ANNUAL REPORT

FY 2017-18

Cybersecurity Education, Research and Outreach Center

College of Engineering

Tennessee Tech University

Table of Contents

Executive Summary

CEROC's FY18 could be described as the center's "coming of age" year. The center achieved some substantial milestones which will establish a solid foundation for future growth. Among those milestones are the following:

- Completion of Lab and Workspace Renovations
- Completion of Center Staffing Plan
- Expansion of Graduate Student Support and Related Research
- Phase One Installation of the Cyber Range
- Establishment of Three Cyber Interest Groups (CTF, Defense, Offense)
- Become the First Tennessee University to have both CyberCorps SFS and DoD Cybersecurity Scholar Programs
- Execute the Center's First State-Funded Budget Plan

FY17 was the center's Year 0 where much effort was put into the development of our education and outreach pillars. Through these programs, CEROC has developed a recognized brand among key members (state and national level) in the education, government, and industry sectors. Our CyberCorps SFS Bootcamp, the first of its kind in the program's history, has established CEROC as a formative leader in the current program and its future forms.

With FY18 complete, FY19 will feature a greater focus on research initiatives through the expansion of graduate assistantships, research partnerships, and research seeding programs. Building out our research portfolio will complete our third center pillar.

About Tennessee Tech

Tennessee Tech University (https://www.tntech.edu/about) is located in the city of Cookeville in Putnam County, Tennessee. With a population of 31,004 in Cookeville and 75,931 in the county, the area is regarded as the hub of the Upper Cumberland region, which include the 14-county area surrounding Putnam. The county has earned this designation due to its relative economic strength and concentration of academic and industrial resources. Complete profiles on Putnam County (and surrounding counties) can be found at https://www.tnecd.com/county-profiles. Quick facts and summaries of state information can be found at https://www.tnecd.com/research-and-data/tn-quick-facts/.

The areas of the Upper Cumberland region that surround Putnam County are mostly rural areas where unemployment and poverty rates are generally higher, CEROC outreach programming has focused on these areas, providing opportunities for students in rural schools to see cybersecurity educational material, encouraging consideration of cybersecurity as a field of study, sparking interest in cybersecurity competitions, and encouraging participation of underrepresented populations in STEM areas. We have replicated some of these programs for use in other venues across the state and at national conferences.

Tennessee, as a state, has become nationally recognized as an educational reform and workforce development state with multiple programs supporting the goals set forth by Governor Bill Haslam's administration. A complete listing of publications about these efforts can be found at https://www.tnecd.com/research-and-data/publications/. Education specific to post-secondary education reform and develop programs include (https://driveto55.org):

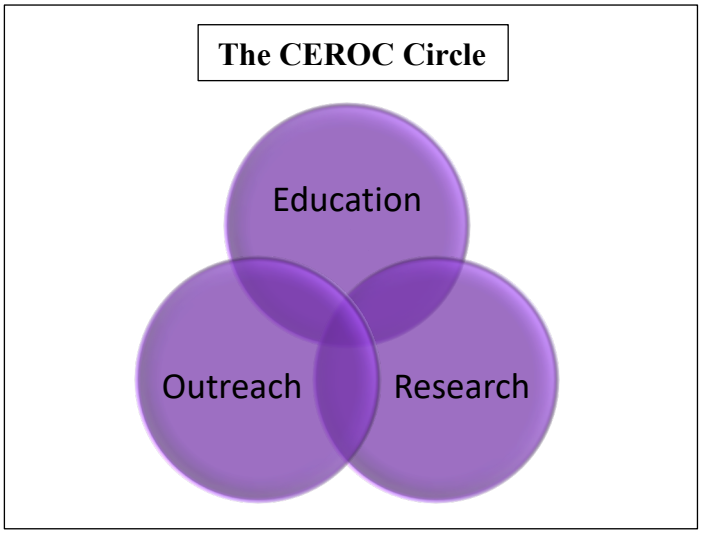
- Drive to 55 Alliance: drive to get 55% of Tennesseans equipped with a college degree or certificate by 2025
- Tennessee Reconnect: aid adult learners in entering or returning to higher education to gain new skills, advance in the workplace, and completing a degree or credential.
- Tennessee Promise: the first PK-14 program in the nation providing Tennessee high school graduates the opportunity to complete an associate's degree tuition free

As in many current labor publications, cybersecurity is not specifically targeted but is included among a variety of computer and information technology job titles. The positioning of the Middle Tennessee market as a healthcare management and technology capital in the nation as well as a manufacturing technologies capital in the southeastern region strongly support the need for the development of a stronger cybersecurity workforce to protect these vital infrastructures. Tennessee Tech via CEROC has dedicated itself to achieve this vital workforce development through the training of our nations next generation of cyber defenders.

About CEROC

General

The Cybersecurity Education, Research and Outreach Center (CEROC) at Tennessee Tech University (TnTech), virtually established in October 2015 and physically established in January 2016, is a center of academic excellence in cyber defense (CAE-CD) accredited by the National Security Agency (NSA) and Department of Homeland Security (DHS). The center was established by the Department of Computer Science and the College of Engineering to integrate university-wide existing activities and initiatives in cybersecurity education, research and outreach, the emphasis of which makes it unique in the state.



The goals of CEROC were developed during the establishment of the center and were heavily influenced by the CAE-CD program and CyberCorps SFS programs. These goals are:

1. Provide quality cybersecurity education - one of the essential skillsets for the 21st century;
2. Supply adequately trained students in cybersecurity workforce pipeline;
3. Facilitate and advance research in trending areas in cybersecurity;
4. Increase public awareness of information assurance and cybersecurity;
5. Promote and disseminate cybersecurity educational and research artifacts and experience in the academic community;
6. Share expertise with partners in collaborative initiatives in cybersecurity workforce development and research.

CEROC was awarded the CyberCorps SFS scholarship grant in December 2015 (NSF Award# 1565562) with the title of "Tennessee CyberCorps: A Hybrid Program in Cybersecurity." Tennessee Tech was the first university in the State of Tennessee (TN) to be awarded the opportunity to manage this prestigious scholarship and remains the largest such program in the state. The primary focus of the program was to produce candidates with M.S. degrees. Since the original award, the program has been expanded twice to include community college students joining during their sophomore year at their original school and transferring to Tennessee Tech for two additional years completing a B.S. degree in three years. With current extensions to the grant, we will produce approximately 30 workforce ready cybersecurity professionals over the next four years. Tennessee Tech is one of ten (10) universities participating in the CyberCorps 2Y community college bridge program working with two of our four community college partners in the state.

With the overarching goals of increasing the number of qualified students entering the fields of information assurance and cybersecurity and contributing to the capacity of the cybersecurity workforce, the objectives of the center are as follows:

1. Expand higher education choices in cybersecurity for Tennessee students;
2. Provide opportunity for Tennessee students, including those benefited by the TN Promise Act for community colleges, to apply for scholarships in cybersecurity;
3. Create an additional pipeline of qualified cybersecurity professionals in industry and federal agencies from Tennessee (and the region);
4. Increase women and under-represented minority students' participation in cybersecurity;
5. Enhance students' knowledge, skill, research aptitude, and service learning motivation through a program that values fair participation in education, research, and outreach; and
6. Assess performance of the program.

To achieve these goals, we provide:

1. Scholarship opportunities in an accelerated path to TnTech undergraduates in Computer Science within the CyberSecurity Concentration (during last two years of their curriculum) that allows for the completion of a graduate degree in half the time of a traditional path;

2. Technical and professional development training to supplement formal education and prepare students for challenging careers in cybersecurity in all sectors;
3. Opportunities for field-related work experiences and research guided by mentors from TnTech, and center partners;
4. Opportunities to participate in professional development events such as competitions and conferences in the field;
5. Opportunities to participate in student communities and professional societies; and
6. Opportunities for active involvement in outreach at different events organized by TnTech.

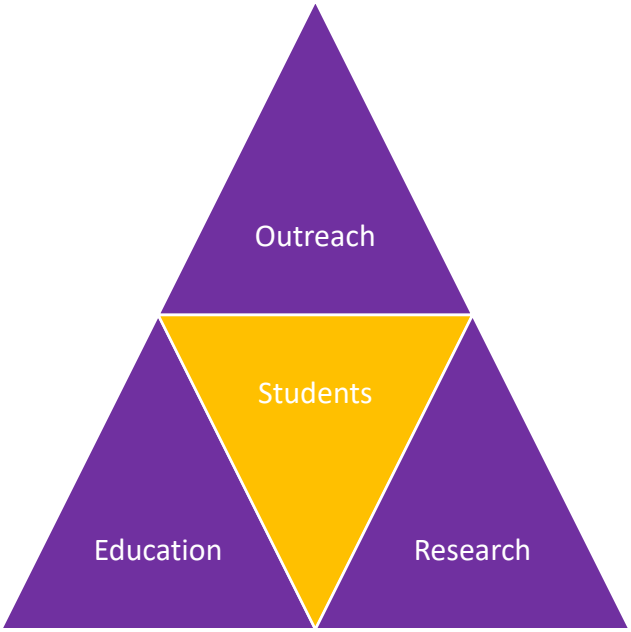
Diversity Background

CEROC has a rich history of diversity and outreach programming. Dr. Ambareen Siraj, CEROC director, is the founder of the National Women in Cybersecurity (WiCyS) conference and Non-Profit organization. This is the largest initiative of its type in the nation focusing on workforce development and recruitment of women in the field of cybersecurity. More information about the initiative may be found at https://www.wicys.net.

The Computer Science Department has recently submitted an application to the BRAID (Building, Recruiting, And Inclusion for Diversity) initiative (https://anitab.org/braid-building-recruiting-and-inclusion-for-diversity/). The program, led by the Anita Borg Institute and Harvey Mudd College, provides support to computer science departments to help increase the percentage of women and underrepresented minority students in their undergraduate computing programs. Regarding gender analysis in Tennessee Tech's computer science program over the past five years, modest gains have been made partially as a result of local diversity efforts such as participation in the Women in Cybersecurity conference, the establishment of an ACM-W and CyberEagles-W chapters, and direct recruitment. The table below shows a steady increase in female enrollment. Note that Spring 2012 is the last semester prior to many of the new diversity recruitment efforts.

Term	Spring 2012	Spring 2014	Spring 2016	Spring 2018
Female Enrollment	27 / 8.94%	31 / 8.49%	32 / 9.28%	60 / 13.48%
Male Enrollment	275 / 91.06%	334 / 91.51%	313 / 90.72%	385 / 86.52%
Total Enrollment	302	365	345	445

CEROC Focus Areas and Goals



Education

Goal E1: To provide quality cybersecurity education – one of the essential skill sets for the 21st century

Objectives:

1. Increase the number of cybersecurity courses in the computer science curriculum based upon peer and industry feedback
2. Increase the number of cyber-related workshops focusing on professional development of educations in K12 and higher education offered by CEROC and its partners

Goal E2: To supply trained students for the cybersecurity workforce pipeline

Objectives:

1. Educate and mentor CyberCorps SFS and DoD CySP students to participate in quality professional development opportunities and internships positioning them to take their place in the federal, cybersecurity workforce
2. Education and mentor CEROC student affiliates to engage in professional development and research projects to development cyber skills which contribute to improved internship opportunities leading to better positioning for cyber careers in the public and private sector

Research

Goal R1: To facilitate and advance research in trending areas in cybersecurity

Objectives:

1. Collaborate with faculty members at Tennessee Tech and other peer / partner higher education institutions to develop proposals for emerging areas in cybersecurity related to high performance computing, big data, smart grid, smart manufacturing, IoT, and critical infrastructure
2. Increase recruitment efforts for M.S. and Ph.D. students especially in the 250-mile radius of campus referred to as Eagle's Reach where perspective students will be offered in-state tuition rates

Goal R2: To share expertise with partners in collaborative initiatives in cybersecurity workforce development and research

Objectives:

1. Expand undergraduate student research programs to reach out to K12 teachers and guidance counselors and to community college transition coaches thereby increasing an interest in the field
2. Develop strategies for workforce development and training exchange within National Guard and Army Reserve units through on-site and online programs

Outreach

Goal O1: To increase public awareness of information assurance and cybersecurity

Objectives:

1. Continue and expand, where possible, programs such as the Cyber STEMmobile and NSA GenCyber to reach more K12 students, teachers, and guidance counselors increasing an interest in the field.
2. Continue and expand media advisory and publication programs directed at the general public through traditional media outlets
3. Expand and improve the social media and traditional media footprint of the center

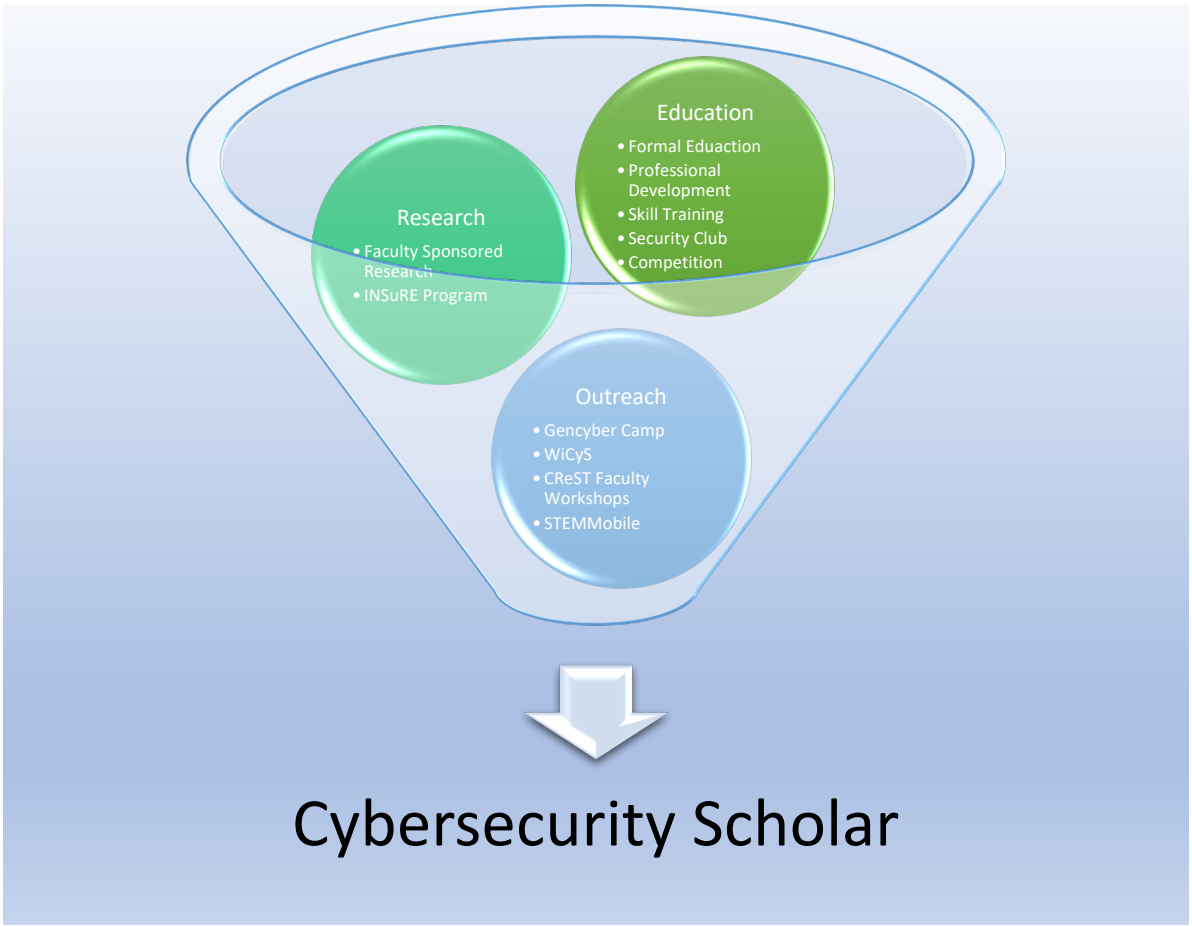
Goal O2: To promote and disseminate cybersecurity educational and research experience in the academic and commercial communities.

Objectives:

1. Continue a presence at major cybersecurity conferences featuring a mix of academia, industry, and Department of Defense presenting current research projects and prospective new projects focusing on critical infrastructure as defined by Presidential Policy Directive 21 (https://www.dhs.gov/critical-infrastructure-sectors)
2. Publish training materials via public project distribution points such as GitHub making resource kits available on a variety of computer platforms

Our Students

At CEROC, we facilitate an integrated experience for our cybersecurity students ensuring their participation in research and outreach activities alongside education activities in cybersecurity.



Education

FORMAL Education

The Department of Computer Science (CS) at TnTech has an ABET-accredited bachelor's program and offers degrees in multiple concentrations, as well as both MS and Ph.D. degrees. The degree requirements include those of the University, the College (COE), and the Department (CS).

Undergraduate Program in Cyber-Security

TnTech's undergraduate CS curriculum has included a concentration in the field of cybersecurity since Fall 2014. The purpose of this concentration is to provide a career path for TnTech students to obtain a Bachelor's degree in CS with an Information Assurance and Cybersecurity focus. This concentration includes a CS background with security relevant concepts that are applicable to computer and information systems security. There are 15 courses in the undergraduate cybersecurity curriculum that map to 22 knowledge units (KU) as specified in the CAE IA/Cyber

Defense academic requirements. The curriculum offers dedicated security courses as well as courses where security topics are integrated:

Dedicated security courses

- *CSC 4570 – IT Security (Fall only)*: This required course covers the fundamentals of computer security needed for information technology (IT) professionals. It is an overview of various technical and administrative aspects of information security. It introduces students to assets in a typical IT infrastructure, potential threats to assets, common associated vulnerabilities, asset protection strategies, and responses to security incidents.
- *CSC 4575/5575 - Information Assurance and Cryptography (Spring only)*: This required course introduces students to the fundamentals of information assurance and cryptographic techniques along with their application to the prevention, detection, and mitigation of cyber threats.
- *DS 4125/5125 – Computer Forensics and Investigations*: This elective course covers investigation, discovery, and analysis of digital computer evidence. Students work in groups to use computer hardware and forensic software to perform computer forensic investigations and solve sample cases.
- *CSC 4580/5580 Malware Reverse Engineering:* This elective course offers basic concepts of and general techniques used for reverse engineering. Reverse engineering includes basic static and dynamic analysis of malware executables, study of malware behavior, techniques that malware uses to thwart detection and analysis, and hands-on exercises using malware analysis tools and best practices.
- *CSC 5901/6901 Ethical Hacking:* This elective course offers the basic concepts of and general techniques used for pen testing. It includes pre-engagement interactions, intelligence gathering, threat modeling, vulnerability analysis, validation, exploitation, privilege escalation, post-exploitation attacks, and reporting.

Integrated security modules in traditional CS courses

With institutionalization of the Security Knitting Kit Project - SecKnitKit (NSF Award #1140864), five of the upper-division courses *(CSC 4610: Software Engineering I, CSC 4620: Software Engineering II, CSC 3300: Database Management Systems, CSC 4100/5100: Operating Systems, and CSC 4200/5200: Networks)* have been integrating relevant security modules with active learning exercises. In addition, the two-semester capstone sequence (*CSC 4610: Software Engineering I, CSC 4620: Software Engineering II*) is designed to place students in teams to build a real-world application for an industry partner. The Cybersecurity concentration students are assigned to projects with security requirements.

Graduate Program in Cybersecurity

Fast-track Program

Through this program, students can take graduate courses for undergraduate credit that can then be applied toward a graduate degree in CS at TnTech. The Fast-track program is designed to enable TnTech CS undergraduates to accumulate up to 12 credit hours of graduate coursework while still pursuing their undergraduate degree and transition to the graduate program smoothly,

with accelerated completion. Up to six hours of the graduate coursework, exclusive of directed study, taken during the student's junior/senior year can also be used to satisfy both undergraduate and graduate degree requirements. Fast-track students are mentored by their M.S. advisor for course enrollment and thesis research. If they are able to successfully start their research early and earn a minimum grade of "B" in the graduate courses upon successful admission into the graduate program, they will be able to complete their MS in one additional year.

Master of Science

The Department of Computer Science offers advanced studies leading to a Master of Science (MS) degree in CS with a concentration in Internet-Based Computing. One of the areas of specialization is Information Assurance and Security. In addition to *CSC 5575: Information Assurance and Cryptography*, this specialization includes the following dedicated security courses:

- *CSC 6575 – Internet Security (Spring only):* This course covers security-related special issues, concerns and trends in the complex environment of the Internet. Topics include (but are not limited to) vulnerabilities, attacks and security mechanisms to the networking protocols, email security, web security, online game security, social networking security, ecommerce security and mobile security.
- *CSC 6800: Advanced Topics in Security:* This course offers students the opportunity to delve deeper into their area of interest. The main objective is to critically evaluate research papers and write one.

M.S. students are also allowed to take Ph.D.-level dedicated security courses such as:

- *CSC 7575: Security Topics in the Smart Grid (Bi-annual)*: This course introduces students to timely topics related to security issues, concerns and trends in the modern power grid.
- *CSC 7210 –Anomaly and Intrusion Detection Systems (Bi-annual)*: This course covers traditional intrusion and anomaly detection systems, as well as current advances in this ever-growing field.
- *ECE 7970 – Selected Topics: Advanced Cryptography Applications in Emerging Wireless Networks (Bi-annual)*: Offered by the Electrical and Computer Engineering department, this course covers advanced topics in the design of security and privacy protocols for the emerging wireless networks.

INFORMAL Education and Professional Development

Hands-on Offense/Defense Training

Hands-on active learning is an integral part of education. It has been found that students actively engaging with concepts from course material learn more effectively. For students to effectively contribute in the defense of our nation in cyberspace, it is crucial for them to gain experience in active hands-on offense/defense training. Most of the courses with security content already contain hands-on exercise modules for students to actively engage with course concepts.

Cybersecurity Student Club

TnTech CyberEagles is a student organization with a mission to raise the computer and information security consciousness and proficiency of students in using, designing, developing and operating computing technology. The club welcomes student members interested in cybersecurity from departments across TnTech. Students in the Cybersecurity concentration are especially encouraged to participate in club activities. The club is advised by CS faculty. Currently there are 100+ members, and membership continues to grow. The club is supported by internal funds available to student clubs, sponsorship from regional security organizations and professional societies such as Middle TN ISSA, Middle TN ISACA and industry partners such as HP. The club has applied and been recognized as a National Cybersecurity Student Association affiliated club.

The club is very active and conducts bi-weekly seminars for club members such as: invited talks by external speakers from diverse walks of life including research, industry, and government service sectors, virtual CAE NSA Tech talks, training in tools such as Bettercap, Metasploit, Nmap etc., regional security conference attendance, and training for and participation in competitions. The club has been a very positive influence on our students. Aside from the educational benefit of these meetings, CyberEagles is an important part of our internal recruitment strategy to get more TnTech students to consider the cybersecurity focus area. Scholarship students also formally present in these meetings to discuss their current research work and experiences of being a funded scholar providing essential communications practice for future work. Senior members of the club, especially those in scholarship positions, are strongly encouraged to take leadership roles to improve their organizational and management skills.

Competition Participation

TnTech students regularly participate in several security competitions including the Annual Southeast Regional Collegiate Cyber Defense Competition (SECCDC), Collegiate Penetration Testing Competition (CPTC), National Cyber League, and different “Capture the Flag” competitions. Our students will continue to participate in these various competitions and improve their skills with experience. Competition teams are a crucial element in the hard skills development of cybersecurity scholars. CEROC has established three standing interest groups out of which competition teams are developed, which are:

- The **capture the flag (CTF) training team** has approximately 30 members. There is no primary competition for this team as it is newly formed. This group competes in a variety of online CTF competitions such as National Cyber League. An additional goal for this team is to facilitate local competitions and events for K12 CTF teams either at on-campus events or on-site at local schools. The student report from this group can be found in Appendix A.
- The **defensive training team** has approximately 50 members. The primary competition for this team is the Collegiate Cyber Defense Competition. Our team competes in the SECCDC event held at Kennesaw State University. This team has been in existence since 2013. The student report from this group can be found in Appendix B.
- The **offensive training team** has approximately 70 members. The primary competition for this team is the Collegiate Penetration Testing Completion. Our team competes in the CPTC event held at the Rochester Institute of Technology. The team has been in existence since 2016. The student report from this group can be found in Appendix C.

Service Learning with Cyber Reviews

As a hybrid program involving both outreach and research, CEROC has collaborated with the Tennessee 3-Star Industrial Assessment Center (IAC) at TnTech to provide cybersecurity risk assessments for small to mid-sized manufacturing companies the State of Tennessee. As part of a joint effort funded through a grant with the Department of Energy, CEROC and the 3-Star IAC deploy student assessment teams led by CEROC's assistant director to conduct cyber reviews for local and regional manufacturing companies. The reviews involve an on-site evaluation component providing students the opportunity to exercise their team and client development skills. Once data collection activities (via survey and personal interview) are complete, the students begin processing the collected data and evaluating it against a scoring rubric based upon the NIST Cybersecurity Framework and other NIST SP documents. A final report is delivered by the student team with recommendations for improvement of their security posture. So far,

CEROC student teams have conducted four such reviews as part of their service learning. Currently, we are also working with local Tennessee Small Business Development Center (TSBDC) to provide similar services for small businesses in surrounding counties.

New Scholar Bootcamp

Since 2016, TnTech has organized the annual Cybersecurity Scholar Bootcamp (funded through an extension of our original SFS grant) every summer. This first of its kind camp provides cybersecurity scholars from across the country an opportunity to attend a day and a half workshop covering a wide variety of essential soft skills for their future academic and professional careers. Topics covered during the camp include: financial planning, communications, diversity awareness, resume development, and research ethics and methodologies. The TnTech cohort have an additional half day of training conducted in the Volpe Library to become further acquainted with University research resources.

Soft Skills Development

CEROC student affiliates are included in most of our outreach events, which requires them to practice and exercise their soft skills for audiences in K12, higher education, and industry. A sample of the activities in which a Cybersecurity Scholar would be involved include:

- Presenting current research projects and training works at conferences and workshops
- Instructing a group of students on a CEROC-developed exercise
- Assisting in the development of cybersecurity exercises through creation, proofing, or implementation review activities
- Participating/presenting in diversity events

Cybersecurity Ambassadors

Aside from the regular workload of our cybersecurity scholars, they also serve a critical role as ambassadors of our programs. We encourage our scholars to participate in locally-hosted workshops as project presenters, counselors, panel participants, and guest facilitators. These social settings are a key part of our holistic approach to scholar development. Such soft skills are important when leading project teams with diverse opinions and personalities.

Professional Organization Membership

All scholars (Cybersecurity and SFS) are required to join and participate in professional organizations internal and external to TnTech. The center facilitates these memberships to the extent possible. CEROC, via the work of one of our SFS scholars, has affiliated our CyberEagles student cybersecurity club with the National Cybersecurity Student Association (https://www.cyberstudents.org) and CyberEagles-W student cybersecurity club with the National Women in CyberSecurity organization (https://www.wicys.net/organization). We also require that all scholars apply for membership with InfraGard (https://www.infragard.org). Our scholars will be involved in the establishment of an Upper Cumberland sub-chapter of the Middle Tennessee chapter. Other organizations introduced to the students include Middle Tennessee ISACA (https://www.issca.org/chapters1/middle-tennessee) and the Middle Tennessee ISSA

Chapter (https://issa-midtn.org). We also encourage and support our students to volunteer at regional cybersecurity events such as InfoSec and attend peer-training meetings such as BSides Nashville.

Active Involvement of TnTech Student Success Center

The CoE-based Clay N. Hixson Student Success Center (SSC) at TnTech focuses on initiatives and programs that develop and provide resources to help students achieve their goals of becoming engineers and computer scientists. The center provides support to our scholarship program with the following existing SSC resources that will be specially tailored for potential and new scholars:

- Access to tutors to help with challenging hands-on Cybersecurity concentration courses including programming, IT security, assembly language, operating system, etc. The SSC currently employs and trains engineering students to work as tutors in the Center.
- Access to the Student Ambassador Program where senior students are recruited to mentor new students. The Ambassador Program provides leadership and professional development opportunities for high-achieving students.
- Access to sponsored programs, such as participating in regional conferences and competitions.

Programs offered by the TnTech Library

The TnTech Library also offers tutoring services as well as a program called Class+ which includes regularly-scheduled peer-assisted study sessions and informal review sessions where students learn how to integrate course content and study skills while working together toward common goals. Internal studies have shown that students who attend similar programs earn on average one-half to one full letter grade higher than their classmates who choose not to attend. We believe that access to programs that offer academic assistance with historically difficult courses in the cybersecurity concentration increases retention in the program.

Programs offered by TnTech TLSAMP Alliance

For retention of women and underrepresented minority students in the program, the Tennessee Louis Stokes Alliance for Minority Participation (TLSAMP) program and its resources are leveraged. The students in the IASP program are encouraged to participate in weekly and monthly activities such as informal meetings/dinners with the COE Director of Diversity, study groups, club activities of local chapters of NSBE and WiCyS.

Support for Military Veterans

TnTech has been consecutively ranked as a “Military Friendly School” (G.I. Jobs Magazine and Victory Media), honored as a “Best College” for veterans (Military Advanced Education), ranked as a top ten university in the South for veterans (U.S. News and World Report), and was the first university in the State of Tennessee to be publicly recognized as a VETS Campus (Tennessee Higher Education Commission). The Office of Military and Veterans Affairs has dedicated staff assigned to the direct service of our military veterans providing a range of transition support services. Most recently, the OMVA opened a Veterans’ Lounge on campus providing access to

technology, personal and career support information, and other support systems. The OMVA operates under the direction of Mary Benedict, M. Div.

Placement Plan

Cybersecurity and SFS Scholars regularly participate in career fair events until successful internship/final employment opportunities are contracted. We have students participate in the SFS virtual job fair in the Fall of each year and take students to the annual SFS Job Fair in Washington. We also include the CAE Virtual Career Fair as one of the regular events assuring scholars have ample opportunities to engage with potential employers. Additionally, scholars have an opportunity to participate at the WiCyS job fair held as part of the annual conference (https://wicys.net). A review of job application efforts is conducted at each, bi-weekly meeting of the Cybersecurity and SFS Scholars. Students struggling with their job search are further counseled by CEROC staff using other employer contact avenues.

Research

Faculty-Mentored Research Projects

During their course of study, Cybersecurity Scholars are required to conduct research under the guidance of a CS faculty mentor. This mentorship may be orchestrated through *CSC 4040: Undergraduate Research Experience*. The course allows the students to experience research under faculty supervision with students submitting a technical report/paper based on their semester-wide project.

There are multiple CS faculty who are active in security-related research and are interested in working with students in cybersecurity-related topics as mentors. In return for their time, the mentors get to work with a student to advance research in his/her areas of interest. Like CyberCorps SFS Scholars, DoD Cybersecurity Scholars will also be paired with an academic/research advisor upon entry into their respective programs. The faculty advisor will provide them an opportunity to "shop" among the various research projects within the computer science program and the College of Engineering. Research areas in security include (but not limited to):

- Cyber Physical Systems security
- IoT security
- Vehicular ad-hoc network security
- Network security
- Healthcare security
- Big Data and security

TnTech Research and Creative Inquiry Day

Research and Creative Inquiry Day (https://www.tntech.edu/research/research-day/) is an annual event designed to promote student research and creative inquiry and provide a venue for presenting that work. This event is open to undergraduate and graduate students from all departments who want to display their research and creative projects. SFS and Cybersecurity

Scholars are encouraged to present their current work at this event. The event is open to the public and advertised within the Upper Cumberland business community.

Outreach

CEROC also delivers multiple outreach efforts programs working within the K12, higher education, and industry sectors. Along with other TnTech students, SFS and Cybersecurity Scholars will actively participate in various outreach activities hosted by CEROC, which includes but not limited to the following:

- Women in CyberSecurity conference
- Faculty development workshops (onsite and offsite)
- Computer Security Awareness and Training Workshop for TNTech and Staff
- GenCyber Summer Camp
- FAB Fridays at the Tennessee Tech STEM Center (elementary and middle school)
- Cybersecurity Awareness Workshops informing students about topics within cybersecurity and opportunities to study in the field at Tennessee Tech
- Cybersecurity Risk Assessments and Workshops informing small to mid-sized businesses on techniques to improve risk mitigation postures
- GenCyber on Wheels deployments to area schools.

Please note that all these outreach events are presented as options to our scholars to earn service learning time. It is ultimately their decision to select the ones in which they want to participate, as they are not required to participate in all of them.

Our Team

Dr. Ambareen Siraj, Professor of Computer Science at Tennessee Tech, teaches security courses at both the undergraduate and graduate level. She has focused her research on the vast areas surrounding cybersecurity, including security in cyber-physical systems, Internet of Things, situation assessment in network security, security education and workforce development.

As the founding director of Tennessee Tech's Cybersecurity Education, Research and Outreach Center (CEROC), Dr. Siraj is the leader on several National Science Foundation and National Security Agency grants involving cybersecurity, and is the founder of the national Women in CyberSecurity conference, an initiative to recruit, retain and advance women in the cybersecurity industry.

Dr. Siraj's effort to educate students and enhance the cybersecurity field of study goes beyond classes, research and outreach projects, workshops and conferences. She has authored or co-

authored more than 40 journal and conference articles while taking an active part in promoting cybersecurity training throughout the nation.

Mr. Eric Brown serves as the assistant director for CEROC managing daily operations of the center. He holds a B.S. and M.S. in computer science from Tennessee Tech. He served 20 years in the Computer Science Department at Tennessee Tech as an information and instructional technology specialist and adjunct instructor teaching portions of the information technology curriculum. He also has extensive experience in K12 education administration through his work on the Putnam County School Board and Tennessee Department of Education.

Ms. Lana Richardson serves as the financial associate for CEROC managing financial operations of the center and many of its grant programs. She has extensive experience in institutional proposal development and pricing from her years with Verizon. She has also worked in front office operations at Putnam County Schools.

Mr. Joseph Cross serves as the cybersecurity technologist for CEROC responsible for development and maintenance of the center's cyber range and supporting technologies. He holds a B.S. in computer science from Tennessee Tech. Prior to joining CEROC, Mr. Cross worked in enterprise IT management within the healthcare sector.

A complete list of CEROC faculty and staff associates can be found on our website at https://www.tntech.edu/ceroc/people.

Our Facilities

Administrative Spaces

As of August 2018, CEROC has four administrative spaces assigned to the center that includes office space for the director, assistant director, financial associate, and cybersecurity technologist.

Cyber (Eagles) Range

The CEROC Cyber (Eagles) Range is a laboratory space consisting of six, four-person team workstations. This space is supported by virtualization hardware located in the university's datacenter.

Aside from the virtual air-gapping provided by the virtualization software, the room is also physically and logistically air-gapped through the wired and wireless network supported by Information Technology Services (ITS). Design was based on an immersive, collaboratory concept, and the stand-up stations provide a 49-inch display allowing students to plug in their own laptops (or center-owned equipment) to collaboratively work within the group. The room has a collection of portable whiteboards which can be configured to facilitate the needs of working teams at any given time. Aside from the team workstations, the room also has a regular four-person conference table in the center of the room to facilitate small group conferences where only whiteboards may be needed. The space has been designed to support multiple use cases including:

- Cybersecurity course support active learning
- Competition team training
- Workshop training
- R&D (using actual hardware or virtualized hardware)

Student Research and Development Lab

The primary goal for this space is to provide researching students a quiet place to work in between classes and meetings. The Student Research and Development Lab is an area providing 20 workstation areas for students participating in the CyberCorps SFS, Cybersecurity Scholar, or CEROC-funded research programs. Each workstation provides a work surface with two hard-wired network connections, university wireless connections, and a storage cabinet. The area also provides a general office work counter and a high-performance B/W copier. A large message board display provides rotating information slides about upcoming deadlines and events. Similar to the Cyber (Eagles) Range, the area has multiple, rolling whiteboards to create ad-hoc collaboration spaces for students working on common projects. The area is built upon an open concept model with half-wall workstations encouraging collaboration with peers.

Multi-Center Video Conference Room

The SIP-enable conference room can natively host Skype and Zoom conferences. Aside from group meetings, this video-capable room can support remote training.

FY18 Highlights

Ambareen Siraj, director of the Cybersecurity Education, Research & Outreach Center (CEROC), has been recognized by the Colloquium for Information Systems Security Education (The Colloquium) for "Exceptional Leadership in Education."

Among the notable highlights during FY18:

- Dr. Ambareen Siraj was recognized by the Colloquium for Information Systems Security Education Exceptional Leadership in Education Award.
- Dr. Ambareen Siraj has been invited to serve on a committee which will help form CyberCorps SFS version 2.

- CEROC was awarded the DoD Cybersecurity Scholarship Program (scholarship and capacity building proposals) on the first attempt. The award places TnTech in another first in Tennessee to achieve category having both the CyberCorps SFS and DoD Cybersecurity Scholarship Program grants.
- CEROC has established an Education Partnership Agreement with the Naval Surface Warfare Center – Dahlgren Division. This agreement will provide fast-track opportunities for future grants as well as new opportunities for faculty and student professional development.
- The cybersecurity focus area of the CS program now represents the largest subgroup of all CS students. The CS program is now the second largest program in the College of Engineering.
- CEROC students have participated in more competitions this year than in all prior years combine continuing to place in the upper 20% in their respective groups.

Publications

1. Enahoro Oriero and **Mohammad Ashiqur Rahman**, Privacy Preserving Fine-Grained Data Distribution Aggregation for Smart Grid AMI Networks, the 37th International Conference for Military Communications (MILCOM), Los Angeles, USA, October 2018. [Accepted]

2. Anshu Bhattarai, **Ambareen Siraj**, "Increasing Accuracy of Hand-Motion Based Continuous Authentication Systems", Proceedings: *to 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)* to be held in New York, NY, November 8-10, 2018.

3. Vitaly Ford, Daniel Taylor, **Ambareen Siraj**, "AMIsim: Application-layer Advanced Metering Infrastructure Simulation Framework for Secure Communication Protocol Performance Evaluation", Proceedings: *11th USENIX Workshop on Cyber Security Experimentation and Test (CSET '18)* held in Baltimore, MD, August, 2018.
4. **A H M Jakaria** and **Mohammad Ashiqur Rahman**, Formal Analysis of k-Resiliency for Collaborative UAVs, The 42nd IEEE Computer Society International Conference on Computers, Software, and Applications (COMPSAC), Tokyo, Japan, July 2018 (acceptance rate~ 24%).
5. MGM Mehedi Hasan, **Amarjit Datta**, **Mohammad A. Rahman**, and Hossain Shahriar, Chained of Things: A Secure and Dependable Design of Autonomous Vehicle Services, 13th IEEE International Workshop on Security, Trust, and Privacy for Software Applications (STPSA) in conjunction with the 42th IEEE COMPSAC, Tokyo, Japan, July 2018.
6. Madhukrishna Priyadarsini, Padmalochan Bera, and **Mohammad A. Rahman**, A New Approach for Energy Efficiency in Software Defined Network, Fifth International Conference on Software Defined Systems (SDS), Barcelona, Spain, Apr 2018.
7. Bahman Rashidi, Carol Fung, and **Mohammad A. Rahman**, A Scalable and Flexible DDoS Mitigation System Using Network Function Virtualization, IEEE/IFIP Workshop on Security

for Emerging Distributed Network Technologies in association with IEEE/IFIP NOMS, Taipei, Taiwan, Apr 2018.

8. **Mohammad Ashiqur Rahman** and **Amarjit Datta**, Impact of Stealthy Attacks on Optimal Power Flow: A Simulink-Driven Formal Analysis, IEEE Transactions on Dependable and Secure Computing (TDSC), February 2018 (Online).

9. **A H M Jakaria**, **Mohammad Ashiqur Rahman**, and Carol Fung, Automated Synthesis of NFV Topology: A Security Requirement-Oriented Design, the 13th International Conference on Network and Service Management (CNSM), Short Paper, Tokyo, Japan, November 2017.

10. **Amarjit Datta** and **Mohammad Ashiqur Rahman**, Cyber Threat Analysis Framework for the Wind Energy Based Power System, ACM Workshop on Cyber-Physical Systems Security & Privacy (CPS-SPC) in conjunction with the 24th ACM CCS, Dallas, Texus, USA, November 2017.

11. Bata Krishna Tripathy, Ashray Sudhir, Padmalochan Bera, **Mohammad Ashiqur Rahman**, Formal Modelling and Verification of Requirements of Adaptive Routing Protocol for Mobile AdHoc Network, The 41st IEEE Computer Society International Conference on Computers, Software, and Applications (COMPSAC), Torino, Italy, July 2017 (acceptance rate~ 20%).

12. Islam, S., **Eberle, W**., & **Ghafoor, S.** (2018). Credit Default Mining Using Combined Machine Learning and Heuristic Approach.

13. **Mahmoud, Mohamed** & Saputro, Nico & Kumar Akula, Prem & Akkaya, Kemal. (2017). Privacy-Preserving Power Injection over a Hybrid AMI/LTE Smart Grid Network. IEEE Internet of Things Journal. 4. 870-880. 10.1109/JIOT.2016.2593453.

14. Saputro, Nico & Tonyalı, Samet & Akkaya, Kemal & Cebe, Mumin & **Mahmoud, Mohamed**. (2017). Efficient Certificate Verification for Vehicle-to-Grid Communications. 3-18.

15. Khalid, Faiq & Nanjiani, Sunil & **Hasan, Syed Rafay** & Hasan, Osman & Shafique, Muhammad & Awwad, Falah. (2018). Low Power Digital Clock Multipliers for Battery-Operated Internet of Things (IoT) Devices. 10.1109/ISCAS.2018.8351102.

16. Mohammed, Hawzhin & **Rafay Hasan, Syed** & **Ashiqur Rahman, Mohammad**. (2018). Load Control and Privacy-Preserving Scheme for Data Collection in AMI Networks.

17. Khalid, Faiq & **Hasan, Syed Rafay** & Hasan, Osman & Awwad, Falah. (2018). Runtime Hardware Trojan Monitors Through Modeling Burst Mode Communication Using Formal Verification. Integration the VLSI Journal. 61. 62-76. 10.1016/j.vlsi.2017.11.003.

18. Hailesellasie, Muluken & **Hasan, Syed Rafay** & Khalid, Faiq & Awwad, Falah & Shafique, Muhammad. (2018). FPGA-Based Convolutional Neural Network Architecture with Reduced Parameter Requirements. 10.1109/ISCAS.2018.8351283.

19. Khalid, Faiq & **Hasan, Syed Rafay** & Hasan, Osman & Awwad, Falah. (2017). Behavior Profiling of Power Distribution Networks for Runtime Hardware Trojan Detection. 10.1109/MWSCAS.2017.8053173.

20. Hailesellasie, Muluken & **Hasan, Syed Rafay**. (2017). Intrusion Detection in PLC-Based Industrial Control Systems Using Formal Verification Approach in Conjunction with Graphs. Journal of Hardware and Systems Security. 10.1007/s41635-017-0017-y.

21. **Hasan, Syed Rafay** & Tangellapalli, Phani. (2017). Area efficient soft error tolerant RISC pipeline: Leveraging data encoding and inherent ALU redundancy. 699-702. 10.1109/MWSCAS.2017.8053019.

22. Adegbite, Oluwadara & **Hasan, Syed Rafay**. (2017). A Novel Correlation Power Analysis Attack on PIC Based AES-128 without Access to Crypto Device. 10.1109/MWSCAS.2017.8053174.

23. Fulum Mossa, Siraj & **Hasan, Syed Rafay** & Elkeelany, Omar. (2017). Hardware trojans in 3-D ICs due to NBTI effects and countermeasure. Integration, the VLSI Journal. 59. 10.1016/j.vlsi.2017.03.009.

24. Kottler, Sam & Khayamy, Mehdy & **Hasan, Syed Rafay** & Elkeelany, Omar. (2017). Formal verification of ladder logic programs using NuSMV. 1-5. 10.1109/SECON.2017.7925390.

Grants

Proposals

FUNDING AGENCY	TITLE	PIs	PROPOSAL NUMBER	Project Period	Total Funding
JULY			**JULY**		
National Science Foundation	CAREER: Towards Secure and Privacy-Preserving Data-Driven Intelligent Transportation Systems	Mahmoud	21 (17-18)	5/1/2018-4/30/2023	**$432,623**
SEPTEMBER			**SEPTEMBER**		
Oak Ridge National Lab	Detection and Analysis of Malware in Critical Infrastructure	Ghafoor	1718M0744 52 (17-18)	10/1/18-9/30/19	**$98,952**
OCTOBER			**OCTOBER**		
Google (Google Faculty Research Award)	Proactive Resiliency Threat Detection and Mitigation for Dependable Internet of Things	Rahman	62 (17-18)	1/1/18-12/31/18	**$39,500**
National Science Foundation	SaTC: CORE: Medium: Collaborative: Control-Aware Dynamic moves for Attack-Resilient CPS	Rahman	72 (17-18)	8/16/18-8/15/21	**$414,999**
National Security Agency and National Science Foundation	GenCyber Camp at Tennessee Technological University - Summer 2018	Siraj	1718M0753 84 (17-18)	4/1/18-3/21/19	**$123,245**
NOVEMBER			**NOVEMBER**		
National Science Foundation	SaTC: CORE: Small Collaborative: Towards Secure and Privacy Preserving Communications for Smart-Grid Energy Storage Units	Mahmoud	98 (17-18)	9/1/18-8/31/21	**$257,867**
Purdue University (via NSA funds)	Tennessee Tech's Participation in Addressing Research Problems in National Information Security Through the INSURE Project	Siraj	1718M0761 100 (17-18)	1/1/18-5/15/18	**$12,000**
JANUARY			**JANUARY**		
National Science Foundation	Collaborative Research: Secure and Enhanced Spectrum Utilization for Low-Power Wide Area Networks in White Spaces	Rahman	121(17-18)	9/1/18-8/31/21	**$224,746**
Subcontract Hamad Bin Khalifa University (Prime Award from Qatar National Research Fund (QNRF)	A Reliable, Secure, and Privacy-Preserving Solution for Wireless Electric Vehicle Charging in Smart Grid	Mahmoud	132 (17-18)	9/1/18-8/31/21	**$119,999**
FEBRUARY			**FEBRUARY**		
Department of Defense / National Security Agency	DoD Cybersecurity Scholarship Program	Siraj	151(17-18)	8/22/18-8/21/19	**$261,284**
MARCH			**MARCH**		
APRIL			**APRIL**		
MAY			**MAY**		
National Science Foundation	FMitF: Collaborative Research: Formal Analysis for Real-Time Sensor-Actuator Network	Rahman	170 (17-18)	1/1/19-12/31/22	**$499,999**
JUNE			**JUNE**		
Oak Ridge National Laboratory	Detection and Analysis of Malware in Critical Infrastructure	Ghafoor	1718M0744	10/1/17-9/30/18	**$15,763**
					$2,500,977

Activations

FUNDING AGENCY	TITLE	PIs	PROPOSAL NUMBER	Project Period	Total Funding	ACTIVATION No.
National Science Foundation	Supplement to Tennessee Cybercorps: A Hybrid Program in Cybersecurity - For TTU Cyber Bootcamp Yr. 2 of 2	Siraj	216 (15-16)	7/1/2016-6/30/2018	**$50,973**	27 (17-18)
National Science Foundation	Supplement to Tennessee Cybercorps: A Hybrid Program in Cybersecurity - For Community College Inclusion Yr. 1 of 3	Siraj	192 (16-17)	8/1/2017-7/31/2020	**$121,252**	26 (17-18)
National Science Foundation	CyberTraining:CDL:iPDC - Summer Institute for Integrating Parallel and Distributed Computing…	Ghafoor, Rogers, Brown	119201617	9/1/17-8/31/20	**$143,215**	32 (17-18)
Oak Ridge National Laboratory	Detection and Analysis of Malware in Critical Infrastructure Yr. 1 of Yr. 1 Partial Allocation Only	Ghafoor	52 (17-18)	10/4/17-9/30/18	**$1,900**	70 (17-18)
Oak Ridge National Laboratory	Detection and Analysis of Malware in Critical Infrastructure Yr. 1 of 1	Ghafoor	52 (17-18)	10/4/17-9/30/18	**$14,592**	88 (17-18)
Purdue University (via NSA Funds)	Tennessee Tech's Participation in Addressing Research Problems in National Information Security through the INSuRE Project Yr. 1	Siraj	100 (17-18)	8/28/17-8/27/18	**$12,000**	118 (17-18)
Oak Ridge National Laboratory	Detection and Analysis of Malware in Critical Infrastructure	Ghafoor	52 (17-18)	10/4/17-9/30/18	**$24,738**	124 (17-18)
National Security Agency and National Science Foundation	GenCyber Camp at Tennessee Tech University - Summer 2018 Yr. 1 of 1	Siraj	84(17-18)	4/1/18-3/31/19	**$123,245**	150 (17-18)
National Science Foundation	Supplement to Tennessee Cybercorps: A Hybrid program in Cybersecurity-Community College Inclusion	Siraj, Rahman, Talbert	216 (15-16)	8/19/16-8/19/19	**$54,906**	160 (17-18)
Oak Ridge National Laboratory	Detection and Analysis of Malware in Critical Infrastructure	Ghafoor	52 (17-18)	10/4/17-9/30/18	**$43,796**	173 (17-18)
					$590,617	

FY18 Expenditures

FY18 represented the first year in which the center received funding from the state. These non-reoccurring funds are included as a line item in the THEC budget. As specified in the FY 2018 state budget documents, "$500,000 to Tennessee Technological University to match funds provided by the National Science Foundation for cyber security research (year 1 of 4)". As noted, these funds are allocated to match the CyberCorps SFS grant.

Given the startup efforts which took place in FY18, the center experienced some one-time financial opportunities. The largest of these opportunities was lapse funds from the unfilled cybersecurity technologist and financial associate 4 positions. Both of these lines were filled in November 2017. Additionally, the assistant director received release funds for two grants which activated that year. These funds were used to support the heavy financial lift of space renovations as well as starting funds for the cyber range.

FY 2018 Expenditure Summary

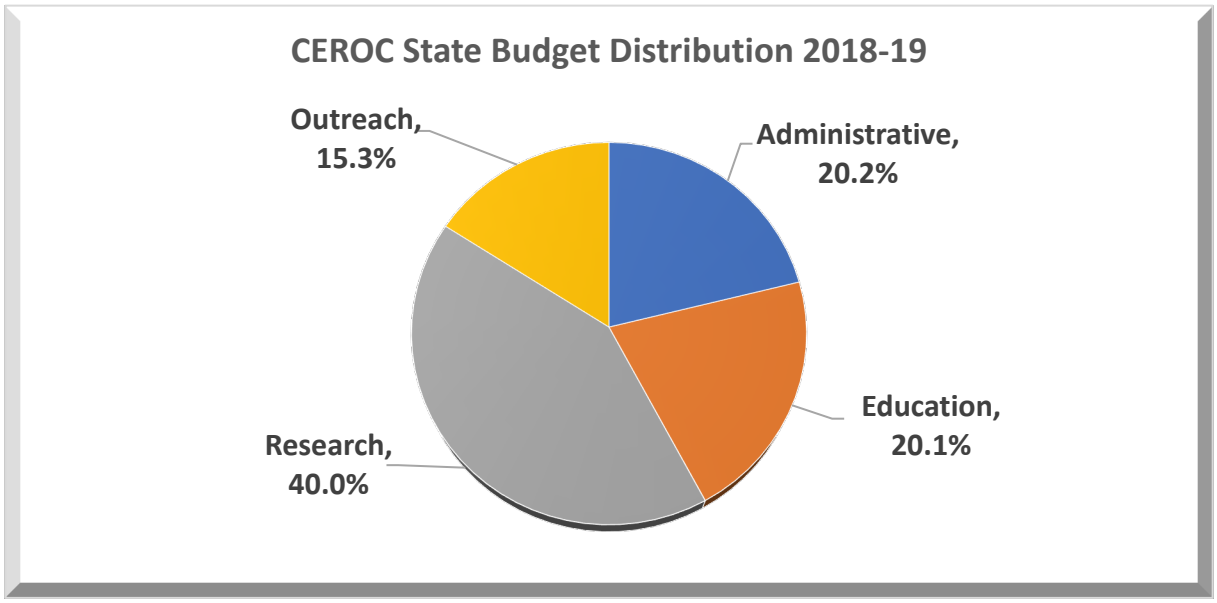
Description	Amount
Personnel Expense	
Center Personnel	$ 158,867.76
Student Support	$ 76,585.00
subtotal	**$ 235,452.76**
Administrative Expense	$ 58,233.40
Instructional Expense	$ 2,300.00
Renovation Expenses	$ 144,684.52
Research Supply Support	$ 8,372.77
subtotal	**$ 213,590.69**
grand total	**$ 449,043.45**

FY 18 also represented the establishment of center supplies for outreach events. These supplies included activity materials, branded promotional items, and branded office stationary items. These items, in addition to locally developed materials, were used in recruiting and outreach events, some of which resulted in students attending Tennessee Tech.

FY19 Budget Review

As mentioned in our FY18 budget update, a large portion of our funds were focused on infrastructure projects to provide students with workspaces conducive to collaborative research and project development. With the close of FY18, those projects have been completed with the exception of the cyber range virtualization infrastructure buildout. The center's focus will turn to more research initiatives.

The FY19 budget begins the transition from building infrastructure to feeding the research engine. Research assistantship funding has been increased to incorporate a CEROC Research Fellowship at the Ph.D. level as well as the addition of another M.S. line. Funding has also been included to provide release time for a Research Engineer providing research and mentoring support for graduate students working in the Internet of Things (IoT) cybersecurity area.



As indicated in the chart above, we are still operating the center with a 20.2% administrative overhead – a number within acceptable norms for operation. The FY19 budget also incorporates a 2.5% contingency fund.

Our research investments have now reached 40% with the new initiatives in this budget. We will continue to conduct our outreach events at comparable levels using materials developed during FY 2018 while enhancing their content. We will continue to seek grant opportunities to expand our outreach efforts. Education funding will be used to support curriculum expansion efforts as well as bridging programs for the CyberCorps SFS community college program.

Cyber range virtualization infrastructure expansion funding will be sought through grant opportunities and direct solicitation from industry partners working through workforce pipeline programs in the cybersecurity education sector. Funding for part of the project has been secured

through remaining Women in Cybersecurity NSF grant funds for the development of laboratory-based outreach programming in service to underrepresented populations. With the award of the DoD Cybersecurity Scholar grant, and additional server will be added to the cluster. Dell donated a SEED server which will serve as the third system. Some additional CEROC funds will be used to bring this server up to hardware equivalency with the other two servers. Some carryover funds from FY18 will be used to complete vSAN and connectivity projects completing the cluster hardware procurement efforts.

FY 2019 - CEROC Budget Proposal Summary	
Description	**Total**
Senior Personnel and Regular Staff	$ 231,825.28
Undergraduate Student Support	$ 23,252.40
Research Assistant Support	$ 127,500.00
Total Personnel Expense	**$ 382,577.68**
Adjunct Support	$ 5,000.00
Tennessee Tech STEMmobile	$ 3,300.00
Total Instructional Expense	**$ 8,300.00**
Travel	$ 15,000.00
Printing and supplies	$ 20,000.00
Recruitment / Promotion	$ 20,000.00
Total Administrative Expense	**$ 55,000.00**
Research Engineer - Release	$ 12,288.91
Research Engineer - Release Benefits	$ 4,072.54
Cyber Range Technological Infrastructure Expansion	$ 12,500.00
Research Supply Support	$ 12,500.00
Total Research Expense	**$ 41,361.45**
97.4% of state allocation	**$ 487,239.13**

Over the past two years, CEROC has established itself as a leader in cybersecurity education with a brand well-known in the sector. The building of the brand and an infrastructure to support the work of the center was a critical element allowing CEROC to take the next steps into expanded research efforts. This budget represents the center's commitment to making our brand known in the research sector as we have in education and outreach.

Appendix A – CTF Cyber Interest Group Report (student reported)

Current Leadership

CTFCIG Lead: Connor Gannon
CTFCIG Co-Lead: Samuel Wehunt

Mentors in Training

CTFCIG currently has one active mentor-in-training: Ryan Brewer
There are several things that mentors-in-training are expected to do.

1. Participate in as many CTF competitions as possible. How they rank does not matter as much as actually competing, because competing is very valuable learning experience. Mentors in training are also expected to create write-ups about competitions they compete in.
2. Create challenges for others in the group. The way we want to grow our group is by creating novel challenges for each other which will allow us to get better without relying solely on competitions others have made

High Level Overview

CTFCIG is a cyber interest group focused on competing in Capture the Flag competitions. These competitions are frequently designed as a jeopardy-style with many different categories of cyber related challenges. In order to excel in these types of competitions our group aims to build a solid set of general problem-solving skills which can be used to solve any variety of challenges. We can then gauge our skillset against other groups in the country by entering in competitions.

Competitions

CTF competitions are very frequent, and our group attempts to enter in as many as possible. Below is a list of past competitions as well as our ranking (multiple rankings indicate multiple teams or multiple years of competition):

- NCL: 23/264
- Summit CTF: 3/25, 12/25
- Pico CTF: 1233/11339, 3106/11339, 2091/11339
- SFSCON CTF: 1/10

Competition write-ups are being performed by members who have competed in the above competitions.

--

Appendix B – Defense Cyber Interest Group (student reported)

Leadership

Team Leader - Derek Singh
Team Co-Leader - Kirill Kozlov

Lead Mentors

-Gustavo Angeles
-Travis Lee
-Josh Vick
-Cordell Medlin
-Jordan Johnson

Mentors in Training & CyberPatriot Ambassadors

-Kaitlyn Cottrell (*CyberPatriot*)
-Jeremy Potts (*CyberPatriot*)
-Elena Becker (*CyberPatriot*)
-Caleb Smith (*CyberPatriot*)
-Abigail Bradfield (*CyberPatriot*)
-Grant Brown (*CyberPatriot*)
-Austin Brown (*CyberPatriot*)
-Julianne Cox (*CyberPatriot*)
-Nick Stone (*CyberPatriot*)
-Ryan Brewer (*CyberPatriot*)
-Tate Seyler
-Kendall Land
-Ahsan Ayub
-Alex Marti
-Alyssa Meadows
-Lukas Motykowski

Mentoring Model

Our goal for training our upcoming mentors is to get them heavily involved in the research phase of learning new tools and techniques that are utilized in real-world applications. We have them present their findings to other mentors or at the defense meetings. This helps give them practice for discovering new topics and how to present to a large group. We also are utilizing some mentors in our CyberPatriot outreach program, where TTU students go to local schools and assist teaching the fundamentals of security.

Defense Interest Group Goals/Plans

Our intentions are to make students aware of the practices utilized in the cyber defense industry. We use real-world scenarios and show them how & why to secure commercial environments.

Our goal is to give our students a foundation to build from so they can continue to grow and learn new techniques of security. We incorporate the NIST framework and Saltzer & Schroeder's security principles. Additionally, our meetings also assist students enrolled (or plan to enroll) in CSC-4570 IT Security, taught by Dr. Ambareen Siraj.

Our main focus this year is to create an introductory course that will be hosted online for new members to learn the fundamentals of security. This will help ensure that our meetings continue to be productive with bringing new ideas & techniques for students to build on. Moving forward, we intend to have new members utilize this training course on their own time, while maintaining advance topics in our meetings.

CyberPatriot Outreach

CyberPatriot is The National Youth Cyber Education Program where students in middle and high schools compete and learn how to secure servers and services. Most schools across the nation are under qualified with their staff to support such programs. To assist with this gap, we have created a group of mentors (listed above) to help elaborate what is needed for a successful program to function & compete. Our intention is to create a well-formed document that would contain training materials for students/teachers to give any school the capability to become involved and learn cybersecurity.

Defense Competitions

This year we are planning to compete at the Department of Energy's CyberForce competition and the Collegiate Cyber Defense Competition (CCDC). In years past, we have not had a strong foundation to work from, so our lead mentors are preparing topics for our defense meetings to help assist the growth of knowledge so that we become a successful competitive program. Our focus this year will be to incorporate automation with the use of scripting languages to ensure that setup and repair occur in a timely fashion to ensure that we gain the most amount of points during each competition. We will continue to elaborate on the fundamentals of securing services and machines to give us the best possible outcome at each competition.

--

Appendix C – Offense Cyber Interest Group (student reported)

Overview

The Cyber Eagles: Offense Cyber Interest Group (OCIG) is a student-led organization dedicated to the exploration of offensive cybersecurity, ethical hacking, penetration testing, and red teaming. OCIG empowers TTU students to safely practice the tools, tactics, and procedures used by real-world cyber adversaries and penetration testers.

Goals

1. Expose students to hands-on experience with offense security beyond the classroom
2. Empower students to employ an adversarial mindset when building, configuring, and defending systems as cyber defenders
3. Provide baseline experience and leadership opportunities for students interesting in cyber offense careers
4. Promote teamwork and professionalism via competitions and crowdsourcing OCIG content preparation

Leadership

OCIG leadership is structured to leverage the knowledge of more experienced students while preparing the next group of leaders to step up as leaders graduate. There are three tiers of OCIG leaders: Co-Leads, Mentors, and Mentors-In-Training.

Co-Leads

Co-Leads are the face of OCIG and represent it at many TTU events.

- Joe Bivens — Cybersecurity Graduate Student
- Max Layer — Cybersecurity Undergraduate Student

Mentors

Mentors are the most senior OCIG members and work with the Co-Leads to prepare and lead OCIG activities. They have a diverse background and set of interests and may be leaders or mentors of other Cyber Interest Groups.

- Darren Cunningham — Graduate Student
- David Yantis — Graduate Student
- Sam Wehunt — Graduate Student
- Connor Gannon — Graduate Student
- Shritesh Bhattarai — Undergraduate Student
- Kirill Kozlov — Undergraduate Student

Mentors-In-Training

Mentors in Training are OCIG members of varying technical knowledge and academic standing that are motivated to become OCIG Mentors (or Leaders) in the future. Mentors provide external resources and tiered challenges for Mentors-In-Training (MITs). MITs report their progress as they complete challenges and are encouraged to utilize Mentors as a resource throughout their

journey. They act as Team Leaders during OCIG activities and are expected to participate in Offense competitions.

- Will Johnson
- Jake Geasley
- Quentin Johnson
- Carli Williams
- Andrew McDole
- Andrew Craig
- Clayanna Brandon
- Robert Jordan
- Colton Wrisner
- Nick Hatfield
- Susan Jeziorowski
- Derek DePriest
- Elena Becker
- Justin Presley
- Kaitlyn Cottrell
- Tate Seyler
- Richard Brown
- Trenton Chrisman
- Ethan Borton

Members

While membership is open to any member of CyberEagles (and all majors are welcome), the majority of members are Computer Science in the Cybersecurity concentration. There are 70 OCIG members as of Fall 2018, including OCIG leadership. Peak meeting attendance is 50 students.

Infrastructure

Virtual CyberRange

To host workshops and the majority of OCIG events, we heavily utilize vCenterCEROC, a vSphere / vCenter server accessible from the campus network. Virtualization allows OCIG Mentors to build large-scale target networks with many machines and complex network topologies that can safely be scanned and exploited in a controlled environment. Virtual machine images can also be duplicated and consistently deployed. There are over 30 vulnerable virtual machines hosted on the Virtual CyberRange. These machines are a mixture of publicly available vulnerable images, custom machines hand-crafted by OCIG Mentors, and randomly generated vulnerable VMs.

To support the construction of challenge VMs in the future, OCIG Mentors have obtained the full dataset of applications hosted by ExploitDB (27GB of vulnerable applications for a variety of platforms). Additionally, OCIG mentors have created and maintain a set of TTU-internal GitLab projects focusing on CyberRange infrastructure management.

Physical CyberRange

OCIG Mentors have independently implemented a portable, "physical" CyberRange as well. This setup allows OCIG members to VPN into the CyberRange from their own, personalized Virtual Machines and allows a mixture of virtual machines and physical devices (such as Raspberry Pis) to be connected to the network. While vCenterCEROC is obviously the superior platform for hosting OCIG activities, the experience gained through designing and implementing the infrastructure was valuable, and it serves as a clear proof of concept for a VPN-accessible CyberRange capable of hosting physical devices.

Activities

Competitions

Department of Energy: Cyber Defense Competition (CDC) — Spring 2018

DoE CDC (now rebranded as "CyberForce Competition") is a cyber defense competition that focuses on defending cyber-physical systems in the electric grid. OCIG sent several volunteers that participated as part of the official CDC Red Team, which emulates cyber adversaries that aim to disrupt the electric grid and the attached Industrial Control Systems (ICS).

Team

- David Yantis
- Sam Wehunt
- Connor Gannon
- Joe Bivens
- Darren Cunningham

Results

The Red Team is not scored, but we gained valuable experience and worked side-by-side with professional penetration testers to compromise Blue Teams (students competing in the competition) nationwide. Operating with a goal of disrupting and destroying systems was a unique experience. Interest in SCADA / Industrial Control System exploitation was a key takeaway.

eSentinel: North American Open — Fall 2018

eSentinel is a "King of the Hill" style Capture the Flag competition with offensive and defensive elements. Each team is tasked with hacking their way into vulnerable servers, marking them with their team's flag, and then defending the server (and maintaining uptime) as it is attacked by other teams. The competition team was a mix of OCIG and Defense Cyber Interest Group leaders.

Team

- Derek Singh
- Joe Bivens
- Kirill Kozlov
- Max Layer

Results

We obtained 10th place out of 44 teams across North America. The competition was particularly interesting due to the need to rapidly harden and defend services after they were captured. The need to quickly identify low-hanging fruit through automation was a key takeaway.

Collegiate Penetration Testing Competition (CPTC) — Fall 2018

CPTC is a cyber offense competition where teams roleplay as penetration testers for a fictitious company. All interactions with the customer are in-character and professional. The goal of the competition is to provide a detailed, actionable penetration testing assessment for the company that allows them to improve their security posture.

Team

- Joe Bivens
- Darren Cunningham
- Connor Gannon
- Max Layer
- Sam Wehunt
- David Yantis

Results

TnTech placed 2nd in the Central Region and is one of the 10 teams advancing to the National CPTC competition November 2nd, 2018. The competition is an excellent simulation of a real-world business scenario, with special emphasis put on maintaining client uptime and the goal of improving the security of the client through our findings. The ability to quickly adapt to unfamiliar systems and the need for “soft-skills” in presentation and technical writing were key takeaways for the team.

Department of Energy: CyberForce Competition — Fall 2018 (Planned)

After our incredible experience at the Spring 2018 CDC / CyberForce competition, we are excited to participate again in the DoE: CyberForce Competition November 30th, 2018 as part of the Red Team. Confirmations are still pending, but many of the OCIG Mentors-In-Training have volunteered as well.

Team (Tentative)

- Joe Bivens
- Darren Cunningham
- Connor Gannon
- Max Layer
- Sam Wehunt
- David Yantis
- Carli Williams
- Quentin Johnson
- Jordan Johnson
- Clayanna Brandon
- Cordell Medlin

- Joseph Cross

Workshops

Workshops occur bi-weekly on Monday evenings. OCIG workshops are hands-on activities led by an OCIG Mentor. They often focus on a relevant tool or topic and vary in technical depth. Developing a strong backlog of workshop content that can be used in future semesters is a primary goal of the Fall 2018 - Spring 2019 year.

Example Topics

- Network Fundamentals
- Network Scanning
- System Enumeration
- Vulnerability Scanning
- Linux Fundamentals
- Windows Fundamentals
- Basics of Shells
- Metasploit
- Basic Persistence
- Advanced Persistence
- Exploit Development
- Remote Access Tool Development
- Reporting

Practice Scenarios

To practice for cyber competitions and hone our offense skills, we regularly meet (typically every other Saturday) for scenario-driven events. These exercises typically involve large networks of exploitable machines where OCIG members are tasked with discovering and documenting the exploits.

Outreach

OCIG is frequently represented at Cybersecurity and CyberEagles events throughout the academic year. We have successfully used these events for recruitment. In the future, we look forward to opportunities for community outreach.

Wargames

Cross-CIG collaboration is a priority for all Cyber Interest Groups at TTU. This is especially true for Offense / Defense collaboration. OCIG is working closely with the Defense Cyber Interest Group to host monthly Wargames, where Defense tries to defend a vulnerable network while maintaining uptime and Offense tries to exploit and maintain persistence in the target machines.

Future Plans and Challenges

External Training

OCIG Mentors would love to partner with cyber professionals in our training, workshop preparation, and workshop leadership. This would allow us to offer more in-depth, relevant content to our members and help guide us as a group moving forward. Learning from experienced professionals would be invaluable as we prepare for cyber competitions. Additionally, workshops with guest presenters would be an excellent way to expose OCIG members to career opportunities relevant to the group.

Content Library

OCIG Mentors are working hard to develop hands-on workshops at varying levels of technical depth. This process is very time consuming and we are looking for ways to keep up with the demand for additional content. We hope that OCIG Mentors can establish a collection of workshops that can be reused in future semesters, so that the total collection of OCIG content grows each year and can be offered as additional practice material outside of OCIG meetings.

Scenario Building

Currently, all scenarios are constructed by OCIG Mentors. Many vulnerable VMs are taken from sites such as VulnHub. While these VMs provide a challenge for both OCIG Mentors and Members and can easily be added to a network with DHCP, they are typically fully standalone machines. Creating virtual networks that emulate real-world corporate networks (e.g. full domains with firewalls and different security zones) requires a significant amount of effort. These realistic networks are the most valuable for competition practice and wargames, but if OCIG Mentors create and configure the entire network, they will benefit less from practicing against it (as they would have full knowledge of all vulnerabilities present).

The OCIG is hopeful that a CEROC-supported “Purple Team” will be created, guided by cyber professionals, that can create a steady stream of reliably deployable, realistic scenarios for competitions and Wargame events.

Competitions

OCIG is currently searching for additional offense competitions in which to compete. Currently, CPTC, CyberForce, and eSentinel are competitions in which we regularly participate. Many OCIG members also participate in CTFs, but we are particularly interested in locating more King of the Hill CTFs and any additional penetration testing competitions.