



The Violation Detection Framework TOPAS

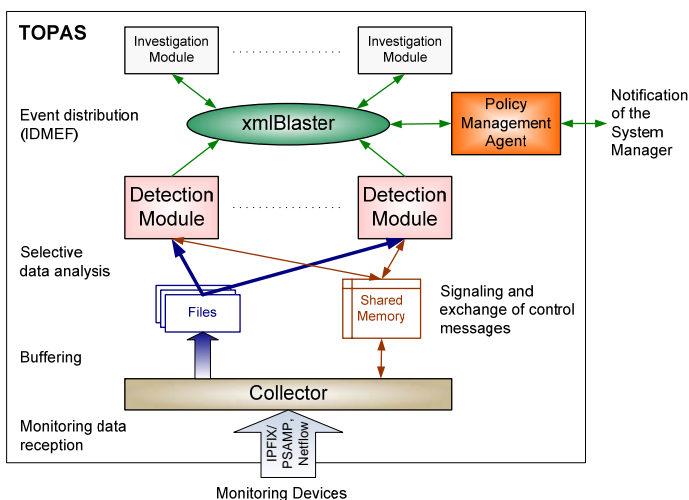
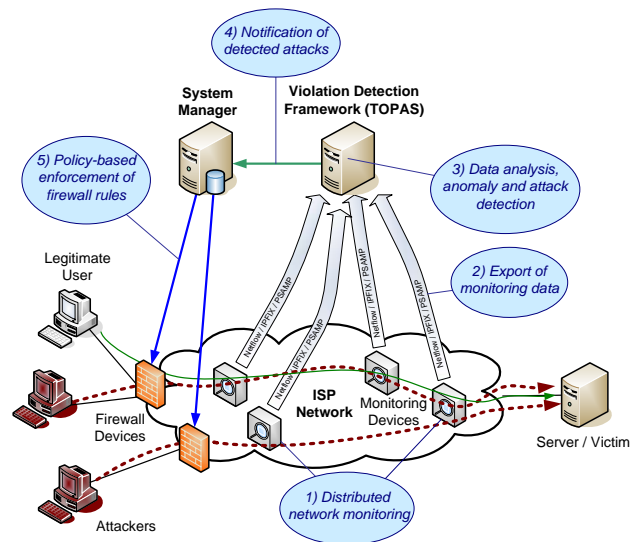
Gerhard Münz, Lothar Braun, Raimondas Sasnauskas,
Jan Petranek, Georg Carle



Computer Networks & Internet
University of Tuebingen

Violation Detection in Diadem Firewall

- ➔ Based on passive network monitoring
 - ▶ Distributed network monitors observe packets and flows
- ➔ Detection of traffic anomalies and (D)DoS attacks, e.g.:
 - ▶ Web server overloading attack
 - ▶ TCP SYN flood attack
- ➔ Identification of attack sources
 - ▶ Non-intrusive IP traceback
- ➔ Notification of detected attacks to trigger response actions



TOPAS = Traffic flow and Packet Analysis System

- ➔ Support of standard protocols for easy integration in existing and future networks
 - ▶ IPFIX protocol (IP Flow Information Export)
 - ▶ PSAMP protocol (Packet Sampling)
 - ▶ Cisco Netflow.v9
- ➔ Real-time processing of monitoring data
- ➔ Data analysis in multiple detection modules
 - ▶ Parallel deployment of different detection algorithms
- ➔ Event-based distribution and post-processing of detection results
 - ▶ XML encoded results using IDMEF
 - ▶ Result aggregation and correlation
- ➔ Record/replay of monitoring data
 - ▶ Easy debugging and testing of modules

Performance Evaluation

- ➔ Throughput tests on a dual-processor PC
- ➔ Packet sequence repeated at different rates:
 - ▶ 1 packet including an IPFIX template set
 - ▶ 28 packets including a set of 10 flow records
- ➔ Up to 77,000 records/sec @ 4 detection modules
 - ▶ Sufficient for medium size core networks
- ➔ Causes for packet losses:
 - (1) UDP socket buffer too small
 - (2) RAM disk too small or modules too slow
- ➔ Even better performance through optimized configuration

Number of active modules	3,000 pkts/sec	5,000 pkts/sec	8,000 pkts/sec	10,000 pkts/sec
1	no losses	no losses	no losses	losses (1)
2	no losses	no losses	no losses	losses (1)
4	no losses	no losses	no losses	losses (2)
5	no losses	losses (1)	losses (2)	losses (2)
8	losses (2)	losses (2)	losses (2)	losses (2)