ISO/IEC 24767-1

Edition 1.0 2008-09

INTERNATIONAL STANDARD

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



ISO/IEC 24767-1:2008(E)

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

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 It also gives information on projects, withdrawn and replaced publications.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

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 24767-1

Edition 1.0 2008-09

INTERNATIONAL STANDARD

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

PRICE CODE K

ICS 35.200

ISBN 2-8318-1000-1

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

Not for Resale

CONTENTS

FOREWORD 4
1 Scope 5
2 Terms, definitions and abbreviations 5
2.1 Terms and definitions 5
2.2 Abbreviations 6
3 Conformance 6
4 Security requirements for home electronic systems and networks 6
4.1 General 6
4.2 Home electronic system security 7
4.3 Issues related to HES security but out of scope of this standard 11
5 Challenges 12
5.1 General 12
5.2 Always-on challenge 12
5.3 Power line challenge 12
5.4 Wireless challenge 13
5.5 Complex assortment devices challenge 13
5.6 Many and diverse user needs 13
5.7 Many and diverse applications 13
6 Security models 14
6.1 Introduction 14
6.2 Owner supported single home HES (OSS) 14
6.3 Externally supported single home HES (ESS) 14
6.4 Externally supported multiple homes HES (ESM) 14
7 Threat analysis 15
7.1 General 15
7.2 Unauthorized access 15
7.3 Malicious software and configuration 16
7.4 Denial of service 17
7.5 Unintended modification of data during communication 17
7.6 User errors 17
7.7 System failures 17
7.8 Security service providers 17
8 Security requirements 17
8.1 General 17
8.2 Access control 18
8.3 Data and message authentication 19
8.4 Remote access control 19
8.5 Protection of communications 19
8.6 Firewalls 20
8.7 Virus protection 20
8.8 Protection against denial of service attacks 20
8.9 Auditing 21
8.10 Recovery 21
9 Requirements on security solutions 21

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

9.1 General 21
9.2 Different levels of security services for different applications in a home 21
9.3 Convenience 22
Annex A (informative) Comparison between office IT systems and home electronic system security requirements 23
Bibliography 24

Figure 1 – A concept model of home networks 10
Figure 2 – Different considerations in different home environments 11

Table 1 – Security threats and corresponding defences 18

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

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 – 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.

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.

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

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 – 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”.

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

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

2.2 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

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

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 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.

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.

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

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

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.

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.

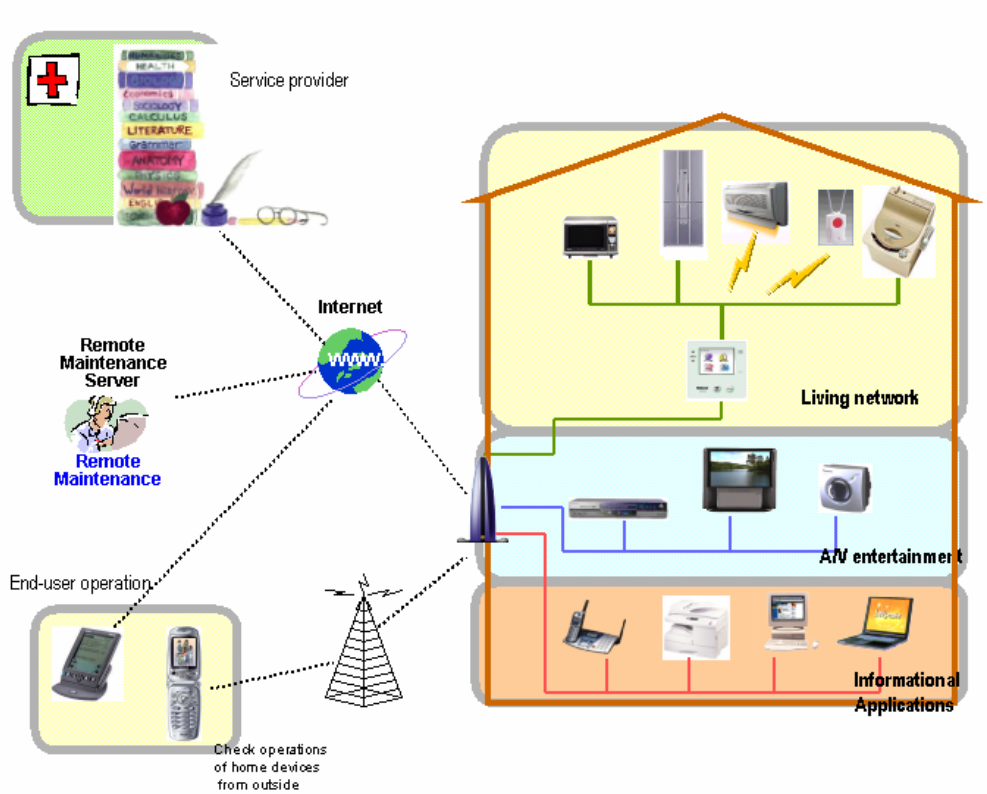
However, there still exist some different characteristics between domestic applications and corporate applications, home networking infrastructure and enterprise networks, residential users' needs and business workers' needs. Therefore, it is necessary first to introduce some

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

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.

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



Living network: May comprise a washing machine, an air conditioner and an electric rice cooker and can provide control operations of activation/deactivation from either inside or outside.

A/V network: May comprise TVs, DVD players and other audio/video equipment and can provide Internet connection through TV (providing discriminative services compared with those offered by PCs).

Versatile composite home theatre systems capable of sharing audio/video resources between audio/video equipment and PCs.

Information equipment network:

May comprise home servers, printers, PCs, laptops, PDAs, image phones, VoIP servers and handsets and can provide

printing out DTV screen to some printer connected with PC,

searching application data stored in PCs, PDAs or image phones,

VoIP-based video/audio communications.

Figure 1 – A concept model of home networks

Lastly, at careful examination of the possibilities of home networks, it comes to light that the security requirements can be divided into two parts: defence against outside threats and defence against inside threats. Figure 2 shows different considerations in different home environments.

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

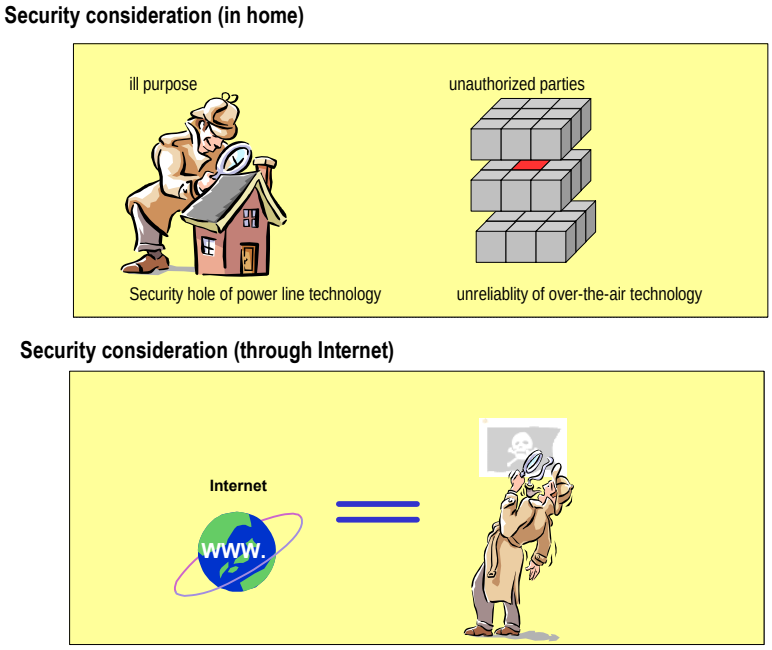


Figure 2 – Different considerations in different home environments

For the inside-home issues, security problems may come from insecure networking technologies, such as power line or wireless, and access control for different users/usages. As for the outside-home issues, they may almost be the same as security holes over the Internet.

4.3 Issues related to HES security but out of scope of this standard

4.3.1 DRM

Digital rights management (DRM) is concerned with the problem of illegal copying and distribution of digital material with copyright. Typical examples are computer software, music and movies. These may either be delivered over the network or on a device such as a CD.

It is in the interest of content providers that no illegal copying of content is made by a home owner/inhabitant. Since this is not a threat to the home owner/inhabitant, but rather to the content provider, it is out of scope of this standard.

4.3.2 Parental control

In many homes where children are present there can be a need for the parents to protect their children from access to data that may cause them harm, such as films with violence and pornography. The technology to achieve this is by means of access control. This can be in various forms. One is to forbid access to unwanted service providers. Another is to only allow access to a selection of permitted providers. In addition, data can be marked as not suited for children and thus allow for an access control mechanism based on this information. This latter method only works if the data has been appropriately marked and that this marking can be understood by the access control method. Neither of these can, however, be guaranteed.

4.3.3 Crime reducing products and services

Criminogenic products and services is the term used for products and services with a propensity to become the targets or the tools of crime. There are presently no standards in this area, but one should note that in the future there might be technical requirements on the HES in order to reduce crime on both products installed in the home as well as on services.

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

4.3.4 Consumer issues

There exist several guidelines on how to use a system. All users of the HES may be well served by guidelines on how to use the system (e.g. electronic shopping) and how to maintain and update a system in order to avoid vulnerabilities, such as avoiding viruses, worms, etc.

4.3.5 Service provider issues

There are security requirements on service providers in order to enable the users and owners of HES to trust the data from them. This is true for all types of service providers, such as those providing data for users (e.g. in the form of A/V services), those providing services for the home (e.g. monitoring burglar alarms), and those providing services to the HES (e.g. delivering software and firmware updates). All these service providers shall give the HES users and owners assurance that the incoming data can be accepted, that is that the data is coming from a trusted source and that the data is protected during the communications both for privacy reasons and against malicious modifications.

4.3.6 Fallback issues

In any complex electronic and software system there is the possibility of things going wrong, for example by equipment failure, software bugs, human error, lightning, flooding or malicious damage. It is thus important to consider fallback technologies and procedures for safety critical components of the home. As an example, door locks that depend on the HES need a fallback mechanism so that the inhabitants will still be able to unlock and lock the doors.

4.3.7 Outsourcing issues

There is an issue on how to maintain the security of the HES when the responsibility for support of information processing has been outsourced to another organization. The contract shall at least address the risks, security controls and procedures. ISO/IEC 27002 [1] gives examples of issues that such a contract may address.

5 Challenges

5.1 General

The challenges of home networks mainly come from a complex assortment of devices, various types of physical media and the different communications protocols used. Some security challenges when deploying some well-known home networking infrastructure are listed below.

5.2 Always-on challenge

"Always-on" broadband connectivity makes Internet access fast and easy. Unfortunately, it also leaves your home, office or business wide open to Internet hazards, such as hackers and viruses.

Home devices with “always-on” connections are especially vulnerable to attacks, since they are usually kept on-line for 24 hours a day and always connected to the Internet with the same IP address.

5.3 Power line challenge

Issues of ensuring data stay secure arise for houses using the same power lines, especially those in older areas. Most houses share the same “power-line subnet” with neighbouring houses connected to the same distribution transformer. Power-line commands from one house can easily reach devices in other near-by houses and thus interfere with the intended controlling of those devices.

---

[1] See Bibliography.

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 Wireless challenge

Wireless networks pose many new security challenges as opposed to traditional wired networks. The nature of wireless networks makes them vulnerable to various forms of attacks such as passive eavesdropping, active interfering, leakage of secret information, data tampering, impersonation and denial of service. Malicious users no longer need to gain physical access to the network medium. They can simply stay within the transmission range of a sending node to intercept that user's transmissions.

5.5 Complex assortment devices challenge

Potential networked home appliances comprise: white goods, brown goods, telecom equipment, computer equipment, lighting systems, house maintenance systems, alarm and monitoring systems, health care systems, and so on. Some of them, such as white goods or lighting systems, are constrained by limited resources and cannot offer complex computation. But some of the information devices or A/V devices support variant applications and require higher security strength to protect data. Security services for these variant devices need different consideration.

5.6 Many and diverse user needs

When speaking of user needs, one recognizes that each user is an individual with specific needs based upon his/her lifestyle, economic situation, education, and so on. Different home models bring different security requirements, for example, security concerns coming from a family with only a couple may differ from those of a couple with teenagers.

Most teenagers are trying to establish some degree of independence. This might include ownership of personal networked devices and probably would include inviting friends over to the house. What if the teenagers don't want to share their contents in DVD with their parents? What if those friends want to plug their own networked components into the home networks?

On the other hand, parents may want to impose some limitations on their children. For instance, parents may want to ensure that children will not be able to access TV programs after 7 PM on school days, or children under 12 years may not be allowed to view an R-rated movie on the DVD-player.

For a single-person home, all the devices within the home belong to that person and there may be no access control requirement inside the home. However, the householder may still want to delegate some privileges to service providers for maintenance purposes, which makes the task of securing the network from outside access necessary.

5.7 Many and diverse applications

Applications in home networks could be roughly categorized as

a) home automation: home control, home security and monitoring,

b) entertainment,

c) information and communication.

For these different applications, security requirements may not be the same.

For home automation, white goods manufacturers will include a network interface in their products so that service providers with householders' permission can remotely monitor the status of equipment and consumables. In addition, steps shall be taken to ensure that control commands can only come from approved, secure source addresses.

For entertainment, users always wish to connect their home entertainment devices together to enable the distribution and sharing of digital video and audio throughout the house. But the

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

access control problems arise due to the convenience of connectivity. Also, device owners may wish to make sure that the authorized users use only certain content.

For information and communication, protection of privacy has become more important than other issues because communication may include some financial statements, bank account and credit card information as well as personal details.

6 Security models

6.1 Introduction

Creating a complex HES that is trustworthy and managing it in order to keep it trustworthy is a non-trivial task. This task depends on security policy enforcement methods which in turn rely on the application of security techniques such as access control, integrity protection, etc. Three completely different scenarios or models can be identified for the security of HES. It is not surprising to see that all of these resemble different forms of enterprises. The threats and security requirements in a home are, however, often weighted differently from those in an enterprise. This standard denotes the three models as:

- the owner supported single home HES (OSS);
- the externally supported single home HES (ESS);
- the externally supported multiple homes HES (ESM).

6.2 Owner supported single home HES (OSS)

The first and simplest model consists of an isolated unit with its own HES (comprising one or more system units), which is managed entirely by the owner or inhabitant of the house. This corresponds roughly with the private use of a computer system with Internet connections as seen today. Many of the threats and weaknesses of such a computer system are also to be found in this architecture.

However, most home owners/inhabitants are generally unfamiliar with computer security and would benefit from the availability of guidance in the form of security checklists. A better approach might be to use professional support for the security of the HES. This leads us to the next architecture.

6.3 Externally supported single home HES (ESS)

The second scenario also involves single homes. But instead of letting the owner/inhabitant be responsible for the HES, and in particular for the security and trustworthiness of it, the responsibility is outsourced to a professional IT service provider. This is very similar to the way most small enterprises, too small to possess an own IT department, are set up. The service provider can ensure that appropriate security solutions are selected, correctly installed and maintained. The advantage with this scheme is that security and trust, which can be difficult and time-consuming to install, maintain and keep up to date, is under responsibility of professional expertise.

One can, however, go a step further and let the HES be held, run and handled by a professional service provider. This leads us to the third model.

6.4 Externally supported multiple homes HES (ESM)

The third model is where a service provider serves a number of homes. These can be non-localized homes spread out over a large area. But it can also be an apartment house or a group of townhouses, where all apartments in the house or the townhouses in the area are served by a local service department. One of the major differences between the first two models and this one is that in the former the communications to and from the house are direct whereas in the latter the communications are through the ESM.

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 this scenario, the home owner/inhabitants have a similar role as an employer or department in a large organisation with a professional IT department. This would certainly be the most convenient and secure solution for most home owners and inhabitants. If this architecture were the most common one, its success would certainly depend on the monthly cost these services would charge. These charges might be counterbalanced if insurance companies reduced the premiums for those clients adopting these services.

7 Threat analysis

7.1 General

In a threat analysis one looks at possible damages for home owner/inhabitant caused by actions on the HES, the home network or any pieces of information in the system.

Threats to home system and networks are similar to those to enterprise system and networks. However, various threats differ in significance for domestic, rather than commercial, network configurations and applications. For instance, while repudiation (denying that a transaction took place) is obviously a serious issue for a bank or brokerage firm, it is of less concern for the home, where the transaction is likely to be entirely private and non-commercial. Conversely, businesses have little to gain by concealing which hours of the day their networks are busiest, whereas residential users may very well wish to conceal traffic that indicates whether or not they are at home.

Home users may feel less vulnerable because their network devices aren't mission-critical corporate systems holding vital company information and will not very likely become the target of attacks, but such a view is outdated. Home network devices may not be the final target to hack, but a launching point to attack other devices targeted by intruders.

Because it is not usually possible to determine the motive while you are under attack, home users need to be sufficiently aware of the threats and know what solutions are available.

The following threats to the home system and network have been identified.

7.2 Unauthorized access

It is obvious that home users care about "which things are authorized to do what actions or access what data on each device?" For example, in the case of a VCR player and its controller, only the VCR controller corresponding to the VCR player can access the VCR player. In other words, the VCR controller owned or operated by the non-family member, such as a guest visiting the home, a neighbour or a user accessing through the Internet, may not be allowed to access the VCR player owned by a particular family. There is thus a need to protect the HES from unauthorized users and from events triggered by unauthorized systems in and/or outside the home.

An unauthorized intruder may, for example, be an automated system that is programmed to search for vulnerable messages, or a person who has wiretapped or otherwise violated the integrity of the communications channel.

The access may be passive or active. A passive interception amounts to eavesdropping, in effect, reading someone else's traffic. An active interception may involve changing the contents of the message, deleting or rearranging part of the communication, or changing its protocol control information, particularly the header (including the destination or source address).

Most threatening is an active (local or remote) intruder who is able to manipulate the HES, install a Trojan horse or perform services on behalf of the house owner/inhabitant. A Trojan horse can allow unauthorized users and processes access to the data and the system thus violating confidentiality and integrity and potentially also the availability of data and system.

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

A form of unauthorized access is when an imposter pretends to be a legitimate user, such as the home owner. This is called masquerade. The imposter could also pretend to be a service provider that has contracted with the home owner.

Another way an imposter may trick the home system into thinking it is an authorized user is for the imposter to capture a legitimate message and resend it at a later time. This is called a replay attack. For example, if the imposter can intercept a message to the home's burglar alarm system, telling it to turn off, a replay of that same message at a later time may achieve an undesired result.

A passive intruder who is only able to read data can also be a threat. Data can be sensitive either from a privacy point of view or can indicate if the house is empty. The former can reveal personal data and an example of the latter is that the reading of the heating settings can be very informative for a potential burglar. These threats exist for all three models. It is thus important to ensure that only authorized users have access to the HES and its data and that alien systems cannot easily tap this type of data from the HES.

Even if all communication employs integrity and confidentiality services, an eavesdropper can still learn a great deal about the home network by monitoring source and destination information and the time of each message. This is called traffic analysis.

The threats to privacy infringements are larger for the two latter architectures (ESS and ESM), since in these not only the inhabitants but also external organisations supporting the HES may be authorized to access the system. It is recommended that these organisations, however, only be able to maintain the HES and would not access privacy-critical information. This is a non-technical issue and relies on the trust relationship between the service providers and their customers.

7.3 Malicious software and configuration

Malicious software or configuration can, for example, enter the HES through communication links or by loading an infected software package at home. The most obvious examples of malicious software are a virus that enters the HES. A virus may destroy data and software programs and make the system inoperable. These are threats to the integrity of the software and configuration information on the access device and home network devices.

A Trojan Horse is an unauthorized program that enters the home or the access device hidden in a legitimate message. Once in the home, the Trojan Horse can reside in a processor in any networked device. For example, a Trojan Horse can be inserted into an intercepted MPEG transport stream as private data and take up residence in the processor of the digital television. It could then use the resources of the television's processor and the digital home network, to compromise the security of the internal network.

Worms and viruses have received considerable publicity in both the technical and popular press. A worm is a program that can replicate itself and send copies from computer to computer across network connections. Upon arrival, the worm may be activated to replicate and propagate again. In addition, the worm usually performs some unwanted functions. A worm that invades the home network could thus spread across the network to multiple devices; if the worm performs harmful activity, such as wiping out the non-volatile memory of the device, the home owner could find that multiple appliances, from DTVs to toasters, no longer work properly.

A virus is code embedded within a program that causes a copy of itself to be inserted in one or more other programs, as well as performing some unauthorized functions on the host machine. Unlike a worm, a virus will not actively try to spread itself to other processors on the home network, so its damage will be confined to a single appliance. However, an appliance essential to the operation of the home network may function in unpredictable and undesired ways.

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

Certain attacks may attempt to compromise the home network configuration by altering security information. Three examples of this type of security information are addresses of external servers, trusted public keys or passwords used in the authentication process and rules for filtering unwanted traffic at an access interface.

7.4 Denial of service

Denial of service makes the system inoperable. For some installations inoperability causes inconvenience and only requires a retry at a later time. In other situations it can be a serious threat to the home, for example by disabling an alarm system.

A denial of service (DoS) attack is affected by flooding an access network with useless traffic and preventing legitimate messages from reaching the home network. The incoming messages could also force the home network to try to respond, tying up resources in the access device, thus impairing outgoing traffic. The home network may be a victim of a DoS attack, or an unwitting participant. If a computer on the home network is compromised, the attacker may be able to use it to contribute to the packet flood without the knowledge of the home owner. This is called a distributed denial of service (DDoS) attack.

7.5 Unintended modification of data during communication

It may happen that a piece of information is accidentally modified or replayed during the communication so that the message is wrongly interpreted. Minor modifications of single bits during the transfer may be corrected by standard error correcting code, but real integrity protection during the communication requires cryptographic technologies.

7.6 User errors

There is a risk that an authorized user makes errors and invokes the wrong service or gives faulty parameters in a command. Such errors are likely to be of less significance when the inhabitant is at home than when away from home. One way to minimize such errors is to provide the user with a device with a simple user interface that is easy to use and that performs input validation. Another countermeasure is to limit the set of commands that can be invoked when away from home.

7.7 System failures

Failures to a home electronic system will most certainly occur sometime. This can either be due to a security breach or due to instability of system, power failure, lightning, or many other reasons. The effect is that parts or all of the data and system are no longer available. There is thus a need for a recovery process, and possibly for fallback technology and procedures.

7.8 Security service providers

Finally, it has to be stated that for the security service provider, as the central focusing point in the third architecture (ESM), a whole set of sophisticated security measures has to be installed. These are similar to many other organisations handling sensitive data, and they shall be operable 24 hours a day seven days a week. These requirements will, however, not be described in this standard.

8 Security requirements

8.1 General

A home owner/inhabitant can build his/her trust relationship with the help of a number different devices and procedures. Trust in the HES will generally comprise a mixture of technical counter measures (such as Firewalls, anti-virus software, etc.), procedural measures (such as application of software upgrades, backup and restore measures, security training and awareness) and miscellaneous measures such as insurance. This includes the

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

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

following guidelines and procedures on, for example, how to install, configure, maintain, update or use the system.

It should be noted that many of the security mechanisms and services that have been developed to counter potential threats in business environments may not be appropriate for home networks due to the limited IT capabilities such as sensors and household appliances.

Below follows a set of security threats, some very serious and others less so, for which security solutions are available for a HES in order to improve the trust in it. Table 1 summarizes some defence mechanism against the threats listed in Clause 7.

Table 1 – Security threats and corresponding defences

Threat	Defence
Active interception:	
adding messages	Data authentication,
modification of data	Data integrity
Denial of Service	Firewall, access control, ingress filtering
Eavesdropping	Confidentiality services
Masquerade	User / device authentication (part of access control)
Remote access	Access control
Replay	Anti-replay services, replay protected authentication
Repudiation	Public key cryptography
System failure	Recovery, fallback, failsafe
Traffic analysis	Padding of messages
Unauthorized access to data in communication	Confidentiality services
Unauthorized access to data in system	Access control
Unauthorized access to system	Access control
Unintended modification of data	Error correcting code, data integrity service
User error	User interface, remote access control
Virus, worm, Trojan Horse:	
Open files and attachments	Management, software
Install new SW	Management, software
Update SW on line	Authentication
Update SW locally	Management, software

8.2 Access control

Unauthorized access to the HES and its services is the most severe threat as was identified in Clause 7. The protection against this threat is a good access control mechanism. It is good practise that different levels of access rights are given to different persons. For the first model (OSS) it is important to distinguish the user, acting as an administrator of the system, from the same person acting as a normal user. Several levels of access rights are plausible. There are some functions that can be permitted to anyone, whereas to other functions only limited access will be given, for example to children. There are also good reasons to provide more limitation of the access rights when away from home than when acting from home (see remote access and control below.)

Firstly, enrolment and registration of authorized users. It is important to carefully manage registered and authorized users. For example, it is good practice to immediately revoke the

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

access rights of users if their pattern changes, for example the rights for a visitor to enter the home shall be revoked if the visitor leaves earlier than initially planned.

Secondly, proper authentication of the user, that is the verification of the identity of the user, is a necessary condition for an access control system. Only after the identity of the authorized user has been verified by the HES can the correct access rights for the requested resources for that user be provided. The first step is, however, the requirement to register the authorized users. This is not so difficult in the first model described above, but for the other two, and in particular for the third architecture it is important that the service provider register the house owner/inhabitants and users correctly.

Masquerade can be thwarted by use of access control with proper authentication and combined with a data integrity service.

However, authentication falls short of effectively coping with replay attacks. Nevertheless, replay attacks can be defended using time-variant parameters providing uniqueness and timeliness. One simple way is to check for repeated messages; this can be done, for example, by checking the timestamp or sequence number fields against previously stored messages.

In addition to the physical and logical access control to the building, sensitive devices of the HES need to be protected. For example, if maintenance is made by an outsider at the home it is good practice to require an authentication before giving access to the building and equipment. Also any remote updates and maintenance require authentication.

8.3 Data and message authentication

Another concern is proper authentication of messages coming from the service requester, where the messages in either direction (from user to home or from home to user) require authentication. The authentication requirement on messages from user to home is obvious, since these are the messages that will effect certain actions inside the home. However, it is also good practice to let the response messages from the home to the user also be authenticated lest an adversary inserts a fake acknowledge or confirmed message when in fact the original message was never received. Also, authenticated notifications and responses from home may eventually include status information, such as the temperature of the house or whether the alarm system is turned on.

8.4 Remote access control

Often the inhabitant wants to access the HES when away from home. It is thus necessary to allow access to the system from outside. This requires good authentication mechanisms as described above. Compared with business environments, where a user normally only accesses the IT environment and thus normally receives the same access rights as usual, a home environment in addition supports remote control on many house devices. This may require a different access control with less access rights when acting remotely in order to limit the number of operations and parameters that can be used. Since unintended operations are harder to observe when away from home, attention to the user interface on the device used for remote access also require special attention in order to avoid mistakes.

8.5 Protection of communications

In general, a user will not want any eavesdropper to understand the content of a message. This applies not only to the body of the message (which will contain the command to be executed), but also to its header fields that may reveal information about the devices one owns. For example, the [To:] header field will contain a URL of the addressed entity, which may also indicate its device type and location. A user may not want anyone to know whether there is a television set in the home and certainly not in which room it is located.

There are four types of communications in a home environment. By cable in the home, wireless in the home and by cable or wireless to and from the home. All of these, perhaps with the exception for data sent by cable within the home require confidentiality and integrity

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

protection in order to ensure that only authorised users have access to the data and that unauthorized modifications can be detected. The security requirements for communications by means of cable within a single home depend on what form of cable is used. Generally, it can be stated that if there is a likelihood that communications can be detected outside the home, then there is a need for confidentiality protection. Furthermore, if an outsider is able to modify or insert data to the system, integrity protection might also be required.

Protection against traffic analysis can be made by creating dummy traffic to hide useful messages.

The protection of data during communications is taken care of by confidentiality, integrity and privacy protection services and by authentication services at the target. It is important to base such solutions on internationally accepted standards in order to ensure interoperability with the external world.

8.6 Firewalls

If home users are concerned about protecting home devices and data in the houses from outside intruders, they need a firewall. A firewall is usually located between the local network and the Internet. Additional firewalls may be used to segment the local network into multiple security domains to protect individual devices. It can be used to control ingoing and outgoing network traffic.

The main purpose of a firewall is to prevent network hacking attacks from the outside. System responses to service refusals shall be designed to prevent a potential hacker deducing useful system information such as physical IP addresses.

It should be noted that a firewall that is effective against the IPv4 protocol-based communications might not be effective for communications based on the emerging IPv6 protocol.

8.7 Virus protection

To have a virus, worm or a Trojan Horse on a HES is everyone’s nightmare. Protection against these is not a purely technical issue. Much is due to the behaviour of the users of the HES. One shall therefore follow a strict policy, which, for example, says to be careful when opening email attachments from unknown sources. Another counter against a virus attack may be obtained by an access control mechanism by denying access by any party that is not able to correctly authenticate themselves.

Technically, there are different methods to detect such malicious software. There is, however, no standard that can be applied to protect against viruses. New viruses enter the international network every day and there are several companies working hard to find protections against them. It can either be entering the system through external communications like attachments in emails, but can also arrive through loading of infected software within the HES. The suggested approach is to get a virus protection software package from one of the manufacturers of virus protection tools and make sure it is regularly updated.

8.8 Protection against denial of service attacks

There are two kinds of denial of service. One occurs when a genuine user of the HES tries to access a remote service and this access is denied. In this case the service to be accessed might be overloaded or it has been hit by a denial of service attack. The options for the genuine user are very limited. In this case, it is possible to try another service or to wait until the traffic load is reduced or the service is reset.

The other situation is that the HES has received a denial of service attack. Denial of service attacks are almost impossible to defend against in real time. In fact, security mechanisms alone cannot be effective against denial of service attacks, as it is trivially easy to overwhelm

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

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

any defence by sending additional bogus messages. Careful design and implementation of the protocol and access device can mitigate resource exhaustion, whereby the flooding ties up parts of the home network or access device. For example, if the access device recognizes that it is being asked to open 5 000 simultaneous TCP connections, it could go to an alarm condition, in which it ignores additional incoming requests that are not properly cryptographically authenticated, and it gives priority on its output queues to messages originating in the home.

To ensure the home network does not become an unwitting participant in a distributed denial of service attack, measures shall be taken to ensure illicit software is not installed. Access control devices with implemented ingress filtering, as specified in RFC 2267 prevents the use of spoofed IP addresses. It should be noted, however, that it has no effect if the attacker uses valid network addresses. Ingress filtering makes tracking down the source of the attack much easier because the packet source address is the source of the traffic. An additional benefit is that the victim's response is returned to the attacking system, thus preventing additional damage. To perform ingress filtering, the access devices block any packets with source addresses that do not originate from within the home network.

8.9 Auditing

Auditing is a security mechanism that does not perform any protection mechanism but which is commonly used to control and verify that applied security mechanisms are functioning as intended. Auditing records sensitive security related operations. It has to be decided which security operations have to be recorded. If all security related operations on the system are recorded then it might be difficult to detect any unintended event among the large amount of data recorded. On the other hand, if only very limited sensitive operations are registered, security breaches may not be detected.

In general, one can state that at least those operations that are related with the setting of security parameters, like registration of users and all failed authentication attempts ought to be registered. Even the successful authentications are often useful, since one can then determine by whom the system was used at a certain time.

8.10 Recovery

In case of failure of the system, there is a need to be able to restart it. It is irrelevant if the system has broken down due to a security breach or from another type of failure. The most appropriate method in preparing a recovery is to regularly make back-ups of the system. How often back-ups need to be made depends on how often changes to the HES are made.

9 Requirements on security solutions

9.1 General

The requirements in this clause specify the form and capability of a security solution rather than the type of protection it provides.

9.2 Different levels of security services for different applications in a home

For different activities, different levels of security are often adopted. For example, controlling an air-conditioner's temperature in a bedroom from the living room does not require the same level of security as controlling a home device from outside. Due to various factors in home networks, it is almost impossible to have a turnkey solution to provide security services that could cover different home networking models, diverse user needs and applications at a time.

There is thus a requirement that a security solution shall be able to support several security quality levels within a single home.

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

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 Convenience

In general, residential users will choose solutions that will not cost them too much money and will not require much knowledge to make the solutions work. So the chosen solutions shall as much as possible meet the following requirements:

a) low cost,

b) low complexity,

c) easy to use (as automatic as possible).

Also, reliability is essential to residential users. If the process is not maintenance-free, easy to use, quick to install, it is not likely to be adopted. Users don't to engineer or administrate a complex system. This is particularly important for the security model OSS, but also for ESS and to a lesser degree the ESM model described above.

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

Annex A
(informative)

Comparison between office IT systems and home electronic system security requirements

An office IT system is a pure information system that, in contrast to home electronic systems (HES) is not used to control devices except IT devices such as printers, etc. The internal network and security requirements can thus differ substantially. The security on the external network are, however, much more similar. Since a home office is part of the HES, a HES encompasses all external requirements as an office system. In addition, there are a few other threats to the home that need to be considered.

The few additional requirements that have been identified on external information security for HES compared to home and office IT environments are the following.

- Like some offices too, the intelligent home is on line 24 hours a day 7 days a week.
- There are not only the requirements of remote access to the system, but also remote control of devices in the home, such as the heating. However, not the same access rights are given to the devices when controlling them remotely as when controlling them from within the home. Thus, it must be distinguished if the control is made from within the home or remotely. This might, for example, be solved by letting the gateway direct the communications to a different access control mechanism than that used when accessing the system from within the home.
- The equipment, from which the devices in the home are controlled, in particular in case of remote control, must be designed in such a manner that mistakes are avoided. There are thus security requirements on the user interface of the device from which the remote control is made.
- In case of a system failure, there must be fallback solutions, that is, it must also be possible to control the devices that normally are managed via the home electronic system without the system, for example locks on the doors. A failing system must not block the use of those devices.

The HES must also be failsafe. This means that in case of a failure the devices must be set in a state that cannot cause harm to the building or inhabitants. This requirement is mostly concerned with the devices controlled by the system and not by the system itself.

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

ISO/IEC 10116, *Information technology – Security techniques – Modes of operation for an n-bit block cipher*

ISO/IEC 18028 (all parts), *Information technology – Security techniques – IT network security*

ISO/IEC 18033-3, *Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers*

ISO/IEC 27002, *Information technology – Security techniques – Code of practice for information security management*

European commission COM (2001) 298

Network and Information Security: Proposal for A European Policy Approach

http://ec.europa.eu/transparency/regdoc/liste.cfm?&type=1&annee=2001&numero=298&ElementsPerPage=20&tri=cote&CL=en

Freier, A.O., P. Carlton and P.C. Kocher, The SSL Protocol Version 3.0.

Dierks, T. and C. Allen, The TLS Protocol Version 1.0, RFC 2246, Internet Engineering Task Force, January 1999.

Kent, S., R. Atkinson, Security Architecture for the Internet Protocol, RFC 2401, Internet Engineering Task Force, November 1998.

NIST, FIPS PUB 197, "Advanced Encryption Standard (AES)," November 2001.

RFC 2267, *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing*

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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 919 02 11
Fax: + 41 22 919 03 00
info@iec.ch
www.iec.ch

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