Biologically Inspired Security Infrastructure for Tactical Environments

Appropriation Account:	RDT&E, Defense-Wide
Line Item:	Computer & Software Technology (PE 0602783A)

Project Description: In today's highly volatile world, various governmental and nongovernmental organizations must be able to form *ad-hoc* groups for immediate response in times of crisis. Given the nature of their work, it is essential that such groups come together quickly and function efficiently. Often, the tactical environments required by such military and/or civilian operations and disaster relief missions lack a centralized electronic network infrastructure that can coordinate and enforce network security policies and practices. In such scenarios, the critical need to quickly combine communication resources and capabilities often creates vulnerabilities that can compromise the mission in unforeseen and potentially devastating ways. The lack of a centralized monitoring infrastructure in these cases makes it extremely difficult to support an external trusted mechanism for system verification in the field, leaving the system macroscopically vulnerable to attack.

As support and soldier information systems become increasingly flexible and powerful, it is imperative to ensure that changes in applications, system configuration, or mode of operation in the battlefield will not leave our men and women in uniform vulnerable to exploitation by a technologically-sophisticated enemy. Fiscal year 2007 funding will allow for the development of a distributed security infrastructure designed to ensure that networked systems and devices deployed in the field accommodate security requirements in terms of application integrity, policies, and configuration. The goal is to enable flexible in-field system customization and evolution while ensuring compliance with a basic set of policies and configurations that are conducive to maintaining information security.

The *ad-hoc* nature of the network in such environments makes it difficult to apply traditional approaches to monitoring and security. The proposed framework addresses this challenge by creating self-organized hierarchies autonomically. Nodes will detect improper configurations and rogue applications in their peers and take preventive security measures and/or alert users about possible threats and vulnerabilities in the trusted network. The framework will be adaptive in the sense that it will not only comply with pre-established security policies, but it will also learn by example about acceptable changes in configuration and applications. Policies and inferences will be based on similarities within hierarchical functional groups that are formed autonomically by the framework as nodes exchange information about their configuration and state. The capabilities provided by the proposed framework will support increased flexibility and adaptability of deployed systems. Vulnerabilities and penetrations could then be quickly identified, isolated, and reported.

The proposed research will be performed by a team led by the Florida Institute of Technology (FIT) and include the Florida Institute for Human and Machine Cognition (IHMC).