

Data Mining Historical Network Data to Increase the Effectiveness  
of Intrusion Detection Analysis

Kerry S. Long and Joan B. Morgan  
U.S. Army Research Laboratory  
Aberdeen Proving Ground, MD

ABSTRACT:

The Army Research Lab Center for Intrusion Monitoring Protection (CIMP) maintains long-term repositories of network data activity collected from monitored sites. Until recently, this historical data was used mainly for the verification of past cyber events and incidents, and occasionally as forensics evidence.

The CIMP now leverages these data stores by extracting relevant patterns through the use of fundamental data mining techniques. Knowledge derived from the mining process are in turn used to make filtering decisions to reduce redundant data produced by various analysis products such as the network traffic capture program and the network flow reporting tool.

KEYWORDS: Intrusion Monitoring Protection, data mining, network traffic

CONTACT: Kerry S. Long, U.S. Army Research Laboratory, AMSRD-ARL-CI-HN,  
Aberdeen Proving Ground, MD, Tel: (301) 394-2720, Email:  
[klong@arl.army.mil](mailto:klong@arl.army.mil)

Joan B. Morgan, U.S. Army Research Laboratory, AMSRD-ARL-CI-HN,  
Aberdeen Proving Ground, MD, Tel: (301) 394-1237, Email:  
[joan.morgan@arl.army.mil](mailto:joan.morgan@arl.army.mil)