Intrusion Detection Systems

Taxonomy and Survey

Papers

- Intrusion Detection Systems: A survey and Taxonomy.
- Research in Intrusion Detection Systems: A Survey

  – Stefan Axelsson

IDS - Introduction

- Detecting inappropriate, incorrect or anomalous activities.
- Host-based, Network based.
- Host-Based: Monitoring activities in the host.
- Network –Based: Monitor network activities.
- “Burglar alarms”: Site Security Officer (SSO) responds to the alarm.

IDS - Components

- Audit agent, detector proper, SSO
- Audit Agent: Collects data from the observed entity.
- Detector proper: Processes the collected data.
- SSO : Gets input (alarm) from Detector Proper and decides on further investigation/Action.

IDS - Taxonomy

- Detector Proper : Central to IDS.
- Intrusion Detection Principles: Intrusion detector, Intrusion that needs to be detected and the environment in which the intrusion is detected.
- How to formalize intrusion detection decision.
- Current Research systems are classified based on their implementation mechanisms but not on the detection principles.

IDS - Anomaly/Signature/Compound

Intrusion Detection decision is based on:

- Anomaly detection:
  - Abnormalities of traffic in question.
  - “abnormal” is probably suspicious.
- Signature detection:
  - Knowledge of intrusions and its traces.
- Compound detection:
  - Hybrid of anomaly and signature.

IDS - Anomaly Detection

- Detection principle is based on:

- What is normal for the subject under observation?

- On what percentage of activity to flag abnormal?

- How to make this particular decision?

- Anomaly Detection is further classified:

- Self-Learning

- Programmed.

IDS - Anomaly Detection Self Learning systems

Learns from Examples of “normal” behavior

- Rule Modelling: Studies normal traffic and formulates “rules”.

  Applies the rules and raises alarm if there is deviation.
- Descriptive Statistics: Creates a profile of statistics of different system parameters. Constructs a distance vector of the observed traffic to the profile and alarm is raised if the deviation is more.

IDS - Anomaly Detection Self Learning systems

- ANN (Artificial Neural Network) based:

  The system’s normal traffic is fed in to an ANN and it subsequently learns the pattern.

  After this “training” phase, new traffic is fed and intrusion detection decisions are taken.

IDS - Anomaly Detection Programmed systems

- Some one has to teach the system to detect anomalies.
- User has to determine what behavior is abnormal that should result in signaling security violation.
- Further divided in to:

- Descriptive Statistics.
- Default Deny.

IDS - Programmed systems Descriptive statistics

- Descriptive Statistics:

  Profile of normal behavior built from descriptive statistics on number of system parameters.

- Simple statistics: higher level components use simple stats to arrive at more abstract intrusion detection decisions.

- Simple Rule Based: User provides rules to apply on the collected statistics.

- Threshold: When the system has collected necessary statistics, the user can program predefined thresholds to determine whether to raise alarm or not.

IDS - Programmed systems Default Deny

- Default Deny: Explicitly state the circumstances under which the system operates in a secure-benign manner, and to flag all deviations from this as intrusive.
- Based on security policies.

- State Series Modelling: Policy is encoded as a set of states.

IDS - Signature Detection

- Decision based on the model of intrusion and its traces.
- Detecting intrusive behavior without idea of the normal behavior or background traffic of the system.
- Looks for patterns that are suspicious.

IDS - Signature Detection Programmed systems

- Programmed systems: Idea is to determine explicitly the traces of intrusion.

Types:

1. State-Modelling:

- The intrusion is encoded as states.
- The states form a simple chain and all that states must be traversed for the intrusion to be considered as taken place.
- The states can form a petrinet with a general tree structure.

IDS - Signature Detection Programmed systems

2. Expert-System: Reason about the security state of the system based on rules that describe an intrusive behavior.
3. String-matching: Searching malicious substrings within a long string (audit data).
4. Simple-rule based: Less complex expert systems with faster execution.

IDS – Compound Detectors.

- Hybrid of Anomaly and signature based detection techniques.
- Decision is made based on both the normal behavior of the system and the intrusive behavior of the intruder.
- Signature Inspired.
- Most advanced!
- Mostly self learning: The system learns the normal and intrusive behaviors during the training phase.

IDS - Categories: Type of Intrusions

- Well Known: Intrusions that are well known and a ‘static’, well defined pattern can be found. Detected by Signature based IDS systems.
- Generalisable: similar to well-Known with slight variations. Detected by compound systems based on self learning. (RIPPER)
- Unknown: IDS does not know what to expect. Anomaly detection based IDS may detect.

IDS - Taxonomy: system characteristics

- Taxonomy based on the approach employed by Intrusion detection systems on the audit data.

1. Time of Detection. (real time, non real-time)
2. Granularity of audit data processing.
3. Source of audit data (network or host).
4. Response to detected intrusions. (Passive vs. Active)

   (Active Systems : may exercise control on the attacked or attacking system or both)

IDS - Taxonomy: system characteristics

5. Locus of data processing. (central or distributed)
6. Locus of data-collection. (Central or distributed)
7. Security: IDS security.
8. Interoperability.

Paper categorizes the surveyed ID systems in the above categories also.

IDS - Trends

- Present research on IDS tend more towards:
- IDS with “Active” type of response.
- From centralized to Distributed IDS.
- Security of IDS. (Resistant to attack on IDS itself)
- From host to network. (Problem with encrypted data)

IDS: Open Research Questions

- Research done till date fails to answer:

1. Nature of intrusions that the system is trusted to detect.
2. To what degree the IDS classify intrusions? Can it be trusted to respond “actively” to them?
3. What audit data to collect and how to collect, store, prune and transmit effectively?
4. Have we found all possible types of intrusions?
5. Run-time efficiency.

IDS - MIDAS

- First Signature based detection IDS.
- Has a “rules” database.
- Introduction of a new rule triggers reevaluation of existing rules and this in turn will introduce additional new rules.
- Rule database is populated with rules from different categories (User anomaly, immediate attack, system state).

IDS - IDES

- Anomaly based intrusion detection.
- Motivation is “users behave in a consistent manner”
- IDES monitors various parameters for the user behavior (CPU usage, Command usage, Network activity etc) and builds detection rules.