Contribution ID: **415** Type: **oral**

Flexible Session Management in a Distributed System

Tuesday, March 24, 2009 5:30 PM (20 minutes)

Many secure communication libraries used by distributed systems, such as SSL, TLS, and Kerberos, fail to make a clear distinction between the authentication, session, and communication layers. In this paper we introduce CEDAR, the secure communication library used by the Condor High Throughput Computing software, and present the advantages to a distributed computing system resulting from CEDAR's separation of these layers.

Regardless of the authentication method used, CEDAR establishes a secure session key, which has the flexibility to be used for multiple capabilities. We demonstrate how a layered approach to security sessions can avoid round-trips and latency inherent in network authentication. The creation of a distinct session management layer allows for optimizations to improve scalability by way of delagating sessions to other components in the system. This session delegation creates a chain of trust that reduces the overhead of establishing secure connections and enables centralized enforcement of system-wide security policies. Additionally, secure channels based upon UDP datagrams are often overlooked by existing libraries; we show how CEDAR's structure accommodates this as well.

As an example of the utility of this work, we show how the use of delegated security sessions and other techniques inherent in CEDAR's architecture enables US CMS to meet their scalability requirements in deploying Condor over large-scale, wide-area grid systems.

Primary author: MILLER, Zachary (University of Wisconsin)

Co-authors: BRADLEY, Daniel (University of Wisconsin); SFILIGOI, Igor (Fermilab); TANNENBAUM, Todd (University of Wisconsin)

Presenter: MILLER, Zachary (University of Wisconsin)

Session Classification: Software Components, Tools and Databases

Track Classification: Software Components, Tools and Databases