国　际　电　信　联　盟

ITU-T X.1580

(09/2012)

国际电信联盟
电信标准化部门

X系列：数据网、开放系统通信和安全性

网络安全信息交换 – 确保交换

实时网际防御

ITU-T X.1580 建议书

国际电信联盟

ITU-T X 系列建议书

数据网、开放系统通信和安全性

公用数据网	X.1–X.199
开放系统互连	X.200–X.299
网间互通	X.300–X.399
报文处理系统	X.400–X.499
号码簿	X.500–X.599
OSI组网和系统概貌	X.600–X.699
OSI管理	X.700–X.799
安全	X.800–X.849
OSI应用	X.850–X.899
开放分布式处理	X.900–X.999
信息和网络安全	
一般安全问题	X.1000–X.1029
网络安全	X.1030–X.1049
安全管理	X.1050–X.1069
生物测定安全	X.1080–X.1099
安全应用和服务	
组播安全	X.1100–X.1109
家庭网络安全	X.1110–X.1119
移动安全	X.1120–X.1139
网页安全	X.1140–X.1149
安全协议	X.1150–X.1159
对等网络安全	X.1160–X.1169
网络身份安全	X.1170–X.1179
IPTV安全	X.1180–X.1199
网络空间安全	
计算网络安全	X.1200–X.1229
反垃圾信息	X.1230–X.1249
身份管理	X.1250–X.1279
安全应用和服务	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1339
网络安全信息交换	
网络安全概述	X.1500–X.1519
脆弱性/状态信息交换	X.1520–X.1539
事件/事故/探索法信息交换	X.1540–X.1549
政策的交换	X.1550–X.1559
探索法和信息请求	X.1560–X.1569
标识和发现	X.1570–X.1579
确保交换	**X.1580–X.1589**

欲了解更详细信息，请查阅 ITU-T建议书目录。

ITU-T X.1580 建议书

实时网际防御

摘要

有关实时网际防御（RID）的此建议书概述了促进自动分享事件处理信息的一种主动网际通信方法。落实可与现有的事件管理系统以及发现、来源确定和缓解机制相结合，以形成更加完善的事件处理解决方案。RID规定了安全交流事件信息，实现交换事件对象描述交换格式（IODEF）可扩展标记语言（XML）文件的一种方法。RID提供了一种传送安全、政策和隐私控制，以实现潜在敏感信息交换的技术方法。技术能力可与适当的政策相对应，使得业务提供商或组织可根据其政策做出适当的决定。

此建议书通过列举RFC 6545的相关条款并说明其为标准或是用于参考的方式规定了RID。

沿革

版本	建议书	批准日期	研究组	
1.0	ITU-T X.1580	2012-09-07	17	

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）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“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”等其它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它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，这可能并非最新信息，因此特大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

目录

引言

有关“网络安全信息交换的概述”的X.1500建议书，提供了交换包括本ITU-T建议书所载事件和指标在内的网络安全信息的导则。机构可以通过交换事件信息，增进对事态的了解并受益于其他组织的协助。事件信息的交流，使机构能够共享事故确定资源，减轻针对其计算资源的恶意活动，并洞察潜在威胁。

事件处理可能涉及事件的检测、报告和缓解，无论它是无害的配置问题、一个IT事件、对业务等级协议（SLA）的违背，还是社会上策划的系统破坏或拒绝服务（DoS）攻击等。发现事件后的响应可能包括提交报告、将报告送交事件来源、请求业务提供商提供可能解决/缓解问题的援助或要求查找其根源。

实时网际防御（RID）概要介绍了有助于共享事件处理信息的主动网间通信方法。可将RID与现有的事件管理、检测、根源识别和缓解机制相结合，以获得完整的事件处理方案。RID提供的技术手段可提供安全、策略和隐私管理，以实现潜在敏感信息的交换。RID有助于事件对象描述交换格式（IODEF）扩展标记语言（XML）文件的安全和自动交换。这一做法通过将策略和协议映射至提供的技术管理，使业务提供商或机构具有根据其策略做出适当决定的选择。RID包括有关事件信息交换的私密性、保密性、完整性和认证的规定。

RID 信息数据体现为采用 IODEF 和 RID 包络的 XML 文件。遵循这一模式的 IODEF 和 RID 可构成与其它事件处理工具相结合的应用程序接口。提供的数据标记和 XML 枚举值指出了建议采取哪些行动才能停止或缓解事件或攻击造成的影响。RID 旨在提供一种通报相关信息的方法。鉴于 RID 和相关的传输协议仅提供了一种工具间自动通信的接口，它可以通过各种现有和未来可行的检测和响应方式实现互操作性。事件可能包括计算机安全或其它类型的事件。

由于有可能通过RID信息交换潜在敏感的信息，安全和隐私方面的考虑受到极大关注。RID消息利用的现有技术包括XML安全功能，还有通过RID图表提出隐私和策略要求的XML数据标记。RID图表是用于传送IODEF文件的XML包络。IETF RFC 6545对RID提出了定义。RID消息可在封装后得到安全传送。单独的ITU-T X.1581建议书提出了RID传送的定义。RID和RID传送的认证、完整性和授权等综合特性可用于达到必要的安全等级。

无数程序、诚信、策略和法律方面的考虑，可能限制或阻碍信息交流。

ITU-T X.1580 建议书

实时网际防御

1 范围

本建议书概述了实时网际防御（RID）并提供了一种安全交换事件信息的方法。本建议书提供了一套在实体间安全传送IODEF文件所需的事件协调信息。RID基本上是用于IODEF可扩展标记语言（XML）文件的包络，其中包括所有IODEF的扩展。这种标准的信息和交换格式包括全球事件协调计划所需的安全、隐私和策略选择/考虑。RID是通过IODEF-RID XML图表选项和RID通信流安全要求提供的IODEF文件和传送协议之间的安全层。

实现事件信息交换的落实工作必须提供遵守所有适用的国家和区域法律、规定和策略的功能。

所有ITU-T建议书，包括ITU-T X.1580建议书及相关技术的实施者和用户，都应遵循所有适用的国家和区域法律、规则和策略。

2 参考文献

下列ITU-T建议书和其他参考文献的条款，在本建议书中的引用而构成本建议书的条款。在出版时，所指出的版本是有效的。所有的建议书和其它参考文献均会得到修订，本建议书的使用者应查证是否有可能使用下列建议书或其它参考文献的最新版本。当前有效的ITU-T建议书清单定期出版。本建议书引用的文件自成一体时不具备建议书的地位。

[IETF RFC 6545] IETF RFC 6545 (2012), 实时网际防御(RID)， https://datatracker.ietf.org/doc/rfc6545/。

3 定义

3.1 他处定义的术语

无。

3.2 本建议书定义的术语

无。

4 缩写词和首字母缩略语

CSIRT 计算机安全事件响应组

DoS 拒绝服务

IODEF 事件对象描述交换格式

IT 信息技术

RID 实时网际防御

SLA 服务水平协议

5 惯例

下列术语被视为彼此等同：

- 在国际电联，“shall”和“must”在使用时彼此等同，其反义表达亦视为彼此等同。
- 国际电联使用的“shall”一词与IETF使用的“MUST”一词等同。
- 国际电联使用的“shall not”短语与IETF使用的“MUST NOT”短语等同。

注 – 在IETF，“shall”和“must”（小写）两词用于资料性文本。

6 实时网际防御（RID）

第6款定义了IETF RFC 6545提及的实时网际防御（RID）信息。该款通过款与节编号的统一，例如第6点x款与相同标题的IETF RFC 6545 x节相统一，提供了对IETF RFC6545的直接参引。

6.1 引言

[b-IETF RFC6545]第1节为告知性。

6.1.1 源自RFC 6045的修改

[b-IETF RFC6545]第1.1节为告知性。

6.1.2 规范性和告知性

[b-IETF RFC6545]第1.2节为告知性。

6.1.3 术语

[b-IETF RFC6545]第1.3节为规范性。

6.2 事件特性

[b-IETF RFC6545]第2节为告知性。

6.3 CSIRT和业务提供商之间的通信

[b-IETF RFC6545]第3节为告知性。

6.3.1 网际提供商的RID消息

[b-IETF RFC6545]第3.1节为告知性。

6.3.2 RID通信拓扑

[b-IETF RFC6545]第3.2节为告知性。

6.4 消息格式

[IETF RFC6545]第4节为规范性。

6.4.1 RID数据类型

[IETF RFC6545]第4.1节为规范性。

6.4.1.1 布尔值

[IETF RFC6545]第4.1.1节为规范性。

6.4.2 RID消息类型

[IETF RFC6545]第4.2节为规范性。

6.5 IODEF-RID图表

[IETF RFC6545]第5节为规范性。

6.5.1 RIDPolicy等级

[IETF RFC6545]第5.1节为规范性。

6.5.1.1 ReportSchema

[IETF RFC6545]第5.1.1节为规范性。

6.5.2 RequestStatus

[IETF RFC6545]第5.2节为规范性。

6.5.3 IncidentSource

[IETF RFC6545]第5.3节为规范性。

6.5.4 RID命名空间

[IETF RFC6545]第5.4节为规范性。

6.5.5 编码

[IETF RFC6545]第5.5节为规范性。

6.5.6 包括IODEF或其它XML文件

[IETF RFC6545]第5.6节为规范性。

6.5.6.1 包括RID中的XML文件

[IETF RFC6545]第5.6.1节为规范性。

6.6 RID消息

[b-IETF RFC6545]第6节为规范性。

6.6.1 请求

[IETF RFC6545]第6.1节为规范性。

6.6.2 收悉通知

[IETF RFC6545]第6.2节为规范性。

6.6.3 结果

[IETF RFC6545]第6.3节为规范性。

6.6.4 报告

[IETF RFC6545]第6.4节为规范性。

6.6.5 查询

[IETF RFC6545]第6.5节为规范性。

6.7 RID通信交换

[b-IETF RFC6545]第7节为规范性。

6.7.1 上游跟踪通信流量

[IETF RFC6545]第7.1节为规范性。

6.7.1.1 RID TraceRequest实例

[b-IETF RFC6545]第7.1.1节为规范性。

6.7.1.2 信息收悉通知实例

[b-IETF RFC6545]第7.1.2节为告知性。

6.7.1.3 结果消息实例

[b-IETF RFC6545]第7.1.3节为告知性。

6.7.2 调查请求通信流量

[IETF RFC6545]第7.2节为规范性。

6.7.2.1 调查请求实例

[b-IETF RFC6545]第7.2.1节为告知性。

6.7.2.2 收悉通知消息实例

[b-IETF RFC6545]第7.2.2节为告知性。

6.7.3 报告通信流量

[b-IETF RFC6545]第7.3节为规范性。

6.7.3.1 报告实例

[b-IETF RFC6545]第7.3.1节为告知性。

6.7.4 查询通信流量

[IETF RFC6545]第7.4节为规范性。

6.7.4.1 查询实例

[b-IETF RFC6545]第7.4.1节为告知性。

6.8 RID图表定义

[IETF RFC6545]第8节为规范性。

6.9 安全要求

[b-IETF RFC6545]第9节为规范性。

6.9.1 XML数字签名和加密

[IETF RFC6545]第9.1节为规范性。

6.9.2 消息传送

[IETF RFC6545]第9.2节为规范性。

6.9.3 公共密钥基础设施

[IETF RFC6545]第9.3节为规范性。

6.9.3.1 认证

[IETF RFC6545]第9.3.1节为规范性。

6.9.3.2 多跳请求认证

[IETF RFC6545]第9.3.2节为规范性。

6.9.4 企业集团和公共密钥基础设施

[IETF RFC6545]第9.4节为规范性。

6.9.5 隐私问题和系统使用导则

[IETF RFC6545]第9.5节为规范性。

6.9.6 共用概况和策略

[IETF RFC6545]第9.6节为规范性。

6.10 安全考虑

[b-IETF RFC6545]第10节为规范性。

6.11 国际化

[IETF RFC6545]第11节为规范性。

6.12 IANA考虑

[IETF RFC6545]第12节为规范性。

6.13 总结

[b-IETF RFC6545]第13节为告知性。

6.14 参考资料

6.14.1 规范性参考

[b-IETF RFC6545]第14.1节为告知性。

本ITU-T建议书将RFC6545第14.1节确定为告知性，因为ITU-T对于涉及这一建议书的任何参引都不持立场。然而众所周知，IETF为RFC6545确定了一系列规范性参考。

6.14.2 告知性参考

[b-IETF RFC6545]第14.2节为告知性。

参考资料

[b-ITU-T X.1500] ITU-T X.1500建议书, 网络安全信息交换技术（CYBEX）概述

[b-ITU-T X.1541] ITU-T X.1541建议书，事件对象描述交换格式。

[b-ITU-T X.1581] ITU-T X.1581建议书，实时网际防御讯息的传输。

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	视听及多媒体系统
I系列	综合业务数字网
J系列	有线网络和电视、声音节目及其它多媒体信号的传输
K系列	干扰的防护
L系列	电缆和外部设备其它组件的结构、安装和保护
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	测量设备的技术规范
P系列	电话传输质量、电话设施及本地线路网络
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、开放系统通信和安全性**
Y系列	全球信息基础设施、互联网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
2013年，日内瓦