Cyber Eagles Reach Newsletter

Term: Fall
Date: October 2, 2022

Editor: Jake Graves, Computer Science

Cyber Club Happenings

By: Asia McKissack

To start the semester, we had our first CyberEagles meeting on August 25th. If you don't know what CyberEagles is, it's a student lead organization for cybersecurity majors to learn more about cyber, tools, and opportunities. CyberEagles isn't just for computer science majors, though! If you are interested in cybersecurity and want to learn more about it, you can attend the meetings and cyber interest groups. In the first meeting, we're introduced to the CyberEagles team, cybersecurity interest groups, and CyberEagles sister chapter, Women in Cybersecurity (WiCyS).

The interest groups are Offense, Defense, and Capture the Flag (CTF). The Offense group is a red team that looks at vulnerabilities within a system and tells the blue team, which is the defense group, how to fix it. During meetings, you'll learn more about the red team and be able to participate in competitions. The next offense group meeting is October 6 at 6pm. The Defense group is the blue team that defends the system. They conduct activities and lessons to help you! The meetings are open to all skill levels, so if you're interested in learning more, the next defense meeting is October 12 at 6 pm. CTF is an exercise where " flags " are secretly hidden in purposefully vulnerable programs or websites you have to find. During meetings, you'll be able to learn more about CTF and do different challenges. We had another CyberEagles meeting on September 8th, where a panel of students answered questions about their summer internships. If you missed the first two CyberEagles meetings, don't worry! The last meeting was on September 22nd during dead hour, where we were able to have an amazing guest speaker talk about their experiences working in a research lab. Amanda L. Theel joined us virtually to describe what their work is like, and to advertise several cyber competitions coming up! If you want to learn more, check out the cyber eagles discrod.

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

As the semester starts be sure to work hard and find time for yourself! Even though you are the future of the world, you must find time to enjoy the present.

~CEROC

Infosec 2022

By: Jake Graves

Infosec 2022 was recently held in Nashville at the Music City Convention Center on September 9. Infosec is a confrence where professionals, students, and anyone interested in cyber could come learn and socialize with professionals that are already well established in the field. CEROC was able to send a group of volunteers to help run the rooms, sign in people, and spend the day socializing with professionals.

The connections that our students made were very valuable. Almost all of the professionals who saw the Tennessee Tech logo already knew who we were, and were questioning us about where to find people to hire from our campus. This is just another sign that if you chose to go to Tennessee Tech, you chose correctly! We are known far and wide, with professionals competing to take our students into their workplace!

Scholarship Student Highlight

My name is Mike Soare. A little bit about me. I'm originally from Knoxville, TN, but decided Tennessee Tech would be the best fit for my future, so I decided to come here. So far, my experience at Tech has been a positive one. As a freshman, I got heavily involved with the CyberEagles, going to each meeting they had available and pushing myself to network with as many people as possible. Due to my involvement with CEROC, the CyberEagles, and having a pretty good GPA, I was able to obtain the CyberCorps: SFS scholarship. This has been my first semester with the scholarship, but so far it has opened several doors for my professional and academic growth. I'm very excited to see what the future has to offer. I'm focusing on my studies and hope to land a job in intelligence or incident response. Who knows, maybe I'll get to work on some cool stuff! To close things out, I'll leave you with two things. First; get involved in whatever your interest may be, even if it's outside of computer science; seek greatness… and lastly, have fun, enjoy your time in college!

Mike Soare

Stress Management

By: Jake Graves

Stress is something that everyone in the world has to deal with, but if you take on too much stress or you take on too little it could leave you in a sticky situation. College is an ideal time to learn how much you can take on, and how to deal with it accordingly. There are several ways to help lessen the stress load.

1. **Schedule out what you have to do.**
If you have specific times when you need to work and rest, it helps your brain visualize what needs to get done in what amount of time, and helps you relax more during breaks.

2. **Make friends in your classes**
Creating a group to discuss hardships will oftentimes reduce stress of the overall group because you can all reaffirm each other.

Even though stress is not something we want, having some stress is a good motivator. If you are worried about an assignment, you are more likely to do it sooner! Always remember there is a healthy balance, and to seek professional help if you think you need it. Remember, Tech offers free consoling!

Tips on How Not to Procrastinate

By: Jake Graves

Here are some tips to help you organize your work and time better as a college student!

1. Get a physical calendar to write your important events and projects on.
2. Get a study group to keep you accountable.
3. Find a place to work that is not your dorm or house.
4. Schedule your time off so you know when you can take breaks.

4 Biggest Dangers of Using Public Wi-Fi Networks

By: Asia Mckissack

Public Wi-Fi makes it easy to access the Internet anywhere, whether it's the public library, fast food restaurants, or retail stores. Even though public Wi-Fi is convenient, it's not as safe as some think. Free Wi-Fi doesn't need authentication to get a network connection, making it easy for hackers to access unprotected devices. Four of the most significant risks you take by connecting to public Wi-Fi networks are Man-in-the-Middle Attacks, Malware Infections, Snooping and Sniffing, and Evil Twin Attacks.

When you access the Internet through Wi-Fi, your device establishes a link with the router or server connecting your device to the internet. A Man-In-The-Middle Attack happens when a hacker puts themselves between you and the connection point. Instead of communicating directly with the intended parties, you send your data to the attacker. With Malware Infections, the hackers can infect an unsecured Wi-Fi connection with malware. Some attackers can connect to the connection point itself and send fake pop-ups requesting you to update software. Once the malware infects your system, the attacker can access sensitive information and deleted files. Snooping and Sniffing are when hackers can eavesdrop on an unsecured public network. Using special software, an attacker on the network can see what you're doing on your device. Lastly, the Evil Twin Attacks or Honeypot attack is where attackers set up a malicious Wi-Fi hotspot intending to steal users' data. Once you connect to the malicious hotspot, the hacker can monitor and steal your personal information. There are ways to protect yourself from the dangers of public Wi-Fi, and some of them are using a VPN app, using your mobile dating, or making sure you're connecting to websites securely.

Source: **https://www.makeuseof.com/biggest-dangers-using-public-network-wifi/**

Faculty Highlight

Travis Brummett

I grew up in a very small town in Kentucky called Albany. After graduation, I attended the local branch of KCTCS Somerset Community College. Once I completed my associate degree, I moved to Bowling Green Kentucky and began attending Western Kentucky University. I proceeded to graduate with my bachelor's degree and started the master's program there. I became a teaching assistant for Dr. Michael Galloway. Dr. Galloway got me interested in doing cloud computing. Once I had completed my coursework and only had my thesis left, I began working at Fruit of the Loom. I maintained a shipment database and did some Java development for them. I worked there until I graduated with my master's and joined Vanderbilt's Ph.D program. At Vanderbilt, my research area shifted to distributed stream processing and meta-modeling. Overall, I was dissatisfied with this. I then left Vanderbilt with a second master's in computer science to come to be a lecturer at TTU. Here at Tennessee Tech, my primary duties are to teach and advise students. In addition to this, I serve on the Diversity and Inclusion and was approached to be the faculty advisor for the aspiring Board and Card Game Club. The best part of the job is working with the students. I get to see them learn and grow. It is an absolute honor to be a part of that process. Words cannot express how thankful I am for the opportunity to teach and hopefully inspire my students just as my professors did for me.

Microsoft Teams' GIFShell Attack

By: Warren Proctor

So, what exactly happened? A group of malicious actors exploited a vulnerability found in Microsoft Teams. This vulnerability was found in features and configurations that were not correctly set. They proceeded to use these features to act as a command and control (C&C) attack for malware, and to exfiltrate data using GIFs without being detected by end point detection and response (EDR). Fortunately, this attack needs a device or user that is already compromised. When this attack is successful it uses base64 encoded GIFs in teams to create a reverse shell that delivers malicious commands and works to exfiltrate output through GIFs retrieved by Microsoft's infrastructure.

The first step in this attack is to create the reverse shell, for this to occur the attacker must first compromise a computer to plant malware, which in this case would be a malicious stager. This can be done through a phishing email. Once the stager is in place the attacker can create their own Microsoft Teams tenant and contacts other Microsoft Teams users outside of the organization. Then the attacker can use a GIFShell Python script to send a message to a Teams user that contains a specific kind of GIF which has been modified to included commands to execute on a target's machine. Once the target receives the GIF they do not even have to open the message for the attack to be in progress due to the way Teams runs their background processes. The stager then comes into play because it monitors Teams logs until it finds a GIF with commands to run. Microsoft's servers will then connect the attacker's server URL to retrieve the GIF which is named using the base64 encoded output of the executed command. The GIFShell server running on the attacker's server will take this request and decode the data which will allow the attackers to see the output of the commands run on the exploited device. This is how the Microsoft Teams vulnerability is exploited, and it shows that given a little creativity anything is possible.

Source: **https://thehackernews.com/2022/09/microsoft-teams-gifshell-attack-what-is.html**

History of Cyber: Origins of Cyrptography

By: Warren Proctor

Cryptography is the study of techniques for secure communication between parties and has been around nearly as long as written languages have. Examples of these early encryptions can be found in stone and cuneiform tablets as well as papyruses. Ancient civilizations such as the Hebrews, Egyptians, Babylonians, and Assyrians devised protocryptographic systems to limit information and increased the significance of the information when it was revealed to a wider audience. The first record of cryptography being used was between the military commanders of the Spartans as early as 400BC. They employed a cipher device called a scytale ("History"). This device was an incredible example of ingenuity for the period. When an admiral or a general wanted to send important messages to one another they would start by wrapping a piece of leather parchment, or a thin leather strip, around their scytale. Once the scytale, which was essentially a special stick, was completely covered in this parchment they would write their message and unravel it which worked to completely mix the letters of the words they were sending. The generals then only had to send the strip which the receiver would wrap around their identical scytale to translate the encoded message ("Ancient"). With such simple beginnings it is amazing what the field of cryptography has transformed into today.

Source: **https://antigonejournal.com/2021/06/deciphering-spartan-scytale/**

AND

https://www.britannica.com/topic/cryptology/History-of-cryptology

Security Toolbox

By: Jake Graves

Burp Suite

Burp Suite is a web app penetration tester tool to test for vulnerabilities in a system. Many companies and individuals use this tool due to its easy to learn UI. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities. It is not easy to learn, but once you do learn it, there are millions of uses for it. Especially because of the need for developers to understand and implement security as they are working, this tool will help you find and squash vulnerabilities as they appear

Source: **https://www.pluralsight.com/paths/web-security-testing-with-burp-suite#:~:text=Burp%20Suite%20is%20an%20integrated%20platform%2Fgraphical%20tool%20for%20performing,finding%20and%20exploiting%20security%20vulnerabilities.**

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!

Fun Corner

Source: **https://xkcd.com/970/**

A Lesson on Good Password Policy

By: Asia Mckissack

A recent report released that e-commerce provider Shopify uses weak password policies on their website. According to the report, Shopify requires its customers to use a password of at least five characters that doesn't begin or end with a space. Specops researchers examined a list of a billion passwords known to have been breached, and 99.7% of those passwords follow Shopify's requirements. A study by Hive Systems shows the dangers of using weak passwords. The study explores the amount of time it takes to brute force crack passwords of numerous lengths and different levels of complexity. According to Hive Systems, a five-character password can be cracked instantly, regardless of the complexity. Given the ease with which shorter passwords can be cracked using brute force, organizations should ideally request users use at least 12 characters. What e-commerce providers can do to start strengthening their IT security internally other than changing their minimum password requirements is to look at a way to improve password security on their networks. Organizations can use Specops Password Policy to help strengthen their password policies instead of using the tools built into Windows. One of the more effective tools that Specops Password Policy offers is the ability to compare passwords used in an organization against a database of billions of passwords known to have been compromised. Users can change their password with that tool before it becomes a problem.

Source: **https://thehackernews.com/2022/09/shopify-fails-to-prevent-known-breached.html**

Current Student Highlight

Nate Dunlap

My name is Nate Dunlap and I am a Sophomore studying computer science with a concentration in cybersecurity here at TNTech. I was born and raised in middle Tennessee with the exception of living in Tallahassee FL for 8 years before moving back to TN in 2013. From the moment I visited Tech, I knew it was the perfect fit for me. The campus, people, and culture are all amazing and I'm convinced I will likely never find anything similar to what I have found here. I'm currently the president of TNTech's Association for Computing Machinery student chapter through which I work as hard as I can to tell people about computer science and build a strong community around it. Being that my concentration is in cybersecurity, I am also heavily involved in the resident cybersecurity club: CyberEagles. The advice I would give to a student can be summarized by a favorite Latin saying of mine: "Semper admove ante". This statement translates to "Always move forward" and I often use it to remind myself to become better than I was yesterday. So make some small steps each day and you'll find they will add up to great leaps over time.

PHD Student Highlight

Trey Burks

My name is Trey Burks, I am in my second year of the Ph.D. program, and am a CyberCorps Scholarship For Service recipient. I am originally from McMinnville, Tennessee, which is a small town to the south of Cookeville. After graduating high school, I completed my Associate's degree at Motlow State Community College before transferring to Tech in the Spring of 2018. Since then, I have competed in many cybersecurity competitions and am heavily involved with CyberEagles, the CIGs, and CEROC. For research, I am currently interested in the security of quantum satellite networks, which I am looking into under Dr. Ismail. After graduating, my goal is to be a professor and to continue research on quantum networks and space infrastructure. My advice for other students is to get involved and talk to people, especially upper classmen and your professors. It might seem intimidating, but many of them are willing to take the time to answer questions and help. I would also advise everyone to take time for themselves, even if it's just an hour or two a day, it can make a huge difference for motivation and prevent burn out.

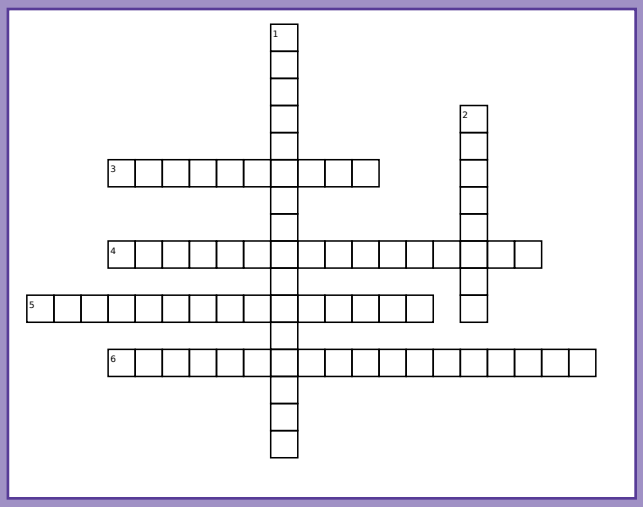
Crossword Puzzle

Across:

3. an attacker submitting many passwords or passphrases with the hope of eventually guessing one correctly.
4. is an attack that attempts to access many usernames with a few commonly used passwords.
5. is spyware that records a user's activity by logging keyboard strokes.
6. a cyberattack method in which attackers use lists of compromised user credentials to breach into a system.

Down:

1. an attempted illegal entry to a computer system that uses a dictionary wordlist to generate possible passwords.
2. When an attacker posing as a trustworthy party sends you a fake email, hoping you will reveal your personal information voluntarily



Accolades

- B. Northern and D. Ulybyshev, "Building Secure Environments for Microservices", Intl. Workshop on Secure and Reliable Microservices and Containers, co-located with 41st IEEE Intl. Symposium on Reliable Distributed Systems (SRDS) 2022. Accepted, in-press
- T. Seyler and D. Ulybyshev, "SEMAFORE: Secure Mobile Field Diagnostics for Cyber-Physical Systems", IEEE 6th World Conference on Smart Trends in Systems Security and Sustainability (WorldS4), 2022. Accepted, in-press
- R. Manicavasagam, A. Palmer, M. Rogers, S. Mahajan, R. Craven, C. Emeghara and R. Senz, "Testbed for Evaluating and Analyzing Smart Grid Behavior in Demand Response Scenarios". The 14th International Congress on Ultra Modern Telecommunications and Control Systems. October, 2022. Accepted.

Opportunities

- **Scholarship Application Deadline:** Don't forget to apply for scholarships **before December 15**. All students must complete this application in order to be eligible for Tennessee Tech scholarships in the Fall 2023, Spring 2024, and Summer 2024 terms. Even if your scholarship repeats, you have to reapply every year. If you need any help with learning how to apply, email your advisor and they will help you!