IDS/IPS Definition and Classification

Contents

- Overview of IDS/IPS
- Components of an IDS/IPS
- IDS/IPS classification
  - *By scope of protection*
  - *By detection model*

Overview of IDS/IPS

- Intrusion
  - A set of actions aimed at compromising the security goals (confidentiality, integrity, availability of a computing/networking resource)
- Intrusion detection
  - The process of identifying intrusion activities
- Intrusion prevention
  - The process of both detecting intrusion activities and managing responsive actions throughout the network.

Overview of IDS/IPS

- Intrusion detection system (IDS)
  - A system that performs automatically the process of intrusion detection.
- Intrusion prevention system (IPS)
  - A system that has an ambition to both detect intrusions and manage responsive actions.
  - Technically, an IPS contains an IDS and combines it with preventive measures (firewall, antivirus, vulnerability assessment) that are often implemented in hardware.

Overview of IDS/IPS

- Some authors consider an IPS a new (fourth) generation IDS – a convergence of firewall and IDS.
- IPS use IDS algorithms to monitor and block/allow traffic based on expert analysis.
- The ”firewall” part of an IPS can prevent malicious traffic from entering/exiting the network. It can also alert the operator about such activities.

Overview of IDS/IPS

- A complete IPS solution usually has the capability of enforcing traditional static firewall rules and operator-defined white - lists and blacklists.
- IPS are very resource intensive. In order to operate with high performance, they should be implemented by means of the best hardware and software technologies.
- IPS hardware often includes ASICs (Application Specific Integrated Circuits)

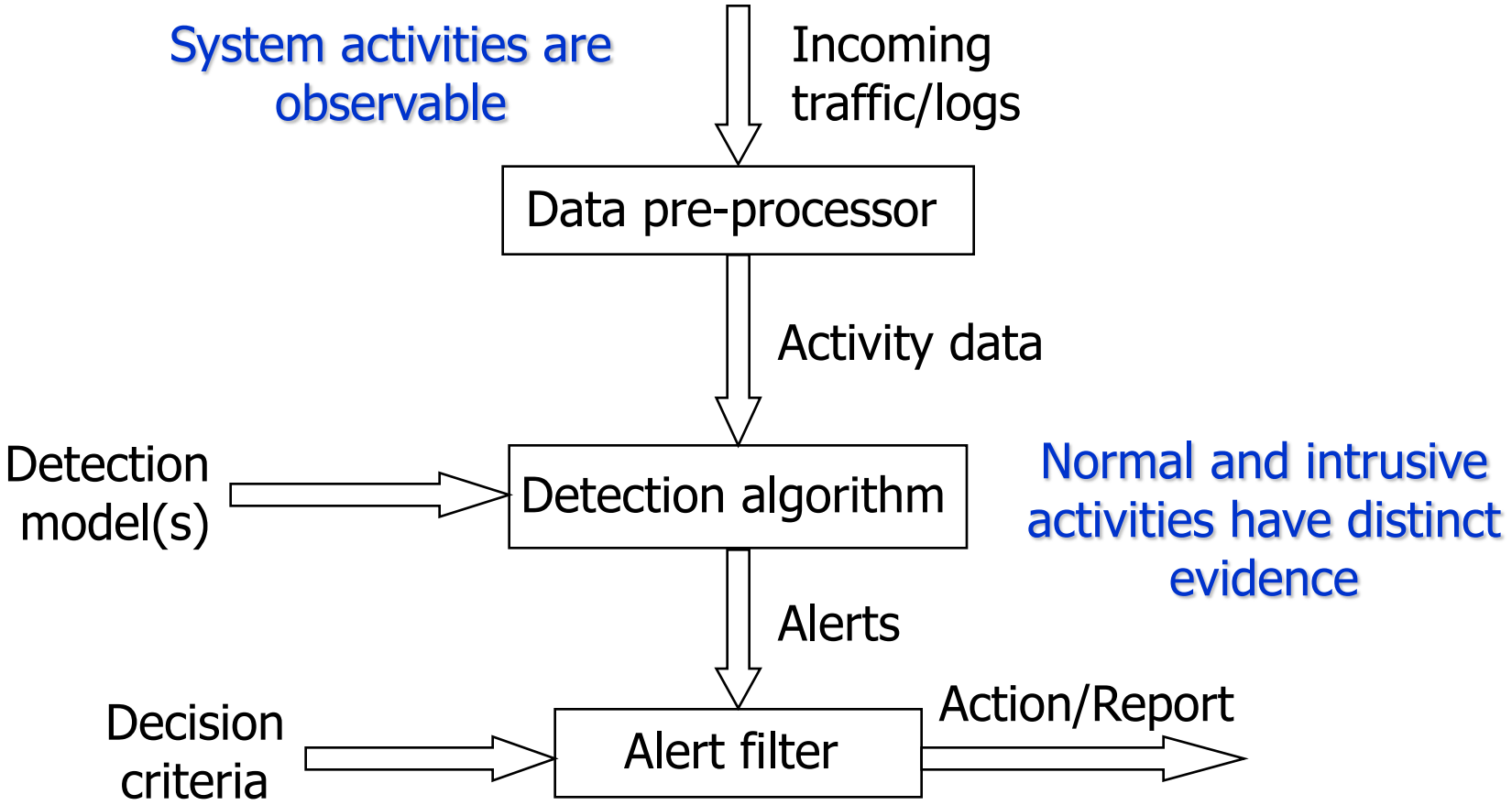
Overview of IDS/IPS

- Principal differences between IDS and IPS:
  - IPS try to block malicious traffic, unlike IDS that just alert personnel to its presence.
  - IPS acts to combine single-point security solutions (anti-virus, anti-spam, firewall, IDS, …).

Overview of IDS/IPS

- Basic assumptions:
  - System activities are observable
  - Normal and intrusive activities have distinct evidence – the goal of an IDS/IPS is to detect the difference.

Components of an IDS/IPS



Components of an IDS/IPS

- Data pre-processor
  - Collects and formats the data to be analyzed by the detection algorithm.
- Detection algorithm
  - Based on the detection model, detects the difference between ”normal” and intrusive audit records.
- Alert filter
  - Based on the decision criteria and the detected intrusive activities, estimates their severity and alerts the operator/manages responsive activities (usually blocking).

Components of an IDS/IPS

- Incoming traffic/log data
  - Packets – headers contain routing information, content may (and is more and more) also be important for detecting intrusions.
  - Logs – a chronological set of records of system activity.

Components of an IDS/IPS

- Incoming traffic/log data (cont.)
  - Problems related to data
    - Inadequate format for intrusion detection
    - Information important for intrusion detection is often missing (e.g. in log files).
  - Thus we need some data pre-processing
    - Adjust data format (relatively easy)
    - Resolve for missing data (not so easy)
      - Insertion of reconstructed values
      - Special distances (for unequal-length data patterns).

Components of an IDS/IPS

- Detection algorithm
  - Checks the incoming data for presence of anomalous content.
  - A major detection problem
    - There is no sharp limit between “normal” and “intrusive” – it often depends on the context – hence statistical analysis of the input data may be useful.
    - To determine the context, a lot of memory is needed.

Components of an IDS/IPS

- Alert filter
  - Determines the severity of the detected intrusive activity.
  - A major decision problem
    - It is difficult to estimate the severity of threat in real time.
    - Filtering is normally carried out by means of a set of thresholds (decision criteria). Thresholds should be carefully set in order to maintain a high level of security and a high level of system performance at the same time.

IDS/IPS classification

- By scope of protection (or by location)
  - Host-based IDS
  - Network-based IDS
  - Application-based IDS
  - Target-based IDS
- By detection model
  - Misuse detection
  - Anomaly detection

IDS classification

- Host-based
  - Collect data from sources internal to a computer, usually at the operating system level (various logs etc.)
  - Monitor user activities.
  - Monitor executions of system programs.

IDS classification

- Network-based
  - Collect network packets. This is usually done by using network devices that are set to the promiscuous mode. (A network device operating in the promiscuous mode captures all network traffic accessible to it, not just that addressed to it.)
  - Have sensors deployed at strategic locations
  - Inspect network traffic
  - Monitor user activities on the network.

IDS classification

- Application-based
  - Collect data from running applications.
  - The data sources include application event logs and other data stores internal to the application.

IDS classification

- Target-based (integrity verification)
  - Generate their own data (by adding code to the executable, for example).
  - Use checksums or cryptographic hash functions to detect alterations to system objects and then compare these alterations to a policy.
  - Trace calls to other programs from within the monitored application.

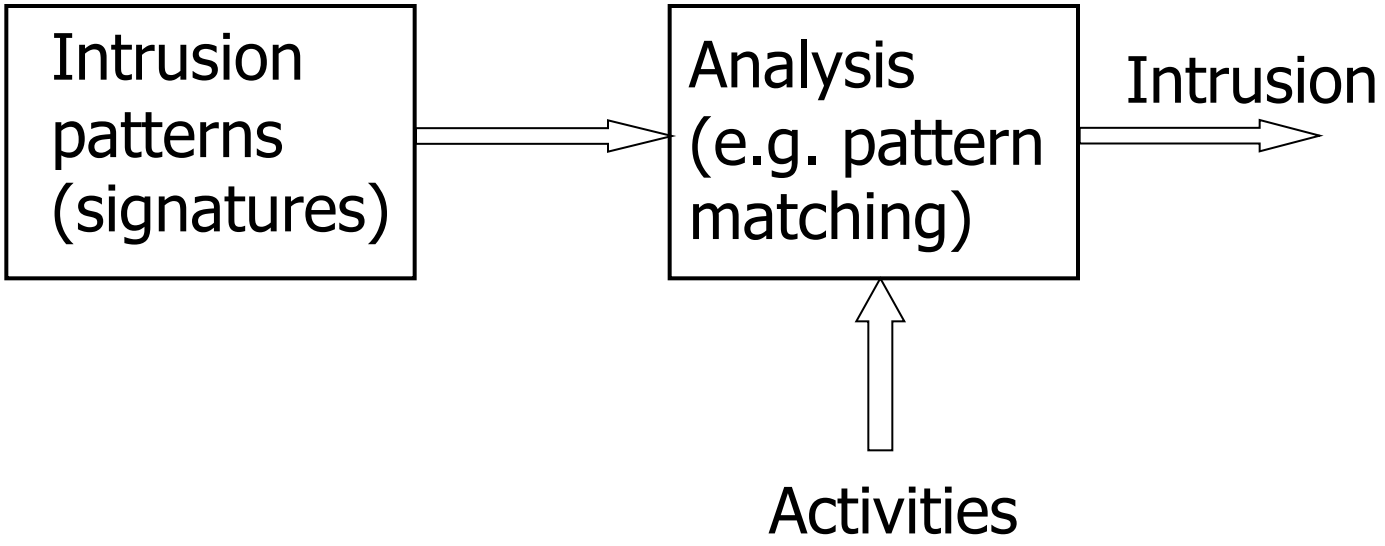
IDS classification

- Misuse detection
  - Asks the following question about system events: Is this particular activity bad?
  - Misuse detection involves gathering information about indicators of intrusion in a database and then determining whether such indicators can be found in incoming data.

IDS classification

- Misuse detection (cont.)
  - To perform misuse detection, the following is needed:
    - A good understanding of what constitutes a misuse behaviour (intrusion patterns, or signatures).
    - A reliable record of user activity.
    - A reliable technique for analyzing that record of activity (very often – pattern matching).

Misuse Detection



Signature example: **if** src_ip = dst_ip **then** "land attack"

IDS classification

- Misuse detection (cont.)
  - It is best suited for reliably detecting known misuse patterns (by means of signatures).
  - It is not possible to detect previously unknown attacks, or attacks with unknown signature. A single bit of difference may be enough for an IDS to miss the attack.
  - However, it is possible to use the existing knowledge (for instance, of outcomes of attacks) to recognize new forms of old attacks.

IDS classification

- Misuse detection (cont.)
  - Misuse detection has no knowledge about the intention of activity that matches a signature.
  - Hence it sometimes generates alerts even if the activities are normal (normal activities often closely resemble the suspicious ones).
  - Hence IDS that use signature detection are likely to generate *false positives*.

IDS classification

- Misuse detection (cont.)
  - New attacks require new signatures, and the increasing number of vulnerabilities causes that signature databases grow over time.
  - Every packet must be compared to each signature for the IDS to detect intrusions. This can become computationally expensive as the amount of bandwidth increases.

IDS classification

- Misuse detection (cont.)
  - When the amount of bandwidth overwhelms the capabilities of the IDS, it causes the IDS to miss or drop packets.
  - In this situation, *false negatives* are possible.

IDS classification

- Anomaly detection
  - Anomaly detection involves a process of establishing profiles of normal user behaviour, comparing actual user behaviour to those profiles, and alerting if deviations from the normal behaviour are detected.
  - The basis of anomaly detection is the assertion that abnormal behaviour patterns indicate intrusion.

IDS classification

- Anomaly detection (cont.)
  - Profiles are defined as sets of metrics - measures of particular aspects of user behaviour.
  - Each metric is associated with a threshold or a range of values.

IDS classification

- Anomaly detection (cont.)
  - Anomaly detection depends on an assumption that users exhibit predictable, consistent patterns of system usage.
  - The approach also accommodates adaptations to changes in user behaviour over time.

IDS classification

- Anomaly detection (cont.)
  - The completeness of anomaly detection depends on the selected set of metrics – it should be rich enough to express as much of anomalous behaviour as possible.
  - Capable of detecting new attacks.

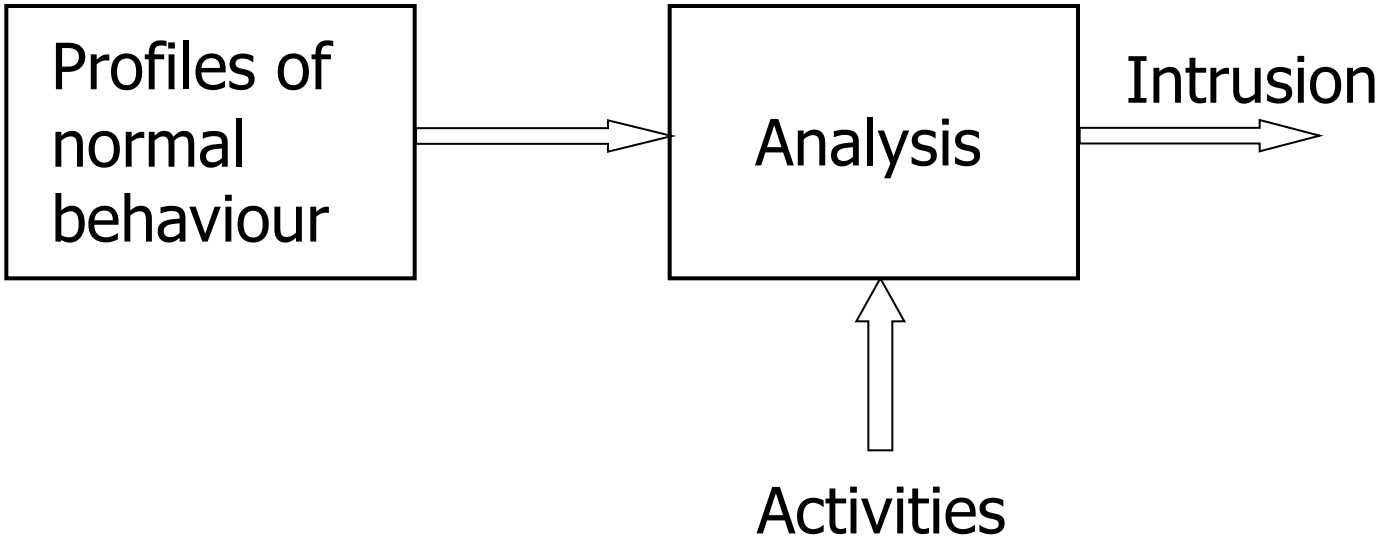
IDS classification

- Anomaly detection (cont.)
  - An attacker can replicate a misuse detection system and check which signatures it detects.
  - Then he/she can use the attack not detectable by the IDS in question.
  - This is not possible to do with an anomaly detection system.

IDS classification

- Anomaly detection (cont.)
  - However, it is not always the case that abnormal behaviour patterns indicate an intrusion – sometimes, rare sequences represent normal behaviour. This is a major problem in anomaly detection – *false positives*.
  - If anomaly detection IDS thresholds are set too high, we may miss the attacks and have *false negatives*.

Anomaly Detection

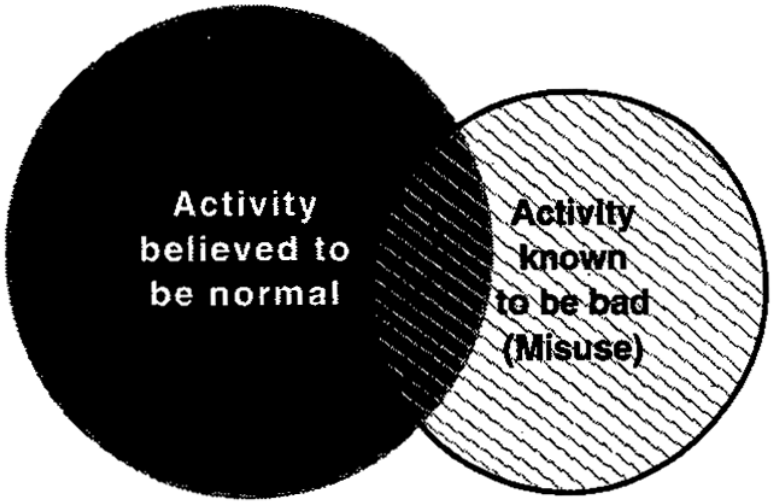


IDS classification

- Anomaly detection (cont.)
  - Methods of anomaly detection:
    - Statistical methods
    - Artificial intelligence (cognitive science,…)
    - Data mining
    - Mathematical abstractions of biological systems (neural nets, immunological system simulation, process homeostasis…)
    - Etc.

IDS classification

- The fundamental debate between proponents of anomaly detection and proponents of misuse detection:
  - Overlap of the regions representing "normal," and "misuse “ activities.



IDS classification

- The proponents of anomaly detection assert that the intersection between the two regions is minimal.
- The proponents of misuse detection assert that the intersection is quite large, to the point that given the difficulties in characterizing "normal” activity, it is pointless to use anomaly detection.

IDS classification

- The solution of this problem is probably in combining the two detection models.
- Although the IDS/IPS manufacturers do not publish the details of their designs, it is quite probable that they combine misuse detection and anomaly detection approach in their solutions.