KENTUCKY
CYBERSECURITY AND
FORENSICS CONFERENCE

Kentucky Cybersecurity and Forensics Conference

November 10-12, 2023

Cambria Hotel Louisville Downtown - Whiskey Row
(120 South Floyd Street, Louisville KY, 40202)

Hosted by
UNIVERSITY OF
LOUISVILLE®

Explore Phishing Email Generation and Detection via ChatGPT

Judy Wang
School of Arts and Sciences
Georgetown University, Washington DC United States
jw2180@georgetown.edu

Shonda Bernadin
Department of Electrical and Computer Engineering
Florida A&M University
Tallahassee, Florida
United States
bernadin@eng.famu.fsu.edu

Mark Weatherspoon
Department of Electrical and Computer Engineering Florida A&M University Tallahassee, Florida
United States
weathers@eng.famu.fsu.edu

Hongmei Chi
Dept. of Computer and Info Sciences Florida A&M University
Tallahassee, Florida
United States
hongmei.chi@famu.edu

With the rapid advancements in natural language processing and artificial intelligence, language models like ChatGPT have emerged as powerful tools, capable of generating human-like text. However, this raises concerns about their potential misuse in generating phishing emails that are difficult to distinguish from legitimate messages. This paper investigates the use of ChatGPT for both phishing email generation and detection. Firstly, we explore the capabilities of ChatGPT in crafting phishing emails that imitate genuine communications, allowing cybercriminals to scale their attacks rapidly and target specific individuals or organizations. By examining the characteristics and patterns of these generated emails, we identify key indicators that differentiate them from legitimate messages. Through empirical evaluations using a diverse dataset of phishing emails, genuine communications, and LLM-generated messages, we assess the effectiveness and robustness of the proposed detection methods. The results shed light on the challenges and opportunities in leveraging ChatGPT's capabilities for cybersecurity purposes.

CAE and Models for the Expansion of Cybersecurity Knowledge in the United States of America

Michael Losavio and Sharon Kerrick

University of Louisville
Louisville, Kentucky, USA
michael.losavio@louisville.edu

The United States is in need of a new paradigm in the development of cybersecurity knowledge and skills, one that democratizes them for all people. The CAE model is an excellent foundation that can be expanded to accomplish this for a distributed model of cybersecurity. We discuss options for this expansion via cybersecurity teaching projects across multiple domains. Those domains range from computer science and engineering to law enforcement to the fundamental computing skills curricula of middle schools and high schools and college studies in non-computing areas, from psychology to the humanities. This is the essence of democratic cybersecurity.

A Comprehensive Review of Facial Recognition Technology in the Modern World

Alex Hamade
University of Louisville
Louisville, Kentucky, USA
ashama01@louisville.edu

Facial recognition technology (FRT) is a topic as hot as ever. It has serious applications across various fields that could prove to be invaluable in their development. While FRT provides a reliable method for verifying identities, concerns have been raised about its impact on privacy, accuracy, and the current lack of regulation. This paper aims to analyze the technical abilities of FRT and investigate existing implementations in society, with a primary focus on the United States, to provide recommendations for improvement. The convolutional neural network (CNN) is a preferred model for FRT, as it can identify facial features with high accuracy. The importance of regulation is highlighted and it is suggested to implement strict standards for FRT to ensure ethical and legal use. Recent court cases involving FRT's use in criminal convictions seem to indicate courts are warming up to the idea of FRT being acceptable forms of evidence in the future. This paper aims to inform policymakers, law enforcement, and interest groups on the technical, legal, and ethical implications of FRT.

Issues Presented by The Use Of Social Media And Social Network Analysis By Police

legally, technically and from social science data and management principles

Mohamed Abukar
J.B. Speed School of Engineering
University of Louisville
Louisville, Kentucky USA
mohamed.abukar@louisville.edu

Social Media usage has made sharing information and networking easier than ever and is used by a majority of U.S adults[1] But this treasure trove of information is being used by law enforcement to assist in criminal investigation by finding evidence and making connections . This paper will go over the many perspectives of using social media to serve law enforcement in criminal investigation. Those perspectives include from a legal, technical, social science data, and management principles point of view.

Is cryptography dead? Security in the Quantum Era

Alejandro Giraldo Quintero
J.B. Speed School of Engineering
University of Louisville
Louisville, Kentucky USA
alejandro.giraldoquintero@louisville.edu

Daniel Sierra-Sosa
Department of Computer Science and
Information Technology
Hood College
sierra-sosa@hood.edu

Quantum computing is on the verge of a major breakthrough; a breakthrough that will have far-reaching consequences in science and engineering by addressing formerly intractable problems and thereby advancing basic sciences and commercial applications. At the same time, the ability to quickly solve previously computationally difficult or intractable problems presents new risks and challenges to those concerned with information and data security. As a result of these risks and challenges, two of the most important and active areas of application of quantum technologies are information security and cryptography. In this talk we will provide a brief description of the current state of Quantum Technologies and will discuss future implications in security, detailing some of the encryption alternatives to secure the information in the years to come.