MYSEA: An Approach to Building High Assurance Composite System for Cloud Computing

Thuy D. Nguyen, Cynthia E. Irvine
Department of Computer Science, Naval Postgraduate School
Monterey, California 93943, USA

Abstract

The need for highly robust enterprise-level architectures that implement multi-domain information protection mechanisms is widespread and growing, especially in the context of cloud computing which promotes dynamicity, scalability and collaboration across domains and organizations.

The Monterey Security Architecture (MYSEA) addresses this need by integrating cloud computing functionality with the strong security properties required by a highly robust multi-domain system. The MYSEA architecture combines highly trustworthy multilevel secure servers and special-purpose multi-domain authentication components to provide centralized cross-domain security policy enforcement. Users can continue to use commodity workstations and familiar web-based applications for collaboration and access to data across domains. MYSEA’s security features include strong cross-domain access controls, protection of system assets (data and services) with different security classifications, resource isolation, service replication and dynamic control of Quality of Security Service attributes.

The MYSEA cloud is oriented towards the Cloud Software as a Service (SaaS) model and supports many characteristics associated with cloud computing, including broad network access, resource pooling and measured services. In terms of ownership, administrative domain, and availability to a larger community, the MYSEA cloud is deployable as a private cloud, a community cloud, or a hybrid cloud.

The MYSEA design requires that both the MYSEA servers and special-purpose authentication components run on high assurance trusted foundations. The MYSEA server currently runs on an EAL5-augmented trusted platform (i.e., BAE XTS-400) and the special-purpose authentication components are being designed to run on a Least Privilege Separation Kernel that is targeted for an EAL7 evaluation. The MYSEA Target of Evaluation Security Functionality is comprised of trusted processes of both the MYSEA server and authentication components. This paper describes the MYSEA TOE architecture, including both physical and logical boundaries, the composition of TSF and non-TSF processes, and the MYSEA’s approach for building high assurance composite multilevel secure systems.