

# MASTER OF SCIENCE IN SOFTWARE ENGINEERING

---

## REAL-TIME INTRUSION DETECTION FOR WINDOWS NT BASED ON NAVY IT-21 AUDIT POLICY

H. Steven Kremer-DoD Civilian

B.S., San Diego State University, 1982

Master of Science in Software Engineering-September 1999

Advisors: Neil C. Rowe, Department of Computer Science

Ronald Broersma, SPAWAR Systems Center, San Diego

A Navy directive orders the migration of Navy computer systems to an Internet-connected network of Windows NT workstations and servers. Windows NT possesses the security features of a class C2 computer system but does not offer a standard real-time host-based tool to process the security-event audit data to detect intrusions or misuse. We discuss what would entail in general. We also report on experiments with a sensor program, which resides on each workstation and server in the network and provides some real-time processing of NT host-based events. It passes information to an Agent that communicates to other Agents in the network, in an effort to identify and respond to an intrusion into the network. The Navy audit policy and the methods of implementing the policy are also investigated in this thesis.

**DoD KEY TECHNOLOGY AREAS:** Command, Control, and Communications, Computing and Software

**KEYWORDS:** Intrusion Detection, Artificial Intelligence, Autonomous Agents, Computer Security