CFIC@SHSU

Sam Houston State University

Cyber Forensics Intelligence Center Newsletter

TABLE OF CONTENTS

WHAT IS THE CFIC?

The Cyber Forensics Intelligence Center at SHSU is dedicated to the advancement of cyber forensic and security research, practices, and education. Together with Researchers and Industry Leaders the Center is affirmed to the vision of social progress through cyber forensic and security innovation.

MISSION STATEMENT

To conduct world-class, leading-edge cyber forensic and security research to resolve real-world challenges.

RESEARCH AREAS

*Artificial Intelligence
*Bioinformatics
*Cryptography
*Data Mining
*Information Security
*Internet of Things
*Multimedia Forensics
*Operating Systems
*Steganography
*Wireless Networks

MEET THE NEW DIRECTOR

I am the Director of the newly revamped Cyber Forensics Intelligence Center and an Associate Professor in the Department of Computer Science at Sam Houston State University.

The focus of my current research is Digital Forensics, Information Assurance, Software Engineering and Applied Computing Science with specific interest in the security, business and health care implications associated with residual data. This encompasses a wide range of research including, theoretical research focusing on the integration of security into large scale development practices along with investigating ways to improve information security incident response, empirical research based on industrial collaborations, software engineering solutions to forensics and security issues along with the development of practical methods for evaluating applied real-world computing solutions.

The CFIC is partnering with industry to perform research that impacts all stages of the business model. We are seeking new industry partners, so call or email us with research initiatives and proposals!

Recent Publications

Brown, A.J., W.B. Glisson, T.R. Andel, and K.-K.R. Choo, Cloud forecasting: Legal visibility issues in saturated environments. Computer Law & Security Review, (2018)

Daniel Bradford Miller, William Bradley Glisson, Mark Yampolskiy, Kim-Kwang Raymond Choo: Identifying 3D printer residual data via open source documentation. Computers & Secuirty 75: 10-23 (2018)

Patrick Luckett, Jeffrey Todd McDonald, William Bradley Glisson, Ryan Benton, Joel Dawson, Blair A. Doyle: Identifying stealth malware using CPU power consumption and learning algorithms. Journal of Computer Security 26(5): 589-613 (2018)

HEDERA HACKATHON 2018

The Hedera18 hackathon was the first global, decentralized hashgraph hackathon, gathering developers to compete in nine cities around the world: Dallas, San Francisco, London, Paris, Bangalore, Moscow, São Paulo, Singapore, Tel Aviv. This three-day event offered developers the opportunity to build what's next in fast-moving industries, including: gaming, social causes and micro-payments.

Sam Houston State University students competed with teams around the world for the title of Hedera18 Hackathon Global Winner. Following the competition they gained access to educational sessions presented by the Hedera team, industry experts, and ecosystem developers, where they had the opportunity to learn how to build a new class of decentralized applications (dApps). Congratulations to these students on your hard work and success!

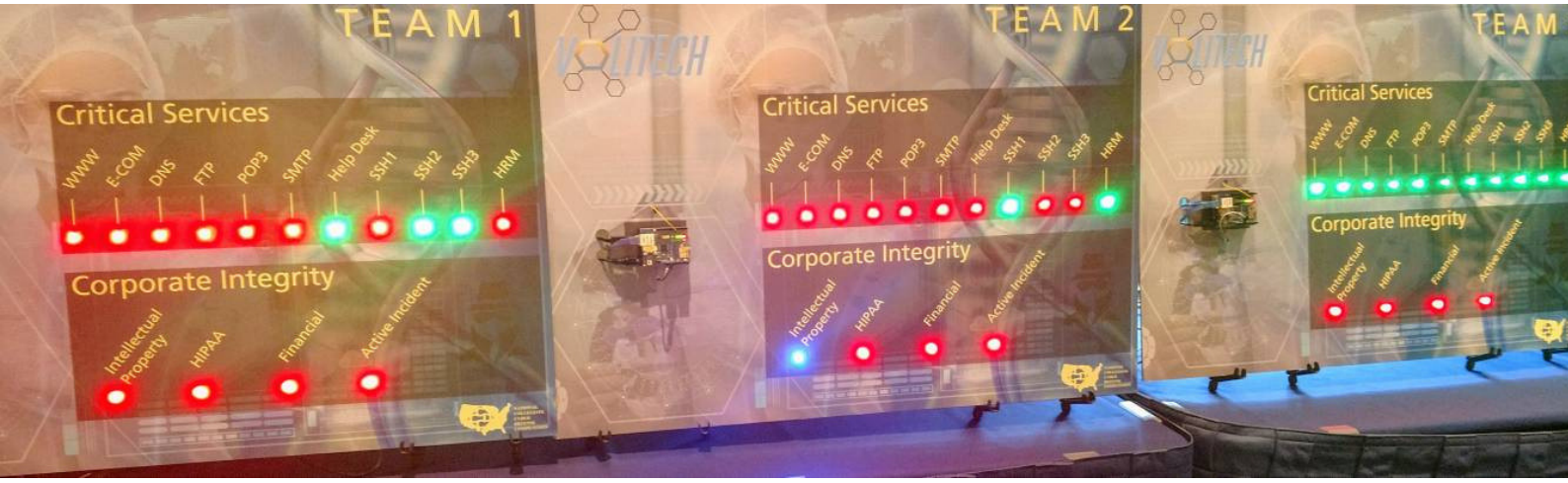
Email CFIC@SHSU.edu for information or to join next years team

H.I.S.D ROBOTICS WORKSHOP

The Department of Computer Science at SHSU periodically supports Robotic Workshops for middle school students. The first workshop took place in 2015. These workshops strive to initiate interest in computer science concepts at an early age. Dr. Li-Jen Lester organizes and supports this initiative in the Department of Computer Science. The most recent workshop took place in November 2018.

Dr. Li-Jen Lester recruited six seniors in her COSC4349, Professionalism and Ethics class, to be trained as instructors and mentors. These students helped to deliver the robotics hardware aspects of the curriculum. The assistance helps guide the middle schoolers when they are building their team vehicle. This workshop focused on the hardware aspects of building a robot. The middle schoolers have already inquired about coming back again next semester to continue developing their robots through software development. The impact of this workshop is not only to motivate middle schooler desires from a technology perspective but also to encourage our college students to make a difference in the community. These mentors fulfilled the motto of SHSU: "The measure of a life is its service!"

JOIN THE CFIC COLLEGIATE CYBER DEFENSE COMPETITION TEAM



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.

Each team begins the competition with an identical set of hardware and software and is scored on their ability to detect and respond to outside threats, maintain availability of existing services such as mail servers and web servers, respond to business requests such as the addition or removal of additional services, and balance security needs against business needs.

Throughout the competition an automated scoring engine is used to verify the functionality and availability of each team's services on a periodic basis and traffic generators continuously feed simulated user traffic into the competition network. A volunteer red team provides the "external threat" all Internet-based services face and allows the teams to match their defensive skills against live opponents.

Stop by CFIC at AB1 208 to sign up today!!!

NATIONAL COLLEGIATE CYBER DEFENSE COMPETITION

CALL FOR PAPERS

Cybersecurity Investigations and Digital Forensics Mini-track

In the Software Technology Track

As technology is incorporated into more aspects of daily life, cybersecurity and digital forensics evolve and diversify. This results in the need to develop innovative managerial, technological and strategic solutions. Hence, a variety of responses are needed to address the resulting concerns. There is a need to research a) technology investigations, b) technical integration and solution impact, c) the abuse of technology through attacks along with d) the effective analysis and evaluation of proposed solutions. Identifying and validating technical solutions to access data from new technologies, investigating the impact that these solutions have on the industry, and understanding how technologies can be abused is crucial to the viability of commercial, government, and legal communities.

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:

- Anti-forensics techniques and solutions
- "Big Data" investigations - collection, analysis, and visualization of "Big Data" related to security incident and digital forensic investigations
- Data/information dissemination about threats, attacks, and incidents resulting from security incident investigations
- 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
- Forensic investigations involving cloud and virtualized environments
- Forensic investigations within emerging domains such as transportation systems, industrial control systems, and SCADA.
- Investigations related to mobile devices, embedded systems, or Internet of Things (IoT) devices
- Malware analysis and the investigation of targeted attacks
- 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 53 will be here before you know it! Start thinking about your Papers for the Cybersecurity Investigations & DigitalForensics Mini-track. Please contact the Mini-track Chair, Dr. Brad Glisson with any questions @ glisson@shsu.edu.

PH.D. IN DIGITAL AND CYBER FORENSIC SCIENCE

The new Doctor of Philosophy in Digital and Cyber Forensic Science is designed to produce students of the digital forensics and cyber-security realms with the technical skills, critical thinking ability, problem-solving skills, and advanced, discipline-specific knowledge to allow them to advance into leadership positions in business and industry as well as academia.

This is accomplished by demonstrating the ability to perform independent and collaborative original research, the successful completion of academic coursework, hands-on experience in the laboratory, and collaboration with digital forensics and cyber-security agencies, institutes, and partners. The program will provide students with the theoretical, conceptual, methodological, and computational skills needed to understand the role of digital and cyber forensic science in post technological societies.

The program will allow students to explore the potential for forensically sound digital data capture and analysis and to develop new tools and methods for handling digital and cyber forensic evidence. In doing so, this program has, as its primary focus, research into the computational and scientific basis for forensic and cyber technologies.

Get more information and apply at SHSU.com

UPCOMING SPEAKER ANDY BENNETT

Andy Bennett is a boot wearin' native Texan who serves the State of Texas as the Deputy Chief Information Security Officer. He has a diverse IT background covering 22 years of experience in roles across the enterprise and in a variety of sectors including government, banking, higher education, applied research, oil and gas, law enforcement, Fortune 500 consulting services, and more. He specializes in incident response, investigations, and change efforts and has a passion for security. He is the primary author of the State of Texas' incident response redbook template and is involved in strategic planning and rulemaking at the statewide level. His professional philosophy is "Show works better than tell, every time."

Strategic Planning: A Core Security Component

This is sure to be a lively and thought provoking discussion on strategic planning as a critical security function. It will cover a wide range of strategic planning topics from stakeholder engagement and cross functional alignment to resource planning and how to project out 5 or more years in such a rapidly changing field. Throughout the discussion, the State of Texas Cybersecurity Strategic Plan will be used to guide and inform the discourse using a concrete example. This will be an interactive session with plenty of opportunity for attendees to participate and make the most of the event.

PREVIOUS SEMINAR SPEAKER ALEJANDRO VILLEGAS

Alejandro is the Head of security engineering for Amazon Physical Stores, and previously Amazon Finance. Security evangelist that has held engineering roles at Amazon, Microsoft, F5 Networks, Hewlett-Packard, cPanel and Softlayer (IBM). Ethical hacker with a diverse educational and professional background (alphabet soup upon request) obsessed with security engineering, due diligence, and customer trust.

Alejandro enjoys attending security conferences, publishing security papers, and developing security tools with the ultimate purpose of protecting hardware, firmware and software to safeguard: 1) customer trust, 2) unintended distribution of cash, and 3) the confidentiality, integrity and availability of personal and financial data. Active in the security industry and a public speaker that has recently presented at external and internal conferences such as the International Symposium on Digital Forensics and Security (Turkey and Romania), the International Multi-Conference on Complexity, Informatics and Cybernetics (Florida), the CISO Global Forum (Atlanta), Secure World Seattle and Portland, BSides San Diego, BSides Edinburgh (UK), Cloud Security Alliance (Seattle Chapter), FinSecCon '18, and FinTech RiskCon '18.

We thoroughly enjoyed Alejendro's presentation. In case you missed it, here is a synopsis of his talk.

Security Engineering: A Pragmatic Deep Dive Into the Intricacies of this Challenging and Ever-evolving Realm.

What does 'Security Engineering' really mean? What kind of skills does it take to become a well-rounded full stack Security Engineer? How do you protect your stakeholders via holistic end to end security engineering methodologies? What are some of the current cyber security and forensic challenges? This talk is meant to be interactive and the goal is to provide students with an insight into the expectations of this field as a Security Engineering professional.

Future Speakers

April 8: Andy Bennett, Deputy CISO, State of Texas
Topic: Strategic Planning as a Core Security Component

April 15: Dr. Bing Zhou, SHSU
Topic: Improving Database Security with Pixel-based Granular Encryption

April 22nd & 29th: PhD in Digital and Cyber Forensic Science Presentations

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.

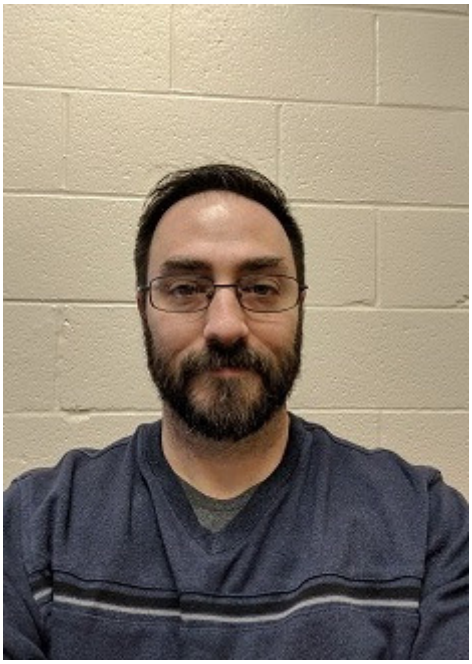
Seminar Presentations

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.

MEET THE TEAM

Christopher Arcos, M.A.
Program Manager
arcos@shsu.edu
936-294-2479

Chris is from Houston, Texas and an alumnus of Sam Houston State University. He graduated with a double bachelor's in Political Science and Criminal Justice and a Masters in Higher Education Administration. In his free time, Chris enjoys going to concerts, checking out the latest movies, and traveling with his wife and friends. He is excited about the research opportunities with industry partnerships that the Cyber Forensics Intelligence Center will bring to the students of SHSU, and looks forwards to helping the center achieve its mission.



Dustin Thornton
Lab Manager
dustin.thornton@shsu.edu
936-294-4785

Dustin is a graduate of Sam Houston State University and is the Lab Manager for the Cyber Forensics Intelligence Center. He has 15 years of experience working in Information Technology and likes to tinker and understand the ever-changing world of technology in his spare time, building a variety of toys and small-scale systems. He is happy to be part of the Cyber Forensics Intelligence Center team and looks forward to helping the Center grow. As a new father, Dustin spends as much time as possible with his wife and son.

Megan Ellisor
Administrative Assistant
mme014@shsu.edu
936-294-4768

Megan is the administrative support to Dr. Glisson. Megan assists with building relationships with industry and business clients as well as assisting with community and educational outreach for the CFIC. Megan greets visitors and can answer many of the questions about the center. Megan graduated from Sam Houston State University with her business degree and in her spare time likes to travel, watch the latest Netflix shows, and enjoys spending time with her friends, family, and cat Chloe.

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

TM