OUR Journal: ODU Undergraduate Research Journal

Volume 7 *Special Issue: Interdisciplinary Cybersecurity Research* Article 1

2020

Special Issue on Interdisciplinary Cybersecurity Research: A Critical High-Impact Practice in Cybersecurity Education

ChunSheng Xin
Old Dominion University

Brian K. Payne
Old Dominion University

INTRODUCTION

INTERDISCIPLINARY CYBERSECURITY RESEARCH:
A CRITICAL HIGH-IMPACT PRACTICE IN CYBERSECURITY EDUCATION

By Chunsheng Xin and Brian Payne

Cybersecurity is a priority area of national need. Numerous cyber attacks happen every day. The Symantec 2018 Internet Security Threat Report (ISTR) revealed 4800 websites compromised every month in 2018, and one out of ten URLs is malicious. Thousands of data breaches were reported every year, including high-profile companies and government agencies such as US Office of Personnel Management, Facebook, and Capital One. Experts agree that cybersecurity is a multifaceted problem that should be addressed through an interdisciplinary framework. Developing interdisciplinary programs can be challenging with various issues such as a lack of a basic interdisciplinary foundation among faculty and students alike. To address the challenges, the NSF funded project with grant #DGE-1723635, "Bridging the Disciplinary Gaps in Cybersecurity Curricula through General Education, High Impact Practices, and Training for Incoming Freshman," integrates student-focused high impact practices into an interdisciplinary cybersecurity major and minor at Old Dominion University. Various studies have shown that the undergraduate research is one critical high impact practice to better engage cybersecurity students and train them to master cybersecurity skills and techniques needed for their future career. Therefore, an important component of this project is to support cybersecurity undergraduate students to work with faculty and industry mentors to carry out research on various popular cybersecurity problems.

This special issue presents 8 papers from the research findings of undergraduate researchers supported by the NSF grant. Those researchers are from the Cybersecurity related programs at ODU, and bring multifaceted cybersecurity research efforts to readers. The paper “Understanding of the Use of Malware and Encryption” by Eva Castillo introduces ransomware and discusses how to simulate ransomware and a defense scheme through encryption. The paper “Detection of Rouge Drones based on Radio Frequency Classification” by Akashi Gosai proposes an improved energy detection algorithm to detect the appearance of drones through an improved Hack-RF software defined radio. The third paper, “Topical Review of Vulnerability Management for Local Hampton Roads Industry,” by Greg Hubbard and Mathew Eunice presents common vulnerabilities in multi-user networks by describing a historical background on cyber security, as well as outlining current methods of vulnerability management. The paper “Study of the Feasibility of a Virtual Environment for Home User Cybersecurity” by Sean Powell and Russell Haines introduces how to utilize virtual machines as a layer of security to prevent cyber attacks. The fifth paper, “Systemic Analysis of the use of Artificial Intelligence (AI) in Regulating Terrorist Content on Social Media Ecosystem using Functional Dependency Network Analysis (FDNA),” by Alaina Roman and Cesar Pinto presents a systemic analysis of emerging risks to the use of Artificial Intelligence (AI) in regulating terrorist content on social media ecosystem analysis, including identifying failure scenarios for each element and establishing causalities among elemental attributes leading to failure scenarios. The sixth paper, “the Influence of Blockchain Technology on Fraud and Fake Protection,” by Youngju Yun and Tamer Nadeem introduces current approaches and solutions

that make use of Blockchain in minimizing the fraud and theft issues in some businesses and our society. The seventh paper, “Cognitive Resource Management in 5G Networks,” by Kelvin Franco-Argueta explores 5G technologies and the resource management for 5G networks. The last paper, “Application of Quantum Cryptography to Cybersecurity and Critical Infrastructures in Space Communications,” by Rita Meraz introduces an interesting frontline problem: quantum cryptography. We invite you to read those interesting papers and explore a variety of state-of-the art topics in cybersecurity.