Cyber Security and Privacy Research Institute

THE GEORGE WASHINGTON UNIVERSITY

Exploring Ways to Give Engineering Cyber Security Students a Stronger Policy and Management Perspective

Costis Toregas
Lance J. Hoffman
Rachelle Heller

April 20, 2016
Report GW-CSPRI-2016-01

Exploring Ways to Give Engineering Cyber Security Students a Stronger Policy and Management Perspective

Costis Toregas The George Washington University - toregas1@gwu.edu
Lance Hoffman, The George Washington University - lanceh@gwu.edu
Rachelle Heller The George Washington University- sheller@gwu.edu

Abstract:
This paper describes lessons learned teaching cybersecurity classes in a cross-disciplinary cybersecurity scholarship program at the George Washington University that has been successfully completed by over six dozen students in ten majors. The majority of the students have obtained master's degrees in computer science, but almost half have been from other disciplines, with a significant number of undergraduates, a couple of community college transfer students, and a few doctoral students.

A required seminar in Cybersecurity and Governance that mixes the students from all majors for common projects and events is described in detail. Cooperation among internal and external academic institutions is discussed. We conclude with some predictions for future directions in cybersecurity education and comments that could be generalized for other educational programs with students from a multitude of academic discipline backgrounds.

Note: Support for this work was partially provided by the National Science Foundation CyberCorps Scholarship for Service (SFS) program under Award no. 1433425 Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

Introduction: The Need for an Educated Cybersecurity Corps

"It's now clear this cyber threat is one of the most serious economic and national security challenges we face as a nation…[w]e're not as prepared as we should be, as a government or as a country."

-President Barack Obama, May 2009

The need for educated personnel in the cyber security workforce is critical to the nation's security. President Obama has identified cyber-security as one of the most serious economic and national security challenges we face as a nation, but one that we as a government or as a country are not adequately prepared to counter (The White House, 2015). He noted that it is the people with the right knowledge, skills, and abilities to implement those technologies who will determine success. However, there are not enough cyber-security experts currently within the Federal Government or private sector, and he called for a national strategy not unlike the efforts following the Sputnik challenge of the late 1950s to establish a strong cyber-security workforce. In 2015 alone, for example, the US Cyber Command called for hiring over 6,000 individuals with strong, leadership skills in cyber-security.

The Scholarship for Service (SFS) program is a successful program to fill this need in the government space (Booz Allen Hamilton, 2015). One of the most successful feeder institutions into this pipeline, educating and sending computer security experts into government service for over a decade, is The George Washington University (GW) and its successful Scholarship for Service program. What defines this SFS program is that all scholarship recipients must work after graduation for a Federal, State, Local, or Tribal Government organization in a position related to cybersecurity for a period equal to the length of the scholarship.

The GW multidisciplinary academic program in cybersecurity, a Signature Seminar (described below) that has our students meet numerous government and private sector cyber experts, and our location at the center of the federal government cyber security activities make the program attractive for students and the government. Our almost-perfect placement rate for SFS CyberCorps graduates reflects a level of excellence, as does our success in recruiting and graduating much higher than average numbers of women when compared with nationwide engineering placement rates. This paper will underline some success factors and draw conclusions that might help other programs that might like to

strengthen cyber security through academic pipeline development centered in engineering schools, and well as educators who are leading other multidisciplinary programs.

The Scholarship for Service Program

Admissions Process

Every year, scholarships are widely advertised directing applicants to our website (https://www.seas.gwu.edu/cybercorps/) with detailed information on the program: information on how to apply, information for specific audiences, and points of contact for students wishing to major in various departments, all related to cybersecurity, practical information for current GW CyberCorps students and for government employers interested in hiring our students. Applications include official transcript, two letters of recommendation that describe the applicant's ability to identify, analyze, and solve problems and the applicant's knowledge of information technology and information security. Each applicant also submits a short written statement on why they should be selected for a scholarship. All applications are read by a team of educators representing both a cybersecurity focus as well as a departmental focus. Follow up interviews are arranged for the candidate with the highest potential for the scholarship.

A single Seminar Blending Students from Several Disciplines

GW requires all CyberCorps scholarship students to complete Computer Science 6534, Cybersecurity and Governance, for each semester they are supported by the SFS program. This is GW's distinctive Signature Seminar that underlies its success in educating and placing Cyber Corps graduates in federal agencies. Students' participation in this course begins the process of building working relationships with current government leaders as well as with SFS colleagues that become a very important success factor in their future careers. It is the unifying and reinforcing experience that prepares students with the knowledge, perspective, and expertise to perform competently in their future government positions, repay the federal government its hefty investment in their education, and serve their country. The course readies students to be able to contribute to a government cybersecurity environment on their first day in the federal workforce.

Unique in the GW approach is that we take students from a variety of disciplines and with a variety of skill sets, and insure that they all have grounding in current federal regulations, processes, and challenges, as well as in the basic technologies necessary for leaders in cybersecurity. At a dedicated weekly time during both academic years of the program, for a full twelve credit hours of instruction (only three are counted for the student's degree), the course brings our CyberCorps students together and guides them through a curriculum designed to give them a thorough understanding of the roles and responsibilities of the federal government

in cybersecurity(their intended career and required placement for the SFS program), an overview of the technical aspects of cybersecurity, and familiarity with the Federal Information Security Management Act (FISMA) and other cyber legislation currently proposed and under discussion. The course grooms GW's CyberCorps students to succeed by developing their technical, analytical, managerial, presentation, and writing skills with regard to cybersecurity issues. The course also provides a baseline of relevant federal policies and mandates and gives an informed picture of federal government roles, responsibilities, and processes in cyber security. It reviews basics of the U.S. Constitution and law and steeps students in the CSIA elements necessary to planning federal computer systems within a framework that is cognizant of privacy, cost, risk, civil liberties, and public acceptance. It routinely discusses contemporaneous speeches, reports, guides and laws that are shaping how the government and the private sector and nonprofits deal with cybersecurity issues.

The class is usually taught by former SFS graduates now in the federal government, young enough to relate to the students but experienced enough to know about the ins and outs of working for the government. They often bring in other federal government employees and other cybersecurity practitioners as guest lecturers. The course content is designed to be contemporary with ongoing federal policy developments and is able to present new proposed laws and regulations through speakers who are creating, launching, or currently reacting to such legislation. The course also provides students with a view of likely upcoming changes that they may face in their first years in the federal workforce. Students who complete the course emerge with an appreciation of government-related issues obtained from up-to-date lectures by internationally recognized specialists in cybersecurity and by guest lecturers who daily address the technical, administrative, and policy challenges of cybersecurity in government systems and large enterprises.

The students also study current federal policy and compliance programs by examining the FISMA process and the related set of security controls. They engage in the entire Security Certification and Accreditation, audit, and System Security Plan processes. The course begins each fall with second-year students presenting their federal agency summer internship experiences to the cohort of their peers and new first-year SFS students. Then, each week, the instructor assigns different students to discuss a current attack affecting federal systems. In examining each attack, students study the attack method used, system vulnerabilities, and mitigation strategies that correspond to FISMA controls that would have prevented the attack. These student presentations lead to lively and informative discussions among the students, instructor, and guest lecturers who are able to add key insights, knowledge and observations. In addition, the process effectively builds esprit de corps and public speaking skills, both essential to the development of these future government cadres.

More experienced students develop a System Security Plan for a fictitious government system that is iteratively critiqued and refined through interaction of both the instructor and student. By the end of students' (typically) two years of participation in the course, they are well-versed in the use of government processes to analyze computer systems, perform risk assessments and document systems' FISMA compliance. As a result of these exercises, one student reported a sense of "standing out from the veteran employees" and subsequently received a job offer during his summer internship.

Almost every week, an invited government official or industry expert also speaks, reinforcing concepts, sharing insights, and meeting informally with scholarship students. These speakers present a wealth of up to date, practical government- and policy-related material often not readily accessible to students and instructors in cybersecurity classes. Many of our speakers give us permission to video-record their talks, which are then used for both traditional and online future GW cybersecurity classes. Many of the talks are already available on the CSPRI channel on YouTube. (CSPRI YouTube 2014)

Finally, the course provides students with valuable informal networking and contacts. Personal interactions with speakers, program alumni, and instructors have led to internships and jobs. Students and graduates establish and rely on these personal and professional friendships and contacts to serve as sounding boards for work-related advice and to provide assistance in their searches for their next positions.

In addition to the speakers, students discuss assigned readings, current affairs and future trends, report on events at any conferences they attended, and discuss career skills such as marketing their ideas internally and externally, finding internships and jobs, and the ins and outs of security clearances.

The Signature Seminar CSci 6534 is now presented both in traditional format and, due to popular demand from non-SFS students, also as an online course with one in-person class meeting during the term. This online course is made available to non-SFS students and to also to any SFS students with schedule conflicts that prevent them from taking the in-person class.

Lessons Learned

During August and September 2015, online surveys and a focus group were used to assess the GW SFS program. Specifically, three surveys were developed and launched to gather information from the following stakeholders: 1) SFS Application Reviewers, 2) GW Faculty who taught SFS classes, and 3) current students and alumni of the GW SFS program. In addition, current students who were enrolled in the Seminar class participated in a Focus Group in which they were able to provide detailed responses to questions related to their experience with the program.

Overall, faculty reported that SFS students in their classes demonstrate a higher level of motivation, commitment to cyber-security, engagement within the class, and have a stronger cyber-security knowledge base prior to taking their classes than students who were not participating in the SFS program. They also report that SFS students generally have either higher or equal earned grades and critical thinking skills than their non-SFS peers. We attribute this to the detailed screening process used by the scholarship program that is described above.

GW SFS Student/Alumni Survey and Focus Group

To best assess the experiences of current and past GW CyberCorps SFS students, two sources of data were used. First, all current students and alumni of the SFS program were invited to participate in a short online survey. Of the 76 current students and Program alumni who were invited to participate, 16 (a 21% response rate) usable surveys were completed. Second, students who were enrolled in the Signature Seminar took part in a focus group. The results of the survey and focus group data are presented below.

Student Participant Demographics

Focus group

Six currently enrolled GW SFS students participated in the focus group on September 3, 2015. Four of the students were male, two were female; three were returning students and three were students who were new to the GW SFS program.

Survey

Seventy-six current SFS students and alumni were invited via email to participate in an online questionnaire between August 19 and September 4, 2015. Sixteen participants completed the survey. Twelve of the respondents were graduates of the program and four were 2nd year students (see Table 1). Twenty-five percent of the respondents were female (N=4) and 69% (N=11) were male. Recipients were asked to select the race/ethnicity category/categories that best represent them, therefore more than one race/ethnicity group could be selected. The majority of the respondents identified themselves as Caucasian/White (N=10), however six race/ethnicity categories were selected at least once by the participants, and one participant declined to answer.

Table 1. Student Survey: GW SFS Student Participants by Year in Program

GW SFS Student Standing	Alumni		2nd year		Total	
	N	%	N	%	N	%
Year in the GW SFS program	12	75.0%	4	25.0%	16	100.0%

Why Do These Good Students Apply?

During the focus group, participants were asked to discuss their motivation(s) for applying to the program. Five students provided responses to the questions "What motivated you to apply to the SFS program?" The participants each offered multiple reasons that contributed to their motivation to apply to the GW SFS program.

From the focus group responses (see Table 2), three primary areas emerged from a number of participants as associated with their motivation to apply to the program: CSPRI web site (N=5), flyers (N=3), financial assistance (N=3), recommendation of a non-GW professor (N=2), and alignment with employment goals (N=2). Survey data revealed some overlap with the focus group information, but included important differences as well. Specifically, the majority of the survey participants indicated that they were motivated to apply to the GW SFS program based on their interest in cyber-security (N=10), followed closely by the program's offer of financial assistance (N=9), and because the program aligned well with their employment goals (N=8).

Table 2. Student Survey: Motivation for Applying to SFS

Primary Motivation for Applying to SFS	**Focus Group N (%)**	**Survey N (%)**
Flyers on campus (in halls or provided as part of an informational session)	3 (60%)	0
Financial assistance	3 (60%)	9 (56%)
Professor recommendation (from non-GW college/university)	2 (40%)	0
Program aligned with employment interests (Federal job)	2 (40%)	8 (50%)
Quality of the program/Great opportunity	1 (20%)	1 (6%)
Interest in cyber-security	1 (20%)	10 (63%)
Secondary Motivation for Applying to SFS		
Conversation(s) with a Principal Investigator	2 (40%)	N/A
CSPRI web site research	5 (100%)	N/A
OPM SFS web site research	2 (40%)	N/A

Focus group participants noted that the application process was easy to navigate, but the wait for information about funding from the SFS program posed some problems (N=4) in terms of deciding to accept the GW offer and making travel plans.

More than half of focus group respondents (60%) and survey participants (56%) indicated that the financial assistance offered through the SFS program was associated with their motivation to apply to the program. However, while the focus group was more keyed into the flyers on campus, survey participants were more likely to report an interest in cyber-security and/or alignment with employment goals as a motivation for program admittance.

Focus group and survey participants were also asked to provide feedback on their experience with the GW SFS program. They were asked to compare their motivation to learn in SFS classes with their non-SFS classes, as well as the cyber-related skills they learned as part of their SFS curricula. In addition, focus

group students were asked to determine which program activities benefitted their overall cyber-security knowledge and the extent to which they saw benefits related to the program's commitment to diversity.

Focus group participants explained that compared to their non-SFS classes, courses for the SFS program offer early insight into cyber-security before they're brought up in other classes (N=3). They also indicated that they are more interested in the SFS classes, especially the research project (N=2). In addition, three of the focus group participants noted that their ability to apply knowledge learned in SFS classes was valuable. For instance, one student noted: I work in a bubble so I was surprised when SFS topics came up at work. I could explain it to co-workers."

Several benefits related to the program were also noted when asked: What kind of cyber-related skills and knowledge have you gained as a participant in the program? Three focus group members responded with a number of responses. All three explained that their cohort, guest speakers, and networking were critical to learning the cyber-security skills that are needed in the program and to obtain a government job in cyber. Specifically, they noted that they were able to apply cyber skills specifically to potential government jobs, skills are used for the SFS research project. They also included the SFS cohort and networking as important in their pursuit of cyber-related skills and knowledge. Specifically, one student noted, the cohort is important as it provides networking, other students, and a Google hangout group for assistance from peers.
Guest speakers were also discussed as important to their cyber-security skills and knowledge building. And, networking was identified as important as well as it related to applying for jobs, knowing the skills that are needed, and navigating the government application process.

In addition the majority of the participants "Strongly Agree/Agree" that the required courses were beneficial as they provided a solid core knowledge of cyber-security (N=14, 93.3%) while also allowing for customization of courses depending on student interest (N=10, 62.5%). Most student survey participants also indicated that they "Strongly Agree/Agree" that the internship provided a useful opportunity for advancing skills, knowledge, and abilities (N=13, 86.7%) and provided a good opportunity for networking (N=13, 86.7%).

Survey participants were also asked to identify the benefits of the SFS program. Of the six response options to the question: Which of the following do you perceive as benefits of the SFS program?, networking was indicated by nearly all participants as a benefit of the program, while the exclusiveness of the small group (N=13) was also highly rated as a benefit. Ten respondents indicated that the professors associated with the program and the guest lecturers were also a benefit of the program.

To further probe the benefits associated with the GW SFS program, survey respondents were also asked: "What aspect of the SFS program do you feel provided you with the BEST information, opportunity, and/or advantage for your career?" Nine respondents provided responded to the question with a number of additional benefits of the program. Table 3 displays the four themes that emerged from the student responses. Networking was the aspect of the program that was noted the most often (N=4) by the participants.

Table 3: Student Survey: Primary Benefit of the SFS Program

Benefits of the SFS Program	**N**
Exposure to CISSP [Certified Information Systems Security Professional] material/specialized training	2
Guest speakers	1
Networking (e.g., with government employees, experts, employers	4
Professor relationships (e.g., mentorship, advice, connections)	2

Beyond the GW PISCES CyberCorps: SFS Program

The SFS program is designed to train students for cyber-related employment in the federal government. As such, it is important to determine the extent to which alumni intend to remain in the government after their initial post-SFS commitment is met. It is also important to determine the extent to which current students consider government employment after they meet their SFS employment commitment post-graduation.

Alumni survey participants were asked: "Do you intend to remain within the federal government after your SFS program commitment is met or seek employment in the private or nonprofit sector?" Of the 12 alumni who completed the question, the majority indicated that they stayed with the government (N=7), while four indicated that they were already in the private sector, and one was undecided about whether s/he would remain in the government.

From the focus group data, many of the participants expected to participate in government occupations as well. When asked: "Do you intend to remain within the federal government or seek employment in the private or non-profit sector?" Three of the five participants who responded to the question noted that working for the government was an option for them. However, they also noted, that if better options were presented to them from the private sector, they would strongly consider a transition.

Respondents also provided a range of areas in which they were planning on working after completing the SFS program. Their responses were varied as the six participants offered several ideas about their future employment areas. Areas of interest included research, programming application, penetration tester, development, wireless network analysis and program language, defense or law enforcement, financial intelligence background, and research on motivation of cyber criminals.

Lessons learned for Cybersecurity Educators in an Engineering Setting

Recruiting students for undergraduate or advanced degrees is challenging in today's marketplace. Students are searching for financial support or expediency through scholarships or community college education. Certainly hosting a well endowed scholarship program provides a base to attract students. However, in a program that brings students from various disciplines (in our case, computing, forensics, policy, business, even law) being able to vet their applications is important. We solved this issue by establishing a cadre of faculty who have come to know and respect the SFS program and are willing to add their voice to the selection process.

Once included in the program, students benefit from the seminar course which focuses on the role of their potential employer (in our case governmental agencies) and identifies how each of these technical and non-technical fields fit together toward a larger mission. The course encourages students to work across disciplines in teams in research projects and on competitions, thereby giving students an insight into how the "real world" looks when working in teams. Moreover, while GW's engineering school has a high representation of women, bringing the various disciplines together provides a diverse team environment.

Finally, networking, as a skill garnered in the seminar, is a life skill from which emerging professionals benefit. It is important to provide students with varied and not-overwhelming opportunities to meet with professionals in their chosen field. Having near peer mentors, in the recent alumni of the program, is effective as a guide to career choices as well as a "safe" interaction in which students can address concerns they might not share with potential employers.

Lessons for multidisciplinary programs

While the GW SFS program is focused on cybersecurity, there are themes that generalize to programs that encompass multiple disciplines: programs in sustainability, policy and the nexus of food, energy and environment being good examples. Bringing students together, providing them with access to working professionals who represent their specific discipline within the larger cosmos of the program area is an important way to legitimize each discipline role. Moreover,

it instills confidence in students that their pathway forward to future learning or career is based on the discipline within the program.

The role of authentic learning has been promoted in educational circles, but in a multidisciplinary program, it gains importance. By reviewing and discussing and using materials and processes from the working professional world, students learn the material and, more importantly, are ready to begin their careers.

Finally, writing, public speaking and critical argument, often called soft skills are important and presenting in them in a realistic fashion heightens their usefulness. In a multidisciplinary program this is even more important as the members of sub-disciplines oft have their own particular vocabulary. Learning to speak, write and persuade across these lines is an important skill.

SUMMARY

It is vital that efforts in cybersecurity education not concentrate exclusively on technical aspects, nor be contained within a single academic discipline. If academic institutions are to provide the much heralded and needed strong and effective workforce, care should be taken to include the policy and human relationship skills essential for leading the cybersecurity efforts of the future. An institution must have a structure that supports cross-disciplinary research and teaching, and incentivizes the starting up of new programs, and those that allow a lot of breadth in their electives. At The George Washington, such is the case. With a successful SFS program in cybersecurity education for well over a decade, and with new programs such as GW's newly-approved Master's of Engineering in Cybersecurity Policy and Compliance and Master's of Cybersecurity in Computer Science, GW is showing the way forward; our strategy can be replicated in other settings, and expected to give strong results.

Bibliography

1. McDuffy and Piotrowski, "The future of Cybersecurity Education" IEEE August 2014
2. Hoffman, Burley and Toregas "Holistically Building the Cybersecurity Workforce" , IEEE Security & Privacy vol. 10, no. 2 (March/April 2012),
3. McGettrick,"Towards Curricular Guidelines for Cybersecurity" Report of a workshop on cyebrsecurity education and training, ACM August 2013
4. Ronald C Dodge, Costis Toregas, Lance Hoffman, *Cybersecurity Workforce Development Directions*, Proceedings of the Sixth International Symposium on Human Aspects of Information Security and Assurance HAISA 2012.