An Overview

Intrusion Detection System in wired LAN.

By Khurram Bhatti

Presented at CHASE-06 Lahore

Introduction.

- A defense system.
  - Ability to provide a view of unusual activity and issue alerts notifying administrators.
  - According to Amoroso [1], intrusion detection is „a process of identifying and responding to malicious activity targeted at computing and networking resources"

What is not an IDS?

- Network Logging systems.
- Vulnerability assessment tools.
- Anti-virus products.
- Firewalls.

Need for Intrusion Detection Systems.

- No bug free softwares.
- Cryptographic methods.
- Internal user abusing system.
- Reactive rather than pro-active agent

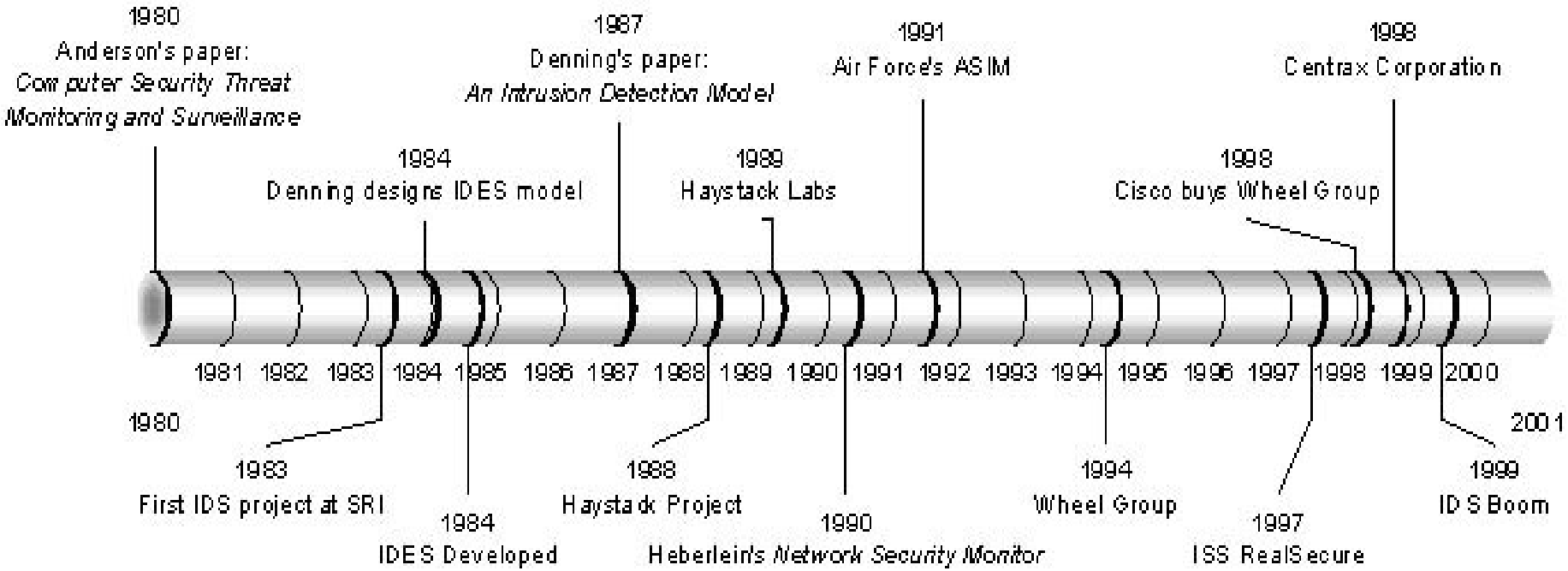
IDS statistics

- Over 90% running IDS detected breaches over prev year last 12 months.
- Only 0.1% companies spend budget on IDS.
- Mostly misunderstood, thought of as a firewall.

Origin

- Electronic Data Processing (EDP) auditing.
  - Construct events.
  - Assess damage.
  - Deter improper use.
- Anderson published paper
  - Risk taxonomy.
  - Audit reduction.
  - Base lined.
  - Pertinent details.
  - Profiling.

IDS Trend


1980
Anderson's paper:
Computer Security Threat Monitoring and Surveillance
1984
Denning designs IDES model
1987
Denning's paper:
An Intrusion Detection Model
1989
Haystack Labs
1991
Air Force's ASIM
1998
Cisco buys Wheel Group
1998
Centrax Corporation
1981 1982 1983 1984 1985 1986 1987 1988 1989 1990 1991 1992 1993 1994 1995 1996 1997 1998 1999 2000
1980
1983
First IDS project at SRI
1984
IDES Developed
1988
Haystack Project
1990
Heberlein's Network Security Monitor
1994
Wheel Group
1997
ISS RealSecure
1999
IDS Boom
2001

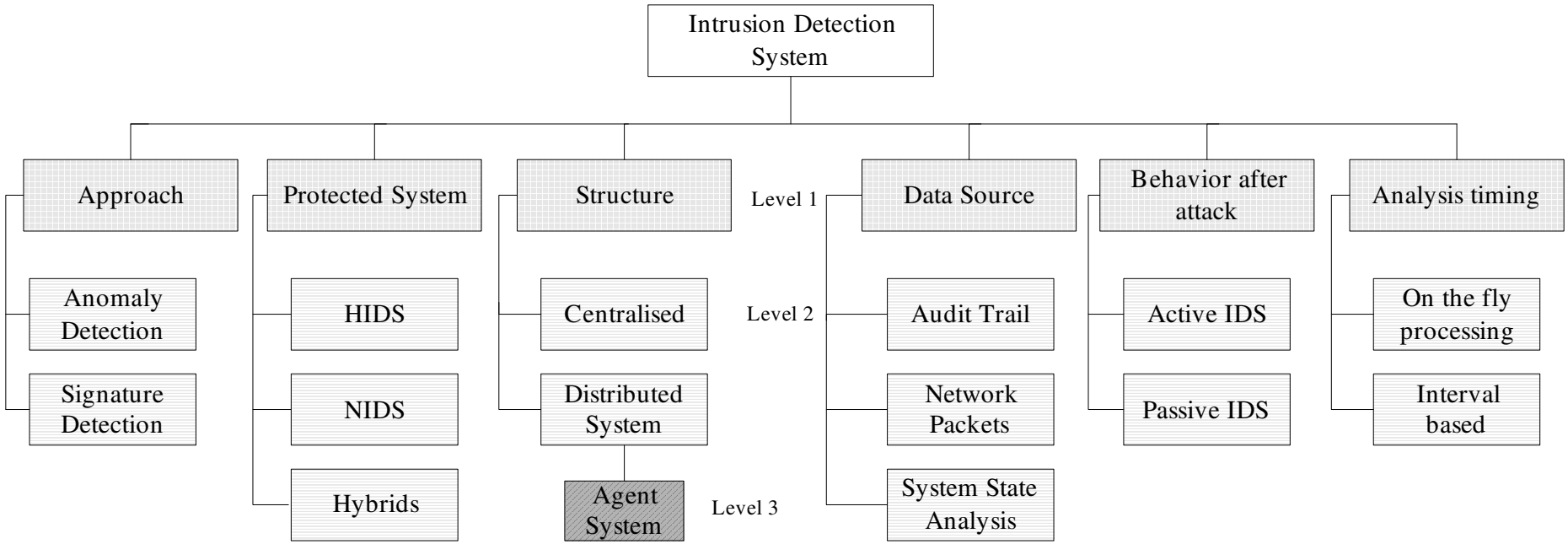
Basic definitions

- Attack
- Incident
- Intrusion
- Security
  - CIA
- Threat
- Signature
- Detection rules

Classification of Intrusions

- Attempted break-ins
- Denial of service
- Malicious use
- Leakage
- Masquerade

IDS decomposition Tree



Intrusion Detection Systems Classifications

- Information Sources
  - Target
  - Hosts
  - Network
  - Application
- Architecture
  - Host-based
    - Monitor activities on host
    - Host-based IDS use an agent-console model -- Agent based.
    - Data collection occurs per-host basis.
    - Attacker who compromise a host can also attack and disable host-based IDS.

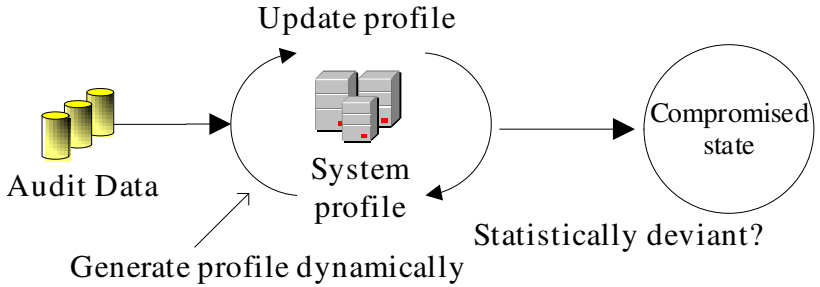
Intrusion Detection Systems Classifications (Cont…)

- Network-based
  - Monitor entire network
  - Passive devices
  - Secure against attack undetectable
  - Large network traffic overlooked.
  - Can't analyze encrypted data.
  - Requires manual involvement.
- Network-node

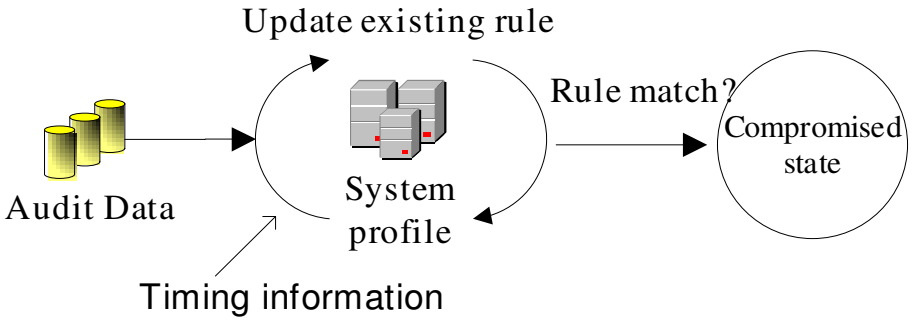
- Type of analysis
  - Misuse
  - Anomaly

Intrusion Detection Systems Classifications (Cont…)

- Timing
  - Real time
  - Given Interval

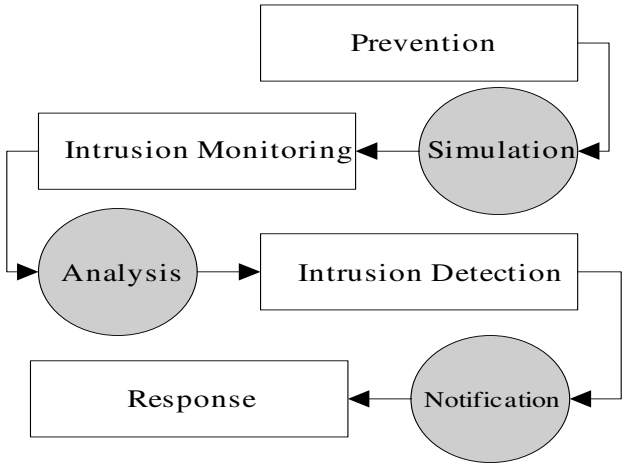


Anomaly based technique

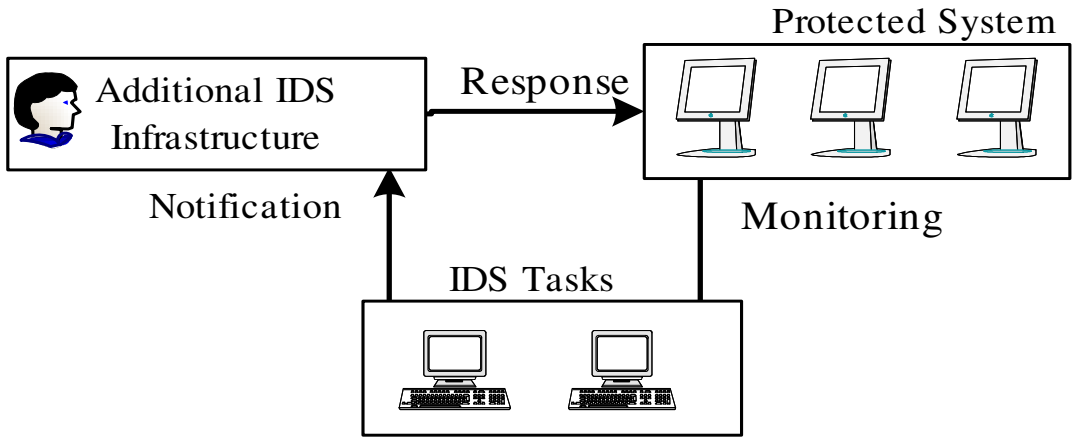


Misuse based technique

Intrusion detection system tasks



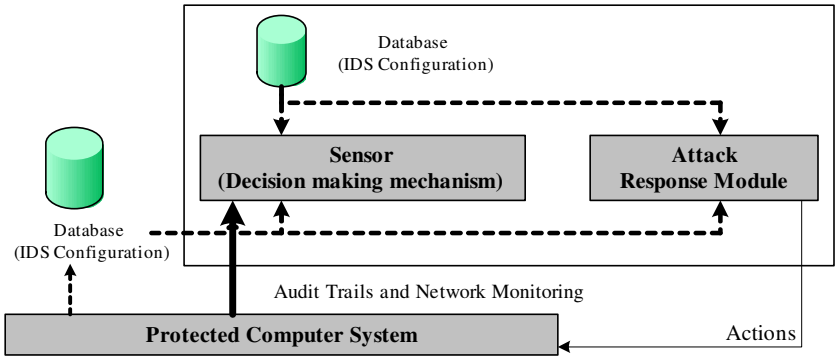
Intrusion detection system Tasks



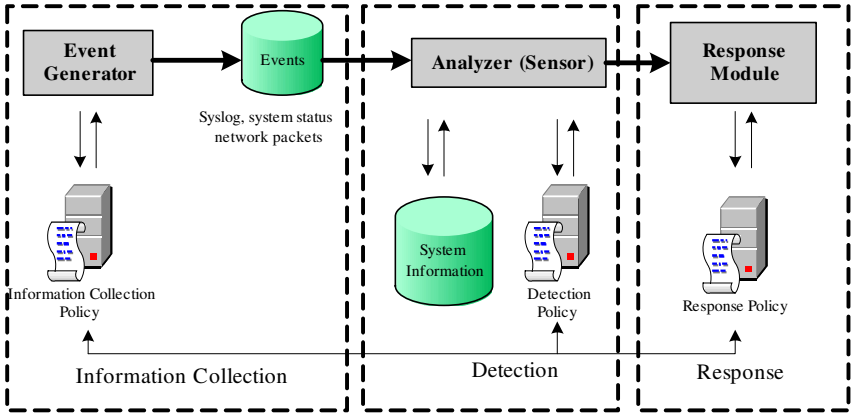
IDS infrastructure

IDS Architecture

- Sensor
- Event Generator
- Analyzer



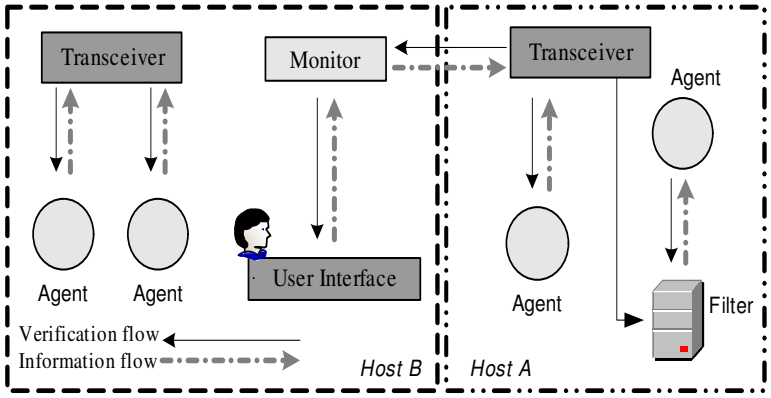
Structure & Architecture of IDS



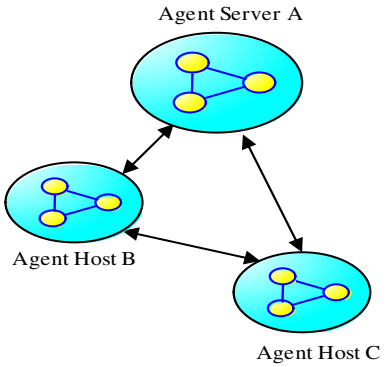
Major components of IDS

IDS structure

- Centralized
- Distributed
  - Agent based



Intrusion detection system employing autonomous agents



Mobile Agents model

Conclusion.

References