Designing and Leveraging Trustworthy Provenance-Aware Architectures

Adam Bates

Department of Computing & Information Science & Engineering
University of Florida
Gainesville, FL

1:00 p.m., Wednesday, January 27, 2016

Abstract

In a provenance-aware system, mechanisms gather and report metadata that describes the history of each object being processed on the system, allowing users to understand how data objects came to exist in their present state. However, little attention has been given to securing provenance-aware systems. Provenance itself is a ripe attack vector, and its authenticity and integrity must be guaranteed before it can be put to use. In this talk, I will detail my efforts to bring trustworthy data provenance to computing systems. These efforts have led to the design and implementation of a provenance-aware operating system anchored in trusted hardware, and a mechanism that leverages the confinement properties provided by Mandatory Access Controls to perform efficient policy-based provenance collection. Using these architectures, I will demonstrate that provenance is an invaluable tool for combating critical security threats including data exfiltration, SQL injection, and even binary exploitation. By addressing key security and performance challenges, this work paves the way for the further proliferation of provenance capabilities.

1313 W. Wisconsin Avenue, Cudahy Hall, Room 401, Milwaukee, WI 53201-1881

For further information:  http://www.mscs.mu.edu/mscs/resources/colloquium.html, or contact Dr. Naveen Bansal: 414-288-5290, naveen.bansal@marquette.edu.

POST-COLLOQUIUM REFRESHMENTS SERVED IN ROOM 342 AT 2:00 P.M.