**Paper Submission**

# GrIDS–A Graph-Based Intrusion Detection System for Large Networks

S. Staniford-Chen (POC), R. Crawford, M. Dilger,
J. Frank, J. Hoagland, K. Levitt, D. Zerkle

*Department of Computer Science,*
*University of California, Davis,*
*Davis, CA 95616*

phone: (916) 754-8742
messages: (916) 752-7004
FAX: (916) 752-4767
email: *stanifor@cs.ucdavis.edu*

**Abstract**

There is widespread concern that large-scale malicious attacks on computer networks could disrupt a country's economy and pose a threat to its national security. We present the design of GrIDS (Graph-Based Intrusion Detection System). GrIDS will collect data about activity on computers and network traffic between them. It will aggregate this information into *activity graphs* which approximately represent the causal structure of network activity. This will allow large-scale automated attacks to be detected in near real-time. In addition, GrIDS will allow network administrators to state policies specifying which users may use particular services of individual hosts or groups of hosts. By analyzing the characteristics of the activity graphs, GrIDS will detect and report violations of the stated policy. GrIDS will use a hierarchical reduction scheme for its graphs, which will allow it to scale to large network applications. An early prototype of GrIDS has successfully detected a worm attack.