Title: Cognitive Cyber Security Assistant: Design Overview

Speaker: Carla Sayan

Abstract: This paper focuses on the design and implementation of an Intelligent Cyber Security Assistant (ICSA) architecture that would provide intelligent assistance to a human security specialist. The ability to focus on rapidly developing malicious events which have the most impact on the normal operations of cyber resources and services is both critical and challenging. Effectively responding to cyberattacks, which have been expanding at alarming rates, will require advanced machine learning to automatically detect attacks and intelligently recommend the mechanisms to render attackers incapable of re-launching new attacks. To effectively address these challenges, we present the design and implementation of an intelligent cyber assistant that will assist security analysts by efficiently and promptly defending cyberspace resources and services against both existing and novel attacks. Additionally, we show that the ICSA can adapt and learn efficiently to improve our intelligence gathering and analytics capabilities to perform sophisticated cyber situation awareness tasks and to develop automated and semi- automated actions to protect against discovered vulnerabilities.