

I n t e r n a t i o n a l T e l e c o m m u n i c a t i o n U n i o n

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.235.5

(09/2005)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS
Infrastructure of audiovisual services – Systems aspects

H.323 security: Framework for secure authentication in RAS using weak shared secrets

ITU-T Recommendation H.235.5



International
Telecommunication
Union

Documents
Document Sharing Hub

ITU-T H-SERIES RECOMMENDATIONS
AUDIOVISUAL AND MULTIMEDIA SYSTEMS

CHARACTERISTICS OF VISUAL TELEPHONE SYSTEMS	H.100–H.199
INFRASTRUCTURE OF AUDIOVISUAL SERVICES	
General	H.200–H.219
Transmission multiplexing and synchronization	H.220–H.229
Systems aspects	H.230–H.239
Communication procedures	H.240–H.259
Coding of moving video	H.260–H.279
Related systems aspects	H.280–H.299
Systems and terminal equipment for audiovisual services	H.300–H.349
Directory services architecture for audiovisual and multimedia services	H.350–H.359
Quality of service architecture for audiovisual and multimedia services	H.360–H.369
Supplementary services for multimedia	H.450–H.499
MOBILITY AND COLLABORATION PROCEDURES	
Overview of Mobility and Collaboration, definitions, protocols and procedures	H.500–H.509
Mobility for H-Series multimedia systems and services	H.510–H.519
Mobile multimedia collaboration applications and services	H.520–H.529
Security for mobile multimedia systems and services	H.530–H.539
Security for mobile multimedia collaboration applications and services	H.540–H.549
Mobility interworking procedures	H.550–H.559
Mobile multimedia collaboration inter-working procedures	H.560–H.569
BROADBAND AND TRIPLE-PLAY MULTIMEDIA SERVICES	
Broadband multimedia services over VDSL	H.610–H.619

For further details, please refer to the list of ITU-T Recommendations.

ITU-T Recommendation H.235.5

H.323 security: Framework for secure authentication in RAS using weak shared secrets

Summary

This Recommendation provides the framework for mutual party authentication during H.225.0 RAS exchanges. The "proof-of-possession" methods described permit secure use of shared secrets such as passwords which, if used by themselves, would not provide sufficient security.

Extensions to the framework to permit simultaneous negotiation of Transport Layer Security parameters for protection of a subsequent call signalling channel are also described.

In earlier versions of the H.235 sub-series, this profile was contained in H.235 Annex H. Appendices IV, V, VI to H.235.0 show the complete clause, figure, and table mapping between H.235 versions 3 and 4.

Source

ITU-T Recommendation H.235.5 was approved on 13 September 2005 by ITU-T Study Group 16 (2005-2008) under the ITU-T Recommendation A.8 procedure.

Keywords

Authentication, passwords, security.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

© ITU 2006

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

CONTENTS

Page

1	Scope	1
2	References.....	1
2.1	Normative references.....	1
2.2	Informative references.....	1
3	Definitions	2
4	Abbreviations.....	2
5	Conventions	3
6	Basic framework.....	3
6.1	Improved negotiation capabilities in H.235.0	3
6.2	Use between endpoint and gatekeeper	3
6.3	Use of profile between gatekeepers.....	6
6.4	Signalling channel encryption and authentication.....	6
7	A specific security profile (SP1).....	6
8	An improved security profile (SP2).....	8
8.1	Call Signalling sequence number	9
8.2	Generation of Weak Encryption Key from password	9
8.3	Nonce size	9
8.4	Initialization vector salting.....	9
8.5	ClearToken encoding.....	10
9	Extensions to the framework (Informative).....	10
9.1	Using the master key to secure the call signalling channel via TLS	10
9.2	Use of certificates to authenticate the gatekeeper	12
9.3	Use of alternative signalling security mechanisms	12
10	Threats (Informative).....	12
10.1	Passive attack.....	12
10.2	Denial-of-Service attacks	12
10.3	Man-in-the-Middle attacks	13
10.4	Guessing attacks	13
10.5	Unencrypted gatekeeper half-key.....	13

Introduction

In many applications, an endpoint (or its user) and its gatekeeper may share only a "small" secret such as a password or a "personal identification number" (PIN). Such a secret (which we shall hereafter refer to as a "password"), and any encryption key derived from it, is cryptographically weak. The challenge/response authentication schemes, as described in clause 10, provide samples of plaintext and corresponding ciphertext and are, therefore, subject to a brute-force attack by an observer of the transaction when the authentications are keyed by simple passwords. Thus, the observer may recover the password or PIN and later pose as the endpoint to obtain service.

A family of protocols under the generic heading of Encrypted Key Exchange use a shared secret to "obscure" a Diffie-Hellman key exchange in such a way that the attacker must solve a series of finite logarithm problems in order to validate a brute-force attack against the shared secret. In the Encrypted Key Exchange (EKE) of Bellovin and Merritt [B&M], the shared secret is used to encrypt the Diffie-Hellman public keys under a symmetric algorithm. In the Simple Password Exponential Key Exchange (SPEKE) method of Jablon [Jab], the shared secret is used to choose a different generator of the Diffie-Hellman group. These protocols combine the security of a strong Diffie-Hellman key exchange with use of the shared secret in such a way that an attacker cannot obtain known plaintext for use in a brute-force attack against the secret without solving the Diffie-Hellman finite logarithm problem. An advantage of such protocols is that they multiply the strengths of the Diffie-Hellman problem by the strength of the secret-key encryption (or vice versa). A potential disadvantage is that they are typically subject to patent protection.

ITU-T Recommendation H.235.5

H.323 security: Framework for secure authentication in RAS using weak shared secrets

1 Scope

This Recommendation is usable by any gatekeeper or endpoint using the H.225.0 RAS protocols.

2 References

2.1 Normative references

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation

- ITU-T Recommendation H.225.0 (2003), *Call signalling protocols and media stream packetization for packet-based multimedia communication systems*.
- ITU-T Recommendation H.235.0 (2005), *H.323 security: Framework for security in H-series (H.323 and other H.245-based) multimedia systems*.
- ITU-T Recommendation H.235.1 (2005), *H.323 security: Baseline security profile*.
- ITU-T Recommendation H.245 (2005), *Control protocol for multimedia communication*.
- ITU-T Recommendation H.323 (2003), *Packet-based multimedia communications systems*.
- Federal Information Processing Standard FIPS PUB 180-2, *Secure Hash Standard*, U.S. Department of Commerce, Technology Administration, National Institute of Standards and Technology, 1 August 2002.
- NIST Special Publication 800-38A 2001, *Recommendation for Block Cipher Modes of Operation – Methods and Techniques*. <http://www.csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf>.

2.2 Informative references

- [AES] IETF RFC 3268 (2002), *Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security*.
- [B&M] BELLOVIN (S.), MERRITT (M.): U.S. Patent 5,241,599, August 31, 1993, originally assigned to AT&T Bell Laboratories, now assigned to Lucent Technologies.
- [Jab] JABLON (D.): Strong Password-Only Authenticated Key Exchange, *Computer Communication Review*, ACM SIGCOMM, Vol. 26, No. 5, pp. 5-26, October 1996.
- [NIST SP 800-57] NIST Draft Special Publication 800-57 (2005), *Recommendation for Key Management, Part 1: General Guideline*.
<http://www.csrc.nist.gov/publications/drafts/draft-800-57-Part1-April2005.pdf>
- [RFC2104] IETF RFC 2104 (1997), *HMAC: Keyed-Hashing for Message Authentication*.