|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| The International Teleocmmunication Union - Connecting the World. | | **国 际 电 信 联 盟**  **电信标准化局** | |  |
|  | | | 2025年7月23日，日内瓦 | |
| **文号：** | **电信标准化局第50号通函**  SG17/XY | | **致：**  - 国际电联各成员国主管部门；  **抄送：**  - ITU-T部门成员；  - ITU-T第17研究组部门准成员；  - 国际电联学术成员；  - ITU-T第17研究组正副主席；  - 电信发展局主任；  - 无线电通信局主任 | |
| 电话： | +41 22 730 6206 | |
| 传真： | +41 22 730 5853 | |
| 电子邮件： | [tsbsg17@itu.int](mailto:tsbsg17@itu.int) | |
|  |  | |
| **事由：** | **就拟提交2025年12月3-11日在日内瓦召开的ITU-T第17研究组会议批准的、已确定的ITU-T X.1062（原X.shcd）、X.1238（原X.sgc-rcs）、X.1128（原X.mt-feature）、X.1129（原X.mt-integrity）、X.1130（原X.tg-fdma）、X.1457（原X.str-irs）、X.1753（原X.gdsml）、X.1649（原X.sgmc）新建议书草案和经修订的ITU-T X.1250和X.1631建议书与成员国进行磋商** | | | |

尊敬的先生/女士：

1 ITU-T第17研究组（安全）拟采用WTSA第1号决议（2022年，日内瓦，修订版）第9节所述传统批准程序，在2025年12月3-11日于日内瓦召开的下一次实体会议上批准上述建议书草案。有关ITU-T第17研究组会议的议程和所有相关信息将在第[4/17](https://www.itu.int/md/T25-SG17-COL-0004/en)号集体函中提供。

2 拟议批准的ITU-T建议书草案的标题、摘要及出处见**附件1**。

电信标准化局说明1 – 尚未针对这些已确定的案文提交任何ITU-T A.5理由说明。

电信标准化局说明2 – 截至本通函发布之日，电信标准化局尚未收到任何有关这些已确定案文的知识产权（IPR）声明。欲了解最新情况，请各成员通过以下链接查阅知识产权数据库：[www.itu.int/ipr/](http://www.itu.int/ipr/)。

3 本通函根据第1号决议第9.4条，就是否可在即将召开的会议上审议并批准这些案文启动与国际电联成员国的正式磋商。请成员国于**2025年11月21日**协调世界时23时59分前填妥并返回**附件2**中的表格。

4 如果70%或以上的成员国在回复中支持审议并批准，则将专门召开一次全体会议应用批准程序。拒绝授权继续此项工作的成员国应向电信标准化局主任通报持有这一意见的理由，并提出可能的修改建议，以推动该项工作取得进展。

顺致敬意！

Icon

Description automatically generated电信标准化局主任  
尾上诚藏

**附件：** 2件

附件1  
已确定的ITU-T X.1062（原X.shcd）、X.1238（原X.sgc-rcs）、X.1128  
（原X.mt-feature）、X.1129（原X.mt-integrity）、X.1130（原X.tg-fdma）、X.1457（原X.str-irs）、X.1753（原X.gdsml）、X.1649（原X.sgmc）  
新建议书草案和经修订的ITU-T X.1250和X.1631建议书的摘要和出处

# 1 ITU-T X.1062新建议书草案（原X.shcd）[[SG17-R6](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T25-SG17-R-0006)]

安全人员的能力发展框架

## 摘要

网络安全是一个庞大且不断发展的主题，需要不断地学习和拓展技能。本建议书规范了安全人员的能力发展框架，通过拓展安全从业人员和专业人士的能力并认可其在组织内的安全技能和知识，为其发展提供指导原则。

# 2 ITU-T X.1238新建议书草案（原X.sgc-rcs）[[SG17-R7](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T25-SG17-R-0007)]

打击富媒体通信服务（RCS）消息垃圾信息的指导原则

## 摘要

本建议书规定了支持富媒体通信业务（RCS）提供商根据RCS特性防止垃圾信息传播的指南和技术推动因素，并定义了RCS客户机支持的垃圾信息防控机制。

本建议书引用了GSMA [b-GSMA RCC.07]中定义的RCS架构，并侧重于如何缓解RCS消息的垃圾信息风险。

# 3 ITU-T X.1128新建议书草案（原X.mt-feature）[[SG17-R8](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T25-SG17-R-0008)]

评估移动终端安全性的安全特征

## 摘要

移动终端，尤其是智能手机，正在改变人们的工作和生活方式。例如，移动支付正呈现快速增长态势，因为消费者将移动终端作为现代动态生活方式的一部分；越来越多的企业支持员工使用个人移动终端访问企业服务；等等。然而，移动终端安全是移动应用服务面临的重大挑战。例如，用户可能在不知不觉中使终端暴露于恶意软件，从而使敏感数据面临数据泄露的风险。

本建议书提供了用以评估移动终端安全性的安全特征，并提供了关于相关利益攸关方如何使用本建议书中的安全特征的信息。

# 4 ITU-T X.1129新建议书草案（原X.mt-integrity）[[SG17-R9](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T25-SG17-R-0009)]

移动终端完整性保护的安全导则

## 摘要

移动终端完整性保护的目标是确保移动终端以预期的方式运行。这意味着，移动终端上的硬件、固件和软件（例如，操作系统、预安装的应用程序）没有被任何手段或以任何方式损害。如果攻击者损害固件或软件，或者修改硬件（例如，ROM、保留单元）的配置，或者改变硬件（例如，闪存），则攻击者可以控制或破坏移动终端的功能。

当移动终端开机时，它从启动阶段开始，以验证硬件组件和加载一个或多个软件模块。此后，移动终端进入运行阶段，并达到操作状态，在该状态下，移动终端准备好用于其预期目的。为了修复固件/软件（FW/SW）的漏洞和弱点，移动终端需要不时地更新。这称为FW/SW更新阶段。这些阶段中的每一个阶段都可能使攻击者有机可乘，对移动终端完整性构成安全威胁。

本建议书分析了移动终端在启动阶段、运行阶段和固件/软件更新阶段面临的安全威胁，定义了安全要求，并为移动终端完整性保护提供了安全导则。

# 5 ITU-T X.1130新建议书草案（原X.tg-fdma）[[SG17-R10](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T25-SG17-R-0010)]

检测移动应用程序恶意活动的技术导则

## 摘要

随着移动设备和应用程序的广泛使用，APP已经成为恶意活动的主要载体。例如，恶意APP可能伪装成合法的信用或购物应用程序来欺骗用户。为了检测和防止此类恶意活动，传统方法依赖于APP商店的审核和来自移动设备中安装的安全软件的警报。但是，此解决方案面临一些挑战。虽然APP商店的审核可以帮助阻止恶意应用程序，但攻击者不断开发新技术来逃避检测并绕过APP商店的审核。此外，一些恶意应用程序通过第三方平台分发，引诱用户下载和安装。移动安全软件主要关注检测病毒和应用程序漏洞，这使其很难有效识别专门用于实施恶意活动的恶意应用程序。

移动设备上的恶意应用程序通常通过四个阶段运行：下载、安装、执行和诱导支付。每个阶段都有不同的风险。

在下载和安装阶段，恶意应用程序常常伪装成合法应用程序以逃避安全软件的检测。在此阶段，恶意应用程序还可能在移动设备上植入木马。

在执行阶段，这些应用程序可能会通过植入的木马窃取用户信息，或者通过模仿合法应用程序来诱骗用户自愿泄露敏感数据。

在诱导支付阶段，恶意应用程序通常通过各种方案提供小额奖励或收益来建立信任。一旦建立起用户信任，他们就会引诱用户进行转账。在某些情况下，欺骗是直接的，例如，通过伪装成合法的购物应用程序来利用毫无戒心的用户。

检测和防止恶意活动的整个过程非常复杂，需要移动设备和应用程序之间的密切协调。本建议书分析了多个阶段（包括下载、安装、执行和诱导支付）的恶意应用程序的特性和风险，并根据移动设备和应用程序之间的互动为检测和防止恶意活动提供了全面的技术解决方案。

# 6 ITU-T X.1457新建议书草案（原X.str-irs）[[SG17-R11](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T25-SG17-R-0011)]

信息推荐服务的安全威胁和要求

## 摘要

信息推荐服务广泛用于不同的网站和应用程序。例如，教育信息推荐服务是实现教育信息共享的重要因素。在海量的教育信息中，用户可以快速找到自己需要的教育信息资源，满足用户的学习需求，给用户带来良好的学习体验。然而，信息推荐服务中涉及的安全问题不容忽视，例如，数据完整性威胁、数据中毒、逃避攻击等。

本建议书分析了信息推荐业务的安全威胁和要求。它确定了信息推荐服务中涉及的安全威胁，并规定了应对这些安全威胁的安全要求。

# 7 ITU-T X.1753新建议书草案（原X.gdsml）[[SG17-R12](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T25-SG17-R-0012)]

在大数据基础设施中使用机器学习的数据安全导则

## 摘要

在大数据基础设施中，数据收集、存储、处理和管理过程中存在诸多安全威胁。如何动态地、智能地监测、分析和响应数据安全威胁，是大数据基础设施中需要解决的问题。机器学习具有自动学习和模式识别的能力，可以从大量数据中发现潜在的安全威胁和异常行为，从而采取主动防御措施。利用机器学习增强数据安全已逐渐成为大数据基础设施中的一项必要技术。

本建议书分析了大数据基础设施中的数据安全威胁，以及机器学习可用于大数据基础设施中数据安全保护的场景，并提供了使用机器学习来保护大数据基础设施数据安全的导则。

# 8 ITU-T X.1649新建议书草案（原X.sgmc）[[SG17-R14](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T25-SG17-R-0014)]

多云安全导则

## 摘要

本建议书概述了多云，包括其定义及新兴背景。本建议书还分析了安全风险并为多云制定了适当导则，以降低安全风险。

# 9 ITU-T X.1250建议书修订草案[[SG17-R15](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T25-SG17-R-0015)]

增强全球身份管理和互操作性的基准能力

## 摘要

本文件概述了在电信和信息技术网络中开发和部署结构化、可互操作的身份管理系统的关键条款，确保隐私并符合区域性政策。它涵盖的主题包括用于安全高效的身份交换的结构性身份管理模型、保护和提供身份属性，以及发现身份服务提供方。它还涉及身份平台之间的互操作性、缓解威胁的安全措施、合规性审计，以及可用性和可扩展性的重要性。总体目标是创建稳健、透明且适应性强的身份管理系统，在与监管标准保持一致的同时，增强数字交互中的信任、安全和用户体验。

# 10 ITU-T X.1631建议书修订草案[[SG17-R13](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T25-SG17-R-0013)]

基于ISO/IEC 27002的云服务信息安全控制

## 摘要

本建议书 | 国际标准所载导则是对ISO/IEC 27002:2022所述导则之补充。

具体而言，本建议书 | 国际标准为云服务客户（CSC）和云服务提供商（CSP）实施信息安全控制提供了指南。一些指南针对实施控制的CSC，其他指南针对支持实施这些控制的CSP。确定适当的信息安全控制以及所提供导则的利用程度将取决于相关风险评估的结果以及是否存在任何法律、法规、合同或其他云计算特定的信息安全要求。

附件2  
事由：成员国对电信标准化局第50号通函的回应：  
就已确定的ITU-T X.1062（原X.shcd）、X.1238（原X.sgc-rcs）、X.1128  
（原X.mt-feature）、X.1129（原X.mt-integrity）、X.1130（原X.tg-fdma）、X.1457（原X.str-irs）、X.1753（原X.gdsml）、X.1649（原X.sgmc）  
新建议书草案和经修订的ITU-T X.1250和X.1631建议书与成员国进行磋商

|  |  |  |  |
| --- | --- | --- | --- |
| **致：** | 国际电信联盟电信标准化局  主任  Place des Nations  CH 1211 Geneva 20, Switzerland | **自：** | [姓名]  [正式职务/头衔]  [地址] |
| **传真：** | +41-22-730-5853 | **传真：** |  |
| **电子邮件：** | [tsbdir@itu.int](mailto:tsbdir@itu.int) | **电子邮件：** |  |
|  |  | **日期：** | [日期，] [地点] |

尊敬的先生/女士：

关于电信标准化局第50号通函所列已确定案文草案与成员国进行的磋商，在此谨向您通报本主管部门的意见，如下表所示。

|  | **请从两个方框中选择一个** |
| --- | --- |
| **X.1062新建议书草案（原X.shcd）** | **授权**第17研究组审议批准该案文（在这种情况下，请在两种方案中选择一种⃝）：  ⃝ 无意见或无修改建议  ⃝ 后附意见和修改建议 |
| **不授权**第17研究组审议批准该案文（后附不授权的理由并概述可能的修改方案，以推动工作进展） |
| **X.1238新建议书草案（原X.sgc-rcs）** | **授权**第17研究组审议批准该案文（在这种情况下，请在两种方案中选择一种⃝）：  ⃝ 无意见或无修改建议  ⃝ 后附意见和修改建议 |
| **不授权**第17研究组审议批准该案文（后附不授权的理由并概述可能的修改方案，以推动工作进展） |
| **X.1128新建议书草案（原X.mt-feature）** | **授权**第17研究组审议批准该案文（在这种情况下，请在两种方案中选择一种⃝）：  ⃝ 无意见或无修改建议  ⃝ 后附意见和修改建议 |
| **不授权**第17研究组审议批准该案文（后附不授权的理由并概述可能的修改方案，以推动工作进展） |
| **X.1129新建议书草案（原X.mt-integrity）** | **授权**第17研究组审议批准该案文（在这种情况下，请在两种方案中选择一种⃝）：  ⃝ 无意见或无修改建议  ⃝ 后附意见和修改建议 |
| **不授权**第17研究组审议批准该案文（后附不授权的理由并概述可能的修改方案，以推动工作进展） |
| **X.1130新建议书草案（原X.tg-fdma）** | **授权**第17研究组审议批准该案文（在这种情况下，请在两种方案中选择一种⃝）：  ⃝ 无意见或无修改建议  ⃝ 后附意见和修改建议 |
| 不授权第17研究组审议批准该案文（后附不授权的理由并概述可能的修改方案，以推动工作进展） |
| **X.1457新建议书草案（原X.str-irs）** | **授权**第17研究组审议批准该案文（在这种情况下，请在两种方案中选择一种⃝）：  ⃝ 无意见或无修改建议  ⃝ 后附意见和修改建议 |
| **不授权**第17研究组审议批准该案文（后附不授权的理由并概述可能的修改方案，以推动工作进展） |
| **X.1753新建议书草案（原X.gdsml）** | **授权**第17研究组审议批准该案文（在这种情况下，请在两种方案中选择一种⃝）：  ⃝ 无意见或无修改建议  ⃝ 后附意见和修改建议 |
| **不授权**第17研究组审议批准该案文（后附不授权的理由并概述可能的修改方案，以推动工作进展） |
| **X.1649新建议书草案（原X.sgmc）** | **授权**第17研究组审议批准该案文（在这种情况下，请在两种方案中选择一种⃝）：  ⃝ 无意见或无修改建议  ⃝ 后附意见和修改建议 |
| **不授权**第17研究组审议批准该案文（后附不授权的理由并概述可能的修改方案，以推动工作进展） |
| **X.1250建议书 修订草案** | **授权**第17研究组审议批准该案文（在这种情况下，请在两种方案中选择一种⃝）：  ⃝ 无意见或无修改建议  ⃝ 后附意见和修改建议 |
| **不授权**第17研究组审议批准该案文（后附不授权的理由并概述可能的修改方案，以推动工作进展） |
| **X.1631建议书 修订草案** | **授权**第17研究组审议批准该案文（在这种情况下，请在两种方案中选择一种⃝）：  ⃝ 无意见或无修改建议  ⃝ 后附意见和修改建议 |
| **不授权**第17研究组审议批准该案文（后附不授权的理由并概述可能的修改方案，以推动工作进展） |

顺致敬意！

[姓名]

[正式职务/头衔]

[成员国]主管部门

\_\_\_\_\_\_\_\_\_\_\_\_\_\_