International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

M.3016.1

Corrigendum 1

(11/2005)

SERIES M: TELECOMMUNICATION MANAGEMENT, INCLUDING TMN AND NETWORK MAINTENANCE

Telecommunications management network

Security for the management plane: Security requirements

Corrigendum 1

ITU-T Recommendation M.3016.1 (2005) – Corrigendum 1

ITU-T M-SERIES RECOMMENDATIONS

TELECOMMUNICATION MANAGEMENT, INCLUDING TMN AND NETWORK MAINTENANCE

Introduction and general principles of maintenance and maintenance organization	M.10–M.299
International transmission systems	M.300–M.559
International telephone circuits	M.560–M.759
Common channel signalling systems	M.760–M.799
International telegraph systems and phototelegraph transmission	M.800–M.899
International leased group and supergroup links	M.900–M.999
International leased circuits	M.1000–M.1099
Mobile telecommunication systems and services	M.1100–M.1199
International public telephone network	M.1200–M.1299
International data transmission systems	M.1300–M.1399
Designations and information exchange	M.1400–M.1999
International transport network	M.2000–M.2999
Telecommunications management network	**M.3000–M.3599**
Integrated services digital networks	M.3600–M.3999
Common channel signalling systems	M.4000–M.4999

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

ITU-T Recommendation M.3016.1

Security for the management plane: Security requirements

Corrigendum 1

Summary

This corrigendum corrects a number of defects to ITU-T Rec. M.3016.1 that have been identified and resolved.

Source

Corrigendum 1 to ITU-T Recommendation M.3016.1 (2005) was approved on 13 November 2005 by ITU-T Study Group 4 (2005-2008) under the ITU-T Recommendation A.8 procedure.

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 not 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.

CONTENTS

ITU-T Recommendation M.3016.1

Security for the management plane: Security requirements

Corrigendum 1

1) Resolved defects

1.1) Clause I.2.2: SNMP security

In the 1st sentence, replace the phrase:

... offers the ability to:

with this phrase:

... offers (among other things) the ability to:

In the second paragraph, replace the 5th sentence:

Therefore, SNMP Versions 1 and 2 should be used only as a last resort.

with the following:

Moreover, in December 2002, the IETF declared SNMPv1 and SNMPv2c HISTORIC and replaced them with SNMP Version 3, which is a (full) Internet Standard (STD 62). Therefore, SNMP Versions 1 and 2 should not be used.

In the 2nd paragraph, delete the last sentence and its following 2 dash items (because the revised ITU-T Rec. Q.812 was published in 2004):

ITU-T Study Group 4 is considering the establishment of two new protocol stacks:

– SNMPv3 or V2C with TLS over transmission control protocol (no access control); and

– SNMPv3 with user security model over user datagram protocol (as a forward looking stack)

In the 3rd paragraph, replace the 1st sentence:

Where SNMP is deployed, Version 3 is the preferred level. SNMP Version 3 is more secure and should be used in all new systems because it provides protection against modification of data, masquerade, re-ordering of messages, and loss of confidentiality.

with:

SNMP Version 3 is more secure and must be used in all new systems because it provides protection against modification of data, masquerade, re-ordering of messages, and loss of confidentiality.

Delete the 3rd dash item below the 3rd paragraph (because for SNMPv3, there is NO community string, so this item does not make sense in a list of measures for SNMPv3):

– The default community string should not be used.

Replace 5th dash item below the 3rd paragraph (because DES is obsolete and easily broken now. DES only has a 56-bit key which is now considered weak):

– SNMPv3 uses the data encryption standard as default; however, more secure algorithms can be used.

with:

– SNMPv3 uses the data encryption standard (DES) as default; however, more secure algorithms SHOULD be used (for example AES as specified in RFC 3826).

Replace the 6th dash item below the 3rd paragraph:

– SNMPv3 should be used at least with AuthNoPriv, which provides authentication but no confidentiality of transactions. Preferably, AuthPriv will be used.

with:

– SNMPv3 allows for 3 levels of security, namely: noAuthNoPriv, authNoPriv and authPriv. Depending on which MIB objects are being accessed, one should use the appropriate securityLevel. The Security Considerations Section of the MIB documents should be carefully evaluated and then proper configurations for access control should be made in VACM.

Replace the 8th dash item below the 3rd paragraph:

– Any service or capability not explicitly required should be disabled, including SNMP if it is enabled.

with:

– Any service or capability not explicitly required should be disabled. In other words, if SNMP service is not required/needed, then it should be disabled.

1.2) Bibliography

Replace the following references:

– IETF RFC 1157 (1990), *A Simple Network Management Protocol (SNMP),* (available at http://www.ietf.org/rfc/rfc1157.txt?number=1157).

– IETF RFC 2271 (1998), *An Architecture for Describing Simple Network Management Frameworks,* (available at http://www.ietf.org/rfc/rfc2271.txt?number=2271).

– IETF RFC 2272 (1998), *Message Processing and Dispatching for the Simple Network Management Protocol*, (available at http://www.ietf.org/rfc/rfc2272.txt?number=2272)

– IETF RFC 2273 (1998), *SNMPv3 Applications*, (available at http://www.ietf.org/rfc/rfc2273.txt?number=2273).

– IETF RFC 2275 (1998), *View-based Access Control Model for the Simple Network Management Protocol*, (available at http://www.ietf.org/rfc/rfc2275.txt?number=2275).

– IETF RFC 1905 (1996), *Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)*, (available at http://www.ietf.org/rfc/rfc1905.txt?number=1905).

with the following references:

– IETF RFC 1157 (1990), *Simple Network Management Protocol (SNMP)*, (Also STD0015) (Status: HISTORIC) (available at http://www.ietf.org/rfc/rfc1157).

– IETF RFC 3410 (2002), *Introduction and Applicability Statements for Internet Standard Management Framework*, (Status: INFORMATIONAL) (available at http://www.ietf.org/rfc/rfc3410.txt).

– IETF RFC 3411 (2002), *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks*, STD 62 (available at http://www.ietf.org/rfc/rfc3411.txt).

– IETF RFC 3412 (2002), *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)*, STD 62 (available at http://www.ietf.org/rfc/rfc3412.txt).

– IETF RFC 3413 (2002), *Simple Network Management Protocol (SNMP) Applications*, STD 62 (available at http://www.ietf.org/rfc/rfc3413.txt).

- IETF RFC 3414 (2002), *User-Based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*, STD 62 (available at http://www.ietf.org/rfc/rfc3414.txt).
- IETF RFC 3415 (2002), *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*, STD 62 (available at http://www.ietf.org/rfc/rfc3415.txt).
- IETF RFC 3416 (2002), *Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)*, STD 62 (available at http://www.ietf.org/rfc/rfc3416.txt).

Add the following new references to the bibliography:

- IETF RFC 1901 (1996), *Introduction to Community-based SNMPv2*, (Status: HISTORIC) (available at http://www.ietf.org/rfc/rfc1901.txt).
- IETF RFC 3826 (2004), *The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model*, (Status: PROPOSED STANDARD) (available at http://www.ietf.org/rfc/rfc3826.txt).

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	**Telecommunication management, including TMN and network maintenance**
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2006