Cyber Eagles Reach Newsletter

Term: Spring
Date: February 15, 2022

Editor: Jake Graves, Computer Science

Cyber Club Happenings

by Warren Proctor

On January 27th Cyber Eagles hosted Dr. Stacy Powell who is the Chief Cybersecurity Research Scientist at Oak Ridge National Laboratory. The topic of discussion was how to secure systems against cyber threats and other vulnerabilities. He explained how systems are interconnected and how security needs to be applied in order to prevent these connections from being exploited. He also told an anecdote of how easily systems can crash when pressure is applied. In this case it was a malware stick used to test systems detection mechanisms, but when it was used it caused the whole system to go dark for a moment and caused a great deal of panic as workers thought it was a real attack. This talk was very eye opening and Cyber Eagles was honored to have such an awesome speaker.

Our WiCyS student chapter had their first meeting of the semester in January where the Tennessee Tech's women in cyber got together to play a nice competitive game of cyber trivia. This game held all the cyber basics to start building a toolbox of knowledge, and provided a light, approachable way to get started in the field. The second meeting of the semester students will be presenting lightning talks about topics such as JSON web tokens, the best cyber practices, advanced persistent threats and more. These talks will allow the students to practice getting in front of a crowd to present a cyber topic that interests them and gives those who participate a good public speaking experience.

Be sure to check out these amazing clubs! The times and meeting locations are all listed in this newsletter!

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

Another year full of hope! Yet still, the same pandemic in different forms…. but now, we can see the light at the end of the tunnel. For some, this pandemic has brought more than physical illness. It has contributed to mental health fallouts because of its various impacts. If you are one of them (and there are many), please know that this shall pass. Hang in tight. Find a friend/listener. Share your pain as it is a burden to carry it all alone. As someone who can relate, artist Demi Lovato's words: "You don't have to struggle in silence." Be un-slient, remain resilient!

Facing Burnout

Brought to you by: Warren Proctor

Starting a new semester may seem like a strange time to be talking about burnout, but if you start watching for the signs now when everything is gearing up, you will have a better chance of preventing burnout farther down the line. So, what is burnout? It is feeling disengaged, having blunted emotions, the loss of motivation or even hope, and this could lead towards depression. The best way to deal with burnout is with the Three R approach from Help Guide. **Recognizing** and watching for the warning signs of burnout. **Reverse** the damage by seeking support from friends, family, and counselors while working to manage your stress. Lastly work to build **Resilience** by taking care of your physical and emotional health. I have found that rethinking the way I look at tasks or changing my routines and habits can help stunt burnout and work to keep me motivated throughout the semester. In the end, remembering to take care of yourself can go a long way towards your success in school and in life. Take care of yourselves Eagles and have a good semester!

Source: **https://www.helpguide.org/articles/stress/burnout-prevention-and-recovery.htm**

Ways To Get Involved on Campus

by: Jake Graves

Joining clubs and meeting a whole new community can be a daunting task. Here is a short list of ways to get more involved in the cyber community here at Tennessee Tech:

1. Joining the Cyber Clubs will help you find peers with similar interests.

2. Talk with people in your computer science classes. You will probably be in more classes with them in the future, in which you can work through some of the more challenging courses together.

3. Check your email often. Many great opportunities are sent out by professors.

Why Your Grades Do Not to Define You

Brought to you by: Asia Mckissack

Going into this semester we have to remember to take care of our mental health. One way of doing that is by reminding ourselves that our grades don't define us. While in college we tend to look at our grades to prove how smart we are, and if they don't reflect how we think they should, we get angry or dejected. To try to combat this, I have found 4 reasons why our grades don't define us. The first reason is that our grades don't determine our potential. As I mentioned before, we tend to look at our grades to determine our intelligence but that's not the case. Our grades don't dictate how successful we will be in the future; just because you get a C in the course doesn't mean you won't be good at your job. The second reason is our grades don't show the amount of effort we put in. You could put so much effort into the class, but you still don't get the grade you wanted, but that shouldn't get you down because we don't get graded by our effort, just on what someone else thinks we can do. The third reason is in 3 years, no one will ask for them. The only thing that will matter is the qualifications you have, and how you perform. The last reason is not all learning is done in school. Just because you didn't get what you wanted in that class and feel dejected about your career doesn't mean you won't have the option to learn it again in the real world. Even if you don't get the grade you want, remember that it's not the end of the world. Looking at these reasons hopefully will remind you that your grades do not define you and your future.

Source: **https://jessicakatie.com/6-reasons-why-your-grades-dont-define-you/**

Three Signs You've Been Hacked

by: Warren Proctor

Because of the large variety of attacks malicious actors can pursue, there are many different signs that a system has been breached. Here are a couple big red flags to look for. First, an obvious one, a ransomware message takes over the screen. The best way to counteract this is having a reliable back-up system to prevent losing data. While the attackers might promise to release the effected systems, it does not mean they will restore them back to working condition. A second red flag is receiving a fake antivirus message. This is when a pop up informs the user that their computer has been infected. Sometimes it will even ask the user to call a toll-free number, or pressure them with a countdown before a force system restart. The best way to handle this is to just close the tab and restart the browser. This should fix the problem. If this does not work, you can restart your browser in incognito or private mode and move to a different page to stop the antivirus message from appearing. Another big sign that something is wrong is if antimalware, task manager, or registry editor is disabled. If one of these is disabled and the user did not do it themselves, then this is a clear sign of possible exploitation. The best thing to do is to perform a complete restore, but if the user wants to start with something a little less drastic then they can run Microsoft Autoruns or Process Explorer on a Windows computer to try to root out the malicious program. A general rule of thumb is to just keep an eye out for suspicious activity. If something goes wrong or begins acting weird and a restart does not fix the problem, then it might be a sign of a possible attack.

PHD Student Highlight

Shazibul Islam Shamim

I am Shazibul Islam Shamim, a Ph.D. student at Tennessee Tech in the Computer Science department. I was born and raised in Bogra, Bangladesh. I got my bachelor's degree in Computer Science and Engineering from Bangladesh University of Engineering Technology, Dhaka. After graduation, while working as a software engineer, I got the first-hand experience to face software engineering challenges in DevOps. Hence, pursuing a research-oriented career in Software Engineering to tackle the emerging challenges in DevOps was my next logical step. I joined Tennessee Tech in Spring 2020 as a graduate research assistant in the PASER group under the supervision of Dr. Akond Rahman, where I work in the area of DevOps security. Currently, I am investigating insecure practices in open-source Kubernetes repositories. I received a Bronze award in ACM ESEC/FSE 2021 for my research at Tennessee Tech. My research aims to help practitioners securely develop Kubernetes manifests to deploy their applications. I am privileged to interact with many intellectual students and faculty at Tennessee Tech, and it has been an incredible experience for me. As the whole IT domain is changing so rapidly, I suggest you to move out of your comfort zone to adapt to the changes and learn new tools and technology to build employable skills.

Identity Thief Behind Bars

Brought to you by: Asia McKissack

While on vacation in Greece in September 2020 Slava Dmitriev was arrested and extradited to the U.S. in January 2021. He was sentenced for access device fraud with the possession and sale of over 1700 stolen identities on the dark web. Dmitriev profited off of buying and selling people's stolen identities and thought that he was safe because he was overseas. The FBI is using this case as a reminder that the they will work with international law to get justice for victims. How Dmitriev did this, according to U.S attorney Erskine, was that he used the GoldenAce to buy and sell stolen identities, including social security numbers, names, and dates of birth on the darknet marketplace AlphaBay. From May 2016 through July 2017 Dmitriev sold 1764 items on Alphabay for approximately a hundred thousand dollars. Dmitriev also collaborated with the cyber-extortionist group "The Dark Overload." In June, he sent the TDO access credentials and in July 2017 Dmitriev received a spreadsheet from TDO contained approximately two hundred thou- sand identities. September 8th, 2020, Dmitriev was arrested in Greece. The following day, police got a search warrant on his residence and found his computer containing emails discussing the buying and selling of identities and social security numbers as well as a video about how to perpetrate identity theft. Dmitriev pleaded guilty on August 30th, 2021, and was sentenced to three years in prison followed by three years of supervised release.

Source: **https://www.justice.gov/usao-ndga/pr/canadian-man-sentenced-federal-prison-trafficking-stolen-identities-dark-web**

Current Student Highlight

Hayden Keller

Hey there! I'm Hayden Keller, and I'm a junior computer science and cybersecurity student from Roane County, Tennessee. I chose to come to Tech for a couple of reasons, but actually had no intention of going into cyber when I first got here. That was until I discovered how excellent the culture was around the department, and I haven't looked back since; we all take care of one another, and it's a perfect environment to grow and develop both as a person and a professional. Outside of class, I work as an undergraduate research assistant with a focus on Android and IoT malware analysis under Dr. Gupta. Additionally, I spend a lot of my time helping with CEROC outreach events like our GenCyber camp. As far as where I'm headed, my biggest passion lies in education, so I'm definitely looking at a PhD and becoming a professor. My advice to students is to seek community; if that's with the cyber department, great! If it's in Spanish club, awesome! It's unimportant. All that matters is you find a place for you that fosters growth and improvement. Strive to be a lifelong learner, and always pay it forward!

Cyber News Bytes

Merge between Nord Security and Surfshark—Will other VPN Providers Consider the Same Strategy?

Brought to you by: Alexandra (Apple) Lee

Nord Security, parent company of NordVPN, and Surshark finalize a merger agreement between the two cybersecurity companies to create the new company—Cyberspace. While both cybersecurity providers will continue to operate autonomously, this agreement will help direct the resources into providing both companies that'll create a safer Internet with accelerated innovation without compromising the authenticity of the brands.

Source: **https://cybernews.com/news/nord-security-and-surfshark-merge-to-create-the-largest-security-powerhouse/**

Good News: Russian Government Cracks Down on Hacker Group REvil

Brought to you by: Matthew Burst

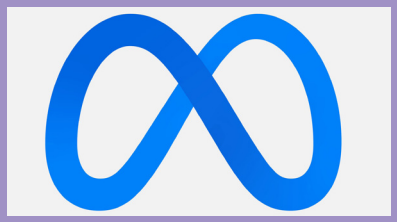
Following multiple ransomware attacks on US companies, the Russian government has finally neutralized the REvil hacker group. Members of the group were arrested and around 500,000 dollars in cryptocurrency were seized from them. For many years, Russia has been a safe haven for hacker groups, many of which target western businesses. These arrests send a strong message to hacker groups like REvil and show the possibility of government collaboration against these groups.

Source: **https://www.bbc.com/news/technology-59998925**

Facebook Cracks Down on Spies

Brought to you by: Asia McKissack

Meta, Facebook's parent company, kicked six alleged spy-for-hire "cyber mercenaries" off their site along with a Chinese law enforcement supplier. They accused the entities of collectively targeting about 50,000 people of surveillance. Meta had been following a month-long investigation which ended up with them removing 1,500 fake accounts linked to the spying entities, and during their investigation they saw engagement with and/or exploitation of alleged victims. With their findings, they decided to share it with other platforms and security researchers. They also issued cease-and-desist warnings to six of the groups and has warned targeted people in more than 100 countries. The global surveillance-for-hire industry targets people to collect intelligence, manipulate and compromise their devices and accounts across the internet. While the cyber mercenaries claimed that their services only targeted criminals and terrorists, Meta's investigation concluded that random journalists and critics of authoritarian regimes and more were affected. This means that many average people who posed no real threat were spied on by these for hire hackers. One of the more famous cases that was uncovered was involving Harvey Weinstein, who hired a cyber mercenary to spy on and intimidate a woman who he had wronged.



Source: **https://threatpost.com/facebook-bans-spy-hire/177149/**

Southeast Collegiate Cyber Defense Team

by: Kaitlyn Carroll

I was part of the team from CEROC that competed in the Southeast Collegiate Cyber Defense Competition, SECCDC, on Saturday, February 12th. The team was comprised of both graduate students and undergraduate students. Our team included me, Andy Brown, Nate Dunlap, Hayden Keller, Justin Presley, Mike Soare, Jacob Sweeten, and Mimi Vertrees. Our alternates and non-competiting team members included Trey Burkes, Tate Seyler, Evyn Price, and Ryan Brewer.

SECCDC is a competition wherein teams are given access to a competition network owned by a fictional company. Competitors have to secure while also being actively targeted by hackers. Competitors are also tasked with completing business injects and responding to any incidents that occur on the network. The competition is always a lot of fun, and it is a good way to practice your defensive cyber skills. SECCDC is challenging in many ways. It challenges not only your cybersecurity abilities, but also your business and professional skills, your organizational capabilities, and your ability to work under pressure. It does well in simulating a high-stress work environment. While difficult, SECCDC is a valuable experience. We had a wonderful time competing, and look forward to competition again in the future.

Club Meeting Information

- **Cyber Eagles**: 2/24, 3/10
  -11am-12pm In Prescott 215
- **Offense Group**: 2/17, 3/3
  -6-8pm In Prescott 411
- **Defense Group**: 2/24, 3/10
  -6-8pm In Prescott 411

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**: 2/22, 3/3, 3/8, 3/10, 2/24,
  -11am-12pm In Bruner 228
- **ACM**: 2/24
  -6-8pm In Bruner 228
- **ACM**: 3/10
  -6-8pm In Bruner 119

Heart Breaking Scams

Brought to you by: Warren Proctor

Tis the season for crimes of love, and this year a study has predicted Americans will lose roughly $800 million due to Valentine's Day scams. Those looking for love may actually be looking for a victim to exploit. Attackers use photos from across the web and look to gain the trust of their target. Once the trust is gained, they use this to get money, whether it be asking for gifts or claiming financial troubles, they will attempt to use this newfound connection for profit. They will delay any in person meetings and will claim to be working internationally or to be in the military. A keyway to spot these attackers is spelling errors in their claims and unruly persistence. The minute they ask for money it should be an automatic red flag. As cold as it is to say, also be on the lookout for sad background stories and cases of hard luck. Attackers will not hesitate to play on the empathy and kindness of their victims. To avoid being a victim, keep on the lookout for suspicious messages and requests and know you can reverse image search to see if the person you are seeing is who they say they are. To avoid romantic nightmares this valentine's day season be wary of who you are talking to and remember, if it seems too good to be true, it probably is.

Source: **https://abc11.com/romance-scam-valentines-day-valentines-how-to-spot-a/11544190/**

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!

Some of our students took a trip to do an escape room together!

Alum Highlight

Jeremy Potts

My name is Jeremy Potts, and I am from White House, TN. I graduated from Tech December of 2020 with my Bachelor's degree. I am currently employed at CEROC as one of their Cyber Range Engineers, and I am also enrolled as second semester graduate student pursuing my Master's degree. I started at Tech in fall of 2017. I knew that I wanted to enter the field of computer science but was undecided on the concentration path I wanted to take. I was extremely lucky in two ways my freshman year: 1. I received the Federal Work Study and 2. I was assigned to CEROC for the Work Study. It was through this program that I was originally exposed to cyber security. Through my student work at CEROC I was able to participate in lots of outreach events and extracurriculars that guided me to where I am today. If I were to offer one piece of advice to current students, it would be to involve yourself in as much as you reasonably can. You WILL feel like you don't know enough or aren't skilled enough, but the only way to overcome those feelings is to get in there and DO.

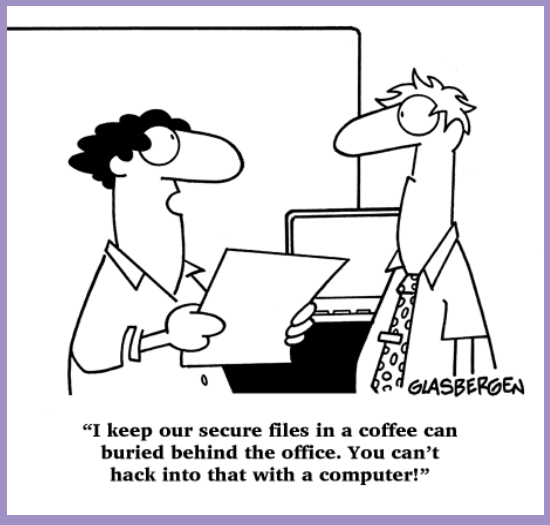
What is Catfishing?

Brought to you by: Warren Proctor

What is catfishing? This term was coined after the process that fisherman use to keep catfish moving after they are hooked, but in the cyber realm it is used to describe the creation of a false identity to trick others into giving them information or getting access to their systems. This can happen via dating apps or really any social media (not even LinkedIn is safe). This comes in the form of imagery. Catfishes will grab a photo from the internet and assume a new identity, or steal someone else's, and use that to exploit others. Catfishing is a personal crime. One might choose to catfish for revenge and to hurt others while another might simply want to experience being perceived as someone else. Regardless of motives though, claiming to be someone else is not okay, can hurt others, and is treated as a cybercrime. Catfishing should always be treated as a security threat to personal information. A concerning issue that we face is that there are no specific laws against catfishing, and this makes it harder for officials to catch the criminals. In conclusion, everyone should always be careful about receiving messages from unknown senders and treat the messages received with caution.

Source: **https://thebusinessprofessor.com/en_US/criminal-civil-law/catfishing-cybercrime-definition**

Fun Corner



"I keep our secure files in a coffee can buried behind the office. You can't hack into that with a computer!"

Source: **https://www.glasbergen.com/ngg_tag/i-keep-our-secure-files-in-a-coffee-can-buried-behind-the-office-you-cant-hack-into-that-with-a-computer/**

Scholarship Student Highlight

Daniel Simpson

Hello! My name is Daniel Simpson and I am a first semester graduate student here at Tech. My hometown is Burns, Tennessee. I transferred to Tech from Nashville State Community College in the Spring of 2020 and I hope to complete an M.S. in May of 2023. Most of my time here has been spent with the wonderful people I was introduced to through CEROC. The CyberEagles club and its special interest groups provided me a framework for peer learning that I had never seen before and it pushed me to learn new things and to get involved with cyber competitions that I never would have tried on my own. I cannot recommend these enough to new students. I am able to continue my education because I was allowed into the SFS program through CEROC. This has been a wonderful opportunity and I encourage interested students to apply. My current research is under Dr. Maanak Gupta on ML-assisted malware analysis with a focus on android and IoT malware. The best advice I can offer is to make time to try new things and apply for anything you are interested in. Displaying active interest opens more doors than you would expect.

Security Research at HPC and Systems Lab

Faculty Supervisor: Sheikh Ghafoor
Students: William A. Johnson, William Lambert, John Housley, Hallie Sevier, Halley Burnel

I am a professor at the department of Computer Science and my group's cybersecurity research in HPC and Systems lab focuses mainly on cyber-physical systems, including smart grid, industrial control systems, vehicular systems, and security of scientific workflow. One of our research projects involves Remote Attestation (RA) in embedded systems, where we focus on developing RA schemes that can be deployed across a wide variety of embedded systems with different hardware architectures, peripherals, and manufacturers. Embedded systems often fall victim to malware because they are not designed with security in mind. Unlike traditional computing systems, direct forensics methods cannot be used to detect a compromise, because embedded systems are often deployed in hard-to-reach locations, not designed to be disassembled, works under real-time constraints, and vulnerable to fileless malware. RA is a security protocol designed to help detect a malware compromise while a system is in operation.

The operations of current and emerging vehicles are controlled by hundreds of small purpose-built embedded computers called Electronic Control Units (ECUs). These ECUs communicate with each other using real-time network protocols, such as CAN, LIN, (LIN), and others. These protocols were not designed with security in mind and are vulnerable to attacks. We are working on several projects regarding security in vehicular echo system. One of our projects focuses on developing an extensible, innovative, and open architecture testbed (XiveNet) where researchers can simulate, test, and validate variety of protocols and system designs. Another project is focusing on developing secure CAN protocol, called SecCAN, that uses lightweight encryption and message authentication using segmentation-based shared secret group keys. We are also investigating adopting emerging protocols such as automotive ethernet and name data network in vehicle space. Our projects have been funded by National Security Agency, Oak Ridge National Laboratories, and SFS program.

Seperating Home From Work

Brought to you by: Jake Graves

During this pandemic, there have been many changes that we have had to become accustomed to. For example, working remotely from our homes which often begins as quite convenient. There are many benefits, such as no driving, no getting dressed for work, and you can usually have a lot more freedom. Unfortunately, over time, there can become some problems separating your workspace from your relaxing living space. luckily, there are several easy ways to give yourself the distinction from work and home life. Here are a few:

1. Find a quiet space to work away from home, such as the library. Working from home can cause us difficulty managing our time because our brain is torn between when to work and when to relax.
2. Track how much time you are working, and be sure to keep your hours consistent. The more unsure your hours are, the more unnecessary anxiety occurs because you are thinking of work on your off time.
3. The most important tip is be realistic in what you take on when it comes to work. When your superior asks you if you can do something extra, if you are already overwhelmed, do not accept!

Working from home can be quite a challenge in a number of ways! We all live very different lives, and we all work very differently too, but, if you work hard, you can achieve anything!

Source: **https://www.wework.com/ideas/professional-development/creativity-culture/how-to-keep-home-and-work-separate-while-working-remotely**

Accolades

- A. Adeyemo*, T. A. Odetola*, S. R. Hasan“Towards Enabling Dynamic Convolution NeuralNetwork Inference for Edge Intelligence”, accepted for publication in IEEE International Symposium on Circuits and Systems–ISCAS’22.
- A. Takiddin, M. Ismail, U. Zafar, and E. Serpedin. “Deep Autoencoder-Based Anomaly Detection of Electricity Theft Cyberattacks in Smart Grids”, IEEE Systems Journal, 2022.
- Adkisson, Mary, Jeffrey C. Kimmell, Maanak Gupta, and Mahmoud Abdelsalam. "Autoencoder-based Anomaly Detection in Smart Farming Ecosystem." In 2021 IEEE International Conference on Big Data (Big Data), pp. 3390-3399. IEEE, 2021.
- Akond Rahman and Tushar Sharma, “Lessons from Research to Practice on Writing Better Quality Puppet Scripts”, in 29th IEEE International Conference on Software Analysis, Evolution and Reengineering (SANER), 2022.
- B. Northern, D. Ulybyshev, T. Burks, M. Hatcher, M. Rogers, "Systems and Methods for Cyber Risk Assessment for Computing Systems", Provisional patent submitted, application approved by the Intellectual Property Advisory Committee (IPAC) of the University.
- Bhuyan, Bikram Pratim, Ravi Tomar, Maanak Gupta, and Amar Ramdane-Cherif. "An Ontological Knowledge Representation for Smart Agriculture." In 2021 IEEE International Conference on Big Data (Big Data), pp. 3400-3406. IEEE, 2021.
- J. Massengille, T. Burks, R. Mitchell, J. Tice, D. Ulybyshev, "Data Protection and Export for Transaction Ledgers in Permissioned Blockchain Platforms", IEEE 3rd Workshop on Blockchain-based Architectures (BlockArch 2022), in conjunction with International Conference on Software Architecture (ICSA) 2022. Accepted, in-press
- Md Ahsan Ayub, and Ambareen Siraj: “Similarity Analysis of Ransomware based on Portable Executable (PE) File Metadata,” Proceedings: IEEE Symposium Series on Computational Intelligence Conference (IEEE SSCI) held December 4th – 7th 2021, Orlando, FL.
- Mohammad Mehedi Hassan and Akond Rahman, “As Code Testing: Characterizing Test Quality in Open Source Ansible Development”, in International Conference of Software Testing, Validation, and Veriification (ICST), 2022.
- Sontowski, Sina, Nigel Lawrence, Deepjyoti Deka, and Maanak Gupta. "Detecting Anomalies using Overlapping Electrical Measurements in Smart Power Grids." In 2021 IEEE International Conference on Big Data (Big Data), pp. 2434-2441. IEEE, 2021.
- T. Sandefur*, S. R. Hasan “Framework to Benchmark CNNs (FaBCNN) for Processing Real-Time HD Video Streams on FPGAs”, accepted for publication in IEEE International Symposium on Circuits and Systems–ISCAS’22.
- Tolulope A. Odetola*, Katie M. Groves*, Yousufuddin Mohammed$, Faiq Khalid, and Syed Rafay Hasan. "2L-3W: 2-Level 3-Way Hardware–Software Co-verification for the Mapping of Convolutional Neural Network (CNN) onto FPGA Boards." SN Computer Science 3, no. 1 (2022): 1-25.

Think Before You Scan

Brought to you by: Warren Proctor

QR codes or "Quick Response Codes" can be seen everywhere but be careful just scanning and following the prompts. Cyber criminals can easily use these quick scannable links to steal login information, credit card or bank account numbers, and personal information too. The possibility for malicious attacks is endless considering these QR code generators are free online for everyone to access. The victim may believe they are downloading their favorite song or a restaurant menu and find that they have downloaded malicious software instead. Some quick tips when using QR codes are as follows: make sure to check the URL to see if it is the site you were intending to go to. Also make sure to download apps from their provider, and if you receive an email stating that you must complete a payment through a QR code contact the provider to verify. Most phones have a QR code scanner built in, so it is unnecessary to download an app. Convenience often allows for attackers to take advantage of a vulnerable party. To avoid an attack always remember to check the legitimacy of the QR code before you give out any information.

Source: **https://www.hawaiinewsnow.com/2022/02/09/what-tech-fbi-warns-cyber-criminals-using-qr-codes-steal-information/**

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

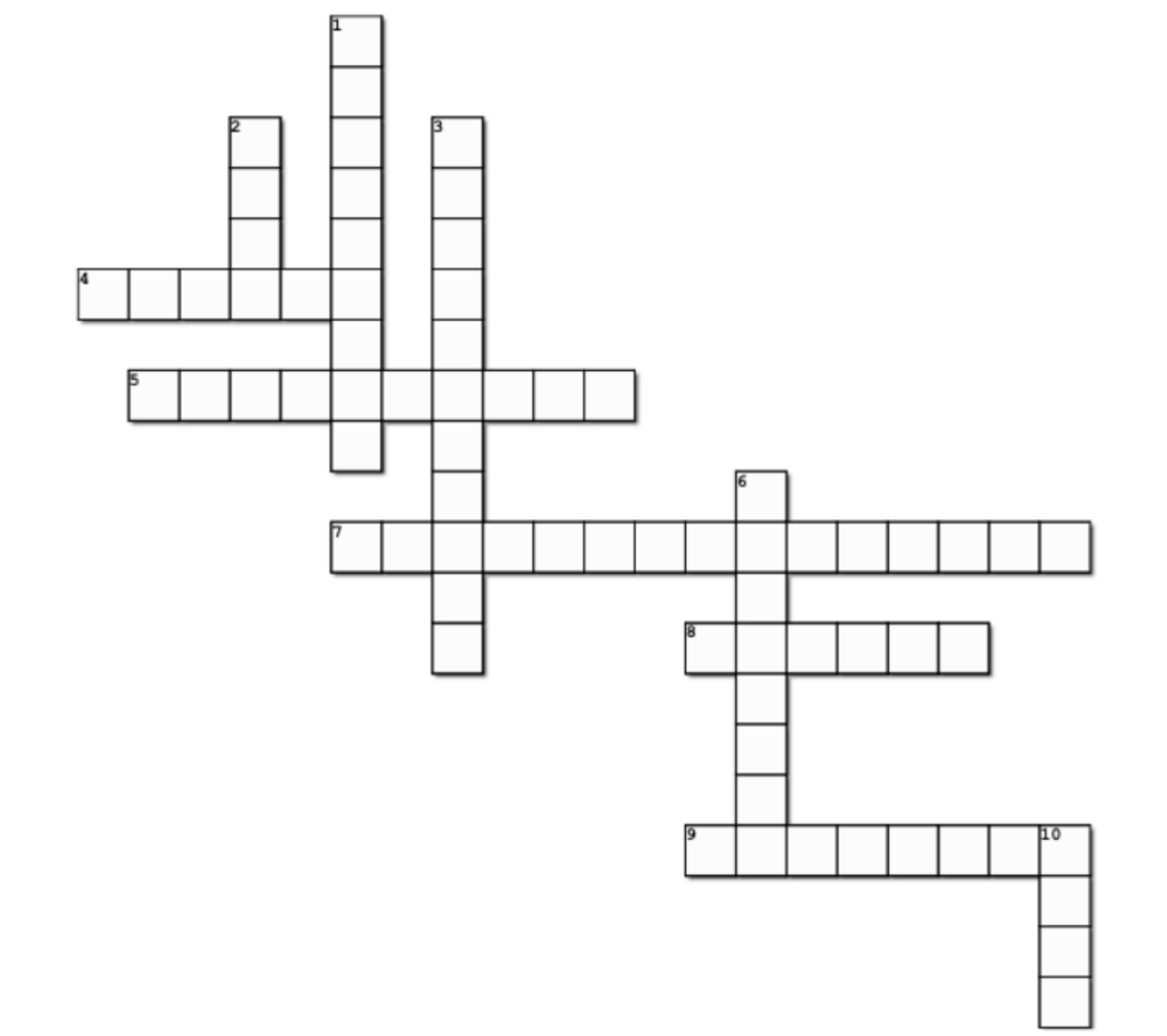
WiCyS Webinar Series

Faculty Highlight

Susmit Shannigrahi

I am an assistant professor in the Computer Science department and leads the next-generation networking lab (https://tntech-ngin.net). Before joining the CS department, I was a graduate research assistant at Colorado State. The tech experience has been very rewarding. I enjoy teaching networking and systems topics. I also enjoy advising undergraduate and graduate students in research. My advice to the students will be to explore different things and enjoy your time in school. Finally, we have paid positions at all levels (undergraduate, masters, and Ph.D) - if you are interested, drop me a note. We also meet every Friday in Bruner 407 - everyone is welcome to join our group meetings. We discuss cutting edge networking papers and projects we are working on. You can learn more about our work here: **https://tntech-ngin.net**

Crossword Puzzle



Across:

4. Language used for game Development.
5. File format that the computer can read
7. Type of selection control mechanism used to allow the value of a variable or expression to change the control flow of a program.
8. Language the computer can understand.
9. An electronic or electromechanical hardware device that can be used for entering data.

Down:

1. Designed by Bjarne Stroustrup in 1985.
2. Commonly used for desktop computing, other mobile computing, games, and numerical computing.
3. This is the process of performing a particular computation, usually by designing or building an executable computer file.
6. Data values.
10. Block of code that will repeat.

Scholarship Student Highlight

Mary Adkisson

My name is Mary Adkisson and I am graduating with my Master's degree in Computer Science in May! I've lived in Cookeville for most of the last 5 years, but am originally from Roane County, TN. I live here with my husband, Ian, and my cat named Raleigh. I love to run, cook, do crafts, and am learning Finnish as a second language! Receiving the SFS scholarship has been instrumental in my pursuit of a graduate degree. This was never something I was going to be able to do without financial assistance, and it has definitely changed the course of my career for the better. Computer Science is what I'm passionate about and I get to do it surrounded by the great people in CEROC and I am so lucky for that. My advice for any other student is to acknowledge what a privilege it is to pursue an education and to not waste any time doing it. There is always more to learn

Graduating Student Highlight

Austin Brown

My name is Austin Brown, and I am a soon to graduate Masters student here at Tech. I completed my B.S. in cybersecurity Fall of 2020, and have been working on automated machine learning for malware detection under the supervision of Dr. Maanak Gupta. My time here can be best expressed in the friendships I've created and the drive for continuous learning fostered in CEROC. I can't say enough about how the center has helped me succeed and build a solid foundation for my career. In the spirit of giving back, I'll offer some advice for new students in the cybersecurity field. First, in the friendships you create during your time here, pay special attention to developing friendships that challenge you to learn and grow both in cyber and your personal life. Second, never allow yourself to reach a point where you are satisfied in your understanding; if you are not confused, you won't learn anything new. Third, when you find interest in a specific aspect of computing, there is no better way to learn about it than trying to set it up or create it yourself. Fourth, you have a wealth of understanding available with students at CEROC. If someone knows something you're interested in, never be afraid to ask too many questions, both parties will benefit from the experience. Finally, your academic performance is very important, but make sure you take time to enjoy your college years, they may be the quickest and best years of your life.

Security Toolbox

By Jake Graves

Malwarebytes

Malwarebytes is a completely free to use anti-virus program that can scan your PC for any suspicious programs or files. Once detected, Malwarebytes will then isolate the suspicious process, alert you of it, and then offer to delete it off of your computer. Even if you have not been working with any malware, clicked on anything suspicious, or gone anywhere suspicious online, it is always a good idea to regularly scan your PC for any suspicious activity.

CEROC Project Highlight

CEROC will be hosting a Gen-Cyber residential student camp from June 19-24, 2022 for high school students across the state of Tennessee. The week-long, residential camp will include thirty five diverse students with pre-camp and post-camp outreach activities to reach additional students.

In preparation to the camp, this month we conducted four pre-camp outreach events starting from Jan 26 to Feb 2 where 72 middle schools and 146 high school students registered to attend and more than 80% participated. The goal of this outreach was to ignite interest in cybersecurity among a diverse body of middle and high school students in Tennessee. In this respect, we conducted two virtual GenCyber Teaser events, which were 2 hour-long after-school hours workshop sessions for middle and high students where they engaged in hands-on activities in cybersecurity, and met college students studying cybersecurity to learn about their experiences, path, opportunities, and resources for students. They also learned about the upcoming 2022 GenCyber camp and the application process. Both workshop series preceded by an hour-long introduction webinars on the cybersecurity landscape and the activities as part of the GenCyber program. Almost all students reported pre-camp engagement events to be extremely useful. Unfortunately, the camp now has more applications than capacity.

Opportunities In Cyber

Oakland University-Undergraduate Computer Research (UnCoRe) Program in Cybersecurity: The application to sign up for the summer 2022 UnCoRe program in Cyber Security at Oakland University. The Computer Science and Engineering (CSE) Department at Oakland University (OU) focuses on interdisciplinary Cyber Security & Privacy research at the interface of Mobile security, Network Security, Data Security, Digital Forensics, Internet of things (IoT) security and Vehicular Ad Hoc Networks (VANETs) security. Many former UnCoRe students attend graduate school and have received many awards and opportunities. If you are interested in applying for the UnCoRe program scan the QR code to the right.

James K. Goldston Cybersecurity Scholarship *(formerly the James K. Goldston INFOSEC Scholarship): The purpose of this scholarship is to aid students in Tennessee who are pursuing undergraduate programs in computer engineering, computer science, cyber science, or cyber security. The scholarship is a one-time award of $1,700 for one year. To be eligible, you must be planning to attend college/university and be involved in one of the previously mentioned programs. All applicants must have a GPA of 2.5 and be a full-time undergraduate at an accredited not-for-profit public or private college. More information can be found by scanning the QR code to the right!

CERIAS Annual Security Symposium: This year's CERIAS Annual Security Symposium will be happening March 29 & 30, 2022. Join us as industry, government, and academic researchers and practitioners examine where we've been, where we're at, and what may be on the horizon. Scan the QR code on the right for more information!.