Recent Advances in Self-directed Network Intrusion Detection

Paul Barford
University of Wisconsin, Madison

Network attacks and intrusions have been a fact of life in the Internet for many years and continue to present serious challenges for network researchers and operators alike. In the first part of this talk, I will outline the network security problem space by describing the characteristics of the current generation of malicious traffic and software based on data collected in our large monitoring infrastructure over the past several years. Our results highlight the variability and heterogeneity in malicious traffic, and the growing sophistication of malicious software. This detailed empirical understanding of attack characteristics forms the foundation of our work to enable real time network "situational awareness" for security analysts. Our approach is to develop methods and systems that automate or otherwise enhancing key activities in security operations. In the second part of this talk, I will describe our Nemean intrusion detection system that has the unique capability to automatically generate intrusion signatures. Unlike standard intrusion signatures, Nemean's signatures are protocol-aware, which we show greatly enhances their resilience to false alarms. I will present our experiences in the operational use of Nemean including comparisons with other open-source and commercial systems. Finally, I will describe our current efforts to scale Nemean's capabilities to next generation high speed networks by pushing critical functions into network processor hardware.

Keywords:

Network security: The policies, systems and configurations used by network administrators to protect networked systems and data from unwanted access. Typical systems include firewalls, intrusion detection systems and intrusion prevention systems.

Intrusion detection systems: A device that monitors traffic on a network link and generates an alert message to a network administrator when malicious activity (such as scans, worms or denial of service attacks) is identified.

Honeynet: A portion of routed but otherwise unused Internet address space that is monitored. By definition all traffic on unused address space is malicious (or occasionally caused by misconfigurations), thus honeynets are a valuable source of data on unwanted traffic.