T-BASS (Trust-Based Agent Security Services)

Trust-Based Agent Security Services - A sophisticated trust model has been defined to allow for the autonomous establishment/maintenance of meaningful, individual trust relationships among interacting agents, the monitoring of behavior and adaptation of behavior based on cognitive abilities and on changes in the trust relationships with other agents and the environment. A biologically inspired trust fabric is envisioned that captures the way humans establish and maintain trust relationships (i.e., through experiences from repeated interaction and association with trusted entities). Mechanisms are required that counteract the concerns produced by the mobile code and behavioral changes due to adaptability and flexibility of a mobile agent system. This project has developed the following fundamental components: The *identification of threats and trust factors* leveraging experiences from previous and related work to focus especially on the requirements and scenarios present in critical cyber infrastructures such as the national power grid (i.e., malicious agents and compromised hosting environments, coordinated attacks, and cascading/common mode fault conditions). *A hybrid, multi-level trust model uses* trust factors and threat levels to change the status of trust agents place in each other. The model addresses issues on how trust changes over time and enables adaptive, self-correcting behavior and a fine granularity of trust. The hybrid component reflects different computational abilities of components, not typically find in humans (e.g., using cryptographic hardware when trust is established or reevaluated due to recent events). *Inter-agent trust communication fabric is provided* for agents and hosting environments to exchange information about trust status separate from the functional communication mechanisms between the agents (e.g., if an agent A detects unusual behavior in agent B it should be able to convey a subsequent loss of trust to other agents C and D that interact with B). Protocols for distributed agreement and voting, the exchange of typical behavioral patterns and other contextual information are required. *Dynamic reconfiguration, reactive mechanisms and countermeasures:* The survivability of the overall system depends much on the agents' ability to adapt their behavior based on their current and evolving trust beliefs as well as elevated privileges that are bound to certain environmental conditions (i.e. such as increased threat levels, state of emergency) in an effort to provide quick response and recovery from failures. Further, if trust in an agent is lost then this agent should not be assigned critical tasks or be trusted to provide reliable information (i.e., other agents may choose to ignore a rogue agent). *Hardware-enhanced security mechanisms for highly trusted to* explore hardware secured execution environments as well as semi-mobile agents that reside in the protected compute environments of smart cards including the performance/security tradeoffs in different threat environments – Sheldon/Ferragut

POC: Frederick Sheldon, PhD, MS; Erik Ferragut, PhD
Cyberspace Sciences & Information Intelligence Research (CSIIR) Group
Oak Ridge National Laboratory P.O. Box 2008, Oak Ridge, TN 37831-6418
www.ioc.ornl.gov