Research Statement

Imani Palmer

I have a profound passion for security and privacy research. My key research focuses on science of security, applied hacking, and security education. My current research focuses on improving the digital forensic analysis process through the application of artificial intelligence, data mining, and graph theory. I am also passionate about educating the future security workforce. I conduct research in building effective security curriculums for K-12 and community college, and undergraduate.

To me, research is often a bridge to an ambitious goal, a bridge that requires smaller steps in order to cross. I am truly focused on working on projects, that try to bring research ideas to practice. This is not a trivial task as practical situations often requires less assumptions to be made, than conventional research. However, in assuming less usually provide new research opportunities, and solving these problems typically require a multidisciplinary approach. During my time as a doctoral student, I have organized and collaborated on various research efforts, which are discussed below.

Dissertation Work: Forensic Analysis of Computer Science

Digital forensics is the science involved in the discovery, preservation, and analysis of evidence on digital devices. The end goal of digital forensics is to determine the events that occurred, who performed them, and how were they performed. In order for an investigation to lead to a sound conclusion, it must demonstrate that it is the product of sound scientific methodology.

Digital forensics is inundated with many problems. These problems include an insufficient number of capable examiners, without a standard for certification there is a lack of training for examiners and current tools are unable to deal with the more complex cases, and lack of intelligent automation.

This work perpetuates the ability of computer science principles to digital forensics creates a basis of acceptance for digital forensics in both the legal and forensic science community. This work focuses on three solutions. In terms of education, there is a lack of mandatory standardization, certification, and accreditation. Currently, there is a lack of standards in the interpretation of forensic evidence. The current techniques used by forensic investigators during analysis generally involve ad-hoc methods based on the vague and untested understanding of the system. These forensic techniques are the root of the significant differences in the testimony conducted by digital forensic expert witnesses. Lastly, digital forensic expert witness testimony is under great scrutiny because of the lack of standards in both education and investigative methods.

To remedy this situation, we developed multiple avenues to facilitate more effective investigations. To improve the availability and standardization of education, we developed a multidisciplinary digital forensics curriculum [1]. To improve the standards of forensic evidence interpretation, we developed a methodology based on graph theory to develop a logical view of low-level forensic data [2]. To improve the admissibility of evidence, we developed a methodology to assign a likelihood to the hypotheses determined by forensic investigators [3]. Together, these methods significantly improve the effectiveness of digital forensic investigations. Overall, this work calls the computer science community to join forces with the digital forensics community in order to develop, test and implement established computer science methodology in the application of digital forensics [5].

Ongoing Work: Science of Security

In this scope, I am working on a wide variety of projects from securing commodity monolithic operating systems, to performing behavioral analytics on industrial control systems. The science of security domain relies on the application of other fields to improve the security of a domain. This has lead me to learn various topics including software engineering, artificial intelligence, and graph theory.

I am working on a collaborative project with my friend Nathan Dautenhahn who is now a post-doctoral student at the University of Pennsylvania. The primary goal of this research is the development of abstractions, mechanisms, and polices for securing commodity monolithic OSs. OSs are difficult to secure because they operate at the highest privilege level, which means that standard protection mechanisms and common assumptions of suer level approaches are not available. The end goal is to understand how to automatically derive least-privilege compartments. I work on μScope [4], which is revealing strong natural separation in Linux, which could otherwise be considered a complex mesh of an OS.

As a research programmer at the Information Trust Institute, I am responsible for taking a unique look at industrial control systems. Industrial Control Systems (ICS) is an integral part of the nation's infrastructure. ICS are often closed and built on specialized proprietary protocols and interfaces. ICS systems are vulnerable to cyber threats and has become a growing concern for researchers to introduce security and sufficient safety features. Most ICS security approaches are adaptions of conceptional methods for securing traditional IT systems. I work on using data analysis and machine learning to detect intrusions and to obtain a better understanding of the ICS proprietary protocols [6].

Ongoing Work: Applied Hacking

My research in applied hacking is mainly focused on the manipulation of the rules of a system. The goal is to ensure the function of the systems and if a possible attack is identified, the aim is to implement counter-measures. Virtual machine introspection (VMI) has grown into a number

of novel security measures in recent years. Virtualized environments provide isolation, which gives way to better security. This paper presents an extension, WinWizard, of LibVMI that creates a VMI-based intrusion detection system (IDS) with emphasis on memory introspection. WinWizard is able to detect rootkits that attempts to hide processes from the administrator. Rootkits are able to subvert traditional virus scanning services because they are able to run at the kernel level. Rootkit detection becomes difficult because if the operating system has been subverted, especially at the kernel level, then it is difficult to find unauthorized changes to itself or its components. Most anti-viruses and other rootkit detectors that work on infected systems are usually only effective against rookits that have a defect in their hiding techniques. Rootkit detection through VMI is one way to effectively detect rookits. VMI detection tools will also be useful in industry. Industry is beginning to advance in its usage of cloud based workspaces. Examples of companies include Amazons Workspaces and Citrix XenDesktop. They offer remote desktops for small and medium sized businesses. These workspaces offer a fully managed cloud-based desktop experience where users can access their work resources from a variety of devices. Many universities and small businesses use services like these to reduce the number of IT staff and ease administration of a large number of desktops. As this field becomes more accessible, rootkits are going to drastically affect the performance and security of not only one users desktop, but on entire cloud infrastructures. The main way to detect a rootkit inside of these workspaces would be through virtual machine introspection. WinWinzard has demonstrated to be successful in detecting these types of rootkits, while causing little additional overhead to other virtual machines being hosted on the same hypervisor [7].

Ongoing Work: Security Education

There is a great need to educate students in the domain of security. I have designed the curriculum for two courses.

To help address the need for qualified digital forensics professionals, this project develops an adoptable curriculum. The goal is to distribute it as a self-contained curriculum package. This includes an instructor handbook, a lab instructor handbook, lecture slides, and question sets. This will be a significant contribution to the digital forensics education community. When complete, the program will consist of an introductory, an advanced course in digital forensics with accompanying hands-on laboratory sessions, and a special topics course. The introductory course is accessible to a wide range of students from many disciplines and valuable as a stand-alone offering. The second course is more technically intensive, but it is intended to be accessible and valuable to students from non-technical disciplines. The third course is a purely technical course, and it focuses on new relevant topics of digital forensics.

This DF program is not necessarily a job-track training program intended to prepare students to directly enter the job market as digital forensic examiners and analysts. Instead, it provides a broadly applicable education in the field of digital forensics that will be valuable for students going into many disciplines related to digital forensics, such as law, in addition to forensic

analysts. It is expected that these students will receive additional education training specific to their career paths and some on-the-job training specific to their eventual professional roles. At the time of writing, this project developed curriculum for the introductory and advanced course. The pilot courses of both were taught and in the process of curriculum revision for distribution to other institutions. The content includes modules developed collaboratively by faculty experts in multiple fields of computer science, law, psychology, social sciences, and accountancy [1].

In the rush to prepare the next generation of cybersecurity professionals, it is vital that we maintain a holistic view of the education these professionals need. Along with technological expertise, these professionals require an education that will cultivate and develop wide-ranging capacities, skills, and dispositions that will prepare them to address ethical and technological conundrums that stand to shape the future of society. Innovative approaches to cybersecurity education are needed to equip these professionals to be technologically savvy as well as ethically minded and capable of meeting the heavy burden of responsibility that comes with increased technological skills and access to sensitive data.

Future Work and Vision

My completed work demonstrates my determination to improve the field of security. In the future work, I hope to expand security education programs across the United States. Through the development of both in class and online programs. I would work in conjunction with the Center for Assessment of Science, Technology, Engineering and Mathematics to improve the methodologies used by evaluators in the assessment of educational interventions in the STEM disciplines. I also hope to work with the Center for Cyber Security and Privacy (CCSP) to support education and research in these fields. Security requires a cross-discipline approach with the development of open-source tools and technologies to share across academia and industry.

References

1. Palmer, Imani, et al. "Digital forensics education: a multidisciplinary curriculum model." *International Conference on Digital Forensics and Cyber Crime*. Springer, Cham, 2015.
2. Nagy, Stefan, et al. “An Empirical Study on Current Methods for Reasoning about Digital Evidence." *SADFE 2015*: 47.
3. Palmer, Imani, Boris Gelfand, and Roy Campbell. "Exploring Digital Evidence with Graph Theory." ADFSL, (2017).
4. Nathan Dautenhahn, Jai Pandey, Imani Palmer, Derrick McKee, Chris Akatsuka, Vasileios P. Kemerlis, Mathias Payer, Adam Bates, Vikram Adve, Andre DeHon, and Jonathan M. Smith. Under the ´ µSCOPE: Analyzing Least-Privilege Separation in Monolithic Operating Systems. In preparation for ASPLOS (2018).
5. Imani Palmer. Forensic Analysis of Computer Evidence. PhD Thesis, University of Illinois at Urbana-Champiagn, May 2018. Advisor: Roy H. Campbell.

6. Yardley, Tim. "SCADA: issues, vulnerabilities and future directions." *; login:: the magazine of USENIX & SAGE* 33.6 (2008): 14-20.
7. Lamps, Jereme, Imani Palmer, and Read Sprabery. "WinWizard: expanding Xen with a LibVMI intrusion detection tool." *Cloud Computing (CLOUD), 2014 IEEE 7th International Conference on*. IEEE, 2014.