22 - STUDENT - Real-Time and Resilient Intrusion Detection: A Flow-Based Approach

Rick Hofstede (University of Twente)

Due to the demanding performance requirements of packet-based monitoring solutions on network equipment, flow-based intrusion detection systems will play an increasingly important role in current high-speed networks. The required technologies are already available and widely deployed: NetFlow and the newer IPFIX aggregate packets into flows and are applicable in networks with line speeds in excess of 1Gbit/s. Intrusion detection systems need to be modified in order to deal with the aggregated flow data. As such, we have to consider constraints on the real-time and accurate
detection of intrusions, imposed by the nature of current flow monitoring technologies. This poster presents a framework for flow-based intrusion detection, aiming to detect intrusions in real-time, and to be resilient against negative effects of attacks on monitoring systems.