An Approach To Vulnerability Assessment For Navy Supervisory Control And Data Acquisition (SCADA) Systems

Dennis Hart
The unfortunate events of September 11, 2001 have caused a renewed effort to protect our Nation’s Critical Infrastructures. SCADA systems are relied upon in a large number of the sectors that make up the critical infrastructure and their importance was reinforced during the massive power outage that occurred in August 2003. Growing reliance upon the Internet has emphasized the vulnerability of SCADA system communications to cyber attack. Only through diligent and continuous vulnerability assessment and certification and accreditation of these systems will the United States be able to mitigate some of the vulnerabilities of these systems. A case study presented here has validated the need for continued focus in this area. This thesis consolidates some of the research that has already been done in the area of SCADA vulnerability assessment and applies it by developing an initial vulnerability assessment checklist for Department of the Navy systems. This checklist can and should also be used in the certification and accreditation of DoN SCADA systems. A promising technology was also discovered during this research that should be explored further to secure SCADA communications. This will be touched on briefly.

Dmca