Cyber Eagles Reach Newsletter

Term: Spring | Issue: 3 | Date: May 1, 2021 **Editor: Jake Graves, Computer Science**

Graduating Students

Congratulations!

- Adam Christopher Horton
- Alison Diane Rust
- Allyson Baylee Jones
- Andrew McDole **- Masters**
- Anthony Taylor Ramirez
- Austin Robert Lane
- Austin T. Tice
- Christopher D. Lewis
- Daniel Josiah Cruickshank Roberts
- David Isaac Feier
- Dulce Kaiser - **Masters**
- Ethan Thomas Newman
- Glen Lannom Cathey Jr.
- Jacob H. Perdue
- Jacob Dalton Strickler
- James Matthew Massengille
- Jeffrey Calen Kimmell
- Jevin Evans **- Masters**
- Julianne Marie Cox
- Kendall Land **- Masters**
- Marena Bertha Soulet
- Mayson J. Stickel
- Michael A. Lieb
- Nicholas Cobb Stone
- Noah David Geiger
- Noah Anthony Treutel
- Patrick R. Adcox
- Sina Sontowski
- Stephen Dominick Meshotto
- Tate J. Seyler
- Tyler Alexander White

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

You are almost there... just a week left. Keep working hard and you will make it! I know summer experiences will be different for all of you: some will intern, some will take summer courses, some will focus on research, some will work, some will take care of family or personal business, some will travel, and some will just chill at home. Whatever you do, hope this summer goes well for you and you come back to school (yes, school... not zoom) in Fall rejuvenated. I really hope that in between all that you do in summer, you will find time to keep your curiosity up and LEARN new things: there is just so much to nibble in cyber! Check out some resources here: **https://www.tntech.edu/ceroc/cyber_resources/**

Live as if you were to die tomorrow. Learn as if you were to live forever.
Mahatma Gandhi

Take care. Enjoy summer. SEE you in Fall.
Dr. Ambareen Siraj, CEROC Director, Professor CS, Tennessee Tech
https://www.linkedin.com/in/ambareensiraj/

NCL Spring Season 2021

by Jacob Sweeten

Overview:
The National Cyber League Team Game is by far the most challenging section of the competition. This season, it seemed that most of the challenges were easier than previous seasons except for one: Web Exploitation 3, A.K.A. "Hire-A-Hacker." Within 24 hours, we had completed all of the challenges except for Web Exploitation 3. Although we used every trick we could think of (And new ones we learned along the way), we were unable to even scratch the surface of the challenge. Hour by hour went by with absolutely no progress and hopes dwindled until the competition closed for the season and the challenge was left incomplete. Only three teams had managed to complete Web Exploitation 3: the three teams that tied for 1st place. This left us tied for 4th place with fourteen other teams. Our accuracy placed us in 10th place overall out of 922 teams.

Unexpected Occurrences:
In previous seasons, accuracy rarely mattered since very few teams ever made it to the top. However, since this season was a bit easier, more people tied for the higher rankings. While we had an excellent accuracy, several other teams had even better accuracy than we did, so our rank was lower than we had hoped.

Looking Forward:
In the future, we plan to have a more rigid system for turning in solutions to prevent simple mistakes that could hurt our accuracy. Hopefully, we can achieve 1st place in future seasons. While we have now been provided with the solution to Web Exploitation 3, this information does not guarantee a win in future seasons since the solution was rather unexpected and trivial and not a reflection of poor or lacking methodology on our part.

Larry Whiteside Jr.'s presentation

by Jake Graves

We at CEROC would like to thank Larry Whiteside Jr. for taking the time to talk with our students. His presentation was inspiring to everyone who attended, and the story of his life kept us all glued to our screens. For those reading this who did not get a chance to attend, here are some of the main takeaways that Larry really wanted to drive home:

- We are shaped by our past, not defined by it.
- Don't be your own obstacle.
- It's 30% what you know, and 70% who you know.
- Life is about choices.
- Don't let your yesterday ruin your tomorrow.

While these takeaways are powerful within their own right, they pale in comparison in the way that Larry was able to present them to us. He used the story of his life to prove a lot of these sayings, and show us how he was able to use them in his life. If you have not yet seen his presentation, we at CEROC urge you to click the link and watch the entirety of it here: **https://sites.tntech.edu/csc-diversity/2021/03/09/spring-2021-diversity-inclusion-series-larry-whiteside-jr/**

Across The Wire

Compiled by Ahsan Ayub

What do we need to know about IoT Botnets?

An IoT botnet is a network of devices connected to the Internet of Things (IoT), e.g., routers, that have been infected by malware and have fallen into the control of malicious actors. Cybercriminals use it to launch Distributed Denial of Service (DOS) attacks on target entities to disrupt their operations and services. Typically, botnets are controlled from a single command-and-control (C&C) server that is connected to all the infected devices (called “bots”). The TrendMicro research team has identified three main IoT malware codebases, such as Kaiten (2001), Qbot (2008), and Mirai (2016), on which most of today’s IoT botnets are based. Due to the continuing development and the broadening use of the IoT botnets, we are likely to see that it is going to evolve into a formidable threat that will be much harder to take down in the future. That being said, the TrendMicro research team has shared the following few preventive strategies against IoT botnets to limit such attacks.

- Manage vulnerabilities and apply patches as soon as possible. Vulnerabilities are the main way malware infects devices. Applying patches as soon as they are released can limit the chances of potential exploits.
- Apply secure configuration. Users must ensure that they are using the most secure configuration for their devices to narrow openings for compromise.
- Use strong, hard-to-guess passwords. Botnet malware takes advantage of weak and common passwords to take over devices.

Reference:
https://www.trendmicro.com/vinfo/us/security/definition/iot-botnet?utm_source=trendmicroresearch&utm_medium=smk&utm_campaign=0321_IoTBotNetDef

Security Toolbox

Snort – Snort is one of the top Intrusion Prevention Systems (IPS) on the market. Snort has three main uses: as a packet logger, as a packet sniffer, or as an intrusion prevention system. The first mode records packets to disk and the second mode displays the packets to the screen in real time. These two modes act more as an Intrusion Detection System (IDS). This means that Snort will send alerts, but no actual action is taken. The third mode performs detection and analysis on packets and can prevent some attacks from being executed on a network or machine. Snort is open-source and has both a free and paid version. The free version is developed by the Snort community with help from Cisco Talos whereas the paid version is completely developed by Cisco Talos.

https://www.snort.org/

PHD Student Highlight

Ibrahim Yilmaz

My name is Ibrahim Yilmaz, a third-year Ph.D. student in Computer Science at Tennessee Tech University. I was born in Germany to a Turkish family. I have two bachelor's degrees in Computer engineering with the honor of summa cum laude from the University of Warsaw and Zirve University. After working as a software engineer at global companies like Stanley Black & Decker and IBM in Poland for five years, I decided I was ready for another challenge. Pursuing a doctoral degree in the United States was the logical next step. My research interests include cyber-physical systems, smart grids, machine learning models, and network security, under the supervision of Dr. Ambareen Siraj. My education in Computer Science at Tennessee Tech has been exceptionally preparing me for my career development and improving critical and creative-thinking skills necessary to be more successful in the future. My motto for life is to always keep learning. The information technology industry changes so quickly that computer engineers must keep up with technological advancements to adapt the environment. You always need to make sure that you are still employable in the IT field.

Linkedin:
https://www.linkedin.com/in/ibrahim-y%C4%B1lmaz-642239131/

Across The Wire

Compiled by Ahsan Ayub

Cyberattacks Against Colleges Increase Amid Pandemic

The Chronicle of Higher Education reports that a message, "emailed to thousands of students and employees at the University of Colorado's Boulder campus last week" said that their personal information, "including addresses, phone numbers, Social Security numbers, academic progress reports, and financial documents, had been stolen." Their university was "refusing to cooperate with extortion demands" and as a result, the data "was starting to be posted on the dark web, the shadowy back channel of the internet where cybercriminals lurk." Elsewhere around the country, students and employees "at least nine other universities were receiving similar warnings." The campuses are "part of an escalating number of extortion and ransomware attacks the FBI has been tracking since March 2020, when the COVID-19 pandemic took hold in the US." Cybercriminals have "taken advantage of the unique circumstances of the pandemic to double down on their demands." Reference: **https://www.chronicle.com/article/cyberattacks-are-spiking-colleges-are-fighting-back**

Graduating Student Highlight

Justin Murphy

My name is Justin Murphy, and I am a CyberCorps SFS Scholar graduating with my M.Sc. in Computer Science. I am originally from Nashville, TN, where I was a high school mathematics teacher before coming back to school. After graduating, I will be heading to Washington, D.C., to work for Cybersecurity and Infrastructure Security Agency (CISA), a sub-agency of the Department of Homeland Security (DHS). I have enjoyed my time at Tennessee Tech, acquiring a great education, having wonderful professors, and being exposed to an abundance of opportunities to build valuable skill sets for my future career. I have been an active member of CEROC, participating in competitions and serving as the lead for the CTF Cyber Interest Group. I have been able to serve the community and give back through various CEROC outreach events. I have been able to conduct fun and exciting research in the area of Secure Software Development, supported by my advisor Dr. Rahman. My advice to current and prospective students is to step out of your comfort zone, ask for help, get involved with CEROC, CyberEagles, WiCyS, INSuRE, etc., and do not convince yourself that you are "not ready yet" or cannot do something before even trying. You might be surprised if you just try.

Marena Soulet

Hi, my name is Marena Soulet and I am set to graduate with my bachelor's degree this upcoming May! I am from Puerto Rico (Wepa!), but have since then moved to Tennessee where I've been able to find an incredibly supportive community within Tennessee Tech. Throughout my time here my professors and advisors have continuously encouraged me to challenge myself both personally and professionally by learning and trying new things. Getting out of my comfort zone has opened doors to so many new opportunities, including the honor of becoming a CyberCorps SFS scholar. It's been life-changing to say the least, and I'm absolutely thrilled to continue my cybersecurity research as a master's student in the fall! For those that are just starting the program, my advice would be to not shy away from getting involved in extracurricular activities. Get involved within the cyber interest groups, participate in cybersecurity competitions, have fun and ask questions! Even if you don't think you're qualified or "good" enough. Impostor syndrome is very real, but just know that you are enough. Taking that first step will enable you to discover and learn the skills and interests you're truly passionate about, and that is everything.

Across The Wire

Compiled by Ahsan Ayub

A Look at Linux: Threats, Risks, and Recommendations

Linux, one of the most powerful Operating Systems (OS), dominates the cloud platforms and servers all around the world currently. With that, cybercriminals have shifted their focus and resources to target these environments as the enterprises migrate to the cloud. Exploiting vulnerabilities are one of the most common methods attackers use to gain initial access to the Linux platform. It leads to SQL injection, cross-site scripting (XSS), XML external entities (XXEs), insecure deserialization, and breaches. For example, a well-known breach at Equifax was a result of the exploitation of a vulnerability in Apache Struts, known as the identifier CVE-2017-5638. Security misconfiguration, e.g., using a default or weak password, exposed services on the internet (aka open ports), open file shares, exposed and unprotected APIs, in the Linux-based cloud platform is another way an adversary can gain access to systems and environments. With the motivation of financial gain, espionage, sabotage, and hacktivism, all the underlying security threats that come in with malware, such as ransomware, cryptocurrency miners, user- and kernel-mode rootkits, worms, trojans, backdoors, and remote access trojans (RATs), are also present in the Linux platform. As more users and high-value enterprises rely on Linux for their online infrastructures and systems, it is inevitable that cybercriminals will continue targeting the Linux environments for financial gain. Therefore, the TrendMicro research team has given the following security recommendations to keep Linux systems secure:

- Adopt infrastructure as code (IaC) practices to ensure that systems are created properly and that their configurations remain as intended.
- Adopt the principle of least privilege and the shared responsibility model.
- Keep visibility at the forefront. Monitor all devices, systems, and networks.
- Replace default passwords with strong and secure ones. Always opt for multi-factor authentication.
- Regularly patch and update systems.

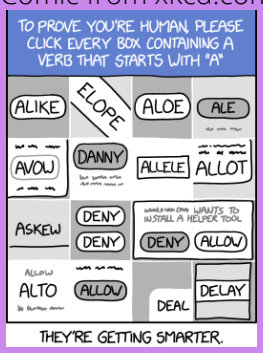
Reference:
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/a-look-at-linux-threats-risks-and-recommendations

Fun Corner

What do you call a turtle that surfs the dark web?

A TORtoise

Comic from xkcd.com



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

Use a botnet.

https://www.helpsystems.com/blog/35-cybersecurity-jokes-make-any-security-geek-chuckle-or-groan

Scholarship Student Highlight

Sina Sontowski

Hi, I'm Sina Sontowski, and I'm a Computer Science senior here at Tennessee Tech. I transferred to Tech after receiving my Associates from Pellissippi State Community College in Knoxville, Tennessee. Originally, I lived in Germany until I moved to Knoxville, TN when I was 15 years old. What I enjoyed the most about Tennessee Tech is meeting other students in the Cybersecurity program. I'm not sure what I would do without my friends here at Tech, because they truly shaped my experience. I do believe that I have grown a lot, career-wise and personality-wise, while I attended Tech. For you new students out there, how much you put in, is how much you get out of your experience here at Tech. So, explore as much as you can and take advantage of every opportunity. And don't worry too much, that's not good either. My plan for the future is getting my master's completed and getting a job in the cybersecurity field that I can enjoy and where I can make an impact. Also, I would really like to get a third dog because apparently, I'm addicted to getting slobbered on and being a walking dog hair collector.

Accolades

Publications:

- A. Shafee, M. Nabil, M. Mahmoud, W. Alasmary, and F. Amsaad, “Detection of denial of charge (DoC) attacks in smart grid using convolutional neural networks,” International Symposium on Networks, Computers and Communications (ISNCC, June 2021).
- Cherner, T. Fegely, A., & Gleasman, C. "An analysis of corporate technology certification programs." Concurrent session at Society for Information Technology & Teacher Education (SITE), Virtual Conference. April, 2021.
- D. B. Bose, A. Rahman, and S.I.Shamim,"'Under-reported' security defects in kubernetesmanifests",to appear in the 2nd International Workshop on Engineering and Cybersecurity of Critical Systems(EnCyCriS2021), co-located with the 43rd International Conference on SoftwareEngineering (ICSE2021),June 3-4,2021.
- F.A.Bhuiyan,A.Rahman,P.Morrison,"Practitioner perception of vulnerability discovery strategies",to appear in the 2nd International Workshop on Engineering and Cybersecurity of Critical Systems (EnCyCriS2021),co-located with the 43rd International Conference on SoftwareEngineering (ICSE2021),June 3-4,2021.
- Gleasman, C., Cherner, T. Fegely, A., & Boz, T. "Educational innovation and its relationship with teacher education." Panel leader at Society for Information Technology & Teacher Education (SITE), Virtual Conference. April 2021.
- Kim, C., Belland, B., Vasconcelos, L., Umutlu, D. & Gleasman, C. Initial design of scaffolding for debugging block-based code. Paper presented at American Educational Research Association (AERA), Virtual Conference. April, 2021.
- K. Cottrell, D. B. Bose, A. Rahman, "An Emperical Study of Vulnerabilities in Robotics", IEEE Computers, Software, and Applications Conference (COMPSAC 2021). Accepted.
- M. Alsabaan, W. Alasmary, A. Alquniah, M. Mahmoud, and M. Nabil , "Distributed surveillance system using positive orthogonal codes", IEEE Access, January 2021. Accepted.
- M. A. Ayub, S. Smith, A. Siraj, and P. Tinker, “Domain Generating Algorithm based Malicious Domains Detection.” Accepted in the 8th IEEE International Conference on Cyber Security and Cloud Computing (IEEE CSCloud 2021), Washington DC, USA.
- M. Badr, M. Baza, S. Abdelfattah, M. Mahmoud, and W. Alasmary, “Blockchain-based ridesharing scheme with accurate matching and privacy preservation,” International Symposium on Networks, Computers and Communications (ISNCC, June 2021).
- M. Badr, M. Ibrahem, M. Baza, M. Mahmoud, and W. Alasmary, “Detecting electricity fraud in the net-metering system using deep learning,” International Symposium on Networks, Computers and Communications (ISNCC, June 2021).
- 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, R. Amer, A. Rasheed, G. Srivastava, M. Mahmoud, W. 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.
- M. Ibrahem, M. Badr, M. Mahmoud, M. Fouda, and W. Alasmary, “Countering presence privacy attack in efficient AMI networks using interactive deep-learning,” International Symposium on Networks, Computers and Communications (ISNCC, June 2021).
- M. Rayhan A. Mithu, M. Rogers, D. Ulybyshev, R. Manicavasagam, R. A. Awad, "Feature Classification for Control System Devices", The 34th International FLAIRS Conference. May 17-19, 2021. Accepted.
- M. Gupta, and R. Sandhu. "Towards Activity-Centric Access Control for Smart Collaborative Ecosystems." Accepted in ACM Symposium on Access Control Models and Technologies (SACMAT - 2021)
- R. Paudel, L. Tharp, D. Kaiser, W. Eberle, and G. C. Gannod, “Visualization of Anomalies using Graph-Based Anomaly Detection”, (to appear) in proceedings of the 34th Florida Artificial Intelligence Research Society (FLAIRS) Conference, AAAI, May 2021.
- S. Abdelfattah, M. Baza, M. Mahmoud, and W. Alasmary, “CSES: Customized searchable encryption scheme with efficient key management over medical cloud data,” International Symposium on Networks, Computers and Communications (ISNCC, June 2021).

Graduate Defense:

- A. McDole,“Analyzing Online Behavioral Malware Detection in Cloud using Convolutional Neural Networks”, Dr. M. Gupta.
- J. Evans,"A Development of Hands-On Cybersecurity Educational Material", Dr. M. Ismail.
- K. Dulce,"Visualization of a Stream-Based Approach of Graph-Based Network Anomaly Detection", Dr. J. Gannod.
- K. Land,"Blockchain Based Farm-to-Fork Supply Chain Tracking", Dr. A. Siraj.
- R. Shakya,"Growing the Science of Validation and Verification for Julia Programs", Dr. A. Rahman.

Recognition:

- J. C. Kimmel. Winner (Undergraduate) Research and Creative Inquiry Day
- K. Land and A. Siraj, " Farm-to-Fork Supply Chain Tracking using Blockchain." Proceedings of Student Research and Creative Inquiry Day (2021). Awarded for Best Poster in the Computer Science Graduate (Masters) track.
- M. A. Ayub and A. Siraj, "A Data-Driven Study on Understanding Ransomware Behavior using Time Series Analysis for Early Detection." Proceedings of Student Research and Creative Inquiry Day (2021). Awarded for Best Poster in the Computer Science Graduate (Ph.D.) track.
- P. A. Brown – COE Outstanding Senior Award
- S. Sontowski – COE Eminence award for the Bachelor of Science Best Paper
- Tech has performed well in the National Cyber League CTF once again. Three players, Austin Brown, Jacob Sweeten, and Nick Stone placed in the top 100 at 62nd, 68th, and 95th out of almost six thousand competitors in the individual round. Tech's lead team also did well in the team round, coming in a 14-way tie for fourth place in points and 11th overall after the tie was settled on accuracy.

Across The Wire

Compiled by Ahsan Ayub

McAfee Labs Threats Report: April 2021

The highlights of the Q3 and Q4 2020 findings include:

- COVID-19-themed cyber-attack detections increased 114%
- New malware samples averaging 648 new threats per minute
- 1 million external attacks observed against MVISION Cloud user accounts
- Powershell threats spiked 208%
- Mobile malware surged 118%
- New Ransomware, driven by Cryptodefense, grew in volume 69% from Q3 to Q4
- Office malware surged 199% from Q3 to Q4
- MacOS malware exploded in Q3 420% due to EvilQuest ransomware, but came back to normal levels in Q4

Reference:
https://www.mcafee.com/enterprise/en-us/lp/threats-reports/apr-2021.html

Current Student Highlight

Kaitlyn Carroll

Hello, my name is Kaitlyn Carroll, and I am a senior here at Tennessee Tech. I am in the CyberCorps: Scholarship for Service program, and I am also the Tennessee Tech Women in CyberSecurity student chapter president. I am from Wartburg, Tennessee and attended. As a student who came in with virtually no experience in cybersecurity or even Computer Science, I was amazed with the amount of opportunities available here at Tech for students at every level — even if they had never even done more with a computer than use Microsoft Office (just kidding; I'm a Google Docs gal all the way). I quickly jumped into the cyber interest groups and regularly attended WiCyS and CyberEagles meetings. I learned a lot from these meetings, and was even able to use some of what I learned in my classes. The cyber interest groups also enabled me to compete in multiple cyber competitions including multiple National Cyber League CTF competitions, the Collegiate Cyber Defense Competition, and the Collegiate Penetration Testing Competition, among others. All-in-all, what makes Tech such a great place for cybersecurity isn't just the stellar curriculum, but also the awesome community of students. Cyber interest groups and general club meetings are a great way to meet other people in your program who are just as excited about cyber and are as driven as you are. They are quick to offer advice, lend a helping hand, and share their experiences.

Vadim Kholodilo

I am an international computer science student with concentration in cybersecurity. I came here as an exchange student, but I fell in love with the university and decided to continue my studies here as a seeking degree one. I love Tech, because it gives me everything, I need to become a great person and high-quality specialist. I have never seen so many amazing professors in one place. They really care about students and always ready to explain something if it is not clear. Students who only start their university journey, I would advise focus not only on the academical part, but also try to do more and more personal projects. However, the best would be if you can find a team to work on a project. There are many opportunities at Tech. Just keep searching. As an example, I work with Doctor Ulybyshev, we implement several solutions related to medical systems security, industrial systems and IOT security. In addition to this, I work with Doctor Siraj. I help her to redesign cybersecurity exercises. It helps me a lot, because I have to go through them and I use them to prepare for different cybersecurity contests. After my graduation, I would like to work as a cybersecurity specialist. My main focus would be security of smart devices.

Breaking the CodeBreaker

by Austin Brown and Austin Tice

During the first weekend in April, Scholarship for Service (SFS) students across the country were participating in the SFS Mini-Codebreaker Challenge. This CTF was sponsored and put together as a joint effort between the National SSecurity Agency (NSA) and New Mexico Institute of Mining and Technology. We, as members of Tennessee Tech SFS Team (https://www.tntech.edu/ceroc/education/sfs/) managed to finish second in this national competition. The team consisted of us (Austin Brown, Austin Tice) and several other SFS students. However, we could have finished first place (unethically) by a considerable margin by exploiting a vulnerability that we found in the scoring system. Without going into too much detail, here is a brief summary of the story of how we broke the CodeBreaker challenge application.

The exploit journey, as many do, began with an educated guess at the construction of the first challenge. After some careful guess work, we discovered the answer to the first challenge to be the MD5 hash of the email address used to register. The predictable solution to this problem began to make us wonder if it could be leveraged to acquire an arbitrary number of points, leading us to investigate any vulnerabilities on the website. We discovered that during this CTF, if at any time we were to refresh the page, it logged us out. This annoyance led us to wonder how the web application knew it was us who submitted flags - since it did not store data in cookies or any other persistent storage.

After further investigating how challenges were submitted, we discovered an open API. It accepted an email and solution for any of the challenges to assign points to a player, and there was never any secret authentication required in this process. This was the first step in developing the planned exploit. With the knowledge of how to submit flags to the backend, we then needed to figure out how to acquire points for the team. This question led us to investigate the form to sign up for the event. We realized that the sign-up form would accept any email, valid or not, that ended in ".edu". If we register accounts with any fake @tntech.edu email addresses and use them to submit the first challenge, we can script the whole process and run it as many times as we would like, which could potentially grant our team infinite points. We wrote a Proof-of-Concept to demonstrate how this vulnerability can be exploited. Obviously, being the ethicalhackers that we are, we did not run this exploit, rather responsibly disclosed it to the event organizers. Although we did not place first, the organizers were thrilled with our reporting and honesty and apart from becoming second by merit, we, the Tennessee Tech SFS team, were acknowledged with a special "Breaking the CodeBreaker" award!
All in all: A great day of learning, team work, principles, and fun!!

Faculty Highlight

Dr. Mohamed Mahmoud

Dr. Mohamed Mahmoud received a Ph.D. degree from the University of Waterloo (Ontario - Canada) in April 2011. From 2011 to 2013, he worked as a postdoctoral fellow at the University of Waterloo and Computer Science department at Ryerson University, Toronto. In 2013, Dr. Mahmoud joined the Electrical and Computer Engineering (ECE) Department of Tennessee Tech University (TTU) as an assistant professor. He has been promoted to Associate Professor in 2018 (early promotion). The research interests of Dr. Mahmoud include security and privacy preservation in different networks and applications, such as smart grid, Blockchain, intelligent transportation systems, cloud, etc. In these areas, he has published over 100 papers in IEEE conference proceedings and journals. For external research fund, Dr. Mahmoud is the PI of 10 external competitive grants including four NSF grants. The total amount of these grants is more than $5.3 million, where TTU share is around $2 million. For awards, Dr. Mahmoud has won several competitive awards such as two Canadian national awards (NSERC-PDF and MITACS-PDF) and three Best Paper Awards from IEEE ICC'09 and IEEE WCNC'16, and IEEE SmartNets'19 conferences. At TTU, Dr. Mahmoud won Kinslow Engineering Research Award in 2018 and 2020, Brown-Henderson Outstanding Engineering Faculty Award in 2018, Scholastic Research Award in 2018, Wings up 100 Research Achievement Award in 2019, and Rising Renaissance Engineer Faculty Scholar award in 2017. His teaching was recognized by the Center for Advancing Faculty Excellence in the Office of the Provost and the Center for Innovation in Teaching and Learning. Dr. Mahmoud has advised six Ph.D. and six M.S. graduates. His Ph.D. graduates are currently faculty members in different US universities. Dr Mahmoud has served on the technical committees of several IEEE conferences and served in several NSF panels. He is also a reviewer to several IEEE Transactions and Associate Editor of IEEE Internet of Things and the Springer journal of Peer-to-Peer Networking.

Alum Highlight

Darren Cunningham

My name is Darren Cunningham, and I'm a Tennessee Tech Cybercorps alum from Nashville, TN. I am currently a Network Professional working for the Department of Defense. My experience at Tech helped springboard me to where I am now. A lot of my success is due to the knowledge and skillsets I gained at tech. My biggest advice is to never give up. I didn't have the best of grades starting out, but I never gave up and I had incredible advisors/professors who helped me stay focused so that I would be successful. The second piece of advice I have is to always try to be active with any of the groups and activities being offered by CyberEagles or CEROC. Most employers are looking to see if you were more than just a bookworm. They want to see that you applied what you learned in school to things outside of school like competitions (CCDC, CPTC, CTFs), interest groups (Cyber Eagles Red, Blue, and Green teams), research, and internships. Don't be afraid to sign up for any of these even if you are new to cybersecurity. The whole point is to learn, have fun, and gain experience.

CEROC Outreach Projects

The **NSA** and **NSF** funded **GenCyber Camp** provides cybersecurity engagement experiences for students and teachers at the K-12 level and has the following goals:

- Increase cybersecurity awareness among high school students.
- Increase interest in cybersecurity among diverse body of students.
- Help all students understand correct and safe on-line behavior.
- Provide training for students with instructional activities based upon the GenCyber Cybersecurity Concepts.

CEROC is hosting a **Gen-Cyber camp** from May 24-29, 2021 in cooperation with Putnam County Schools! Learn more with the link bellow!
https://www.tntech.edu/ceroc/outreach/gen-cyber.php

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. According to NSA press release “this workforce development program, redefines the academic path to a successful career in cybersecurity” for MSI and HBCU students. The universities interested in establishing a cybersecurity program are connected with NSA’s Centers of Academic Excellence-designated institutions in their region to provide opportunities, resources and advice on program development. Learn more with the link bellow!
https://www.tntech.edu/ceroc/outreach/cedi.php

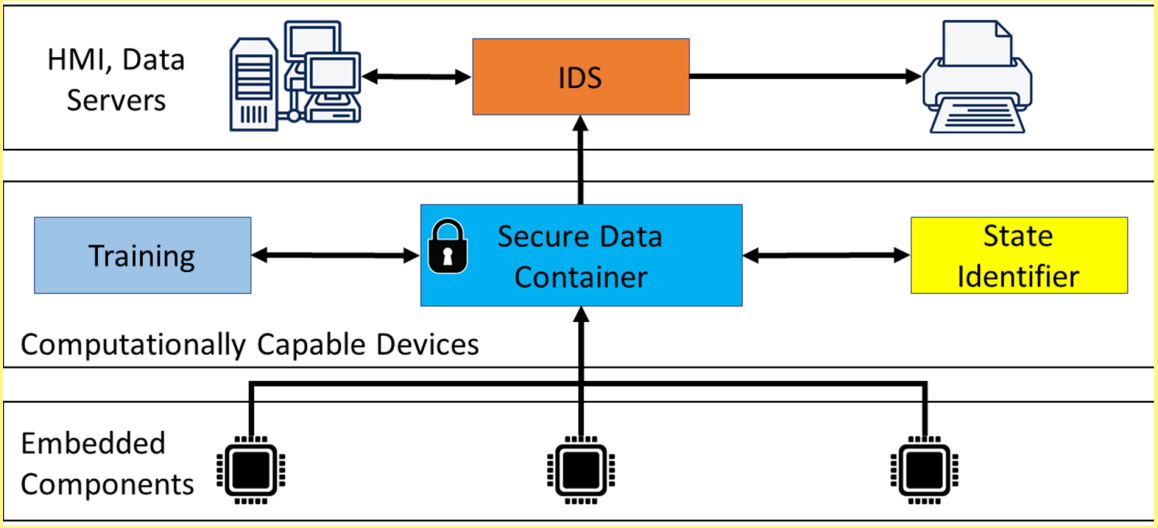
The **Department of Defense (DoD) funded Community College Cyber Enrichment (C3E) Program** (Award# H98230-20-1-0321) which provides opportunities and knowledge about cybersecurity to students currently enrolled in community colleges across the state. The primary goal of C3E is to grow the pipeline of community college students in Tennessee to join the cybersecurity workforce with baccalaureate degrees at 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:
http://www.tntech.edu/ceroc/outreach/c3e.php

Secure Industrial Control System with Intrusion Detection

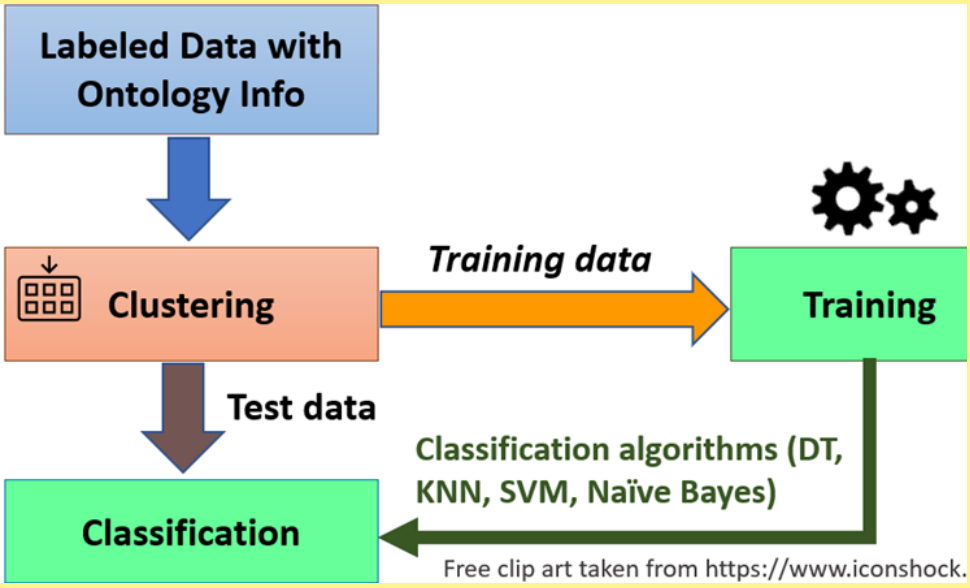
Students - M Rayhan Ahmed Mithu, Rajesh Manicavasagam
Dr. Mike Rogers, Dr. Denis Ulybyshev

A control system is a set of interconnected devices that coordinate to control dynamic systems in industry, the power grid, and smart cities. Control systems can be found anywhere that automation is needed to increase productivity, consistency, and safety. Control devices monitor and control other devices and tend to require little energy but are computationally slower than commodity hardware. Historically, due to their lack of processing power, these devices lack the security measures of commodity hardware because they were typically isolated and lacked connection to a network. However, controls systems are now often deployed in uncontrolled environments, such as buildings accessible by many employees, or out in the field. Furthermore, these devices have become more remotely accessible through wide area networks and the Internet. The increased accessibility has also increased the opportunity for attacks, which can have severe, even life-threatening, consequences.

As more and more industrial control systems are deployed in critical infrastructures, securing these systems are becoming just as important as using them. Most of the typical security solutions are using intrusion detection systems (IDS) for detecting any unauthorized activity. An IDS usually takes the network data and uses the pre-defined rules to label the data as normal or attack. Using only the network data is not enough most of the times, as it generates a lot of false positive or false negatives. Our ongoing work is to incorporate additional information about the devices with this network data to improve intrusion detection. We are using machine learning to combine **device state** information with the **network data** to create a profile of a device that helps the IDS to detect intrusion. All the information about the device state is stored in a secure data container to ensure that it has not been tampered with. The figure below explains the secure architecture we propose for the industrial control systems.



Machine learning is used to extract the device raw data and identify the components of the device as well. This process uses an ontology data about the system itself to identify device components from the raw data. The system **ontology** defines the components inside the system, how all the components interact with each other, the relationship between different components, and the type of data being processed by the devices. These ontology data allow the machine learning algorithm to extract the raw data and label them according to the device component of the system. This process is shown in the figure below.



Opportunities In Cyber

CEROC Summer Internship: CEROC is looking for passionate dedicated hard working students for various summer internships in cybersecurity education, research and outreach projects. Apply here: **https://www.surveymonkey.com/r/CEROC-Summer21Work**

Raytheon Intelligence & Space Woman's Cyber Security Scholarship: Applications open April 1, 2021 and Close Monday, June 1, 2021 at 11:59 PM EDT. Apply using the link: **https://iamcybersafe.org/s/raytheon-womens-scholarship**

RSAC College Day: RSA Conference College Day provides you a unique opportunity to join cybersecurity professionals who stand against cyberthreats around the world. Here is an amazing opportunity to gain experience, network and attend the world's largest cybersecurity event.
Please register using the following link: **https://www.rsaconference.com/collegeday**

US Cyber Games to find Best Cybersecurity Athletes: The program will run from April to October 2021 and consist of the US Cyber Open, the US Cyber Combine Invitational, and the selection of the first-ever US Cyber Team™ to represent the United States at the 2021 International Cyber Security Challenge (ICSC) held in Athens, Greece in December.
Learn more at: **uscybergames.com.**

Suricon 2021 Training Scholarship: Large scale data breaches, advanced persistent threats, targeted attacks – the ability to proactively monitor a network has never been more important. Suricata is pleased to offer two student scholarships for the upcoming training Threat Hunting with Suricata and tickets to SuriCon 2021. Applications close August 20th, so click the link for more information: **https://www.caecommunity.org/event/suricon-2021-training-scholarship-scholarship-closes-august-20-2021**

IEEE S&P 2021: Registration for the 2021 IEEE Symposium on Security and Privacy is now open! As with last year, this year's conference is fully online. Registration is $50 USD for general attendees and only $35 USD for students. We hope that this virtual format along with the low cost will allow everyone that wants to learn more about security and privacy research to attend. To register, please visit **https://hopin.com/events/ieeesp2021.** There are also student travel grants here: **https://www.ieee-security.org/TC/SP2021/travel_grants.html**

CAE Tech Talks: Every month CAE Tech Talks provide a forum where subject matter experts from the field and from academia can present research and information on a spectrum of cybersecurity topics. Find out more here: **https://www.caecommunity.org/content/cae-tech-talk-resources**

WiCyS Webinar: There are weekly webinars that WiCyS hosts with professionals in the field! Check it out here: **https://www.wicys.org/events/webinars/**

Give us your feedback about EaglesReach!