Contribution ID: **118** Type: **poster**

AutoBlocker: A system for detecting and blocking of network scanning based on analysis of netflow data.

Tuesday, 28 September 2004 10:00 (0 minutes)

In a large campus network, such as Fermilab's ten thousand nodes, scanning initiated from either outside of or within the campus network raises security concerns, may have very serious impact on network performance, and even disrupt normal operation of many services. In this paper we introduce a system for detecting and automatic blocking of excessive traffic of different nature, scanning, DoS attacks, virus infected computers. The system, called AutoBlocker, is a distributed computing system based on quasi-real time analysis of network flow data collected from the border router and core routers. AutoBlocker also has an interface to accept alerts from the IDS systems (e.g. BRO, SNORT) that are based on other technologies. The system has multiple configurable alert levels for the detection of anomalous behavior and configurable trigger criteria for automated blocking of the scans at the core or border routers. It has been in use at Fermilab for about 2 years, and become a very valuable tool to curtail scan activity within the Fermilab campus network.

Primary authors: BOBYSHEV, A. (FERMILAB); LAMORE, D. (FERMILAB); DEMAR, P. (FERMILAB)

Presenter: BOBYSHEV, A. (FERMILAB)

Session Classification: Poster Session 1

Track Classification: Track 7 - Wide Area Networking