INTERNATIONAL STANDARD

ISO/IEC 18043

First edition
2006-06-15

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

Technologies de l'information — Techniques de sécurité — Sélection, déploiement et opérations des systèmes de détection d'intrusion

Reference number
ISO/IEC 18043:2006(E)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

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

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

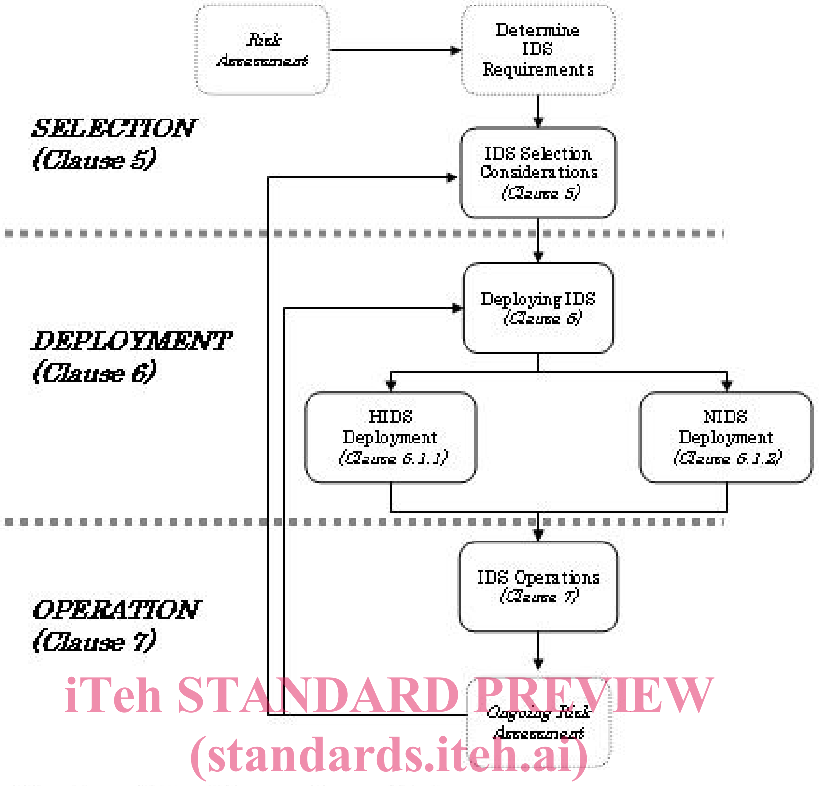
An organization should understand that the source of information and the different analysis approaches may result in both advantages and disadvantages or limitations, which can impact the ability or inability to detect specific attacks and influence the degree of difficulty associated with installing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


Risk Assessment
Determine IDS Requirements
SELECTION (Clause 5)
IDS Selection Considerations (Clause 5)
Deploying IDS (Clause 6)
DEPLOYMENT (Clause 6)
HIDS Deployment (Clause 6.1.1)
NIDS Deployment (Clause 6.1.2)
IDS Operations (Clause 7)
OPERATION (Clause 7)
Ongoing Risk Assessment

Note: Boxes with dotted line are out of scope of this document.

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.