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 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

Contents

Foreword

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

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

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.

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.

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.

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.

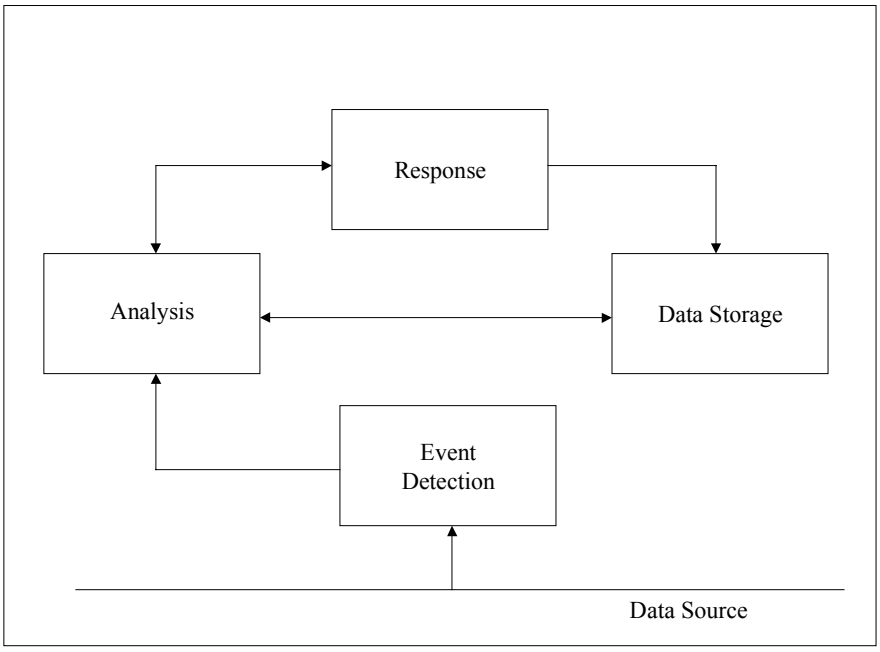

Figure 1 - Generic Model of Intrusion Detection

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.

- 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.