The Lynne and William Frankel Center
for Computer Science
Department of Computer Science
Ben Gurion University of the Negev
Tel:08-6428032 **Fax**:08-6429021
fradmin@cs.bgu.ac.il

Distinguished Lecturer Series

Marco Pistoia

Manager, Research Staff Member, Master Inventor - IBM T.J. Watson Research Center

Secure Language Design and Program Analysis for security: Lessons Learned in the Industry

13:00-14:00 on Sunday 24th of November Harry and Carol Saal Auditorium, Alon Building for Hi-Tech (37/202)

ABSTRACT: Security auditing of industry-scale software systems mandates automation. Static taint analysis enables deep and exhaustive tracking of suspicious data flows for detection of potential leakage and integrity violations, such as cross-site scripting (XSS), SQL injection (SQLi) and log forging. Research in this area has taken two directions: program slicing and type systems. Both of these approaches suffer from a high rate of false findings, which limits the usability of analysis tools based on these techniques. Attempts to reduce the number of false findings have resulted in analyses that are either (i) unsound, suffering from the dual problem of false negatives, or (ii) too expensive due to their high precision, thereby failing to scale to real-world applications. In this talk, I present a novel approach for enabling precise yet scalable static taint analysis. The key observation informing this new approach is that taint analysis is a demand-driven problem, which enables lazy computation of vulnerable information flows, instead of eagerly computing a complete data-flow solution, which is the reason for the traditional dichotomy between scalability and precision. We have implemented our approach in ANDROMEDA, an analysis tool that computes data-flow propagations on demand, in an efficient and accurate manner, and additionally features incremental analysis capabilities. ANDROMEDA is currently in use in a commercial product. It supports applications written in Java, .NET and JavaScript. Our extensive evaluation of ANDROMEDA on a suite of sixteen production-level benchmarks shows ANDROMEDA to achieve high accuracy and compare favorably to a state-of-the-art tool that trades soundness for precision. In this presentation, I also discuss the challenges introduced by JavaScript and the specific analysis techniques that ANDROMEDA has to include in order to analyze JavaScript programs. This presentation covers work jointly performed with Patrick Cousot, Radhia Cousot and Omer Tripp.

Cyber Security Course

10:00-12:00 on Sunday 24th of November Harry and Carol Saal Auditorium, Alon Building for Hi-Tech (37/202)

ABSTRACT: It can be argued that no concept in Computer Science is more interdisciplinary that Cybersecurity. Any Computer Scientist must have a solid foundation of security, because security is involved in any component of a computer system, including hardware, operating system, applications, databases, and network. Furthermore, security is a key requirement in every single phase of the software lifecycle: design, development, testing, analysis, deployment, provisioning and execution. With the advent of Mobile Computing, security threats have increased dramatically because mobile devices, which often contain large amounts of confidential information, are almost always on and are, unfortunately, easy to lose or steal. With the new "Bring Your Own Device" trend, another challenge is to allow personally owned mobile devices to host both personal and enterprise applications and store both personal and enterprise data, while preventing intentional or unintentional interference, leaking of private data, and contamination of security-sensitive operations. In this talk, I will present the challenges of today's Cybersecurity, and the skills that any Computer Science student must have to be prepared to work in the industry.

Dr. Marco Pistoia received his Ph.D. in Mathematics from New York University in May 2005. He is a Manager, Research Staff Member and Master Inventor at the IBM Thomas J. Watson Research Center in New York, where he leads the Mobile Middleware and Language-based Security group. He has authored numerous conference papers, journal articles and books in the areas of programming languages, program analysis and security. He is the inventor of thirty patents. He has been the recipient of two ACM SIGSOFT Distinguished Paper Awards. In the course of his career, he has designed and implemented numerous static-analysis components and contributed large amounts of code to IBM's main products for software quality and security enforcement. Dr. Pistoia is also an Adjunct Professor at New York University, and has lectured at numerous research institutions worldwide.