Journal of Cybersecurity Education, Research and Practice

Volume 2016
Number 2 *Two*

Article 3

December 2016

Planning and Implementing a Successful NSA-NSF GenCyber Summer Cyber Academy

Bryson R. Payne
University of North Georgia, bryson.payne@ung.edu

Tamirat Abegaz
University of North Georgia, tamirat.abegaz@ung.edu

Keith Antonia
University of North Georgia, keith.antonia@ung.edu

Planning and Implementing a Successful NSA-NSF GenCyber Summer Cyber Academy

Abstract
The GenCyber program is jointly sponsored by the National Security Agency (NSA) and the National Science Foundation (NSF) to help faculty and cybersecurity experts provide summer cybersecurity camp experiences for K-12 students and teachers. The main objective of the program is to attract, educate, and motivate a new generation of young men and women to help address the nationwide shortage of trained cybersecurity professionals. The curriculum is flexible and centers on ten cybersecurity first principles. Currently, GenCyber provides cyber camp options for three types of audiences: students, teachers, and a combination of both teachers and students. In 2016, over 120 GenCyber camps were funded, serving 5,000+ students and teachers, and the NSA hopes to double the program in 2017. GenCyber camps can be offered at colleges, universities, public or private school systems, or non-profit institutions. The purpose of this paper is to describe the GenCyber program, provide lessons learned from a successful program implementation, and encourage PI's to plan and implement a GenCyber summer cyber academy.

Keywords
cyber security, education, workforce development

Cover Page Footnote
The work described in this paper was funded by the National Security Agency and National Science Foundation under GenCyber grant project #H98230-16-1-0262. The authors thank the EC-Council for multiple in-kind donations supporting this work.

INTRODUCTION

The GenCyber program is designed to inspire and prepare young Americans in an effort to fill the critical shortage of current and future experts in the constantly evolving field of cybersecurity (Dark and Bianca, 2015; GenCyber Program Director Guide, 2016). The GenCyber program documentation states three main goals: *to increase interest in cybersecurity careers and diversity in the cybersecurity workforce of the Nation, to help all students understand correct and safe online behavior, and to improve teaching methods for delivering cybersecurity content for K-12 curricula* (GenCyber Program Director Guide, 2016). The program introduces basic principles of cybersecurity to enhance the interest of primary and secondary students in future careers in cybersecurity to protect and defend the nation. The GenCyber program sponsors cybersecurity boot camps mainly targeting middle and high school students and their teachers, with a few specialized K-5 programs. The program is designed to attract talented and enthusiastic students to gain a thorough understanding of cybersecurity principles and practices. In addition, it also strives to build a cyber-curriculum and labs earlier in students' education.

The GenCyber program was started in 2014 with eight prototype camps. The program was modeled after a very successful language camp program called StarTalk. The main objective of StarTalk summer camps was to inspire students to study less common but strategic languages such as Mandarin Chinese, Japanese, Arabic, Russian, and Korean. The StarTalk program began in 2007 and has been very successful in meeting its goals. GenCyber is leveraging the success of StarTalk by utilizing many of its principles and practices. In 2015, the number of cyber camps grew to 43 nationwide. As of 2016, the number expanded to 133 camps (31 teacher camps, 82 student camps and 20 combination camps featuring both students and teachers).

The GenCyber program's curriculum focuses on delivering ten cybersecurity first principles: process isolation, domain separation, resource encapsulation, information hiding, minimization, simplicity of design, least privilege, layering, and modularization. Each camp is expected to create opportunities for participants to gain a thorough understanding of cybersecurity principles and practices. The remainder of this paper is organized as follows. Section II presents an overview of GenCyber camps and curriculum. In Section III, we describe the implementation of our GenCyber program from start to finish. Section IV presents the GenCyber learning outcomes and program evaluation methods. Finally, conclusions and lessons learned in the experience of a successful GenCyber program at the University of North Georgia will be presented in Section V.

GENCYBER CAMPS, CURRICULUM AND ROLES

The GenCyber program identifies three types of camps, ten cybersecurity "first participles" to be included in the camp curriculum, and two categories of prominent roles.

GenCyber Camp Types

The GenCyber program is framed to implement three types of camps: student camps, teacher camps, and combination student- teacher camps. Each GenCyber participating entity can apply to host one or more camp types. In addition, the participating institutions or not-for-profit organizations will determine how to organize the training program. In other words, the training program could be offered as residential, commuter, or online.

The curriculum and the evaluation criteria are roughly the same for all camp types. For instance, the cybersecurity first principles are central to GenCyber curriculum design at all three levels. In addition, the evaluation criteria for all three cyber camp types requires participants to answer similar questions such as whether a program meets their expectations, which aspects of the program they like best, and how to improve the program. Some questions cater to specific aspects of the individual types of programs; for example, participants who attend a residential program receive additional questions inquiring about their out-of-class experiences (Dark and Bianca, 2015; GenCyber Program Director Guide, 2016).

The program office personnel noted in the Spring GenCyber Meeting (2016) that they value a mix of different types of programs: from highly technical to beginner programs, residential and day-camp options, with program lengths ranging from a few days to several weeks.

One constant across all GenCyber programs, though, is an emphasis on hands-on, active learning and sound pedagogical practices. Successful GenCyber grant proposals must demonstrate both the intent and the capability to provide engaging, long-lasting, and substantial learning experiences to improve cybersecurity awareness, understanding and/or proficiency among diverse participants. Program materials cite Bloom's taxonomy (Bloom, 1994), authentic assessment, whole-group vs. small-group lesson design and flexible groupings, cognitive scaffolding, cooperative learning, Marzano's six-step vocabulary (Marzano, 2004), multi-modal learning (Moreno & Mayer, 2007), and a variety of other pedagogical techniques and considerations.

Furthermore, the GenCyber site visit and final program evaluation assess the use of these practices. A successful GenCyber program will focus on learning outcomes using a variety of instructional approaches.

GenCyber Curriculum

The GenCyber program defines ten first principles of cybersecurity (Dark and Bianca, 2015; GenCyber Program Director Guide, 2016). **Domain Separation** is a mechanism to protect the functionality (e.g, operating system vs. user apps) data (e.g., testing data vs. operational data) tasks (development vs. maintenance) or region (e.g, US vs. Cuba) from interfering with each other. It is extremely important in enforcing security and protection. **Process Isolation** enables systems to execute on the same platform without interfering with one another. From the computer scientist's point of view, a process is a program in execution. Isolating a process ensures correct operation, security, and protection. **Resource Encapsulation** enables manipulation of resources only as intended by the resource owners by preventing unauthorized access. On the other hand, **Least Privilege** is a strategy to assign the minimum but sufficient power to get a job done. It is mainly implemented in user roles in managing system resources to ensure correct operation, security, and protection.

Layering is a mechanism to build multiple levels of defense to ensure resilience from attack. From the computer security viewpoint, the goal of **Abstraction** is to remove any clutter from a system that can distract and possibly be used in an incorrect or malicious manner. **Information Hiding** is the mechanism to prevent certain features from being available to the pubic. For instance, Information hiding enforces secure coding by preventing programmers' to expose only the necessary functions to the external applications (users). On the other hand, from computer science point of view, **Modularity** is a design concept that emphasizes the principles of divide and conquer by breaking up complex problems into something more manageable components (modules). It enhances interoperability, ease of maintenance, security, and protection. Similarly, the concept of **Simplicity of Design** enables us to better understand the functionalities of the system by minimizing unnecessary details to accomplish reliability and security. Lastly, from a cybersecurity point of view, the goal of **Minimization** is to reduce the number of attack vectors using various ways such as turning off unused ports and unnecessary features.

Overall, the first principles of cybersecurity are designated as the fundamental concepts in any GenCyber curriculum. A solid understanding of the first principles of cybersecurity is important to produce talented individuals for cybersecurity industry and government.

GenCyber Roles

GenCyber roles can be roughly categorized into the Site Visit Team and Camp Representative roles. The site visit team include the following members: **Team Leader**, **Site Visitors**, and **Observers**. The team leader is a person who *"works most closely with the program and leads the site visit team"*. The site visors are those individuals "*who offer their cybersecurity and/or pedagogical expertise to the site visit team".* On the other hand, observers are individuals *"who want to learn more about the program but do not contribute to the site visit report* "

The GenCyber camp team roles include at least the **Program Director** and the **Lead Instructor**. According to (Dark and Bianca, 2015; GenCyber Program Director Guide, 2016), *"the Program Director is the primary POC [point of contact] for the GenCyber program. The success of the GenCyber program is reliant upon open communication between the Program Director and the Team Leader."* Similarly, the lead instructor is a person who is responsible for delivering the course content to the participants. In some cases, the Program director can play both roles. Overall, the success of a particular GenCyber camp depends on the collaborative work of the stakeholders, led by the roles specified above.

IMPLEMENTING THE GENCYBER PROGRAM

The narrative in this section will focus on our institution's approach to implementing a successful GenCyber grant application and educational program in the form of the National Cyber Warrior Academy, with observations on the applicability of this approach in developing other successful programs.

Campus Coordination

Perhaps the most crucial component in developing a successful GenCyber grant application is the coordination across all the campus units that will be involved. Two months before the grant call-for-proposals (CFP), our project team began meeting with both functional and leadership representatives in academic affairs, student affairs, military programs, IT, grants and contracts, continuing education, campus housing, student health services, university relations, campus police, and more.

The three most important partnerships outside of the core grant-writing team were with IT, the Corps of Cadets, and a sister program, the Federal Service Language Academy. IT supported the highly specialized lab imaging, network and local computer accounts, wireless access, a separately segmented network with its own dedicated firewall, learning management system support, and more, and they provided several highly qualified guest speakers with operational roles in networking and information security.

The Commandant's staff and Corps of Cadets provided virtually all logistical support thanks to their experience piloting similar summer programs for high-school students. The Commandant's staff interfaced with student housing, health services, recreational sports, continuing education, campus police all the way to securing transportation for the field trip.

We based our program on a sister program, the Federal Service Language Academy (FSLA). FSLA is a three-week, residential, intensive and immersive foreign language training program with a successful six-year track record at UNG. The FSLA team shared operational plans, daily schedules, waiver and release forms, application packets, and more. This collaboration was key in making our program a manageable pilot with very few staff resources allocated.

Our guidance based on this effort is to seek out prior successful summer programs within your organization, and build on a model that works for your particular institution and service area.

Program and Grant Development

Using the residential, intensive FSLA as a model, we developed an instructional proposal for a two-week residential program based on the Certified Ethical Hacker (CEH) curriculum. We chose the CEH materials because of the emphasis on hands-on lab activities, and due to the instructors' familiarity with the subject. We developed supplemental instruction for cyber basics and introductory Linux, as well as Windows systems administration. In addition, we planned evening activities involving small, programmable drones, robots, and 3D printing.

We made use of institutional, military, and industry contacts in securing guest speakers from the FBI, Navy, Army, National Guard, Lockheed Martin, NASA, and several CS faculty and IT staff within the university.

More complete information on the specifics of the academy's format follow in Section below, but our highly technical, hands-on approach, combined with our rural, impoverished, and ethnically diverse service area, made for a winning proposal.

Recruitment

Recruitment took three main forms: printed brochures mailed to 212 high school principals in the university's 32-county service area, email sent to over 2, 000 high school advisement counselors and ROTC instructors in the southeast region, and a program web site and press releases from institutional university relations staff disseminated electronically.

The associate vice president for military programs at UNG sent a letter on university stationery to all 212 high school principals to accompany the stack of printed brochures for the National Cyber Warrior Academy sent to each school.

The email campaign consisted of an initial notification and regular update communications, and the web press releases were picked up by several local newspapers.

Due to a delay in funding notification for our program, we had just about 30 days (from April 20 to May 20) to recruit for the 40 slots in our program. We did not track the individual results from each of the printed, email, and web recruitment strategies, but we received 137 applications for the 40 seats in our pilot GenCyber program. The majority of the applications received were from in-state applicants, primarily in the university's traditional 32-county service area, but a number of out-of-area and out-of-state students also applied.

Selection

The program staff reviewed all 137 applications received and ranked the applications based on merit: by grade point average (GPA), students' self-reported computer interest as demonstrated by a written essay, and student experience with computing or involvement in extra-curricular computing activities (programming, robotics, or cyber competition teams or related clubs). Due to the university's emphasis on global engagement and strategic languages, priority consideration was given to students with experience or proficiency in a Department of Defense (DOD) strategic language, including Arabic, Farsi, Japanese, Korean, Russian or Mandarin Chinese.

The 40 top applicants were selected in merit-ranked order, with 13 alternates selected in case any students declined the invitation to attend or were unable to participate for any reason. Acceptance letters were sent via email and via postal mail to the 40 top applicants. Alternate/waitlist email notifications were sent to the 13 students selected as alternates, and non-select emails with an invitation to apply to a future program were sent to the remaining 84 applicants.

Of the 40 selected applicants, 37 accepted and sent in their information packets, and three alternates filled the remaining three slots (by gender, to maintain dorm assignments: two females and one male).

The final participants were both highly talented, with an average weighted GPA above 3.8, and highly diverse, with 24 males and 16 females (60% male, 40% female), 22 students who self-identified as Caucasian and 18 students from minority ethnic groups (55% Caucasian, 45% minority).

Staffing

Two faculty from the department of computer science and information systems served as the Program Director and the Lead Instructor for the program, with support from the office of the Associate Vice President for Military Programs. One undergraduate student intern served as the program coordinator, and five undergraduate cadets served as the cadet mentors for the program, each assigned to eight (8) program participants, by gender.

The two participating faculty were supported by the university in completing their CEH certification training before the grant program began, and the grant provided funding for CEI (certified EC-Council instructor) training and certification for both instructors, as well as additional training support and travel to two required GenCyber meetings.

The five cadet mentors (two female and three male cadets) each received the full CEH version 9 curriculum materials. Cadet mentors were selected based on instructor or assistant commandant's recommendation, interview, and qualifications. All five cadet mentors have expressed interest in returning next summer to serve as lead mentors for multiple GenCyber programs if funded.

The Two-Week, Residential Program

UNG's National Cyber Warrior Academy (NCWA) GenCyber program began with parents dropping off students Sunday afternoon, June 19 (University of North Georgia, 2016). Out-of-state students were picked up at the airport by two of the cadet mentors. Parents signed various release forms, including consent to participate in the IRB-approved research study, and students were given network account information and assistance logging in to the UNG network.

Each day of instruction, students participated in physical recreation activities before breakfast, not at the level of physical readiness training (PRT) for our Corps of Cadets, but enough to get their blood flowing and prepare their minds and bodies for intensive cyber training all day long. Class began at 9 AM, with lunch from 12-1 PM, lab instruction from 1-5 PM, followed by dinner and 2-3 hours of planned evening activities, including guest speakers and group activities.

Some of the group activities included: drone programming, Sphero robot activities, car hacking, 3D printing, capture-the-flag and NAO robotics.

The primary curriculum for the program consisted of the EC-Council's Certified Ethical Hacker (CEH) training material, specifically, the hands-on labs. The CEH curriculum consists of 18 modules, from hacking individual operating systems to web servers to mobile devices, and from cryptography to cloud computing to social engineering. The core focus of CEH is to look for weaknesses and vulnerabilities to assess the security of target systems [4]. Ethical hacking emphasizes systems hardening and defense, as well as ethical computing principles, starting with always having explicit, written permission before conducting any vulnerability testing.

The CEH lab manual includes over 700 pages of step-by-step security and vulnerability testing labs, with dozens of additional lab activities available through the EC-Council web portal. Both instructors in the NCWA program held the CEH credential, and the convenience of having industry-level certification lab materials prepared in advance was attractive given the intensive nature of the two-week program.

A field trip to Georgia Tech Research Institute's (GTRI) security operations center (SOC) in Atlanta on the Saturday between the two weeks of instruction reinforced the classroom and hands-on labs. Students were able to see real-time and aggregated information across 10 60-inch monitors in the unclassified level of GTRI's SOC.

Team-building activities were woven throughout the program, from typical ice-breaker activities to recreational activities like ultimate Frisbee to the capture-the-flag challenges.

An early afternoon graduation ceremony followed a simulated CEH certification exam and lunch on the last day, and all parents were invited to attend. Students received a National Cyber Warrior Academy certificate featuring the seals of the NSA, NSF, and the university, from the template supplied by the GenCyber program office.

GENCYBER PROGRAM OUTCOMES AND EVALUATION CRITERIA

Like any NSF-supported grant program, significant emphasis is placed on program outcomes and evaluation. Program evaluation took place across five dimensions: a site visit by an NSA/GenCyber evaluation team; administration of a 3-hour simulated CEH certification exam; the GenCyber Student Survey administered the last day of the program; an institutional review board (IRB)-approved research questionnaire; and the university's internal after-action review and required GenCyber Final Report.

NSA/GenCyber Site Visit Team Report

The GenCyber program requires a site visit for every funded GenCyber project, usually on the middle day of instruction (Wednesday for a one-week camp, Friday of the first week for two-week programs, etc.). The purpose of the site visit is to serve as a formative evaluation, analyzing learning materials, teacher effectiveness, and so on. The spirit of the evaluation is to facilitate and generate best practices to enhance individual camps and the program as a whole. The site visit team includes educators and an NSA representative.

The site visit team observes one full day of instruction, interviews participants as well as instructors and staff, and provides an on-site briefing in addition to a site visit report. In the exit briefing, both the educators and the NSA staff provided constructive feedback to enhance the program that we were able to act upon to improve the second week of instruction. As one example, the site visit team noted that students wanted to collaborate in groups that were not separated by gender. Our original team groupings and mentor assignments were based on dorm assignment, as each suite accommodates 8 students, and suites were assigned by gender. Armed with this information, we were able to change the format of the capture-the-flag (CTF) exercises the second week to accommodate student teams composed of two females and three males. We received positive feedback from the students about these changes, both the smaller group sizes and the opportunity to work with both male and female cohort members.

The site team's written report is delivered shortly after the program ends, and contains a more comprehensive evaluation of the strengths and opportunities for improvement in future years. Among the strengths noted in the report for our program were verbal questioning techniques of the instructors, flexibility in adjusting curriculum based on participant comprehension, effective use of hands-on technology, and so on. Opportunities to improve that were noted included having students do more independent research during exercises, using a more collaborative arrangement of the student workspaces (instead of the traditional college lecture rows), and injecting enrichment activities like the drone programming and robotics exercises into the instructional day to break up the long afternoon stretch of labs and lecture.

The on-site briefing and the written report were instrumental in improving both the current project and future academy plans, and the site visit team was very encouraging and supportive throughout.

Simulated CEH Certification Exam

On the last half-day of the program, Friday, July 1, a 3-hour CEH practice exam of 100 questions was administered, in which 9 students (22.5%) scored high enough to pass the CEH certification standard. Thirty-two students (80%) scored within 20 points of passing the certification standard on the simulated exam.

GenCyber Student Survey

The GenCyber program office provided a link to a 23-question exit survey that each student completed the final morning of the academy, before their simulated certification exam. The same survey is used across all 102 student camps and combination student-teacher camps.

Questions included open-ended statements, like "My favorite thing about this camp was ___" and "The camp would be better if ___", demographic questions (gender, ethnicity, and traditional Likert-scale survey questions about cybersecurity proficiency, career interest, and the like.

Perhaps most notably, the number of students who Strongly Agreed with the statement "Before this camp I was thinking about a career in cybersecurity" increased from 17.95% to 46.15% who Strongly Agreed with "This camp has made me more likely to pursue a career in cybersecurity", an increase of 257%. Further, 77% either Agreed or Strongly Agreed that they are more likely to pursue a career in cybersecurity based on their experiences in the program. Somewhat predictably, 95% rated themselves higher on cybersecurity proficiency, knowledge, and ability to explain why cybersecurity is important than when they began the program.

IRB-Approved Research Questionnaire

The authors designed a research study to evaluate the impact of the GenCyber program on students' future career paths. The research identifies the following two questions: would participating in the GenCyber summer program impact K-12 students' interest in future STEM careers; and, would participating in the GenCyber summer program minimize students' gender bias toward future STEM careers? The experimental data was collected using pre-training and post-training surveys. The analysis examines different categories via mixed factorial design. Each design includes gender as the between-subject design. Together with gender, four categories of future career interest were identified and investigated. The results of this research will be published separately, and we plan to apply the same research in future years.

AAR and GenCyber Final Report

The Commandant's staff and mentors from the Corps of Cadets provided an after-action review (AAR) that included information and recommendations across virtually every component of the program, from daily schedules to activities to medical support and discipline. In total, the Commandant's crew has collected over 150 pages of supporting information and documentation for subsequent GenCyber and related programs.

The importance of this disciplined approach to continuous improvement and replicability of the program cannot be overstated. Our GenCyber program owes the lion's share of its success to the Corps and the university's institutional memory; we built many of our materials, from the coordination plan to the student acceptance packets, based on previous successful programs like the Federal Service Language Academy.

The required GenCyber Final Report provided an additional opportunity to capture lessons learned in the days immediately following the conclusion of the cyber academy. The GenCyber program office requires submission of the final report within 3 weeks of the end of each camp. While the short suspense added a small amount of additional stress, the fact that the experience was still fresh on the minds of the faculty and staff helped make it a more meaningful and substantive review of the program from an internal perspective.

Thanks in part to the observations we made in our final report, our faculty have been asked to speak at the upcoming Fall GenCyber Meeting about the novel use of drones, 3D printers, and robots in the National Cyber Warrior Academy, as well as on the OpenGarages.org (Open Garages 2016) car-hacking materials we used in the program.

CONCLUSIONS

In addition to successful program outcomes noted across the multiple evaluations in the previous section, a number of benefits were noted anecdotally. A number of students indicated they are now interested in federal or military service, and most are interested in cyber in college and as a career option. Over half of participants stated they would be interested in an advanced camp next year, especially one focused on computer and network forensics. In addition, several students stated a desire to start cyber competition teams in their high schools (CyberPatriot, MITRE, etc.).

The collaboration among so many units of the university, including academic affairs, student affairs, the Corps of Cadets, university relations, advancement, business & finance, grants & contracts, and especially our information technology (IT) staff was both a necessary component of and a fortuitous outcome from a successful GenCyber summer program.

Finally, the decision to host a GenCyber summer program is an institutional commitment, not just a departmental one, perhaps more so than in any comparable federal grant program of this scale. Healthy internal communication, strong administrative support, and substantial participation from representatives across the institution were both prerequisites for a successful program and were reinforced through the execution of the program. That level of commitment, combined with support from the GenCyber program office and the wisdom gleaned from past GenCyber projects, resulted in a potentially life-changing experience for 40 high school students and possible future cyber professionals.

REFERENCES

Dark, M. & McNair, B. (2015). *GenCyber Evaluation Report*

National Security Agency GenCyber (2016). *Program Director Guide*

National Security Agency GenCyber (2016). *GenCyber progam*. Retrieved from page: https://www.nsa.gov/resources/students/summer-camps/gencyber/ (accessed, Sep 2016)

GenCyber (2016). *Inspiring the next generation of cyber stars.* Retrieved from page: https://www.gen-cyber.com/proposals/ (accessed, Sep 2016)

Certified Ethical Hacking Certification. (2016). Retrieved from page: https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/ (accessed, Sep 2016)

Bloom, B. S. (1964). *Taxonomy of educational objectives* (Vol. 2). New York: Longmans, Green.

Marzano, R. J. (2004). *Building background knowledge for academic achievement*: Research on what works in schools. Alexandria, VA: ASCD.

Moreno, R., & Mayer, R. (2007). *Interactive multimodal learning environments*: Special issue on interactive learning environments: Contemporary issues and trends. Educational Psychology Review, 19(3), 309-326. doi:10.1007/s10648-007-9047-2

GenCyber Spring Meeting (2016), San Francisco, May 14-15.

University of North Georgia. (2016). Retrieved from page: http://ung.edu/cyber-operations-education/national-cyber-warrior-academy.php (accessed, Sep 2016)

Open Garages (2016). Retrieved from page https://opengarages.org (accessed, Sep 2016)