TECHNICAL REPORT

ISO/IEC TR 15947

First edition
2002-10-15

Information technology — Security techniques — IT intrusion detection framework

Technologies de l'information — Techniques de sécurité — Cadre de détection de l'intrusion dans les systèmes des technologies de l'information

Reference number
ISO/IEC TR 15947:2002(E)

© ISO/IEC 2002

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

PDF disclaimer

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

Adobe is a trademark of Adobe Systems Incorporated.

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

© ISO/IEC 2002

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

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

Printed in Switzerland

--`,,`-`-`,,`,,`,`,,`---

::

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

© ISO/IEC 2002 – All rights reserved

Not for Resale

TECHNICAL REPORT

ISO/IEC TR 15947

First edition
2002-10-15

Information technology — Security techniques — IT intrusion detection framework

Technologies de l'information — Techniques de sécurité — Cadre de détection de l'intrusion dans les systèmes de technologies de l'information

Reference number
ISO/IEC TR 15947:2002(E)

© ISO/IEC 2002

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

PDF disclaimer

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

Adobe is a trademark of Adobe Systems Incorporated.

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

© ISO/IEC 2002

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

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

Printed in Switzerland

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

© ISO/IEC 2002 – All rights reserved

Contents

1 Scope....1
2 References....2
3 Terms and Definitions....2
4 Introduction to Intrusion Detection....2
4.1 The Need for Intrusion Detection....2
4.2 Types of Attacks....3
4.2.1 Host-based Attacks....4
4.2.2 Network-based Attacks....4
5 Generic Model of Intrusion Detection Process....4
5.1 Data Sources....5
5.2 Event Detection....6
5.3 Analysis....6
5.4 Response....7
5.5 Data Storage....7
6 Characteristics of Intrusion Detection....7
6.1 Data Source....8
6.1.1 Host-based....8
6.1.2 Network-based....9
6.2 Event Detection and Analysis Frequency....9
6.2.1 Continuous/Near Real-Time....9
6.2.2 Periodically/Batch Processed....9
6.2.3 Initiated Only Under Special Circumstances....9
6.3 Intrusion Detection Analysis....9
6.3.1 Misuse-based....10
6.3.2 Anomaly-based....10
6.4 Response Behavior....10
6.4.1 Passive....10
6.4.2 Active....10
7 Architecture Considerations....11
8 Management of an IDS....12
8.1 Configuration Management....12
8.1.1 Detection Function....12
8.1.2 Response Function....12
8.2 Security Services Management....12
8.3 Integration with Other Management Systems....12
8.4 Security of Management Operations....13
8.4.1 Authentication....13
8.4.2 Integrity....13
8.4.3 Confidentiality....13
8.4.4 Availability....13
8.5 Management Model....13
9 Intrusion Detection Analysis....14
9.1 Signature Analysis....14
9.2 Statistical Approach....15
9.3 Expert Systems....16
9.4 State-transition Analysis....16
9.5 Neural Networks....16
9.6 User Anomalous Behavior Identification....16
9.7 Hybrid Analysis....16
9.8 Other....16
10 Implementation and Deployment Issues....17
10.1 Efficiency....17
10.2 Functionality....17

© ISO/IEC 2002 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

10.3 Personnel for IDS Deployment and Operation....18
10.4 Other Implementation Considerations....18
11 Intrusion Detection Issues....19
11.1 Intrusion Detection and Privacy....19
11.2 Sharing of data on intrusions....20
11.3 Future Standardization....21
12 Summary....21
Bibliography....22

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
© ISO/IEC 2002 – All rights reserved
Not for Resale

Foreword

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

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 3.

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

In exceptional circumstances, the joint technical committee may propose the publication of a Technical Report of one of the following types:

— type 1, when the required support cannot be obtained for the publication of an International Standard, despite repeated efforts;

— type 2, when the subject is still under technical development or where for any other reason there is the future but not immediate possibility of an agreement on an International Standard;

— type 3, when the joint technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example).

Technical Reports of types 1 and 2 are subject to review within three years of publication, to decide whether they can be transformed into International Standards. Technical Reports of type 3 do not necessarily have to be reviewed until the data they provide are considered to be no longer valid or useful.

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

ISO/IEC TR 15947, which is a Technical Report of type 3, was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

© ISO/IEC 2002 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

--`,,,`-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

Information technology — Security techniques — IT intrusion detection framework

1 Scope

This is a Type 3 Technical Report (TR), which defines a framework for detection of intrusions in IT systems. Many classes of intrusions are considered. These include intrusions that are intentional or unintentional, legal or illegal, harmful or harmless and unauthorized access by insiders or outsiders. The TR focuses on:

- establishing common definitions for terms and concepts associated with an IT intrusion detection framework,
- describing a generic model of intrusion detection,
- providing high level examples of attempts to exploit systems vulnerabilities,
- discussing common types of input data and the sources needed for an effective intrusion detection capability,
- discussing different methods and combinations of methods of intrusion detection analysis,
- describing activities/actions in response to indications of intrusions.

This framework explains intrusion detection terms and concepts and describes the relationship among them. Further, the framework addresses possible ordering of intrusion detection tasks and related activities.

This TR provides the basis for a common understanding of intrusion detection. This material aims to assist IT managers to deploy within their organizations Intrusion Detection Systems (IDS) that interact and work together. This TR should facilitate collaboration among organizations across the world where collaboration is desired and/or essential to counter intrusion attempts.

This framework document is not intended to cover every possible detail involved in intrusion detection, such as detailed attack patterns, or statistical anomalies, or the many configurations that an IDS could have.

© ISO/IEC 2002 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

2 References

ISO/IEC TR 13335 (all parts), *Information technology – Guidelines for the management of IT Security*

ITU-T Recommendation X.816 (1995) | ISO/IEC 10181-7:1996, *Information technology – Open System Interconnection – Security frameworks for open systems: Security audit and alarms framework*

3 Terms and Definitions

For the purposes of this Technical Report, the terms and definitions given in ISO/IEC TR 13335, and the following, apply.

- **attack** is an attempt to exploit an IT system vulnerability**.**
- **event** is an occurrence of some specific data, situation, or activity.
- **exploit** is a defined way to breach the security of an IT system through a vulnerability.
- **intrusion** is deliberate or accidental unauthorized access to, activity against, and/or activity in, an IT system
- **intrusion detection** is the process of identifying that an intrusion has been attempted, is occurring, or has occurred.
- **intrusion detection system (IDS)** is a technical system that is used to identify and respond to intrusions in IT systems.
- **sensor** or **monitor** is a component/agent of an IDS, which collects event data from an IT system under observation.

4 Introduction to Intrusion Detection

Over the years fundamental changes have occurred in the IT environment. Personal Computers and Workstations are nearly everywhere and can be interconnected via networks which provides new challenges for IT security. However, there are business reasons to connect to the Internet and other networks despite the fact that there are vulnerabilities that can be exploited.

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 will result from the attack.

4.1 The Need for Intrusion Detection

The first layer of defence to protect IT systems uses physical and technical controls that should encompass identification and authentication, physical and logical access control, auditing, and cryptographic mechanisms. However, it is economically impossible to completely protect every IT 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 defense 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.

--`,,,`-`-`,,`,,`,`,,`---
© ISO/IEC 2002 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Firewalls, as an important level of protection, may be used to control perimeter access to IT systems and services, and can provide a form of event data used in intrusion detection. However, it is impossible and cost prohibitive to protect against all intrusions. Thus, a layer of defence, simple or complex, is needed in order to detect intrusions when they occur and to react to them in a safe and appropriate manner. That layer of defence is the function of an IDS.

Intrusion detection attempts to identify computer misuse or an action that does not conform to security policy. Typical misuse takes advantage of vulnerabilities in system configuration, poorly designed software, user neglect and carelessness, and basic design flaws in protocols and operating systems. Outsiders frequently exploit these vulnerabilities. However, more harm can occur from malicious behavior by trusted insiders (e.g., disgruntled employees, trading partners, temporary employees) than from penetrations by outsiders. This is because an authorized user can take advantage of their physical access, privileges, and knowledge of local security safeguards.

Like every safeguard, intrusion detection has to be justified by an IT security risk analysis and management process and integrated into the security policies of an enterprise. These aspects are covered by the Guidelines for the Management of IT Security (GMITS), TR 13335, which provide guidance on the management aspects of IT security. These aspects include how to identify and justify the need for safeguards like an IDS. Corporate and the relevant system or service security policy should state that safeguards be selected as appropriate to manage the risks of intrusion. These safeguards include those that:

- reduce the chances of intrusions occurring,
- detect and recover effectively from intrusions that may occur.

In the latter situation, if the risks are deemed sufficient, an IDS should be selected. Further, it should be mandatory for the IDS to be linked to a security incident management (reporting and handling) scheme as discussed in WD 18044, Information Security Incident Management. That scheme should encompass a dedicated incident management function to receive incident reports, including regarding incidents identified by an IDS, conduct investigative analysis, respond and deal with the incidents, facilitate recovery, facilitate weakness resolution and conduct incident pattern and trend analysis.

Further, there should be feedback from an IDS to refine the information on threats and vulnerabilities in risk analysis support ‘databases’. This should, in turn, improve the quality of risk analysis and management reviews.

4.2 Types of Attacks

Attacks on computers and networks can successfully exploit configuration faults, and implementation faults. They could also exploit conceptual faults of network protocols or services and/or applications, and could potentially take advantage of abnormal user behavior.

These attacks can give the attacker valuable information about the system, service and/or network that is to be the focus of an attack. Further these attacks may permit the attacker to access a protected network or server. Loss of system integrity (e.g., degradation of service), loss of data integrity or confidentiality during the data transfer, or, loss of integrity or confidentiality for the stored data on a host are some potential consequences of these attacks.

Attacks can be further broken down and considered as being either host-based or network-based or a combination of both.

© ISO/IEC 2002 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

4.2.1 Host-based Attacks

Host-based attacks are generally considered to be attacks:

- on the application layer (SMTP, DNS, NFS, NIS) (e.g., e-mail forgery, spamming, buffer overflow attacks, race condition attacks, man-in-the-middle attacks);
- on an authentication system (e.g., attacks utilizing eavesdropping or password guessing);
- that introduce compromising malicious code (e.g., attacks utilizing Trojan horses, worms, or viruses);
- on WWW services (e.g., attacks aimed at cgi, ActiveX, or JavaScript);
- on system availability (e.g., denial-of-service attacks);
- on the operating system; and
- on network and application management systems (e.g., SNMP attacks).

4.2.2 Network-based Attacks

Network-based attacks are generally considered to be attacks on the:

- physical and data-link communications protocols and the systems that implement them (e.g. ARP-spoofing, MAC-address cloning),
- network and transport communications protocols and the systems that implement them (IP, ICMP, UDP, TCP) (e.g. IP-spoofing, IP-fragmentation attacks, buffer overflow attacks, SYN flooding attacks, Malformed TCP-header information attacks).

5 Generic Model of Intrusion Detection Process

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. The following Figure 1 shows the manner in which these functions relate to each other.

--`,,`-`-`,,`,,`,`,,`---
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
© ISO/IEC 2002 – All rights reserved
Not for Resale

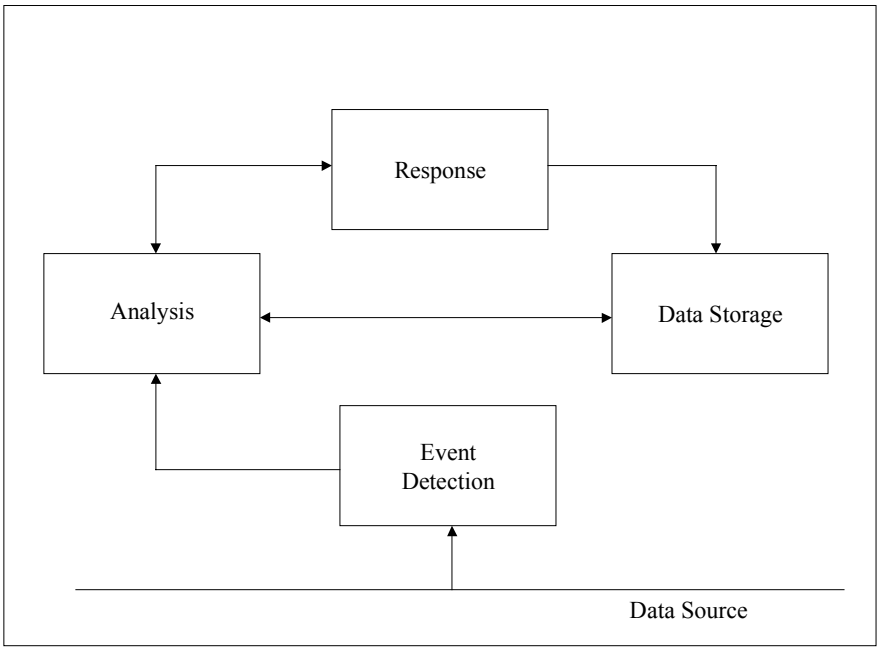

Figure 1 - Generic Model of Intrusion Detection

The purpose of the event detection function is to detect and provide information about events for use in the analysis function. This may include eliminating unnecessary data and extracting relevant information.

The analysis function analyzes and processes input from the event detection function and other relevant data. Its role is to further refine security-relevant information and to assess the probability that an intrusion has been attempted, is occurring, or has occurred.

Event detection and analysis can produce large quantities of data. The frequency of event detection and analysis will affect the amount of data and also contribute to the effectiveness of the intrusion detection process. This information must be made available to the system's administrator or a management workstation.

The data storage function of intrusion detection defines the means to store security-related information (e.g., attacks which occurred) and make it available at a later time.

The intrusion detection process includes a response function, which provides warnings and possibly countermeasure capabilities; for example, terminating TCP sessions or modifying router control lists in the case of network countermeasures. In this way the intrusion detection process may prevent further attacks from occurring after initial attacks are detected.

5.1 Data Sources

The success of the intrusion detection process depends upon the data sources from which information is taken for the detection of intrusions or intrusion attempts. The following sources can be delineated:

- 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.

© ISO/IEC 2002 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

- Allocations of system resources by the operating system:

  System monitoring parameters like CPU workload, memory utilization, starvation of system resources, I/O rate, quantity 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., source routing, SYN-flag) are useful for the IDS. It is helpful to collect the raw data at a low level referring to the OSI model, because there are fewer possibilities for the data to be manipulated prior to collection. If raw data is only gathered at a higher level of abstraction, for example, from a proxy server, then the information that was present at the lower level may be lost,

- Other data sources:

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

5.2 Event Detection

An "event" can be simple or complex. Simple events may be events that are commonly part of an attack but which also occur during normal operation. Complex events may be combinations of simple events that are highly likely to indicate a particular attack and may occur over an extended period of time. For example, an event can be an attempt to modify a computer log in its syslog file. An event need not be evidence of an intrusion in and of itself. Event detectors are the sensory organs of a complete intrusion detection “system.” These sensors and monitors can be positioned on a network device (e.g., router, bridge), on a firewall, or on a specific computer (e.g., application server, database server).

5.3 Analysis

Analysis of events and other relevant data is performed to correlate and refine security-relevant information and to assess the probability that an intrusion has been attempted, is occurring, or has occurred.

The analysis function may utilize information or data from many sources. It may use:

- data collected from event detection,
- data that has resulted from previous analysis and deemed relevant for further analyses,
- data generated from the knowledge about how an individual or system is supposed to behave (i.e. having known tasks supposed to be performed or having actions authorized to be done),
- data generated from the knowledge about how an entity or system is not supposed to behave (i.e., from known attacks or from known harmful actions),
- other relevant auxiliary data such as suspected attack source sites, individuals, or localities.

© ISO/IEC 2002 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

5.4 Response

The response function presents the appropriate results of the event processing by the analysis component to the system administrator or the security officer. These results are usually presented on a management console with a graphical user interface, where the alerts of all supervised IT systems and networks are brought together. Various ways to inform the system administrator should be provided, e.g. by e-mail, pager, or by messenger service.

The response function should also help the system administrator to assess the severity of the intrusion and to make the right decision with regard to implementing the appropriate countermeasures. If a countermeasure component is included with the IDS, an automated process can be started to curtail the intrusion or to minimize the consequences of the attack.

The activities of the response function should be consistent with the organization's incident management scheme. Some IDS may provide a reaction as the appropriate response. A reaction could be a re-configuration of an attacked system, the locking of an attacked account, or a protocol-conformant closing off for a session. This approach helps to minimize the damage an attacker may cause.

5.5 Data Storage

The data storage function would store the detected events, the audit logs, and whatever data necessary for the analyses in a database. The results of the analyses, including detected intrusions, are stored in a database for reporting, as well as for other purposes. The database may contain the collection of profiles of known attacks, the profiles of normal behavior, and may contain analyses indicating suspicious events that later can be used for coordination of suspicious event analysis. It can also contain detailed raw event data collected and preserved as evidence (e.g., for traceability) once a security alarm is raised. Data retention and data protection policies are needed to address various concerns such as completion of analysis, data forensics, and evidence preservation.

6 Characteristics of Intrusion Detection

The characteristics of intrusion detection may be divided into functional and non-functional areas as shown in Figure 2.

Functional characteristics refer to the internal mechanisms of the intrusion detection process, namely its input information, its reasoning mechanism, and its interaction with an IT system, service or network. The non-functional area is characterized by the frequency of event detection and analysis.

© ISO/IEC 2002 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

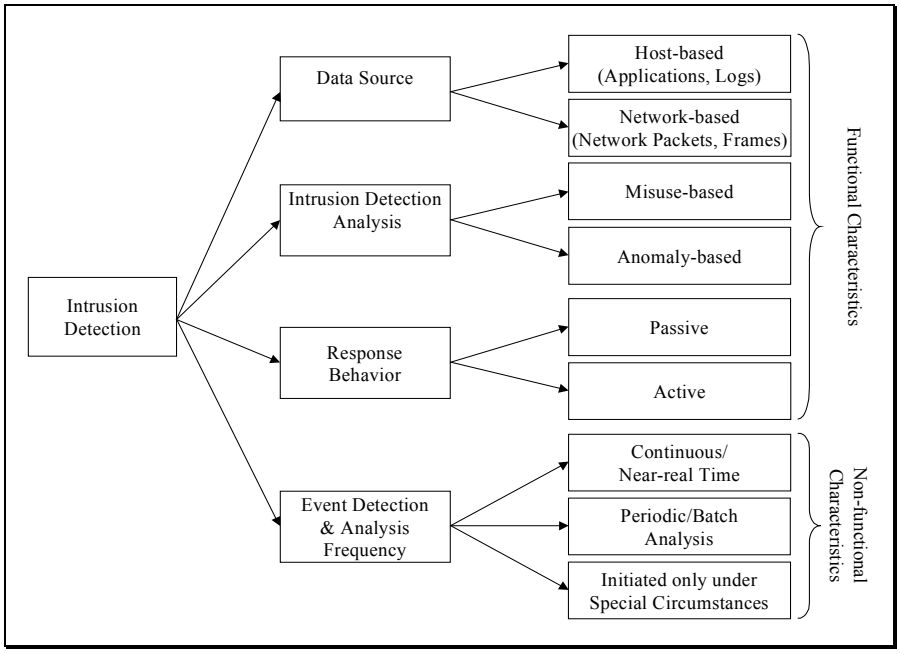

Figure 2 - Characteristics of Intrusion Detection

6.1 Data Source

The differentiation based on the location of the data source is a predominant one in the world of intrusion detection. It is based on the kind of input information used for the event detection. There are two different basic source locations for collecting raw data to be used in event detection and analysis: hosts and networks. Therefore, these data sources will be called host-based and network-based. Event logs/security audit trails and system logs from hosts or applications can be examined in the host-based case. Network packets or frames are primary sources of network-based information, as are firewalls, switches, routers and IDS-specific sensors/monitoring agents.

6.1.1 Host-based

As noted earlier host-based intrusion detection typically monitors system, event, and security logs in their environments, i.e., monitors data sources in the host. Other technologies have been included in host–based intrusion detection. For example, one popular method for detecting intrusions inspects key system files and executables via checksums at regular intervals for unexpected changes. Another inspects the log files for changes. When any of the log files change, the intrusion detection process compares the new log entry with known attack signatures to check if there is a match. The timeliness of the response is in direct relation to the frequency of the polling interval.

Host-based data sources:

- support a forensic analysis focus on host-specific event data,
- provide monitoring of specific system activities (user logon/logoff activities, file access activity, attempts to install new executables and/or to access privileged services, system resource usage, administrator activities such as adding user accounts and changes to key system files and executables),
- permit the detection of attacks that network-based data sources do not, e.g., attacks from the keyboard of a critical server.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
© ISO/IEC 2002 – All rights reserved
Not for Resale

6.1.2 Network-based

Network-based intrusion detection data include network management logs, raw network packets or frames typically extracted by network adapters running in promiscuous mode monitoring and analyzing all traffic in real-time/near real-time as it travels across the network. It also includes event data from firewalls, switches, routers and IDS-specific sensors/monitoring agents. Network-based data sources permit real-time or near real-time detection and response by providing data on suspicious attacks as they occur (e.g. a denial-of-service attack).

6.2 Event Detection and Analysis Frequency

6.2.1 Continuous/Near Real-Time

In this scenario the event detector continuously looks for occurrences of specific data, situations, or activities and detects events as they occur. Similarly, analyses are carried out continuously. In other words, analyses are being done in real-time as opposed to being done periodically or batch processed.

Real-time intrusion detection is not necessarily "real-time" in a strict computing sense. Depending upon the parameters such as the source of event data and the detection method, a time lag may exist between the occurrence of an event and the time at which it is detected and reported. Moreover, the elapsed time between when an attack is initiated and when the target system is penetrated may vary depending upon the nature of the attack. Therefore, in some cases, the attack may be completed before it is detected and reported to the proper authority. These delays between the attack and its corresponding detection may or may not impose a threat depending upon the resilience of the implemented IDS and the targets it is protecting.

6.2.2 Periodically/Batch Processed

Data or events can be processed on a periodic basis or be batch processed. For example, audit trails or system logs are generally produced continually but they are processed or analyzed when the load on an information system is lower, like at night. They may also be spun off onto tape or other storage media and processed periodically by an auxiliary off-line subsystem. This may also be beneficial in order to protect registered data.

6.2.3 Initiated Only Under Special Circumstances

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

6.3 Intrusion Detection Analysis

There are two general approaches to intrusion detection analysis: misuse-based and anomaly-based. Specific methods within each of these categories will be discussed later. Some misuse-based methods are also known as knowledge-based detection for detection by known attack appearance. Some anomaly-based methods are sometimes described as behavior-based detection for deviation from observed behavior.

Anomaly detection focuses on abnormal behavior of users. Normally the analysis in its role as a detector is bundled with a database in which known attack signatures or the pre-defined rules or properties of normal user behavior are stored. The analysis function evaluates the probability that the analyzed event can be considered as an intrusion attempt.

© ISO/IEC 2002 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

6.3.1 Misuse-based

Misuse-based intrusion detection refers to the detection of intrusions by precisely defining misuses ahead of time and watching for their occurrence. Misuse detection methods concentrate on the search for evidence of attacks based on knowledge accumulated from known attacks and unauthorized activity. The current prevailing methods use:

- signature analysis,
- expert systems,
- state transition analysis.

These methods will be described in Section 9.

6.3.2 Anomaly-based

Anomaly-based intrusion detection generally involves the search for deviation from a profile of usual behavior based on observations of a system during normal operation or a profile defined by other expected use parameters. A profile is a predetermined specific event pattern usually related to a series of events, stored for the purposed of comparison.

The methods base their decision on the variance of observed behavior from predicted or expected behavior and usually involve one or more of the following:

- statistical approach or a variation of the statistical approach known as expert systems,
- neural networks,
- user anomalous behavior identification,
- combinations of the above.

These methods will be described in Section 9.

6.4 Response Behavior

Response behavior describes the response of the intrusion detection process to attacks. When a response has been decided upon it must be protected from interference. If an intruder is able to delete or alter this communication he can potentially stop the intrusion detection process from carrying out responses due to detected policy violations.

6.4.1 Passive

If the response is limited to activities within the intrusion detection process itself that do not modify IT system behavior, e.g., to merely generate alarms on the administrator console, the response is said to be passive. Passive response systems respond by notifying the proper authority. They do not take any measures to prevent or limit the damages of an attack.

6.4.2 Active

When the response is to react to the attack by taking either corrective actions (modifying system behavior) or proactive actions (logging out possible attackers, closing down services), then the response is said to be active. Active response mechanisms may not only notify the proper authority, but also initiate countermeasures. These countermeasures often seek to limit the damage inflicted by the attack. This may be achieved by reconfiguration of other security services such as firewalls and routers. In some cases counter-attacks or session termination techniques can be utilized to prevent further damage, although if used they need to be used with caution.

© ISO/IEC 2002 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

7 Architecture Considerations

IDS may be implemented in various ways.

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

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

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

- way in which the several IDS are interconnected and interrelated,
- concentration or distribution of tasks within the IDS architecture.

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

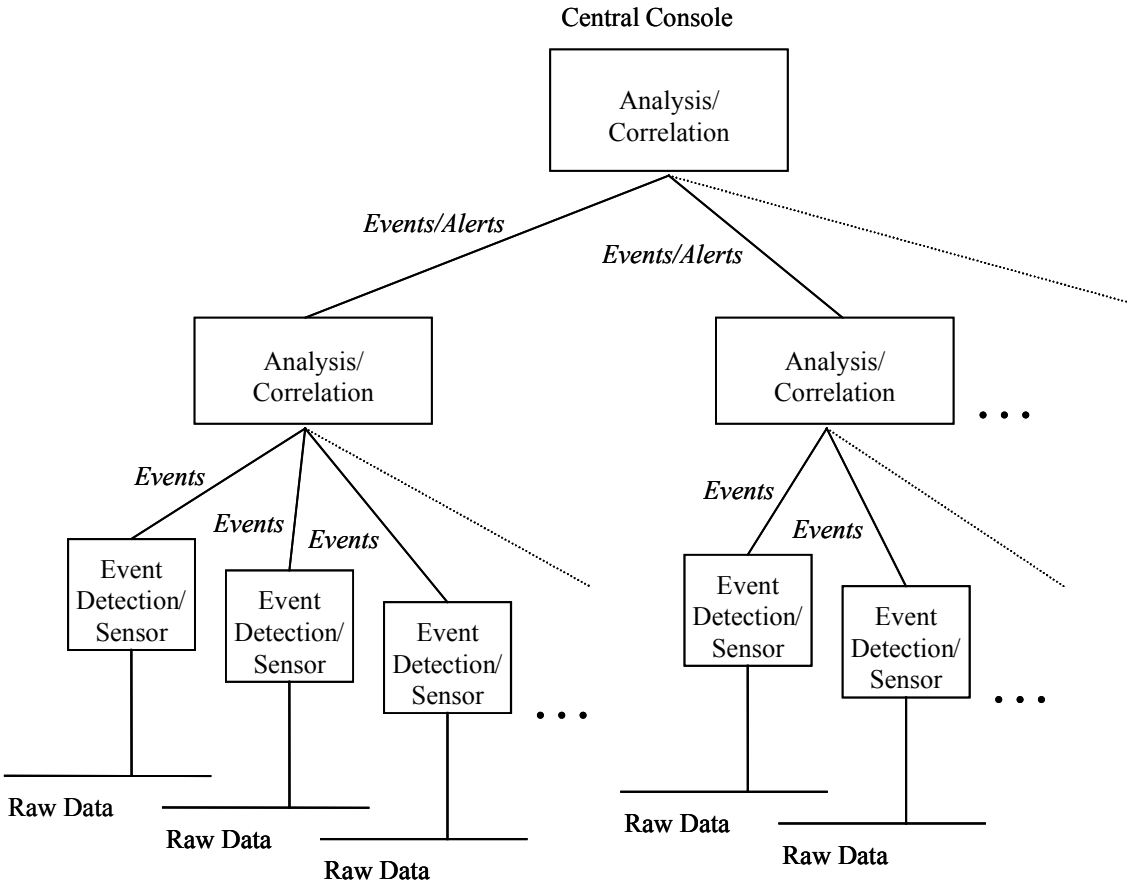

Figure 3 - Hierarchical Intrusion Detection Architecture

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

© ISO/IEC 2002 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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

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

8 Management of an IDS

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

8.1 Configuration Management

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

8.1.1 Detection Function

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

8.1.2 Response Function

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

8.2 Security Services Management

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

8.3 Integration with Other Management Systems

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

© ISO/IEC 2002 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

8.4 Security of Management Operations

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

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

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

8.4.1 Authentication

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

8.4.2 Integrity

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

8.4.3 Confidentiality

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

8.4.4 Availability

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

8.5 Management Model

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

© ISO/IEC 2002 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

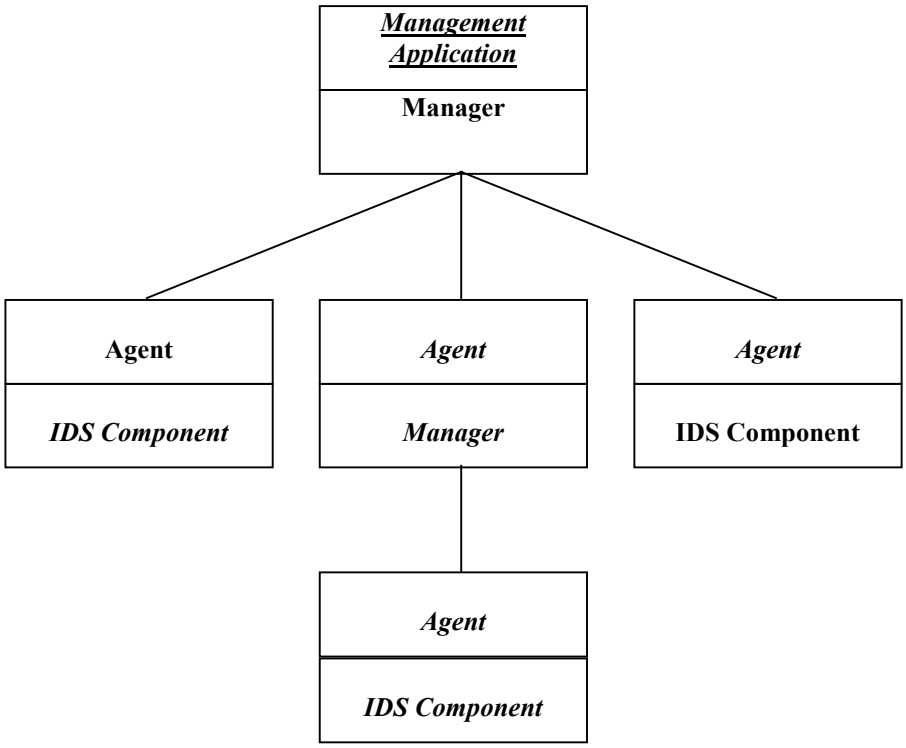

Figure 4 - An Intrusion Detection Management Model

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

- many-to-many - several management consoles can manage many distributed agents,
- one-to-many - one management console can manage many distributed agents,
- one-to-one - one management console can manage a single agent.

9 Intrusion Detection Analysis

Several methods are used for intrusion detection analysis, and are described below.

9.1 Signature Analysis

Specific signatures or patterns characterize attack attempts. Semantic descriptions or signatures of known attacks are collected or formulated and stored in a database.

One type of signature analysis, audit trail analysis, compares information found in the audit trails, i.e., a system's built-in audit log or event log, with the attack signatures. This method is probably the most commonly known way to analyze the status of a computer system. It expects that any security-relevant action initiated on a computer system will lead to a corresponding audit log entry. Traditionally in audit trail analysis, the analysis process itself only interprets the corresponding entries off-line. As the goal of intrusion detection is to identify security violations or system attacks as soon as possible, the audit trails should be processed in near real-time.

Attack scenarios might be translated into sequences of audit events, or into patterns of data that can be sought in the event data generated by the operating system of a computer, by applications, routers, firewalls, switches, or IDS-specific sensors/monitoring agents. Other patterns or sequences may be

--`,,,`--`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
© ISO/IEC 2002 – All rights reserved
Not for Resale

found in a stream of network traffic. When a sequence of events is found that matches a predefined signature of an attack, an attempt of an intrusion is indicated.

Protocol analysis is a form of network specific signature analysis and uses the well-defined structure of communications protocols. Protocol analysis can process elements like packets, frames and connections faster and more appropriately than regular pattern matching. Using this method may reduce the size of the attack signature database.

Signature analysis intrusion detection methods can be used with or without thresholds. If no thresholds are defined an alarm is generated when an attack signature is recognized. If a threshold is defined, an alarm is only generated when the number of events or sequences of events with that attack signature exceeds the threshold. A threshold could be a percentage, or a number, of occurrences per time period or some other measure.

An optimal signature analysis scheme should make use of information available at different levels (application, network, and system) and from different sources. This is difficult if these local audit trails do not have a common audit format. The main drawback of the signature analysis technique – like all misuse-based approaches – is the need for frequent updates to keep up with the stream of newly discovered vulnerabilities/attacks. The signature database being used for this purpose may be updated in its entirety or incrementally due to efficiency reasons. Never-the-less proper trust in the source of the update needs to be established in both cases using appropriate authentication and integrity services.

9.2 Statistical Approach

The most widely used approach for anomaly-based intrusion detection is statistical. User or system behavior is measured by a number of variables sampled over time and stored in a profile. 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.

Specific denial-of-service attacks that make use of weaknesses in the Internet Protocol suite can be detected using the statistical approach. One example is the so-called SYN flood attack where an attacker sends many connection requests with a faked (altered) origin IP address and requires the attacked system to acknowledge these requests without finally receiving a confirmation. Though the attacker seems to behave according to the communications protocol, the attack can only be detected by the quantity of connection requests received within a certain period of time. The quantity of requests together with the configured number of allowed open connections define the threshold for this type of attack.

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

The current behavior of each user is maintained in a profile. At regular intervals the current profile is merged with the stored profile. Anomalous behavior is determined by comparing the current profile with the stored profile.

The original model keeps averages of all these variables and detects whether thresholds are exceeded based on the standard deviation of a variable. More complex models have been developed which compare profiles of long-term and short-term user activities. The profiles are regularly updated as the behaviors of users evolve.

--`,,`-`-`,,`,,`,`,,`---
© ISO/IEC 2002 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

9.3 Expert Systems

Expert systems contain rules that describe attacks in the case of misuse-based analysis. In the case of anomaly-based analysis a set of rules is generated statistically describing the behavior of the users based on recordings of their activities over a given period of time. 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 attack or to detect inconsistent behavior. This method increases the abstraction level of the event data by attaching semantics to it. The rule base must be continually updated to accommodate new descriptions of attacks or new usage patterns.

Rule-based description languages form natural tools for modeling the knowledge that experts have collected about attacks. This approach allows a systematic browsing of the audit trail in search of evidence of attempts to exploit known vulnerabilities. They are also used for verifying the proper application of the security policy of an organization.

The main limitations of this approach are: (1) the difficulties of extracting knowledge about attacks, and (2) the processing speed.

9.4 State-transition Analysis

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

9.5 Neural Networks

Neural networks are algorithms that learn about the relationship between input-output vectors and "generalize" them to obtain new input-output vectors in a reasonable way. The main use of neural networks for intrusion detection is to learn the behavior of actors in the system (e.g., users, daemons). The advantage of using neural networks over statistics resides in having a simple way to express nonlinear relationships between variables, and in learning/retraining the neural network automatically. Neural networks are still a computationally intensive technique, and are currently not widely used in the intrusion detection community.

9.6 User Anomalous Behavior Identification

This non-statistical technique models the normal or authorized behavior of users by the set of tasks they have to or are authorized to perform on the system. These tasks and facets of the system's security policy are then represented as patterns for users' expected or authorized actions such as access to particular files or types of files. These actions are related to the audited or logged events, e.g. security related events, which are observed and recorded by the system. The analyzer keeps a set of tasks or patterns that each user is expected to perform. The individuals' actions found in the audit trails are compared, either real-time or off-line, with their desired or authorized patterns. An alarm is issued if the action pattern differs from the authorized pattern. This method matches patterns of proper activity, whereas signature analysis matches patterns of improper activity.

9.7 Hybrid Analysis

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

9.8 Other

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

© ISO/IEC 2002 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

research area called Computer immunology. Most of this research is yet to be applied in commercial systems.

10 Implementation and Deployment Issues

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

10.1 Efficiency

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

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

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

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

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

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

10.2 Functionality

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

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

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

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

© ISO/IEC 2002 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

10.3 Personnel for IDS Deployment and Operation

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

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

- customize the IDS so that it looks for events that are relevant to the IT environment where it is deployed,
- interpret what the IDS is telling you when an alarms goes off,
- develop policies and procedures for responding to IDS alerts that appear to be real,
- correct the vulnerabilities that caused the intrusion to be successful.

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

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

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

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

10.4 Other Implementation Considerations

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

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

© ISO/IEC 2002 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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

11 Intrusion Detection Issues

11.1 Intrusion Detection and Privacy

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

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

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

- intrusion detection has to serve the purpose of data or system protection,
- the data collection (network packets, audit logs) has to be adequate to the purpose of protection,
- a policy covering requirements to protect the privacy of personal information collected in IDS should be developed and applied.

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

The second aspect points out that only those data should be gathered and analyzed which are necessary to recognize attacks. After the comparison of event data with the attack signatures of the IDS, data that is no longer needed or with which there has been no indication of an attack should be deleted; the relevant data, which indicate an attack, should be stored in a secure way. However, deleting the data may not be adequate in some instances; event data may need to be archived for later inspection, e.g., for purposes of traceability to the attacker or for forensic analysis at a later date. Some data may at first

© ISO/IEC 2002 - All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

appear to be benign. After further analysis it may prove to be related to an attack. Correlation with data collected later may also prove it to be related to an attack. In any event the data should be strongly protected from access for many purposes, including privacy. The actions taken should be consistent with the security policy of the organization.

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

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

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

11.2 Sharing of data on intrusions

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

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

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

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

--`,,`-`-`,,`,,`,`,,`---
© ISO/IEC 2002 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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

11.3 Future Standardization

There are many hard intrusion detection problems that need to be solved. One of the hard problems is interoperability that could be aided by the establishment of intrusion detection standards.

Today IDS are based upon competing proprietary solutions that in many cases prevent competing vendor products from working together and make interoperability in a multi-vendor environment very tedious and difficult. Ideally an IDS would be fully interoperable with network management systems, other IDS, logging services, and response mechanisms. However, because of the lack of IDS standards, this type of interoperability is not possible.

Future IDS standardization to improve interoperability can be anticipated in the following areas:

- terminology,
- testing scenarios,
- reporting formats,
- attack signatures and nomenclature,
- common APIs,
- common interfaces including message formats,
- control flow,
- requirements for audit logs and journals,
- intrusion information exchange formats.

A standard format is needed that will facilitate rapid distribution of information among IDS developers and related groups in order to achieve "critical mass" in the coverage. This should include information that ensures automated repeatability, detection, and diagnosis of each intrusion sample.

The Internet Engineering Task Force (IETF), a group that develops standards for the Internet is designing an intrusion detection alert standard. This standard involves sending XML based alerts over an HTTP-like communications format. If implemented by the IDS vendors this will significantly enhance the automated exchange and correlation of information from different IDS vendors.

12 Summary

This Technical Report provides an overview of the need for intrusion detection. It provides a generic model for, and outlines the characteristics of intrusion detection. Principles for architectures that can be used to implement IDS, management requirements and intrusion analysis methods are then discussed. The final sections discuss implementation and deployment issues and possible future standardization initiatives that are expected to make IDS easier to implement and more effective.

© ISO/IEC 2002 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Bibliography

[1] Edward Amoroso: Intrusion Detection. An Introduction to Internet Surveillance, Correlation, Trace Back, Traps and Response, Intrusion Net Books, New Jersey, 1999, ISBN: 096667007

[2] Herve Debar, Marc Dacier, Andreas Wespi: Towards a Taxonomy of Intrusion Detection Systems, Computer Networks 31, 1999, pgs 805-822

[3] Josef von Helden, Stefan Karsch: Grundlagen, Forderungen und Marktübersicht für Intrusion Detection Systeme (IDS) und Intrusion Response Systeme (IRS), Bonn, 1997 (BSI-Studie)

[4] Internet Security Systems: Network- vs. Host-based Intrusion Detection. A Guide to Intrusion Detection Technology, Atlanta, 1998

[5] Sandeep Kumar: Classification and Detection of Computer Intrusions, PhD Thesis, Purdue University, 1995

[6] Stephen Northcutt: Network Intrusion Detection, An Analyst's Handbook, New Rider Publishing, Indiana, 1999, ISBN: 0735708681

[7] Thomas Ptacek, Timothy Newsham: Insertion, Evasion and Denial-of-Service: Eluding Network Intrusion Detection, Calgary, 1998

[8] Stuart Staniford-Chen, et al: Common Intrusion Detection Framework, Internet-Draft, http://www.dis.org/comega/cidf.txt, 1998-

[9] The President's National Security Telecommunications Advisory Committee (NSTAC)-Network Group Intrusion Detection Subgroup: Report on the NS/EP Implications of Intrusion Detection Technology Research and Development, Washington, 1997

[10] Ulf Lindquist and Erland Jonsson: How to Systematically Classify Computer Security Intrusions, *Proceedings of the 1997 IEEE Symposium on Security & Privacy*, Oakland, CA, 1997

[11] Herve' Debar, Marc Dacier, Andreas Wespi: A Revised Taxonomy for Intrusion-detection Systems, Annals of Telecommunications, 55, pgs. 7-8, 2000

[12] Rebecca Gurley-Bace: Intrusion Detection, Macmillan Technology Series, December 21, 1999, ISBN: 1578701856

[13] Ulf Lindqvist, Douglas Moran, Phillip Porras, and Mabry Tyson: Designing IDLE: Intrusion Data Library Enterprise, RAID 98 First International Workshop on the Recent Advances in Intrusion Detection, September 14-16, 1998, Louvain-la-Neuve, Belgium

[14] ISO/IEC WD 18044: 2001, Information technology - Security techniques - Information Security Incident Management

© ISO/IEC 2002 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

ICS 35.040

Price based on 22 pages

© ISO/IEC 2002 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale