EAGLES REACH NEWSLETTER

Cybersecurity Education, Research & Outreach Center

TENNESSEE TECH

Edited by: Jake Graves, Computer Science

UPCOMING EVENTS IN MARCH

cybereagles.org/calander/

Tuesday March 2: Defense interest meeting 6:30-8pm

Thursday March 4: CyberEagles meeting 11-12pm

Thursday March 4: CEDI Webinar 6:30-8pm

Monday March 8: CySP meeting 6:30-8pm

Monday March 8: WiCYs Student Chapter meeting 6:30-8pm

Tuesday March 9: SFS Teams meeting 4:30pm

Wednesday March 10: Offense interest group meeting 6:30-8pm

Thursday March 11: CEDI meeting CTF training 6:30-8pm

Saturday March 13: CEROC spring showcase 9:30-11:45am

Tuesday March 16: Defense interest group meeting 6:30-8pm

Wednesday March 24: Offense interest group meeting 6:30-8pm

Thursday March 25: CyberEagles meeting 11-12pm

Thursday March 25: CTF Interest Group Meeting 6:30-8pm

Tuesday March 30: Defense group meetin6:30-8pmg

Scan this QR code to make sure you do not miss an issue!

Scan this QR code sign up to be a member of the CyberEagles club!

MESSAGE FROM CEROC

It was Walt Disney who said: "Don't just fly, soar!!" And why not! You are an EAGLE! Moreover, a cyber EAGLE! The world is at your REACH, not limited by distance or boundary but by only your imagination and dedication!

These times have been hard for everyone: students, faculty, employees, parents… but we are ALL doing what we can do under the circumstances! On top of that, the whole CEROC has been devastated by the recent snow/ice storm and displaced. However, the inaugural EaglesReach newsletter only shows that Eagles can't be restrained…

We hope you will find some role models, inspirations, knowledge, opportunities and get a chuckle or two from our CEROC newsletter, which is FOR you and BY you!

If you would like to join our editorial team (we do need help), send an email to ceroc@tntech.edu

Dr. Ambareen Siraj, EaglesReach Advisor

Director CEROC, Professor Computer Science, Tennessee Tech

https://www.linkedin.com/in/ambareensiraj/ Cybersecurity Education, Research and Outreach Center

Box 5125 | 1020 Stadium Drive, Prescott Hall, Room 414

Cookeville, TN 38505

Phone: (931) 372-3519 | ceroc@tntech.edu

FACULTY HIGHLIGHT

Mike Rogers is an associate professor of Computer Science at Tennessee Technological University. He is originally from the state of Kentucky in the USA, and he received his Ph.D. from the University of Kentucky 2002 and has been at TnTech since then. His current research is in the areas of Parallel and Distributed Computing (PDC), High Performance Computing (HPC), systems security, and controls system simulation and security. He typically teaches systems oriented courses and TnTech including operating ststems, reverse engineering for malware, database management systems, distributed operating systems, and programming courses. Dr. Rogers is also actively engaged in the Computer Science education community and is working to integrate PDC and HPC throughout the Computer Science undergraduate curriculum. Dr. Rogers is married to Michelle Rogers, has two grown children, and he is a Christian who enjoys being with his church family, - and he also enjoys reading (a lot).

GRADUATING STUDENT HIGHLIGHTS

Julianne Cox

My name is Julianne Cox (pictured above) and I'm a fifth-year undergraduate student graduating this upcoming May! I spent my first year of college at Volunteer State Community College, but the last four have been spent here at Tech. It's been an absolutely incredible experience – from the professors to the courses to the extracurricular opportunities, Tech truly has it all. Especially when you're interested in cybersecurity! If I had any advice to students in the program now, I would say that you shouldn't be afraid to say "yes" to as many opportunities as you can. Even if you think you're not fully prepared for something, the point of college is to learn as you go! Say yes to things even if they're scary, and you may find a new passion or skill that you didn't know you had. I know I found some surprising interests during these past few years! I also gained real world experience after being encouraged to apply for summer internships by the faculty. These internships have led to a full-time job offer after graduation, which I am thrilled about! I'll be leaving college and headed to a job as a cybersecurity analyst with an amazing company outside the Nashville area. I couldn't have done it without the support and development opportunities available here on campus, and I'm forever grateful that I ended up at Tennessee Tech!

Kendall Land:

My name is Kendall Land, I am in my second semester of graduate school, and I am scheduled to graduate at the end of this semester. After I graduate, I will be going to work for SpaceX in their Information Security Department. For clubs, I have done a lot with Cybereagles, namely the cyber interest groups and WiCyS. The cyber interest groups are what enabled me to take part in a lot of competitions. The groups both helped me gain the knowledge to perform well in the competitions through their meetings, as well as gave me the opportunity to compete in the first place. The competitions I did were usually either focused more on the defensive side, or they were more of a jeopardy style CTF competition. Out of all the competitions I competed in, one of the best moments was when we were able to get 2nd in the nation for Hivestorm. I got the opportunity my senior year to be the lead of the defense interest group. I also got to be a part of two of the Gencyber camps that Tech hosts over the summer. These were always fun getting to introduce high school students to the field through fun activities. My advice to students would be to get involved with Cybereagles and the interest groups and have fun. Getting to hang out with other people interested in the same things, whether a competition or just a meeting, was always a great time and one of my favorite things to do.

Linkedin: https://www.linkedin.com/in/kendallland/

PHD STUDENT HIGHLIGHT

Farzana Ahamed Bhuiyan:

I am Farzana Ahamed Bhuiyan, a fourth-year Ph.D. student at Tennessee Tech University. I am doing my Ph.D. on leveraging vulnerability discovery strategies for secure machine learning development, supervised by Dr. Akond Rahman. My research interests include software security, deep learning, multimodal learning, and machine learning. I love the academic environment at Tennessee Tech. I have met different people with admirable goals, including our faculty, willing to mentor each other which makes my academic journey an enjoyable one. I am from Bangladesh, a beautiful country in South Asia. I graduated with a B.Sc. in Computer Science and Engineering from Bangladesh University of Engineering and Technology. Currently, I am looking forward to my upcoming internship as a software engineer intern at Facebook in Summer, 2021. My motto for life is to keep going until the dreams come true. To know more about me and my work, please visit my website: https://fbhuiyan42.github.io

Linkedin:
https://www.linkedin.com/in/farzana-ahamed-bhuiyan/

CURRENT STUDENT HIGHLIGHTS

Carli Williams

My name is Carli Williams, and I am currently a junior at Tennessee Technological University. I am originally from Franklin, Tennessee where I grew up playing video games and rescuing feral cats. The Tech Experience for me is finally being able to get out of my bedroom and meeting new people. That eventually led me to Cybereagles and all the competitions I participated in throughout my academic life here. Unfortunately, due to the pandemic, a lot of my social life and competition life has been limited, but it gives me more time to focus on my studies. I currently have no idea where I will end up after Tech, but I my long-term goal in cybersecurity is to become a penetration tester. Some advice I want to give to students is that it is ok to take breaks. This sounds easier said than done, but you will eventually get extremely frustrated with a problem to the point that you can not think straight. If you have a hobby, do the hobby to clear your mind. After an hour, come back to the work and see if you can solve the problem. This has helped me a lot in my studies.

Linkedin:https://www.linkedin.com/in/carli-williams-7832961b6/

Quincy Card

My name is Quincy Card. I am a rising Junior at Tennessee Tech, and I have recently joined CEROC as an NCL coach in the C3E Program. My experience at Tech has been challenging, educational, and rewarding. Pretty much all of the professors that I have had have been very accommodating and willing to help me grow as a Computer Science student, as well as student of life. I am currently applying for the DoD and SFS scholarships and seeking internship opportunities to see how to apply all of the theory I have learned in class and gain a much-needed real world perspective. If I had to give any advice to students, it is to budget your time and hold yourself accountable. I believe time management is one of those fundamental skills that everyone needs, and you need to set aside time each day to work on classes, maybe do some practice outside of class, and even rest. Burnout can hit a student hard, and to avoid that you need to keep yourself from procrastinating until you're cramming all of the work you missed every night for a week straight. I hope everyone has a good semester!

Linkedin:
https://www.linkedin.com/in/quincy-card-3443481bb/

ACCOLADES

Tennessee Tech University with joint collaboration of Tennessee Tech Cybersecurity Education, Research and Outreach Center (CEROC), Computer Science department and the Oak Ridge National Laboratory recently hosted the virtual 16th International Conference on Cyber Warfare and Security (ICCWS) held February 25-26, 2021. The conference attracted academics, military professionals and practitioners from around the world to present their research findings in the form of empirical studies, case histories and other theoretical and practical contributions. More information can be found here: https://www.academic-conferences.org/conferences/iccws/

Shout out to the team of tech students who participated in annual Southeast Collegiate Cyber Defense Competition hosted virtually by Kennesaw State University in February.

Kaitlyn Carroll (Captain),Phillip Brown, Austin Brown , Jacob Sweeten, James Massengille, Austin Tice, Tate Seyler, Daniel Simpson, Mike Soare

- William A. Johnson, Ph.D student and CyberCorps scholar has successfully defended his doctoral thesis proposal under the guidance of Dr. Sheikh Ghafoor on his research about security of SCADA networks. He is expected to defend his thesis in Spring of 2022.
- William A. Johnson, Sheikh Ghafoor, Stacy Prowell. Companion Assisted Software Based Remote Attestation in SCADA Networks. To appear in the proceedings of 16th International Conference on Cyber Warfare and Security February 25-26, 2021, TN, USA.
- Juan Lopez, Joel Asiamah, Raymond Borges-Hink, and Sina Sontowski,. Resilience Analysis of Real-Time Automation Controllers (RTAC) under Cyber Stress. Presented at 16th International Conference on Cyber Warfare and Security February 25-26, 2021, TN, USA.
- Farzana Ahamed Bhuiyan, Akond Rahman and Patrick Morrison, "Practitioner Perception of Vulnerability Discovery Strategies", to appear in the 2nd International Workshop on Engineering and Cybersecurity of Critical Systems (EnCyCriS 2021), co-located with the 43rd International Conference on Software Engineering (ICSE 2021).
- Dibyendu Brinto Bose, Akond Rahman and Shazibul Islam Shamim, "'Under-reported' Security Defects in Kubernetes Manifests", to appear in the 2nd International Workshop on Engineering and Cybersecurity of Critical Systems (EnCyCriS 2021), co-located with the 43rd International Conference on Software Engineering (ICSE 2021).
- Akond Rahman and Effat Farhana, "An Empirical Study of Bugs in COVID-19 Software Projects", to appear in the Journal of Software Engineering Research and Development (JSERD), 2021.
- Farzana Ahamed Bhuiyan, Md. Bulbul Sharif, and Akond Rahman, "Security Bug Report Usage for Software Vulnerability Research: A Systematic Mapping Study", to appear in the journal of IEEE Access, 2021.
- Akond Rahman, Md. Rayhanur Rahman, Chirs Parnin, and Laurie Williams, "Security Smells in Ansible and Chef Scripts: A Replication Study", in the journal of ACM Transactions on Software Engineering and Methodology (TOSEM), 2021.
- Yilmaz, I., Kapoor, K., Siraj, A., & Abouyoussef, M. (2021). "Privacy Protection of Grid Users Data with Blockchain and Adversarial Machine Learning" Proceedings: ACM Workshop on Secure and Trustworthy Cyber-Physical Systems (SaT-CPS 2021) to be held virtually on April 28, 2021.
- Ibrahim Yilmaz and Ambareen Siraj, " A Privacy-Preserving Energy Consumption Scheme for Smart Meters with Adversarial Machine Learning" accepted in IEEE Access, 2021
- Denis Ulybyshev, Ibrahim Yilmaz, Bradley Northern, Vadim Kholodilo, Michael Rogers. 2021. Trustworthy Data Analysis and Sensor Data Protection in Cyber-Physical Systems. In ACM Workshop on Secure and Trustworthy Cyber-Physical Systems 2021 (SaT-CPS 2021). Accepted, in-press.
- M. Alsabaan, W. Alasmary, A. Alquniah, M. Mahmoud, and M. Nabil , "Distributed surveillance system using positive orthogonal codes", IEEE Access, January 2021. Accepted.
- M. Baza, M. Pazos-Revilla, M. Nabil, A. Sherif, M. Mahmoud, W. Alasmary, "Privacy-preserving and collusion-resisting charging coordination schemes for smart grid", IEEE Transactions on Dependable and Secure Computing (TDSC). Accepted. Published online Jan. 2021.
- M. Baza, Ramy Amer, Amar Rasheed, Gautam Srivastava, Mohamed Mahmoud, Waleed Alasmary, "A blockchain-based energy trading scheme for the electric vehicles," IEEE Consumer Communications Networking conference (CCNC'21) WKSHPS STP-CPS, Las Vegas, USA, 2021.

SCHOLARSHIP STUDENT HIGHLIGHT

Jevin Evans:

Hi, I am Jevin Evans, a second-year master's candidate at Tennessee Technological University. My master's project is titled the "Development of Education Material for Cybersecurity Courses," supervised by Dr. Muhammad Ismail. My research has allowed me to dive into and create labs for attacks, defenses, and concepts that affect the Internet on each layer of the OSI model. As a Tech student, I have had many experiences from being a resident assistant for Residential Life to being a member of the Cybersecurity Education Research and Outreach Center (CEROC). Being a member of CEROC has allowed me to mentor, educate, and give back to my community using my cybersecurity skills. I am a recipient of the DoD CySP Scholarship Program (link: https://www.tntech.edu/ceroc/education/cysp/ which has allowed me to continue my education and has offered me a job with the Department of Defense when I graduate in May 2021. My experiences have taught me that cybersecurity is a universal concept that can be applied to whatever you can dream of and create.

Linkedin: https://www.linkedin.com/in/jevinevans/
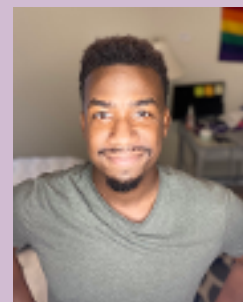
ALUM HIGHLIGHT

<u>Winson Phillips</u>

My name is Winston Phillips and I graduated Tennessee Tech in December 2019. I met some amazing people in the program that consistently motivated me to learn more, both in the classroom and CEROC! This school's cyber security program helped further my understanding of cyber and it's impact in our modern world. After graduation, I landed a job as a cyber security analyst at Nashville based Cybermaxx and am loving it! In cyber security, I am challenged every day, explore my critical thinking skills, and work with amazing people who share the similar love for knowledge.

Linkedin:https://www.linkedin.com/in/winston-phillips/

CEROC OUTREACH PROJECTS

The Department of Defense (DoD) funded Community College Cyber Enrichment (C3E) Program (Award# H98230-20-1-0321) which provides opportunities and knowledge about cybersecurity to students currently enrolled in community colleges across the state. The primary goal of C3E is to grow the pipeline of community college students in Tennessee to join the cybersecurity workforce with baccalaureate degrees at the least. From informational seminars to workshops to summer bridge programs, C3E project is undertaking multiple initiatives to foster an interest in cybersecurity and provide community college students exposure to careers available in this field.

More information about C3E project and opportunities to engage/participate is available at: https://www.tntech.edu/ceroc/outreach/c3e.php

The Department of Defense (DoD) funded Cyber Education Diversity Initiative (CEDI) Coalition Program has been created with the purpose of developing lasting support systems for students in Minority Serving institutions (MSI)s and Historically Black Colleges and Universities (HBCU)s. As part of this nine partner NCAE-C designated academic institutions, CEROC (Award# H98230-20-100385 with FORD0061-30353) serves as a resource for MSIs and HBCUs and provides different services to the students and faculty of these institutions which include student and faculty training, student competitions, resources for organizing student cohorts and CAE designation application guidance.

More information about CEDI project and opportunities to engage/participate is available at: https://www.tntech.edu/ceroc/outreach/cedi.php

FUN CORNER

Grant Brown:

Why do cybersecurity students throw the best parties? They're great at social engineering.

Jesse Holland:

What do you tell a hacker after a bad breakup? There are plenty of phish in the sea.

Mimi Vertrees:

Why doesn't Superman fight cybercrime? He's afraid of Krypto Currency!

Winston Phillips:

I would tell you a joke about UDP, but you may not get it....

ACROSS THE WIRE
Compiled by Jake Graves

Apple was recently caught amping up their security due to an exploit that was used on the iMessaging app. This new security feature was called "Blast Doors" and was written in a coding language known as "swift" because of its safe memory language. This new service inspects all incoming information and can detect malicious software before it even interacts with the OS. This new system allows for increased security with no extra steps from the user. It will take an attacker a day and a half to do what they were able to do in minutes now according to a google project zero researcher.

source: https://thehackernews.com/2021/01/google-uncovers-new-ios-security.html

5 Cybersecurity statistics for 2021:

1. Global cybercrime damage predicted to hit $10.5 trillion annually by 2025.

2. Cybersecurity spending will exceed $1 trillion from 2017 to 2021.

3. The world will have 3.5 million unfilled cybersecurity jobs by the end of 2021.

4. Ransomware damage costs are predicted to grow more than 57X from 2015 to 2021.

5. The human attack surface will reach 6 billion people by 2022.

source: https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2021-to-2025/

A new and more advanced phishing kit has been created and used by cybercriminals. The kit goes by the name "LogoKit", and it has the ability to copy logos and pictures. The kit does this by looking at the URL keywords and searching for the logo in a database like google for an image that relates to the company. The kit can even go so far as to mimic the log in page of many sites. Many people do not check the URL for their logins when logging into a website that looks like what they normally lof into, so this is a very large threat.

source: https://blog.knowbe4.com/heads-up-new-phishing-kit-spotted-on-over-700-domains

As many as 8 different counties have joined forces against the cyber threat of Emotet, a email based malware that is behind many botnet spams and ransomware attacks. This is a huge victory because this particular malware has been active and used for more than a decade, and with its huge versatility, it was a force to be recokend with. After more than two years of tracking and mapping the servers, the infrastructure of Emotet has been located and the servers are confinscated. The members responsible for the maintenance and use of Emotet can be facing 12 years in prison! Globally, Emotet has cost the world 2.5 billion. Emotet is set to be completely wiped off the map by april 25, 2021.

source: https://thehackernews.com/2021/01/european-authorities-disrupt-emotet.html

As the cases of COVID-19 rise, so do the risks of identity theft in 2020. In the year 2020, identity theft has doubled from 2019. As the government has given out aid and support to those in need, many have attempted to create fake personas in order to get more money. A report says around 394,000 people were caught getting government benefits fraud. While there are more people doing this, on the other side, there are many who suffer from this. People who are at home also suffer from theft. Many people who are not as competent with technology are suffering at home with sending personal information to who they think are companies. It is important to know who you are sending your information to, especially during these times.

Source: https://www.darkreading.com/attacks-breaches/ftc-id-theft-doubled-in-2020/d/d-id/1340042

SECURITY RESEARCH SHOWCASE

Blockchain for Privacy-Preserving Smart Grid Applications

Recently, **Dr. Muhammad Ismail** and his research team have been carrying out research work related to security and privacy issues in the blockchain with applications to the smart grid such as demand-side management and electric vehicle charging coordination. Such efforts have led to the recent acceptance of a research paper of Ph.D. student Mr. Mahmoud Abouyoussef under the supervision of Dr. M. Ismail in the IEEE International Conference on Communications (ICC) 2021, an IEEE flagship conference. The title of the paper is: "Blockchain-based Networking Strategy for Privacy-Preserving Demand Side Management". In this paper, **Mr. M. Abouyoussef** and **Dr. M. Ismail** pointed out that while existing blockchain platforms can support user anonymity, they cannot support data unlinkability. In this sense, while existing blockchain platforms support user anonymity through the adoption of public and private keys, all the submitted transactions by a given user can eventually be linked to the same key. This results in a severe concern when adopting such blockchain platforms to support privacy-preserving demand-side management. The paper by Mr. M. Abouyoussef and Dr. M. Ismail addresses such a concern by proposing a novel networking strategy based on a private blockchain. The proposed strategy employs a group signature to ensure the customer's anonymity and data unlinkability. Further, a novel decentralized random number generation scheme is proposed to support customer-utility interaction for demand-side management, billing, and auditing while ensuring data unlinkability. In their paper, Mr. M. Abouyoussef and Dr. M. Ismail presented an implementation of the proposed blockchain-based strategy, investigated its scalability, and provided low-bound empirical expressions on computational time and storage overhead. Simulation results demonstrated that the proposed strategy can be successfully implemented to support privacy-preserving fine-grained data exchange over a large neighborhood area.

HOMELAB SHOWCASE

I have set up a CTF challenge involving Discord bots. The process of creating them taught me a bit about how vulnerabilities might exist in NodeJS and even about what built in security measures exist (That I had to circumvent). The bots will stay running for a little while, so I will leave a breadcrumb to the challenge:

624539695a326c61546a685254793932
6469357a5a3252796148687a4c793836
614756706158633d.

Conttributed by: Jacob Sweeton

SECURITY TOOLBOX

Wireshark – Wireshark is a free open-source tool that is used for capturing and analyzing network traffic. All network traffic consists of packets and frames. Wireshark makes a carbon copy of all packets and frames that pass through a point in a network without interrupting the flow of information. The captured packets provide a vast amount of useful upfront information like, Source and Destination IPs, type of protocol used, and time it took to travel. Wireshark also provides an in-depth breakdown of individual packets that can provide a user more detailed information like the URL visited, message sent/received, application used, etc. With all of this useful information, Wireshark makes it easier for network administrators to see suspicious activity and even in-progress attacks on their network.

*DO NOT USE THESE TOOLS ON NETWORKS YOU DO NOT OWN OR DO NOT HAVE PERMISSION TO EDIT!

Contributes by: Jeremy Potts

OPPORTUNITIES IN CYBER

National Cyber League (NCL) Competition is powered by Cyber Skyline, a leading cloud-based cybersecurity skills evaluation platform offering a safe environment for students to practice their cybersecurity skills. Together with NCL, Cyber Skyline presents the biannual NCL Competition. Spring Season Registration is Open!

Please note that registration closes at **11:59PM Eastern Time March 5** and with late March 9. https://nationalcyberleague.org/competition

EPB summer Internship: EPB has summer internship openings for IT, engineering, graphic design, and accounting. Applications to be completed by mid-April. https://epb.com/

TVA Internship: Two representatives from TVA will be participating in the virtual Engineering Fair on March 3, 2021. They would encourage anyone interested in a summer internship or a future position with TVA to sign up for a time slot through the HNADSHAKE app to meet with either of them!

The US Cyber Challenge: The US Cyber Challenge's 12th annual CyberQuests competition is now open. This FREE online competition was designed to see how competitors rank against others throughout the nation. Being recognized as a top performer, the best competitors are invited to join one of our summer cyber camps and compete in our advanced CTF – a definite resume boost and a badge of honor recognized by America's leading employers. The competition is open now and will continue to March 14. For more information, to register and to compete – visit www.CyberQuests.org

NSA GenCyber Camp by CEROC: CEROC is seeking cybersecurity students to work for the NSA Gen Cyber camp (https://www.gen-cyber.com/) for high school students to be held on campus during the last week of May. If you are interested, please email ceroc@tntech.edu

WiCyS Student Volunteer Scholarship (Deadline TODAY): The eighth annual WiCyS conference is set to be held September 8-10 at the beautiful Gaylord Rockies in Aurora, Colorado. The call for presentations for workshops, tech talks, panels, lightning talks and student posters are OPEN now until March 1 deadline as are the applications for student scholarships, faculty lodging grants, the BIPOC Fellowship Award, and the Veterans Fellowship Award. All students MUST apply for WiCyS scholarship to attend the conference. QR code for tech students! https://www.wicys.org/events/call-for-participation/ is link for call for presentations

CyberStart: SANS institute is offering our WiCyS student chapter leaders the ability to give away up to 250 free licenses to CyberStart Game to our interested students to help them prepare for the Cyber FastTrack scholarship competition. CyberStart Game is a gamified learning platform comprised of over 200 interactive challenges that teach students about cryptography, web exploitation, social engineering, steganography, XSS, SQL injection, python, and much more. Students playing CyberStart can participate in Cyber FastTrack, which is an online scholarship competition created by experts at the SANS Institute. It is a 2-day Capture-the-Flag competition, with the chance to win one of 400 $1,000 cash scholarships and up to $21k of certified professional cybersecurity training that makes your resume more desirable for employers. Use QR code to sign up!

Give us your feedback about EaglesReach!