The Virtual Institute of

Cyber Operation and Research

(VICOR)

Presents

RESEARCH SHOWCASE

Friday, April 28, 2023

9am – 12:30pm

VICOR Research Showcase

April 28, 2023

Schedule at a Glance

All times are Eastern Daylight Time (EDT)

8:50am – 9:00am	**Join the session**
9:00am – 9:10am	**Welcome and Opening Remarks**
9:10am – 9:30am	**Talk**: Security Challenges of Mobile Edge Computing and IoT Devices *Samantha Carollo, Michael Danquah, and Janna Shearer*
9:30am – 9:50am	**Talk**: Anomaly Detection of Embedded Systems Utilizing Kernel Structures *Andy Carvajal, Edward Grisham, Aron Jones, Kevin Perez, and Jason Masters*
9:50am – 10:10am	**Talk**: Cybersecurity of Space Infrastructure *Brianna Bace and Rian Davis*
10:10am – 10:25am	**Talk**: Improving Ethics Surrounding Collegiate-Level Hacking Education: Comprehensive Implementation Plan & Affiliation with Peer-Led Initiatives *Shannon Morgan*
10:25am – 10:45am	**Talk**: Internet of Battlefield Things *Amaechi Anyene and Dyonne Lindsay*
10:45am – 11:00am	**Talk**: Cyber Threat Modeling for Water and Wastewater Systems: Contextualizing STRIDE and DREAD with the Current Cyber Threat Landscape *Rian Davis*
11:00am – 11:15am	**Talk**: Implications of AI in Cyberbiosecurity *Alex Kalena*
11:15am – 11:35am	**Talk**: Active Defense *Samantha Mayers, Nikolas Golyatdinov-Novikov, Nora Howell, and Marshal Williams*
11:35am – 11:55m	**Talk:** A Survey on Network Traffic Anomaly Detection: Applications and Challenges *Desiree Glynn, Franyel Castillo, and Raul Jarquin*
11:55am – 12:10pm	**Talk**: Gray-Zone Operations in the Post-Fact World: The Use of Deepfakes in PRC Disinformation Campaigns *Tony Ventura*
12:10pm – 12:30pm	**Talk:** Virtualization and Validation of Emulated STM-32 Blue Pill using QEMU Open-Source Framework *William Ocampo and Diana Gutierrez*
12:30pm – 12:35pm	**Closing Remarks**

ABSTRACTS

Security Challenges of Mobile Edge Computing and IoT Devices
Samantha Carollo, Michael Danquah, and Janna Shearer
Mentor: Dr. Benjamin Yankson
Date/Time: 9:10am – 9:30am

Internet of Things devices are beginning to appear in the everyday lives of many citizens, and one extremely impactful solution to providing faster, more efficient, and secure wireless communications is Mobile Edge Computing, expanding these capabilities within the cloud. This paper will amplify critical areas within our federal and local government interests that could utilize this technology in future projects, as well as identify possible risks and current challenges. A research method to gather more information on the use of IoT devices within military operations and utility or urban planning infrastructure is defined, allowing for the development of specific future work for these areas.

Anomaly Detection of Embedded Systems Utilizing Kernel Structures
Andy Carvajal, Edward Grisham, Aron Jones, Kevin Perez, and Jason Masters
Mentor: Dr. Alexander Perez-Pons
Date/Time: 9:30am – 9:50am

Anomaly detection in embedded systems is crucial for identifying abnormal processes that may compromise the performance or security of devices. This research paper presents a novel approach for detecting anomalies at the kernel level using a driver to collect data from the task_struct in a Raspberry Pi 4. The primary objective is to develop a machine-learning model that accurately identifies abnormal processes running on the device. The paper introduces the subject and research question, focusing on kernel-level anomaly detection in embedded systems. The methodology comprises the development of a custom driver to gather data from the kernel's task_struct, which includes various features representing the different fields in the data structure. The data collected from a Raspberry Pi 4 is used to train the machine learning model, enabling it to detect anomalies based on the features extracted from the kernel. The research findings reveal the effectiveness of the proposed approach in identifying abnormal processes with high accuracy. The model's performance is evaluated using various metrics and compared to existing methods, demonstrating its applicability in real-world scenarios. This research contributes to the field of embedded system anomaly detection and offers a practical solution for securing devices such as the Raspberry Pi 4.

Cybersecurity of Space Infrastructure
Brianna Bace and Rian Davis
Mentor: Dr. Unal Tatar
Date/Time: 9:50am – 10:10am

Space infrastructure plays a fundamental role in the functioning of critical systems and serves as the foundation for national security and economic prosperity in the United States. In this paper, we set out to answer two research questions: (1) Does the US space sector qualify as a critical infrastructure (CI) sector under the current US definition of CI? and (2) How does international law apply to the cyber domain, when taking a space sector perspective? To begin, we provided a review of the assets, threats, and vulnerabilities that exist within the United States space sector. We also discuss the commercialization of space and the significant dependencies that CI has on space infrastructure. To answer our first research question, we use the definition of CI originally provided in the USA PATRIOT Act of 2001 with language found in recent space policies, directives, and frameworks, such as Space Policy Directive 5 (SPD-5), to create our justification for designating space as the seventeenth recognized US CI sector. In the second part of our paper, we propose that cyberattacks on space infrastructure could have the potential to violate international law outside of an armed conflict. Using the Tallinn Manual 2.0 as a guide, we look at the principle of sovereignty, the prohibition of intervention, and the prohibition of the use of force and create three hypothetical cyberattack scenarios on space infrastructure that could trigger these laws. The scenarios were created based on past cyber incidents affecting space infrastructure.

Gray-Zone Operations in the Post-Fact World: The Use of Deepfakes in PRC Disinformation Campaigns
Tony Ventura
Mentor: Dr. Brian Nussbaum
Date/Time: 10:10am – 10:25am

Information operations are the touchstone of public policy and security concerns today. Domestically and abroad, trust in factual information, deference to scientific consensus, and the reliability of online references have decayed. This has opened a new front in the realms of intelligence, defense, and law enforcement. Since the 2016 election and continuing through Russia's invasions of Ukraine in 2014 and 2022, information operations have proven a formidable and ubiquitous weapon in the cyber-statecraft arsenal. But these digital gray-zone operations, in general, are underexplored with respect to synthetic media; still-nascent "deepfake" technology, in particular, has an especially far-reach and destructive potential. As noted by the US Secretary of Defense, the Chinese Communist Party (CCP) is America's current "pacing threat." While the CCP's employment of information as a weapon is well known, there is little data on their propensity to utilize deepfakes and their proficiency in creating and deploying them. The present study identifies likely targets, narratives, and objectives for CCP-originating deepfakes in disinformation campaigns via what is known about their information

warfare doctrine, existing examples of Chinese information operations, and known cases of deepfake use by other entities to affect social, political, or military goals.

Internet of Battlefield Things
Amaechi Anyene and Dyonne Lindsay
Mentor: Dr. Benjamin Yankson
Date/Time: 10:25am – 10:45am

The Internet of Battlefield Things (henceforth, IoBT) is an emergent and rapidly evolving computing concept that connotes the integration of connected, intelligent devices and computer systems on the battlefield. Given its capacity to inspire and drive the creation of highly performant and resilient smart computational and sensing services, IoBT has the potential to revolutionize modern warfare by providing tailored tactical network edge and facilitating real-time monitoring and situational awareness to enhance efficacy. IoBT is, however, not without issues, posing fundamental challenges, especially with regards to erosion of privacy, security anonymity, personal liberty, technical intricacies, and limitations, as well as raising a number of deep-seated ethical concerns. As an emerging and rapidly evolving technology, comprehensive research into these issues remains fundamentally wanting. This research endeavors to bridge this gap by (1) providing an in-depth overview of the opportunities and challenges associated – directly or otherwise – with the applications of IoBT in military operations and (2) examining the overall implications of these applications in contemporary warfare. The analysis also draws insights and conclusions from extant literature, including scholarly peer-reviewed publications, to explore, albeit transiently, the ethicality (or lack thereof) of IoBT and subsequently reflect on the potential benefits and detriments of this technology. Overall, the findings reveal that although IoBT provides substantial potential for military applications, its adoption and subsequent usage should be undertaken cautiously and with careful contemplation of its ramifications both in the short- and long term. It specifically calls for the need to design robust cybersecurity safeguards and address the ethical concerns arising from the increasing adoption of IoBT.

Cyber Threat Modeling for Water and Wastewater Systems: Contextualizing STRIDE and DREAD with the Current Cyber Threat Landscape
Rian Davis
Mentor: Dr. Omer Keskin
Date/Time: 10:45am – 11:00am

Water and Wastewater Systems (WWS) are integral to maintaining public health and safety, with numerous other infrastructure sectors also being reliant upon the services WWS provides. Given these dependencies and how critical WWS is to public health and safety, it is integral to understand all possible threats. As water and wastewater infrastructure increases the integration of cyber systems in its infrastructure, the threat posed by malicious cyber threat actors and the risk of cyberattacks has increased concurrently. The growing attack surface of water systems has been targeted in various ways in the past, including the release of wastewater by an insider threat, gaining remote access to a dam's SCADA network by state-backed hackers, and installing malware on water systems by cybercriminals. Such incidents show how industrial control system networks in critical water infrastructure require attention. In this project, the project team will provide an analysis of the WWS threat landscape through an overview of 22 incidents that occurred from 2000 to 2022 and consultation with previous work related to threat modeling.

Implications of AI in Cyberbiosecurity
Alex Kalena
Mentor: Dr. Saltuk Karahan
Date/Time: 11:00am – 11:15am

Cyberbiosecurity, defined as the common ground where cybersecurity and biotechnology meet, is an emerging field that will become more and more relevant as both technology and threats to security develop. The term, in part pioneered by Dr. Jean Peccoud of Colorado State University, is typically applied to biological and biomedical developments. As a field, it is a proposed solution to address the possible exploitation of information that lies at the intersection of biology and digital systems, such as the synthesis of biological weapons, vaccine information, biomedical engineering, and containment of samples. Artificial intelligence, another rapidly progressing technological advancement, may seem unrelated at first glance. The presence of AI is felt all around us, in our cars, phones, weapons, and the devices that order our shopping; while AI is a useful tool, it comes with its own list of potential flaws and security risks. It is entirely possible, however, that artificial intelligence can be incorporated as a security measure in the field of cyberbiosecurity, thanks to an equally lengthy list of exciting possibilities. This paper explores the benefits and vulnerabilities of artificial intelligence, especially in regard to its implementation in cyberbiosecurity.

Active Defense
Samantha Mayers, Nikolas Golyatdinov-Novikov, Nora Howell, and Marshal Williams
Mentor: Dr. Sanjay Goel
Date/Time: 11:15am – 11:35am

This research paper focuses on the concept of active defense in cybersecurity and explores its different tactics, including detection, deterrence, and attribution. Active defense involves using offensive measures to prevent cyber-attacks instead of simply reacting to them after they have occurred. Cyber deception plays a critical role in many active defense tactics, helping to deceive attackers during an attack. The paper highlights various tactics used in active defense in specific honeypots. It also explores how detection can help catch threats quickly to reduce response time, using examples like honeypots and intrusion detection systems. The paper also discusses how attribution can be used to create reports on attackers. Additionally, the paper examines the concept of passive defense and how it uses system characteristics to fix damaged data. Overall, the paper provides an overview of active defense and its different tactics, highlighting its significance in preventing cyber-attacks.

A Survey on Network Traffic Anomaly Detection: Applications and Challenges
Desiree Glynn, Franyel Castillo, and Raul Jarquin
Mentor: Dr. Himanshu Upadhyay
Date/Time: 11:35am – 11:55am

Anomaly detection is a valuable tool for detecting fraud, network intrusion, and other unusual occurrences that might be important but are difficult to notice. Anomaly detection can help you manage risk and detect fraud. To address the drawbacks of knowledge-based detection strategies, intrusion detection researchers have focused heavily on machine learning methodologies. Based on stated behaviors and qualities, this paper presents an overview of machine learning methods and approaches. In this survey, we analyze reviews of several machine learning and deep learning algorithms applied for analyzing network traffic. Moreover, we also highlight and discuss several applications of machine learning in network traffic analysis such as Intrusion Detection Systems (IDS), Network Intrusion Detection Systems (NIDS), Anomaly detection, and network traffic prediction. Finally, we identify and discuss some challenges related to the application of machine learning in network traffic.

Improving Ethics Surrounding Collegiate-Level Hacking Education: Comprehensive Implementation Plan & Affiliation with Peer-Led Initiatives
Shannon Morgan
Mentor: Dr. Sanjay Goel
Date/Time: 11:55am – 12:10pm

As technology continues to develop and advance at a rapid rate, the demand for cybersecurity professionals is also rising to protect these systems and devices. On a global scale, universities are now offering a wide range of tech-related majors and programs (e.g., cybersecurity, informatics, IT, digital forensics, computer science, & engineering) to aid in filling these workforce gaps. It is critical to produce graduates that possess the proper knowledge and skillset to actively combat a major component of the tech realm – cyber criminals. However, during the conceptual and technical instruction of these students, it brings to light the ethical concern regarding hacking education. The purpose of this paper is to examine the implementation of hacking as a learning tool within the college education system from an ethical standpoint. The culmination of this research study will provide comprehensive suggestions that can establish a safer education for students that will work to safeguard assets from cyber criminals. The provided recommendations will gather a variety of social, technology-based, and ethical constructs that, when implemented, will prove to be a strong defense against student abuse of learned hacking knowledge during their collegiate studies.

Virtualization and Validation of Emulated STM-32 Blue Pill using QEMU Open-Source Framework
William Ocampo and Diana Gutierrez
Mentor: Dr. Alexander Perez-Pons
Date/Time: 12:10pm – 12:30pm

As computer systems become increasingly sophisticated, it is critical to ensure that proper security protocols are in place to ensure the integrity of digital infrastructure. In some cases, penetration testing of a digital system can be deemed destructive. For example, an aircraft has many flight computers and attack entry points. There is no way to inject malware into a system for testing that can cause damage to a product or risk people's lives. With an emulated environment, it is possible to bring physically embedded computer systems to the virtual world. Throughout our development, the team emulated the STM32 microcontroller, which is a model of the physical device.