

## Process Authentication for High System Assurance

### Abstract:

This paper points out the need in modern operating system kernels for a process authentication mechanism, where a process of a user-level application proves its identity to the kernel. Process authentication is different from process identification. Identification is a way to describe a principal; PIDs or process names are identifiers for processes in an OS environment. However, the information such as process names or executable paths that is conventionally used by OS to identify a process is not reliable. As a result, malware may impersonate other processes, thus violating system assurance. We propose a lightweight **secure** application authentication framework in which user-level applications are required to present proofs at runtime to be authenticated to the kernel. To demonstrate the application of process authentication, we develop a system call monitoring framework for preventing unauthorized use or access of system resources. It verifies the identity of processes before completing the requested system calls. We implement and evaluate a prototype of our monitoring architecture in Linux. The results from our extensive performance evaluation show that our prototype incurs reasonably low overhead, indicating the feasibility of our approach for cryptographically authenticating applications and their processes in the operating system.

**SMART REACH**  
(S/W CREATORS & TRAINERS)



Ph: 9585554590, 9585554599

Email: [support@salemsmartreach.com](mailto:support@salemsmartreach.com)

URL: [www.salemsmartreach.com](http://www.salemsmartreach.com)

**450/526, Trichy Main Road, Near Sri Sakthi Kaliamman Temple, Dadhagapatti Gate,  
Salem-636 006, Tamil Nadu, India.**