NSUComputing

2nd Annual Cybersecurity Graduate Research Symposium

October 23, 2024

Nova Southeastern University -
Cortex Labs Rm 309,
Mailman Hollywood Building

Join us for our Cybersecurity Graduate Research Symposium located in the CORTEX Labs, Room 309 of the Mailman-Hollywood Building.

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 and Engineering

2nd Annual Cybersecurity Graduate Research Symposium
Nova Southeastern University (NSU)
Symposium hosted by The College of Computing and Engineering
October 23, 2024

Schedule

9:00-9:30 **Announcements and Refreshments**

Breakout Session A

9:35-9:55 *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 (In-Person)**

10:00-10:20 *Quantum Computing: An Introduction, Applications, and Impact on Latin America by* **Heriberto Acosta Maestre (In-Person)**

10:25-10:45 *Adapting to the AI-powered Workforce by* **Guillermo Perez (In-Person)**

10:50-11:10 *Unlocking the Orbital Domain by* **George Antoniou (In-Person)**

11:15-11:35 *Enhanced Shoulder-Surfing Cued-Recall Graphical Password System: Sequential PassPoint (SPP) by* **Titus Fofung (In-Person)**

11:45-12:45 **Lunch and Networking**

1:00-3:25 **Breakout Session B**

1:00-1:20 *Implementing a Secure Hub Ecosystem Prototype in Defending IoT Devices in Smart Homes by* **Stephen Mujeye (In-Person)**

1:25-1:45 *Examining Consumers' Selective Information Privacy Disclosure Behaviors in an Organization's Secure e-Commerce Systems by* **Patrick Offor (In-Person)**

1:50-2:10 *Using Ontological Methods to Compare Cybersecurity Maturity Model Certification 2.0 and COBIT-19 by* **Aaron Ramey (Virtual)**

2:15-2:35 *Assessing Organizational Investments in Cybersecurity and Financial Performance Before and After Data Breach Incidents of Cloud SaaS Platforms by* **Munther Ghazawneh (Virtual)**

2:40-3:00 *A Universal Cybersecurity Competency Framework for Organizational Users by* **Patricia Baker (In-Person)**

3:05-3:25 *Cyber-Security Synthetic Data with Generative AI Gemini by* **Thuan Luong Nguyen (In-Person)**

3:30-4:00 **Award Honoree and Closing Remarks**

4:00-4:30 **Industry Advisory Board Meeting**

4:30-7:00 **Scotch Tasting Alumni Networking Reception – NSU Shark Club**

***All times subject to change

2nd Annual Cybersecurity Graduate Research Symposium
Nova Southeastern University (NSU)
Symposium hosted by The College of Computing and Engineering
October 23, 2024

Welcome to the 2nd Annual College of Computing and Engineering Cybersecurity Symposium! In 2023, we hosted the first one and honored our first inductee, Loretta Neff into NSU's Computing Hall of Fame. This year we are proud to induct John Machado 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

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.

Quantum Computing: An Introduction, Applications, and Impact on Latin America
Heriberto Acosta Maestre

We provide a comprehensive overview of quantum computing, its applications, and its impact on Latin America and hemispheric security. Quantum computing uses qubits, which can exist in multiple states simultaneously, allowing for faster complex calculations. We cover fundamental concepts like superposition and entanglement, and discuss applications in cryptography, drug discovery, and optimization. We also explore the state of Quantum Computing Research in Latin America, its security implications, and its broader geopolitical and economic impacts.

Adapting to the AI-powered Workforce
Guillermo Perez

AI is transforming how we work in profound ways. As machine learning and natural language processing advance, AI is automating routine tasks, generating insights from data, and enhancing human capabilities. This frees up employees' time for more strategic, creative work. AI is also shaping the workforce, changing required skills and creating new types of jobs. This research endeavor is to provide perspectives on how organizations and workers can proactively adapt to the AI-powered workforce.

Unlocking the Orbital Domain
George Antoniou

Digital Forensics in Satellite and UAV Technologies Abstract: The expansion of digital forensics into satellite and UAV technologies addresses the critical need to secure these systems, integral to global communication, navigation, and surveillance. This field faces unique challenges, including physical inaccessibility, system heterogeneity, and legal complexities. Innovative tools such as remote forensics, AI, and digital twins are being developed to overcome these obstacles. This paper explores the emerging methodologies and technologies in satellite and UAV digital forensics, highlighting the importance of legal and ethical considerations to ensure responsible and effective investigations.

Enhanced Shoulder-Surfing Cued-Recall Graphical Password System: Sequential PassPoint (SPP)
Titus Fofung

During the past two decades, many graphical passwords have been used widely as an alternative to text-based passwords. However, most graphical password systems are plagued by shoulder-surfing problems, usability, and remembering capability. This study proposed a new graphical password called SPP (Sequential PassPoint), allowing users to remember three click-points on two images in specified order and image order. When the image order changes, the click order is reversed. Two decoy images for three random clicks were introduced to enhance the security of SPP. The proposed SPP system was validated both theoretically and empirically.

Breakout Session B

Implementing a Secure Hub Ecosystem Prototype in Defending IoT Devices in Smart Homes
Stephen Mujeye

The Internet of Things (IoT) technology has revolutionized how businesses operate and changed our daily lives. IoT devices are used in different areas, including smart cities, smart agriculture, smart healthcare, and smart homes. The number of IoT devices connected worldwide continues to rise, and 75 billion devices are expected to be connected by 2025. Even though IoT devices are rapidly spreading, they come with security and privacy challenges. This project aims to design and implement a secure hub ecosystem prototype with an intrusion detection system (IDS), including ML, to defend IoT devices in a smart home. The data will be collected and analyzed to reveal the effectiveness of an IDS with ML in securing an IoT-based network.

Examining Consumers' Selective Information Privacy Disclosure Behaviors in an Organization's Secure e-Commerce Systems
Patrick Offor

The study examines the paradoxical changes in the consumers' intended and actual personal information disclosure online. The argument is that consumers' privacy paradox is based on their predisposition and need signal. Conceptual underpinning inherent in the Privacy Regulation Theory (PRT) was adopted and advanced and was validated using Structural Equation Modeling. The result indicates that consumers' intention to disclose personal information online depends on their natural or desired state of information privacy, and their actual disclosure behavior depends on their privacy equipoise.

Using Ontological Methods to Compare Cybersecurity Maturity Model Certification 2.0 and COBIT-19
Aaron Ramey

This research study utilized Resource Description Framework (RDF) triplets to break down security controls between the Cybersecurity Maturity Model Certification and COBIT-19. Protégé was used to create ontologies and knowledge graphs to support the identification of similarities. The equations used to identify similarities were the Simple Matching Coefficient and the Jaccard Index. This research study then provided the results of these comparisons to a collection of over 50 self-identified Subject Matter Experts to measure their perception of the value of RDF Similarity Scores to Defense Industrial Base organizations.

Assessing Organizational Investments in Cybersecurity and Financial Performance Before and After Data Breach Incidents of Cloud SaaS Platforms
Munther Ghazawneh

Prior research indicated that providing inappropriate investment in organizations for cybersecurity makes these organizations suffer from cybersecurity vulnerabilities that may cause data breach incidents. Data breaches in

cloud Software as a Service (SaaS) platforms lead to the disclosure of sensitive information, which causes disruption of services, damage to the organizational image, or financial losses. Cybersecurity risks and vulnerabilities cost organizations millions of dollars a year as organizations may face an increase in cybersecurity challenges.

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 Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NCWF) was created. 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.

This 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.

Cyber-Security Synthetic Data with Generative AI Gemini
Thuan Luong Nguyen (In-Person)

Generative artificial intelligence (AI) has offered unprecedented opportunities and complex challenges as a double-edged sword in cybersecurity, g. On the one hand, generative AI models can enhance cybersecurity defenses. For instance, these models can generate realistic synthetic data to train and test security systems,

making them more robust against adversarial attacks. Additionally, large language models (LLM) can be used to identify patterns and anomalies in network traffic, aiding in detecting cyber threats. However, generative AI also poses severe risks to cybersecurity. Adversaries can leverage sophisticated and robust models to create convincing phishing emails, deep-fake videos, and other deceptive content. Moreover, generative AI can be employed to automate the generation of malware and exploits, making cyberattacks harder to detect.

Cyber-security attacks, such as Distributed Denial of Service (DDoS), pose a significant threat to enterprise networks, disrupting operations and causing substantial financial losses. Traditional defense mechanisms often struggle to adapt to new tactics employed by attackers. Generative Adversarial Networks (GANs) have been used as a promising approach for generating synthetic DDoS attack data to enhance the training of defense models. However, the complexity of GAN frameworks and the intricacies of the data generation process present challenges for effective implementation. This research introduces Google's Gemini 1.5 Flash, a sophisticated but fast and low-cost generative AI model. By serving as a comprehensive orchestrator and facilitator, Gemini streamlines and enhances the entire process of generating synthetic cyber-security attack data for training GAN models, reassuring the audience about the efficiency of the process.

Gemini's capabilities are employed through various critical GAN-based synthetic data generation pipeline stages. Gemini 1.5 Flash guides the selection of an appropriate GAN architecture; Gemini then aids in configuring the GAN framework and optimizing hyperparameters like learning rates, batch sizes, and activation functions to ensure efficient training.

Data preparation is always a crucial step in training any robust neural networks, including GAN models. For this task, Gemini helps create a diverse and representative dataset of DDoS attack patterns, which includes collecting raw network traffic data, cleaning it to remove noise and anomalies, and transforming it into a suitable format for GAN training.

Another critical task is designing the GAN model architecture, in which Gemini assists in guiding the selection of appropriate generator and discriminator architectures. The task involves determining the number of layers, types of layers (convolutional, dense, etc.), and the connectivity between layers. Gemini's understanding of GAN principles aids in crafting a model architecture that can effectively capture the nuances of DDoS attack traffic.
The performance of a GAN model critically depends its hyperparameter optimization that can be done with advanced optimization techniques such as Bayesian optimization or genetic algorithms. In the optimization process, Gemini helps to systematically explore the hyperparameter space and identify the optimal configuration for generating realistic cyber-security training data, e.g., DDoS (Distributed Denial of Service) attack data. This iterative refinement process ensures that the GAN model converges to a state where it produces high-fidelity synthetic data.

Moreover, Gemini facilitates the implementation of real-time monitoring mechanisms to track the progress of the GAN's learning. The process involves visualizing the generated data, evaluating the discriminator's ability to distinguish between real and synthetic data, and assessing the generator's capacity to create increasingly realistic attack patterns.

For a GAN model to be successful, it requires iterative refinement. Gemini plays a crucial role in this process, analyzing the feedback from the monitoring and evaluation stage. Based on the observed performance, Gemini suggests modifications to the GAN architecture, hyperparameters, or training data to enhance the quality of the generated synthetic data. This iterative cycle, guided by Gemini, continues until the GAN produces DDoS attack data that is statistically indistinguishable from real attack traffic. This process instills confidence in the quality of the synthetic data, ensuring that it is of the highest standard for training defense models.

In conclusion, this research aims to demonstrate that Google Gemini 1.5 Flash – a small, fast, and low-cost generative AI model – can be used as a comprehensive orchestrator and facilitator to generate synthetic attack data using GANs. By streamlining and enhancing various critical stages of the process, Gemini 1.5 Flash enables cybersecurity professionals to create high-quality synthetic data that can significantly improve the training of defense models against DDoS attacks, ultimately bolstering the resilience of enterprise networks.