

IOWA STATE UNIVERSITY
DEPT OF COMPUTER SCIENCE
Presents

Hybrid System Call Interposing

Prem Uppuluri

Computer Science Department
University of Missouri at Kansas City

Solutions to many important operating system problems are based on extending/enhancing operating system functionality. However, this is a difficult and expensive task as modern operating systems are very large and complex – running into millions of lines of code which have been developed over many years by a large number of programmers. An alternate approach is interposition, wherein extension code is interposed at well-defined system interfaces SLIC. This approach requires no modifications to existing operating system code - instead, each call to an operation in the interface is intercepted and routed to the extension code.

System-call interposition, which involves interposing extension code at the application to operating system boundary, is one of the well-researched interposition approaches, discretionary access control, file system encryption, stackable file systems, sandboxing, intrusion prevention and detection, performance isolation, checkpointing, process migration as it offers several advantages over other forms of interposition. We propose a new framework that is inspired by the network packet-filtering model to develop system-call interposition based extensions called hybrid interposition. The key contributions of our approach over the current state of the art in system call interposition are: (a) A high level rule-based language called Behavior Monitoring Specification Language (BMSL) which provides an expressive, efficient mechanism to code extensions and (b) a hybrid interposition mechanism which intercepts system calls inside the kernel and processes them in user space.

Prem Uppuluri has a BE in Computer Science from Osmania University India, M.S from Iowa State University and Ph.D from the State Univ. of New York at Stony Brook (2003). He is currently an Asst. Professor in Computer Science at the University of Missouri, Kansas City. His research includes computer system security (intrusion prevention, secure operating systems), network management (protocol monitoring and fault injection) and operating systems (interposing extension code and file system).

November 13, 2003, 3:40 pm, 223 Atanasoff Hall
Refreshments will be served at 223 Atanasoff Hall