Research Statement

Assad Maalouf
Assistant Professor of Computer Science
Maharishi International University
amaalouf@miu.edu

My research focuses on the intersection of cybersecurity and static analysis, a specialized area of computer science that is crucial for ensuring the reliability and security of software systems. I completed my Ph.D. at Oakland University in Michigan, USA. My dissertation concentrated on static program analysis of Java program code, with a particular focus on security vulnerabilities in mobile applications, especially those running on the Android platform.

Research Background and Contributions

Static program analysis is a powerful tool in cybersecurity. It enables the automatic detection of vulnerabilities within software code. Unlike dynamic analysis, static analysis does not require execution. This approach employs formal methods and mathematical models to identify potential flaws. It seeks correctness, which makes it invaluable in the ongoing effort to protect sensitive data, networks, and systems from cyber threats. My work has primarily focused on developing new, theoretically sound software analysis techniques, as well as enhancing the accuracy and performance of existing techniques. The ultimate goal is to improve the automated discovery of critical vulnerabilities. Automation, crucial for developing secure software, is essential in any software development methodology, especially in continuous integration and continuous delivery, where it ensures the security and reliability of software.

During my doctoral studies, I focused on static analysis techniques for Java programs, particularly applying these techniques to enhance the security of mobile applications. My work primarily focused on string analysis, numerical analysis, taint analysis, and command injection analysis. Taint analysis is used to trace the flow of sensitive information through a program, identifying paths where data might be exposed through public sinks. This method is crucial in preventing data breaches and ensuring that sensitive information is not inadvertently leaked. On the other hand, command injection analysis investigates how unsanitized input might be exploited by malicious actors, potentially leading to the execution of unauthorized commands with the same privileges as the host application. Value sensitivity was used to improve the accuracy of both analyses, reducing false positives and the need for manual intervention.

Research in static program analysis is highly theoretical, requiring a deep understanding of formal methods and their application to real-world problems. However, I have always prioritized the practical implications of my work, striving to bridge the gap between theory and application. My work primarily focuses on the practical application of theoretical research, with emphasis on securing mobile technologies. As mobile technologies have become integral to modern life, ensuring their security is critically important.

Current and Future Research Directions

Since completing my PhD, my research has expanded to explore the integration of static program analysis within the broader context of software development methodologies, particularly DevOps and CI/CD. DevOps has become a critical methodology in modern software engineering, emphasizing automation to enhance the reliability and efficiency of software release cycles. My recent work has focused on investigating how static program analysis can be leveraged to ensure the security, verification, and assurance of code within DevOps pipelines. By automating the detection of vulnerabilities and verifying the correctness of code before deployment, static analysis can reduce the need for manual code reviews, thereby optimizing the software development process.

In addition to my work on static analysis in mobile applications, I have also investigated its application in distributed web programs, which share similar challenges related to lifecycle and control flow as those encountered in Android development. My goal is to develop tools that can automatically analyze and verify distributed systems, ensuring they meet security and performance requirements without the need for extensive manual intervention.

Looking ahead, I plan to further explore the role of static program analysis in emerging software engineering practices. This includes investigating how these techniques can be adapted to new paradigms such as microservices, serverless computing, and other distributed architectures that are becoming increasingly prevalent in industry. My goal is to develop innovative solutions that integrate static analysis seamlessly into the software development lifecycle, ensuring that security and reliability are maintained even as the complexity of systems continues to grow.

Impact and Vision

The impact of my research extends beyond the academic community, contributing directly to the development of safer and more secure software systems. By improving the tools and methods used to detect vulnerabilities, my work helps ensure that the software upon which society heavily relies is both reliable and secure.

Moreover, I am committed to continuing my contributions to scholarly communication through publications in high-quality, peer-reviewed conferences and journals. I believe that sharing knowledge and collaborating with others in the field is essential to advancing the state of the art in cybersecurity.

At the core of my research is a dedication to addressing real-world challenges. As I look to the future, I am excited to continue pushing the boundaries of what is possible in static program analysis, with the ultimate goal of creating a safer digital environment for all.