

Keynote (D-2): Understanding Multistage Attacks in the Cyberspace to Address the Grand Challenges in Security

Shambhu Upadhyaya

*Center of Excellence in Information Systems Assurance Research and Education (CEISARE)
University at Buffalo - SUNY*

Secure computing practices today mandate the deployment of attack detection and mitigation tools such as firewalls, anti-virus software and intrusion detection sensors (IDS). Yet, with the expansion of the cyberspace, computer attacks have progressively become more sophisticated and harder to detect. One of the primary concerns today is the threat of organized cyber attacks that are aimed at disrupting the nation's critical infrastructures and the national security. Consequently, researchers have shifted focus to event correlation and fusion techniques to identify coordinated attacks. However, the techniques so developed are useful primarily from the standpoint of forensic analysis and network hardening. Situation awareness of attacks in near real-time can provide the benefits of possible attack mitigation and containment. Validation of research prototypes with realistic data is also an important requirement.

The effective situation awareness of coordinated multistage attacks calls for a good understanding of the attack model, consideration of the suitable granularity levels of event data generated on the networks, attack semantics, and data dimensionality for effective comprehension and visualization. In this talk, we will review the current state-of-the-art in the disciplines, the inadequacy of current solutions to address the attacks that may be coming from within an organization, and some proposed solutions. We will end the talk by identifying the grand challenge problems in security and some predictions on the state of security looking forward several years.