NSUComputing

3rd Annual Cybersecurity Graduate Research Symposium

October 30, 2025

Nova Southeastern University -
Cortex Labs Room 309
Mailman Hollywood Building

Join us for our annual Cybersecurity Graduate Research Symposium to hear from NSU Alumni about their previous and current cybersecurity research.

Followed by a Scotch Tasting Reception located at NSU's Fort Lauderdale/Davie Campus Shark Club

SCAN ME

National Center of Academic Excellence in Cybersecurity (NCAE-C)
Cyber Defense (CD) and Cyber Research (R)

Symposium hosted by The College of Computing, AI, and Cybersecurity

3rd Annual Cybersecurity Graduate Research Symposium

Nova Southeastern University (NSU)
Symposium hosted by The College of Computing, AI, and Cybersecurity
October 30, 2025

Schedule

11:00-11:30 **Welcome by Greg Simco, Ph.D. and Refreshments**

11:35-12:55 **Breakout Session A**

- **11:35-11:55** *Analyzing IoT Vulnerabilities: A Longitudinal Study of CVE Disclosures and Exploitability Trends by* **Stephen Mujeye**
- **12:05-12:25** *Cybersecurity and Ransomware in Critical Infrastructure: Threats, Cases, and Strategies for Latin America by* **Heriberto Acosta Maestre**
- **12:35-12:55** *Experimental Study to Assess the Role of Environment and Device Type on the Success of Social Engineering Attacks: The Case of Judgment Errors by* **Tommy Pollock**

1:00-2:00 **Lunch and Networking**

2:10-4:00 **Breakout Session B**

- **2:10-2:30** *Regional Community Engaged Learning to Support First Responders by* **Michael Lehrfeld**
- **2:40-3:00** *Usability Challenges to Securing Car Key Fobs from Hacking by* **Ann-Marie Horcher**
- **3:10-3:30** *Toward a SOC Maturity Model for Artificial Intelligence: Insights from Emerging Cybersecurity Environments by* **George Antoniou**
- **3:40-4:00** *A Universal Cybersecurity Competency Framework for Organizational Users by* **Patricia Baker**
- **4:10-4:30** Implementing RSA Accumulators for Asynchronous and Permissionless Reliable Broadcasting by **Eric Webb**

4:30-7:00 **Scotch Tasting Reception and Award Honoree – NSU Shark Club**

***All times subject to change

3rd Annual Cybersecurity Graduate Research Symposium
Nova Southeastern University (NSU)
Symposium hosted by The College of Computing, AI, and Cybersecurity
October 30, 2025

Welcome to the 3rd Annual College of Computing, AI, and Cybersecurity Symposium! In 2024, we hosted the second one and honored our second inductee, John Machado, into NSU's Computing Hall of Fame. This year, we are proud to induct Victoria Ranger Nunez into NSU's Computing Hall of Fame.

Nova Southeastern University has been designated as a National Center of Academic Excellence in Cybersecurity (NCAE-C) Cyber Defense (CD) and Cyber Research (R) through the academic year 2028. This new designation complements our re-designation as a National Center of Academic Excellence in Cybersecurity in 2021.

Breakout Session A

Analyzing IoT Vulnerabilities: A Longitudinal Study of CVE Disclosures and Exploitability Trends.
Stephen Mujeye

The proliferation of IoT devices has amplified cybersecurity risks, driven by weak authentication, poor encryption, and delayed patching. This study analyzes IoT vulnerability trends over the past decade, linking CVE disclosure to real-world exploitation, and integrates threat intelligence sources to track evolving risks. Machine learning models (SVM, BERT, K-Means, DBSCAN) are applied to classify and prioritize vulnerabilities. Findings highlight high-risk device categories, inform improvements to Coordinated Vulnerability Disclosure (CVD), and advance automated IoT risk assessment.

Cybersecurity and Ransomware in Critical Infrastructure: Threats, Cases, and Strategies for Latin America
Heriberto Acosta Maestre

Critical infrastructure has become a prime target for ransomware, with Latin America facing rising incidents across energy, healthcare, finance, and transport. This presentation reviews ransomware types, extortion models, and key cases such as Conti in Costa Rica, Fog in Brazil, and BlackCat/ALPHV in Colombia, comparing them with global incidents like Colonial Pipeline. It highlights regional vulnerabilities and offers strategies based on NIST CSF and ISO 27001 to strengthen resilience through cooperation and preparedness.

Experimental Study to Assess the Role of Environment and Device Type on the Success of Social Engineering Attacks: The Case of Judgment Errors
Tommy Pollock

Phishing continues to be an invasive threat to computer and mobile device users. Cybercriminals continuously develop new phishing schemes using e-mail and malicious search engine links to gather the personal information of unsuspecting users. This information is used for financial gains through identity theft schemes or draining victims' financial accounts. Many users of varying demographic backgrounds fall victim to phishing schemes at one time or another. Users are often

distracted and fail to process the phishing attempts fully, then unknowingly fall victim to the scam until much later. Users operating mobile phones and computers are likely to make judgment errors when making decisions in distracting environments due to cognitive overload. Distracted users cannot distinguish between legitimate and malicious emails or search engine results correctly. Mobile phone users can have a harder time distinguishing malicious content due to the smaller screen size and the limited security features in mobile phone applications.

The main goal of this research study was to design, develop, and validate experimental settings to empirically test if there are significant mean differences in users' judgment when: exposed to two types of simulated social engineering attacks (phishing & Potentially Malicious Search Engine Results (PMSER)), based on the interaction of the kind of environment (distracting vs. non-distracting) and type of device used (mobile vs. computer). This research used field experiments to test whether users are more likely to fall for phishing schemes in a distracting environment while using mobile phones or desktop/laptop computers. The second phase included a pilot test with 10 participants testing the Subject Matter Experts (SME) validated tasks and measures. The third phase included the delivery of the validated tasks and measures that were revised through the pilot testing phase with 68 participants.

The results of the first phase have SME validated two sets of experimental tasks and eight experimental protocols to assess the measures of users' judgment when exposed to two types of simulated social engineering attacks (phishing & PMSER) in two kinds of environments (distracting vs. non-distracting) and two types of devices (mobile phone vs. computer). The second phase results, the phishing mini-IQ test results, do not follow what was initially indicated in prior literature. Specifically, it was surprising to learn that the non-distracting environment results for the Phishing IQ tests were overall lower than those of distracting environment, which is counter to what was envisioned. These Phishing IQ test results may be assumed to be because, during the distracting environment, the participants were monitored over zoom to enable the distracting sound file. In contrast, in the non-distracting environment, they have marked the selections independently and may have rushed to identify the phishing samples.

In contrast, PMSER detection on a computer outperformed mobile devices. It is suspected that these results are more accurate as individuals' familiarity with PMSER is much lower. Their habituation to such messages is more deficient, causing them to pay closer attention and be more precise in their detections. A two-way Analysis of Variance (ANOVA) was conducted on the results. While it appears that some variations do exist, none of the comparisons were significant for Phishing IQ tests by environment ($F=3.714$, $p=0.061$) or device type ($F=0.380$, $p=0.541$), and PMSER IQ tests by environment ($F=1.383$, $p=0.247$) or device type ($F=0.228$, $p=0.636$). The results for the final phase showed there were no significant differences among both groups for Phishing and PMSER ($F=0.985$, $p=0.322$) and PMSER ($F=3.692$, $p=0.056$) using a two-way ANOVA. The two-way ANOVA results also showed significant differences among both groups for Phishing and PMSER vs. Device Type and Environment, Phishing ($F=3.685$, $p=0.013$), PMSER ($F=1.629$, $p=0.183$). A two-way ANOVA was evaluated for significant differences between groups. The results of the two-way ANOVA showed there were significant differences among both groups for Phishing and PMSER vs. Device Type and Environment. Phishing

(F=3.685, p=0.013), PMSER (F=1.629, p=0.183). The p-values of the F-test for the Phishing IQ vs. Device Type and Environment were lower than the .05 level of significance. The two-way Analysis of Covariance (ANCOVA) results showed significant differences between Phishing vs. Environment and Device Type plus PMSER vs. Environment and Device Type. Specifically, the Education covariate for Table 32(F=3.930, p=0.048), Table 33(F=3.951, p=0.048), Table 34(F=10.429, p=0.001), and Table 35(F=10.329, p=0.001) was lower than the .05 level of significance.

Breakout Session B

Regional Community Engaged Learning to Support First Responders
Michael Lehrfeld

This initiative examines the role of advanced technology and cross-sector collaboration in strengthening emergency preparedness and disaster response. At its core is the Real Time Crime Center (RTCC) at East Tennessee State University, which operates as a central hub connecting law enforcement, first responders, and community partners. By integrating dynamic platforms such as the NIBIN bullet forensics lab and ATAK, the RTCC enhances real-time data sharing, situational awareness, and ballistic intelligence. These tools enable the creation of dynamic Intelligence Analyst and Crime Center type curricula that train the next generation of first responders.

Usability Challenges to Securing Car Key Fobs from Hacking
Ann-Marie Horcher

Remote keyless entry to vehicles is popular because it is easy and convenient. Unfortunately, sophisticated hackers have learned to intercept a key fob signal using commercially available and completely legal equipment. Though efforts to engineer a solution are in development, there are still millions of cars on the road that are at risk. Garfinkel's usable security principles state it is necessary to provide "Good security now." Designers must create the best security possible with existing technology. This research looks at strategies to secure key fobs that rely on hacking human behavior by applying a Security Acceptance Model that relies on usability.

Toward a SOC Maturity Model for Artificial Intelligence: Insights from Emerging Cybersecurity Environments
George Antoniou

Security Operations Centers (SOCs) are critical for monitoring and responding to cyber threats, yet many emerging environments lack the processes and resources required to establish them effectively. This research, conducted during a Fulbright Scholar residency at the University of Tirana, proposes a new SOC maturity model designed for artificial intelligence (AI) integration. Building on the Capability Maturity Model (CMM) and incorporating established AI governance frameworks, the model defines progressive stages of readiness for AI-driven operations. Rather than adapting existing SOC structures, it addresses environments.

A Universal Cybersecurity Competency Framework for Organizational Users
Patricia Baker

The global reliance on the Internet to facilitate organizational operations necessitates further investments in organizational information security. Such investments hold the potential for protecting information assets from cybercriminals. To assist organizations with their information security, The National Institute of Standard and Technology (NIST) created the National Initiative for Cybersecurity Education (NICE) framework.

The framework referenced the cybersecurity work, knowledge, and skills required to competently complete the tasks that strengthen their information security. Organizational users' limited cybersecurity competency contributes to the financial and information losses suffered by organizations year after year. While most organizational users may be able to respond positively to a cybersecurity threat, without a measure of their cybersecurity competency they represent a cybersecurity threat to organizations.

The main goal of this research study was to develop a universal Cybersecurity Competency Framework (CCF) to determine the demonstrated cybersecurity Knowledge, Skills, and Tasks (KSTs) through the NCWF (NICE, 2017) as well as identify the cybersecurity competency of organizational users. Limited attention has been given in cybersecurity research to determine organizational users' cybersecurity competency. An expert panel of cybersecurity professionals known as Subject Matter Experts (SMEs) validated the cybersecurity KSTs necessary for the universal CCF. The research study utilized the explanatory sequential mixed-method approach to develop the universal CCF.

his research study included a developmental approach combining quantitative and qualitative data collection in three research phases. In Phase 1, 42 SMEs identified the KSTs needed for the universal CCF. The results of the validated data from Phase 1 were inputted to construct the Phase 2 semi-structured interview. In Phase 2, qualitative data were gathered from 12 SMEs. The integration of the quantitative and qualitative data validated the KSTs. In Phase 3, 20 SMEs validated the KST weights and identified the threshold level. Phase 3 concluded with the SMEs' aggregation of the KST weights into the universal CCF index.

The weights assigned by the SMEs in Phase 3 showed that they considered knowledge as the most important competency, followed by Skills, then Tasks. The qualitative results revealed that training is needed for cybersecurity tasks. Phase 3 data collection and analysis continued with the aggregation of the validated weights into a single universal CCF index score. The SMEs determined that 72% was the threshold level.

The findings of this research study significantly contribute to the body of knowledge on information systems and have implications for practitioners and academic researchers. It appears this is the only research study to develop a universal CCF to assess the organizational user's competency and create a threshold level. The findings also offer further insights into what

organizations need to provide cybersecurity training to their organizational users to enable them to competently mitigate cyber-attacks.

Implementing RSA Accumulators for Asynchronous and Permissionless Reliable Broadcasting

Eric Webb

Asynchronous consensus protocols are critical for decentralized and trustless environments such as decentralized finance, supply chains, and voting systems. These protocols avoid centralized authority and timing assumptions, improving resilience and security. As networks scale communication overhead becomes a major bottleneck limiting performance. The Aleph protocol is a notable example that offers both asynchronous and permissionless Byzantine Fault Tolerance. Unlike many prior designs, Aleph does not depend on a trusted dealer or fixed membership, making it well suited for open blockchain systems. Aleph's design advances decentralization and security in the blockchain trilemma but at the cost of higher communication complexity and hindering scalability. The Aleph consensus relies on a Chain Reliable Broadcast protocol (ch-RBC) that suffers from quadratic communication overhead in large networks. This study enhances ch-RBC by replacing its Merkle tree-based transaction validation with Rivest–Shamir–Adleman (RSA) accumulators. RSA accumulators provide compact and constant sized proofs that can be batched and parallelized, thus reducing the protocol's complexity from $O(Tr + N^2 \log N)$ to $O(Tr + N^2)$, where T and r denote the number of transactions and rounds respectively. This modification lowers bandwidth consumption and improves scalability while preserving security guarantees. In this study both Merkle and RSA based versions of ch-RBC were implemented in Rust and deployed on AWS EC2 instances using the AWS CDK. Experiments were scaled from 5 to 104 nodes with batch sizes up to 1024 transactions per round. Key metrics included throughput, latency, communication overhead, and resource utilization. Results demonstrated that RSA accumulators significantly improve scalability as the network increases, showing promise for future asynchronous and permissionless consensus.