Distributed Measurements for Attack Detection

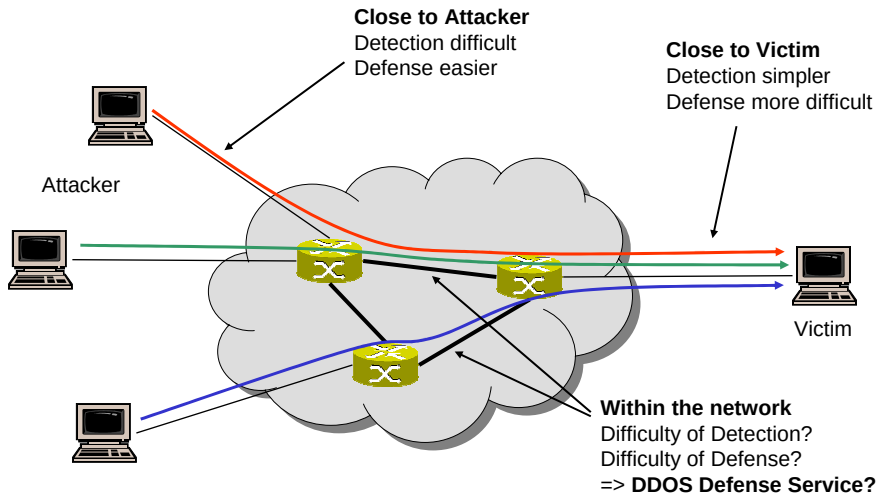
Prof. Dr. Georg Carle
Chair for Computer Networks and Internet
University of Tübingen
Germany
carle@informatik.uni-tuebingen.de
http://net.informatik.uni-tuebingen.de

joint work with Falko Dressler and Gerhard Münz in the context of the IST FP6 project DIADEM Firewall

Outline

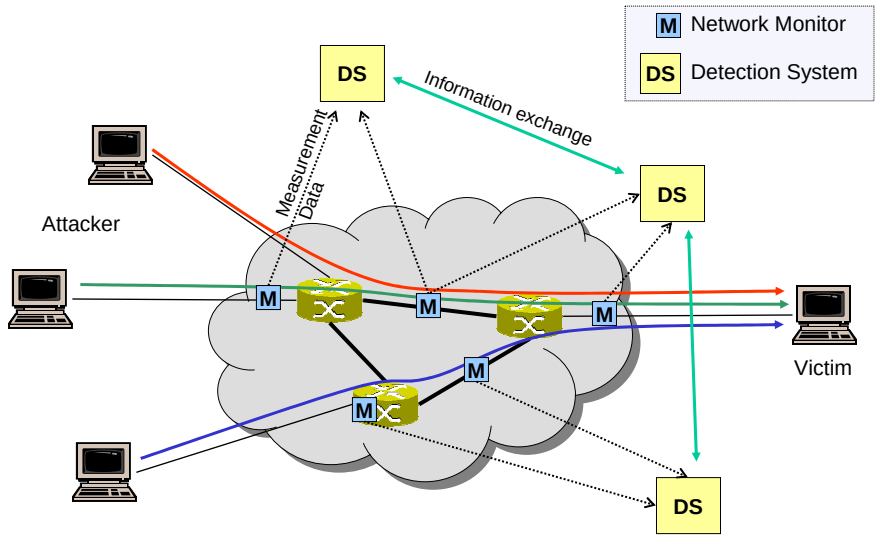
- Introduction
- DDoS Scenario
- Challenge of Attack Detection and Prevention
- Distributed Attack Detection and Defense
- Conclusions
- Future Work

DDoS Scenario – Location of Attack Detection and Defense



3

Distributed Attack Detection Scenario



4

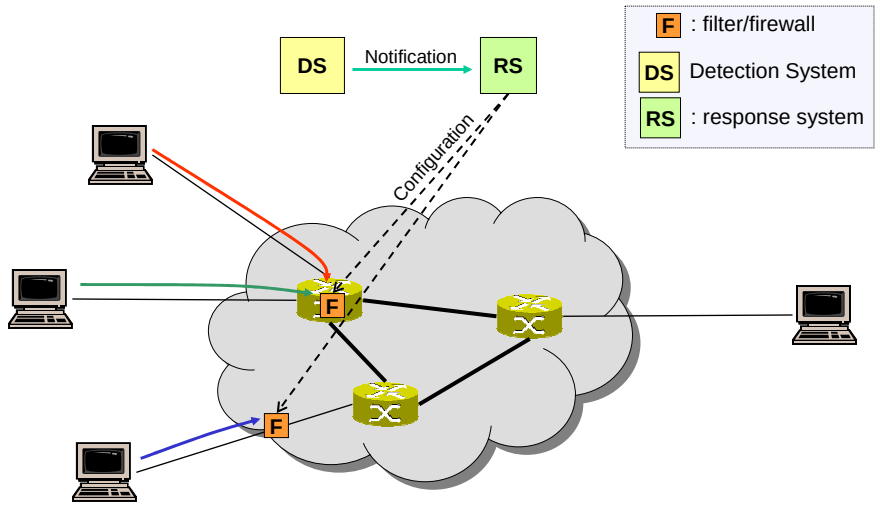
Attack Detection Methods

- **Knowledge-based Detection**
  - Search for known attack characteristics
    - Known packet sequences
    - known bit sequences in packets
    - known errors
  - Disadvantage: not suitable to detect new types of attacks

- **Anomaly detection**
  - Search for deviation from regular behaviour
    - Statistical tests
    - Data analysis (analysis of standard deviation, cluster analysis,...)
    - Pseudo tests (with unspecifiable error range)
    - Methods from pattern recognition (neural networks, Bayes networks,...)
  - Disadvantage: high probability of false positives, false negatives

5

Defense Initiation



6

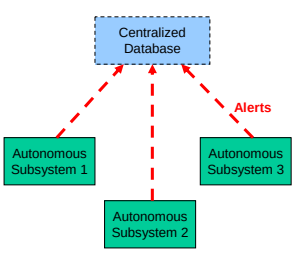
Challenge of Attack Detection

- **Characteristics of DDoS Attacks**
  - Synchonisation of senders ⇨ communication among attackers
  - Individual senders send traffic not identifiable as attack itself
  - Aggregation makes attack effective and detectable
  - Forged addresses, masquerade etc. make detection attackers difficult
- **Challenges**
  - Control traffic among attackers frequently remains undetected
  - Detection requires detecting aggregates
  - Similarity of legitimate traffic and attack traffic
  - Identifying attackers is difficult, requires trace-back - possibly across domains
  - Scalability to high speeds

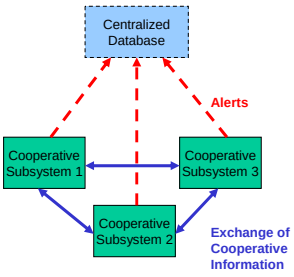
7

Taxonomy of Detection Systems

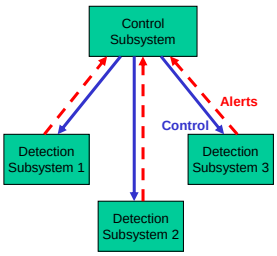
- 3 types of distributed detection systems:



(1) Distributed detection system with autonomous subsystems



(2) Distributed detection system with cooperative autonomous subsystems



(3) Distributed detection system with interdependent subsystems

8

Existing Distributed Attack Detection Systems

- EMERALD, Stanford Research Institute (SRI), 1997
  - Distributed detection and response system
  - Primarily conceived to detect host-based intrusions
  - Employs interdependent monitors on multiple hierarchical levels
- Prelude IDS, Open-source project, since 1998
  - Three functional components: sensors, managers, countermeasure agents
  - Supports various types of sensors (host-based and network-based)
- D-WARD, Peter Reiher/Jelena Mirkovic, UCLA, 2002
  - System of independent subsystems
  - Each subsystem controls traffic originating from a source-end network
- COSSACK, Christos Papadopoulos, ISI, 2003
  - Uses so-called watchdogs located at edge networks to detect and trace ongoing attacks

9

Overview of Distributed Detection Systems

System	Type of detection	Detection methods	Relationship between subsystems
EMERALD	host-based	knowledge-based + anomaly detection	interdependent
Prelude IDS	host-based and network-based	knowledge-based detection	interdependent
D-WARD	network-based	anomaly detection	autonomous
COSSACK	network-based	anomaly detection	cooperative
CATS	network-based	knowledge-based + anomaly detection	cooperative

10

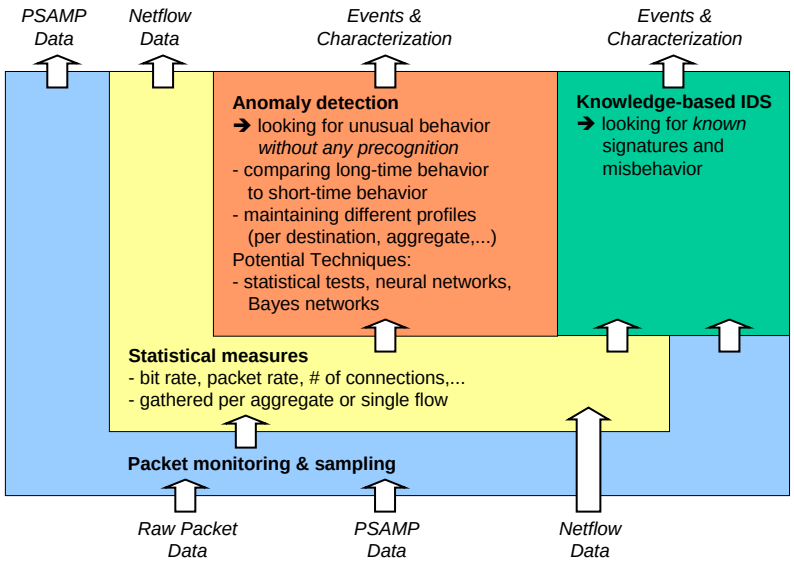
Cooperating Autonomous Detection Systems (CATS)

Concept and Benefits

- 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
  - Self-configuration
  - Self-maintainance
  - Self-optimisation
- 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

11

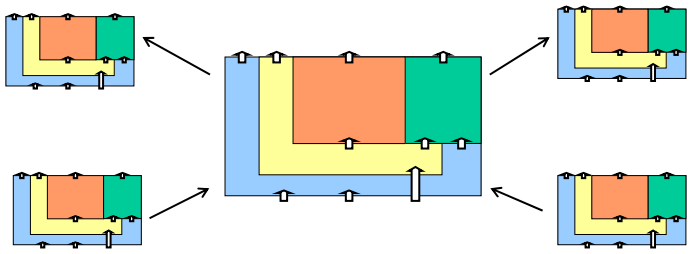
Monitor Architecture



12

Interactions of Autonomous Detection Systems

- Autonomous detection systems exchange two types of information in order to enable attack detection in global context:
  - Selected monitoring data (sampled packets and flow statistics)
  - Information about suspicious network traffic



13

Assessment

		EMER-ALD	Prelude IDS	D-WARD	COSS-ACK	CATS
Attack detection	Local context	yes	yes	yes	yes	yes
	Global context	no (host-based)	no	no	yes	yes
	Knowledge-based detection	yes	yes	no	no	yes
	Anomaly detection	yes	no	yes	yes	yes
Autonomous behavior		no	no	yes	yes	yes
Distributed intelligence	Sep. of monitoring & detection	no	no	no	no	yes
	Distributed detection	yes	partly	no	no	yes

14

Conclusions

- Attack detection and defense is an important application are that benefits from self-organisation
- Cooperating Autonomous Detection Systems (CATS) provides network-based attack detection based on the following main principles:
  - Distributed monitoring and detection
  - Cooperation between autonomous detection systems
- Benefits:
  - Scalability by adapting monitoring and detection to the current load
  - Increases detection performance by adding global context information to the detection process
  - Robustness due to self-X properties
- Next Steps
  - 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 competing systems