ISO/IEC 24767-1

Edition 1.0 2008-09

INTERNATIONAL STANDARD

Information technology – Home network security –
Part 1: Security requirements

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 24767-1:2008
https://standards.iteh.ai/catalog/standards/sist/74c5a048-ccf5-4991-b778-b42bcbc97776/iso-iec-24767-1-2008

ISO/IEC 24767-1:2008(E)

THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2008 ISO/IEC, Geneva, Switzerland

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 IEC or IEC's member National Committee in the country of the requester.

If you have any questions about ISO/IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

- Catalogue of IEC publications: www.iec.ch/searchpub
The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, withdrawn and replaced publications.

- IEC Just Published: www.iec.ch/online_news/justpub
Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.

- Electropedia: www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.

- Customer Service Centre: www.iec.ch/webstore/custserv
If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:
Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 24767-1:2008
https://standards.iteh.ai/catalog/standards/sist/74c5a048-ccf5-4991-b778-b42bebe97776/iso-iec-24767-1-2008

ISO/IEC 24767-1

Edition 1.0 2008-09

INTERNATIONAL STANDARD

Information technology – Home network security – Part 1: Security requirements

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 24767-1:2008
https://standards.iteh.ai/catalog/standards/sist/74c5a048-ccf5-4991-b778-b42bcbc97776/iso-iec-24767-1-2008

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

PRICE CODE K

ICS 35.200

ISBN 2-8318-1000-1

CONTENTS

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 24767-1:2008
https://standards.iteh.ai/catalog/standards/sist/74c5a048-ccf5-4991-b778-b42bcbc97776/iso-iec-24767-1-2008

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 24767-1:2008
https://standards.iteh.ai/catalog/standards/sist/74c5a048-ccf5-4991-b778-b42bcbc97776/iso-iec-24767-1-2008

INFORMATION TECHNOLOGY –
HOME NETWORK SECURITY –

Part 1: Security requirements

FOREWORD

1) ISO (International Organization for Standardization) and IEC (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. Their preparation is entrusted to technical committees; any ISO and IEC member body interested in the subject dealt with may participate in this preparatory work. International governmental and non-governmental organizations liaising with ISO and IEC also participate in this preparation.

2) In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. 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.

3) The formal decisions or agreements of IEC and ISO on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC and ISO member bodies.

4) IEC, ISO and ISO/IEC publications have the form of recommendations for international use and are accepted by IEC and ISO member bodies in that sense. While all reasonable efforts are made to ensure that the technical content of IEC, ISO and ISO/IEC publications is accurate, IEC or ISO cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.

5) In order to promote international uniformity, IEC and ISO member bodies undertake to apply IEC, ISO and ISO/IEC publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any ISO/IEC publication and the corresponding national or regional publication should be clearly indicated in the latter.

6) ISO and IEC provide no marking procedure to indicate their approval and cannot be rendered responsible for any equipment declared to be in conformity with an ISO/IEC publication.

7) All users should ensure that they have the latest edition of this publication.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 24767-1:2008
https://standards.iteh.ai/catalog/standards/sist/74c5e048-ccf5-4991-b778-b42bcbc97776/iso-iec-24767-1-2008

8) No liability shall attach to IEC or ISO or its directors, employees, servants or agents including individual experts and members of their technical committees and IEC or ISO member bodies for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication of, use of, or reliance upon, this ISO/IEC publication or any other IEC, ISO or ISO/IEC publications.

9) Attention is drawn to the normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.

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

International Standard ISO/IEC 24767-1 was prepared by subcommittee 25: Interconnection of information technology equipment, of ISO/IEC joint technical committee 1: Information technology.

The list of all currently available parts of the ISO/IEC 24767 series, under the general title *Information technology – Home network security*, can be found on the IEC web site.

This International Standard has been approved by vote of the member bodies, and the voting results may be obtained from the address given on the second title page.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

INFORMATION TECHNOLOGY – HOME NETWORK SECURITY –

Part 1: Security requirements

1 Scope

This part of ISO/IEC 24767 specifies home network security requirements that may come from inside or outside a home. It serves as a foundation for the development of security services against threats affecting the home environment.

The discussions about security requirements in this standard are presented in a relatively informal manner. Although many of the items discussed here are expected to guide the design of security mechanisms applied either inside home networks or through the Internet, they are not considered formal requirements.

Various devices are connected to the home network; see Figure 1. The devices of the "living network", the devices for "A/V entertainment" and the devices for "informational applications" provide different features and performance. This standard provides means to analyse the risks for each networked device and to define its specific "security requirements".

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 24767-1:2008
https://standards.iteh.ai/catalog/standards/sist/74c5a048-ccf5-4991-b778-b42bcbc97776/iso-iec-24767-1-2008

2 Terms, definitions and abbreviations

2.1 Terms and definitions

For the purpose of this document the following definitions apply.

2.1.1
brown goods
A/V devices that are mainly used for entertainment, for example, television or DVD recorder

2.1.2
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities or processes

2.1.3
data authentication
service used to ensure that the source of the data claimed by a party to a communication is correctly verified

2.1.4
data integrity
property that data has not been altered or destroyed in an unauthorized manner

2.1.5
user authentication
service used to ensure that the identity claimed by a party to a communication is correctly verified, whereas an authorization service ensures that the identified and authenticated party is entitled to access a particular device or application on the home network

2.1.6
white goods
appliances that are used for daily life, for example, air conditioner, refrigerator and so on

2.2 Abbreviations

For the purpose of this document the following abbreviations apply.

A/V	Audio / Visual
DDoS	Distributed Denial of Service
DoS	Denial of Service
DRM	Digital Rights Management
DTV	Digital TeleVision
DVD	Digital Versatile Disc
ESM	Externally Supported Multiple homes HES
ESS	Externally Supported Single home HES
HES	Home Electronic System
ICT	Information and Communication Technology
IP	Internet Protocol
IPSec	IP Security protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IT	Information Technology
MPEG	Moving Picture Expert Group
OSS	Owner supported single home HES
PDA	Personal Digital Assistant
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
URL	Uniform Resource Locator
VCR	Video Cassette Recorder
VoIP	Voice over Internet Protocol

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 24767-1:2008
https://standards.iteh.ai/catalog/standards/sist/74c5a048-ccf5-4991-b778-b42bcbc97776/iso-iec-24767-1-2008

3 Conformance

This part of ISO/IEC 24767 provides guidelines and contains no conformance requirements.

4 Security requirements for home electronic systems and networks

4.1 General

With the rapid development of the Internet and related networking technologies, computers in offices as well as homes have been enabled to be connected to each other or to the outside world to gain lots of resources. Today, the same technologies behind these successes are extending their reach right into our homes to make devices as connectable as ordinary PCs. In doing so, they will not only permit users to monitor and control their home appliances from inside or outside the home, but also create new service development and opportunities, such as remote controlling and maintenance of home appliances. This means that a simple home computing environment will evolve into a home network of multiple devices for which security will also be demanded.

A HES needs to be trusted by the inhabitants, users and owners of both the home and the system. The purpose of security of the HES is to provide trust in the system. Since many components of HES will be in operation 24 hours a day continuously and automatically exchange information with the outside world, IT security is necessary in order to maintain the confidentiality, integrity and availability of the data and the system. A well implemented security solution implies for example that only authorized users and processes have access to the system and the data stored on the system or is communicated to and from the system, and that only authorized users are able to use and modify the system.

Security requirements for HES can be described in several ways. This standard is limited to IT security of the HES. However, information technology security needs to look beyond the system itself, since the home shall be able to function, although with limited functionality, in case of a break down of the IT system. There exists in an intelligent home features that are normally supported by the HES that shall be possible to function also when the system breaks down. In such cases one realizes that there exist security requirements that cannot be part of the system itself, but that the system shall not prohibit the implementation of fallback solutions.

There are several stakeholders in security. Not only inhabitants and owners of the HES have to trust it, but also service providers and content providers. These latter have to trust that their offered services and content are only used as authorized by them. However, one of the foundations of the security of a system is that it has to be under the responsibility of a single security manager. It is obvious that this has to be the responsibility of the inhabitants/owners of the system. Whether this is done by him/herself or outsourced is irrelevant. It is still the security manager who has the responsibility. The way service and content providers trust that the HES and its users handle their services and content correctly is reduced to a contractual issue. The contract may, for example, state functions, components or processes that shall be supported by the HES.

It is not expected that a single architecture of HES can support all types of homes. Each model might have a different set of security requirements. Three different models of designing a HES will be described, each with a different set of security requirements.

It is obvious that some security requirements are seen as more important than others. Thus, it can be seen that the support of some countermeasures will be optional. Furthermore, countermeasures can be of different quality and cost. Also, the management and maintenance efforts of these countermeasures can require different skills. This standard tries to explain the reasons for the listed security requirements and thus allow the designer of the HES to determine which security features a specific HES shall support. And considering quality requirements and management and maintenance efforts, which mechanism shall be chosen for that particular feature.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 24767-1:2008
https://standards.iteh.ai/catalog/standards/sist/74c5a048-ccf5-4991-b778-
b42bcbc97776/iso-iec-24767-1-2008

The security requirements in a home network depend both on how security and “home” are defined and they also depend on what is envisioned as the “network” within that home. If the network is just a link from a single PC to a printer or a cable modem, then security measures applied to that cable and the equipment connected at either end of it could accomplish all the network security that the home owner needs.

However, when a home contains dozens, if not hundreds, of networked devices, with some belonging to the entire household and some belonging to individuals within the home, more complex security measures will have to be taken into consideration.

4.2 Home electronic system security

4.2.1 Definition of HES and of system security

A home electronic system and networking can be defined as the collection of elements that process, manage, transport and store information, enabling the connection and integration of multiple computing, control, monitoring and communication devices in the home.

Ultimately, home electronic systems and networks will enable entertainment, information, communication and security devices, in addition to appliances in the home, to communicate with each other. These devices and appliances will share information and can be controlled and monitored either within the home or remotely, and accordingly all home networks will require some security mechanisms to safeguard their daily operations.

Network and information security can be understood as the ability of a network or an information system to resist, at a given level of confidence, accidental events or malicious actions. Such events or actions could compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data as well as related services offered via those networks and systems.

The security incidents may be grouped as follows:

- Electronic communication can be intercepted and data copied or modified. This can cause damage both through invasion of the privacy of individuals and through the exploitation of data intercepted.
- Unauthorized access into computer and home computer networks is usually carried out with malicious intent to copy, modify or destroy data and is likely to be extended to systems and automatic equipment in the home.
- Disruptive attacks on the Internet have become quite common and in future the telephone network may also become more vulnerable.
- Malicious software, such as viruses, can disable computers, delete or modify data or reprogram home equipment. Some virus attacks have been extremely destructive and costly.
- Misrepresentation of people or entities can cause substantial damages, for example customers may download malicious software from a website masquerading as a trusted source, contracts may be repudiated and confidential information may be sent to the wrong persons.
- Many security incidents are due to unforeseen and unintentional events such as natural disasters (floods, storms and earthquakes), hardware or software failures, and human errors.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 24767-1:2008
https://standards.iteh.ai/catalog/standards/sist/74c5a048-ccf5-4991-b778-b42bcbc97776/iso-iec-24767-1-2008

In addition to these incidents, there are other security related topics which also are important for a home, such as the reliability of the system. Safety and physical security are outside the scope of security information. Safety is related to the prevention of harming humans or buildings. Physical security includes the protection of the home, the hardware of the home electronic system by means of suitable door and window locks. These topics, although relevant for the home, are not treated in this standard.

Since a home electronic system cannot be made completely reliable or security protected, it shall be assumed that a failure of all or part of the system can occur. This loss of availability shall be accounted for. There is thus the need to have recovery processes prepared in order to be able to restart those parts of the data and system, and possibly to support fallback technologies and procedures. A fallback solution is obviously outside the scope of the HES, but it shall not forbid the existence of such solutions.

The security requirements of home networks not only address in-home usage, but also those demanded by outside-home applications, all of which may have significant impact on services ranging from residential user operations, vendor remote maintenance to multiform service-providing applications. Once the boundaries of home networks become adjacent to the outside world, security consideration in home networks will turn out to be similar to those faced by the information and communications technology (ICT) department of a business. And most of these have been widely discussed (see for example ISO/IEC 18028 series) and Annex A.

However, there still exist some different characteristics between domestic applications and corporate applications, home networking infrastructure and enterprise networks, residential users’ needs and business workers’ needs. Therefore, it is necessary first to introduce some existing home networking models and illustrate some of their application domains, and then look into these models to identify possible threats to home networks and, finally, detail the security requirements.

Figure 1 shows a conceptual home networking model. A gateway is placed between a home and the outside world: the Internet. Inside the home, there are a variety of devices possibly falling into some categories as specified in Figure 1.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 24767-1:2008
https://standards.iteh.ai/catalog/standards/sist/74c5a048-ccf5-4991-b778-b42bcbc97776/iso-iec-24767-1-2008