International Working Group
on Data Protection
in Telecommunications

Working Paper on Intrusion Detection systems (IDS)

- adopted at the 34th meeting, 2-3 September 2003, Berlin -

What is an IDS ?

Intrusion detection is the process of detecting unauthorized use of systems and networks through the use of specialized software and/or hardware.

An IDS provides the ability to view network and system activity in real time, identify unauthorized activity and provide a nearly real-time automated response. IDS products also provide the ability to analyze today's activity in view of yesterday's activity to identify larger trends and problems.

Purpose and Benefits of IDS

The primary purpose of performing intrusion detection is to help to prevent the consequences caused by intrusions if undetected. Implementing a program of effective security controls is an effective starting point for establishing the supporting security infrastructure. Being able to detect an intrusion attempt or its preparation in real time is an important aspect of intrusion detection. Knowing when an attack is in progress and being able to take immediate action significantly improves the odds of successfully terminating intrusions and tracing intrusion attempts to their source. Real time detection depends upon having a watchdog system that sits in the background and monitors all activities involving the connected devices. The monitoring system must be able to interpret various incidents and diagnose actual attacks.

Most traditional IDS take either a network or a host-based approach to identifying and protecting against attacks[1]. In either case, IDS look for attack signatures, specific patterns that ordinarily indicate malicious intent or suspicious activity. A truly effective IDS will employ both methods.

[1] See technical annex for details

Secretariat
Berliner Beauftragter für
Datenschutz und Informationsfreiheit
An der Urania 4-10
D-10787 Berlin
Phone +49 / 30 / 13889-0
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.datenschutz-berlin.de

Privacy concerns

IDS gathering and logging lot of traffic or event data containing certainly some personal data, the privacy concerns seem to be evident.

In this context, the Working Group deems it necessary to draw the attention of all the actors responsible in the implementation of the IDS about the following issues:

Recognizing or deflecting intrusions requires the analysis of network traffic and/or audit trails of operating systems while looking for attack signatures or specific patterns that usually indicate malicious or suspicious intent.

Collected network traffic or event data may contain some personal data, i.e., data that can be related to a specific person. The hardware or IP-address may be one example of such a datum. Thus, intrusion detection could be used as an instrument for monitoring users and their behavior. If intrusion detection is to be applied for detecting “internal” intruders, i.e., organizational employees, one must consider the implications.

Three principles that reflect the privacy challenges should be addressed if intrusion detection is employed:

?? intrusion detection has to serve the purpose of data or system protection,

?? the data collection (network packets, audit logs) has to be adequate to the purpose of protection,

?? a policy covering requirements to protect the privacy of personal information collected in IDS should be developed and applied.

As to the first aspect, it questions the conditions of compatibility of supervision of the behaviour of users/employees with intrusion detection objectives.

The second aspect points out that only those data should be gathered and analyzed which are necessary to recognize attacks. After the comparison of event data with the attack signatures of the IDS, data that is no longer needed or with which there has been no indication of an attack should be deleted; the relevant data, which indicate an attack, should be stored in a secure way. However, deleting the data may not be adequate in some instances; event data may need to be archived for later inspection, e.g., for purposes of traceability to the attacker or for forensic analysis at a later date. Some data may at first appear to be benign. After further analysis it may prove to be related to an attack. Correlation with data collected later may also prove it to be related to an attack. In any event and for different reasons including privacy, the data should be strongly protected from unlawfull access. The actions taken should be consistent with the security policy of the organization.

The third point means that the privacy of personal information needs to be protected and managed in accordance with an organizations overall privacy policy and/or any laws that may apply to sensitive personal information.

At the moment there are very few special legal and regulatory requirements associated with intrusion detection. Laws or regulations are expected to emerge that provide for adequate privacy protection for individuals while at the same time allowing IDS and associated event logs to collect and use sufficient data to identify potentially damaging intrusions. Already some national regulations contain the criteria of adequacy and the related purpose of the use of personal data. Some nations have regulations concerning the protection of workers’ personal data and the right of workers’ participation in the privacy of their personal data. In addition, various national regulations and treaties regarding transborder data flow may impact on intrusion detection and privacy.

Some national legislation and regulation requires that if monitoring of the activities of people is to take place, e.g., through event logs and IDS-specific sensors/monitoring agents, then the employees and contractors concerned must be specifically informed of, and acknowledge this before operations commence. This could be in the form of signed contractual terms of employment or a particular paper or any other way in accordance with the national legislation.

The essentials of these considerations addressing privacy issues have already been formulated by some data protection authorities[2] and notably integrated in the draft revised text of the following project of standard .

?? ISO/IEC WD 18043, 'Guidelines for the implementation, operation and management of intrusion detection systems (IDS)'

Considering the present developments in the standardisation context, the Working Group fully supports the integration of the above considerations in all international, regional and national standards affecting the above mentioned privacy issues .

[2] The Belgian Data protection Authority has been specially active with this regard.

Technical annex

The principal types of IDS

Host-based IDS

Host-based intrusion detection started in the early 1980s before networks were as prevalent, complex and interconnected as they are today. In this simpler environment, it was common practice to review audit trail logs for suspicious activity
Host-based IDS still use audit trail logs, but they are much more automated, having evolved to include more sophisticated and responsive detection techniques. Host-based IDS typically monitor systems, events and security logs on. When any of these files change, the IDS compares the new log with attack signatures to determine if there are any matches. If so, the system responds with administrator alerts and other calls to action. It monitors files on systems for changes. The primary host-based IDS purpose is to monitor systems for individual file changes.

Host-based IDS have expanded to include other technologies. One popular method of detecting intrusions checks key system files and executables via checksums at regular intervals for unexpected changes. The timeliness of response is directly related to the frequency of the polling interval. Finally, some products monitor port activity and alert administrators when specific ports are accessed. This type of detection brings an elementary level of network-based intrusion detection into the host-based environment.

Network based IDS

Network-based IDS use raw network packets as the data source.

Network-based IDS typically utilize network adapters running in promiscuous mode to monitor and analyze network traffic in real time. Promiscuous mode makes it extremely difficult for an attacker to detect and locate.

Attack recognition functionality uses three common techniques to recognize an attack signature :

?? Statistical anomaly detection

In the anomaly detection model the IDS detects intrusions by looking for activity that is different from a user's or system's normal behavior. Anomaly-based IDS establish baselines of normal behavior by profiling particular users or network connections and then monitoring for activities which deviate from the baseline.

?? Pattern, expression or byte code matching

The majority of commercial products are based upon examining traffic looking for documented patterns of attack. This means that the IDS is programmed to identify each known exploit technique. This can be as simple as a pattern match. The classic example is to examine every pattern on the network segment for a defined pattern of activity that indicates an attempt to access a vulnerable script on a web server. Some IDS are built from large databases that contain thousands of such patterns. The IDS monitors every packet, looking for packets that contain one of these defined patterns.

?? Correlation of lesser events