

An Extended-OpenBSD Security Architecture: MYSEA

Cynthia Irvine, Timothy Levin

Center for INFOSEC Studies and Research

Naval Postgraduate School

The Monterey Security Enhanced Architecture (MYSEA) project is constructing a prototype demonstration of a potential high assurance distributed operating environment for enforcing multi-domain security policies and running unmodified COTS productivity applications. The distributed prototype system is composed of a combination of many low-assurance commercial components and relatively few specialized, multi-domain enforcement components. The primary enforcement component is a security-enhanced version of the OpenBSD operating system. The demonstration architecture permits the on-going DoD and U.S. Government investment in commodity PC operating systems and applications to be integrated into a high assurance environment where enforcement of critical security policies is assigned to more trusted elements. The modularity of the architecture permits alternate configurations, for example to include an EAL7- (or Class A1-) evaluated high assurance multi-domain enforcement component.

Our goals are to demonstrate extended file system attributes to enforce multi-domain access controls in existing open operating systems and to demonstrate trusted interoperability for these extended capabilities with open source and COTS workstations, and office productivity applications.

For this project, we have chose OpenBSD as the open source base which we will extend. However, the modifications we have defined are modular and conceptually simple enough that they could be accomplished on a variety of open source or evaluated high assurance platforms (e.g., Linux). We intend to demonstrate techniques for vertical integration of application security requirements with underlying security services, and we will apply an existing Quality of Security Service model and framework to the integrated security structure to better understand the overall effects on security policy, security service, and security mechanism interactions. Additionally, the MYSEA system will support trusted path communications between the user and the trusted OS, and will also support single sign-on for interaction with multiple trusted servers.

We expect that this project will result in significant new and improved security functionality for existing open source operating systems and will provide the capability to significantly reduce vulnerabilities in mission critical information systems and networks.