

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1450

(10/2018)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Available – Security protocols (2)

Guidelines on hybrid authentication and key management mechanisms in the client-server model

Recommendation ITU-T X.1450

ITU-T X-SERIES RECOMMENDATIONS
DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES (1)	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols (1)	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1360–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1389
Distributed ledger technology security	X.1400–X.1429
Distributed ledger technology security	X.1430–X.1449
Security protocols (2)	X.1450–X.1459
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699

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

Recommendation ITU-T X.1450

Guidelines on hybrid authentication and key management mechanisms in the client-server model

Summary

Client and server are often asymmetric regarding security credential management. Since in most cases there are many clients and a few servers, server credentials are distributed and managed with relatively low cost, but client credentials are apparently not. As most mobile services increasingly communicate security and privacy sensitive data, industry need to provide secure channel in client-server model using secure yet cost-effective methods addressing such asymmetric security requirements.

Passwords could be effective in terms of client credential management, and guidelines such as [ITU-T X.1151] are available for password-authenticated key exchange protocols. When client credentials are compromised, however, the adversary could impersonate not only clients but also service providers. Such server impersonation attacks could be mitigated by using public key techniques for server authentication with low credential management cost.

Recommendation ITU-T X.1450 provides guidelines for hybrid authentication and key exchange mechanisms in the client-server model. The underlying mechanism suggests the use of shared secrets and public key techniques for authentication and key exchange. This Recommendation covers service scenarios, and security threats and methods to mitigate such attacks.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1450	2018-10-14	17	11.1002/1000/13729

Keywords

Identity-based schemes, key exchange, password-based authentication, PKI.

* To access the Recommendation, type the URL <http://handle.itu.int/> in the address field of your web browser, followed by the Recommendation's unique ID. For example, <http://handle.itu.int/11.1002/1000/11830-en>.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). 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, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2019

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

Table of Contents

	Page
1 Scope.....	1
2 References.....	1
3 Terms and definitions	1
3.1 Terms defined elsewhere	1
3.2 Terms defined in this Recommendation.....	2
4 Abbreviations and acronyms	2
5 Conventions	3
6 Overview.....	3
7 Security threats	3
7.1 Server impersonation.....	4
7.2 Other types of attacks	4
8 General model.....	5
8.1 Entities.....	5
8.2 Operational procedure of HAKE.....	6
8.3 Requirements for HAKE	7
9 Protocols	8
9.1 Two types of HAKE.....	8
9.2 HAKE protocols using shared secrets and identity-based cryptosystem	8
9.3 HAKE protocols using shared secrets and public key infrastructure (PKI)...	12
10 Extensions of HAKE	14
Appendix I – Comparison of HAKE protocols.....	15
Bibliography.....	16

Recommendation ITU-T X.1450

Guidelines on hybrid authentication and key management mechanisms in the client-server model

1 Scope

This Recommendation describes hybrid authentication and key management mechanisms in the client-server model. It analyses the typical service scenarios, security threats and attack methods, and provides technical methods to mitigate these risks.

2 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 X.509] Recommendation ITU-T X.509 (2016) | ISO/IEC 9594-8:2017, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.
- [ITU-T X.1151] Recommendation ITU-T X.1151 (2007), *Guideline on secure password-based authentication protocol with key exchange*.
- [ITU-T X.1158] Recommendation ITU-T X.1158 (2014), *Multi-factor authentication mechanisms using a mobile device*.

3 Terms and definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

- 3.1.1 authentication** [b-ITU-T Q.1743]: A property by which the correct identity of an entity or party is established with a required assurance. The party being authenticated could be a user, subscriber, home environment or serving network.
- 3.1.2 authentication factor** [b-ITU-T X.1154]: A type of credential; there are three types of authentication factors: ownership factor, knowledge factor and biometric factor.
- 3.1.3 authentication protocol** [b-ITU-T X.1254]: A defined sequence of messages between an entity and a verifier that enables the verifier to perform authentication of an entity.
- 3.1.4 certification authority (CA)** [ITU-T X.509]: An authority trusted by one or more entities to create and digital sign public-key certificates. Optionally the certification authority may create the subjects' keys.
- 3.1.5 credential** [b-ITU-T X.1252]: A set of data presented as evidence of a claimed identity and/or entitlements.
- 3.1.6 digital signature** [b-ITU-T X.843]: A cryptographic transformation of a data unit that allows a recipient of the data unit to prove the origin and integrity of the data unit and protect the sender and

the recipient of the data unit against forgery by third parties, and the sender against manipulated forgery by the recipient.

3.1.7 hybrid authentication [b-ISO/IEC 25185-1]and [b-CCHK15]: A type of authentication using symmetric (or weak secret) and asymmetric authentication systems.

3.1.8 mobile device [ITU-T X.1158]: A small, hand-held computing device with a subscriber identity module (SIM) card, typically having a display screen with touch input and/or a miniature keyboard and is not heavy.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 hybrid authentication and key exchange (HAKE): A type of authenticated key agreement where a client and a server make use of hybrid authentication to negotiate and authenticate one or more shared secret keys.

3.2.2 identity-based cryptography: A type of public-key cryptography in which a publicly known string representing an individual or organization is used as a public key. The public string could be an email address, domain name, or an IP address (Definition based on [b-S84]).

3.2.3 identity-based signature scheme: A type of digital signature scheme in which a publicly known string representing an individual or organization is used as a public verification key to verify a signature (Definition based on [b-S84]).

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CA	Certification Authority
DNS	Domain Name System
HAKE	Hybrid Authentication and Key Exchange
IBC	Identity-based Cryptosystem
IBE	Identity-based Encryption
IBS	Identity-based Signature
KE	Key Exchange
KGA	Key Generation Authority
MFA	Multi-Factor Authentication
MITM	Man-in-the-middle
OTP	One-Time Password
PA	Password-based Authentication
PAKE	Password-based Authentication and Key Exchange or Password-Authenticated Key Exchange
PKC	Public Key Cryptography
PKI	Public Key Infrastructure
RP	Relying Party