INTERNATIONAL STANDARD

ISO/IEC 27039

First edition
2015-02-15

Corrected version
2016-05-01

Information technology — Security techniques — Selection, deployment and operations of intrusion detection and prevention systems (IDPS)

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

Reference number
ISO/IEC 27039:2015(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT), see the following URL: Foreword — Supplementary information.

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Security techniques*.

This first edition of ISO/IEC 27039 cancels and replaces ISO/IEC 18043:2006, which has been technically revised.

This corrected version of ISO/IEC 27039:2015 incorporates the following corrections.

The title of this document has been corrected with the addition of the words 'and prevention'.

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 (SP800-94 rev1, July 2012) in the development of the ISO/IEC 27039 International Standard. However, the NIST retains the right to use, copy, distribute, or modify the SP800-94 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 modification, risk retention, risk avoidance, risk sharing) should be implemented to prevent similar intrusions in the future. Organizations should also recognize and deter 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 and prevention systems (IDPS) to fulfil these needs. The general use of IDPS continues to expand with a wider range of IDPS 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 IDPS, the process of IDPS 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 IDPS 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 IDPS selection, deployment, and operation, as well as fundamental knowledge about IDPS. 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 Series.

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 27002:

   — 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 IDPS 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, IDPS services or products certification.

Information technology — Security techniques — Selection, deployment and operations of intrusion detection and prevention systems (IDPS)

1 Scope

This International Standard provides guidelines to assist organizations in preparing to deploy intrusion detection and prevention systems (IDPS). In particular, it addresses the selection, deployment, and operations of IDPS. It also provides background information from which these guidelines are derived.

2 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 and the following apply.

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

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

Note 1 to entry: This can also be referred to as an attack pattern.

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

Note 1 to entry: See *remote attestation* (2.23).

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
denial-of-service
DoS
unauthorized access to a system resource or the delaying of system operations and functions, with resultant loss of availability to authorized users

[SOURCE: ISO/IEC 27033-1:2009]

2.7
distributed denial-of-service attack
DDoS
unauthorized access to a system resource or the delaying of system operations and functions in the way of compromising multiple systems to flood the bandwidth or resources of the targeted system, with resultant loss of availability to authorized users

2.8
demilitarized zone
DMZ
logical and physical network space between the perimeter router and the exterior firewall

Note 1 to entry: The DMZ can be between networks and under close observation but does not have to be so.

Note 2 to entry: They are generally unsecured areas containing bastion hosts that provide public services.

2.9
exploit
defined way to breach the security of information systems through vulnerability

2.10
firewall
type of 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 traverses to another, and vice versa, and only authorized traffic as defined by the local security policy is allowed to pass

[SOURCE: ISO/IEC 27033-1:2009]

2.11
false positive
IDPS alert when there is no attack

2.12
false negative
no IDPS alert when there is an attack

2.13
honeypot
generic term for a decoy system used to deceive, distract, divert, and 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

2.14
host
addressable system or computer in TCP/IP-based networks like the Internet

2.15
intruder
individual who is conducting, or has conducted, an intrusion or attack against a victim's host, site, network, or organization

2.16
intrusion
unauthorized access to a network or a network-connected system, that is, deliberate or accidental unauthorized access to information systems, to include malicious activity against information systems, or unauthorized use of resources within information systems

2.17
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

2.18
intrusion detection system
IDS
information systems used to identify that an intrusion has been attempted, is occurring, or has occurred

2.19
intrusion prevention system
IPS
variant on intrusion detection systems that are specifically designed to provide an active response capability

2.20
intrusion detection and prevention system
IDPS
intrusion detection systems (IDPS) and intrusion prevention systems (IPS) software applications or appliances that monitor systems for malicious activities, where IDS focus is to only alert on the discovery of such activity while IPS have the potent to prevent some intrusions upon detection

Note 1 to entry: IPS is deployed actively in the network if attack prevention is desired. If deployed in passive mode, it will not offer such functionality and effectively function as a regular IDS by providing alerts only.

2.21
penetration
unauthorized act of bypassing the security mechanisms of information systems

2.22
provisioning
process of loading the correct software, security policy, and configuration data for information technology (IT) devices

2.23
remote attestation
processes of using digital certificates to ensure the identity, as well as the hardware and software configuration, of IDPS and to securely transmit this information to a trusted operations centre

2.24
response
incident response or intrusion response
action taken to protect and restore the normal operational conditions of information systems and the information stored in it when an attack or intrusion occurs

2.25
router
network device that is used to establish and control the flow of data between different networks, by selecting paths or routes based upon routing protocol mechanisms and algorithms

Note 1 to entry: The networks can themselves be based on different protocols.

Note 2 to entry: The routing information is kept in a routing table.

[SOURCE: ISO/IEC 27033-1:2009]

2.26
server
computer system or program that provides services to other computers

2.27
Service Level Agreement
SLA
document 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

2.28
sensor
component/agent of IDPS which collects event data from information systems or a network under observation

Note 1 to entry: Also referred to as a monitor.

2.29
subnet
segment of a network that shares a common address component

2.30
switch
device which provides connectivity between network connectivity devices by means of internal distribution mechanisms, with the switching technology typically implemented at layer 2 or layer 3 of the OSI reference model

Note 1 to entry: 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.

[SOURCE: ISO/IEC 27033-1:2009]

2.31
test access port
TAP
typically passive devices that do not install any overhead on the network packet but 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

Note 1 to entry: A TAP also gives the functionality of multiple ports so network issues can be debugged without losing the IDPS capability.

2.32
trojan horse
malicious program that masquerades as a benign application

2.33
virus
type of malware which is software designed with malicious intent containing features or capabilities that can potentially cause harm, directly or indirectly, to the user and/or the user's system

2.34
virtual private network
VPN
restricted-use logical computer network that is constructed from the system resources of a physical network by using encryption and/or by tunnelling links of the virtual network across the real network

[SOURCE: ISO/IEC 18028-3:2005]

2.35
vulnerability
weakness of an asset or control that can be exploited by one or more threats

[SOURCE: ISO/IEC 27000:2012]

3 Background

The purpose of intrusion detection and prevention system (IDPS) is passively monitoring, detecting and logging inappropriate, incorrect, suspicious or anomalous activity that may represent an intrusion and provide an alert and/or an automated response when these activities are detected. It is the responsibility of the appointed IT Security personnel to actively review IDPS alerts and associated logs in order to make decisions on adequate responses. When an organization needs to detect promptly intrusions to the organization's information systems and responds appropriately to them, an organization should consider deploying IDPS. An organization can deploy IDPS by getting IDPS software and/or hardware products or by outsourcing capabilities of IDPS to an IDPS service provider.

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

Fundamental knowledge about IDPS is mainly presented in Annex A. This annex explains the characteristics of different types of IDPS:

— Network-based, which monitors network traffic for particular network segments or devices and analyses the network and application protocol activity to identify suspicious activity;

— Host-based, which monitors the characteristics of a single host and the events occurring within that host for suspicious activity as well as three basic approaches for detection analysis, i.e. signature-based detection, statistical anomaly-based detection, stateful protocol analysis detection.

Behavioural analysis applies to network-based and host-based IDPS. This approach examines network traffic and host activities to identify threats that generate abnormal behaviour, such as distributed denial of service (DDoS) attacks, brute force attacks, certain forms of malware, and policy violations (e.g. a client system providing network services to other systems).

A host-based intrusion detection and prevention system (HIDPS) derives its source of information from one or more hosts, while a network-based intrusion and prevention system (NIDPS) derives its information from traffic of one or more network segments. 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 deemed intrusive or malicious. The anomaly-based approach attempts to detect intrusions by discovering significant deviations from normal behaviour 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 IDPS.

4 General

IDPS 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 IDPS has its strengths and limitations; together they can provide better security event coverage and alert analysis.

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

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

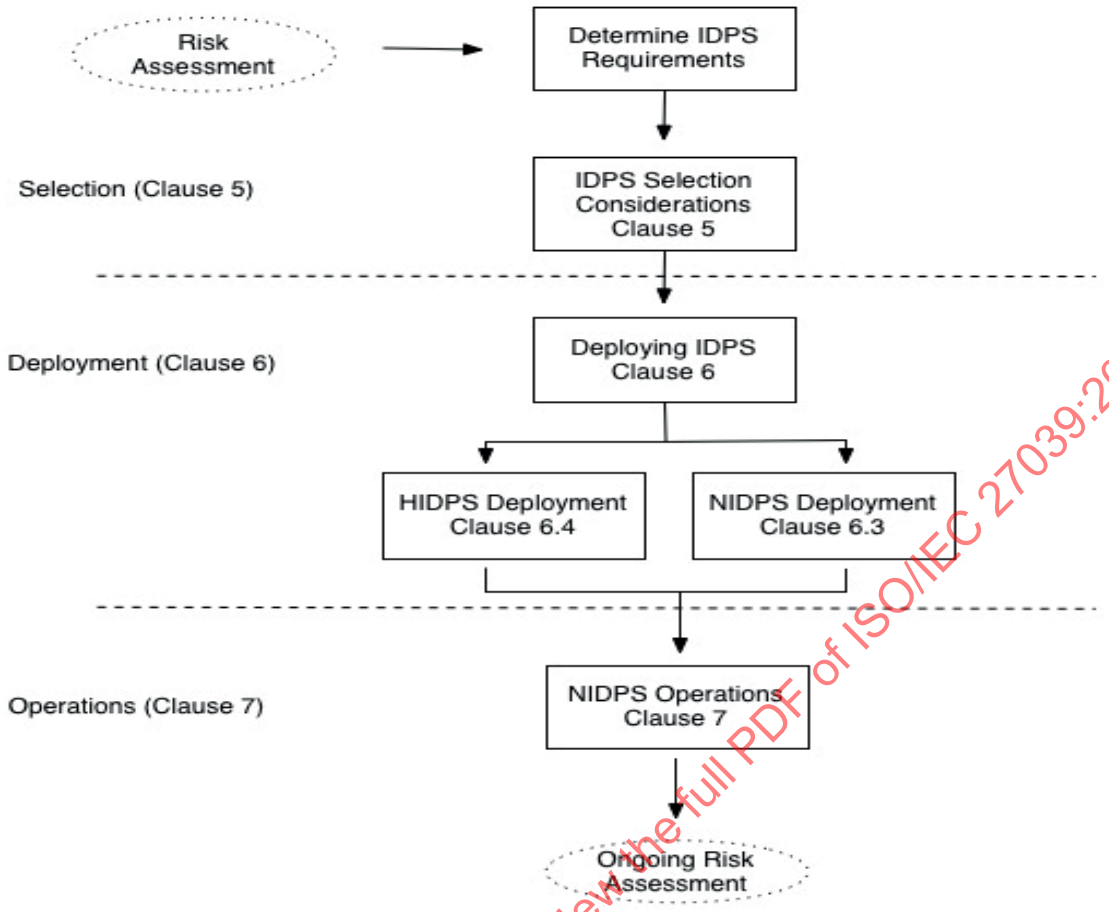

Figure 1 — Selection, deployment, and operations of IDPS

5 Selection

5.1 Introduction

There are many IDPS products and products families 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 IDPS products to choose from, the process of selecting IDPS that represents the best fit for an organization's needs is difficult. Furthermore, there may be limited compatibility between various IDPS 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 IDPS and the integration of these diverse IDPS can be very challenging.

Vendor brochures may not describe how well an IDPS 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 IDPS can perform and avoid false positives and negatives. Also the proactive and reactive capabilities of an IDPS need to be assessed independently and mapped to organizational requirements. This should include the need for deep packet inspection and reassembly versus the need for network performance and cost considerations. Consequently, relying on vendor provided information about IDPS capabilities is neither sufficient nor recommended.

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

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

5.2 Information security risk assessment

Prior to the selection of an IDPS, 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 IDPS.

NOTE Information security risk assessment and management is the subject of International Standard (ISO/IEC 27001).

Once the IDPS is installed and operational an on-going 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.

5.3 Host or Network IDPS

5.3.1 Overview

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

Each option has its own advantages and disadvantages. For example, in the case where an IDPS is deployed outside an external firewall, an IDPS 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.

5.3.2 Host-based IDPS (HIDPS)

The choice of a HIDPS 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 HIDPS on critical hosts only. Therefore the deployment of HIDPS should be prioritized according to risk analysis results and cost-benefit considerations. An organization should deploy an IDPS capable of centralized management and reporting functions when HIDPS is deployed on all or a significant number of hosts.

5.3.3 Network-based IDPS (NIDPS)

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

— Inside external firewalls;

— Outside external firewalls;

— On major network backbones;

— Between trust boundaries.

5.4 Considerations

5.4.1 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 IDPS 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;

— Return paths that are not the same as the incoming connection path, i.e. asymmetric data flow.

5.4.2 Security protection mechanisms

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 (VPNs);

— Any other installed security mechanisms.

5.4.3 IDPS security policy

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

— What information assets are to be monitored?

— What is the policy for fail-open and fail-closed conditions?

— What type of IDPS is needed?

— Where can the IDPS 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 IDPS security policy represents the goals the organization has for the IDPS investment. This is the initial step in attempting to gain the maximum value from the IDPS asset.

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

A review of the existing organization security policy should provide a template against which the requirements of the IDPS 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 IDPS 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 IDPS 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 IDPS 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 27035.

5.4.4 Performance

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

— What bandwidth needs to be processed by the IDPS?

— What level of false alarms can be tolerated when operating at that bandwidth?

— Can the cost of a high speed IDPS be justified or can a moderate or slow IDPS suffice?

— What are the consequences of missing a potential intrusion because of IDPS performance limitations?

— What is the performance impact when deep packet inspection and reassembly occurs?

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 IDPS 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 IDPS 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 is likely to be associated with those assets. This is generally accomplished through a risk assessment process.

— Performance of most IDPS 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 IDPS to look for only attack signatures associated with web traffic.

— Proper load balancing configuration can allow the signature based IDPS to work much faster and more thoroughly because the signature based IDPS 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 IDPS 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 IDPS technology is reaching gigabits speed and as a result the benefits versus cost of load balancing may be minimal.

5.4.5 Verification of capabilities

Reliance on vendor provided information about the capabilities of IDPS is generally not sufficient. An organization should request additional information and perhaps a demonstration of the suitability of a particular IDPS to the organization's environment and security goals. Most IDPS 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 IDPS vendor the following questions:

— What assumptions were made regarding the applicability of the IDPS to specific environments?

— What are the details of the tests that were performed to verify the assertions about the IDPS capabilities?

— What assumptions were made regarding IDPS operators?

— What IDPS 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 IDPS interface be configured with shortcut keys, customizable alarm features, and custom attack signatures on the fly?

— In the case where the IDPS 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 IDPS product adapt to an expanding and increasingly diverse network?

— Does the IDPS provide fail-safe and fail-over capabilities and how do these capabilities integrate with the same capabilities at the network link layer?

— Does the IDPS use a dedicated network for the alarms or are they transmitted in the same network that it monitors?

— What is the vendor's reputation in terms of quality assurance, response to vulnerabilities discovered and product's performance record?

5.4.6 Cost

The acquisition of IDPS is not the only actual cost of ownership. Additional costs include: acquisition of a system to run the IDPS software, specialized assistance in installing and configuring the IDPS, personnel training, and maintenance costs. Personnel to manage the system and to analyse the results are the largest cost. A useful technique for measuring the IDPS 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 IDPS 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 IDPS benefits include:

— Identification of defective or misconfigured equipment;

— Verification of configurations on the fly;

— Providing early system usage statistics.

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

— What is the budget for the initial capital expenditure to purchase the IDPS?

— What is the required time period for IDPS operations e.g. 24/7 or less?

— What infrastructure is needed to process, analyse and report the IDPS outputs and what can it cost?

— Does the organization have the human and other resources required to configure the IDPS to the organization's security policy, to operate, maintain, update, monitor the outputs of the IDPS and respond to alerts? If not, how can these functions be accomplished?

— Are funds available for IDPS training?

— What is the scale of deployment and if HIDPSs are used how many hosts will be protected?

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

The most expensive part of an IDPS 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.

5.4.7 Updates

5.4.7.1 Overview

The majority of IDPS are attack signature based and the value of the IDPS is only as good as the attack signature database against which events are analysed. New vulnerabilities and attacks are being discovered frequently. Consequently, the IDPS 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.

5.4.7.2 Timeliness of updates for signature-based IDPS

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 IDPS 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 on-going attack?

5.4.7.3 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 across enterprise network trust boundaries:

— 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?

5.4.7.4 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.

5.4.8 Alert strategies

The IDPS configuration and operation should be based on an organization's monitoring policy. At a minimum, an organization should ensure that IDPS could 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 IDPS data is used for forensic purposes, including prosecutions and evidence for internal discipline, IDPS 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.

5.4.9 Identity management

5.4.9.1 Overview

Identity management is a critical foundation for realizing IDPS 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 IDPS data and IDPS identity exchange across enterprise network trust boundaries.

5.4.9.2 Remote attestation

IDPS 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 IDPS output. Consequently, strict authenticated access-control over the IDPS 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 IDPS user's request, be provided to any remote party, and in principle has the effect of proving to that party that the IDPS is using expected and unaltered software. If the software on the IDPS has been altered, the certificate generated will reflect that the IDPS code base has changed.

In the case of IDPS, the aim of remote attestation is to detect unauthorized changes to IDPS software. For example, if an attacker has replaced or modified one of the IDPS applications, or a part of IDPS 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 IDPS software by a virus or Trojan can be detected by a remote party (e.g. Network Operations Centre), which can then act on this information. Because the attestation is "remote", others with whom the IDPS interact with should also be able to tell that a particular IDPS has been compromised. Thus, they can avoid from sending information to it, until it has been fixed.

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

5.4.9.3 Provisioning

When remote attestation detects a problem in the IDPS, corrective action is needed to mitigate the problem. This can be achieved by allowing a NOC (Network Operations Centre) to push authenticated configuration, software updates and patches to the IDPS. 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 IDPS. The goal of provisioning is to do as much remotely as possible. This both saves the cost of manpower to physically visit individual IDPS and allows for more timely mitigation of problems, especially attack signature updates. To be effective, the IDPS provisioning capability needs to be securely pushed from a NOC as well as securely pulled by the IDPS. In the latter situation, IDPS 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.

5.5 Tools that complement IDPS

5.5.1 Overview

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

Examples of such devices and tools include:

— File integrity checkers

— Firewalls or security gateway

— Honeypots

— Network management tools

— Security Information and Event Management (SIEM) tools

— Virus/Content protection tools

— Vulnerability assessment tools

5.5.2 File integrity checkers

File integrity checkers are another class of security tools that complement IDPS. 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 information systems or at least the system being verified be taken off line and powered down during the analysis.

5.5.3 Firewall

The primary role of a firewall (see, e.g., ISO/IEC 27033-2) 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 NIDPS 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 NIDPS 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 NIDPS alarm can be used to produce a change in the filtering parameters of the firewall if desirable.

In the case that a NIDPS 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 NIDPS. This NIDPS configuration can greatly enhance the NIDPS accuracy because the Internet background noise due to scanning activity can be removed while controlling the incoming traffic.

5.5.4 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 analysing 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 IDPS operations. By analysing the actions of an intruder within the honeypot system, this information can contribute to the development of an organization's IDPS policy, attack signatures database and the overall approach of the organization towards IDPS best practices in protecting against the analysed 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;

— 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.

5.5.5 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 IDPS alerts may help the IDPS operator appropriately process alerts and evaluate their impact on the systems being monitored.

5.5.6 Security Information Event Management (SIEM) tools

Organizations use a SIEM to consolidate reporting to one management and alert console. A SIEM can collect information from IDPS, 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 IDPS.

Security Information and Event Management (SIEM) tools may also be used to process data obtained by an IDPS. Typically, SIEM 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 IDPS, 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;

— event correlation by building context between security and even non-security related events to detect security breaches that are not pattern related;

— event filtering by mitigating alert levels based on correlation due to relevance, e.g. IDPS alerts and security patch levels;

— event aggregation by collecting and normalizing events based on e.g. source, destination, timestamp and event description etc. to mitigate IDPS alert overflows;

— 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 SIEM 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 SIEM 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 SIEM tool. As with IDPS systems, configuration requires a high degree of expertise and a remarkable amount of work. Given proper set-up and configuration, SIEM tools can provide a high added value, and especially can provide valuable information to trigger further processes and activities like incident management.

5.5.7 Virus/Content protection tools

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

5.5.8 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 IDPS 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 IDPS to detect the vulnerability assessment activity does not indicate that the IDPS cannot detect the attack. Conversely, detection of the vulnerability scanning activity by the IDPS does not mean that the same IDPS can properly detect the attack.

Vulnerability assessment tools are used to test the susceptibility of a network host to compromise. The use of vulnerability assessment tools in conjunction with IDPS provides an invaluable method for examining the effectiveness of the IDPS, 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 IDPS 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;

— Allows organizations to match attack data with known vulnerabilities to determine if the attack was successful;

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 IDPS, vulnerability assessment tools are subject to false positives or false negatives and should be analysed carefully;

— Repeated vulnerability assessments can train many anomaly-based IDPS 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.

5.6 Scalability

An organization should investigate the scalability of specific IDPS before committing to using IDPS. Many IDPS 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 IDPS are not able to scale to large or widely distributed enterprise network environments.

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

5.7 Technical support

Like other systems, IDPS require maintenance and support. IDPS are not "plug and play" technologies. Many vendors provide expert assistance to customers in installing and configuring IDPS. 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 IDPS vendor and is implemented on a case-by-case basis. At a minimum, technical support should include vendor assistance in tuning or adapting IDPS to accommodate special organizational needs, whether they are monitoring a custom or legacy system within an enterprise, or reporting IDPS 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.

5.8 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 IDPS. The demand for qualified IDPS 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 IDPS responsibilities. Due to this situation, many organizations decide to outsource the IDPS operations to a security management service. This option presents its own organizational training issues and risk. For example, even in the case that most on-going functions are outsourced, an organization should train personnel with significant knowledge about IDPS issues and operations or it can lose control of the IDPS process to others. In order for the organization to make optimal use of the IDPS, the organization's personnel responsible for oversight of the IDPS outsourcing operations should become familiar with IDPS operations and procedures. This type of training is generally available from vendors who provide IDPS products. An organization should include this type of vendor training as part of the IDPS purchase cost.

In the case that the IDPS vendor does not provide training as part of the IDPS 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 IDPS and its environment.

6 Deployment

6.1 Overview

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

— A thorough requirements analysis, to include IDPS security needs, based on a risk assessment;

— Careful selection of an IDPS deployment strategy;

— Identification of a solution that is compatible with the organization's network infrastructure, policies, and resource level;

— Specialized IDPS maintenance and operations training;

— Documenting the training and rehearsing procedures for handling and responding to IDPS alerts.

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

6.2 Staged deployment

Organizations should consider a staged deployment of IDPS. This approach can allow personnel to gain experience and to ascertain how many monitoring and maintenance resources can be required to support the IDPS operations. The resource requirements for each type of IDPS 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 IDPS. NIDPS are usually the simplest to install and maintain. The next step is to protect critical servers with host-based IDPS. Further, an organization should use vulnerability assessment tools on a regular schedule to test IDPS and other security mechanisms for proper function and configuration.

6.3 NIDPS deployment

6.3.1 Overview

As with a HIDPS, an organization should ensure that operators are accustomed with a NIDPS in a controlled, but active test and training environment. Various positions of the NIDPS sensors can be experimented with before full-scale deployment on an operational network. The common positions of NIDPS 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.

Additionally, especially in high speed network environments, the level of dropped IP packets needs to be observed as high level drop rates can severely increase the amount of pattern mismatching, resulting in increased false positives or even false negatives. As a remedy appropriate network interface cards offering higher capture rates or similar technologies mitigating packet drop may be required to insure effectiveness.

When deploying a NIDPS 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 NIDPS and not a VLAN or similar technology on a core switch. Switches typically can only allow a single Switch Port Analyser (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 IDPS become non-functional. An organization should dedicate this port to the function of the NIDPS. 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 IDPS capability.

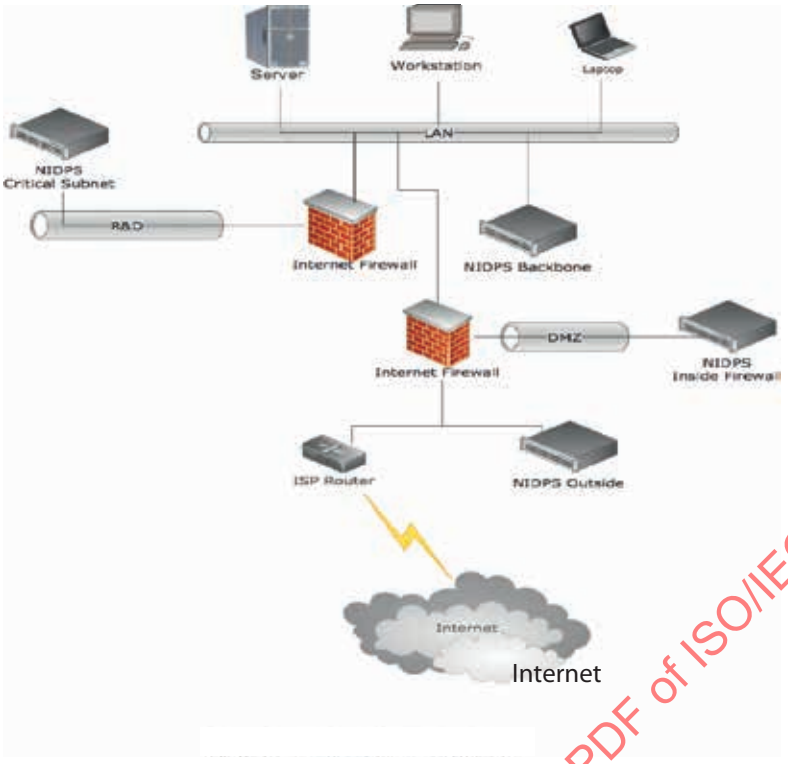

Figure 2 — Typical NIDPS locations

6.3.2 Location of NIDPS 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.

6.3.3 Location of NIDPS 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 IDPS located inside the external firewall, this IDPS 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 IDPS collected data extremely difficult.

— Interaction between the IDPS sensor and the management console may require additional holes in the firewall, resulting in possible external access to the management console.

6.3.4 Location of NIDPS 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 IDPS 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;

— IDPS 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.

6.3.5 Location of NIDPS 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, IDPS related traffic might increase network loading on critical subnets;

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

6.4 HIDPS deployment

Before the operational deployment of a HIDPS an organization should ensure that operators become familiar with its features and capabilities in a sheltered, but active, environment. The effectiveness of any IDPS, but particularly a HIDPS, 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 HIDPS. Since HIDPS are typically not continuously monitored, an organization should establish a schedule for checking the IDPS outputs. This mode of HIDPS operation should significantly reduce the risk that an attacker can tamper with the HIDPS in the course of an attack.

The full-scale deployment of HIDPS should commence with critical servers. Once the operation of HIDPS is routine, other servers may be considered for HIDPS deployment. Installing HIDPS on every host in the organization can be expensive and time-consuming, as each IDPS should be installed and configured for each specific host. Therefore, organizations should first install HIDPS 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 HIDPS operation becomes routine, an organization may want to revisit the initial information security risk assessment results and consider installing more HIDPS. An organization should employ HIDPS that have centralized management and reporting functions. These features can significantly reduce the complexity of managing alerts from the HIDPS that are deployed throughout the organization. In the case that significant numbers of HIDPS are deployed, an organization may want to consider outsourcing the HIDPS operations and maintenance to an information security management service.

6.5 Safeguarding and protecting IDPS information security

The IDPS 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 IDPS 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 IDPS database sufficiently to resist penetrations;

— Sniffing (receive only) cables to connect the IDPS to the Ethernet hub or switch;

— Implementation of a separate IDPS management network;

— Regular vulnerability assessment and penetration testing on the IDPS and connected systems.

Logs should also be stored on a separate log host and not on the local system. IDPS logs, configuration, attack signature and information exchanged between IDPS sensors and collectors, should be protected against unauthorized modification or deletion.

IDPS logs may contain sensitive or privacy related information and should be protected in storage and transmission. Authorized persons responsible for analysing information from IDPS sensors or collectors should safeguard the information.

7 Operations

7.1 Overview

Prior to the IDPS operations phase, an organization should:

— Establish processes, procedures, and mechanisms that ensure the IDPS is covered by the organizations vulnerability management process;

— Prepare an incident management process in accordance to ISO/IEC 27035;

— Define actions that should be taken when an IDPS 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.

7.2 IDPS tuning

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

Most IDPS 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 IDPS installation and some sense of the behaviour of the IDPS within the organization's environment.

As outlined previously, the use of SIEM technology may be of great value in prioritizing and mitigating IDPS alerts, e.g. comparison of vulnerability assessment data and system patch levels with IDPS alert configuration. In this context the use of network discovery tools and traffic analyser may add further value and allow for further tuning of alert rules.

In some situations, an organization should delay activating the full suite of alarm features until an adequate trial period has revealed the best balance of operational requirements and alert possibilities, to ultimately allow for the customization of alert rules and response capabilities. The organization can then decide which features are unnecessary, which ones are more helpful than others, and which ones can benefit their organization the most. In cases where the alarm and response features include automated response to attacks, specifically those that allow the IDPS 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 IDPS feature to deny access to legitimate users, i.e. a self-inflicted denial of service attack. Initially, these types of IDPS features should be placed in a semi-automated mode in which a human should decide if the IDPS response should be activated.

7.3 IDPS vulnerabilities

The unsecured implementation of an IDPS 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 IDPS. The attackers are likely to attempt to disable the IDPS or force it to provide erroneous information. Additionally, many IDPS 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 IDPS sensors and console are implemented in a secure fashion and the potential weaknesses in the IDPS should be addressed.

7.4 Handling IDPS alerts

7.4.1 Overview

Typically, IDPS produces a great deal of output. In order to separate the trivial alerts from ones of a more serious nature, an organization should analyse the IDPS 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 IDPS 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.

7.4.2 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 27035.

7.4.3 Outsourcing

In addition to IDPS products, some security service providers offer managed IDPS services that include consultancy and operations centre 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 IDPS 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 IDPS 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 IDPS?

— 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 pre-set defaults?

— What technical measures are in place to enforce these agreements?

— What security vetting procedures of service provider staff is undertaken?

A well thought-out outsourcing SLA 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 IDPS procedures together and the time needed to follow-up on all the implementation details;

— While there is a need for an awareness of IDPS capabilities in an organization, there is no requirement to provide ongoing specialized training of employees in the latest IDPS 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.

7.5 Response options

7.5.1 Principles

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

7.5.2 Active response

An active response involves an automated action taken by the IDPS 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 IDPS share many similar functions such as packet inspection, protocol validation, attack signature matching, and stateful analysis. However, each device may be deployed for different purposes.

IPS represents the merger of protection capabilities with intrusion detection capabilities and makes it possible to first detect an attack and then protect against it in either a static or dynamic manner.

An IDPS is a passive device that monitors activities and looks for known attack signatures or abnormal situations. An IDPS is an offline device that is designed to tell what malicious activity is happening on a network. Due to the passive nature of IDPS, there are few opportunities for the IDPS 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 IDPS 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 HIDPS, 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 IDPS 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 should be very reliable, should not impact performance, and should not block legitimate traffic.

Advantages:

— Ability to detect and block attacks;

— Provides proactive protection;

— Increases operational efficiencies due to reduced need to react to IDPS 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 IDPS, 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.

7.5.3 Passive reaction

Passive responses provide information to operators or to a pre-specified location. They rely on the IDPS 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.

7.6 Legal Considerations

7.6.1 Overview

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 IDPS.

7.6.2 Privacy

In the course of normal operation, an IDPS 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 IDPS.

7.6.3 Other legal and policy considerations

Implementation and operation of IDPS may be subject to other legal and regulatory requirements as well as the policy requirements of the organization where the IDPS are deployed. Legal, regulatory, and organizational policy requirements should be reviewed and addressed when implementing and operating IDPS. Legal and regulatory aspects are further discussed in ISO/IEC 27035.

7.6.4 Forensics

IDPS 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 IDPS logs should be put in place to enable acceptable forensic scrutiny of the information. There may be additional requirements concerning documentation of IDPS systems and processes to meet forensic and evidentiary requirements.

Annex A
(informative)

Intrusion Detection and Prevention System (IDPS): Framework and issues to be considered

A.1 Introduction to intrusion detection

An organization needs to protect its information systems because there are organizational business reasons to use information systems and to connect them to the internet and other networks despite the fact that there are vulnerabilities in its information systems 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 27002. 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 (IDPS). In addition, feedback from the deployed IDPS can refine knowledge about vulnerabilities of the organization's information systems, which can help for the organization to improve the overall quality of information security.

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

Like every control, an organization needs to justify deployment of IDPS by information security risk assessment and integrate the deployed IDPS 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 IDPS, 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 IDPS. 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; and

— detect and response effectively from intrusions that may occur.

Like every control, an organization needs to justify deployment of IDPS by information security risk assessment and integrate the deployed IDPS 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 IDPS, the intruder or attacker can override it and make the organization confront enormous difficulties.

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

— types of intrusions and attacks to information systems and/or networks,

— generic model of IDPS proposed in this document.

A.2 Types of intrusions and attacks

A.2.1 Introduction

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

Vulnerabilities can permit the intruder and attacker to access protected information systems 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 systems 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 systems,

— 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) attacks, by which an attacker attempts to slow down or create an out of service condition for 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.2.2 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.2.3 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 the intrusion detection process

A.3.1 Introduction

IDPS consists of software and/or hardware products automatically monitor, collect and analyse suspicious events occurring in information systems 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.

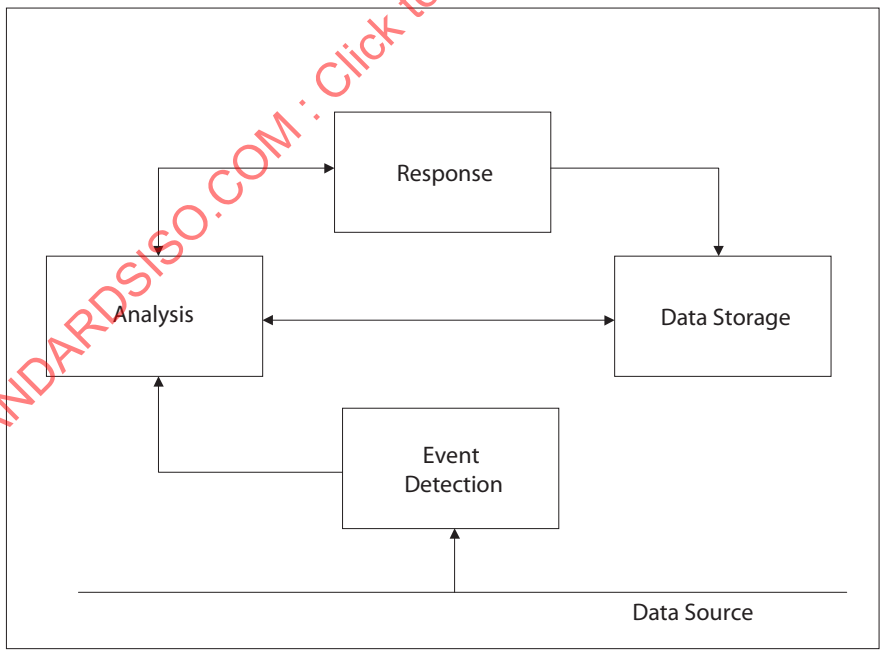

Figure A.1 — Generic model of intrusion detection

A.3.2 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 IDPS. 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 IDPS-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, IDPS can be also classified into two types: host-based and network-based. Host-based IDPS can examine audit trails/logs and other data from hosts or applications. Network-based IDPS can examine network management logs, as well as data from firewalls, switches, routers and IDPS-specific sensors agents.

A.3.3 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 IDPS. 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 IDPS. This situation can also be applied to the following analysis process.

A.3.4 Analysis

A.3.4.1 Introduction

The purpose of the analysis function is to analyse 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.3.4.2 Misuse-based approach

A.3.4.2.1 Overview

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 systems, as well as previous behaviours and actions that were deemed malicious or intrusive, as specific attack signatures, including systematically scanning information systems 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 IDPS.

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.3.4.2.2 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 an 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 IDPS-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.3.4.2.3 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.3.4.2.4 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.3.4.3 Anomaly-based approach

A.3.4.3.1 Overview

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.3.4.3.2 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.3.4.3.3 Expert systems

(Refer to A.3.3.1.2)

A.3.4.3.4 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.3.4.3.5 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.3.4.4 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 IDPS 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.3.4.5 Analysis frequency

A.3.4.5.1 Overview

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

Frequency of analysis may be

— continuous,

— periodical, and/or

— under special circumstances.

A.3.4.5.2 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.3.4.5.3 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 analyse 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.3.4.5.4 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 analyse 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.3.5 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.3.6 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 such as e-mail, text messages, telephone calls etc. in order to escalate and organize responses to the raised alerts.

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 27002. ISO/IEC 27035 also provides useful information about information security incident management.

A.4 Types of IDPS

A.4.1 Introduction

As previously mentioned, there are three types of IDPS: Signature-based IDPS, Anomaly-based IDPS, stateful protocol analysis IDPS. Most IDPS use multiple detection methodologies, either separately or integrated, to provide more broad and accurate detection. The primary classes of detection methodologies are as follows:

Signature-based, which compares known threat signatures to observed events to identify incidents. This is very effective at detecting known threats but largely ineffective at detecting unknown threats and many variants on known threats. Signature-based detection cannot track and understand the state of complex communications, so it cannot detect most attacks that comprise multiple events.

Anomaly-based detection, which compares definitions of what activity is considered normal against observed events to identify significant deviations. This method uses profiles that are developed by monitoring the characteristics of typical activity over a period of time. The IDPS then compares the characteristics of current activity to thresholds related to the profile. Anomaly-based detection methods can be very effective at detecting previously unknown threats. Common problems with anomaly-based detection are inadvertently including malicious activity within a profile, establishing profiles that are not sufficiently complex to reflect real world computing activity, and generating many false positives.

Stateful protocol analysis, which compares predetermined profiles of generally accepted definitions of benign protocol activity for each protocol state against observed events to identify deviations. Unlike anomaly-based detection, which uses host or network-specific profiles, stateful protocol analysis relies on vendor-developed universal profiles that specify how particular protocols should and should not be used. It is capable of understanding and tracking the state of protocols that have a notion of state, which allows it to detect many attacks that other methods cannot. Problems with stateful protocol analysis include that it is often very difficult or impossible to develop completely accurate models of protocols, it is very resource-intensive, and it cannot detect attacks that do not violate the characteristics of generally acceptable protocol behaviour.

There are other types of IDPS:

— application-based IDPS (AIDPS), but it is a special class of HIDPS and have characteristics similar to HIDPS.

In general, IDPS 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, and

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

IDPS 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 IDPS output,

— difficulty to integrate different IDPS 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 IDPS not anomaly based IDPS),

— 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 IDPS 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 IDPS alerts can cause security and availability problems,

— requires in-depth technical and systems knowledge to use effectively.

A.4.2 Host-based IDPS (HIDPS)

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

Operating system audit trails, which HIDPS 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 HIDPS are designed to support a centralized IDPS 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 NIDPS, HIDPS 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, HIDPS permits the detection of attacks from the keyboard of a mission-critical server.

HIDPS 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 IDPS.

HIDPS have unique limitations that should be understood. Significant limitations include

— possibility that certain DoS attacks can disable HIDPS,

— possibility that HIDPS 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.4.3 Network-based IDPS (NIDPS)

NIDPS monitors the traffic destined for host systems on a network. NIDPS 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 IDPS component, they can be more easily secured against

