The Virtual Institute of Cyber Operation and Research (VICOR)

Presents

2nd ANNUAL RESEARCH SHOWCASE

Monday, May 13, 2024

9:00 am – 12:45 pm

Online

The Virtual Institute of Cyber Operation and Research (VICOR) is a Department of Defense (DoD) funded initiative between the University at Albany and Florida International University (FIU) that aims to train the next generation of cybersecurity professionals for future military and civilian leadership positions. It is a competitive program aimed at providing students the opportunity to develop essential cyber operational skills and leadership skills.

VICOR – Research Showcase, April 28, 2023

Schedule at a Glance

All times are Eastern Daylight Time (EDT).

8:45am – 9:00am	**Join the session**
9:00am – 9:05am	**Welcome and Opening Remarks**
9:05am – 9:25am	Privacy Preserving Route Comparison with Homomorphic Encryption *Allan Luedeman, Nicholas Baum*
9:25am – 9:45am	Analysis of Space Infrastructure Dependencies and Their Cascading Impacts *Ethan Fowler, Matthew Niemczyk, Sebastian Hernandez, Trenton Hanan*
9:45am – 10:05am	Exploring Cybersecurity Concerns of Drone-to-Drone Communications *David Balzora, Edward Grisham, Aron Jones, Jacky He, Shoshanna Kusa*
10:05am – 10:25am	Generative AI in Cybersecurity: Opportunities, Risks, and Impacts *Noelle Capodieci, Chris Sanchez-Adames, Joseph Harris*
10:25am – 10:45am	Cyber Threat Actor Psychological Profiling Utilizing Active Defense Mechanisms *Shannon Morgan, Richard Kohler, Nikolas Novikov, Adam Louis*
10:45am – 11:05am	Investigating the Effectiveness of Collegiate Cybersecurity Competitions Developing Practical Skills and Student Success *Liam Mengler*
11:05am – 11:25am	Anonymous: Privacy and Confidentiality Concerns and Solutions in Autonomous Vehicles *Aneeha Sahar, Daniel Peck, Sharie Rhea, Tayquan Sneed, Karina Hernandez*
11:25am – 11:45pm	Fortifying Security and Stability: The Case for a Federal Cyber Insurance Backstop *Brianna Bace*
11:45pm – 12:05pm	A Framework for Automated Data Loss Prevention Against Insider Threats in Sensitive Environment *Jason Masters, Sean Caruso, Connor Bowden*
12:05pm – 12:25pm	Integration and Evaluation of Post-quantum TLS within 5G User Registration Function *John Evanchik, Luisa Cartagena*
12:25pm – 12:30pm	**Closing Remarks**

ABSTRACTS

Privacy-Preserving Route Comparison with Homomorphic Encryption
Allan Luedeman, Nicholas Baum
Mentor: Dr. Kemal Akkaya
Time: 9:05am – 9:25am

As drones are more readily used for activities such as delivering packages, there are concerns that they could collide. An option could be for all drones to share their path. However, we would not want to compromise user privacy by publicly sharing paths with other drones. To address this concern, we propose using homomorphic encryption to have drones be able to determine which path segments a collision would occur. We perform our testing on a VM with similar specs to a Raspberry Pi 4 to emulate the limited computational power a drone may have. Our results have shown that drones can compute if any collision occurs within a few seconds.

Analysis of Satellite Systems' Dependencies and Their Cascading Impacts
Ethan Fowler, Matthew Niemczyk, Sebastian Hernandez, Trenton Hanan
Mentor: Dr. Omer Keskin
Time: 9:25am – 9:45am

Space infrastructure systems play a crucial role in modern society, underpinning various critical functions. This study investigates the complex network of interdependencies within the space infrastructure sector, specifically in satellite systems, and their potential cascading impacts in the face of cyberattacks. The research aims to define and quantify these interdependencies, providing insights into their characteristics and implications. This study involves the application of Functional Dependency Network Analysis, employing a graph-based mathematical approach to analyze the propagation of impact resulting from diverse cyberattack disruption scenarios. Simulated cyber scenarios focus on targeting space infrastructure, offering a detailed examination of the cascading effects within this vital sector. The results of the study include the identification of critical functionalities and improving the cybersecurity of satellite systems. The implications of the results would be beneficial for the threat modeling and design phase of satellite systems to result in higher cyber resiliency.

Exploring Cybersecurity Concerns of Drone-to-Drone Communications
David Balzora, Edward Grisham, Aron Jones, Jacky He, Shoshanna Kusa
Mentor: Dr. Alexander Pons
Time: 9:45am – 10:05am

The proliferation of uncrewed aerial vehicles (UAVs), or drones, has led to their increasing integration into the modern day. The demand for swarms of low-cost, mission-specific drones is ever-increasing. Flying ad-hoc networks provide an advantage to drone swarms due to their innate decentralized mesh topology. Many studies have considered the security of such drones, but few have investigated the susceptibility of Denial of Service (DoS) attacks and eavesdropping on decentralized networks. Examining the resilience of this network architecture against various DOS attack vectors and evaluating the effectiveness of employing security protocols such as WPA3, intrusion detection systems (IDS), machine learning anomaly detection, and access control policies may provide new avenues of securing communications between UAV swarms. Our results show promising insights into anomaly detection and security protocols that combat attacks in Ad-hoc UAV swarms.

Generative AI in Cybersecurity: Opportunities, Risks, and Impacts
Noelle Capodieci, Chris Sanchez-Adames, Joseph Harris
Mentor: Dr. Unal Tatar
Time: 10:05am – 10:25am

This paper explores the evolving role of Generative AI (GenAI) and Large Language Models (LLMs) in cybersecurity. The motivation behind this research is the rapid advancement of GenAI technologies and their potential implications for cybersecurity professionals. This work focuses on assessing how GenAI and LLMs influence cybersecurity practices, including both the opportunities and risks they present. It specifically examines the use of GenAI in cybersecurity, its functions and industries, and the potential impact on the profession. The methodology involves conducting semi-structured interviews with cybersecurity professionals to gather insights on their experiences and perspectives regarding GenAI and LLMs. This qualitative approach allows for a deep exploration of the subjective experiences of these professionals in their work environments. The results indicate a cautious approach towards the adoption of GenAI in cybersecurity. While some professionals have begun to utilize these technologies, there are concerns regarding ethical and safety considerations, information security, and the potential for GenAI to influence the nature of cyber threats. The findings highlight the need for a balanced approach that recognizes the potential of GenAI while addressing the associated risks.

Cyber Threat Actor Psychological Profiling Utilizing Active Defense Mechanisms
Shannon Morgan, Richard Kohler, Nikolas Novikov, Adam Louis
Mentor: Dr. Sanjay Goel
Time: 10:25am – 10:45am

Cybersecurity can greatly benefit from the insights of psychology, and this research demonstrates the significance of integrating psychological principles into threat mitigation strategies. By understanding the psychological factors that influence human behavior, cybersecurity professionals can develop more effective countermeasures against threats. This paper delves into multiple forms of cognitive bias that can be exploited and the tactics used to trigger these biases within a virtual honeypot system. A honeypot is a decoy system set up to attract and monitor threat actors. By understanding and manipulating cognitive biases, we can create more effective honeypots. Cognitive biases, inherent in human decision-making, can be both a pro and a con. While they offer mental shortcuts, they can also lead to irrational judgments.
This research paper explores how these biases can be leveraged in cybersecurity, particularly in the development of hacker profiles and active defenses. The aim of this research is to understand how cognitive bias can be leveraged as vulnerabilities in threat actors. Utilizing experimental research methodology, we created a custom honeypot system with cognitive bias focused active defenses and recruited participants to hack this system. Researchers were able to qualitatively analyze participants' reactions and their ability to complete the attack. Using common patterns found in the results, we determined which bias was most effective and created a use case profile for the participant who did best during the study. Ultimately, this paper outlines the processes used to trigger psychological vulnerabilities some threat actors possess. With some additional testing, researchers could build complete hacker profiles from the results of the analyzed data set. This research, particularly the active defense part, could be applied to an organization's most secure servers to mitigate risk during a cyber intrusion. This research can also be applied to understanding cyber threat actors with the goal of prevention and deterrence.

Investigating the Effectiveness of Collegiate Cybersecurity Competitions Developing Practical Skills and Student Success
Liam Mengler
Mentor: Dr. Unal Tatar
Time: 10:45am – 11:05pm

Cybersecurity students often do not expand their horizons beyond their coursework and miss out on hands-on opportunities. This research explores the positive effects of practical cybersecurity competition experience and the enterprise architecture of a competition system, the Great Dane Defense Competition (GDDC). GDDC is an in-house program at the University at Albany designed to provide students with practical cybersecurity experience. Students play the

role of a blue teamer, protecting their team's network and reporting back to corporate executives as the student-run red team attempts to attack. The competition was designed with standard tools and services in the real world, allowing for early exposure and long-term success. These services include Database, Web, FTP, and Active Directory servers, a security information event management system, and several workstations. The student and alumni-led red team utilized Sliver to deploy implants and maintain command and control. Though Xen Orchestra virtualized those services on server hardware, the competition environment also included physical elements like a switch and a wireless access point to manage workstation network access into each team's environment. Overall, the Great Dane Defense Competition's realistic environment provides students with a comprehensive taste of being vulnerable and facing attacks, preparing them for successful careers in protection and mitigation. These findings and results are essential to help understand the student experience of extracurricular activities to ensure early success in their entry-level careers.

Anonymous: Privacy and Confidentiality Concerns and Solutions in Autonomous Vehicles
Aneeha Sahar, Daniel Peck, Sharie Rhea, Tayquan Sneed, Karina Hernandez
Mentor: Dr. Benjamin Yankson
Time: 11:05am – 11:25am

Autonomous Vehicles (AVs) have gained increasing interest in the past few years for their promised efficiency, safety, and ease of use. However, as the technology becomes more common, it has become increasingly clear that these systems are vulnerable to cyber-attacks. Their large attack surface and massive potential for infrastructure damage and exposed personal information make them a very tempting target for malicious groups. This paper focuses primarily on the protection of privacy and personal information by examining the current research into securing the data stored and transferred between AVs. Our research found that the most commonly recommended techniques in the literature were limiting the transfer of data outside the AV, prepossessing transferred and stored data to remove personal information, and creating a strong regulatory framework around handling personal information.

Fortifying Security and Stability: The Case for a Federal Cyber Insurance Backstop
Brianna Bace
Mentor: Dr. Unal Tatar
Time: 11:25pm – 11:45pm

The surge in cyberattacks poses a grave threat to both national security and economic stability, driving a pressing need for robust cyber insurance coverage. As incidents like the NotPetya cyberattack demonstrate, the financial repercussions of such breaches can be staggering, with global damages exceeding $10 billion. In response to escalating risks, insurers are tightening policies and raising premiums, leaving significant gaps in coverage. Recognizing this urgent

need, the United States Treasury Department has initiated discussions on the potential for a federal insurance response to catastrophic cyber incidents.
This research delves into the imperative for a federal backstop for cyber insurance, analyzing stakeholder perspectives and potential structures for the backstop. Crucially, the study highlights the importance of government intervention amidst an evolving cyber threat landscape and an unstable geopolitical climate. Additionally, the research findings, which represent one of the initial data-driven studies on the subject, offer insights from diverse stakeholders, including the public and private sectors. These insights serve as crucial input for policymakers in addressing the issue effectively.

A Framework for Automated Data Loss Prevention Against Insider Threats in Sensitive Environment
Jason Masters, Sean Caruso, Connor Bowden
Mentor: Dr. Benjamin Yankson
Time: 11:45am – 12:05am

In consideration of the integral nature of information systems for organizations, both public and private, ease of access to sensitive information has expounded the need to plan for insider threats. Disgruntled and highly motivated employees pose a grave threat to information security, necessitating the development of Data Loss Prevention methods. Likewise, user error equally provides a vector for which data loss can occur. The unique nature of insider threats requires a nuanced approach and typically requires evaluation of employee behavior in conjunction with and in consideration of their access privileges and the responsibilities of their position.

Integration and Evaluation of Post-quantum TLS within 5G User Registration Function
John Evanchik, Luisa Cartagena
Mentor: Dr. Kemal Akkaya
Time: 12:05am – 12:25pm

The main point of this project was the measurement of byte sizes and speeds using HTTP/3 with Quic over various algorithm types. Over the time spent researching this topic, we used the research to examine how the three algorithms interacted with HTTP/3 and QUIC and worked to ensure these formats interacted properly. To ensure the measurement was done properly, we used Wireshark over a terminal to make all measurements. Originally, we planned to relate this to HTTP/2 and TLS as well, but it remains a work in the future.
