Bibudh Lahiri

PhD

Computer Engineering

Major Professor: Srikanta Tirthapura

Co-major Professor: Yong Guan

Detecting Exploit Patterns from Network Packet Streams

Network-based Intrusion Detection Systems (NIDS), e.g., Snort, Bro or NSM, try to detect malicious network activity such as Denial of Service (DoS) attacks and port scans by monitoring network traffic. Research from network traffic measurement has identified various patterns that exploits on today's Internet typically exhibit. However, there has not been any significant attempt, so far, to design algorithms with provable guarantees for detecting exploit patterns from network traffic packets. In this work, we develop and apply data streaming algorithms to detect exploit patterns from network packet streams.

In network intrusion detection, it is necessary to analyze large volumes of data in an online fashion. Our work addresses scalable analysis of data under the following situations. (1) Attack traffic can be stealthy in nature, which means detecting a few covert attackers might call for checking traffic logs of days or even months, (2) Traffic is multidimensional and correlations between multiple dimensions maybe important, and (3) Sometimes traffic from multiple sources may need to be analyzed in a combined manner. Our algorithms offer provable bounds on resource consumption and approximation error. Our theoretical results are supported by experiments over real network traces and synthetic datasets.