

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)



AVA Documents
© ISO/IEC 2002
Document Sharing Hub

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

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)



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

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

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

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.