice teachers. *Education Tech Research Development*, 56(2), 181–201.

Pope, N. (2001). An examination of the use of peer rating for formative assessment in the context of the Theory of Consumption Values. *Assessment and Evaluation in Higher Education*. 26(3), 235–246.

Prins, F. J., Sluijsmans, D. M. A., Kirschner, P. A. & Strijbos, J. (2005). Formative peer assessment in a CSCL environment: A case study. *Assessment & Evaluation in Higher Education*, 30(4), 417–444.

Pusey, P., O'Brien, C. O., Lightner, L. (2015). *Resource guide for preparing for the Collegiate Cyber Defense Competition: A guide for new teams and recommendations for experienced players.* https://scout.wisc.edu/cyberwatch/r134/resource_guide_preparing_for_the_collegiate_cyber_defense_competition_ccdc_a_guide_for_new_teams_and_recommendations_for_experienced_players

Pusey, P., Tobey, D. & Soule, R. (2014). An argument for game balance: Improving student engagement by matching difficulty level with learner readiness. *Proceedings of the 2014 USENIX Summit on Gaming Games and Gamification in Security Education*. San Diego: CA.

Richlin, L (1998). Using CATs to help new instructors develop as teachers. *New Directions for Teaching and Learning*, 75, 79–86.

Samanta, S. (1994). CATs in cooperative physics. In Patricia A. Malinowski (Ed.), *Classroom implementation: Issues in assessment* (pp. 34-47), Canadaigua, NY: Fingerlakes Community College.

Schaufeli, W., and Bakker, A. (2003). *UWES—Utrecht Work Engagement Scale: Test manual.* http://www.beanmanaged.com/doc/pdf/arnoldbakker/articles/articles_arnold_bakker_87.pdf

Schaufeli, W., Bakker, A., and Salanova, M. "The measurement of work engagement with a short questionnaire: A cross-national study," *Educational and psychological measurement*. 66, 4 (August, 2006), 701–716.

Sivan, A. (2000). The implementation of peer assessment: An action research approach. *Assessment in Education*, 7(2), 193–213.

Sluijsmans, D. M. A, Brand-Gruwel, S., vanMerriënboer, J. J. G & Bastiaens, T. J. (2003). The training of peer assessment skills to promote the development of reflection skills in teacher education. *Studies in Educational Evaluation*, 29, 23–42.

Sluijsmans, D. M. A, Brand-Gruwel, S., vanMerriënboer, J. J. G & Martens, R. L. (2004). Training teachers in peer-assessment skills: Effects on performance and perceptions. *Studies in Educational Evaluation*, 41(1), 59–78.

Sluijsmans, D., & Prins, P. (2006). A conceptual framework for integrating peer assessment in teacher education. *Studies in Educational Evaluation*, 32, 6–22.

Tal-Elhasid, E., & Meishar-Tal H., (2007). *Models for activities, collaboration and assessment in wiki in academic courses*. Eden conference electronic proceedings. Retrieved April 1, 2008 from www.biu.ac.il/bar-e-learn/eden2007/tal_tal.doc.

Tsai, C.-C., Liu, E. Z.-F., Lin, S. S. J. & Yuan, S.-M. (2001) A networked peer assessment system based on a vee heuristic. *Innovations in Education and Teaching International*, 38, 220–230.

Wen, M. L., Tsai, C.-C., & Chang, C.-Y. (2006). Attitudes towards peer assessment : A comparison of the perspectives of pre-service and in-service teachers. *Innovations in Education and Teaching International*, 43(1), 83–92.

AUTHORS

Portia Pusey (edrportia@gmail.com) is director of instructional design and senior researcher for VivoWorks Inc. She builds educational experiences and leads research projects designed strengthen our national preparedness to protect our digital infrastructure by enriching the engagement and professional skills of cybersecurity learners and professionals. Her professional efforts focus on applying rigorous formative assessment techniques to increase knowledge and skills through professional practice in formal and informal cybersecurity learning situations. She manages discrete project strands to realize a wider program of work which prioritizes the development of differentiating skills in cybersecurity and healthcare fields. She has made significant contributions to the design, implementation, and assessment of curriculum and professional development for online and face-to-face learning.

David Tobey, PhD, (dhtobey@hccenter.org) is currently the director of the Center for Aging Studies at Holy Cross College, a visiting assistant professor at Indiana University – South Bend. He leads a research team investigating and implementing new techniques for competent aging. These techniques seek to: 1.) shorten learning curves during the formative years to address the growing international workforce skills crisis precipitated by the retirement of the baby boom generation; 2.) facilitate lifestyle changes necessary to improve health and vitality during early and middle adulthood; and 3.) reinvigorate brain growth during late adulthood to increase brain health and mitigate or reverse mental decline associated with neurological disease. Tobey's research into the formation of expertise led to the development of a theory of competence development and expert performance and developed a new psychometric technique, Potential Performance Analysis ™. PPA assesses the current level and potential of competence development and identifies appropriate interventions needed to reach or maintain maximum potential.

Diana L. Burley (dburley@gwu.edu) is a professor in the Graduate School of Education and Human Development at George Washington University. She is a nationally recognized cybersecurity workforce expert and also has published extensively on public sector IT use, knowledge management, and information sharing. Prior to GW, she served as a program officer at The National Science Foundation where she managed a multimillion-dollar computer science education and research portfolio and led the CyberCorps program. Based on her work at NSF, Burley was honored by the Federal CIO Council and the Colloquium on Information Systems Security Education (CISSE) for outstanding efforts toward the development of the federal cybersecurity workforce. In 2014, Burley was named the cybersecurity educator of the year by CISSE and one of the top ten influencers in information security careers by Careers Info Security magazine.

Deanne Cranford-Wesley (dwesley@forsythtech.edu) is chair, Davis ITEC Center (Information System Security) at Forsyth Technical Community College. Cranford-Wesley is a cybersecurity professional and has appeared as a subject matter expert on Fox8 and Time Warner News discussing recent advances in cybersecurity vulnerability. She also teaches Information System Security, Computer Forensics. and Networking courses in the Business Information Technology Department. Currently she has led the Business Information Technology department to the designation of Center of Academic Excellence in Information System Security. Additionally, Cranford-Wesley has presented at various conferences, including several presentations at The Colloquium Information System Security Education Conference, CompTIA Educators Conference, and North Carolina Computer Instructor Conference (NCCIA).

Cranford-Wesley has vast experience in online education, curriculum mapping, grant writing, research, and program evaluation. She is a published author of various technology- related articles. She holds a PhD in Education Leadership with a focus in Instructional Technology and a Master of Art in Administration. Furthermore, she has obtained the following certifications; IC3, Security +, Cisco Certified Network Professional (CCNP), Cisco Certified Network Associate (CCNA), and Cisco Certified Instructor (CCAI).

Jacob Frank (jmfrank@email.gwu.edu) is the advanced degree program coordinator for the Executive Leadership Program at George Washington University. He holds an MA in Sociology from Northern Illinois University, and is pursuing a PhD in Social Sciences at Syracuse University.

The Central New York Hackathon: A Case Study on the Collaborative Design and Implementation of a Regional Cyber Defense Event

Jake Mihevc | Ronny Bull | Nick Merante | Brandon Froberg

ABSTRACT

As the demand for cybersecurity practitioners continues to increase, academia is challenged to produce students with both the academic foundation and practical skills necessary to contribute to the cybersecurity workforce. This challenge has contributed to the emergence of cybersecurity conferences and competitions as a means of developing practical skills. Community colleges are uniquely suited to develop regional cybersecurity conferences and competitions. Mohawk Valley Community College and its partners have successfully created such an event, entitled the Central New York Hackathon. The Central New York Hackathon is a biannual collaborative learning event that is now entering its second year. It leverages local cybersecurity professionals and academic faculty to design and implement competitive exercises for students and provide demonstrations and presentations on current cybersecurity topics. Students from the State University of New York Polytechnic Institute, Utica College, Syracuse University, Herkimer County Community College, and Mohawk Valley Community College participate in the event. The process of creating the Central New York Hackathon presented a series of challenges to MVCC and its partners. The challenges fall into five broad categories: coalition building, development of technology infrastructure, exercise design, academic objectives and assessment, and student leadership and teamwork. Exploration of our shared experience in the design and implementation of the Central New York Hackathon can be instructive to other cybersecurity communities as they develop similar events.

INTRODUCTION

The Central New York Hackathon (CNY Hackathon) is a biannual, regional cyber defense event in which central New York cybersecurity students participate in practical cybersecurity exercises and learn from local industry professionals. The CNY Hackathon takes place over a two-day period. On Friday afternoon students attend a kick-off event featuring presentations by local cybersecurity professionals. After the presentations, students are assembled into teams for Saturday's exercises and spend time preparing and strategizing. On Saturday, the teams work to complete a static challenge exercise in the morning, followed by a dynamic capture-the-flag exercise in the afternoon. Over the first three CNY Hackathon events held, student and professional feedback on the event has been extremely positive. Student participation has grown steadily, and student skills and abilities appear to grow more robust with each event.

The process of designing and implementing the CNY Hackathon presented many challenges to Mohawk Valley Community College (MVCC) and its partners. The challenges can be grouped into five broad categories: coalition building, development of technology infrastructure, exercise design, academic objectives and assessment, and student leadership and teamwork. Our coalition experienced both successes and failures in our effort to meet these challenges. Data collected from student participants and cybersecurity professionals serving as observers contributes to the assessment of our performance. This analysis of our shared experience may be instructive to other cybersecurity communities that consider creating a regional cybersecurity event.

COALITION BUILDING

The CNY Hackathon is more than a recurring event; it is also a learning coalition. The formation and maintenance of this coalition has been, and will continue to be, a tremendous challenge. Coalition-building is a natural role for community colleges in cybersecurity education. MVCC is uniquely suited to this role, and serves as the foundation of the CNY Hackathon.

The central goal that unites the coalition is to prepare students for employment in our local cybersecurity workforce. The Air Force Research Laboratory, Information Directorate (AFRL/RI) in Rome, New York, and the information security community that surrounds it create a demand for a highly-skilled workforce. MVCC has become the entry-point to the cybersecurity field for many of our local students, as its Computer Science: Cybersecurity degree had grown to 96 students by the fall of 2014. Through articulation agreements, shared faculty and program advisory boards, and the CNY Hackathon, MVCC's cybersecurity degree program represents the local consensus on the foundation of a cybersecurity education. The majority of MVCC cybersecurity students continue to pursue baccalaureate degrees with our coalition partners, the State University of New York Polytechnic Institute (SUNY Polytechnic) and Utica College. These student and programmatic linkages allow MVCC to maintain the learning coalition behind the CNY Hackathon.

MVCC is also uniquely suited to encourage the participation and input of the local cybersecurity community in the CNY Hackathon. From 2009 through 2013, MVCC's federally funded "CyberJobs" program provided free training in cybersecurity to more than 2,200 participants. Over 30 cybersecurity community entities participated as program partners. The partners provided input on instructional content and many of the program participants. Dialogue within these partnerships contributed to the formation of the CNY Hackathon learning coalition. One of the most significant developments that emerged from the CyberJobs program was the addition of AFRL/RI staff members to the CNY Hackathon coalition. Without their help, the CNY Hackathon would not be what it is today.

The AFRL/RI is located at the former Griffiss Air Force base in Rome, New York, and referred to locally as Rome Research Site (RRS) or simply "Rome Labs." The AFRL/RI has demonstrated a rich heritage of community service, education, and training in the surrounding areas stretching back for decades.

The recent AFRL/RI focus on science, technology, engineering, and math (STEM) education includes such offerings as the Lego Robotics Camp, Cyber Summer Camps 1.0 and 2.0, Summer Engineering Camps, March Math Madness, and an upcoming Arduino Camp. These camps greatly enhance the STEM knowledge base of students from kindergarten to college while increasing early interest in related fields. With such a wide variety of topics, it comes as no surprise that most offerings are at maximum capacity for student attendance.

However, one very common thread has consistently piqued the interest of the labs and local industry professionals alike: cyberspace training and education. AFRL/RI employees have a unique research and development background with respect to cyberspace, as they are at the forefront of future

technology development in cyberspace for the whole of the Air Force. Given this mission, it is a natural extension for service members of the AFRL/RI to give back to the community as volunteers.

As local STEM programs interacted with national programs, a local movement started to occur to expand and enhance cyberspace and information assurance training. One of the most popular and successful programs was the cyber Capture the Flag (CTF) exercises known internally as the "Cyber Defense Workshops," which pitted local secondary school Cyber Patriot students against the employees of the AFRL/RI in a "red" versus "blue" competition. These workshops were part of the genesis that helped fuel the support and participation of AFRL/RI volunteers in the CNY Hackathon events.

DEVELOPMENT OF TECHNOLOGY INFRASTRUCTURE

Bull (2012, 2013) outlines the virtualization platform utilized for the CNY Hackathon competition. This platform has been successfully used to provide interactive laboratory environments for many of the network and computer security, computer science, and telecommunications courses offered at SUNY Polytechnic over the past three years. The platform has shown proven scalability with the ability to host over 200 simultaneously running student virtual machines with adequate resource allocation and was easily extended to support the first regional CNY Hackathon event at SUNY Polytechnic. The platform was then duplicated the following semester at MVCC for the second event. Standardization of the platform facilitates the seamless migration of exercises and virtual machines between host institutions, which provides continuity to the student experience. It also allows MVCC student administrators to develop familiarity with the technology in use at likely upper-division transfer destinations, thus facilitating transition to the next phase of their education. MVCC has also begun the process of adapting some of its current cybersecurity courses to use the platform as a virtualized laboratory environment in order to provide its students with an increased amount of hands-on and experimental learning opportunities.

Infrastructure Design

A competition platform based on a centralized virtualization approach as outlined in previous work (Anderson, Joines, and Daniels, 2009; Bull, 2012; Bull, 2013; Li, 2010; Wang, Hembroff, and Yedica, 2010) is a much more scalable and manageable solution as compared to a purely physical environment. The entire CNY Hackathon competition platform is accessible via a Web browser, allowing the hosting school to utilize existing computer laboratories without having to modify them to suit the competition. Students log in to a generic account on the physical systems and use a Web browser to access their competition virtual machines. Each team is provided with a set of virtual machines that are protected by a unique team login and password combination. When a team member logs into the environment they are presented with a list of their team's virtual machines and have the ability to gain console access to any of the systems. They can also use the interface to power cycle the systems and take snapshots if they wish.

The competition platform also has the ability to integrate into the hosting school's network infrastructure. Specifically administrators can take advantage of existing Virtual Local Area Networks (VLANs) in order to place virtual machines (VMs) on an appropriate sub-network. Typically for cybersecurity competition purposes a *DarkNet* VLAN as described by Bull (2012) is created to which all of the virtual machines are associated. The *DarkNet* VLAN is completely isolated from all other campus network resources by the absence of layer-three routing and a default gateway. This limitation prevents competition traffic from leaving the *DarkNet* VLAN so the hosting school can rest assured that their production networks are not being affected by cybersecurity exercises (Bull, 2012).

As previously stated, student access to the competition virtual machines is completely Web based. Each team is typically provided with enough Kali

Linux virtual machines for each team member to use as a workstation within the *DarkNet* environment. Depending on the challenge, teams may also be assigned a core set of server VMs that they must secure and defend. It is advisable to provide students with large enough monitors on the computer laboratory systems so that they can effectively work with multiple virtual machines simultaneously. Access to the Web portal can be provided in a variety of ways. The open source software that the CNY Hackathon platform uses for this functionality provides authentication via a local database, Lightweight Directory Access Protocol (LDAP), or Active Directory.

Scalability

By using a centralized virtualization approach, the hosting school reduces the physical resources required to build an adequate competition infrastructure. An intercollegiate cybersecurity competition requires an abundance of desktop and server computers in order to be effective and maintain student interest. If these systems are physical then either the hosting school is purchasing new equipment to be used for the competition, or they are re-purposing existing campus systems, which may need to be reverted after the competition is over so they can be used for their original purpose again. The competition also requires an isolated network infrastructure. Setting this up physically is a time-consuming process that may require setting up new switches and routers as well as running new cabling to each of the competition rooms. By using a centralized virtualization approach that the students can access with a simple Web browser from any system, the overhead of creating an effective competition infrastructure is drastically reduced. The competition infrastructure used by the CNY Hackathon is easily scaled for increasing student attendance and can all be centrally managed from a single location. Competition virtual machines are created from base templates, which the black team develops prior to the event, that are easily deployable within minutes. This rapid deployment capability also facilitates recovery should a VM be irreparably damaged during the course of the competition.

Performance

Hosting of the virtual competition platform for the spring 2015 event was provided by SUNY Polytechnic, sharing server and network infrastructure currently in use by several active courses. The spring semester saw an unusually high class utilization level of the virtual environment, with approximately 400 student VMs created to support six classes and assorted student projects. This high class utilization was easily accommodated by a lone HP Proliant server dedicated to the task. A pair of 12-core 2.7 GHz CPUs was found easily able to handle processing needs. 256 GB of RAM was able to accommodate concurrency for all class VMs throughout the semester and 2 TB of RAID 1+0 storage was sufficient for housing all VMs.

The hackathon was expected to add one workstation Kali Linux VM per participant, two competition "attack and defend" VMs per team, and eight support VMs to provide services such as competition scoring, DHCP, DNS, red team attack pivots, and other challenges for the teams. Each Kali VM was allocated 2 GB of RAM due to the high needs of the metasploitable toolkit. The remaining competition and support VMs were more modestly allocated 512 MB each.

Of the three resources, available RAM was projected to be the limiting factor with 96 GB expected to be required to host the event. This exceeded the amount presently available, requiring shutdown of one-third of the spring class VMs for the duration of the competition.

Despite high utilization, the platform proved stable throughout the event with no noticeable service degradation by the black or red teams and none reported by the student participants.

EXERCISE DESIGN

One of the primary drivers for the CNY Hackathon exercise design and execution was to leverage existing work as built for the AFRL/RI Cyber Defense Workshops. There were several events that the AFRL/RI hosted internally and externally that emphasized basic cybersecurity skills that could be tracked in real time on a central scoring and display server. All of the events were simple in design, tracing concepts of Self-Organized Learning Environments (SOLE) as outlined by Dr. Sugata Mitra (2013). Dr. Mitra (2013) discusses a SOLE as an unmanned "School in the Cloud" where students are driven by the big questions which their mediators simply present. The concept of the SOLE is the heart of the AFRL/RI design, and it helped minimize the total infrastructure needs, tracking, and feedback needed in establishing the Cyber Defense Work events. The original design was simple: provide basic cyber defense training and skills, provide an isolated network with Internet access, provide the defenders (Blue Team) with the same and a highly vulnerable machine, let loose the AFRL/RI based volunteer attackers (Red Team), and see what happens.

This Red vs. Blue model has become somewhat traditional in the world of cybersecurity, since cyber CTF events seem to be occurring monthly at various conventions and can be found online through various companies and organizations. Thus, the AFRL/RI volunteers pitched in and brought forth a new CTF construct. First, task the students to both defend and attack against one another as "Purple Teams." Second, task event officials to perform both traditional white and red team roles: enforce rules, conditions, and boundaries, and use red team methods to provide corrective actions during the event. Event officials thus became the "Pink Team."

Such a completely new construct gave a much more difficult challenge to the AFRL/RI volunteers, since they now had to stay ahead of the students' cyber defensive measures. The "White Team" always has a means to fully control an event at any time in traditional CTF events, but the Purple Team vs. Pink Team construct allows for the students to block the staff and educators if they have an advanced cyber defense skill set. This difference greatly challenged the conceptual understanding and execution of the CNY Hackathon and gave fail states that were immediately discovered in the event. For example, the educators and trainers have a threat of failure directly, which is orthogonal to the challenges of exercise execution.

Lessons Learned

Both the first CNY Hackathon event in the spring of 2014 and the second event in the fall of 2014 provided many valuable insights and lessons learned during the execution of the events. Wright (2013) speaks of a "Failure Space" which is a subset in the total "Possibility Space" of a digital environment; failure spaces allow an individual to create, refine, and find fallacies involving the individual's understanding and model of their comprehensive world model. Nested failures allow for the expansion of a person's expectations and understanding of the rules of a given "world." Additionally, Wright (2013) states that individuals can find more enjoyment and will spend a majority of time within "Failure Spaces,", and as long as they understand how they fail, they will learn from their failures.

The exercise design allows for both CNY Hackathon students and staff to have a failure space, which allows for a much richer comprehension of the capabilities, knowledge, and understanding of the cybersecurity lessons learned. With proper feedback the failure space allows for a much more reactive and useful learning platform. Given this inherent design and the ability to fail, the following sections will outline the Pink Team's failures in the first two CNY Hackathon events.

First, the Pink Team failed through the reuse of materials and methods. One of the most shocking revelations was the familiarity and recognition by the students of the CNY Hackathon environment. The original design of the event leveraged the Metasploitable 2.0 edition of Ubuntu Linux that is a training tool for the Metasploitable Framework.

At the time of the event the Metasploitable 2.0 image did not offer support, as it had exceeded its service life and by 2014 was nearly six years old. Limited support of the VM hindered patching and requisition of tools that could have been leveraged by either cyber defenders or cyber offenders. Additionally, the first event had greatly leveraged immutable SSH keys for remote access by the Pink Team. At the conclusion of the first event in the spring of 2014, over 60 percent of the student machines were still accessible. During the second event, this attack vector was patched within minutes. This lesson learned speaks to the incredible ability of students to learn from past events and to share this information amongst each other. Additionally, the Pink Team did not practice the process of execution for the first event. It was brought together as a patch-work assembly, which did not coordinate techniques, tactics, or procedures. This was in contrast with the very well informed and practiced Purple Teams.

Second, the Pink Team failed to implement a provisioning management system. This denied some of the AFRL/RI volunteers the ability to participate in the second CNY Hackathon. Ansible Inc. provides an appropriate tool for such a task. Ansible automates cloud provisioning, configuration management, application deployment, and intra-service orchestration ("How Ansible Works," 2015). The tool follows an established YAML script that can store SSH keys, user names, passwords, and IP addresses, allowing for a rapid, consistent, and verifiable means to ensure deployment of configurations to any and all participating machines. In the absence of the volunteers, a simple bash script was leveraged to help automate the configuration and deployment, but there were many cases in which a bash script would be eclipsed by Ansible's capabilities. For example, Ansible could follow a script to pull the latest sources of a tool, apply custom patches and configurations, and report back the status and final state of the installation. The first CNY Hackathon event focused on using Linux-based VMs, thus an immediate limitation would be portability to other operating systems. Ansible provides for different configurations allowing any and all operating systems.

The lack of an infrastructure management system was addressed for the third CNY Hackathon event. SaltStack was selected as an open-source alternative to Ansible and integrated into competition VM master images prior to replication, and available for Black or Red team use post-deployment and throughout the competition. The SaltStack platform allows for rapid deployment of configuration changes, binary distribution, and execution of arbitrary commands on individual or all deployed virtual machines. Since few teams identified and prevented access to the service, this also became another means for the Red Team to maintain persistence.

Last, the Pink Team failed to implement command and control capabilities modeled on an advanced persistent threat. One of the most effective cyberspace offensive techniques is the Advanced Persistent Threat (APT), which could be summarized as an unblockable, undetectable puppet master of victim machines. The Pink Team failed to secure the mechanisms needed for persistence, thus for most of the second event the Pink Team was ineffective. A desirable mechanism to fulfill such needs would be a Loadable Kernel Module, which would circumvent most, if not all, of the students' means for protection. The necessity to have constant command and control stems from Pink Team's ability to monitor and gage the activity of the students. Keyloggers were installed on all of the student's VMs, but with the lack of a global command and control tool, the files were locked to the given host. The APT allows for the highest privilege level of the control as compared to all other users on a system. Having the APT would allow for the Pink Team to completely control a VM at anytime regardless of the actions of the student defenders. One example of an APT would be the Suterusu RootKit, an open-source Loadable Kernel Module for Linux operating systems. It allows for full control of a Linux operating system with abilities to hide processes, hide

ports, hide directories and files, and has a mechanism to allow for a remote user to transfer and execute files (Copolla, 2014).

Side Challenges

A side challenge was introduced to the third CNY Hackathon event in order to better engage students new to the field who may not be able to contribute to their team as fully as their more experienced peers. This side challenge also allowed all competitors an opportunity to take a short break from the main competition while still remaining productive. Lock picking was selected as a fun, hands-on activity which would not require prior knowledge in order to participate. A tutorial, demonstration, and practice session was held the evening prior to the hackathon competition in order to familiarize participants with tools and lock mechanics. Three grades of locks were selected in increasing difficulty for competition participants to defeat with a tiered reward system instituted to tie the side challenge into the main event. Defeat of a lock would yield one of three clues paired to its difficulty level useful to the attack or defense of the competition virtual machines. Many of the new competition participants took advantage of the side challenge and were successful in obtaining this information for their team, providing these team members their own sense of accomplishment. Plans for the fourth CNY Hackathon include a side challenge based on wireless technology.

ACADEMIC OBJECTIVES

As the CNY hackathon has matured, the execution of the event and its exercises have become more consistent and manageable. This has allowed the coalition to focus on aligning the exercises with academic objectives. The goal of implementing academic objectives is to transition the event from a fun and informative event to an integral component of a cybersecurity education. Establishing academic objectives will also allow our coalition to assess the combined performance of our academic programs.

The primary objective of the CNY Hackathon event is to provide student participants with real life skills that increase their chances of employment as network and computer security professionals. The following academic objectives were first implemented for the spring 2015 CNY Hackathon:

- Students will demonstrate the ability to utilize tools commonly employed by network security professionals to conduct network security audits.
- Students will demonstrate the ability to identity network security threats, vulnerabilities, and exploits.
- Students will demonstrate the ability to secure (harden) systems and services.
- Students will demonstrate their ability to work in a team environment.

For the spring 2015 event we asked students to self-assess through post-event surveys. Eighty-one percent reported an increase in their ability to use tools. Eighty-eight percent reported an increase in their ability to identify threats, vulnerabilities, and exploits. Seventy-five percent reported an increase in their ability to secure systems and services. Eighty-eight percent reported an increase in their ability to work in a team environment. In the future we plan to build objective-oriented milestones into the individual exercises. The group achievement of these milestones will validate student feedback regarding successful completion of academic objectives.

STUDENT LEADERSHIP AND TEAMWORK

During the design phase of the CNY Hackathon, the coalition decided to formulate teams in the manner most conducive to student learning. Creating teams based on institution raised two serious concerns. First, variation in skill level between two-year and four-year students may create an uneven playing field. Second, intercollegiate rivalry and competition may force the students to focus on winning and losing rather than learning. The decision to create mixed teams with students from different

institutions addressed these concerns, and led to some unforeseen positive developments in regard to student leadership.

The primary focus of each team was to competitively operate against each other and the Pink Team in order to secure their systems from attack and penetrate target systems assigned to competing teams. The many avenues of attack and many points to defend forced the teams to operate at as fast of a pace as possible. A mixed team approach distributed the most skilled students among the teams as well as the least experienced students. During first CNY Hackathon, we observed the most experienced team member directly performing the majority of required tasks with the least experienced team members operating as passive observers at a distance far from the action. One person performing the majority of the tasks for the sake of speed was not conductive to the teamwork atmosphere and learning environment envisioned for the CNY Hackathon. This issue was addressed for future events by identifying and promoting the most skilled student on each team to team captain. A rule was then instituted limiting the team captain to a leadership role, thus prevented from direct access to the competition platform. Banning the captain from keyboard access saw several positive results. Each team now has a technically experienced leader, someone who could assess the human resources of each team, effectively using each team member as a force multiplier. Less experienced participants were better engaged, completing tasks assigned by the captain occasionally with the captain's assistance. As a result, this demographic showed a higher satisfaction with the competition and their role in it. This arrangement also allowed brief opportunities for the team captain to serve as a mentor to new participants, developing skills in that capacity as well as team leadership.

The students exceeded all expectations for understanding and performance at each of the CNY Hackathon events. They consistently demonstrated the aptitude, understanding, and self-motivation to develop the skill sets needed for the exercise and to resonate extremely well in the SOLE that they were given for the events. Additionally, the students adapted to the scenarios as originally created, and also kept up with the unique challenges presented to them by the Pink Team. For example, the students found it hard to block connections when the firewall tools were manually deleted, but quickly transferred new binaries.

To leverage previously mentioned concepts, the students exhausted both the possibility and failure spaces of the event, which ultimately caused the CNY Hackathon staff into failure states of their own.

The overall skill set of any given CNY Hackathon student, with respect to education and training, was much less than the coalition staff. Even with this disadvantage, all teams eventually showed that the rudimentary setup of the first CNY Hackathon was quickly eclipsed by their speed of learning and understanding cybersecurity concepts. Lessons learned from the CNY Hackathon events allow all students to learn valid cybersecurity skills which can be leveraged immediately, as compared to awaiting the full completion of formal degree programs.

CONCLUSION

As this paper illustrates, the design and implementation of a regional cybersecurity event is an ongoing process. A learning coalition must be assembled and maintained. The proper technology infrastructure must be implemented and updated as exercises evolve. Exercise design must be dynamic, forward-looking, and anticipate dramatic increases in student capabilities. Academic objectives may be developed and implemented to map the exercise to academic curriculum. Finally, the event rules must be structured to foster student leadership and student learning.

The greatest challenge to the learning coalition, however, is to ensure the event keeps pace with the rapid development of student skills and abilities. The brilliance and creativity of our students makes anticipation of their techniques extremely difficult. Any weakness in infrastructure or exercise design is likely to be exposed by student participants. It

is important that students and event organizers embrace any emergence of "failure space" as an opportunity to explore and learn. The learning coalition at the foundation of the CNY Hackathon has been successful at both meeting the design and implementation challenges presented and leveraging any faults as opportunities to learn and improve.

REFERENCES CITED

Anderson, B.R., Joines, A.K., & Daniels, T.E. (2009). Xen worlds: leveraging virtualization in distance education. In *ITISCE '09 proceedings of the 14th annual ACM SIGITE conference on innovation and technology in computer science education* (p. 293–297).

Bull, R. (2012). Design and implementation of a computer science virtualized lab environment at SUNY IT (master's thesis). *State University of New York Institute of Technology.*

Bull, R. (2013, October). Migrating a voice communications laboratory to a virtualized environment. *SIGITE '13 Proceedings of the ACM SIGITE conference on Information Technology education*, 189–194.

Coppola, M. (2014, September 4). *Suterusu.* Retrieved from https://github.com/mncoppola/suterusu

How ansible works. (2015). Retrieved from http://www.ansible.com/how-ansible-works

Li, P. (2010, December). Centralized and decentralized lab approaches based on different virtualization models. *Journal of Computing Sciences in Colleges*, 26(2), 263–269.

Mitra, S. (2013, February). *Sugata Mitra: Build a school in the cloud*. [Video file]. Retrieved from https://www.ted.com/talks/sugata_mitra_build_a_school_in_the_cloud?language=en

Wang, X., Hembroff, G.C., & Yedica, R. (2010). Using vmware vcenter lab manager in undergraduate education for system administration and network security. In *SIGITE '10 proceedings of the 2010 ACM conference on information technology education* (p. 43–52).

Wright, W. (2013, November 15). *Will Wright—gamifying the world: From simcity to the future (gsummit sf 2013)*. Retrieved from https://www.youtube.com/watch?v=xZ0FODvjs

AUTHORS

Jake Mihevc (jmihevc@mvcc.edu) is the director of the Computer Science: Cybersecurity AS degree program at Mohawk Valley Community College and is a cofounder of the Central New York Hackathon. His background includes systems and platform engineering for a number of start-ups in the San Francisco Bay area during the late 1990s.

Ronny L. Bull (rlbull@utica.edu) is a computer science PhD. graduate student at Clarkson University focusing on Layer 2 network security in virtualized environments. He also is an assistant professor of computer science at Utica College, and was a founding faculty member of the School of Engineering at SUNY Polytechnic Institute in Utica, New York. Bull performs work as an independent consultant specializing in the areas of cyber defense, voice over IP, and virtualized laboratory solutions for educational environments.

Nick Merante (nickm397@cs.sunyit.edu) leads the Computer Science Department's academic computing team at SUNY Polytechnic Institute in Utica, New York., where he also serves as adjunct lecturer in their Network and Computer Security program and advisor to the student NCS Club.

Captain Brandon Froberg (Brandon.Froberg.1@us.af.mil) is a former "Lab Rat" and was stationed at Rome Research Site for the Information Directorate for the Air Force Research Laboratory from 2010–2014. He is a cyber acquisitions officer and specializes in the research, design, and assurance of cyber products for the Air Force. Currently, he is stationed at Wright Patterson Air Force Base in Dayton, Ohio.

NCI Symposium on Security in Cyberspace

Jane LeClair, EdD | Matthew Flynn, PhD

INTRODUCTION

As evidenced by the recent cyber attacks on the Office of Personnel Management (OPM), cybersecurity breaches perpetrated by nation states continue to be an escalating threat to U.S national security. In our ongoing effort to address this growing concern, on May 13, 2015, the National Cybersecurity Institute (NCI) in Washington, D.C., hosted a final symposium of a series of three such events addressing improving security in cyberspace among U.S. government and civilian professionals. As with the previous two meetings in the fall of last year and the winter of this year, the spring symposium gathered together a notable panel of cyber experts to offer their unique perspectives to the attending audience of some 25 participants. The symposium, titled Security in Cyberspace, was held at the main offices of NCI at 2000 M St, NW in the nation's capital.

SYMPOSIUM HIGHLIGHTS

The event was again hosted by Jane LeClair, the chief operating officer of NCI, who introduced the speakers following an informal conversation among the attendees. Those sitting on the panel included Paul Caiazzo from TruShield Security Solutions, Matthew Flynn from the Marine Corps University, Mark Noble of ISACA, and Ron Carpinella from Decooda International. The audience collected professionals from both private business and government service, and the small size of the event allowed extensive participation from those attending.

The discussion was opened with remarks from moderator Irving Lachow of Mitre who began the panel discussion by providing a framework for the conversation centered on better understanding the openness of cyberspace. All participants agreed this element is a key virtue of the medium, but perspectives on what that quality is and how best to advance it varied.

Following Lachow's opening remarks, Paul Caiazzo from TruShield Security Solutions was the first to address the gathering. Caiazzo noted the importance of the Internet and the benefits it provided, but cautioned of its negatives as well. He spoke of the Internet as a vehicle of change, but one that those with malicious intent exploit. Caiazzo posed the question of whether current rules and regulations are doing enough to protect digital information.

Matthew Flynn, professor of war studies at the Command and Staff College, Marine Corps University, spoke of U.S. policy in cyberspace and the importance of maintaining U.S. dominance in that arena. He expressed dismay that U.S. policy decision makers and key leaders in industry continue to voice a desire to embrace openness but also express alarm at American vulnerabilities in that domain due to that very reality of openness. Flynn stressed the ideological platform that is the Internet and one advancing western norms and values, so much so that the West enjoys a permanent, asymmetrical, strategic advantage in cyberspace. What that ideology is and how it reflects a western outlook is where the conversation should be centered, not rooted in the fear of vulnerabilities speaking to a flaw in any U.S. way of life.

Additional presenters included Mark Noble, the cyber/information security practices manager at ISACA, and the final speaker at the event was Ron Carpinella from Decooda International.

The invited speakers spoke not only on the importance of the Internet in our daily lives, but also on the dangers that are associated with it when utilized by those with malicious intent. As evidenced by the relentless attacks on our digital systems by foreign nationals, the information stored on them is highly desired. Defending that data is an evolving and ongoing process that requires our best efforts from everyone involved. This NCI symposium increased awareness of the need for heightened cybersecurity and to further determine what that security should look like. Shutting off openness may well do the work of bad actors in that domain for them. Hopefully, in defining and defending openness, those engaged in seeking better cybersecurity can do so without negatively and unduly impacting this crucial element of cyberspace.

AUTHORS

Jane A. LeClair (jleclair@excelsior.edu), EdD, is currently the chief operating officer at the National Cybersecurity Institute (NCI) at Excelsior College in Washington, D.C., whose mission is to serve as an academic and research center dedicated to increasing knowledge of the cybersecurity discipline. LeClair served as dean of Excelsior's School of Business &Technology prior to assuming her current position. Before joining Excelsior College, LeClair held positions in education and in the nuclear industry, bringing her teaching energies to a number of other colleges while having a full-time career in the nuclear industry. Her work in the industry brought her to the attention of the International Atomic Energy Agency (IAEA) with whom she continues to collaborate. LeClair has also been actively involved in a variety of professional organizations. She is well known for being a vocal advocate for attracting and retaining more women in technology fields. Her areas of interest include social engineering, women in cybersecurity, and cybersecurity training.

Matthew J. Flynn (mflynn92@gmail.com), PhD, accepted a faculty position with the Command and Staff College, Marine Corps University, in July 2012. He has taught at a number of universities and most recently served as an assistant professor at the United States Military Academy, West Point, in both the Military and International Divisions of the History Department. Flynn is a specialist in comparative warfare of the U.D. and the world. His publications include a recent co-authored study titled *Washington & Napoleon: Leadership in the Age of Revolution* (Potomac Books 2012), and books such as *First Strike: Preemptive War in Modern History* (Routledge, 2008), and *Contesting History: The Bush Counterinsurgency Legacy in Iraq* (Praeger Security Int., 2010). Together these works examine a wide range of foreign policy issues across time and in a global context. Flynn received his PhD from Ohio University in 2004 after advanced study in civil-military relations with OU's distinguished Contemporary History Institute. His general areas of interest are great power status, preemptive war, cyber warfare, and piracy.


EXCELSIOR COLLEGE
FOUNDED IN 1971