# CYBER EAGLES REACH NEWSLETTER

Term: Spring | Issue 2 | Date: April 1, 2021

Edited by: Jake Graves, Computer Science

## UPCOMING CYBER EVENTS IN APRIL

cybereagles.org/calander/

Thursday April 1: CyberEagles Meeting 11-12pm

Thursday April 1: FBI Info Session 11am

Monday April 5: WiCyS Chapter Meeting 6:30-8pm

Thursday April 8: CyberEagles Meeting 11-12pm

Thursday April 8: CEDI Meeting Offense Training 6:30-8pm

Friday April 9: NCL Jam 5-6pm

Tuesday April 13: Defense Interest Group Meeting 6:30-8pm

Tuesday April 20: Diversity Inclusion Seminar Series 11am

Wednesday April 21: CTF Interest Group Meeting 6:30-8pm

Thursday April 22: CyberEagles Meeting 11-12pm

Thursday April 22: CTF Interest Group Meeting 6:30-8pm

Friday April 23: NCL Jam 5-6pm

Tuesday April 27: Defense Interest Group Meeting 6:30-8pm

Friday April 30: NCL Jam 5-6pm

Thursday May 6: CyberEagles Meeting 11-12pm

Thursday May 6: CEDI Metting Defense Training 6:30-8pm

May 23-29: NSA Gencyber Camp all day

**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!**

Svool Xbyvi Vztovh! Ru blf xzm wvxlwv gsrh nvhhztv, xlnv gl XVILX Luurxv gl xozrn blfi ivdziw GLWZB!! Nvmgrlm “Vztovh lvzxs”

CLUE: A cipher whose name starts with the letter A and which turns "A" into a "Z", "B" into a  "Y", etc.

## MESSAGE FROM CEROC

After the storm damage last month, you will be happy to know that CEROC is in the process of getting back to our admintrative suites in Prescott 414 this week. We have been very busy this month working on three DoD projects in cybersecurity workforce development and collaborating with partners for future opportunities that we are excited about.

I know you are all very busy…. it’s the last month of the semester! Hope you can still take a moment of your time to enjoy the newsletter.

Keep on swinging your bats! Summer break is just few weeks away.

Sometimes things can seem very challenging BUT do remember:

**There are no secrets to success. It is the result of preparation, hard work, and learning from failure.**

*Colin Powell*

Take care… until next time.

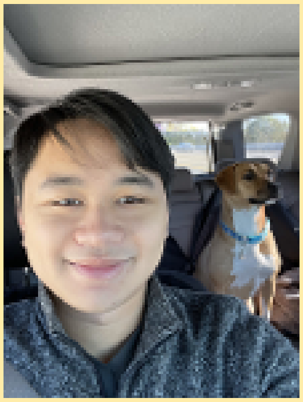
Dr. Ambareen Siraj, CEROC Director, Professor CS, Tennessee Tech

https://www.linkedin.com/in/ambareensiraj/

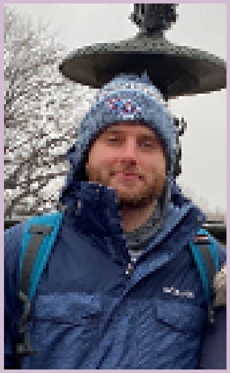
# SCHOLARSHIP STUDENT HIGHLIGHT

**Andrew McDole**

Hello all, I am Andrew McDole, currently completing my master's degree in computer science here at Tech. I have attended the university since the fall of 2016, having moved up from my hometown in Nashville. In my time at Tech, I have met some amazing people. I started off in the dorms living in Evans, and then Madox before moving into an apartment just off campus. Along the way I found myself in the SFS CyberCorps program and began my journey into CyberSecurity. Since joining the program, I have participated in competitions, traveled across the country to conferences, and gained a unique set of skills that were only possible because of the cyber community here at Tech. Going forward, I am looking to work for the Department of Justice. One bit of advice I would give to students faced with indecision is to pick a path begin moving. Doing something, no matter how small puts you ahead of those that are doing nothing at all. I wish everyone here at Tech the best, and I hope that students reading this find amazing success going forward!



# GRADUATING STUDENT HIGHLIGHTS

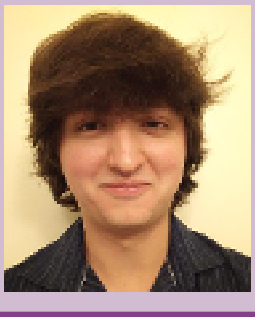


**Joshua Vick**

Hi all! I'm Joshua Vick – a Master's Student and SFS Scholar here at Tennessee Tech studying Cybersecurity. I have enjoyed all my time here! Around my junior year, I got involved with CEROC. I was lucky to get to work with Dr. Siraj and the rest of the team on the GenCyber Camp they run each Summer. After that, I was brought on as a student worker with CEROC. Around that time, I also started working closely with the Defensive Cyber Security Interest Group (DCIG), eventually becoming one of the leads of the group. Working with DCIG and the other interest groups on training material and competitions has definitely been a major highlight of Cyber Security at TTU. When I graduate, I will be working for the federal government. I have previously worked for two National Labs and I am excited to start my career in cybersecurity! Eventually, I am planning to find work with the likes of NASA, SpaceX, etc. Space exploration is my biggest interest so working for someone in that field would be amazing! I cannot overstate the importance of the work that CEROC does for Cyber Security students at TTU. I would most definitely not have been able to achieve as much without their support, along with the support of all my family and friends. For current or future students, Cyber Security is a broad field – try new things and you will find something that fits your interests!

**Jacob Strickler**

My name is Jacob Strickler. I am a fifth-year undergraduate student, and I will be graduating this May. In my time at Tennessee Tech, I have participated in many extracurricular opportunities, and they have shaped not only my college experience, but my interests and aspirations as well. Starting in my freshman year, I began volunteering for outreach events hosted by CEROC, including designing and running activities for Engineering a Future (EaF) and FAB Friday. This led me to volunteer at conferences such as WiCyS, NICE, and ACTE, and to work as a counselor for Tennessee Tech's 2017 and 2018 GenCyber camps. Shortly afterward, I became a CyberCorps SFS scholar, which has allowed me to continue pursuing my education and has exposed me to a community of dedicated, like-minded peers. My advice for students in the program is twofold: firstly, be honest about your own interests and limitations. There are so many opportunities in cybersecurity that one can become easily overwhelmed. Accept opportunities that enrich and excite you, and pass on opportunities that might overburden you. Always remember that no matter how many expectations are placed on you, your life and your future are your own. Secondly, do not be afraid to get involved. We have all felt intimidated or unprepared at some point, and overcoming this fear is an important step to learning. Always put your best foot forward and enter situations with an open mind. You may be surprised at how many wonderful things can happen to you simply because you decided to show up.



# PHD STUDENT HIGHLIGHT

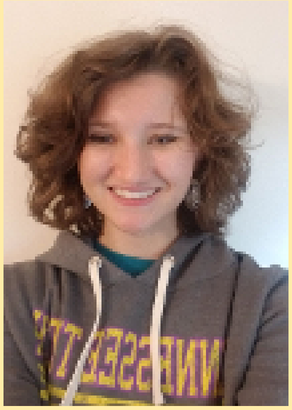
**Ahmed Adel Awad Shafee**

I am Ahmed Adel Awad Shafee, a third-year Ph.D. student at Tennessee Tech University. I am doing my Ph.D. on protecting the electric vehicle infrastructure against cybersecurity attacks, supervised by Dr. Mohamed Mahmoud. My research interests include cybersecurity, machine\deep learning, privacy-preserving machine learning, Adversarial Learning, and Artificial Intelligence. I am from Egypt, which is a very beautiful country in North Africa that is known for its pharaonic civilization. My Tech experience allows me to be open to meet new people and this gives me new insight into new cultures and new traditions. Also, the academic environment of Tennessee Tech enables me to gain a huge knowledge under the supervision of several professional professors who taught me new ways of thinking for solving problems. My advice to the students is to always go after their dreams even if they encounter difficult obstacles during their journey. A single failure does not mean the end of the road; take it as an experience that could be beneficial for you in the future. I plan to apply for teaching and research positions after receiving my Ph.D.

Website:
https://sites.google.com/view/ahmed-shafee-page/home

LinkedIn:
https://www.linkedin.com/in/ahmed-awad-45713454/

# CURRENT STUDENT HIGHLIGHTS



**Mimi Vertrees**

My name is Mimi Vertrees, and I am a cybersecurity freshman attending Tennessee Technological University. I am from Franklin, Tennessee, near the Nashville area, and was homeschooled for most of my life. Although, my time with Tech is just starting, I have learned and experienced a lot this past year at college. I took a deep dive into the computer science community here, being active in the CyberEagles, ACM, and WiCyS clubs while also being a committee member of the CSC Diversity Committee. Additionally, I enjoyed working at iCube for a semester before becoming a student worker at CEROC. Currently, in my free time, I am participating in the Spring season of the National Cyber League (NCL), balancing schoolwork and life, and working on projects at CEROC. While I am still a hardcore rookie, my advice to my peers is to be bold and active in the community here. Attend the meetings, talk in the Discord, reach out to faculty members, do not be shy towards your upperclassmen, and constantly ask questions. It is astonishing how welcoming and inclusive the community here is for those who share the same passion or are merely curious about computers.

Linkedin:

https://www.linkedin.com/in/mimi-vertrees/

**Yoshinori Agari**

My name is Yoshinori Agari, and I am in the second semester of my Sophomore year. I am currently majoring in computer science with a minor in cybersecurity and math. Tennessee Tech has allowed me to learn things in new and creative ways which has really sparked my interests. Being introduced to different cyber interest groups, such as CTF's, has given me the ability to have fun while learning very important skills for future employment. My dream job would be to become a penetration tester, specifically in Japan. Since I am half Japanese, I have several family members in Japan that I don't get to see. The one time I went to Japan, I fell in love with the scenery, culture, and tradition, and I decided that I would want to live there. To be able to achieve this goal I am applying for internships, and consistently looking for CTF experiences. Lastly, for some advice to students, I would suggest finding a hobby to either stay active or get your brain thinking about something else. Getting stuck on an assignment for hours, without taking time for yourself, is more detrimental than you think. Take short breaks and enjoy yourself!

# ACCOLADES

## Grants Awarded:

1. Qatar Foundation, NPRP13S-0205-200270, PI, $600K (TTU share is $85K), 2021 to 2024, “Secure Federated Edge Intelligence Framework for AI-driven 6G Applications”. Collaborator Dr. Mohamed Abdullah (Hamad Bin Khalifa University).
2. Qatar Foundation, NPRP13S-0201-200219, PI, $600K (TTU share is $140K), 2020 to 2023, “Privacy-PreservingHealth Monitoring System Using AI and Non-Intrusive Smart Sensors”. Collaborator Dr. Khalid Abualsaud(Qatar University).

## Publications:

- Sherif Abdelfattah, Mohamed Baza, M. Mahmoud, and Waleed Alasmary, “CSES: Customized searchable encryption scheme with efficient key management over medical cloud data,” International Symposium on Networks, Computers and Communications (ISNCC, June 2021).
- Seham Alansari, Mahmoud Badr, M. Mahmoud, and Waleed Alasmary, “Efficient and privacy preserving contact tracing system for COVID-19 using blockchain,” IEEE ICC 2021 Workshop on Wireless Networking Innovations for Mobile Edge Learning.
- Muneera Alotaibi, Mohamed Ibrahem, Waleed Alasmary, Dawood Al-Abri, and M. Mahmoud, “UBLS: User-based location selection scheme for preserving location privacy,” IEEE ICC 2021 Workshop on Wireless Networking Innovations for Mobile Edge Learning.
- Mahmoud Badr, Mohamed Baza, Sherif Abdelfattah, M. Mahmoud, and Waleed 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).
- 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.
- F.A.Bhuiyan,M.B.Sharif,A.Rahman,"Security bug report usage for software vulnerability research: a systematic mapping study",to appear in the Journal of IEEEAccess,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.
- Deepti Gupta, Smriti Bhatt, Paras Bhatt, Maanak Gupta and Ali Saman Tosun. “Game Theory Based Privacy Preserving Approach for Collaborative Deep Learning in IoT” Accepted in  Deep learning for security and privacy preservation in IoT, Springer.
- 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).
- T. A. Odetola, S. R. Hasan, "SoWaF: Shuffling of Weights and Feature Maps: A Novel Hardware Intrinsic Attack (HIA) on Convolutional Neural Network (CNN)", accepted in in IEEE International Symposium on Circuits and Systems, ISCAS'2021
- A.Rahman and E.Farhana,"An empirical study of bugsin covid-19 software projects",to appear in the Journal of SoftwareEngineering Research and Development (JSERD),2021.
- Ahmed Shafee, Mahmoud Nabil, M. Mahmoud, Waleed Alasmary, and Fathi 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).
- Sai Sree Laya Chukkapalli,  Shaik Aziz, Nouran Alotaibi, Sudip Mittal, Maanak Gupta, and Mahmoud Abdelsalam. "Ontology driven AI and Access Control Systems for Smart Fisheries."  Accepted in ACM SaTC-CPS Workshop 2021.
- D.Ulybyshev,I.Yilmaz,B.Northern,V.Kholodilo,M.Rogers,Trustworthy data Analysisand sensor data protection in cyber-physical systems, to appear in the ACM Workshop on Secure and Trustworthy Cyber-physical Systems (SaT-CPS 2021),Apr 28,2021.
- I.Yilmaz,K.Kapoor,A.Siraj,M.Abouyoussef, Privacy protection of grid usersdata with blockchain and adversarial machine learning, to appear in the ACM Workshop on Secure and Trustworthy Cyber-physical Systems (SaT-CPS2021), Apr 28,2021.
- I.Yilmaz and A.Siraj,"A privacy-preserving energy consumption scheme for smart meterswith adversarial machine learning, to appear in the Journal of IEEEAccess, 2021.

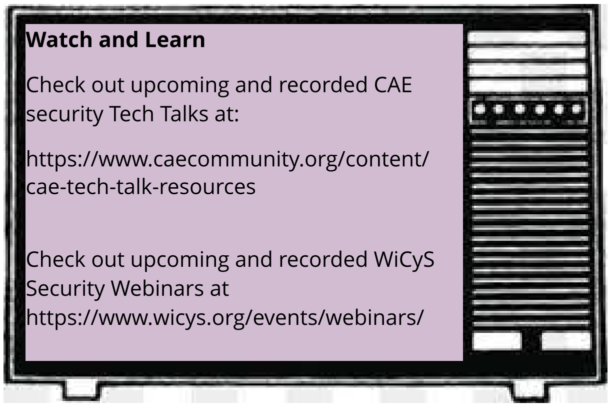
# MEDIA INTERVIEWS

Dr. Maanak Gupta was interviewed by Interviewed by IEEE ComSoc Young Professionals had the opportunity to share his thoughts, experience and research with the IEEE Communication Society Young Professionals group. Here is the full link to read his talk:

https://yp.comsoc.org/yp-chat-dr-maanak-gupta-on-cybersecurity/

Dr. Ambareen Siraj was interviewed by NeoCyber Institute on March 2 as part of their Cyber Career Series and CybHER on March 10 as part of their CybHER Conversations https://www.cybher.org/march-2021/

https://www.neocyberinstitute.net/career-series-recordings



**Watch and Learn**

Check out upcoming and recorded CAE security Tech Talks at:

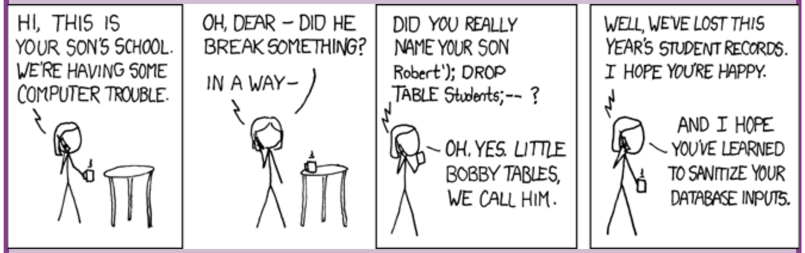
https://www.caecommunity.org/content/cae-tech-talk-resources

Check out upcoming and recorded WiCyS Security Webinars at https://www.wicys.org/events/webinars/

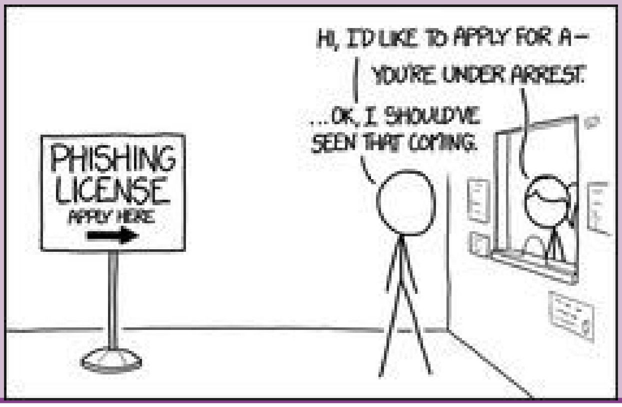
# FUN CORNER

**99 little bugs in the code, 99 little bugs, Take one down, patch it around, 117 little bugs in the code.**

**~ Cameron Winston**


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH, YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

Comics from xkcd.com


HI, I'D LIKE TO APPLY FOR A–
YOU'RE UNDER ARREST.
...OK, I SHOULD'VE SEEN THAT COMING.
PHISHING LICENSE
APPLY HERE

# FACULTY HIGHLIGHT

**Dr. Maanak Gupta**

Dr. Maanak Gupta is an Assistant Professor in the Department of Computer Science at Tennessee Tech University, USA. He received his Ph.D. in Computer Science from the University of Texas at San Antonio and has worked as a Postdoctoral Research Fellow at the Institute for Cyber Security. He also holds an M.S. degree in Information Systems from Northeastern University, Boston. His primary area of research includes security and privacy in cyber space including cyber physical systems, cloud computing, IoT and Big data. Dr. Gupta has worked in developing novel security mechanisms, models and architectures for next generation smart cars, smart cities, intelligent transportation systems and smart farming. His scholarly work is regularly published at top peer-reviewed security venues including ACM SIGSAC conferences and refereed IEEE journals. He was awarded the 2019 computer science outstanding doctoral dissertation research award from UT San Antonio. His research has been funded by the US National Science Foundation (NSF), NASA, US Department of Defense (DoD) and private industry. At Tennessee Tech, he has taught a diverse set of cybersecurity courses at sophomore and senior level. In addition, he will be introducing two graduate courses in AI assisted Cybersecurity and Cloud and Edge security Models and Architectures in the next couple of semesters. His current research NSF supported grant focuses on developing AI assisted Malware Analysis modules for preparing next generation cybersecurity warriors. He has been invited as keynote speaker and delivered guest lectures at various conferences and universities.

## ALUM HIGHLIGHT

**BJ Ledbetter**

My name is BJ Ledbetter. I graduated from Tennessee Tech in both the Spring of 2018 and the Spring of 2019 with my Bachelor's and Master's, respectively. I was a CyberCorps Scholar. The professors were wonderful and helpful, and the opportunities were seemingly endless. Tech and CEROC provided me with so many diverse experiences that have translated quite well into my full-time job as a Computer Forensic Examiner. As a member of the Cyber Defense and Capture the Flag teams, I gained skills and knowledge that I use even today as I review evidence on just about any type of digital storage media. If I had any advice to give, it would be to take advantage of any opportunity that comes your way. You never know what you might enjoy!

## 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**

# ACROSS THE WIRE

Compiled by Ahsan Ayub

**Defense Against Ransomware Attacks**: - According to the recent cyber threat reports, global damage due to ransomware is expected to reach US$ 20 billion this year with recovery from these devastating attacks taking an average of 16 days. Adversaries use different methods to gain the initial access on the target machines, such as phishing emails, vulnerable public-facing software, Remote Desktop Protocol (RDP) brute-force attacks, and stolen accounts. With various tools available, the adversaries can infect multiple machines over the same network. It was reported that before performing the encryption, new ransomware samples would steal sensitive pieces of information about the user to seek leverage against the victim. To combat against this catastrophic attack, researchers and network defenders suggest to do the following:

- Regular back-up of the important files: It is advised to use the 3-2-1 rule, that is to keep 3 back-ups of the data: 2 on different storage types while 1 on offsite.
- Limiting access on the shared/network drives while turning off file sharing mode will help minimize the propagation rate of ransomware infection.
- Incorporating strong secure authentication strategies, e.g., Multi-factor Authentication, will deny adversaries when attempting to access user accounts.
- Disabling local admin account will help prevent admin access by the adversaries.
- Keeping the operating system and the used applications updated will decrease the chances of adversaries exploiting the vulnerabilities..

**Source:**
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-state-of-ransomware-2020-s-catch-22/?utm_source=trendmicroresearch&utm_medium=smk&utm_campaign=0203_StateRansomware

## 2020 Top 10 Industries by Cyber Attack Volume:

**1. Finance and Insurance**

- 28% of attacks were server access attacks while 10% of attacks were ransomware.

**2. Manufacturing**

- 21% of attacks were ransomware while 4x more Business Email Compromise (BEC) attacks experienced in manufacturing companies than any other industry.

**3. Energy**

- 35% of attacks were attempted data theft and leak.

**4. Retail**

- 36% of attacks were credential theft while 18% of attacks were ransomware.

**5. Professional Services**

- 35% of attacks were ransomware (a higher percentage than any other industry) while 13% of attacks were data theft and another 13% were server access.

**6. Government**

- 33% of attacks were ransomware while 25% of attacks were attempted data theft and leak.

**7. Healthcare**

- 28% of attacks were ransomware.

**8. Media**

- 90% of all malicious DNS squatting targeted the media, by far the most-spoofed industry.

**9. Transportation**

- 25% of attacks involved a malicious insider or misconfiguration.

**10. Education**

- 50% of attacks were spam or adware while 10% of attacks were ransomware.

**Source**:

X-Force Threat Intelligence Index 2021 by IBM Security

# ACROSS THE WIRE

**Social Networks as Workplace Attack Vectors**: Organizational emails have been predominantly targeted to launch spear phishing attacks by the cyber criminals. Hence, it is reported that the majority of organizations have implemented spam detection, data loss prevention (DLP), and other solutions to prevent phishing attempts on corporate email accounts. However, McAfee observed and reported a new trend during 2020, that is more sophisticated adversaries are pivoting to target employees via social networking platforms. For example, the adversaries use the messaging features of mainly LinkedIn, WhatsApp, Facebook, and Twitter to engage and develop relationships with corporate employees with a view to compromising the digital assets of enterprises. It has also been observed that gathering information, developing specialized content, and conducting targeted interactions with customers through social media platforms, the adversaries can target high value employees with a deeper level of engagement. As enterprises can only assert security controls over corporate-issued devices and place restrictions on how consumer devices access corporate IT assets, they need to address this situation by providing their employees with additional security awareness training on how to safeguard themselves on different social media platforms to stay secure and agile as well as to reduce the threat surface. McAfee foresees this social network platform vector becoming more common in 2021 and beyond.

**Source:**
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/2021-threat-predictions-report/

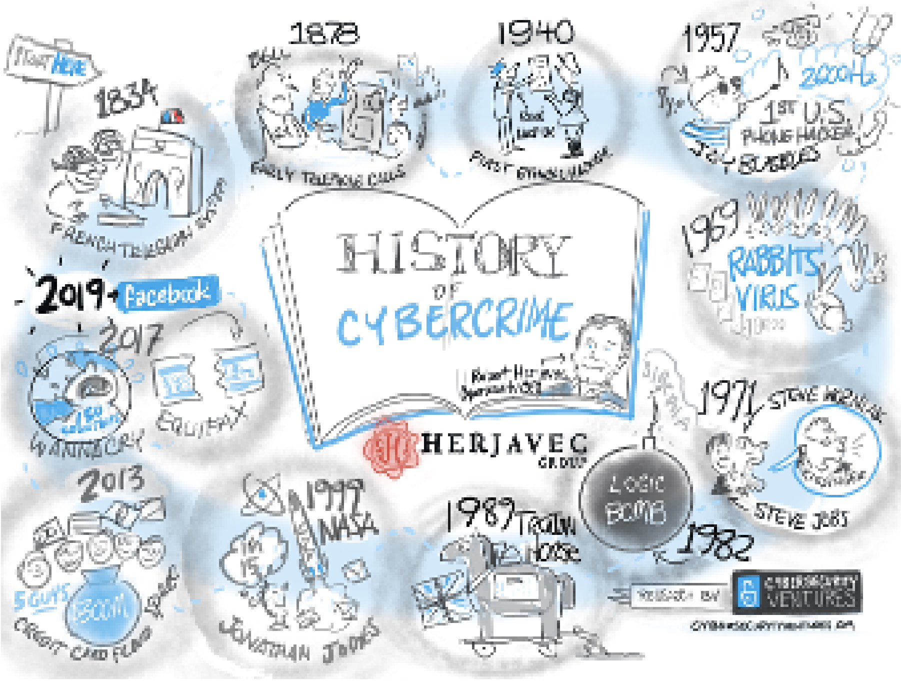
**Defense against Non-Standard Port Attack**: Among 40,000 registered ports, a very few numbers of them are used by the common protocols, such as HTTP and HTTPS use port 80 and 443, SMTP uses port 25. If a service uses a port other than the one assigned to it by default, then it is using a non-standard port. It is reported that the percentage of attacks across non-standard ports grow from 2019's 13% to 25% in 2020. In particular, 46% of all malware attacks came via non-standard ports only in the month of July, 2020. As there are so many ports to monitor and the traditional proxy-based firewalls are typically configured to focus on the standard ports being used, the need of employing advanced security mechanism to protect non-standard ports is paramount. One of the most common defense strategies against non-standard port attack is to apply 'security through obscurity' strategy. Using port 8080 instead of port 80 for web traffic is one of its examples. This will at least keep adversaries confused for a certain amount of time. According to MITRE, Network Intrusion Detection and Prevention Systems, that use network signatures to identify traffic for specific adversary malware, can be used to combat against this type of attack. Additionally, we can also properly configure firewalls and proxies to limit outgoing traffic to only necessary ports for a particular network segment. Security researchers have been proposing different schemes that analyze packet contents to detect communications that do not follow the expected protocol behavior for the port that is being used and network data for uncommon data flows, e.g., a client sending significantly more data than it receives from a server.

**Source:**
https://attack.mitre.org/techniques/T1571/
· SonicWall Cyber Threat Report 2021:
https://www.sonicwall.com/medialibrary/en/white-paper/2021-cyber-threat-report.pdf

# SECURITY RESEARCH SHOWCASE

## Companion Assisted Remote Attestation in Embedded Systems

William A. Johnson, his supervisor Dr. Sheikh Ghafoor, and collaborating researcher Dr. Stacy Prowell from Oak Ridge National Lab have been investigating remote attestation for embedded systems. Their most recent work “Companion Assisted Software Based Remote Attestation in SCADA Systems” was published in the 16th International Conference on Cyber Warfare Security. An embedded system cannot be secured if it is not trustworthy. Remote attestation is a security protocol designed to determine if the embedded system is trustworthy by detecting malware as the system runs. One key challenge to remote attestation is the root of trust. How can evidence provided by an embedded system be trusted if the embedded system cannot be trusted? Three roots of trust exist in modern remote attestation research: hardware, software, and hybrid. Hardware schemes design new hardware features to be added to future embedded systems during manufacturing. Software schemes use strict timing and known execution times to detect cheating during attestation. Hybrid schemes use a combination of existing hardware features with new software to detect ensure message trustworthiness. Hardware and hybrid schemes offer greater assurances of trustworthiness, but they rely on specific hardware features that may not be accessible in existing embedded systems. On the other hand, software schemes target the largest group of embedded systems, but they do not offer strong trustworthiness because they rely on very strict assumptions. William et al. proposed a new device to assist with attestation: the companion. The companion is an Field Programmable Gate Array (FPGA) that is attached to the embedded system via a dedicated line. By using the companion, William et al. were able to offer a stronger software based remote attestation scheme that still covers a very wide range of existing embedded systems.



Cartoon from Cybercrime Magazine:
https://cybersecurityventures.com/cybercrime-infographic/

# SECURITY TOOLBOX

NMAP – Nmap (Network Mapper) is a free open-source tool for network discovery and security auditing. It uses IP packets to find out various information about a network, such as open ports, running services, number of hosts, etc. While Nmap was originally designed to quickly scan a large network, it also works well scanning smaller networks or single hosts for vulnerabilities in the hosts or services running on them. Nmap is also supported by most operating systems with both GUI and command-line interfaces making it very portable. Nmap has become one of the most popular tools used by offensive security specialists and is included in many offensive security toolboxes such as Kali Linux.

https://nmap.org/

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

**Contributes by: Jeremy Potts**

# OPPORTUNITIES IN CYBER

**CEROC Summer Internship:** 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**

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

**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 bellow!.

**https://iamcybersafe.org/s/raytheon-womens-scholarship**

**Summer Smart City Security Research Experiences for Undergraduates (REU):** Undergraduate students who are interested in a summer research experience please apply for the 2021 Summer REU on Secure and privacy-preserving cyber physical systems, and feel free to The site website is **http://www.cae.tntech.edu/~mmahmoud/REU/REU.htm**. Apply soon, the deadline was extended to April 7!

**Secure Web Programming Competition:** The competition is structured in 5 short challenges, each of which focuses on a different topic in web security. In each challenge, you will be shown a code snippet written in HTML and PHP. Your task will be to learn more about specific security aspects, identify problems in the code, and fix any vulnerabilities. To assist you in your work, we developed a chatbot that you can interact with to obtain answers to questions about secure web programming and get code snippets that can help you solve the challenge. The deadline for entering the competition and completing the challenges is **April 15th, 2021 at midnight.** Make an account here: **https://kosh.nku.edu/spbot/auth.php?action=signin**

**NSF Education Grant: Summer Social Engineering Penetration Testing Competition:** The CARE (Cybersecurity in Application, Research and Education) Lab at Temple University is hosting the FIRST ever Social Engineering (SE) Penetration Testing Competition COMPLETELY ONLINE this summer in light of the covid-19 pandemic! Please visit **https://sites.temple.edu/care/se_pentest/** for more information on eligibility and deadlines! Applications are being accepted from NOW till April 15th!

Please note that this is **NOT** a technical CTF like CCDC, CPTC, etc. Student teams **do NOT** need to have skills or experience in pen testing, digital forensics, etc.

**Summer BlockChain Security Research Experiences for Undergraduates (REU)::** We will support participants of this intensive program in 9 weeks to build their knowledge, skills, and expertise, gain their impactful research experiences and provide suggestions on their career choices. Women and students from other underrepresented groups and/or schools with limited STEM research capacity are highly encouraged to apply.

The application deadline is Sunday, April 11, 2021. For more information, check the REU Site homepage at: **https://sites.google.com/boisestate.edu/reu-blockchain/home**

**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**

**Give us your feedback about EaglesReach!**