SEMANTIC INFORMATION INFRASTRUCTURE PROTECTION (INVITED ABSTRACT)

Paul Thompson
Dartmouth College, Hanover, New Hampshire 03755, Paul.Thompson@dartmouth.edu

Abstract: The information infrastructure, consisting of the Internet and numerous intranets, extranets, and other networks, is a key national critical infrastructure, interwoven with other critical infrastructures. Protecting the information infrastructure is important in its own right, and also because of the steadily increasing interdependence of other critical infrastructures on the information infrastructure. This paper describes an approach to information infrastructure protection that was developed as part of the semantic hacking project. Attacks on computer and other networked systems can be categorized as physical, syntactic and semantic. Autonomous agents being fed misinformation in the battlespace is a primary example of a semantic attack. Physical attacks seek to destroy hardware, while syntactic attacks, such as worms and viruses target the network infrastructure. Attacks specifically against a human user of system are also referred to as cognitive attacks. Because misinformation and deception play a much more significant role in intelligence and security informatics than in other informatics disciplines, such as science, medicine, and the law, such an emerging discipline must concern itself with semantic attacks and countermeasures.

Key words: Infrastructure Protection; Network Security; Semantic Attacks.