University of Tübingen

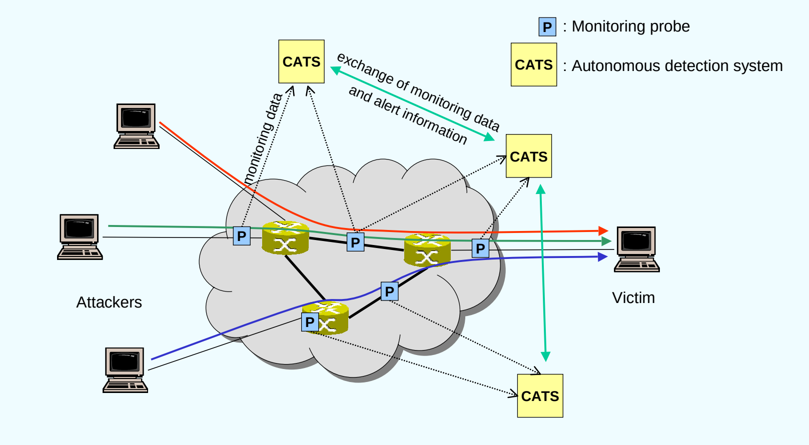
WSI – Computer Networks and Internet

Falko Dressler, Gerhard Münz, Georg Carle

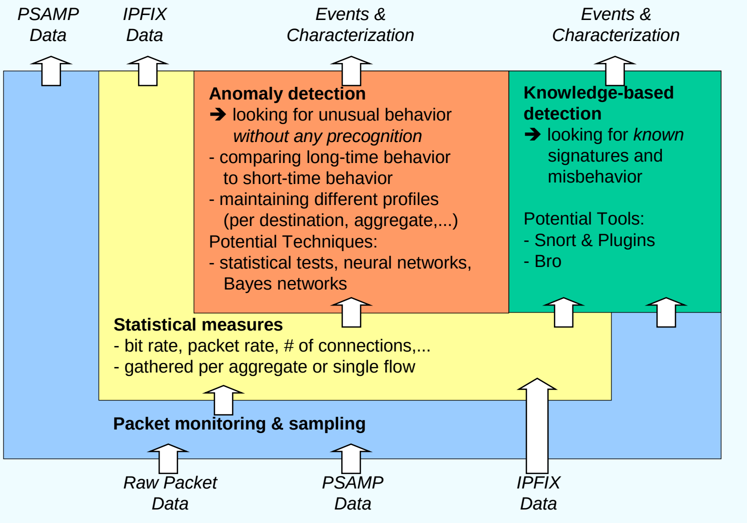
CATS – Cooperating Autonomous Detection Systems

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.


P : Monitoring probe
CATS : Autonomous detection system
CATS
exchange of monitoring data and alert information
monitoring data
CATS
P
P
P
P
P
CATS
Attackers
Victim

DDoS attack scenario



PSAMP Data

IPFIX Data

Events & Characterization

Events & Characterization

Anomaly detection
➔ looking for unusual behavior *without any precognition*
- comparing long-time behavior to short-time behavior
- maintaining different profiles (per destination, aggregate,...)

Potential Techniques:
- statistical tests, neural networks, Bayes networks

Knowledge-based detection
➔ looking for *known* signatures and misbehavior

Potential Tools:
- Snort & Plugins
- Bro

Statistical measures
- bit rate, packet rate, # of connections,...
- gathered per aggregate or single flow

Packet monitoring & sampling

Raw Packet Data

PSAMP Data

IPFIX Data

CATS architecture

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

		EMERALD[1]	Prelude IDS[2]	D-WARD[3]	COSSACK[4]	CATS
Attack detection	Global context	yes	yes	yes	yes	yes
	Local context	no (host-based)	no	no	yes	yes
	Knowledge-based	yes	yes	no	no	yes
	Anomaly	yes	no	yes	yes	yes
Autonomous behavior		no	no	yes	yes	yes
Distributed Intelligence	Separation of monitoring & detection	no	no	no	no	yes
	Distributed detection	yes	partly	no	no	yes

[1] P. A. Porras et al., "EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances," NISSC 1997
[2] Prelude IDS homepage, http://www.prelude-ids.org/
[3] J. Mirkovic et al., "Attacking DDoS at the Source," ICNP 2002
[4] C. Papadopoulos et al., "COSSACK: Coordinated Suppression of Simultaneous Attacks," Discex 2003

Comparison with related systems

Selected references:

R. Bace and P. Mell, "Intrusion Detection Systems,“ NIST 2001

R. K. C. Chang, "Defending against Flooding-Based Distributed Denial-of-Service Attacks: A Tutorial," IEEE Communications Magazine, vol. 10, 2002, 42-51

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

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