

Lecturer: Barton P. Miller
Computer Science Department, University of Wisconsin - Madison

Title: A Framework for Binary Coding Analysis and Static and Dynamic Patching

Abstract: Tools that analyze and modify binary code are crucial to many areas of computer science, including cyber forensics, program tracing, debugging, testing, performance profiling, performance modeling, and software engineering. Many tools used to support these activities have significant limitations in functionality, efficiency, accuracy, portability and availability.

Our goal is the design and implementation of a new framework that will allow for interoperability of the static and dynamic code modification, and enable the sharing and leveraging of this complex technology.

Characteristics of this framework include: multi-architecture, multi-format, and multi-operating system; library-based; open source; extensible data structures; exportable data structures; batch enabled; testable, with each separate component provided with a detailed test suite; and functions with non-contiguous and shared code.

This component-based approach requires identifying key portable and multi-platform abstractions at every level of functionality. Transitioning to this model successfully will enable us to break the "hero model" of tool development of having each group trying to produce its own end-to-end complete tool sets.