Cyber Eagles Reach Newsletter

Term: Spring
Date: March 15, 2022

Editor: Jake Graves, Computer Science

Cyber Club Happenings

by Warren Proctor

On February 24th there was a Cyber Eagles meeting discussing different tools used for both defense and offense. Mike Soare, one of the defense leads, took to the stage to explain Snort. Snort is an open-source intrusion prevention system that uses a series of rules that help malicious network activity and uses those rules to find packets that match against them and generates alerts for users (snort.org). To put it differently this tool can keep track of what is in your system and alert you of suspicious activity. Then Jesse Holland taught the Cyber Eagles in attendance how to use Wireshark. Wireshark is a free open-source packet analyzer that allows the user to capture and monitor network traffic (wireshark.org). This tool is unique as it can be used with both defense and offence. It is also commonly used in instant response scenarios.

The members of WiCyS are gearing up for their 2022 conference in Cleveland, OH. The conference will run from March 17-19 and will allow the students who got the honor to attend an excellent experience to learn and grow as community members as well as cyber specialists. When asked about her experience from last WiCyS Asia McKissack comments, "During the WiCyS conference, I met a bunch of new people and learned a lot of new things. Before the conference, I didn't know a lot of cyber majors and that was difficult at times, so meeting people that I could relate to was exciting! Also, seeing all the women involved in Cyber-Security was reassuring, and I'm looking forward to going again this year!" We wish all those going to WiCyS this year safe travels and hope they have a wonderful time!

QR Codes

Scan this QR to make sure that you do not miss and issue!

Scan this QR code to become a member of the Cyber Eagles

Message from CEROC

A Door unopened is merely a Wall!

When you see doors of opportunities around you, you must gather courage to open them and explore what's behind. You have to get your feet across the other side to take chances. Come out of your comfort zone and engage. If we don't' open the doors, aren't they same as the walls?

Dr. Ambareen Siraj, Director, CEROC

What is an SQL Injection?

Brought to you by: Asia Mckissack

SQL injection, also known as SQLI, is a common attack vector that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed. This information could include any number of items, including sensitive company data, user lists or private customer details. The impact that SQL injection can have on businesses is extensive. A successful SQLI attack may result in unauthorized viewing of user lists, the deletion of entire tables, and in special cases, the attacker could gain administrative rights to a database. All of those things listed could be extremely detrimental to a business. While this could be used to attack any SQL database, websites are the most frequent targets. What is exactly an SQL you might ask; well, an SQL is a standardized language used to access and manipulate databases to build customizable data views for each user. SQL queries are used to execute commands, like data retrieval, updates, and record removals. There are also different types of SQL injections, In-brand SQLI (Classic), Inferential SQLI (Blind), and Out-of-band SQLI. You could also classify SQL injection types based on the methods they use to access backend data and their damage potential.

Source: **https://www.imperva.com/learn/application-security/sql-injection-sqli/#:~:text=SQL%20injection%2C%20also%20known%20as,lists%20or%20private%20customer%20details.**

Campus Career Fair

by: Jake Graves

As you probably have heard, the engineering career fair here at tech happened on Tuesday, March 8. Don't let the title of engineering fool you, this is a very valuable event for both engineers and computer science majors alike. With large companies like Fast Enterprises and FedEx, the employment opportunities do not stop with just your major. If you are a freshman or a sophomore and you think that the career fair is optional, you are going to need to change your mindset fast. This type of event can put you on the fast track to get an internship with huge companies and possibly even a job! If you were unable to attend this event, that is okay because Tech hosts at least one career fair per semester. If you have the opportunity to talk with employers, always take it, because you never know what they might tell you!

Scholarship Student Highlight

Hallie Sevier

Hey! I'm Hallie Sevier and I am a first semester senior here at tech from Livingston, Tennessee. Over the course of my years at Tech so far I have competed in many CTF competitions and outreach events such as GenCyber and Cyber Discovery Day. I plan to graduate from Tech with my Masters in December 2023. As a freshman, I remember looking up to the upperclassmen and hoping that one day I could accomplish as much as them. And now, I am a CyberCorp: SFS Scholar and WiCyS Vice President. My advice for students is to go do what YOU want to do, and don't let anyone (that also means yourself) convince you otherwise. Imposter syndrome and feeling intimidated is a real thing, and it took me a long time to realize that I wasn't the only one with those feelings. The SFS scholarship is one of the things that helped me grow into who I am today and gave me the opportunity to really focus on what I was passionate about. Everyone here at CEROC are great and intelligent people, and if you haven't had a chance to get involved at CEROC yet, you should.

Cyber Events Across the World

Brought to you by: Asia Mckissack

The events happening in the Ukraine are frightening and terrifying but details have come out about a new nation-state sponsored phishing campaign that uncovered setting its sights on European governmental entities, in an attempt to get intelligence on refugees and supply movements in the region. An enterprise security company called Proofpoint detected the malicious emails on Febuarry 24th and labeled the social engineering attacks "Asylum Ambuscade". The email included a malicious macro attachment which utilized social engineering themes referencing to the Emergency Meeting of the NATO Security Council. The email also contained a malicious attachment that attempted to download destructive Lua malware named SunSeed and targeted European government personnel assigned with managing transportation and population movement in Europe. These discoveries helped on an advisory issued by the State Service of Special Communication and Information Protection of Ukraine, which was warned of the phishing messages that were targeting their military personnel with ZIP file attachments with the goal of stealing sensitive information. This comes as Russia's intense military invasion of Ukraine has taken over the cyberspace, with hacktivists, cybercriminals, white hat researchers, and technology companies picking a side. Another security company called Avanan came out and said that they witnessed an eightfold increase in email-borne attacks originating from Russia.

Source: https://thehackernews.com/2022/03/hackers-try-to-hack-european-officials.html

PHD Student Highlight

Ahsan Ayub

Hello, my name is Ahsan Ayub (pronouns: he/him). I am a Ph.D. student in the Department of Computer Science under the supervision of Prof. Dr. Ambareen Siraj with an emphasis on Cybersecurity and Data Science. I have been working at CEROC as a Graduate Research Assistant since Fall 2018. In addition to my research work, I have been appointed as a Security Engineer (Intern) at AllianceBernstein, a global investment management firm, since January 2022. At CEROC, I mainly contribute to the experimental research of both static and dynamic malware analysis for ransomware to propose multi-layered endpoint protection by incorporating Data Science and Reverse Engineering techniques. Additionally, I collaborate with the external security researchers in the industry to initiate and review the scope of research, perform experimentations, observe its progress, and analyze the empirical findings. I believe a solid foundation in core Computer Science concepts (e.g., Programming, Data Structure and Algorithms, Operating Systems, and Computer Networks) is paramount to excel in Cybersecurity. Additionally, obtaining security certification(s) in the desired career path, e.g., CompTIA Security+, before your graduation is considered to be a plus. I wish you the best in your academic journey at Tech, as well as your pursuit of a job.

Scholarship Student Highlight

Jesse Holland

My name is Jesse Holland. I am a second-year master's student from Pikeville Tennessee. I have not been at tech long, but I have thoroughly enjoyed my time here so far. Tech has given me access to all of the resources I could ever need. The professors have all been available and willing to help me learn and the people I have had the privilege of working alongside have always been willing to help me when I was struggling. My advisor is always pushing me to be better and I have come to call many of my peers friends. The community around tech has been very conducive to my learning and I feel at home. As a Cybercorp: SFS Student, my education has come first. The scholarship has allowed me to focus solely on my academic experience. This is a flexibility that I would not have otherwise, as I would need to work to fund my education. I am now able to complete my master's in only two years. Without the scholarship, I would have been set back many years. My advice: Get involved. The best opportunities arise while you are helping others.

Current Student Highlight

Grace Harris

Hi! My name is Grace Harris. I am a non-traditional student from East TN. I was very intimidated by Tn Tech when I first transferred. But since about the second month in my first semester I began to realize that my fears were all for not and that everyone had the same goals of working together and creating paths of success with one another. Since being at Tech different great opportunities have presented themselves and faculty members have worked hard in encouraging me to break out of my comfort zone and jump into these opportunities with both feet. Along with that I have received the TTU Junior/Senior Endowed Scholarship in Computer Science. With the scholarship the financial pressure in continuing my education have significantly lowered thankfully. When I graduate, I look forward to pursing a career in the field of Cryptography. If there was any advice, I would want to give other students it would be: Don't say no to the opportunities you think are impossible. Trusting your instincts will lead you to success. And the last thing would be you are never alone in your struggles, someone will always be there for you at Tech. Cheesy but it's true.

CEROC Project Highlight

After a several month hiatus, CEROC has resumed is cyber risk assessment program in cooperation with the 3-Star Industrial Assessment Center. The program, funded by the Department of Energy, provides cybersecurity risk assessments and industrial plant assessments for small to mid-ranged manufacturing companies in the region. During the COVID mitigation period, CyberCorps (SFS) and Department of Defense Cyber Scholarship (CySP) students have been working to redesign the evaluation system. Work-Based Learning students from White County have also contributed to the work of updating the evaluation criteria to reflect current NIST SP 800-171 and CMMC v.1 Level 1 & 2 criteria. The current risk assessment team is working with a client using a spreadsheet-based method which will inform features to be proposed for the next development iterations for the online system.

The system, originally developed by a Computer Science graduate student, evaluates the cyber security posture of an organization across twelve critical cyber areas ranging from authentication/authorization processes, cyber policy, physical security, to configuration management. In addition to the on-site inspection, the assessment team also interviews key members of the organization including both technical and administrative staff. The final product of these reviews allows companies to conduct systemic improvements to their cyber positioning as they face new requirements to conduct business with federal agencies.

The cyber risk assessment team includes Elena Becker (DoD CySP), Tym Brandel (SFS), Kaitlyn Cottrell (SFS), and Matthew Brotherton. This team includes members of the software engineer group which began the rewrite of the new online system last year. They will also be working with a new software engineering team this spring and fall semester to continue the work of SB-CSET version 2. "The project is an excellent example of how our service-minded, cyber students are using their skills to develop software and processes to improve the security of our regional cyber infrastructure," stated Eric Brown, assistant director for CEROC.

Solar Winds Attack

Brought to you by: Warren Proctor

SolarWinds is a major firm for information technology in the US. This already makes Solar-Winds an excellent target for malicious actors, but the reason the SolarWinds attacks were so devastating is because they spread to all of their clients as well. Foreign hackers were able to hack and spy on companies such as FireEye, and upper-level government officials and organizations like the Department of Homeland Security and the Treasury Department. So why did this attack happen? In early 2020 malicious actors were able to break into Solar Wind's systems that were based out in Texas. This system called "Orion" is commonly used by companies to manage their IT resources. How did their customers get involved? Well software providers regularly send out updates to their systems to either fix bugs or add new features, and as early as March of 2020 SolarWinds sent out software updates to its customers with hacked code. This code created a backdoor in their customers information technology systems, and with it provided access for the hackers to break in and steal information. Of the 33,000 customers mentioned above around 18,000 unknowingly downloaded this meddled update that left them vulnerable to hackers. While more than 80% of the victims targeted were nongovernment agencies, US agencies-including parts of the Pentagon, the Department of Homeland Security, the State Department, the Department of Energy, the National Nuclear Security Administration, and the Treasury-were attacked. Non-government agencies such as Microsoft, Cisco, Intel, and Deloitte were attacks along with the California Department of State Hospitals. The list is as impressive as it is devastating. Considering this hack was done so stealthily some victims may not know whether they were hacked or not. It could take years before the systems affected by these attacks are secure again.

Source: **https://www.businessinsider.com/solar-winds-hack-explained-government-agencies-cyber-security-2020-12**

Talks On Your Own Time

Got some time to kill? Here are a couple of resources to let you listen to professionals talk about topics in cyber!

CAE Tech Talk resources

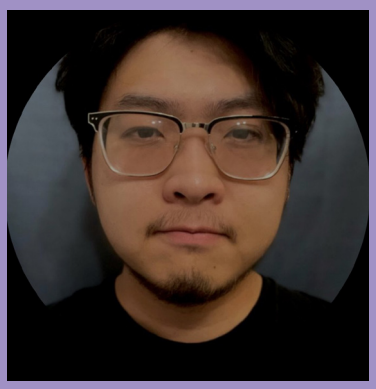
WiCyS Webinar Series

Join Our Community

Have you joined the Cyber Eagles discord yet? We have social events there too! All computer science students are encouraged to come hang out and socialize with their peers. These events range from sports to video games, and they all are with people you will see in your classes! Join us and build a strong community of peers who you can discuss internships, schoolwork, and projects with! Everyone you meet in these meetings ready to help you if they can, or point you to the correct resources if they don't understand. If you are having a problem, odds are one of these cyber students can help you out!

Some of our students working hard in one of our cyber intrest groups!

Graduating Student Highlight



Dee Zhao

Hello! My name is Dee Zhao, I'm currently a graduate student in cybersecurity. I'm originally from California, but I've lived in multiple places growing up. My family and I eventually moved to Nashville in 2010, and I have lived in Tennessee since then. I transfered to Tech from Volunteer State community college in 2017. My time at Tech has been very enjoyable, and is full of wonderful memories and opportunities. I have also been fortunate to make some lifelong friends in my time here. In fall of 2020, I started working under Dr. Siraj as an assistant on a federal grant, where I had the opportunity to meet with a lot of people within the industry. I am very grateful for her guidance in my educational journey, and for her continuous belief in me. I'm graduating this semester, and heading into the security industry as a penetration tester.

Cyber Law

Brought to you by: Jake Graves

On Tuesday, March 1st, the U.S. Senate passed the Strengthening American Cybersecurity Act (SACA) unanimously. This act is meant to strengthen the cyber infrastructure of the U.S. This act will allow the U.S. to be better prepared for new cyber-attacks that are plaguing civilian and government businesses alike. All those who are affected by an attack to contact the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and alert them of any ransomware payments as well. The affected companies and organizations are also asked to save any data from the attack for CISA to review. This act will allow the U.S. to have a more secure understanding of the ever-evolving world of cybersecurity and the cyber battlefield.

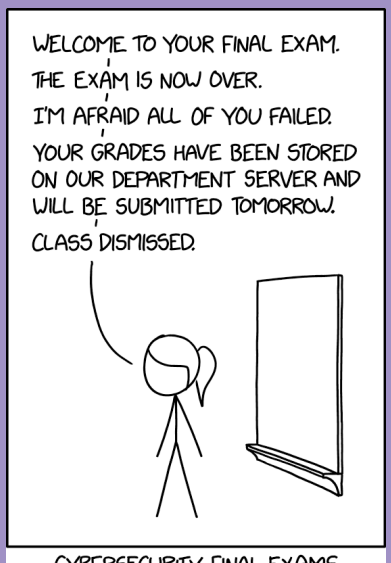
Source: **https://thehackernews.com/2022/03/us-senate-passes-cybersecurity-bill-to.html**

Fun Corner

Cyber Joke:

What's the best way to catch a runaway robot?

Use a botnet.



CYBERSECURITY FINAL EXAMS

Source: **https://xkcd.com/2385/**

Current Student Highlight

Joshua Foster

Hello! My name is Joshua Foster and I am originally from Winchester, Tennessee. I am currently a Junior going for my Bachelor's in Computer Science with a concentration in Cybersecurity. I am participating in the Fast Track program in hopes that I will participate in the graduate Computer Science program. In my first two years here at Tech, I struggled to find myself in the Computer Science program. It wasn't until I got more involved that I truly came to love my studies and the cybersecurity community here on campus. I started working with CEROC a year ago and it has opened the door to opportunities I never would have known about before. Since then, I have met incredible new people in the program, and I have grown closer to my professors who push me to be a better student and more well-rounded person. My advice to all students would be to get involved in activities outside of classroom. Studying cybersecurity here at Tech provides you with so many opportunities to grow in a fun way. With clubs, work, and competitions in the field of cybersecurity, there is something for everyone.

Securing Modern Cyber Infrastructure against Hardware Attacks

Faculty Supervisor: Dr. Syed Rafay Hasan

Students: Tolulope Odetola, Adewale Adeyemo, Travis Sandefur, Jonathan Sanderson

Artificial Intelligence (AI) has very timely evolved to help sifting through the tremendous amount of data, which has been changing the landscape of many research domains. To exploit the full potential of AI, it needs to be readily available to the users. This requires faster and reliable availability of AI that can benefit the nodes and edges of modern Internet of Things (IoT), called as Artificial Intelligence of Things (AIoT). Scope of AIoT will bring amazing experiences, e.g. using head-mounted devices one will be able to get real time information about the building they are seeing, or identify a unique bird they glimpsed in real time. The possibilities are endless, AIoT promises to bring many new applications in several domains ranging from autonomous vehicles, AI-enabled smart cameras, robotics, smart cities, cashier free retail outlets, etc. However, AIoT achieves this success by distributing the complex task of AI to different machines, this methodology is commonly known as distributed deep learning. Due to supply chain limitations it is impossible to maintain high trust level of these devices in AIoT systems with distributed learning. An adversary can take advantage of this situation and include some bug in the hardware units, which can sniff the secret information under the radar without getting detected or even sabotage the system. Securing modern cyber infrastructure (e.g. AIoT) against such hardware vulnerabilities is one of the most challenging cybersecurity problems. Dr. Hasan, with his students, is investigating these threats in modern AIoT systems. Their research is helping the research community understand the vulnerabilities in such distributed AI systems. His research students work on the modern distributed AI network and introduced several new hardware bugs that an adversary may exploit. They are also working towards possible software, hardware and heuristic approaches to save these systems from such attacks.

Homomorphic Encryption

Brought to you by: Warren Proctor

A new vulnerability has been found with homomorphic encryption named the “first side-channel attack.” This was demonstrated by a group of academics from the North Carolina State University and Dokuz Eylul University. For those who don’t know, “Homomorphic Encryption is a form of encryption that allows computation to be performed directly on encrypted data without having to decrypt it,” (Lakshmanan). This attack can be used to leak data during the encryption process. The next generation of encryption technologies is not safe from these side channel attacks explains Aydin Aysu, an author of the study who goes on to say, “Basically, by monitor- ing power consumption in a device that is encoding data for homomorphic encryption, we are able to read the data as it is being encrypted.” This form of encryption is used to share sensitive data with third party services for processing while the underlying information remains encrypted preventing the service provider access to the information. An example of when this would be needed would be when working with commercial cloud environments. The overall goal is to provide end-to-end encryption for data storage and computation services where the data owner does not have to reveal the secrets with the third-party source.

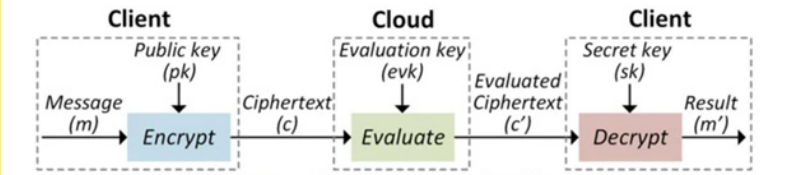


Fig. 1. Homomorphic encryption functions at the client and the cloud. The public key (*pk*) encrypts the message (*m*) to generate the ciphertext (*c*) and the secret key (*sk*) decrypts the received *homomorphically evaluated* ciphertext (*c'*) – both operations execute on the client’s device while *homomorphic evaluations* execute in the cloud.

Source: **https://thehackernews.com/2022/03/researchers-demonstrate-new-side.html**

Accolades

- R. Ujiie, V. Kholodilo, B. Northern, D. Ulybyshev. "Secure Monitoring and Notification System for Cloud Infrastructures", IEEE SoutheastCon 2022 conference, April 2021. Accepted.
- Aghili, Seyed Farhad, Mahdi Sedaghat, Dave Singelee, and Maanak Gupta. "MLS-ABAC: Efficient Multi-Level Security Attribute-Based Access Control scheme." Future Generation Computer Systems (2022).
- Dibyendu Brinto Bose, Gerald Gannod, Akond Rahman, Kaitlyn Cottrell, "What Questions Do Developers Ask About Julia?" to appear in the ACM Southeast Conference (ACMSE) 2022
- Dibyendu Brinto Bose, Kaitlyn Cottrell, Akond Rahman, "Vision for a Secure Elixir Ecosystem: An Empirical Study of Vulnerabilities in Elixir Programs" to appear in the ACM Southeast Conference (ACMSE) 2022
- Gupta, Maanak, Smriti Bhatt, Asma Hassan Alshehri, and Ravi Sandhu. "Access Control Models and Architectures For IoT and Cyber Physical Systems." Springer Book 2022.
- Gupta, Maanak, Ravi Sandhu, Tanjila Mawla, and James Benson. "Reachability analysis for attributes in ABAC with group hierarchy." IEEE Transactions on Dependable and Secure Computing (2022).

Other Awards

- PhD candidate Farzana Ahamed Bhuiyan, who is supervised by Dr. Akond Rahman is expected to defend her dissertation on March 11. She will join as a research scientist at Facebook starting in May. Her research was partially supported by CEROC and the U.S. National Science Foundation (NSF).
- Dr. Maanak Gupta has been elevated to IEEE Senior Member.
- SFS scholar Kaitlyn Cottrell, who is supervised by Dr. Akond Rahman got two papers accepted.
- Farzana Bhuiyan successfully defended her dissertation.

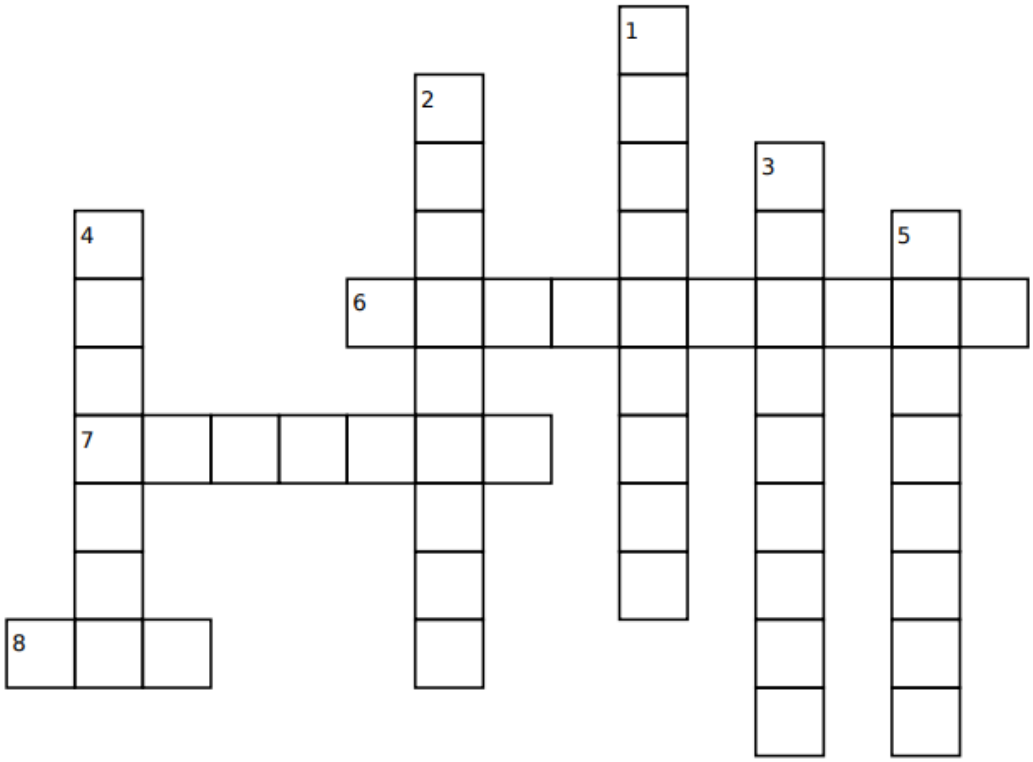
Club Meeting Information

- **Defense Group**: 3/24, 4/7
  -6-8pm In Prescott 411
- **WiCyS**: 3/22
  -11am-12pm In Prescott 225

If you haven't gone to any meetings yet, now is your chance! Consider coming to any of these meetings and get to know your cyber peers! Use the QR code on the front page to get into the discord for cybereagles for more club information!

- **ACM**: 3/29, 4/5
  -11am-12pm In Bruner 228
- **ACM**: 3/22, 4/5
  -6-8pm In Bruner 228

Crossword Puzzle



Across:

6. An open-source tool for exploit developments and penetration testing. Has exploits for both server and client-based attacks
7. The ability to prevent cyber attacks from infecting a computer system or device
8. Protects all onsite resources by channeling internet traffic through an external proxy server

Down:

1. This tool, formerly known as Ethereal, is an open-source network software that can efficiently analyze network protocols and enhance security in real-time
2. Proactive attack on hackers to cripple or disrupt their operations and deter future attacks
3. Is one of the best penetration tools used by organizations to scan their IT systems and networks for vulnerabilities
4. Is one of the most efficient packet sniffer security tools used to monitor and log TCP/IP traffic connected via a network
5. Blocks all known attacks at the boundary of the network

Graduating Student Highlight

Calen Kimmell

My name is Calen Kimmell and I am from Clarksville, Tennessee. I came to Tech in the Fall of 2017 to start my degree in computer science with a focus in cyber security and I will be graduating this May with my Master's. During that journey I was able to learn so much, but more importantly, I was able to build friendships and other connections. My time at Tech has meant so much to me, and being a part of CEROC and the SFS program has really inspired me to be the best version of my self that I can possibly be. I currently don't have a solid plan for where I will end up after I graduate, but I know Tech has fully prepared me to succeed wherever I do end up.

Faculty Highlight

Dr. Syed Rafay Hasan

Dr. Syed Rafay Hasan is an Associate Professor of Electrical and Computer Engineering at Tennessee Tech University (TTU). He received his B.Eng. degree from the NED University, Pakistan, and obtained his M.Eng. and Ph.D. degrees from Concordia University, Montreal, QC, Canada, all in electrical engineering. Before joining TTU, he was an adjunct-faculty with Concordia University, and Research-Associate with Polytechnique Montréal, Canada. Since 2011, he has been with the TTU. He has published more than 85 peer-reviewed journal and conference papers. He has been MS and PhD thesis supervisor of 12 students. His research interests include hardware security in Internet of Things and security of hardware implementation of deep learning on edge devices. He has received SigmaXi Outstanding Research, Faculty Research Award and Kinslow Outstanding Research Paper Award from TTU, and the Summer Faculty Fellowship Award from the Air force Research Lab (AFRL). His teaching and research projects are funded from many government and private sources, including NSF, AFRL, DENSO North America and Intel Inc., with total research funding in access of $1.7 million. He has been the session chair and committee member of several IEEE conferences, reviewer for several IEEE Transactions and NSF panel reviewer for SaTC, and ECCS divisions.

Security Toolbox

By Jake Graves

LastPass

LastPass is an all in one password and note manager built into your web browser. This addition to your search browser will not only keep your passwords safe and auto fill them into websites, but it will also suggest passwords for new accounts being made! Having strong and unique passwords is very difficult to do without writing them somewhere, so using a password manager is very useful for anyone in the field of cybersecurity.

Opportunities In Cyber

The Spring 2022 Cyber Quests competition began February 25th! This is a free opportunity to see how well you stand up against other cyber enthusiasts from across the nation. High scorers are listed in real time on the leaderboard. The top performers will be invited to the 2022 regional US Cyber Challenge virtual camps for award-winning training, direct interaction with employers and the opportunity to compete in each camp's CTF. The winning teams from there then move on to compete in the US Cyber Challenge National Championship CTF.

National Cybersecurity Management Case Competition hosted by the University of Colorado Colorado Springs College of Business is a great opportunity to showcase your Cybersecurity management skills! This competition will be held on April 7th! 1st place wins- $5,000, 2nd place wins $3,000, and 3rd place wins $2,000. You can find additional information with the QR link. Deadline to register your team is March 10th.

March CAE Tech Talk on March 17th starting at 1:00pm EST, the topic will be An Empirical Investigation of Static and Polymorphic Tactile Stimuli's Effect on Habituation to Cybersecurity Warnings. The second talk that will be held a little later at 2:00pm EST will discuss Fast-Flux Attack Detection using Machine Learning and Genetic Algorithms. Both talks are scheduled to last 50 minutes. All you have to do is login as a "Guest" and inter your name in order to listen in.

ACM-W panel discussion on "Mental Health, Wellbeing, and Self-Care," (March 16th, noon PT, 3PM ET) where leading women technologists open on the issue of personal struggles, growth, and resilience and provide strategies for managing such challenges. This panel will also explore the topic of self-care, small steps you can take yourself, and will cover when you may need professional help.

The Cybersecurity Emergent Research Symposium (CERS), which will be held on May 5th and 6th 2022 in Colorado Springs Colorado. This event is hosted by the University of Colorado and Colorado Springs College of Business. The symposium is structured as developmental and will involve engagement and feeback from nationally recognized cybersecurity experts. The research submitted can be at any stage of development. The event will select up to eight promising projects for in-person developmental work.