Journal of Computer Security 7 (1999) 1
IOS Press

Editorial

Special section on Intrusion Detection

In this issue of the *Journal of Computer Security*, there is a special section on Intrusion Detection organized and edited by Phil Porras of SRI International. It includes papers that describe research beyond the scope of, or orthogonal to, what the commercial intrusion-detection community is producing. The intent was to capture results from key efforts in the field, and to understand the directions and motivations that are driving current and future research in this area. The call for papers set the stage as follows:

> "There has been a recent resurgence in efforts within the intrusion-detection research community to investigate and extend intrusion-detection technology to larger distributed computing environments, including work to address such issues as scalability, interoperability, distributed correlation, dynamic deployment, and autonomous operation. Among such efforts has been work involving the cross-pollination of intrusion-detection research with other communities, such as the information retrieval and network management communities. In addition, interest has arisen in applying intrusion-detection technology to new problem domains, such as fraud detection in financial transactions and operations monitoring of telecommunications infrastructures."

The two papers in this special section are "Identification of host audit data to detect attacks on low-level IP vulnerabilities", by T.E. Daniels and E.H. Spafford of Purdue University, and "NetSTAT: A network-based intrusion detection system", by G. Vigna and R.A. Kemmerer of the University of California at Santa Barbara.

Jonathan Millen