



INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1146

(10/2017)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Secure applications and services (1) – Web security

Secure protection guidelines for value-added services provided by telecommunication operators

CAUTION !

PREPUBLISHED RECOMMENDATION

This prepublication is an unedited version of a recently approved Recommendation. It will be replaced by the published version after editing. Therefore, there will be differences between this prepublication and the published version.

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/had not] 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 2017

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

Recommendation ITU-T X.1146

Secure protection guidelines for value-added services provided by telecommunication operators

Summary

With the rapid development of network and user-terminal capability, more and more telecom operators provide various services based on their network resources to the users. These services are called value-added services, which add additional value to basic telecommunication services (e.g., voice call, SMS, MMS and data access). Typical value-added services are including Mobile Office Automation, e-Reading, e-Commerce, etc. In many cases, the value-added services will involve sensitive operations or critical data, which will be the target of the malicious attackers. Malicious users may utilize the service vulnerabilities to get benefits or do harm to the service and other users.

This Recommendation provides secure protection guidelines for value-added services provided by telecommunication operators. In addition to analysing typical service scenarios, security threats and attack methods, this Recommendation provides technical measures to counter threats and attacks. This will help the operators to assure the security of the value-added service, and will also protect the users' benefits.

CONTENTS

1	Scope.....	4
2	References.....	4
3	Definitions	4
3.1	Terms defined elsewhere	4
3.2	Terms defined in this Recommendation.....	4
4	Abbreviations and acronyms	4
5	Conventions	5
6	Introduction.....	5
7.	Typical scenarios for value-added services	6
7.1	User identity authentication.....	6
7.2	Subscription service.....	7
7.3	Payment for service	7
7.3.1	Pre payments	7
7.3.2	Post- payments	7
7.4	User information demonstration.....	8
7.5	Application interface to the external platform.....	8
7.6	Password retrieval	8
8	Threats to value-added services.....	9
8.1	Threats to user identity authentication	9
8.1.1	Fake identity.....	9
8.1.2	False authentication.....	10
8.1.3	Authentication result tampering.....	10
8.1.4	Session attack	10
8.2	Threats to service subscription	11
8.2.1	Subscription information tampering.....	11
8.2.2	Subscription repudiation	11
8.3	Threats to service payment.....	11
8.3.1	Payment amount tampering.....	11
8.3.2	Payment bypass	11
8.4	Current examples of threats to user information	12
8.4.1	Revelation on a terminal	12
8.4.2	Transmission interception	12
8.4.3	Information acquisition without authorization.....	12
8.5	Threats to an application interface with an external platform.....	12

8.5.1	Illegal input	12
8.5.2	Replay attacks	12
8.6	Threats to password retrieval.....	13
8.6.1	Evidence cracking	13
8.6.2	Evidence forgery	13
8.6.3	Authentication on the user-side	13
9	Protection measures	13
9.1	Basic protection measures	13
9.1.1	Confirm measures	13
9.1.2	Tamper-proof measures.....	14
9.1.3	Information check measures.....	14
9.1.4	System analysis measures	14
9.1.5	Session security measures	15
9.1.6	User information protection measures	15
9.1.7	User-side application restriction measures.....	15
9.1.8	Interaction protection measures	15
9.2	Protection measures for typical scenarios	16
9.2.1	User identity authentication	16
9.2.2	Subscription to service	16
9.2.3	Payment of service	16
9.2.4	User information demonstration.....	16
9.2.5	Application interface to an external platform	17
9.2.6	Password retrieval	17

Recommendation ITU-T X.1146

Secure protection guidelines for value-added services provided by telecommunication operators

1 Scope

This Recommendation provides secure protection guidelines for value-added services provided by telecommunication operators. In addition to analysing typical service scenarios, security threats and attack methods, this Recommendation provides technical measures to counter threats and attacks.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

None.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 value-added service: ITU-R M.1224-1 defines value-added service. A service that is offered in addition to or in conjunction with basic telecommunication services (e.g., voice call, short message service (SMS), multimedia messaging service (MMS) and data access). These Value-added services allow operators to drive up their average revenue per user (ARPU). The scope of value-added services in this document is limited to those provided by telecommunication operators and the servers hosting such services reside in operators' networks. Typical value-added services include mobile office automation, e-reading and e-commerce.

4 Abbreviations and acronyms

2G	second Generation
3G	third Generation
4G	fourth Generation
API	Application Programming Interface
ARPU	Average Revenue Per User
ID	Identification
IP	Internet Protocol
LAN	Local Area Network
MMS	Multimedia Messaging Service
SMS	Short Message Service
SQL	Structured Query Language
URL	Uniform Resource Locator