

CEA Standard

Security Services for the Versatile
Home Network

CEA-851.2

December 2002



CEA[®]
Consumer Electronics Association

www.CE.org

NOTICE

Consumer Electronics Association (CEA[®]) Standards, Bulletins and other technical publications are designed to serve the public interest through eliminating misunderstandings between manufacturers and purchasers, facilitating interchangeability and improvement of products, and assisting the purchaser in selecting and obtaining with minimum delay the proper product for his particular need. Existence of such Standards, Bulletins and other technical publications shall not in any respect preclude any member or nonmember of CEA from manufacturing or selling products not conforming to such Standards, Bulletins or other technical publications, nor shall the existence of such Standards, Bulletins and other technical publications preclude their voluntary use by those other than CEA members, whether the standard is to be used either domestically or internationally.

Standards, Bulletins and other technical publications are adopted by CEA in accordance with the American National Standards Institute (ANSI) patent policy. By such action, CEA does not assume any liability to any patent owner, nor does it assume any obligation whatever to parties adopting the Standard, Bulletin or other technical publication.

This CEA Standard is considered to have International Standardization implication, but the International Electrotechnical Commission activity has not progressed to the point where a valid comparison between the CEA Standard and the IEC document can be made.

This Standard does not purport to address all safety problems associated with its use or all applicable regulatory requirements. It is the responsibility of the user of this Standard to establish appropriate safety and health practices and to determine the applicability of regulatory limitations before its use.

(Formulated under the cognizance of the CEA's **R7 Home Network Committee**.)

Published by

©CONSUMER ELECTRONICS ASSOCIATION 2002
Technology & Standards Department
1919 S. Eads Street
Arlington, Virginia 22202

**PRICE: Please call Information Handling Services, USA and Canada (1-800-854-7179)
International (303-397-7956), or
<http://global.ihs.com>**

All rights reserved
Printed in U.S.A.

PLEASE!

DON'T VIOLATE
THE
LAW!

This document is copyrighted by the Consumer Electronics Association (CEA[®])
and may not be reproduced without permission.

Organizations may obtain permission to reproduce a limited number of copies by
entering into a license agreement. For information contact:

Information Handling Services
15 Inverness Way East
Englewood, Colorado 80112-5704
or call U.S.A. and Canada 1-800-854-7179, International (303) 397-7956
See <http://global.ihs.com> or email global@ihs.com

Contents

FOREWORD	4
1 INTRODUCTION	5
2 GENERAL	6
2.1 Scope.....	6
2.2 Normative references.....	7
2.2.1 Normative reference list.....	7
2.2.2 Normative reference acquisition	9
2.3 Informative References	9
2.3.1 Informative document list.....	9
2.3.2 Informative document acquisition	10
2.4 Symbols and abbreviations	10
2.5 Compliance Notation	12
3 Security Services for the Versatile Home Network (VHN)	12
3.1 Coordination of Access Device and Host Security.....	14
3.1.1 IPSec Configurations.....	15
3.1.2 SSL/TLS Configurations.....	16
3.1.2.1 Securing the Browser	19
3.1.3 Authorization	19
3.2 Firewall	20
3.3 Event Logging.....	20
ANNEX A: Security Services	22
A1 Introduction	22
A2 Home Network Threats	22
Software and Configuration Security: Trojan Horses, Worms, Viruses	23
Repudiation	24
A3 Home Network Defenses	24
A3.1 Encryption.....	26
A3.1.1 Conventional Encryption.....	26
A3.1.2 Public-Key Encryption.....	26
A3.1.3 Digital Signatures and Key Exchange.....	27
A3.1.3.1 Diffie-Hellman Key Exchange	28
A3.2 Authentication and Authorization	28
A3.2.1 Firewalls.....	29

A3.3	Integrity and Confidentiality.....	30
A3.3.1	Message Authentication Code (MAC).....	30
A3.3.2	Hash Functions and Digital Signatures.....	31
A4	Home Network Security Solutions	31
A4.1	IPSec	32
A4.1.1	Security Associations and the Security Policy Database	32
A4.1.2	Transport Mode and Tunnel Mode:.....	32
A4.1.3	Authentication Header (AH):.....	34
A4.1.4	Encapsulating Security Payload (ESP) Header:	35
A4.1.5	Combining Security Associations.....	37
A4.1.6	Key Management:.....	38
A4.2	SSL/TLS	39
A4.2.1	SSL/TLS Record Protocol and SSL/TLS Handshake Protocol:	39
A4.2.2	The SSL Session and the SSL Connection:	39
A4.2.3	SSL Session States:	40
A4.2.4	SSL Connection States:.....	40
A4.2.5	SSL Message Exchange:.....	40
A4.2.6	SSL Session Establishment:.....	41
A5	A Note on Link-Level Security in the Home Network	42

Table of Figures

Figure 1: IPSec Transport Mode—One or more security associations apply between end stations (adapted from [42]).	33
Figure 2: IPSec Tunnel Mode—A security association is applied at network boundaries (adapted from [42])......	34
Figure 3: The IPSec Authentication Header (AH) (adapted from [42]).	34
Figure 4: AH in Transport Mode and in Tunnel Mode (adapted from [42]). In this example, the IP payload is a TCP segment.	35
Figure 5: The IPSec ESP Header (adapted from [42]).	36
Figure 6: ESP in Transport Mode and in Tunnel Mode (adapted from [42]). In this example, the IP payload is a TCP segment.	37
Figure 7: Iterated Tunneling in IPSec (adapted from [42])......	38

Figure 8. The SSL Protocol Stack (adapted from [42])..... 39
Figure 9. Operation of the SSL Record Protocol (adapted from [42])..... 41

Table of Tables

Table 1: How IPsec, SSL/TLS and Firewall Defend the Home Network against Common Threats. 13

CEA-851.2, Security Services for the Versatile Home Network

FOREWORD

This standard was developed under the auspices of the R-7.4 Joint CEA/VESA Subcommittee.

The Video Electronics Standards Association (VESA) established the VESA Home Network (VHN) Committee in 1995 to develop architecture for a digital, broadband home network. The VHN standard was initially developed by the VESA Home Network Committee. However, it was never ratified as a VESA standard.

In June 1999, the Consumer Electronics Association (CEA) established the R7 Committee to help harmonize the several efforts being undertaken to develop home networking standards. In January 2000, the Board of Directors of VESA and the Board of Directors of the Consumer Electronics Association agreed to merge the VESA Home Network and the CEA R7 Committee, by establishing the CEA R7.4 Committee.

After publication of EIA/CEA-851, the "VHN Home Network Specification," in October, 2000, R7.4 immediately began work on expanding and augmenting Version 1 of the standard. In order to avoid delays in making new material available, as new sections are developed, they will be issued as separate standards in the 851 series. This standard, EIA/CEA-851.2, specifies the implementation of security services for the VHN. Another standard in this series, EIA/CEA-851.1 "IP-Based Digital Telephony for the Versatile Home Network," was issued earlier. Other standards, dealing with network management and other topics, will be issued in the near future.

1 INTRODUCTION

This standard defines security services for the Versatile Home Network. The threats to a home network are similar to those of an enterprise network. However, the 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.

Given the threats that are common to enterprises networks, we have identified the most likely threats to the Versatile Home Network, and defined a set of security services to defend against those threats. We have recognized that, as those threats are not peculiar to home networks, there is no need to invent *new* security mechanisms for the home network and access device. In fact, the difficulty of designing such mechanisms correctly and standardizing the results of such designs argues strongly against inventing new security mechanisms.

However, for several reasons, security mechanisms appropriate for a business may not adapt well to home network security:

1. The first issue is cost. Some security mechanisms, such as industrial-strength firewalls, cost on the order of \$10,000. Businesses write this off as an expense and recover cost by raising prices. Homeowners have no such option and probably do not perceive the threat to the home network as sufficiently important to merit that level of expense. Thus, a security mechanism must be inexpensive, or be able to be made inexpensive, if it is to be used in the home.
2. The second is complexity. Many security mechanisms are difficult to configure and require an expert to install and maintain. Once again, an enterprise may have an IT department that is responsible for network security. The typical homeowner is unlikely either to acquire the expertise or hire an outside consultant to do this job. Faced with such a choice, she may elect simply to do without security. Thus, simplicity of operation is essential to home network security.
3. The third is convenience. Employees of a business may be willing to endure a certain amount of inconvenience if management decides that's the way the business operates. While passwords and smartcards are accepted as necessary to protect the company's resources, it's not clear how much inconvenience a homeowner may be willing to accept to protect the home's resources. For example, most people will probably understand the necessity of having a password to access a networked digital VCR from a remote location, such as an

airport. However, they might find it inconvenient to use a smart card and may object to a sophisticated set of password complexity and aging rules¹.

4. The fourth is the different security priorities for a home and a business. Enterprises are likely to be concerned with coordinated and targeted attacks by outsiders, with sabotage by insiders, discovery and litigation, and protection of intellectual property. Residential users are, perhaps, more rightfully concerned about privacy of their personal data, physical security and safety of their home, accuracy of credit and billing records, public knowledge of their private life (such as knowledge of their whereabouts and interests), and protection from widespread data gathering, snooping, and junk mail.

The task for home network security, then, is to choose among the security services that have been developed for enterprise networks, within the constraints imposed by cost, complexity, convenience, and relative priorities. As the VHN is a home intranet—and IP-based network using web tools for device access and control—we require SSL/TLS and IPSec for primary protection against threats external to the home network. Furthermore, we require firewall protection at the access device, and define the functional requirements for the firewall. Future versions of this standard will address protection against *internal* threats to the home network (e.g., rogue software that may be introduced via a floppy disk), as well as refinements to the current specifications.

The requirements for VHN security are presented in Section 3. Annex A presents a discussion of security issues, and a discussion of the factors that were considered in formulating the requirements in Section 3.

2 GENERAL

2.1 Scope

This standard specifies security services for the Versatile Home Network (VHN), as defined in EIA/CEA-851, “VHN Home Network Specification.” It assumes an implementation of a VHN that conforms to EIA/CEA-851 in the following sense: The network must be digital, and it must be IP-based; furthermore, it uses web tools, such as HTTP, for device control. (Note that, while the EIA/CEA-851 also defines a network architecture and requires a backbone topology based on IEEE 1394b, the security services specified in this standard are not based on any protocols below layer 3 of the ISO Standard Reference Model; thus, these requirements could be used for networks other than a VHN, so long as they are digital, IP-based, and use web tools for device control.)

This document specifies security services to defend against threats coming from the outside the home into to the home. Security issues stemming from threats originating on devices within the home, or directed from devices within the home to an outside network, will be addressed in a future issue of this standard.

¹ Indeed, one of the persistent problems for managers of enterprise security systems is the tendency of employees to use simplistic passwords; favorites are the user’s own name, the user’s street name, or a common dictionary word.