Security Monitoring and Alert Correlation for Intrusion Detection in Large Networks

Steffen Haas

Attacks on IT systems not only affect individual users but often also have network-wide effects with tremendous consequences for many systems and the overall network operation. Detecting attacks on IT systems early on by an Intrusion Detection System (IDS) can prevent severe damage. However, intrusion detection faces two major problems: First, the IDS must monitor and assess the malicious activity despite IDS-evasion or traffic encryption by the attacker. Second, the full attack story must be reconstructed from the malicious activity to initiate appropriate countermeasures.

After giving an overview of my research contributions along a coherent intrusion detection process, the talk will present an integrated open-source platform that extends the scope of a network IDS with additional data from hosts. This platform can collect, process, and correlate host and network data at large scale for better detection accuracy of malicious activity. Afterwards, an alert correlation algorithm is applied to the detection results to isolate attacks, identify their scenario, and to assemble the individual actions to network-wide attacks such as distributed and multi-step attacks.