CFIC@SHSU

Sam Houston State University

Cyber Forensics Intelligence Center Newsletter

TABLE OF CONTENTS

CFIC MISSION

To conduct world-class, leading cyber forensics and security research, provide real-world training solutions, investigate cutting edge cyber forensic investigation resources; promote professional networking; and participate in open data exchanges.

GOALS

To bring together leading industry participants, practitioners, and faculty members from a variety of disciplines to research cyber forensic and digital security topics that are of interest to governmental, commercial and legal communities in order to:

- Deliver innovative, avant-garde, pioneering research expertise in security and forensics that solves real-world problems
- Partner with governmental, commercial, and legal communities to improve workforce education through world-class training programs
- Provide state-of-the-art research facilities, equipment, and training that empowers faculty to pursue substantial research funding
- Deliver to governmental, commercial, and legal communities a collaborative operational and investigative ecosystem for identifying and resolving cyber forensics and security challenges

DIRECTOR'S MESSAGE

I hope everyone is staying safe in this COVID-19 environment. The CFIC is adhering to social distancing guidelines and not having face-to-face interactions with students or industry partners. Fortunately, technology is bridging the social distancing gap and enabling us to continue interacting to accomplish our goals. The CFIC lab is virtually operational for students and researchers through strong maintenance efforts by essential employees.

Spring of 2020 is off to a productive start. We are proud of our CCDC team for making it to regionals this year, and we are looking forward to competing next year! The CFIC is hosting an internal virtual undergraduate student Cybersecurity competition in May 2020. Stay tuned to the CFIC Web site for competition videos! The internship program is growing; we place an intern with a new industry partner.

In the fall of 2020, the Digital Forensics Information Intelligence (DFII) research group will meet weekly to explore current areas of research and development on all things Digital Forensics. If you are interested in giving a presentation, please let us know. Industry insight is critical to producing well rounded digital forensics and cybersecurity students. Speaking of industry input, I would like to thank the CFIC/DCS Advisory Board for their time, participation and a very successful meeting in March. The board made many great improvement suggestions for the CFIC, and the entire DCS that are already prompting action plans.

Please welcome my administrative assistant, Kaci Moore, Kaic is indispensable to supporting my endeavors, CFIC student and faculty activities. As the situation with COVID-19 continues to evolve rapidly, I encourage you to follow the CFIC through social media on Facebook, Twitter, and LinkedIn. We provide daily updates on global cybersecurity issues, as well as pertinent center information. We look forward to finishing the Spring semester with great success, and I look forward to leading the CFIC to continued innovation, advancement, and growth to reach our goals and support collaborations with industry partners.

CYBERSECURITY COMPETITION MAY, 2020
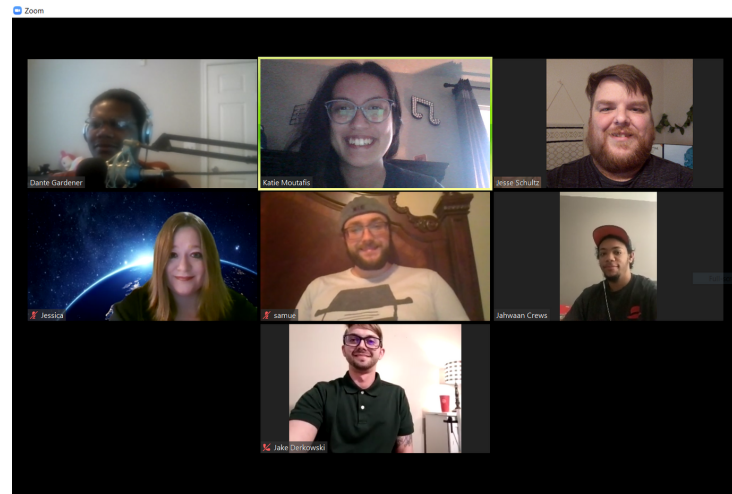
CCDC COMPETITION

CFIC is hosting a virtual internal undergraduate student CyberSecurity competition in May of 2020 for students participating in the DFSC 4317 Information Security Class. Student teams will present, via YouTube video submissions, CyberSecurity research projects for this competition of their choosing.

Two awards will be presented for this competition. The first award is for the most industry-relevant and innovative project. The CFIC advisory board will formally review and judge each submission for this award. The CFIC advisory board consists of industry specialists in cybersecurity and software engineering.

The second award will be judged and decided by the community at large via voting on the projects presented on Youtube.

The general criteria for the ranking include:
- Overall clarity and presentation
- Originality, creativity, and significance
- Accuracy of data analysis, conclusions, and discussion impact

The mission of the Collegiate Cyber Defense Competition (CCDC) system is to provide institutions with an information assurance or computer security curriculum a controlled, competitive environment to assess their student's depth of understanding and operational competency in managing the challenges inherent in protecting a corporate network infrastructure and business information systems.

CCDC competitions ask student teams to assume administrative and protective duties for an existing "commercial" network – typically a small company with 50+ users, 7 to 10 servers, and common Internet services such as a web server, mail server, and e-commerce site.

The Sam Houston CCDC team made it through the Southwest Regional CCDC qualifiers and, despite the challenges of working as a team remotely, were able to compete in the regional competition.

We are extremely proud of our team and celebrate how hard they've worked this year. We look forward to carrying this knowledge and experience forward to next year's competition!

CALL FOR PAPERS

HICSS 54
SHIDLER COLLEGE OF BUSINESS
January 5-8, 2021 | Grand Hyatt Kauai

Call for Participation

Cyber Operations, Defence and Forensics Mini-track In the Software Technology Track

We welcome new, original ideas from people in academia, industry, government, and law enforcement who are interested in sharing their results, knowledge, and experience. Topics of interest include but are not limited to:

- Detection and analysis of advanced threat tactics, techniques, and procedures
- Applying machines learning tools and techniques in terms of cyber operations, defences and forensics
- Case studies surrounding the application of policy in terms of cyber operations, defences and forensics
- Approaches related to threat detection and Advanced Persistent Threats (APTs)
- Solutions that secure different types of data stored in different layers of computer networks
- "Big Data" solutions and investigations – collection, analysis, and visualization of "Big Data" related to cyber operations, defences and forensics
- Malware analysis and the investigation of targeted attacks
- Device investigations that assist with the recovery and reconstruction of digital artifacts
- Digital evidence recovery, storage, preservation, and memory analysis
- Event reconstruction approaches and techniques
- Anti-forensics techniques and solutions
- Investigations related to mobile devices, embedded systems, or Internet of Things (IoT) devices
- Forensic investigations within emerging domains such as transportation systems, industrial control systems, and SCADA
- Network investigations – collection, analysis, and visualization of network forensic data
- Privacy implications related to security incident response and digital forensic investigations
- Research in security incident management
- Situational awareness related to security incident response
- The impact of digital evidence on the legal system

The above list is suggestive, and authors are encouraged to contact the mini-track chairs to discuss related topics and their suitability for submission to this mini-track.

Call for Papers, HICSS 54 will be here before you know it! Start thinking about your Papers. Please contact the Mini-track Chair, Dr. Brad Glisson with any questions @ glisson@shsu.edu.

KACI MOORE
CFIC ADMINISTRATIVE ASSISTANT

Kaci Moore joined the CFIC team in October 2019 as Dr. Glisson's administrative assistant. Kaci supports the center by fielding incoming calls, answers general inquiries, aids in facilitating project progression, identifying and tracking grant application requirements, and performs administrative tasks related to the center.

Kaci is a native Texan. In her downtime, she loves to go for a run and spend time with her dog and family.

Kaci is excited to see what the CFIC accomplishes in the future. She is indispensable in aiding Dr. Glisson and the CFIC with continued growth and the support it offers to SHSU students and faculty.

Partnerships

Internship Program

Organizations partner with the Center to provide on-site internship experiences to students enrolled in the Department of Computer Sicence at SHSU to assist in workforce development.

*Positions available now on jobs4kats

Capstone Project

Provides students with the opportunity to interact with industry while simultaneously introducing them to practical research. These projects are conducted in conjunction with industrial partners at no cost to the organization.

Seminar Presentations

Industrial partners are invited to make presentations during the fall and spring semesters on challenges that they face from cybersecurity, digital forensics, and information assurance perspectives.

CONTACT THE CFIC

Cyber Forensics Intelligence Center

1803 Avenue I, AB1 Room 208

P.O. Box 2090

Huntsville, Texas 77341

Phone: 936.294.4768 Fax: 936.294.4312

Email: cfic@shsu.edu

Directions

I-45, Huntsville, TX 77340 to Avenue I, Huntsville, TX 77340

1.Depart I-45, Huntsville, TX 77340
2. Turn East onto US-190 [SR-30] for 1.1 miles.
3. Turn Right(South) onto SR-75 [N. Sam Houston Ave] for 0.4 miles.
4. Turn Left(East) onto 16th St. for 0.2 miles.
5. Turn Right(South) onto Avenue I for 0.1 miles.
6. Arrive Avenue I.
The Cyber Forensics Intelligence Center is located in AB1 Room 208