INTERNATIONAL STANDARD

ISO/IEC 18043

First edition
2006-06-15

Information technology — Security techniques — Selection, deployment and operations of intrusion detection systems

Technologies de /'information — Techniques de securite — Selection, deploiement et operations des systemes de detection d'intrusion

Reference number
ISO/IEC 18043:2006(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. +41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 18043 was prepared by Joint Technical Committee ISO/IEC JTC 1 *Information technology,* Subcommittee SC 27, *IT Security techniques.*

Legal notice

The National Institute of Standards and Technology (NIST), hereby grant non-exclusive license to ISO/IEC to use the NIST Special Publication on Intrusion Detection Systems (SP800-31) in the development of the ISO/IEC 18043 International Standard. However, the NIST retains the right to use, copy, distribute, or modify the SP800-31 as they see fit.

Introduction

Organizations should not only know when, if, and how an intrusion of their network, system or application occurs, they also should know what vulnerability was exploited and what safeguards or appropriate risk treatment options (i.e. risk transfer, risk acceptance, risk avoidance) should be implemented to prevent similar intrusions in the future. Organizations should also recognize and deflect cyber-based intrusions. This requires an analysis of host and network traffic and/or audit trails for attack signatures or specific patterns that usually indicate malicious or suspicious intent. In the mid-1990s, organizations began to use Intrusion Detection Systems (IDS) to fulfil these needs. The general use of IDS continues to expand with a wider range of IDS products being made available to satisfy an increasing level of organizational demands for advanced intrusion detection capability.

In order for an organization to derive the maximum benefits from IDS, the process of IDS selection, deployment, and operations should be carefully planned and implemented by properly trained and experienced personnel. In the case where this process is achieved, then IDS products can assist an organization in obtaining intrusion information and can serve as an important security device within the overall information and communications technology (ICT) infrastructure.

This International Standard provides guidelines for effective IDS selection, deployment and operation, as well as fundamental knowledge about IDS. It is also applicable to those organizations that are considering outsourcing their intrusion detection capabilities. Information about outsourcing service level agreements can be found in the IT Service Management (ITSM) processes based on ISO/IEC 20000.

Information technology — Security techniques — Selection, deployment and operations of intrusion detection systems

1 Scope

This International Standard provides guidelines to assist organizations in preparing to deploy Intrusion Detection System (IDS). In particular, it addresses the selection, deployment and operations of IDS. It also provides background information from which these guidelines are derived.

This International Standard is intended to be helpful to

a) an organization in satisfying the following requirements of ISO/IEC 27001:

- The organization shall implement procedures and other controls capable of enabling prompt detection of and response to security incidents.
- The organization shall execute monitoring and review procedures and other controls to properly identify attempted and successful security breaches and incidents.

b) an organization in implementing controls that meet the following security objectives of ISO/IEC 17799:

- To detect unauthorized information processing activities.
- Systems should be monitored and information security events should be recorded. Operator logs and fault logging should be used to ensure information system problems are identified.
- An organization should comply with all relevant legal requirements applicable to its monitoring and logging activities.
- System monitoring should be used to check the effectiveness of controls adopted and to verify conformity to an access policy model.

An organization should recognize that deploying IDS is not a sole and/or exhaustive solution to satisfy or meet the above-cited requirements. Furthermore, this International Standard is not intended as criteria for any kind of conformity assessments, e.g., Information Security Management System (ISMS) certification, IDS services or products certification.

2 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

2.1
attack
attempts to destroy, expose, alter, or disable an Information System and/or information within it or otherwise breach the security policy

2.2
attack signature
sequence of computer activities or alterations that are used to execute an attack and which are also used by an IDS to discover that an attack has occurred and often is determined by the examination of network traffic or host logs

NOTE This may also be referred to as an attack pattern.

2.3
attestation
variant of public-key encryption that lets IDS software programs and devices authenticate their identity to remote parties.

NOTE See Clause 2.21, Remote attestation.

2.4
bridge
network equipment that transparently connects a local area network (LAN) at OSI layer 2 to another LAN that uses the same protocol

2.5
cryptographic hash value
mathematical value that is assigned to a file and used to "test" the file at a later date to verify that the data contained in the file has not been maliciously changed

2.6
DoS (Denial-of-Service) attack
prevention of authorized access to a system resource or the delaying of system operations and functions

[ISO/IEC 18028-1]

2.7
Demilitarized Zone
DMZ

logical and physical network space between the perimeter router and the exterior firewall

NOTE 1 The DMZ may be between networks and under close observation but does not have to be so.

NOTE 2 They are generally unsecured areas containing bastion hosts that provide public services.

2.8
exploit
defined way to breach the security of an Information System through vulnerability

2.9
firewall
type of security gateway or barrier placed between network environments - consisting of a dedicated device or a composite of several components and techniques - through which all traffic from one network environment to another, and vice versa, traverses and only authorized traffic is allowed to pass

[ISO/IEC 18028-1]

2.10
false positive
IDS alert when there is no attack

2.11
false negative
no IDS alert when there is an attack

2.12
host
addressable system or computer in TCP/IP based networks like the Internet

2.13
intruder
individual who is conducting, or has conducted, an intrusion or attack against a victim's host, site, network, or organization

2.14
intrusion
unauthorized access to a network or a network-connected system, i.e. deliberate or accidental unauthorized access to an information system, to include malicious activity against an information system, or unauthorized use of resources within an information system

2.15
intrusion detection
formal process of detecting intrusions, generally characterized by gathering knowledge about abnormal usage patterns as well as what, how, and which vulnerability has been exploited to include how and when it occurred

2.16
intrusion detection system
IDS
information system used to identify that an intrusion has been attempted, is occurring, or has occurred and possibly respond to intrusions in Information Systems and networks

2.17
intrusion prevention system
IPS
variant on intrusion detection systems that are specifically designed to provide an active response capability

2.18
honeypot
generic term for a decoy system used to deceive, distract, divert and to encourage the attacker to spend time on information that appears to be very valuable, but actually is fabricated and would not be of interest to a legitimate user

2.19
penetration
unauthorized act of bypassing the security mechanisms of an Information System

2.20
provisioning
process of remotely searching for new software updates from a vendor's website and downloading authenticated updates

2.21
remote attestation
processes of using digital certificates to ensure the identity as well as the hardware and software configuration of IDS and to securely transmit this information to a trusted operations center

2.22
response (incident response or intrusion response)
actions taken to protect and restore the normal operational conditions of an Information System and the information stored in them when an attack or intrusion occurs

2.23
router
network device that is used to establish and control the flow of data between different networks, which themselves can be based on different networks protocols, by selecting paths or routes based upon routing protocol mechanisms and algorithms

NOTE The routing information is kept in a routing table.

[ISO/IEC 18028-1]

2.24
server
computer system or program that provides services to other computers

2.25
Service Level Agreement
contract that defines the technical support or business performance objectives including measures for performance and consequences for failure the provider of a service can provide its clients

2.26
sensor
component/agent of IDS, which collects event data from an Information System or network under observation

NOTE Also referred to as a monitor.

2.27
subnet
portion of a network that shares a common address component

2.28
switch
device which provides connectivity between networked devices by means of internal switching mechanisms

NOTE Switches are distinct from other local area network interconnection devices (e.g. a hub) as the technology used in switches sets up connections on a point-to-point basis. This ensures the network traffic is only seen by the addressed network devices and enables several connections to exist simultaneously routing.

[ISO/IEC 18028-1]

2.29
Test Access Points
TAP
typically passive devices that do not install any overhead on the packet; they also increase the level of the security as they make the data collection interface invisible to the network, where a switch can still maintain layer 2 information about the port. A TAP also gives the functionality of multiple ports so network issues can be debugged without losing the IDS capability.

2.30
trojan horse
malicious program that masquerades as a benign application

3 Background

The purpose of Intrusion Detection System (IDS) is passively monitoring, detecting and logging inappropriate, incorrect, suspicious or anomalous activity that may represent an intrusion and provide an alert when these activities are detected. It is the responsibilities of the appointed IT Security personnel are actively reviewing IDS logs and making a decision on follow-up actions to be taken for any inappropriate access attempts.

When an organization needs to detect promptly intrusions to the organization's Information System and response appropriately to them, an organization should consider deploying IDS. An organization can deploy IDS by getting IDS software and/or hardware products or by outsourcing capabilities of IDS to an IDS service provider.

There are many commercially available or open-source IDS products and services that are based on different technologies and approaches. In addition, IDS is not "plug and play" technology. Thus, when an organization is preparing to deploy IDS, an organization should, as a minimum, be familiar with guidelines and information provided by this standard.

Fundamental knowledge about IDS is mainly presented in Annex A. This Annex explains the different characteristics of two basic types of IDS: Host-based IDS (HIDS) and Network-based IDS (NIDS), as well as two basic approaches for detection analysis i.e. Misuse-based approach and Anomaly-based approach.

An HIDS derives its source of information to be detected from a single host, while a NIDS derives it from traffic on a segment of a network. The misuse-based approach models attacks on information systems as specific attack signatures, and then systematically scans the system for occurrences of these attack signatures. This process involves a specific encoding of previous behaviours and actions that were deemed intrusive or malicious. The anomaly-based approach attempt to detect intrusions by noting significant departures from normal behaviour. And function on the assumption that attacks are different from normal/legitimate activity and can therefore be detected by systems that identify these differences

An organization should understand that the source of information and the different analysis approaches may result in both advantages and disadvantages or limitations, which can impact the ability or inability to detect specific attacks and influence the degree of difficulty associated with installing and maintaining the IDS.

4 General

IDS functions and limitation, presented in Annex A, indicate that an organization should combine host-based (including application monitoring) and network-based approaches to achieve reasonably complete coverage of potential intrusions. Each type of IDS has its strengths and limitations; together they can provide better security event coverage and alert analysis.

Combining the IDS technologies depends on the availability of a correlation engine on the alert management system. Manual association of HIDS and NIDS alerts may result in IDS operator overload without any additional benefit and the result may be worse than choosing the most appropriate output from one type of IDS.

The process of selecting, deploying and operating IDS within an organization is shown in Figure 1 along with the clause that addresses the key steps in this process.

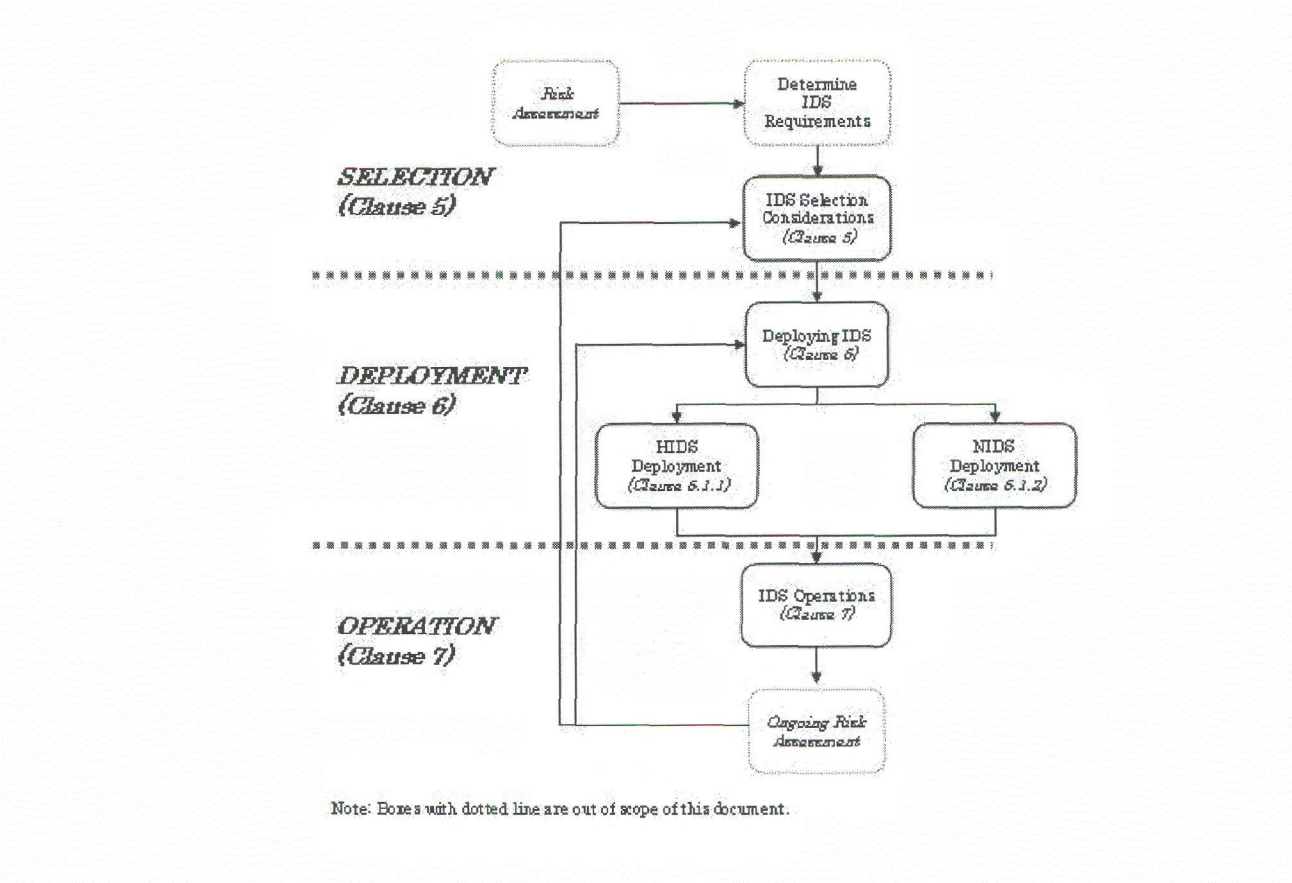

Figure 1 — Selection, deployment and operations of IDS

5 Selection

There are many IDS products and families of products available. They range from extremely capable freeware offerings that can be deployed on a low-cost host to very expensive commercial systems requiring the latest hardware available. As there are so many different IDS products to choose from, the process of selecting IDS that represents the best fit for an organization's needs is difficult. Furthermore, there may be limited compatibility between various IDS products offered in the market place. Additionally, because of mergers and the potentially wide geographical distribution of an organization, organizations may be forced to use different IDS and the integration of these diverse IDS can be very challenging.

Vendor brochures may not describe how well an IDS can detect intrusions and how difficult it is to deploy, operate and maintain in an operational network with significant amounts of traffic. Vendors may indicate which attacks can be detected, but without access to an organization's network traffic, it is very difficult to describe how well the IDS can perform and avoid false positives and negatives. Consequently, relying on vendor provided information about IDS capabilities is neither sufficient nor recommended.

ISO/IEC 15408 (all parts) may be used in the evaluation of an IDS. In such a case, a document called "Security Target" may contain more accurate and reliable description than vendor brochures concerning IDS performance. An organization should use this document in their selection process.

The following clauses provide the major factors that should be used by an organization in the IDS selection process.

5.1 Information Security Risk Assessment

Prior to the selection of an IDS, an organization should perform an information security risk assessment, aimed at identifying the attacks and intrusions (threats) to which the organization's specific information systems might be vulnerable, taking into account factors such as the nature of information used by the system and how it needs to be protected, the types of communication systems used, and other operational and environmental factors. By considering these potential threats in the context of their specific information security objectives, the organization can identify controls which provide cost-effective mitigation of the risks The identified controls would provide the basis of the requirements for the functions provided by their IDS.

NOTE Information security risk management will be the subject of a future International Standard (ISO/IEC 13335-2).

Once the IDS is installed and operational an ongoing process of risk management should be implemented to periodically review the effectiveness of the controls in light of changes to the system's operations and the threat environment

5.2 Host or Network IDS

IDS deployment should be based on an organizational Risk Assessment and asset protection priorities. When selecting IDS, the most effective method to monitor events should be investigated. Both host-based IDS (HIDS) and Network-based (NIDS) can be deployed in tandem. Where such an IDS monitoring method is selected, an organization should implement it in stages starting with a NIDS, as they are usually the simplest to install and maintain, then HIDS should be deployed on critical servers.

Each option has its own advantages and disadvantages. For example, in the case where an IDS is deployed outside an external firewall, an IDS can generate a large number of alerts that do not require careful analysis because a large amount of the alerting events can indicate scans that are already being effectively prevented by the external firewall.

5.2.1 Host Based IDS (HIDS)

The choice of a HIDS demands the identification of target hosts. The expensive nature of full-scale deployment on every host in an organization normally results in the deployment of HIDS on critical hosts only. Therefore the deployment of HIDS should be prioritized according to risk analysis results and cost-benefit considerations. An organization should deploy an IDS capable of centralized management and reporting functions when HIDS is deployed on all or a significant number of hosts.

5.2.2 Network Based IDS (NIDS)

The main factor to consider when deploying a NIDS is where to locate the system sensors. Options include:

- Inside external firewalls;
- Outside external firewalls;
- On major network backbones;
- On critical subnets.

5.3 Considerations

5.3.1 System Environment

Based on a security risk assessment, an organization should first determine, in order of priority, what assets should be protected and then tailor the IDS to that environment. At a minimum, the following system environment information needs to be collected to accomplish this objective:

- Network diagrams and maps specifying the number and locations of hosts, entry points to networks and connections to external networks;
- Description of the enterprise network management system;
- Operating systems for each host;
- Number and types of network devices such as routers, bridges, and switches;
- Number and types of servers and dialup connections;
- Descriptors of any network servers, including types, configurations, application software and versions running on each;
- Connections to external networks, including nominal bandwidth and supported protocols;
- Document return paths that are not the same as the incoming connection path i.e. asymmetric data flow.

5.3.2 Security

After the technical attributes of the system's environment have been documented, the security protection mechanisms presently installed should be identified. At a minimum, the following information is needed:

- Demilitarized Zone (DMZ)
- Numbers, types, and locations of firewalls and filtering routers;
- Identification of authentication servers;
- Data and link encryption;
- MALWARE/Anti-virus packages;
- Access control products;
- Specialized security hardware such as cryptographic hardware;
- Virtual private networks;
- Any other installed security mechanisms.

5.3.3 IDS Security Policy

After the system and general security environments have been identified, the security policy for the IDS should be defined. At a minimum, the policy needs to answer the following key questions:

- What information assets are to be monitored?
- What type of IDS is needed?
- Where can the IDS be placed?
- What types of attacks should be detected?
- What type of information should be logged?
- What type of response or alert can be provided when an attack is detected?

The IDS security policy represents the goals the organization has for the IDS investment. This is the initial step in attempting to gain the maximum value from the IDS asset.

In order to specify IDS security policy goals and objectives, an organization should first identify the organization's risks from internal and external sources. An organization should realize that some IDS vendors define IDS security policy as the set of rules that IDS are used to generate alerts.

A review of the existing organization security policy should provide a template against which the requirements of the IDS can be determined and stated in terms of standard security goals of confidentiality, integrity, availability, and non-repudiation as well as more generic management goals such as privacy, protection from liability, manageability.

An organization should determine how it would react when an IDS detects that a security policy has been violated. Specifically, in the case that an organization wishes to respond actively to certain kinds of violations, the IDS should be configured to do so and the operational staff should be informed of the organization's response policy so that they can deal with alarms in an appropriate manner. For example, a law enforcement investigation may be required to assist in the effective resolution of a security incident. Relevant information, including IDS logs, may be required to be handed over to the law enforcement body for evidentiary purposes.

Additional information concerning security incident management can be found in ISO/IEC TR 18044.

5.3.4 Performance

Performance is another factor to consider when selecting IDS. At a minimum, the following questions should be answered:

- What bandwidth needs to be processed by the IDS?
- What level of false alarms can be tolerated when operating at that bandwidth?
- Can the cost of a high speed IDS be justified or can a moderate or slow IDS suffice?
- What are the consequences of missing a potential intrusion because of IDS performance limitations?

Sustainable performance can be defined as the ability to consistently detect attacks within a given bandwidth utilization. In most environments, there is little tolerance for an IDS missing or dropping packets in traffic that could be part of an attack. At some point, as the bandwidth and/or network traffic increases, many IDS will no longer be able to effectively and consistently detect intrusions.

A combination of load balancing and tuning can increase efficiency and performance. For example:

- Knowledge is required of the organization's network and its vulnerabilities: Every network is different; an organization should determine what network assets need protection and what attack signature tuning are likely to be associated with those assets. This is generally accomplished through a risk assessment process.
- Performance of most IDS can be much better in the case where they are configured to handle a limited amount of network traffic and services. For example, an organization that does a lot of e-commerce can need to monitor all Hypertext Transfer Protocol (HTTP) traffic and to tune one or more IDS to look for only attack signatures associated with web traffic.
- Proper load balancing configuration can allow the signature based IDS to work much faster and more thoroughly because the signature based IDS needs only to process through an optimized smaller attack signature database and not through a database of all possible attack signatures.

Load balancing is used to split available bandwidth in IDS deployment. However, bandwidth splitting is likely to introduce problems such as: additional cost, management overhead, traffic de-synchronization, alert duplication, and false negatives. Furthermore, current IDS technology is reaching gigabits speed and as a result the benefits versus cost of load balancing may be minimal.

5.3.5 Verification of Capabilities

Reliance on vendor provided information about the capabilities of IDS is generally not sufficient. An organization should request additional information and perhaps a demonstration of the suitability of a particular IDS to the organization's environment and security goals. Most IDS vendors have experience in adapting their products as target networks grow and some are committed to support new protocol standards, platform types, and changes in the threat environment. At a minimum, an organization should ask to the IDS vendor the following questions:

- What assumptions were made regarding the applicability of the IDS to specific environments?
- What are the details of the tests that were performed to verify the assertions about the IDS capabilities?
- What assumptions were made regarding IDS operators?
- What IDS interfaces are provided (e.g. physical interfaces, communication protocols, reporting formats for interfacing with correlation engines are all types of important interfaces)?
- What are the alert export mechanisms or formats and are they properly documented (e.g. format or syslog messages or MIB for SNMP messages)?
- Can the IDS interface be configured with shortcut keys, customizable alarm features, and custom attack signatures on the fly?
- In the case where the IDS can be configured on the fly, are the features that provide this capability documented and supported?
- Can the product adapt to growth and change of the organization's systems infrastructure?
- Can the IDS product adapt to an expanding and increasingly diverse network?
- Does the IDS provide fail-safe and fail-over capabilities and how do these capabilities integrate with the same capabilities at the network link layer?
- Does the IDS use a dedicated network for the alarms or are they transmitted in the same network that it monitors?
- What is the vendor's reputation and product's performance record?

5.3.6 Cost

The acquisition of IDS is not the actual cost of ownership. Additional costs include: acquisition of a system to run the IDS software, specialized assistance in installing and configuring the IDS, personnel training, and maintenance costs. Personnel to manage the system and to analyze the results are the largest cost. A useful technique for measuring the IDS cost is the return on investment (ROI) or cost versus benefit analysis. In this case, ROI is computed based on the savings realized by the organization when managing intrusions. The cost of the IDS acquisition and operation needs to be balanced with the cost of the personnel required to help resolve the alerts and the overhead caused by false alerts and inappropriate responses such as reinstalling an Information System because of the inability to determine what has been compromised.

Operational IDS benefits include:

- Identification of defective or mis-configured equipment;
- Verification of configurations on the fly;
- Providing early system usage statistics.

In order to make financial decisions about IDS, questions about the total cost of IDS ownership should be answered. To do this, the expense of deploying IDS across an organization should be analyzed. As a minimum, the IDS cost analysis needs to be based on answers to the following questions:

- What is the budget for the initial capital expenditure to purchase the IDS?
- What is the required time period for IDS operations *e.g.* 24/7 or less?
- What infrastructure is needed to process, analyze and report the IDS outputs and what can it cost?
- Does the organization have the human and other resources required to configure the IDS to the organization's security policy, to operate, maintain, update, monitor the outputs of the IDS and respond to alerts? If not, how can these functions be accomplished?
- Are funds available for IDS training?
- What is the scale of deployment and if it HIDS are used how many hosts will be protected?

The costs to an individual organization may be lessened by sharing overhead costs through outsourcing the IDS monitoring and maintenance functions to a remotely managed intrusion detection services provider.

The most expensive part of an IDS deployment is the response. Figuring out what the response should be, building the response teams, developing and deploying response policy and training and rehearsing are significant costs that should be mentioned

5.3.7 Updates

The majority of IDS are attack signature based and the value of the IDS is only as good as the attack signature database against which events are analyzed. New vulnerabilities and attacks are being discovered frequently. Consequently, the IDS attack signature database should be updated frequently. Therefore, at a minimum an organization should consider the following factors:

- Timeliness of updates;
- Effectiveness of internal distribution;
- Implementation;
- System impact.

5.3.7.1 Timeliness of updates for signature-based IDS

Maintaining current attack signatures is essential to the detection of known attacks. At a minimum, the following questions should be addressed in order to ensure that attack signatures are updated in a timely manner:

- How fast does the IDS vendor issue attack signature updates when an exploit or a specific vulnerability is discovered?
- Is the notification process reliable?
- Is the authenticity and integrity of the attack signature updates guaranteed?
- Are there sufficient skills available in case the attack signatures should be customized within the organization?
- Is there a possibility to write or receive customized attack signatures in order to immediately respond to a high-risk vulnerability or ongoing attack?

5.3.7.2 Effectiveness of internal distribution and implementation

Is the organization capable of quickly distributing and implementing site-specific updates within an appropriate timeframe to all relevant systems? In many cases, attack signatures up-dates should be modified to include site-specific IP addresses, ports, etc. More specifically, at a minimum the following questions should be answered

- In the case that manual distribution processes are in place, do administrators or users implement the attack signature within an acceptable timeframe?
- Can the effectiveness of automatic distribution and installation processes be measured?
- Is there a mechanism to effectively track changes to the attack signature updates?

5.3.7.3 System Impact

In order to minimize the impact of attack signature updates on system performance, at a minimum the following questions should be answered:

- Does an attack signature update impact the performance of important services or applications?
- Is it possible to be selective concerning the attack signature updates? This may be necessary to avoid conflicts or performance impacts on services or applications.

5.3.8 Alert Strategies

The IDS configuration and operation should be based on an organization's monitoring policy. At a minimum, an organization should ensure that IDS can support specific methods of alerting used by an organization's existing infrastructure. Alert features that may be supported include e-mail, paging, Short Message System (SMS), Simple Network Management Protocol (SNMP) event, and even automated blocking of attack sources.

In the case where IDS data is used for forensic purposes, including prosecutions and evidence for internal discipline, IDS data should at a minimum be handled and managed in compliance with the legal and regulatory requirements of the local jurisdictions in which it is likely to applied or submitted.

5.3.9 Identity Management

Identity management is a critical foundation for realizing IDS remote attestation and provisioning without human intervention. Each of these capabilities requires the creation and use of trusted third parties as the authority which despite some differences, is similar to the authority often assumed as part of a public key infrastructure. These capabilities are also important for seamless, secure, controlled IDS data and IDS identity exchange across enterprise network trust boundaries

5.3.9.1 Remote Attestation

IDS may contain millions of lines of code. Intentional insertion of malicious software in this large code base is difficult to discover and can allow an attacker to control the IDS output. Consequently, strict authenticated access-control over the IDS hardware and software is extremely important and should be based in part on the identity of the entity making the access request. Remote attestation can provide this access control capability without humans in the loop.

Remote attestation generates, in hardware, a cryptographic certificate or hash value attesting to the identity of a device or the software running on the device with no user involvement. In the simplest form, identity is represented by a cryptographic hash which allows different software programs or devices to be distinguished from one another or changes in software to be discovered. This certificate may, at the IDS user's request, be provided to any remote party, and in principle has the effect of proving to that party that the IDS is using expected and unaltered software. If the software on the IDS has been altered, the certificate generated will reflect this. That the IDS code base has changed.

In the case of IDS, the aim of remote attestation is to detect unauthorized changes to IDS software. For example, if an attacker has replaced or modified one of the IDS applications, or a part of IDS operating system with a maliciously altered version, the hash value will not be recognized by the remote service or other software. As a result, the corruption of IDS software by a virus or Trojan can be detected by a remote party (e.g. Network Operations Center), which can then act on this information. Because the attestation is "remote", others with whom the IDS interact with should also be able to tell that a particular IDS has been compromised. Thus, they can avoid from sending information to it, until it has been fixed.

For the above reasons, IDS should remotely attest/report to the Network Operations Center (NOC) its status, configuration, and other important information. This attestation capability or IDS authentication is critical to the ability to assess the health of IDS and to perform numerous IDS configuration and update operations. More specifically, attestation is the ability to remotely test the integrity of the IDS. When aggregated, these IDS attestation reports provide situational awareness about the defensive posture of the network and are a critical part of an overall network situational awareness capability

5.3.9.2 Provisioning

When remote attestation detects a problem in the IDS, corrective action is needed to mitigate the problem. This can be achieved by allowing a Network Operations Center to push authenticated configuration, software updates and patches to the IDS. Industry has adopted the term "provisioning" to cover the process of loading the correct software, security policy and configuration data for IT devices to include IDS. The goal of provisioning is to do as much remotely as possible. This both saves the cost of manpower to physically visit individual IDS and allows for more timely mitigation of problems, especially attack signature updates. To be effective, the IDS provisioning capability needs to be securely pushed from an Operations Center as well as securely pulled by the IDS. In the latter situation, IDS should have a secure and automatic capability to remotely search for new software updates from the vendor's website and to download authenticated updates on a timely basis.

5.4 Tools that complement IDS

An organization should detect intrusion promptly and mitigate damage caused by intrusion. Also an organization should understand that IDS is not a sole and/or exhaustive solution to realize this aim. Some network devices and information technology tools may provide such capability that IDS provides. An organization should consider deploying such devices and tools to strengthen and complement the capability of IDS.

Examples of such devices and tools include: File

Integrity Checkers Firewalls or Security

Gateway Honeypots

Network Management Tools Security Information

Management (SIM) Tools Virus/Content Protection

Tools Vulnerability Assessment Tools

5.4.1 File Integrity Checkers

File Integrity Checkers are another class of security tools that complement IDS. They utilize message digest or other cryptographic checksums for critical files and objects, comparing them to reference values, and flagging differences or changes. The use of cryptographic checksums is important, as attackers often alter system files, at three stages of the attack. First, they alter system files as the goal of the attack (e.g., Trojan

Horse placement). Second, they attempt to leave back doors in the system through which they can re-enter at a later time. Finally, they attempt to cover their tracks so that the system owners can be unaware of the attack.

Advantages:

- Determine whether vendor-supplied bug patches or other desired changes have been applied to system binaries;
- Allow quick and reliable diagnosis of the footprint of an attack, especially when conducting a forensic examination of systems that have been attacked;
- Attackers often modify or replace system files and use techniques to retain file attributes that are routinely reviewed by system administrators. Integrity checking tools that use cryptographic checksums can none-the-less detect any changes or modifications;
- Allows the identification of modifications to data files.

Disadvantages:

- May require the information system or at least the system being verified be taken off line and powered down during the analysis.

5.4.2 Firewall

The primary role of a firewall (see, e.g., ISO/IEC 18028-2) is to limit the access between networks. Simple firewalls are designed to filter network traffic based on source and destination Internet Protocol (IP) addresses and port numbers that an organization wants to be accessible. For example, an organization may only want to accept traffic for an email server (port number 25) or for a web server (port number 80). However, application level firewall use application protocol information to provide more sophisticated filtering. In the case that a firewall is positioned within an enclave, it can decrease the amount of traffic that an NIDS is required to examine.

Most firewalls have limited capabilities to monitor network message content and to raise an alert when some prohibited traffic tries to pass through the firewall. In comparison, a NIDS is specifically designed to examine network packets, to detect what constitutes legal and illegal traffic, and can raise an alert when it detects malicious content in the network packets. In many cases, a NIDS alarm can be used to produce a change in the filtering parameters of the firewall if desirable.

In the case that a NIDS is deployed on the organization's side of the firewall, a properly configured firewall should significantly reduce the volume of packets that should be examined by the NIDS. This NIDS configuration can greatly enhance the NIDS accuracy because the Internet background noise due to scanning activity can be removed while controlling the incoming traffic.

5.4.3 Honeypots

Honeypot is a generic term for a decoy system used to deceive, distract, divert and to encourage the attacker to spend time on information that appears to be very valuable, but actually is fabricated and would not be of interest to a legitimate user. The primary purpose of the honeypot is to collect information about the threats to an organization and to lure intruders away from critical systems.

A honeypot is not an operational system and is designed as an Information System capable of being compromised by encouraging attackers to stay on-line long enough for an organization to assess the attacker's intent, skill level and method of operation.

The information gained from analyzing the intruder's activities within the honeypot allows an organization to better understand the threats and vulnerabilities in its systems and therefore improve the organization's IDS operations. By analyzing the actions of an intruder within the honeypot system, this information can contribute to the development of an organization's IDS policy, attack signatures database and the overall approach of the organization towards IDS best practices in protecting against the analyzed types of attacker threats.

In all situations, an organization should use honeypots only after seeking guidance from legal counsel. Data from 'honeypots' may be considered as a form of an entrapment technique and therefore ruled inadmissible in some jurisdictions.

Some of the advantages and disadvantages of honeypots are:

Advantages:

- Attackers can be diverted to system targets that they cannot damage;
- No false positives. Honeypots do not conduct authorized activity and therefore any activity captured by a honeypot is considered suspicious;
- Administrators have additional time to decide how to respond to an attacker;
- Attackers' actions can be easily and more extensively monitored with results used to refine threat models and improve system protections;
- May be effective at catching insiders who are snooping around a network.

Disadvantages:

- The legal implications of using such devices are not well defined;
- An attacker, once diverted into a decoy system, may become angry and attempt to launch a more hostile attack against an organization's systems.
- A high level of expertise is needed for administrators and security managers in order to use these systems.

5.4.4 Network Management Tools

Network management tools utilize various active and passive probing techniques to monitor the availability and performance of network devices. These tools serve as a function for network infrastructure configuration and administration by collecting network component and topology information.

Correlation of network/system management tools with IDS alerts may help the IDS operator appropriately process alerts and evaluate their impact on the systems being monitored.

5.4.5 Security Information Management (SIM) Tools

Organizations use a SIM to consolidate reporting to one management and alert console. A SIM can collect information from IDS, firewalls, sniffers etc and can reduce information overload and make the huge volume of information manageable for the analyst. The second main reason is that this collection of data to one point can correlate multiple small, single packet, multiple source, over long time, under the radar, attacks that may become false negatives to a single IDS.

Security Information Management (SIM) Tools may also be used to process data obtained by an IDS. Typically, SIM tools are used to implement the following functionality

- Collect and maintain security relevant event data from various sources in a centralized database. This can include data from one or more IDS, log files from network devices and hosts as well as event data from anti-virus tools;
- Further process the collected data, especially providing extended filtering, aggregation and correlation capabilities;
- Provide a simple and useful interface for reporting relevant alerts and providing help for further in depth analysis of these alerts based on the collected data.

The major goal of SIM tools is to provide an automated way to distinguish between relevant alerts, posing a possibly high threat, and non-relevant or even false-positive alerts posing no threat. Proper configuration of SIM tools is an indispensable prerequisite to reach this goal and an organization should consider it as an important task when planning the introduction of a SIM tool. As with IDS systems, configuration requires a high degree of expertise and a remarkable amount of work. Given proper set-up and configuration, SIM tools can provide a high added value, and especially can provide valuable information to trigger further processes and activities like incident management.

5.4.6 Virus/Content Protection Tools

Virus/Content protection tools may complement IDS by providing additional data for cross analysis with specific traffic and information on the origin of viruses.

5.4.7 Vulnerability Assessment Tools

Vulnerability assessments are an integral part of risk assessment and a valuable component of good security audit/compliance checking and monitoring strategies. This type of assessment allows an organization to find vulnerabilities and in most cases recommend corrective actions to reduce the opportunity an intruder has to exploit them. Therefore, the use of vulnerability assessment can significantly reduce the number of attacks that IDS should look for.

Vulnerability assessment is focused on assessing the exposure of a given host to a given vulnerability. This assessment process is not the same as executing an attack script. As a result, failure of IDS to detect the vulnerability assessment activity does not indicate that the IDS cannot detect the attack. Conversely, detection of the vulnerability scanning activity by the IDS does not mean that the same IDS can properly detect the attack.

Vulnerability assessment tools are used to test the susceptibility of a network host to compromise. The use of vulnerability testing tools in conjunction with IDS provides an invaluable method for examining the effectiveness of the IDS, in both detecting and reacting to attacks. Vulnerability assessment tools are categorized as either host or network based. Host-based vulnerability tools assess the security of an Information System by querying data sources such as file contents, configuration details and other status information. A host-based tool is granted access to the target host on which it is running via a remote connection. Network-based vulnerability tools are used to scan a number of hosts for vulnerabilities associated with network services. In order to perform host or network vulnerability assessments, an appropriate level of management within the organization should approve the testing. It is important to stress that the use of vulnerability assessment tools complements the use of an IDS and cannot be considered as a replacement.

The advantages and disadvantages of using vulnerability assessment tools are:

Advantages:

- Vulnerability assessment tools provide an effective method for documenting the security state of an Information System and in the case where appropriate re-establishing a security baseline which to return to after system changes;
- Used on a regular basis, vulnerability assessment tools can reliably identify changes in the security state of an Information System;
- The biggest advantage of vulnerability assessment tools is to assist in identifying vulnerabilities.

Disadvantages and issues:

- Host-based vulnerability assessment tools are platform and application specific and are usually more costly than network based tools to build, manage and maintain;
- Network-based vulnerability assessment tools are platform independent and can be less specific than host based tools;

- Vulnerability assessment is a resource consuming activity and may be impractical or may be operated only at the cost of reduced system/network performance or may be operated only with date and time restrictions;
- In many cases, vulnerability assessment is a periodic activity that is conducted weekly, monthly, or even randomly versus continuously and as a result timely detection of security issues may be a challenge at best and sometimes impossible;
- Like IDS, vulnerability assessment tools are subject to false positives or false negatives and should be analyzed carefully;
- Repeated vulnerability assessments can train many anomaly-based IDS to ignore real attacks;
- The need for attack signature updates;
- Host based vulnerability assessment tool will not detect unauthorized systems on your network.

Network vulnerability assessment testing should be confined to the target systems and care should be taken to preserve the privacy of any data collected during the process. The data collected by the vulnerabilities tools is sensitive information that could be used by an intruder to exploit the organization's systems and therefore should be protected.

5.5 Scalability

An organization should investigate the scalability of specific IDS before committing to using IDS. Many IDS function adequately at low data rates, but suffer degradation in performance as bandwidth increases. Performance degradation typically results in a significant increase in errors that produce false negatives (did not produce an alert when an attack occurred) and positives (produced an alert when there was no attack) alarms as more and more packets are dropped and fail to be processed. In other words, many IDS are not able to scale to large or widely distributed enterprise network environments.

Scalability concerns are mostly applicable in NIDS deployments, but also apply to HIDS in the case of host machines that require high performance.

5.6 Technical support

Like other systems, IDS require maintenance and support. IDS are not "plug and play" technologies. Many vendors provide expert assistance to customers in installing and configuring IDS. Others expect that an organization's staff can handle these functions, and provide only telephone or email help desk functions.

The degree of technical support is dependent on the nature of an organization's contractual arrangement with the IDS vendor and is implemented on a case-by-case basis. At a minimum, technical support should include vendor assistance in tuning or adapting IDS to accommodate special organizational needs, whether they are monitoring a custom or legacy system within an enterprise, or reporting IDS results in a custom protocol or format.

An organization should define means for contacting technical support (e.g., email, telephone, online chat, web-based reporting, remote monitoring or response services). Contract provisions normally can specify these technical support services and response times. The contract with the vendor should provide for such services in a fashion accessible enough to support incident handling or other time-sensitive needs.

5.7 Training

Technology alone is not sufficient to detect system intrusions. An organization should need a qualified technical staff to evaluate, select, install, operate, and maintain the IDS. The demand for qualified IDS personnel is very high and in many situations it is very difficult to recruit, hire, and retain personnel who have the experience and knowledge needed to fulfil these IDS responsibilities. Due to this situation, many organizations decide to outsource the IDS operations to a security management service. This option presents

I JTOJIOBHHH (boELZI

j HOpMaTHBHHX
| /T^-^vMeTiTiB

its own organizational training issues and risk. For example, even in the case that most ongoing functions are outsourced, an organization should train personnel with significant knowledge about IDS issues and operations or it can lose control of the IDS process to others. In order for the organization to make optimal use of the IDS, the organization's personnel responsible for oversight of the IDS outsourcing operations should become familiar with IDS operations and procedures. This type of training is generally available from vendors who provide IDS products. An organization should include this type of vendor training as part of the IDS purchase cost.

In the case that the IDS vendor does not provide training as part of the IDS package, an organization should budget appropriately to train operational personnel. Such training should be provided on a continuing basis to allow for staff turnover and changes to the IDS and its environment.

6 Deployment

Based on the criteria provided earlier in this document, successful deployment of either HIDS or NIDS can only be achieved by:

- A thorough requirements analysis, to include IDS security needs, based on a risk assessment;
- Careful selection of an IDS deployment strategy;
- Identification of a solution that is compatible with the organization's network infrastructure, policies, and resource level;
- Specialized IDS maintenance and operations training;
- Documenting the training and rehearsing procedures for handling and responding to IDS alerts.

Due to the benefits and limitations of the two major types of IDS, an organization should consider a combination of network-based IDS and host-based IDS to protect an enterprise-wide network.

6.1 Staged Deployment

Organizations should consider a staged deployment of IDS. This approach can allow personnel to gain experience and to ascertain how many monitoring and maintenance resources can be required to support the IDS operations. The resource requirements for each type of IDS vary widely, and are highly dependent on the organization's systems and security environments.

In a staged deployment, an organization should start with network-based IDS. NIDS are usually the simplest to install and maintain. The next step is to protect critical servers with host-based IDS. Further, an organization should use vulnerability assessment tools on a regular schedule to test IDS and other security mechanisms for proper function and configuration.

6.1.1 NIDS Deployment

As with a HIDS, an organization should ensure that operators are accustomed with a NIDS in a controlled, but active test and training environment. Various positions of the NIDS sensors can be experimented with before full-scale deployment on an operational network. The common positions of NIDS sensors are detailed below and shown in Figure 2. In deploying network sensors, an organization should balance the cost of deployment and on-going operations against the actual level of protection required

When deploying a NIDS for network monitoring, the data capture method should be considered, specifically, in the case where a switch or a TAP (Test Access Port) is to be used. An organization should use a physically separate switch when deploying a NIDS and not a VLAN or similar technology on a core switch. Switches typically can only allow a single Switch Port ANalyzer (SPAN) port to be functional at any give time. SPAN ports also increase CPU usage of the switch, and are typically designed to stop data replication in the case that the CPU hits a threshold of utilization.

Similarly, in the case where this port is then used for network debugging, the IDS become non-functional. An organization should dedicate this port to the function of the NIDS. To address this issue an organization should consider a network TAP (Test Access Port), specifically, an aggregated TAP that combines both the up line and down line streams. These devices are typically passive devices that do not install any overhead on the packet. They also increase the level of the security as they make the data collection interface invisible to the network, where a switch can still maintain layer 2 information about the port. A TAP also gives the functionality of multiple ports so network issues can be debugged without losing the IDS capability.

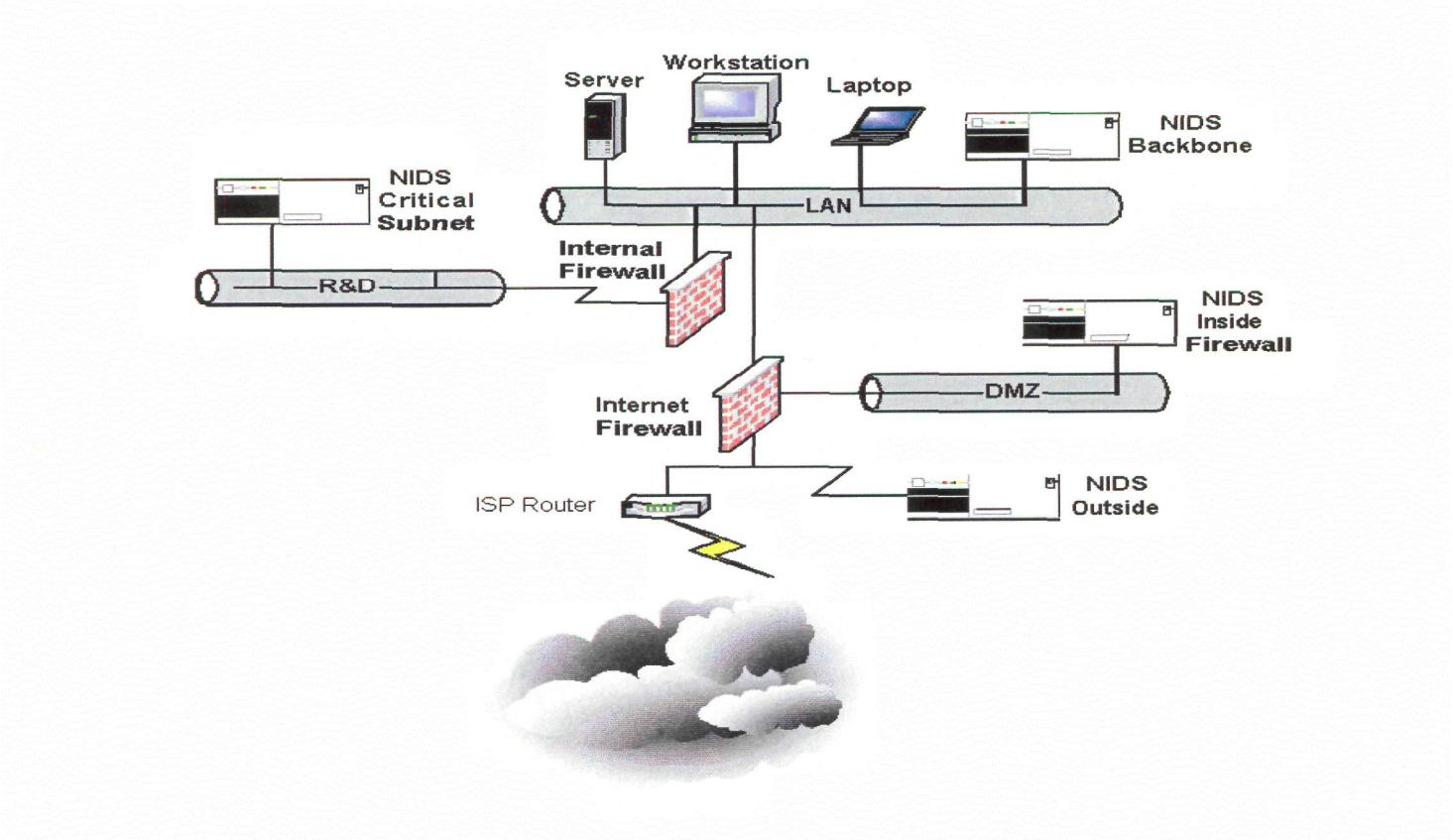

Figure 2 — Typical NIDS locations

6.1.1.1 Location of NIDS inside an Internet firewall: Advantages:

- Identifies attacks originating from external networks that have penetrated the perimeter defences;
- Can help detect errors in firewall configuration policies;
- Monitors attacks aimed at systems in the DMZ (Demilitarized Zone);
- Can be configured to detect attacks against external targets originating from inside the organization.

Disadvantages:

- Not as strongly protected due to its close proximity to the external network;
- Unable to monitor attacks that are blocked (filtered out) by the firewall

6.1.1.2 Location of NIDS outside an Internet firewall

Advantages:

- Allows for the documentation of the number and types of attacks originating from external networks;
- Visibility of attacks that are not blocked (filtered out) by the firewall;
- Can mitigate the impact of denial of service attacks;
- In the case that it used in conjunction with IDS located inside the external firewall, this IDS configuration can assess the effectiveness of the firewall.

Disadvantages:

- As the sensor is located outside the security perimeter of the network it is subject to attack itself and therefore needs to be a hardened stealth device;
- The large amount of data generated at this location makes the analysis of IDS collected data extremely difficult.
- Interaction between the IDS sensor and the management console may require additional holes in the firewall, resulting in possible external access to the management console

6.1.1.3 Location of NIDS on a major network backbone

Advantages:

- Monitors a large amount of a network's traffic, thus increasing the possibility of spotting attacks;
- In the case that an IDS supports a major network backbone, there is the capability of blocking denial-of-service attacks before they can inflict damage to critical subnets;
- Detects unauthorized activity by authorized users within the organization's security perimeter.

Disadvantages

- Risk of capturing and storing sensitive or confidential data;
- IDS should process large amounts of data;
- Attacks that do not cross the backbone will not be detected;
- Host to host attacks on a subnet will not be identified.

6.1.1.4 Location of NIDS on Critical Subnets

Advantages

- Monitors for attacks targeted at critical systems, services and resources;
- Allows focusing of limited resources to the network assets considered of greatest value.

Disadvantages

- Problems with correlating security events between subnets;
- If the alarms are not transmitted on a dedicated network, IDS related traffic may increase network loading on critical subnets.

- If improperly configured, IDS may capture and store sensitive information and give access to this information in unspecified ways.

6.1.2 HIDS Deployment

Before the operational deployment of a HIDS an organization should ensure that operators become familiar with its features and capabilities in a sheltered, but active, environment. The effectiveness of any IDS, but particularly a HIDS, depends on an operator's ability to distinguish between true and false alarms. This requires knowledge of the organization's network topology, vulnerabilities, and other details associated with resolving false alarms. Operational experience over time can identify the normal or baseline types of activity in the environment being monitored by the HIDS. Since HIDS are typically not continuously monitored, an organization should establish a schedule for checking the IDS outputs. This mode of HIDS operation should significantly reduce the risk that an attacker can tamper with the HIDS in the course of an attack.

The full-scale deployment of HIDS should commence with critical servers. Once the operation of HIDS is routine, other servers may be considered for HIDS deployment. Installing HIDS on every host in the organization can be expensive and time-consuming, as each IDS should be installed and configured for each specific host. Therefore, organizations should first install HIDS only on the critical servers. This approach can decrease the overall deployment costs and allow inexperienced personnel to focus on alarms generated from the most important assets. When this portion of the HIDS operation becomes routine, an organization may want to revisit the initial Information Security Risk Assessment results and consider installing more HIDS. An organization should employ HIDS that have centralized management and reporting functions. These features can significantly reduce the complexity of managing alerts from the HIDS that are deployed throughout the organization. In the case that significant numbers of HIDS are deployed, an organization may want to consider outsourcing the HIDS operations and maintenance to an information security management service.

6.1.3 Safeguarding and Protecting IDS information Security

The IDS database stores all the data relating to suspicious activity and attacks within an organization's information infrastructure and is therefore security sensitive. Therefore data protection is needed and the following minimum controls or equivalent are recommended:

- Using checksums to verify the integrity of the stored data;
- Encryption of stored IDS data;
- Proper configuration of the database, especially through the use of access control mechanisms;
- Suitable database maintenance techniques to include back-up procedures;
- Hardening the systems running the IDS database sufficiently to resist penetrations;
- Sniffing (receive only) cables to connect the IDS to the Ethernet hub or switch;
- Implementation of a separate IDS management network.

IDS logs, configuration, attack signature and information exchanged between IDS sensors and collectors, should be protected against unauthorized modification or deletion.

IDS logs may contain sensitive or privacy related information and should be protected in storage and transmission. Authorized persons responsible for analyzing information from IDS sensors or collectors should safeguard the information for which they are responsible.

7 Operations

Prior to the IDS operations phase, an organization should:

- Establish processes, procedures, and mechanisms that ensure the IDS is covered by the organizations vulnerability management process;
- Prepare an incident management process in accordance to ISO/IEC TR 18044:2004;
- Define actions that should be taken when an IDS produces an alert;
- Identify conditions under which automated and semi-automated responses can be permitted and how the outcome of this type of response can be monitored to ensure that a safe and appropriate action is executed;
- Clarify and prepare legal considerations.

7.1 IDS Tuning

Following the deployment of IDS, an organization should decide what, when, and how the IDS alert features can be used and to ensure that these features are routinely adjusted.

Most IDS come with configurable alert features, which allow a wide variety of alert options, including: email, short message system, paging, and network management protocol traps, and even automated blocking of attack sources. Although many of these alarm features may be appealing, an organization should be conservative about using them until it gains a stable well understood IDS installation and some sense of the behaviour of the IDS within the organization's environment.

In some situations, an organization should delay activating the full suite of alarm features for several months after the initial installation. In cases where the alarm and response features include automated response to attacks, specifically those that allow the IDS to direct the firewall to block traffic from the perceived sources of the attacks, an organization should be extremely careful that the attacker isn't using this IDS feature to deny access to legitimate users i.e. a self inflicted denial of service attack. Initially, these types of IDS features should be placed in a semi-automated mode in which a human should decide if the IDS response should be activated.

7.2 IDS Vulnerabilities

The unsecured implementation of an IDS sensor is potentially susceptible to attack in the same as any other device on the network. In the case that an attacker learns of its existence they are more inclined to try and exploit any known vulnerabilities in the IDS. The attackers are likely to attempt to disable the IDS or force it to provide erroneous information. Additionally, many IDS have security weaknesses such as sending unencrypted log files, limited access controls and the lack of integrity checks on the log files. It is imperative that the IDS sensors and console are implemented in a secure fashion and the potential weaknesses in the IDS should be addressed.

7.3 Handling IDS Alerts

Typically, IDS produces a great deal of output. In order to separate the trivial alerts from ones of a more serious nature, an organization should analyze the IDS output thoroughly. Alerts typically contain a concise summary of the detected attack and as a minimum should include:

- Time/date of detected attack;
- IP address of the sensor that detected the attack;
- Vendor specific attack name;

- Standard attack name (if one exists);
- Source and destination IP address;
- Source and destination port numbers;
- Network protocol used in the attack.

Several IDS provide further generic details of attack methods used. This information allows operators to gauge the severity of the attack and should contain the following:

- Text description of the attack;
- Attack severity level;
- Type of loss experienced as a result of the attack;
- The type of vulnerability the attack exploits;
- A list of the software types and version numbers that are vulnerable to the attack;
- A list of relevant patches;
- References to public advisories where details of the attack or vulnerability can be found.

7.3.1 Information Security Incident Response Team (ISIRT)

When an alert is received an organization should have an Information Security Incident Response Team (ISIRT) in place. The plan for the ISIRT should set forth the organization's procedures for handling security incidents, such as viruses, insider abuses of systems and other types of attacks. It should outline the actions that are to be taken in the event of a security incident and establish schedules and content for training personnel about their responsibilities in the incident handling process. Further information on security incident reporting and handling is discussed in ISO/IEC TR 18044.

7.3.2 Outsourcing

In addition to IDS products, some security service providers offer managed IDS services that include consultancy and operations center management. Many organizations prefer to outsource major support roles, including security services to managed service providers, so that they do not have to train and retain personnel with specialized skills. As with the selection of IDS products, the managed security service offerings should be carefully considered to determine if they are financially viable and provide the appropriate level of support while maintaining confidentiality.

When dealing with an IDS vendor that offers a managed security service solution, at a minimum, an organization should ask to the vendor:

- What confidentiality agreements are in place?
- What qualifications are required of the people monitoring the IDS?
- What are the qualifications of the supervisory staff?
- What are liaison and communications arrangements between the service provider and an organization's internal security personnel?
- Does the vendor offer emergency response services to complement the organization's capabilities?

- Does the vendor offer forensic investigation services?
- Does the vendor offer a Service Level Agreement (SLA)?
- What reporting options are available, and can they be customized to an organization's requirements?
- Can the detection policies be customized for an organization's environment, or do you have to use their preset defaults?
- What technical measures are in place to enforce these agreements?
- What Security vetting procedures of service provider staff are undertaken?

A well thought-out outsourcing Service Level Agreement can be required that includes detailed requirements for:

- Content of periodic reports (daily, weekly, etc.);
- Metrics for response times;
- Mechanism for notifying the organization when an attack occurs (email, pager, Short Message System, Multimedia System, telephone, etc.);
- Incident tracking and management procedures;
- Confidentiality and non-disclosure agreements.

Advantages:

- A managed security service provider can typically supply a higher level of security than an equivalent expenditure could produce within an organization providing their own;
- Generally, a 24 by 7 capability can be implemented quicker, more effectively, and may involve less cost;
- Since many managed security service providers can have access to information from many different customers, they may be in a better position to resolve suspicious activity and to identify an attack;
- An organization can reduce the time needed to put effective IDS procedures together and the time needed to follow-up on all the implementation details;
- While there is a need for an awareness of IDS capabilities in an organization, there is no requirement to provide ongoing specialized training of employees in the latest IDS tools and capabilities.

Disadvantages:

- The outsourcer should be monitored and audited for compliance with the organization's security requirements, restrictions and policies;
- The potential exposure of sensitive organizational information to a third party organization;
- Can be more costly than in-house support if not implemented carefully;
- Can deprive an organization of control over sensitive data.

7.4 Response Options

Many IDS support a wide range of response options, which can be categorized as either active or passive.

7.4.1 Active Response

An active response involves an automated action taken by the IDS on the detection of an attack. Intrusion detection systems designed to provide active response are also known as Intrusion Prevention Systems (IPS). Active responses are further categorized as follows:

- Collecting of additional information about the suspected attack;
- Changing of the 'system' environment to stop the attack;
- IPS actively deny the communication and/or end the communication session without a necessary human action after an alert to take preventive action.

IPS and IDS share many similar functions such as packet inspection, protocol validation attack signature matching, and state-full analysis. However, each device may be deployed for different purposes. IPS represent the merger of protect capabilities with intrusion detection capabilities and make it possible to first detect an attack and then protect against it in either a static or dynamic manner.

IDS are a passive device that monitors activities and looks for known attack signatures or abnormal situations. IDS are offline devices that are designed to tell what malicious activity is happening on a network. Due to the passive nature of IDS, there are few opportunities for the IDS to cause a network to malfunction.

On-the-other-hand, IPS allows or denies access to resources based on credentials and some predefined rule-set or policy. IPS is an inline device that is designed to monitor traffic and decide whether to drop packets of data, disconnect connections that contain unauthorized data, or allow traffic. In other words, IPS provides protection for information assets by eliminating malicious network traffic while continuing to allow legitimate activity to occur. The two main types IPS are:

- Host-based IPS (HIPS) - runs software directly on a workstation or server and can detect and prevent threats aimed at the local host.
- Network-based IPS (NIPS) - combines features of standard IDS and IPS and a firewall. Traffic is passed to the detection engine to determine in the case where the traffic poses a threat. Upon detection of malicious traffic, an alert occurs and the traffic is discarded.

As with HIDS, HIPS relies on software that is installed directly on the system being protected and are closely bound to the operating system and services. This allows system calls to the operating system or APIs to be monitored and intercepted in order to prevent and log attacks. NIPS combine the features of an IDS and IPS and a firewall. Packets appear at either the internal or external interface and are passed to the detection engine to determine if the packet poses a threat. In the case that a malicious packet is detected, an alert is raised, the packet is discarded, and the flow is marked as malicious. This results in the remaining packets of that particular TCP session arriving at the IPS device and immediately being discarded. A more refined IPS can stop individual packets rather than the whole session, they can dynamically reset the firewall rules, route traffic to a honeypot or combinations of these activities etc.

The HIPS software intercepts all requests to the system it protects. Consequently it must be very reliable, must not impact performance, and must not block legitimate traffic.

Advantages

- Ability to detect and block attacks;
- Provides proactive protection;
- Increases operational efficiencies due to reduced need to react to IDS event logs.

Disadvantages

- Design to work in-line, thus presents a potential choke point and a single point of failure;
- False positives can be far more serious and far reaching then for an IDS i.e. results can be a self inflicted denial of service attack;
- Under anticipated traffic loads, an analysis should be performed on every packet without any noticeable impact on the traffic flow,
- Active responses may only be applied to a subset of the signature set;
- Given the tight integration of the HIPS software to the operating system kernel, future operating system upgrades could cause problems.

7.4.2 Passive Reaction

Passive responses provide information to operators or to a pre-specified location. They rely on the IDS operators to take subsequent action based on the information provided. Passive responses take the form of:

- Alarms and notifications, usually onscreen alerts, popup window and messages to pagers or mobile phones;
- SNMP traps configured to respond to a central management console.

7.5 Legal Considerations

As with all systems that collect information that may contain sensitive material, employee data or evidence for a later criminal investigation, the data should be stored and processed responsibly and in full compliance with the applicable legislation. The organization should ensure that its employees are aware of their responsibilities in this regard. This clause outlines the legal considerations associated with the use of IDS.

7.5.1 Privacy

In the course of normal operation, an IDS system could collect information about individuals and could be used to monitor the activities of employees. It is possible that this be subject to privacy and applicable legislation in many local jurisdictions. An organization should develop and implement policies to ensure compliance with relevant privacy and applicable legislation for any use of IDS.

7.5.2 Other legal and policy considerations

Implementation and operation of IDS may be subject to other legal and regulatory requirements as well as the policy requirements of the organization where the IDS are deployed. Legal, regulatory, and organizational policy requirements should be reviewed and addressed when implementing and operating IDS. Legal and regulatory aspects are further discussed in ISO/IEC TR 18044.

7.5.3 Forensics

IDS logs may be used for forensic purposes. The forensic requirements of the relevant jurisdictions should be understood and appropriate controls on the storage and handling of IDS logs should be put in place to enable acceptable forensic scrutiny of the information. There may be additional requirements concerning documentation of IDS systems and processes to meet forensic and evidentiary requirements.

Annex A
(informative)

Intrusion Detection System (IDS): Framework and Issues to be Considered

A.1 Introduction to Intrusion Detection

An organization needs to protect its Information System because there are the organizational business reasons to use Information System and to connect them to the Internet and other networks despite the fact that there are vulnerabilities in its Information System that can be exploited, intruded and attacked accidentally or deliberately.

Enhanced techniques and the greater ease of access to information, as well as, new vulnerabilities, are being discovered each week. Simultaneously, attacks are being developed to exploit these vulnerabilities. Intruders are continually enhancing their techniques, and information to aid them is becoming more and more easily available. Equally important, computer literacy is commonplace, and, due to the availability of attack scripts and advanced tools, the skills required to launch attacks are decreasing. Consequently, attacks can be initiated without an individual knowing exactly what occurs or what harm can result from the attack.

The first layer of defence to protect information systems uses physical, managerial and technical controls that should encompass identification and authentication, physical and logical access control, auditing, and cryptographic mechanisms. An organization can find the list of recommendable controls in ISO/IEC 17799. However, it is economically impossible to completely protect every information system, service and network at all times. For example, it is difficult to implement access control mechanisms when the networks being used are global, have no geographical boundaries, and the difference between an insider and an outsider is not obvious. Furthermore, the traditional perimeter defence has become less viable because organizations are increasingly relying on remote access by employees and extended business partners. This IT environment has created complex network configurations that are very dynamic, and include multiple access points into an organization's IT systems and services. Thus, the second layer of defence is needed in order to detect and response promptly and effectively from intrusions when they occur. This layer of defence is undertaken mostly by Intrusion Detection System (IDS). In addition, feedback from the deployed IDS can refine knowledge about vulnerabilities of the organization's Information System, which can help for the organization to improve the overall quality of information security.

An organization can deploy IDS by getting IDS software and/or hardware products from markets or by outsourcing capabilities of IDS to an IDS service provider. In either case, an organization should understand that effective deployment of IDS requires an organization to have knowledge about IDS, as it is not a plug-and-play device.

Like every control, an organization needs to justify deployment of IDS by information security risk assessment and integrate the deployed IDS into the organization's information security management process. In addition, appropriate cares needs be taken considering that, in the case that an intruder or attacker eavesdrop information contained in the deployed IDS, the intruder or attacker can override it and make the organization confront enormous difficulties.. These aspects include how to identify and justify the need for safeguards like IDS. Corporate and the relevant system or service security policy should state that safeguards be selected as appropriate to manage the risks of intrusion. These safeguards include those that:

- Reduce the chances of intrusions occurring;
- Detect and response effectively from intrusions that may occur.

Like every control, an organization needs to justify deployment of IDS by information security risk assessment and integrate the deployed IDS into the organization's information security management process. In addition,

appropriate cares needs be taken considering that, in the case that an intruder or attacker eavesdrop information contained in the deployed IDS, the intruder or attacker can override it and make the organization confront enormous difficulties.

When an organization considers the deployment of IDS, it should understand

— Types of intrusions and attacks to an Information System and/or networks,

— Generic model of IDS proposed in this document.

A.2 Types of intrusions and attacks

Intruders and attackers on Information System can exploit configuration faults, implementation faults and/or conceptual faults of Information System and/or networks, as well as taking advantage of abnormal user behaviour.

Vulnerabilities can permit the intruder and attacker to access protected Information System and information which is being processed and stored in the Information System, and compromise confidentiality, integrity and/or availability of information and information systems. These intrusions and attacks can provide the intruder and attacker valuable knowledge about Information System and/or networks that can be exploited by more complicated intrusion or attack techniques. An organization should recognize that intrusions and attacks are attempted not only by somebody external to the organization, but also by a malicious insider within the organization. For example, authorized users of an organization's Information System may attempt to gain additional privileges for which they are not authorized. Deliberate intrusions and attacks may be used for:

— Information gathering, by which an attacker attempts to retrieve detailed information about targeted Information System,

— Attempts to gain use unauthorized system privileges, resources, or data.

— Compromising a system which may allow the use of the system's resources for further attacks.

— Information disclosure, by which an intruder attempts to use protected information (e.g., password, credit card data) as unauthorized means, and/or

— Denial of service (DoS) attack, by which an attacker attempts to slow down or create an out of service condition for the targeted Information System services.

Considering the vulnerable points likely to be intruded and attacked, intrusions and attacks can also be broken down and considered as

— Host-based,

— Network-based, or

— Combined methods.

A.2.1 Host-based intrusions

Host-based intrusions are generally considered to be intrusive activities that introduce compromising malicious code (e.g., attacks utilizing Trojan horses, worms, or viruses) and on:

— The application layer (SMTP, DNS) (e.g., e-mail forgery, spamming, buffer overflow attacks, race condition attacks, man-in-the-middle attacks);

— An authentication system (e.g., attacks utilizing eavesdropping or password guessing);

— Web-based services (e.g., attacks aimed at CGI, ActiveX, or JavaScript);

— System availability (e.g., DoS attacks);

— The operating system; or

— Network and application management systems (e.g., SNMP attacks).

A.2.2 Network-based intrusions

Network-based intrusions are generally considered to be intrusive activities on:

— Physical and data-link communications protocols and the systems that implement them (e.g. ARP-spoofing, MAC-address cloning); or

— Network and transport communications protocols and the implemented systems (IP, ICMP, UDP, TCP) (e.g. IP-spoofing, IP-fragmentation attacks, SYN flooding attacks, malformed TCP-header information attacks).

A.3 Generic Model of Intrusion Detection Process

IDS consists of software and/or hardware products automatically monitor, collect and analyze suspicious events occurring in Information System or networks for signs of intrusions. A generic model of intrusion detection can be defined by a set of functions. These functions include: raw data sourcing, event detection, analysis, data storage, and response. These functions can be implemented by separate components or be software packages as part of a larger system. Figure A.1 shows the manner in which these functions relate to each other.

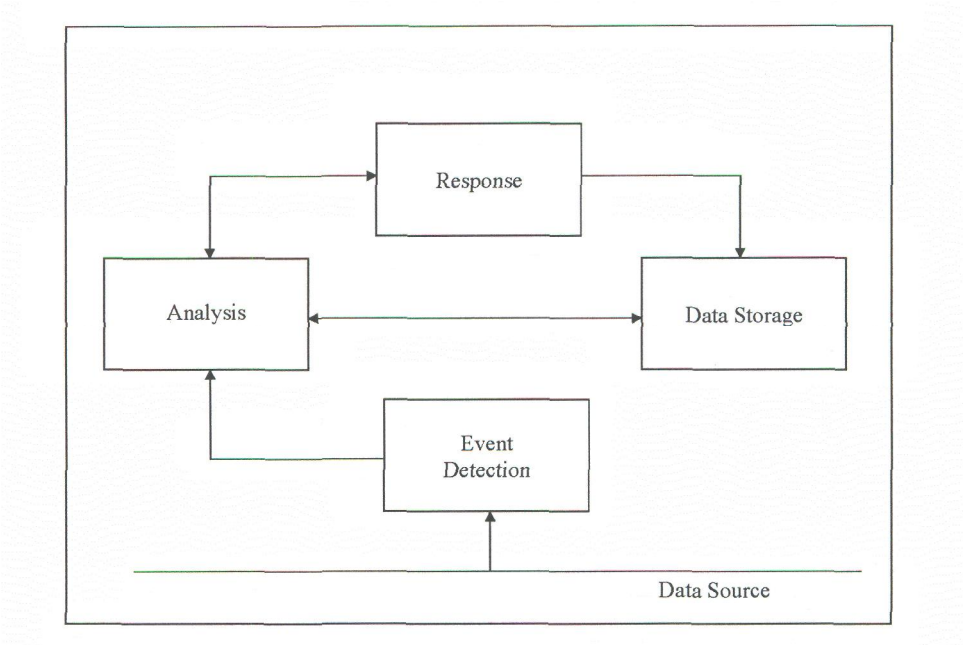

Figure A.1 — Generic model of intrusion detection

A.3.1 Data Sources

The success of the intrusion detection process depends upon the data sources from which information is taken from the detection of intrusion attempts. The following sources can be defined as:

— Audit data from different system resources: Audit data records contain messages and status information ranging from a high level of abstraction to data at a very detailed level showing a chronological stream of events. Useful sources for audit data are the log files of operating systems, which include the log of system events and activities generated by the operating system, e.g. audit trails/logs. Applications that record information about file systems, network services, access attempts, etc, are also good sources for raw data.

— Allocations of system resources by the operating system: System monitoring parameters such as CPU workload, memory utilization, starvation of system resources, I/O rate, number of active network connections, etc., are interesting to help detect intrusions,

— Network management logs: Network management logs provide network device health, status, and device state transition information,

— Network traffic: Network traffic provides parameters like the source and destination addresses, as well as the source and destination ports that are security relevant. Also the different options of the communications protocols (e.g., status flags of IP and TCP, which indicate source routing or connection attempts and acknowledgements) are useful for the IDS. It is helpful to collect the raw data at a low level referring to the OSI model, because there are fewer possibilities for the data to be manipulated prior to collection. In case raw data is only gathered at a higher level of abstraction, for example, from a proxy server, then the information that was present at the lower level may be lost,

— Other data sources: Other data sources include firewalls, switches and routers, and of course IDS-specific sensors/monitoring agents.

The location of the raw data sources can be classified into two: hosts and networks. As the differentiation of the location is predominant in the world of intrusion detection, IDS can be also classified into two types: host-based and network-based. Host-based IDS can examine audit trails/logs and other data from hosts or applications. Network-based IDS can examine network management logs, as well as data from firewalls, switches, routers and IDS-specific sensors agents.

A.3.2 Event detection

The purpose of Event Detection is to detect and provide security related event data for use in the analysis function.

Events detected may be simple events (comprising of parts of attacks or occurrences during normal operation) or complex events (comprising of combinations of simple events that are highly likely to indicate a particular attack). However, event or event data may not serve as evidence of an intrusion.

The event detection function is achieved by the monitoring component of the IDS. They can be installed on a network device (e.g., router, bridge, firewall), or on a specific computer (e.g., application server, database server), depending upon the raw data sources from which the event data is to be detected.

As event detection process can produce large amount of event data, the frequency of event detection can affect the overall effectiveness of IDS. This situation can also be applied to the following analysis process.

A.3.3 Analysis

The purpose of the analysis function is to analyze and process event data that are provided by the event detection function, in order to find if an intrusion has been attempted, is occurring, or has occurred.

In addition to the detected event data, the analysis function can utilize information or data from many sources, including:

— Data that are results of previous analysis and are held by the data storage function,

— Information or data generated from the knowledge about how an individual or system is supposed to behave (i.e. from known tasks supposed to be performed or from actions authorized to be done),

— Information or data generated from the knowledge about how an individual or system is not supposed to behave (i.e., from known attacks or from known harmful actions), and

— Other relevant information or data such as suspected attack source sites, individuals, or location of attackers.

There are two general approaches to analysis: misuse-based and anomaly-based. Some misuse-based approach is also called as knowledge-based. Some anomaly-based approach is also called as behaviour-based.

A.3.3.1 Misuse-based approach

Misuse-based approach focuses on the search for evidence of attacks in the detected event data, based on the knowledge accumulated from known attacks and unauthorized activities.

Typical misuse-based approach attempts to model and encode known attacks on Information System, as well as previous behaviours and actions that were deemed malicious or intrusive, as specific attack signatures, including systematically scanning Information System for occurrences of these attack signatures. Because patterns of known attacks or slight variations of known attacks are called signatures, misuse detection is sometimes called signature-based IDS.

The most common techniques of attack signature-based detection used in commercial products specify each pattern of events corresponding to an attack or unauthorized activity as a separate attack signature. However, some of the more sophisticated mechanisms allow using a single attack signature to detect a group of known attacks and unauthorized activities.

Care needs to be taken that, while misuse-based approach stands on assumption that the event data which are not matched with the attack signatures, does not indicate intrusions or attacks, some unmatched data can still contain evidence of intrusions or attacks, which might be unknown at the time the attack signatures were modelled.

The current prevailing methods used by the misuse-based analysis function are:

A.3.3.1.1 Attack signature analysis

This method is probably the most common way to detect intrusions and based on the expectation that any security-relevant action initiated on Information System can lead to a corresponding audit log entry.

Intrusion scenarios may be translated into sequences of audit logs or patterns of data, which can be found in the data generated by the operating system of a computer, applications, firewalls, switches and routers, or IDS-specific sensors or monitors. Other sequences or attack signatures may be found in a stream of network traffic. Protocol analysis is a form of network specific attack signature analysis and uses the well-defined structure of communications protocols. Protocol analysis can process elements like packets, frames and connections.

By the analysis process, semantic descriptions or attack signatures of known attacks are collected or formulated and stored in a database. When the specific sequence or attack signature that matches a predefined attack signature of an intrusion is found in the audit logs, etc., an attempt of an intrusion is indicated.

Attack signature analysis methods can be used with or without thresholds. In the case that no thresholds are defined, an alarm is generated when an attack signature is recognized. When a threshold is defined, an alarm is only generated when the number of attack signatures exceeds the threshold. A threshold could be a percentage, or a number, of occurrences per time period or some other measure.

The main drawback of the attack signature analysis method is the need for frequent updates to keep up with the stream of newly discovered vulnerabilities and /or attacks.

A.3.3.1.2 Expert systems

In case of misuse-based approaches, expert systems contain rules that describe intrusions. In the case of anomaly-based approaches, a set of rules is generated statistically describing the behaviour of the users based on records of their activities over a given period of time. The rules should be continually updated to accommodate new descriptions of intrusions or new usage patterns.

Audited events are translated into facts carrying their semantics into the expert system. The intrusion analysis function draws conclusions using these rules and facts either to detect the presence of a suspected intrusion or to detect inconsistent behaviour.

A.3.3.1.3 State transition analysis

This technique describes an intrusion with a set of goals and transitions, and represents them as state-transition diagrams. States in the attack signatures, corresponding to system states, have Boolean assertions associated with them that should be satisfied to transition to that state.

A.3.3.2 Anomaly-based approach

Anomaly-based approach focuses on finding irregularities of observed behaviour from predicted or expected usual behaviour, based on previous observations of a system during normal operation or a profile defined by other expected use of parameters. The profile is a predetermined specific event pattern usually related to a series of events, and stored within a database for the purposed of comparison.

Care needs to be taken that, while anomaly-based approach stands on assumption that the event data, which are not matched with the attack signatures, indicate intrusions or attacks, some unmatched data can still contain evidence of normal or authorized behaviours, which might be unknown at the time the attack signatures were modelled.

The current prevailing methods used by the anomaly-based analysis function are:

A.3.3.2.1 Anomalous behaviour identification

This method matches patterns of proper activity of users, whereas attack signature analysis matches patterns of improper activity.

This method models the normal or authorized behaviour of users by the set of tasks they have to or are authorized to perform on the system by using non-statistical technique. These tasks and facets are then represented as patterns for users' expected or authorized actions such as access to particular files or types of files.

The individuals' actions found in the audit trails are compared with their expected or authorized patterns. An alarm is issued in the case where the action pattern differs from the expected or authorized pattern.

A.3.3.2.2 Expert systems

(Refer to A.3.3.1.2)

A.3.3.2.3 Statistical methods

The most widely used method for anomaly-based approaches to detect intrusions is statistical.

User or system behaviour is measured by a number of variables sampled over time and stored in a profile. At regular intervals, the current profile is merged with the stored profile and updated as the behaviours of users evolve.

Examples of these variables include the login and logout time of each session, the duration of resource utilization, and the amount of processor-memory-disk resources consumed during a session or during a given time period.

A profile can be comprised of several types of measures. These types include:

— Activity intensity measures,

— Audit record distribution measures,

— Categorical measures (e.g., relative frequency of logins), and/or

— Numerical measures (e.g., a number value of an amount of CPU or I/O for a specific user).

Anomalous behaviour is determined by examining the current profile with the stored profile whether thresholds are exceeded based on the standard deviation of a variable.

A.3.3.2.4 Neural networks

Neural networks are algorithms that learn about the relationship between input-output vectors and discover the generalized rule to obtain new input-output vectors in a reasonable way. The main use of neural networks for intrusion detection is to learn the behaviour of actors in the system (e.g., users, daemons programs). The advantage of using neural networks over statistics resides in having a simple way to express nonlinear relationships between variables, and in learning and retraining the neural network automatically.

A.3.3.3 Combined Methods

The methods of misuse-based and anomaly-based approaches can be combined to make use of the advantages of each other. The deployment of hybrid IDS allows detection of intrusions based on known attack signatures as well as unidentified patterns such as the number of login attempts of a specific user.

Also there is on-going research exploring additional approaches or methods for intrusion detection. For example, there is research involving the application of Petri nets. There is also a relatively new research area called Computer immunology.

A.3.3.4 Analysis Frequency

Raw data (e.g. audit trails/logs) are generally produced continually but they may not always be processed by the event detection function or analyzed by the analysis function.

Frequency of analysis may be:

— Continuous,

— Periodical, and/or

— Under special circumstances.

A.3.3.4.1 Continuous/Near Real-Time

When the event detection function continuously looks for occurrences of specific data, situations, or activities and provide event data, the analysis function can also carry out continuously.

Care should be taken that the intrusion may be completed in some cases before it is detected and reported, as a time lag may exist between the occurrence of an event and the time at which it is detected and reported. The time lag can be depend upon the parameters such as the source of event data and the detection method, or the nature of the intrusion, which cause the elapsed time between when an intrusion is initiated and when the target system is penetrated.

A.3.3.4.2 Periodical/Batch Processed

In case that raw data and/or detected event data are transferred onto storage media, it is possible to detect and/or analyze them periodically or at appropriate time. For example, detection and/or analysis may be achieved when the load on an IT system is lower, like at night, or by an auxiliary off-line subsystem.

A.3.3.4.3 Initiated Only Under Special Circumstances

Some analysis may only be initiated under special circumstances, such as when a widespread attack has been identified and is causing severe damage. In this case a concentrated effort may be initiated to fully analyze all aspects of the attack and its consequences. These efforts are sometimes called forensic analysis and may be used for the purpose of legal action. In case legal action is contemplated applicable rules of evidence will need to be followed.

A.3.4 Data storage

The purpose of the data storage function is to store security-related information and make it available for the analysis at a later time and/or for reporting.

The stored data may include:

— Detected events and other kinds of data necessary;

— Results of the analysis, including detected intrusions, and suspicious events that can be used later for coordination of suspicious event analysis;

— Collection of profiles of known attacks and normal behaviour; and

— Detailed raw data collected and preserved as evidence (e.g., for traceability), once a security alarm is raised.

There should be data retention and data protection policies in place, which address various concerns such as completion of analysis, data forensics, and evidence preservation, as well as protection against eavesdropping of security- related information.

A.3.5 Response

The purpose of the response function is to present the appropriate results of the analysis to responsible personnel (e.g., system administrator, security officer). As these results are usually presented on a management console with a graphical user interface, additional means to inform the results to relevant personnel can be needed.

While a passive response function is limited to generate alarms on the console, an active response function can also provide appropriate countermeasures to the intrusion. Intrusion detection systems designed to provide active response are also known as Intrusion Prevention Systems (IPS). Some active response function can provide such corrective or proactive measures to curtail the intrusion or to minimize the consequences by:

— Re-configuration of an intruded system,

— Locking out an intruded account, and/or

— Protocol-conformant closing off for a session.

Information provided by the response function can help for an organization's proper authority to assess the severity of the intrusion and decide to implement the appropriate countermeasures. An organization needs to ensure that assessment of the severity and implementation of countermeasures are in line with the organization's information security policies and procedures.

An organization can find the list of recommendable controls, which encompass reporting of information security events, and responsibilities and procedures to recover from security breaches and correct system failures, in Clause 13 of ISO/IEC 17799:2005. ISO/IEC TR 18044 also provides useful information about information security incident management.

A.4 Types of IDS

As previously mentioned, there are two types of IDS: Host-based IDS (HIDS) and network-based IDS (NIDS), and each have its characteristics. There are other types of IDS:

— Application-based IDS (AIDS), but it is a special class of HIDS and have characteristics similar to HIDS.

In general, IDS are able to perform the following functions:

— Monitoring and analysis of system events and user behaviours,

— Recognizing patterns of system events that correspond to known attacks,

— Recognizing patterns of activity that statistically vary from normal activity,

— Alerting appropriate staff by appropriate means when attacks are detected,

— Measuring enforcement of security policies encoded in the analysis engine,

— Allowing non-security experts to perform important security monitoring functions,

— Increasing the perceived risks of discovery and punishment of attackers,

— Identifying many problems that are not prevented by other security devices,

— Coordinating events with other security devices such as firewalls,

— Verifying, itemizing, and characterizing the cyber threats to the Information systems of an organization,

— Providing invaluable information about intrusions that support incident handling, damage assessment, recovery efforts, and legal actions in certain circumstances.

IDS have limitations that should be understood. Significant limitations include:

— Cannot detect novel attacks, nor do they capture most novel variations of attacks;

— Difficulty to compensate for errors and noise from the information sources,

— Difficulty to deal effectively with switched networks,

- Difficulty to be scalable to very large or distributed networks,
- Difficulty to determine the physical and/or virtual location of the intruder from an IDS output,
- Difficulty to integrate different IDS products with network management systems,
- Inability to compensate for weak or missing security policy and/or security mechanisms in the protection infrastructure, such as firewalls, identification and authentication, link encryption, access control mechanisms, and virus detection and eradication,
- Inability to detect, report, or respond quickly enough to certain types of attacks,
- Inability to mitigate against most DoS attacks, in spite of ability to identify them,
- Inability to detect new attacks or some variants of existing attacks (this only applies to signature based IDS not anomaly based IDS),
- Inability to perform detailed analysis of attacks without human intervention,
- Inability to compensate for significant deficiencies in an organization's security strategy, policy, or security architecture,
- Inability to compensate for security weaknesses in network protocols,
- Possibility that outputs of IDS typically contain significant error rates, especially false positives and can take a great deal time and resources to resolve,
- Possibility to be disabled as part of an attack sequence,
- Possibility to be exploited by attackers to generate false positives to distract attention from the main attack,
- Possibility generating a large amount of audit information which may require additional local storage on the system,
- Possibility that automated blocking based on IDS alerts can cause security and availability problems,
- Requires in-depth technical and systems knowledge to use effectively.

A.4.1 Host-based IDS (HIDS)

A HIDS reside on a single computer and provides protection for that specific computer. This allows HIDS to examine computer operating system log data (e.g. audit trails/logs) and other local data. HIDS may also analyze the events occurring within applications by using the operating system or application log files.

Operating system audit trails, which HIDS normally utilize are usually generated at the innermost (kernel) level of the operating systems, and are therefore more detailed and well-protected than system logs. Those system logs, however, are smaller than the audit trails and are easier to understand.

Some HIDS are designed to support a centralized IDS management and reporting infrastructure that can allow a single management console to track many hosts. Others generate messages in formats that are compatible with network management systems.

Unlike NIDS, HIDS can see the outcome of an attempted attack, as it can directly access and monitor the data files and system processes usually targeted by attacks. For example, HIDS permits the detection of attacks from the keyboard of a mission-critical server.

HIDS are designed to:

- Associate specific user identity with the suspicious activities,
- Observe and track user behavioural changes,
- Baseline the security state of a system, and track changes to that baseline,
- Manage operating system audit and logging mechanisms and the generated data,
- Provide application level logging and monitoring when data is transmitted or stored in either encrypted or unencrypted form, and
- Observe data modifications caused by attacks;
- Monitor systems that reside on high speed- networks and in networks which encryption is used;
- Detect attacks that cannot be seen by network-based IDS.

HIDS have unique limitations that should be understood. Significant limitations include:

- Possibility that certain DoS attacks can disable HIDS,
- Possibility that HIDS consumes host resources, including data storage requirements for host audit logs,
- Possibility to require complex installation and maintenance processes due to a great number of installed instances (at least one per host),
- Inability to use in stealth mode, as hosts are typically addressable by higher network layers, and
- Inability to recognize attacks directed at other hosts or at a network.

A.4.2 Network-based IDS (NIDS)

NIDS monitors the traffic destined for host systems on a network. NIDS often consist of a set of single-purpose sensors or hosts placed at various points in a network. These units monitor network traffic, performing local analysis of that traffic and reporting attacks to a central management console. Since the sensors are used specifically as an IDS component, they can be more easily secured against attack. Many of these sensors are invisible to higher network layers (i.e. designed to run in "stealth" mode) in order to make it more difficult for an attacker to determine their presence and location.

NIDS permits real-time or near real-time detection and response by providing information on suspicious intrusions as they occur (e.g. DoS attack), while the timeliness of the response from HIDS is in direct relation to the frequency of the polling interval.

As unique characteristics of NIDS, the functions have such ability as:

- To operate in 'Stealth Mode' and hide the sensor from higher level network protocols (typically layer 3 and above),
- To use a single sensor to monitor traffic for several hosts on a same network segment, and
- To recognize distributed attacks that affects many hosts.

NIDS have unique limitations that should be understood. Significant limitations include:

- Inability to deal well with encrypted network traffic,

— Possibility to require much higher bandwidth and faster processing capability than HIDS because, NIDS performance capacity should be equal to the volume of traffic on the network segment on which it is deployed for maximising the effectiveness

— Possibility that many of the functions provided by NIDS need special technical set-up to be available in modern switch-based networks (e.g. network sensors which need to be connected to the special ports of the network switches which mirrors the data of all other ports),

— Possibility that some NIDS have problems dealing with network-level (IP) or transport level (TCP/UDP) fragmented packets attacks due to issues related to decoding application level (e.g. HTTP, SMTP) protocols, and

— Inability normally to observe whether an attack succeeded.

A.5 Architecture

IDS may be implemented in various ways.

Within smaller organizations, or to protect a well defined and relatively independent system, single IDS may be a good solution.

In environments with quite large and complex infrastructures for networks, systems, and applications, single IDS may not be sufficient or practical to fulfill the requirements of intrusion detection. To meet these requirements, several IDS may be needed, with each being tailored to a defined subsystem or component. In such environments, attacks may target several subsystems or components. In another scenario, an attack may target a specific configuration of the subsystems or components rather than a vulnerability of a subsystem or component itself. In order to detect an attack in such a scenario, the event data from several IDS need to be correlated and analyzed.

The goal of IDS architecture is to implement intrusion detection functionality in an efficient and effective way. Two primary architectural considerations in this context are the:

— way in which the several IDS are interconnected and interrelated,

— Concentration or distribution of tasks within the IDS architecture.

An example of hierarchical intrusion detection architecture is shown in Figure 3.

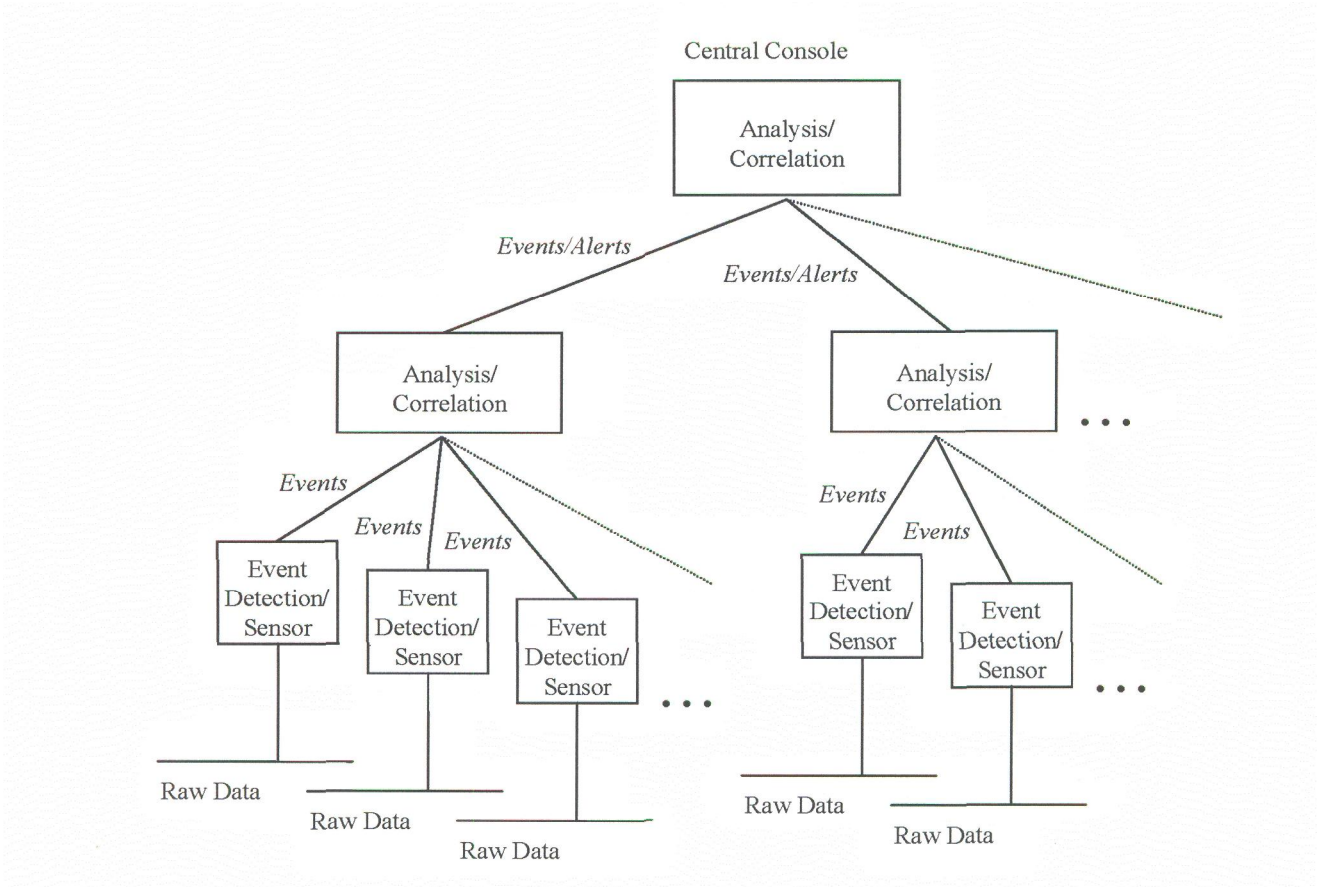

Figure 3 — Hierarchical intrusion detection architecture

In Figure 3, the outputs of several analysis and correlation components are additionally aggregated for a higher level of analysis and correlation. As in any multi-tier application infrastructure, there may be several locations to perform the required functions.

In a centralized architecture, the event detection and sensor components may simply collect raw data and send it to a single component for further analysis and correlation. Although this approach has the benefit of design simplicity, it may not scale well and its use may be appropriate only to smaller environments.

More scalable solutions may perform some IDS tasks in decentralized components with the aim of reducing the raw data as early in the process as possible and forward the relevant events to the next layer of components. A chain of components may further analyze and correlate the event data, passing only the relevant events or alerts to a final, central, component. Such systems may introduce some very complex tasks. As an example, this requires configuring the filters and involved analysis and correlation components in such a way that attack indications find their way to the central component, and that the right alert is issued.

A.6 Management of an IDS

Management of systems for intrusion detection is crucial for efficient and effective deployment in corporate network infrastructures. In order for IDS to be efficient, the management subsystem must provide sufficient functionality. This section addresses various management aspects of IDS.

A.6.1.1 Configuration Management

Configuration management provides functions to exercise control over, identify, collect data from and provide data to entities that are part of the IDS. For the purpose of intrusion detection, configuration management includes management of the detection function and the corresponding response mechanisms used.

A.6.1.2 Detection Function

Configuration of the detection function involves setting the criteria for what events and sequences of events are violations of the security policy. This may also include describing misuse-patterns and normal user behaviour.

A.6.1.3 Response Function

The management of the response function determines the system behaviour upon a security alarm. This includes controlling various response-mechanisms such as audible alarms, administrator and/or security officer notifications, and session termination. The IDS must also be protected from unauthorized response initializations. In case an attacker finds a way to trick the system into responding to non-existing intrusions, this can potentially, depending on the configured responses, cause more damage than would be possible without an installed IDS. The response management should be consistent with an organization's incident management scheme.

A.6.1.4 Security Services Management

Security services management involves managing the security services that are part of IDS. It involves controlling user credentials, confidentiality, integrity, and access control services. Depending on the credentials of the user, access rights may be limited to restrict access to configuration parameters, audit trails and information associated with security events.

A.6.1.5 Integration with Other Management Systems

An IDS management system should securely interface with or be an integral part of the network management, system management and/or security management systems of the environment being protected. This may be necessary to implement certain types of detection functions (e.g. to access logs) and certain types of response functions. The key point is that IDS cannot be selected or implemented in isolation because the IDS management function must integrate well into other system management functions.

A.6.1.6 Security of Management Operations

Security of management operations must be protected to prevent an intruder from accessing information in the IDS or controlling resources of the IDS. Security of management of IDS includes authentication, integrity, confidentiality, and availability of the management service.

The system that runs the IDS management privileges should be configured in accordance with the security policy that requires high levels of security (comparable to that required for other management systems). As the host-based IDS sensors normally run in operating system privileged mode, compromising the management privileges may lead to severe widespread security breaches and potentially all hosts running the IDS agent could be compromised. The consequences of the security breaches of the IDS management privileges are often overlooked especially with the host-based IDS, where most of the commercial offerings have an attack response option of executing a command on the monitored host.

Monitoring of event detectors and sensors to ensure correct operation and functioning is essential to a successful IDS. Event detectors relay information from the sensors to the detection analysis function. Failure to maintain an on-going monitoring function of these devices may lead to a false sense of security should, for example, a sensor fail and the central system (and therefore the organization) be unaware of this technical failure. Thereby the central system would have no alerts or readings to forward to the central operator who still believes all is well.

A.6.1.6.1 Authentication

Management operations should be preceded by proper identification and authentication of the managing entity. A managing entity may be a human user or a system entity.

A.6.1.6.2 Integrity

Management operations should be protected against integrity attacks. It should not be possible to insert, delete or alter a management operation in a manner not authorized.

A.6.1.6.3 Confidentiality

Management operations should be protected against confidentiality attacks. It should not be possible to deduce the intent of any management operation in an unauthorized way.

A.6.1.6.4 Availability

An attack against the network infrastructure, the IDS itself, or the monitored target should not affect the availability of the management service. For example, the management of the IDS should be possible under a denial of service attack. Management of the IDS must be possible even when the IDS is malfunctioning. The IDS and its management should be addressed in the business continuity planning process.

A.6.2 Management Model

Control and management are essential for the successful implementation of intrusion detection, especially in distributed environments where a large number of intrusion detection components are used. Figure 4 provides an example of an implementation of a model of management in a hierarchical way, a model well suited for large organizations. There are occasions where a centralized control represents a single point of failure that, in some environments, might not be acceptable. It will also give an attacker a single point of attack. This could give the attacker an opportunity to delay the detection of the attack and to prevent the administrator from taking appropriate actions.

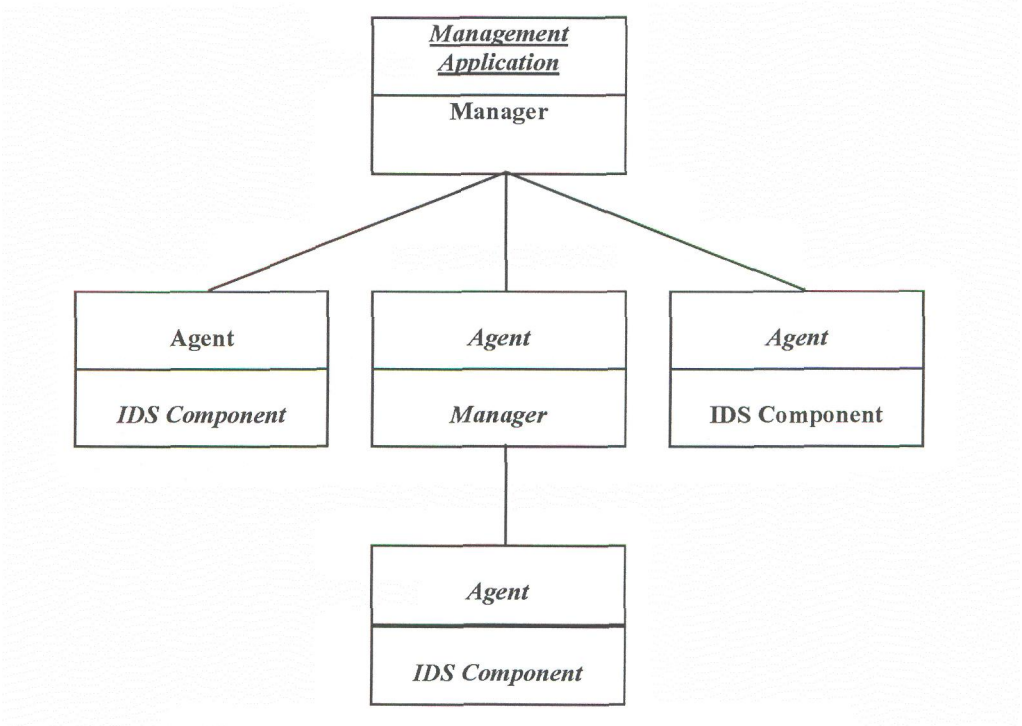

Figure 4 — An intrusion detection management model

Besides the one-to-many cardinality used in the hierarchical model, other cardinalities of management relationships may therefore be appropriate as well:

— many-to-many - several management consoles can manage many distributed agents,

— one-to-many - one management console can manage many distributed agents,

— one-to-one - one management console can manage a single agent.

A.7 Implementation and Deployment Issues

There are many important issues and considerations when it is decided that an IDS is needed for deployment. All IDS are not the same and thus an enterprise's requirements must be considered in light of its IT risk management and security policy in evaluating IDS for deployment.

A.7.1.1 Efficiency

An important consideration in evaluating IDS for deployment is efficiency. To evaluate the efficiency of an IDS several criteria are relevant:

— Accuracy: inaccuracy occurs when an IDS incorrectly identifies activity as an attack (e.g. false positive) or when an IDS incorrectly identifies an attack as legitimate action (e.g. false negative). The ratio of either type of failure to the total number of events examined significantly influences the usability of IDS. The ratio of false positives to false negatives may be an important security policy parameter and is indicative of the bias of the analysis implementation,

— Performance: the performance of IDS is the rate at which audit events are collected, stored, and processed. In case the performance of the IDS is poor, then real-time detection is not possible. Another aspect of performance refers to the network load an IDS may produce,

— Completeness: incompleteness occurs when the IDS fails to detect an attack. This measure is much more difficult to evaluate than the others, because it is impossible to have a global knowledge about attacks or abuses of privileges,

— Fault tolerance: an IDS should itself be resistant to attacks, particularly denial of service, and should be designed with this goal in mind. This is particularly important because most IDS run on top of commercially available operating systems or hardware, which are known to be vulnerable to attacks,

— Timeliness: an IDS has to perform and propagate its analysis as quickly as possible to enable the security officer to react before much damage has been done, and also to prevent the attacker from subverting the data, the data source, or the IDS itself.

A.7.1.2 Functionality

Another important consideration in deploying IDS is functionality over and above the functionality as discussed in the foregoing sections. Some functionality aspects are discussed below:

— Use in encrypted or switched environments - host-based IDS can be well suited for encrypted and switched environments. Since host-based systems reside on various hosts throughout an enterprise, they can overcome some of the deployment challenges faced by network-based IDS in switched and encrypted environments,

— Detecting attacks as they occur - network-based data sources permit real-time detection and response by providing data to detect malicious and suspicious attacks as they occur (e.g., a denial-of-service attack), and so provide faster notification and response. Network-based IDS can detect attacks that host based systems miss. Many IP-based Denial-of-Service and Fragmented-Packet attacks can only be identified by looking at the packet headers as they travel across a network,

— Combined analysis of host-based and network-based data - some IDS utilize data sources from both the host and from the network and thus has integrated host and network components. Network- and host-based IDS solutions each have unique strengths and benefits that complement each other as discussed in 6.1. Host- and network-based intrusion detection techniques can thus be combined in the analysis to create a more powerful information system defence.

A.7.1.3 Personnel for IDS Deployment and Operation

The IDS chosen may be the most advanced, and its subsystems may integrate very well with each other and with your IT system, service and/or network. However, most of the functions must be supported manually by individuals who are trained and knowledgeable about intrusion detection, IT security, including network security, and the organization's IT (including the network topology and configuration).

The intrusion detection process involves installing an IDS and having the human resources that can:

— Customize the IDS so that it looks for events that are relevant to the IT environment where it is deployed,

— Interpret what the IDS is telling you when an alarms goes off,

— Develop policies and procedures for responding to IDS alerts that appear to be real,

— Correct the vulnerabilities that caused the intrusion to be successful.

These manpower intensive operations go beyond the installation of an IDS and must be an integral part of the intrusion detection process.

The analysis function analyzes the data collected by the sensor for signs of unauthorized or suspicious activity or events that may be an indication that probing/scanning of the network is occurring, an intrusion has occurred or a malicious attack is underway. The automated portions cannot function without the aid of human input, configuration, interpretation of the output, and tuning of the IDS.

When an IDS is properly configured, it provides information that must be carefully analyzed in order to understand what intrusive behaviour is occurring in the network. An IDS requires intensive human interaction and does not quietly sit on the network rejecting unwanted packets. An IDS requires skilled individuals that can understand when an IDS output is something about which to be concerned versus just being a false positive (an activity is classified as an intrusion when it is a legitimate) or a false negative (an intrusive activity occurred, but was identified as non-intrusive).

The response function includes both automated tools and manual operations. For example, most IDS today categorize alerts according to some predefined severity criteria, but do little to indicate what should be done when an alert occurs. This situation is further compounded because most IDS today produce a high number of false positives and in most situations, the first level of response will involve fairly inexperienced operators. Even if an organization is fortunate to have operators who are knowledgeable and experienced, it is unlikely they will be knowledgeable about how to properly respond to every type of intrusion that is detected. On the other hand, it is very important to react to an IDS alert quickly and during periods of tension where events are unfolding very rapidly. For these and other reasons, it is extremely important to provide operators with well thought out guidelines that outline what steps should be taken for specific types of IDS alerts. In case these guidelines are not available, the response to an IDS alert may be inadequate, disorganized, or over-reactive. It is not prudent to be totally reliant on automated response mechanisms.

A.7.1.4 Other Implementation Considerations

Listed below are other characteristics that are important when considering the implementation, operation, integration, and selection of an IDS:

— user interfaces,

— placement of network sensors: network sensors can be placed flexibly to support a range of detection and response strategies, e.g. outside firewalls to detect attack attempts,

- system fault tolerance - system integrity is an overriding concern; denial-of-service is one example of attack. If possible the communications among IDS sensors, monitors, and managers should be on a separate network from that being monitored. This will enhance security and availability,
- assurance of the IDS,
- usability, i.e., ease of use,
- scalability of the IDS,
- interoperability with other security products,
- level and quality of vendor support,
- administration - IDS are not plug and play devices; a skilled staff is generally required to analyze and interpret the IDS outputs,
- hardware and software requirements,
- documentation,
- costs - besides the cost of the software, hardware, and installation, there are costs for education, training, operation, and maintenance.

A.8 Intrusion Detection Issues

A.8.1.1 Intrusion Detection and Privacy

Privacy has become an issue for the use of IDS. 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 behaviour. In case 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 considered 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.

The first aspect means that intrusion detection does not need to be used as an instrument for the supervision of the behaviour of employees.

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 the data should be strongly protected from access for many purposes, including privacy. 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 electronic notification.

A.8.1.2 Sharing of data on intrusions

There could be benefits to all organizations that are actively using IDS in the sharing of data about intrusions, and experiences of the use of IDS. For example, early warnings for some organizations of possible intrusions would be possible from analysis conducted on similar intrusions experienced by a number of other organizations, or information on a new type of intrusion would be highly useful to many. Information on experiences of using IDS could help other organizations to improve their IDS operations.

However, it is recognized that there are understandable concerns in most organizations about making public knowledge of intrusions that have affected their IT systems and thence their business operations. Such public knowledge could be at minimum be embarrassing and at maximum could have an effect on business, e.g., profitability, share price. With this in mind, the most appropriate advice is for organizations to participate in collaborative schemes whereby the source of information on intrusions and use of IDS and is sanitised and thus anonymised. Such schemes could be based on the collection of the anonymised knowledge and information in a data base designed to serve the IDS community. Such an intrusion detection database should be designed to:

- coordinate detailed information on vulnerable configurations, intrusion types and instructions to exploit these configurations,
- handle vast amounts of information about a particular intrusion sample to make correct statements about an intrusion type in terms of prerequisites, impact, traces, difficulty, remedies, etc.,
- store technical data about intrusion types and share the primary distinction between two types if their observable traces differ in a significant way,
- ensure trace information is structured in a format that will support downloading of new intrusion descriptions,
- update new rules and/or change parameters when new types of vulnerabilities are discovered,
- be capable of extracting information needed to automatically generate new rules (signatures, parameters, etc.) that identifies new intrusions.

An IDS database could be compared to modern virus detection systems, which often have automatic network-based update functionality.

The intrusion database is not meant to be a database of intrusion incidents where evidence concerning attack cases is stored.

Bibliography

[1] ISO/I EC 13335-1: 2004, *Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management*

[2] ISO/I EC 15408 (all parts), *Information technology— Security techniques— Evaluation criteria for IT security*

[3] ISO/I EC 17799, *Information technology— Security techniques— Code of practice for information security management*

[4] ISO/I EC 18028-1, *Information technology— Security techniques — IT network security — Parti: Network security management* (to be published)

[5] ISO/I EC 18028-2:2006, *Information technology — Security techniques — IT network security — Part 2: Network security architecture*

[6] ISO/I EC 18028-3:2005, *Information technology— Security techniques— IT network security — Part 3: Securing communications between networks using security gateways*

[7] ISO/I EC 18028-4:2005, *Information technology— Security techniques— IT network security — Part 4: Securing remote access*

[8] ISO/I EC 18028-5, *Information technology— Security techniques— IT network security— Part 5: Securing communications across networks using virtual private networks*

[9] ISO/IEC TR 18044:2004, *Information technology— Security techniques— Information security incident management*

[10] ISO/IEC 20000 (all parts), *Information technology— Service management*

ICS 35.040
Price based on 46 pages