CATS – Cooperating Autonomous Detection Systems

Abstract
Today’s communication networks are threatened by an increasing number intrusion attempts, worms, and denial of service (DoS) attacks. Apart from general measures for attack prevention, the possibility to detect ongoing attacks in order to take appropriate countermeasures constitutes an important asset for network security. We present a novel approach for attack detection based on cooperating autonomous detection systems (CATS). While a single detection system is able to identify ongoing attacks autonomously, cooperation with remote detection systems located in other parts of the network can improve the detection performance.

Concept and benefits of CATS:
- Separation of monitoring and detection
- Utilization of a distributed monitoring environment
- Deployment of multiple independently working autonomous detection systems
- Self-X properties of the detection systems
- Improved detection performance through cooperation between multiple detection systems
- Combination of knowledge-based and anomaly detection techniques using both local and global context information
- Export of packet data and flow statistics utilizing standardized protocols, e.g. IPFIX and PSAMP

Further work:
- Implementation of a proof-of-concept prototype in the context of the EU project Diadem Firewall (EU FP6 Project IST-2002-002154)
- Performance evaluation and comparison with competitive systems

Selected references:
B. Claise et al., "IPFIX Protocol Specifications," in draftietf-ipfix-protocol-03.txt, 2004

Comparison with related systems


Project homepage: http://net.informatik.uni-tuebingen.de/projects/diadem/ and http://www.diadem-firewall.org/