国 际 电 信 联 盟

ITU-T M.3016.1

国际电信联盟
电信标准化部门

勘误 1
(11/2005)

M系列：电信管理，包括TMN和网络维护

电信管理网

管理平面的安全：安全需求

勘误 1

ITU-T M.3016.1建议书 (2005)–
勘误 1

国际电信联盟

ITU-T M系列建议书

电信管理，包括 TMN 和网络维护

引言与维护和维护组织的一般原则	M.10-M.299
国际传输系统	M.300-M.559
国际电话电路	M.560-M.759
公共信道信令系统	M.760-M.799
国际电报系统和相片传真传输	M.800-M.899
国际租用一次群和超群链路	M.900-M.999
国际租用电路	M.1000-M.1099
移动电信系统和业务	M.1100-M.1199
国际公众电话网	M.1200-M.1299
国际数据传输系统	M.1300-M.1399
标志和信息交换	M.1400-M.1999
国际传送网	M.2000-M.2999
电信管理网	**M.3000-M.3599**
综合业务数字网	M.3600-M.3999
公共信道信令系统	M.4000-M.4999

欲了解更详细信息，请查阅*ITU-T*建议书目录。

ITU-T M.3016.1建议书

管理平面的安全：安全需求

勘误 1

摘 要

本勘误纠正了在ITU-T M.3016.1建议书中识别出并解决了的一些问题。

来 源

ITU-T第4研究组（2005-2008）按照ITU-T A.8建议书规定的程序，于2005年9月13日批准了ITU-T M.3016.1建议书 (2005) 勘误1 。

前　言

国际电信联盟（ITU）是从事电信领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）是国际电信联盟的常设机构, 负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定 ITU-T 各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA 第 1 号决议规定了批准建议书须遵循的程序。

属 ITU-T 研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工委员会（IEC）合作制定的。

注

本建议书为简要而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其他一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其他机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能不是最新信息，因此大力提倡他们查询电信标准化局（TSB）的专利数据库。

目 录

ITU-T M.3016.1建议书

管理平面的安全：安全需求

勘误 1

1) 已解决的问题

1.1) I.2.2节: SNMP安全

在第1句中，替换下列短语:

... 提供能力到：

替换为:

... 提供（在其他事情中）能力到：

在第2段中，替换第5句:

因此，SNMP版本1和版本2应当仅仅被用作最后的选择。

替换为:

而且，在2002年，IETF宣布SNMP版本1和SNMP版本2c成为历史，用SNMP版本3取代他们，这是一个（完全的）互联网标准(STD 62)。因此，不应该再使用SNMP版本1和版本2。

在第2段中，删除最后一句以及接下来的两项（因为ITU-T Q.812建议书的修订版于2004年出版）:

ITU-T第4研究组认为应当建立下面两个新的协议栈：

— SNMP 版本 3 或具有基于传输控制协议之上的 TLS 的 V2C（无访问控制）；和

— SNMP 版本 3，且具备基于用户数据报协议（作为前转栈）之上的用户安全模式。

在第3段中，替换第1句:

在部署SNMP时，版本3是首选的级别。SNMP版本3具有更多的安全机制，应当被应用到所有的新系统中，版本3提供保护以阻止修改数据、模仿、消息重排，机密性损失等。

替换为:

SNMP版本3具有更多的安全机制，必须被应用到所有的新系统中，版本3提供保护以阻止修改数据、模仿、消息重排，机密性损失等。

删除第3段下面的第3项（因为对于SNMP版本3，没有公共字符串，因此把这项列在SNMP版本3中的对策中没有意义）:

— 不能使用缺省的公共字符串。

替换第3段下面的第5项（因为DES过时了，现在很容易被打破。DES仅有56比特密钥，现在被认为是很弱的）:

— SNMP 版本 3 缺省使用数据密码标准；然而，也可使用更安全的算法。

替换为:

– SNMP版本3缺省使用数据密码标准（DES）；然而，应当使用更安全的算法（例如RFC 3826中规定的AES）。

替换第*3*段下面的第*6*项:

— 使用SNMP版本3时，至少应当具备AuthNoPriv，即提供鉴权但没有传输的机密性保护。一般来说，使用AuthPriv更合适。

替换为:

– SNMP版本3允许采用3级安全，即：noAuthNoPriv、authNoPriv和authPriv。 根据正在接入的MIB目标不同，应该使用合适的安全级。应该认真评估MIB文件中的安全考虑部分，然后在VACM中对接入控制进行合适的配置。

替换第*3*段下面的第*8*项:

— 任何没有明确要求的业务或能力都应停用，包括已经启用的 SNMP。

替换为:

– 任何没有明确要求的业务或能力都应停用。换句话说，如果没有要求/需要SNMP业务，则应该停用SNMP。

1.2) 参考资料

替换下列参考文献:

– 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).

替换为:

– 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).

在参考资料中增加下列新的参考文献:

– 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).

ITU-T 系列建议书

A系列	ITU-T工作的组织
D系列	一般资费原则
E系列	综合网络运行、电话业务、业务运行和人为因素
F系列	非话电信业务
G系列	传输系统和媒质、数字系统和网络
H系列	视听和多媒体系统
I系列	综合业务数字网
J系列	有线网和电视、声音节目及其他多媒体信号的传输
K系列	干扰的防护
L系列	线缆的构成、安装和保护及外部设备的其他组件
M系列	**电信管理，包括TMN和网络维护**
N系列	维护：国际声音节目和电视传输电路
O系列	测量设备技术规程
P系列	电话传输质量、电话装置、本地线路网络
Q系列	交换和信令
R系列	电报传输
S系列	电报业务终端设备
T系列	远程信息处理业务的终端设备
U系列	电报交换
V系列	电话网上的数据通信
X系列	数据网和开放系统通信及安全
Y系列	全球信息基础设施、互联网的协议问题和下一代网络
Z系列	用于电信系统的语言和一般软件问题

瑞士印刷
2006年，日内瓦