Development of Military Friendly Cybersecurity Courses and Programs

Dr. Jeremy Straub, North Dakota State University

Jeremy Straub is the Associate Director of the NDSU Institute for Cyber Security Education and Research and an Assistant Professor in the Department of Computer Science at the North Dakota State University. He holds a Ph.D. in Scientific Computing, an M.S. and an M.B.A. and has published over 40 journal articles and over 120 full conference papers, in addition to making numerous other conference presentations. Straub's research spans the gauntlet between technology, commercialization and technology policy. In particular, his research has recently focused on cybersecurity topics including intrusion detection and forensics, robotic command and control, aerospace command and 3D printing quality assurance. Straub is a member of Sigma Xi, SPIE, the AIAA and several other technical societies, he has also served as a track or session chair for numerous conferences.

Development of Military Friendly Cybersecurity Courses and Programs

Abstract

The North Dakota State University (NDSU) developed a military-friendly cybersecurity graduate certificate program, options as part of Computer Science and Software Engineering M.S. and Ph.D. degrees, a special recognition as part of a B.S. degree in Computer Science and supporting 'anytime, anywhere' courses. Part of a larger state-wide initiative, NDSU identified a specific goal of making the programs that were developed remotely accessible and, specifically, military accessible. Military members (including active duty and veterans) are seen to be excellent cybersecurity students due to their warfighting background, which can be directly leveraged to provide the appropriate frame of mind for cybersecurity operations, whether from an offensive or defensive perspective. This paper covers on the development of the programs and courses at the departmental level. A key decision that was made early in the process was to make all of the courses equally available, synchronously or asynchronously, to both local and distance students. The programs and courses developed are presented and qualitatively assessed.

1. Introduction

This paper discusses the development of a military-friendly cybersecurity graduate certificate program, options as part of Computer Science and Software Engineering M.S. and Ph.D. degrees, a special recognition as part of a B.S. degree in Computer Science and supporting 'anytime, anywhere' courses at the North Dakota State University (NDSU). The programs and courses were designed to respond to the national need for significantly more individuals with cybersecurity skills to protect government agencies and private sector businesses and other entities alike. Recognizing that individuals with military backgrounds, in most cases, already have skills and abilities directly supporting their success in the field, a specific effort was made to make the courses and programs military friendly. With NDSU already designated a Military Friendly School by Victory Media's G.I. Jobs Magazine, core policies and procedures were already in place.

This paper, thus, focuses on the development of the programs and courses at the departmental level. A key decision that was made early in the process was to make all of the courses equally available, synchronously or asynchronously, to both local and distance students. To support this, all of the newly developed cybersecurity courses are taught in a distance enabled classroom and combine pre-recorded videos, in class activities and lectures (which distance students can complete on their on schedule or connect to in real time using video conferencing software), online assessments and bona fide course-integrated research and development projects. Where relevant certifications existed (and are available to be taken by students), the courses were mapped to the objectives for these certifications. Courses have targeted EC Council's Certified Ethical Hacker and Certified Hacking Forensic Investigator certifications and CompTIA's Security+ certification.

The graduate certificate is designed to be able to be completed in conjunction with a graduate degree program or on a stand-alone basis. The certificate is designed, in particular, to help

individuals with a technical background gain the skills required to successfully enter the cybersecurity field. The certificate program requires a sequence of four graduate level courses.

The options as part of the M.S. and Ph.D. programs allow students to gain particular cybersecurity skills while completing their graduate degree programs. All of the options require a sequence of three courses in cybersecurity.

The undergraduate recognition provides a similar benefit to undergraduate students. Like the graduate options, it also requires students to take a specific sequence of three courses. Undergraduate students also benefit from cybersecurity relevant coursework that is otherwise required as part of the B.S. degree in Computer Science.

Each of the aforementioned programs is described in detail and design decisions that have been made to support military students will be highlighted and qualitatively evaluated. In addition to the discussion of the program-level design, military friendly course design decisions will also be discussed. These include key decisions to distance-enable the courses, using individuals with military experience to help deliver certain courses and the use of student assistants to aid the learning of students enrolled in the cybersecurity courses. The paper concludes with a discussion of planned future expansion.

2. Background

Merisotis contends that veterans are "the most nontraditional of all nontraditional students," separated by age, military cultural immersion, experience and other factors from students entering college directly from high school completion [1]. Active duty military members share all of these characteristics; however, they may also be connecting from a different time zone or even a battlefield or base in hostile territory. With 840,000 military enrolments and $445 million in expenditures (in 2006), there is significant interest, by universities, in targeting a military student base [2]. To support these students Minnis says that military cultural training, outreach and services related to careers, counseling, health, disabilities, financial aid and business concerns are needed [3]. Many veteran friendly lists and accreditations consider these services, but fail to consider whether a campus has a "climate geared toward developing student-veterans' holistic success," which Minnis [4] argues is also critical.

Successful veteran serving colleges Smith University and Metropolitan College listened to their veteran students and offered family services, English enhancement courses and accelerated courses for adult learners [5]. They also created a veteran symposium, a dedicated space for veterans and a veteran student organization, along with creating ways for veterans to self-identify to other veterans at these schools. Western Michigan University also implemented these strategies, crating an office to serve active military and veterans, dedicating an individual in the campus's registrar's office to securing their benefits and creating a student organization with a dedicated location on campus [6]. They also implemented veteran-friendly financial and academic policies, in particular defining policies to enable deployed students to continue or pause their courses. The University of West Florida also created a campus organization for military members and veterans, in addition to working with Servicemembers Opportunity Colleges, which facilitates transfer credit between its members [7]. Faculty also attended

seminars and conferences about military culture and worked to create programs that are well suited to distance education students and military members through a special advisory committee and engagement with others on campus and in (or who have served previously in) the military. Dillard and Yu [8] support these strategies and also suggest that a seminar for first-year veterans can aid the transition and student experience. Heineman [9] echoes many of these same suggestions, also suggesting that colleges get veterans engaged in extracurricular activities, develop tracking mechanisms for veterans' progress, retention and other information, and focus on the sustainability of all veteran-supporting activities.

Summerlot, Green and Parker [10] discuss the formation and operations of veterans organizations, noting that successful organizations are veteran-student created and operated; however, they require a suitable campus climate to be successful. These groups can be active in everything from event hosting to lobbying administrators to change problematic policies. Schiavone and Gentry [11] note, however, that veterans success is enhanced through interactions and co-working with those outside their veteran peer group.

The growth of internet-based distance education has enabled education to occur in areas where it was previously not possible. McMurray [12] notes, however, that this also brings with it new problems, including questions of whether educational activities may add stress to an already stressful deployment environment and contribute to a growth in post-traumatic stress disorder cases.

3. NDSU Cybersecurity Courses and Programs

NDSU has implemented six programs or program components related to cybersecurity. These include a department issued recognition, as part of the Bachelor of Science degree, a graduate certificate and a cybersecurity option as part of the department's masters' and doctoral degrees in both computer science and software engineering. All are designed, initially, to be flexible and will be refined over time. Each will now be discussed.

The department issued recognition requires students to take nine credits of cybersecurity coursework, in addition to meeting the other requirements for the Bachelor of Science degree. The department issued recognition can also be issued to those not pursuing Computer Science degrees, in very special cases. The recommended fulfillment of the recognition includes taking CSCI 403 – Defensive Network Security, CSCI 404 – Ethical Hacking and one additional course. Options for this additional course include CSCI 409 – Cybersecurity Law and Policy, CSCI 410 – Computer Crime and Forensics, CSCI 469 – Network Security, CSCI 493 – Undergraduate Research (with an organized cybersecurity focus) or a special topics course focused on cybersecurity. MATH 473 – Cryptology is also accepted. In most cases, the completion of the recognition does not increase the number of credits required for students to graduate, as the recognition can fulfil the computer science upper division electives requirements (which is also 9 credits). Students receive a specialized certificate from the department, upon completion of the recognition requirements.

The Graduate Certificate in Cybersecurity can be completed entirely at NDSU or in partnership with other colleges in the North Dakota University System. It requires students to complete 12

credits of cybersecurity courses. The certificate was developed to be flexible. It can be used as a direct follow up to completing an undergraduate degree, to get and demonstrate more cybersecurity knowledge. Alternately, it can be completed while working towards a graduate degree (M.S. or Ph.D.) or as a way for someone already in the workforce to transition to a cybersecurity-related career. The suggested pathway for completing the certificate is to take CSCI 603 – Defensive Network Security, CSCI 604 – Ethical Hacking, CSCI 609 – Cybersecurity Law and Policy and one additional course. Potential course offerings include CSCI 610 – Computer Crime and Forensics, CSCI 669 – Network Security or a computer science special topics or directed / independent study course with a cybersecurity focus. MATH 673 – Cryptology at NDSU as well as courses including EE 590 – Emerging Threats and Defenses, CSCI 558 – Applied Cryptography and EE 590 – Information Security and Security Practices at system partner schools can also be applied to the program. Upon completion, students receive a certificate from the NDSU Graduate School.

The degree options, as part of M.S. and Ph.D. degrees in both computer science and software engineering require students to complete nine credits of cybersecurity coursework. The requirements mirror the undergraduate department issued recognition. The recommended fulfillment of the recognition includes taking CSCI 603 – Defensive Network Security, CSCI 604 – Ethical Hacking and one additional course. Options for this additional course include CSCI 609 – Cybersecurity Law and Policy, CSCI 610 – Computer Crime and Forensics and CSCI 669 – Network Security or a special topics course focused on cybersecurity. MATH 673 – Cryptology is also accepted. Due to the flexibility of the department's graduate programs, completion of the option does not increase the number of credits required for students to graduate. Completion of the option is noted on the student's transcript along with degree conferral.

All of the courses recommended for the cybersecurity department recognition, certificate and degree options are available both on campus and online. Additionally, many of the optional cybersecurity courses are similarly available online. The B.S. cannot be completed entirely online; however, the graduate certificate is designed to easily support online completion. The M.S. and Ph.D. degrees largely support online completion; however, attendance on campus to take the comprehensive examination and for the defense (for non-coursework option students) is required. The department has, in the past, waived the requirement that these be done in person for students that were unable to visit campus and arranged distance alternatives.

4. Courses and Course Design

In support of the aforementioned programs and program components, several new courses have been designed. These include CSCI 403 – Defensive Network Security, CSCI 404 – Ethical Hacking, CSCI 409 – Cybersecurity Law and Policy and CSCI 410 – Computer Crime and Forensics. Courses on Microsoft Windows and Linux security have been run as special topics courses, previously. In addition, a graduate course on intrusion detection systems has been developed and is currently being offered for the first time under a temporary course number. Courses on malware analysis, social engineering, reverse engineering and steganography are under development.

These courses have a number of common features, which are adapted to the nature and requirements of the particular course, as needed. These include:

- *Distance and technology enabled* – courses are taught in a television studio classroom that facilitates high quality capture of lecture and interactive content. Distance students (or on-campus students that are traveling or otherwise unable to attend class) can also participate live via video conferencing software and a webcam and microphone.
- *Use of outside experts* – courses bring in outside experts, as available. The ethical hacking course has significant instructional participation by an active duty military officer with cyber operations experience. Campus cybersecurity staff, a nationally known forensics consultant and officers from the North Dakota Bureau of Criminal Investigation were brought in as guest speakers for the Computer Crime and Forensics course. Most of these presentations are video-recorded and are available for use in future courses.
- *Pre-recorded lecture content* – key to saving students time and allowing them to access material at the pace best suited to them is the pre-recorded lecture content. This content is recorded live in some cases and using a studio environment in other cases and posted online. All content is now closed-captioned. Content can be viewed and replayed by students. The player also supports different viewing speeds, allowing students to adjust this to suite their needs.
- *Course integrated research and development projects* – students are given hands-on experience in related areas through development projects and other group and individual projects. These develop students' skills and give them something to show to prospective employers, which they can relate to their business needs.
- *Online discussion boards* – most courses have weekly or biweekly discussion boards online, which both distance and on-campus students participate in. This allows distance and on-campus students to interact and learn from each other's respective experiences and knowledge.

5. Military Friendly: Pre-Service, Active Duty and Veterans

NDSU is committed to supporting pre-service and active duty military members and veterans. There are Air Force and Army ROTC units [13], [14] on campus to prepare students for military careers. Distance courses cater to military members worldwide, while on-campus courses are available for military members in the region. NDSU has policies that support pre-service, active duty [15] and veteran military (e.g., [16]) members. The university participates in a state-sponsored Veterans Educational Training [17] program that is designed to aid military members transition into college and other educational programs. The university also has a dedicated organization to aid veteran students, the Veteran Alliance Organization (VALOR) [18] as well as strong ROTC student groups [13], [14]. NDSU also has a dedicated, full time certifying official [19] and has been named as both a Military [20] and Military Spouse [21] Friendly School by Victory Media, which publishes the G.I. Jobs and Military Spouse Magazines.

In addition to the aforementioned support network, NDSU has policies encouraging faculty to accommodate and facilitating faculty accommodations of active duty military students who are deployed or have special schedule or other needs. These policies also apply to reservists who are

activated. Active duty military, pre-service military and veterans also benefit from the regional admiration for military service.

In terms of the NDSU cybersecurity program, in particular, the current Computer Science department chair is a veteran himself. He also serves as director of the NDSU Institute for Cyber Security Education and Research. The design of the program as being distance completable had military students in mind. This allows students to take the courses anywhere in the world. Also, the courses utilize a hybrid format where students can partially participate in person, and partially participate at a distance. Distance participation can be asynchronous. This provides significant flexibility for servicemembers' and employed veterans' schedules. It also provides flexibility to accommodate any service-related disabilities.

Starting with Spring 2019, all cybersecurity video courses are closed captioned (this was available on request, prior to this point, but now is available to all students automatically) and have descriptive audio for the visually impaired. Combined with the flexibility provided by on-campus, distance synchronous and distance asynchronous participation (and the ability to switch back and forth between these options), the course content and format are able to accommodate most disabilities. NDSU's disability services office is available to arrange accommodation for any other disabilities, on request.

There is also a very active cybersecurity student association at NDSU that plans numerous events and activities. These have included traveling to competitions and competing in online competitions. There has been participation in student association activities by ROTC members and mentorship of some activities by active duty military members.

The department and institute have also hosted a number of speakers related to cybersecurity. Active duty military members have been regularly prominently featured among the different speaker series instances. These speakers have drawn particular interest, as well as demonstrably engendering student interest in pursuing military and related cybersecurity careers.

Military members and veterans were identified as a strong group of students for the cybersecurity programs, as a key part of being successful in cybersecurity is to develop an offensive / defensive mindset. This is a qualification that most military members and veterans have, coming into the program and which the ROTC program develops in students.

ROTC students, in the Air Force program, in particular, have enrolled in the computer science B.S. degree with cybersecurity courses to prepare for cyber operations positions. There have also been active duty and veteran military members in the graduate programs with cybersecurity interests.

6. Qualitative Assessment

While significant activities have been undertaken to make the cybersecurity programs at NDSU as military friendly as possible, a number of areas for potential additional improvement have been identified. First, increasing the number of military students in these programs will facilitate greater ability to create military cohorts and special courses geared towards military

cybersecurity. Currently, the program equips students to take the EC Council Certified Ethical Hacker (CEH), EC Council Certified Hacking Forensic Investigator (CHFI) and CompTIA Security + examinations. The CEH and Security + exams, in particular, are recognized by the Department of Defense. The CompTIA PenTest + exam is also supported by current program coursework. Future plans include supporting the CompTIA CySA+ and CASP credentials. The NDSU computer science department has partnered with EC Council, CompTIA, Palo Alto Networks, Cisco Systems and VMWare to offer certification-relevant training, providing significant opportunities for expansion of certification options to students, in the future.

Second, ongoing efforts to recognize military training programs for course and degree credit will benefit the cybersecurity programs, allowing these courses to satisfy core degree requirements and, potentially, cybersecurity recognition requirements. This will reduce the amount of coursework and time required to earn degrees for servicemembers and veterans with relevant prior military training.

Third, in addition to the courses described in Section 3, work is being undertaken to offer additional courses. Particular focus is being paid to developing Department of Defense need-relevant courses. A key planned focus of the program is cybersecurity tool development, building on the strength of the department's software engineering and computer science programs. This focus should prepare students for positions within the Defense Information Systems Agency (DISA) and other relevant areas, in addition to opening doors to relevant positions in industry.

In addition to identifying the aforementioned areas of prospective improvement and augmentation, several areas of excellence have been identified. These are now discussed.

First, the program is very hands-on (including for virtual students). The Ethical Hacking course has a number of labs where students perform actual penetration testing exercises, for example. In Computer Crime and Forensics, students get experience with actual forensic techniques and hands on or virtual access to relevant forensic hardware and software. Even for the hardware elements that distance students can't interact with directly, online videos show students how they work and are recorded by a student employee, to ensure student accessibility.

Second, the program facilitates work between and amongst both online and on-campus students. The on-campus students benefit from the experience of the distance students, while the distance students build friendships with on-campus students and get a (albeit virtual) taste of the on-campus atmosphere.

Third, the development of the region's first cyber range, which is also remotely accessible, facilitates equal access to key capabilities by distance students, while keeping potentially problematic activities confined to a secure containment environment. This is particularly important for deployed students who may not be able to run some applications on their local workstations due to restrictions and security concerns.

7. Conclusions and Next Steps

This paper has described the development of new undergraduate and graduate cybersecurity programs and program components at NDSU. It has explained and evaluated how design decisions have resulted in military friendly courses and programs and identified several key areas of current excellence as well as several areas of potential future enhancement. Cybersecurity program and course development at NDSU is still an area of ongoing rapid growth. New course offerings as well as additional delivery enhancements should enhance the student experience both for on-campus and distance students and civilian, active duty military and veterans alike.

References

[1]   J. P. Merisotis, "President's Message," *Lumina Foundation Focus*, p. 1, 2013.

[2]   D. Lederman, "What Makes a College 'Military Friendly'?," *Inside Higher Ed*, 28-Feb-2008.

[3]   S. E. Minnis, "Take the right steps to become more veteran-friendly," *Recruit. Retaining Adult Learn.*, vol. 17, no. 6, pp. 5–5, Mar. 2015.

[4]   S. E. Minnis, "Consider whether your institution truly qualifies as veteran-friendly," *Recruit. Retaining Adult Learn.*, vol. 17, no. 6, 2015.

[5]   H. Sutton, "Take cues from your student-veterans to build a veteran-friendly community," *Recruit. Retaining Adult Learn.*, vol. 19, no. 8, 2017.

[6]   T. L. Moon and G. A. Schma, "A Proactive Approach to Serving Military and Veteran Students," *New Dir. High. Educ.*, vol. 153, pp. 53–60, 2011.

[7]   D. Ford, P. Northrup, and L. Wiley, "Connections, Partnerships, Opportunities, and Programs to Enhance Success for Military Students," *New Dir. Student Serv.*, vol. 126, pp. 61–69, 2009.

[8]   R. J. Dillard and H. H. Yu, "Best Practices in Student Veteran Education: Making a 'Veteran-Friendly' Institution," *J. Contin. High. Educ.*, vol. 64, no. 3, pp. 181–186, Sep. 2016.

[9]   J. A. Heineman, "Supporting veterans: Creating a 'military friendly' community college campus," *Community Coll. J. Res. Pract.*, vol. 40, no. 3, pp. 219–227, Mar. 2016.

[10]   J. Summerlot, S.-M. Green, and D. Parker, "Student Veterans Organizations," *New Dir. Student Serv.*, vol. 126, pp. 71–79, 2009.

[11]   V. Schiavone and D. Gentry, "Veteran-Students in Transition at a Midwestern University," *J. Contin. High. Educ.*, vol. 62, no. 1, pp. 29–38, Jan. 2014.

[12]   A. J. McMurray, "College students, the GI Bill, and the proliferation of online learning: A history of learning and contemporary challenges," *Internet High. Educ.*, vol. 10, no. 2, pp. 143–150, Jan. 2007.

[13]   North Dakota State University, "Air Force ROTC - Aerospace Studies," *NDSU Website*, 2018. [Online]. Available: https://www.ndsu.edu/majors/airforce/. [Accessed: 30-Apr-2019].

[14]   North Dakota State University, "Military Science," *NDSU Website*, 2018. [Online]. Available: https://www.ndsu.edu/armyrotc/. [Accessed: 30-Apr-2019].

[15]   North Dakota State University, "Deployment Accommodations," *NDSU Website*, 2018. [Online]. Available: https://www.ndsu.edu/veterans/activation/. [Accessed: 30-Apr-2019].

[16]   North Dakota State University, "Enrollment After Activation," *NDSU Website*, 2018. [Online]. Available: https://www.ndsu.edu/veterans/enrollment/. [Accessed: 30-Apr-2019].

[17] North Dakota State University, "Veterans Educational Training," *NDSU Website*, 2019. [Online]. Available: https://www.ndsu.edu/vet/. [Accessed: 30-Apr-2019].

[18] North Dakota State University, "VALOR," *NDSU Website*, 2019. [Online]. Available: https://www.ndsu.edu/valor/. [Accessed: 30-Apr-2019].

[19] North Dakota State University, "NDSU Certifying Official," *NDSU Website*, 2018. [Online]. Available: https://www.ndsu.edu/veterans/varep/. [Accessed: 30-Apr-2019].

[20] Victory Media, "Military Friendly Schools," *Victory Media Military Friendly Website*, 2019. [Online]. Available: https://www.militaryfriendly.com/schools/. [Accessed: 30-Apr-2019].

[21] Victory Media, "2018 Military Spouse Friendly Schools," *Victory Media Military Friendly Website*, 2018. [Online]. Available: https://www.militaryfriendly.com/2018-military-spouse-friendly-schools/. [Accessed: 30-Apr-2019].