国 际 电 信 联 盟

ITU-T X.1582

(01/2014)

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

支持网络安全信息交换的传送协议

ITU-T X.1582 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**
云计算安全	
云计算安全概述	X.1600–X.1601
云计算安全设计	X.1602–X.1639
云计算安全最佳做法和导则	X.1640–X.1659
云计算安全的部署	X.1660–X.1679
其他云计算安全	X.1680–X.1699

欲了解更多详细信息，请查阅 ITU-T建议书目录。

ITU-T X.1582 建议书

支持网络安全信息交换的传送协议

摘要

ITU-T X.1582建议书概要介绍了已经通过并经过改编以用于网络安全信息交换（CYBEX）框架内的传送协议。本建议书概述了传送应用、传送协议特性以及安全方面的考虑。

历史

版本	建议书	批准	研究组	唯一ID*
1.0	ITU-T X.1582	2014-01-24	17	11.1002/1000/12037

关键词

网络安全信息、信息交换协议、信息传输

* 欲访问本建议书，请在网页浏览器地址栏输入URL http://handle.itu.int/ ，然后输入建议书的唯一ID。例如： http://handle.itu.int/11.1002/1000/11830-en。

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

目前，在网络安全信息交换中存在和使用若干交换机制和协议，但其中诸多（如果不是多数的话）亦或为专用协议，亦或未以文件形式记录或并非广为人知，因此，难以将其用于全球网络安全信息交换之中。此外，目前多数交换应用限于有线交换伙伴之间，其数量或网络安全操作领域都十分有限。

为了尽可能支持最广泛的一系列应用之间进行更加全面和可互操作的网络安全信息交换，“网络安全信息交换”（CYBEX）概要介绍一系列实现尽可能多的应用空间网络安全信息交换全球化的具体协议规范。

ITU-T X.1582 建议书

支持网络安全信息交换的传送协议

1 范围

本建议书概要介绍了网络安全信息传送和交换的应用领域内已经过标准化处理和/或正在使用的传送和交换协议以及已经通过并在改编后用于ITU-T X.1500系列建议书中的传送和交换协议。

本建议书最合适的受众是应用设计人员和实施人员，他们负责在本地、区域或全球层面促成网络安全信息的传送和交换。

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。

[ITU-T X.1500] ITU-T X.1500建议书（2011年）– 网络安全信息交换（CYBEX）概述

3 定义

3.1 他处定义的术语

本建议书使用了下列他处定义的术语。

3.1.1 网络安全[b-ITU-T X.1205]：网络安全涉及用以保护网络环境和机构及用户资产的各种工具、政策、安全理念、安全保障、指导原则、风险管理方式、行动、培训、最佳做法、保证和技术。机构和用户的资产包括相互连接的计算装置、人员、基础设施、应用、服务、电信系统以及在网络环境中全部传送和/或存储的信息。网络安全工作旨在确保防范网络环境中的各种安全风险，实现并维护机构和用户资产的安全特性。网络安全的总体目标包括：可用性、完整性（其中可能包括真实性和不可否认性）和保密性。

注 – （非[b-ITU-T X.1205]组成部分）一些国家的具体规定和法律可能要求落实保护个人可识别信息的机制。

3.1.2 交换协议[ITU-T X.1500]：有关两个或多个实体之间进行信息交换的一套技术规则和格式。

3.2 本建议书定义的术语

本建议书定义了下列术语：

3.2.1 网络安全实体：拥有或寻求网络安全信息的任何实体。

4 缩写词和首字母缩略语

本建议书使用以下缩写词和首字母缩略语：

BEEP 块可扩展交换协议
CAPEC 通用攻击模式列表和分类
CYBEX 网络安全信息交换
DDoS 分布式拒绝服务
EVCERT 扩展认证证书
HTTP 超文本传送协议
HSTS 超文本传送协议严格传输安全
IODEF 事件对象描述交换格式
MIME 多用途互联网邮件扩展
RID 实时网间防御
RSS 简单信息聚合
SCTP 流控制传输协议
SOAP 简单对象接入协议
TCP 传输控制协议
TLS 传输层安全
UDP 用户数据报协议
URI 统一资源标识符
XML 可扩展标记语言

5 惯例

无。

6 支持网络安全信息交换的传送协议

6.1 传送应用

网络安全信息交换包含繁复多样的利用若干传送协议即可实现的使用情形，每一个协议都拥有独一无二的特性。为在这些特性之间做出比较，在此说明四种具有代表性的传送应用。

6.1.1 信息传播

网络安全实体可一视同仁地传播信息，即可以通过已得到广泛使用的用于数据提供的现有协议（如RSS）完成。在进行这类信息传播时，可在不经任何过滤或不对数据进行任何针对性调整的情况下向所有人提供同一组信息。

6.1.2 发布-订阅

网络安全实体可在双边基础上向特定信息提供者订购信息，后者为前者量身定制与其有关的具体信息。在这种情况下，信息提供者可称为信息发布方（如软件厂商）和订购方之间

的中间人。这种发布–订购服务需要通过中间商进行过滤，而这反过来又需要人们进行列举（enumeration）和查询，如，列举资产或查询相关信息。

6.1.3 保证信息交换

能力相似的网络安全实体之间可交换信息，以便加大覆盖范围或加速实现事件响应。事件对象描述交换格式（IODEF） [b-ITU-T X.1541]和实时网间防御（RID） [b-ITU-T X.1580]是进行这种细节通信的两种协议。网络安全实体将明确通信端点，并在相互之间进行认证和获得保证。在此类保证交换中，每一个网络安全实体可能都需要发起与其它实体的通信（可通过双向传送协议实现）。

6.1.4 信息拥有证据

网络安全实体可能希望与已观察到特定事件的相关方进行通信，同时不向未受到影响的近邻透露细节，方法是利用特定等级的加密协议，如，隐私保护数据集交会[b-Kissner]。本质上而言，此类加密协议是在不交换信息本身的条件下交换信息拥有证据，从而使敏感信息的保密性得到保证。可在双边传送协议之上实施这类加密协议。

6.2 有关传送协议的考虑

根据网络安全实体所发挥的作用，通信端点可以非对称或对等方式运行。

在两个端点以非对称形式固定的典型情况下，请求-响应协议被认为是适当协议，因为一端总是发起通信的一方。当两个端点对等工作时，两端都可发起通信，因此，双向协议被认为是适当协议。

6.2.1 请求-响应协议

在请求-响应协议中，客户机是连接发起方，服务器是响应方。在此，信息流与客户机-服务器之间的区分没有关系，根据角色区分情况，客户机可以提供信息，也可以消费信息。

在请求-响应协议中，服务器可能无法及时向客户机传播信息，除非客户机拥有轮询服务器。换言之，客户机是信息交换的发起方，而服务器则是信息交换的响应方。

表1总结了现有的请求-响应协议。

表1 – 用于传送和交换的现有请求-响应协议

协议名称	特性	参考文献
超文本传送协议（HTTP）	HTTP提供从响应方检索或向响应方提交信息的基本机制。HTTP可用于交换由统一资源标识符（URI）确定的任何类型信息，且其类型可在多用途互联网邮件扩展（MIME）类型中具体明确。	[b-IETF RFC 2616]
简单对象接入协议（SOAP）	SOAP在HTTP之上开发完成，旨在方便属性-值配对通信。可扩展标记语言（XML）模式用于具体明确属性和值的类型。	[b-SOAP]

6.2.2 双向协议

在双向协议中，两端都可发起信息交流。这种协议可以是非对称的，即，一端被视作客户机，并需要发起连接。另一种此类协议可以是对称的，即，两端都可按各自意愿发起连接。

在双向协议中，无需在定期轮询中产生极大开销即可及时交换信息。双向协议不仅局限于对称使用情况（多个网络安全实体之间进行信息交换），而且在扩大网络传播方面也具有优势（需要在大量客户机节点之间传播信息）。

此外，还可以由一对独立的请求-响应连接进行双向连接。这种组合要求两个端点都既作为客户机也作为服务器发挥作用，但可能会带来更多的软件实施问题。

表2总结了现有的双向协议。

表2 – 用于传送和交换的现有双向协议

协议名称	特性	参考文献
块可扩展交换协议（BEEP）	BEEP能满足对称和非对称端点的要求。两端都可以既是连接发起方，也是响应方。	[b-IETF RFC 3080]
WebSocket	WebSocket协议建立在HTTP之上，因此，客户机始终是连接发起方。尽管对客户机和服务器进行了区分，但服务器可通过由客户机发起的连接发起协议互动。	[b-IETF RFC 6455]

6.3 安全方面的考虑

在CYBEX传送协议中，由网络浏览器支持的协议需要在得到采用前获得谨慎的安全分析，因为一些网络浏览器对跨网站执行的脚本区分很不完善，常常在可信度方面差距甚大。尽管正当网络安全实体可以采用网络浏览器交换信息，但同一网络浏览器实例可被用来浏览不被信任的网站，这些网站可能托管着对特定CYBEX端点带来潜在危害的代码。在这些威胁中，跨网站请求伪造（CSRF）（CAPEC ID 62）和跨网站脚本制作（XSS）（CAPEC ID 63）属于现在已知的能有效破坏具有不同信任程度的网站之间的分离原则。

表3总结了现有的、诸如HTTP扩展的应对此类威胁的对策。根据网络浏览器的品牌和版本，可以支持的扩展可能有所变化。

表3 – 旨在改进安全的现有HTTP扩展

名称	特性	参考文献
内容安全政策（CSP）	CSP可将嵌入对象来源，包括动态运行脚本，限于预先确定的一系列网站。	[b-CSP]
HTTP严格传输安全（HSTS）	HSTS将随后协议互动在特定时间内局限于安全信道，如传输层安全（TLS）。	[b- IETF RFC 6797]
HttpOnly	HttpOnly限制网络浏览器中运行的程序，使其不能接入认证证书，如cookies（信息记录程序）。	[b- IETF RFC 6265]
Origin cookies	Origin cookies限制其它网站对始发网络服务器设定的cookies进行打击，只能由确切起源对起源cookies进行修改。	[b-Bortz]

其它应用层协议亦可能受到类似威胁的影响。由于现代网络浏览器可在浏览器插件中执行任意程序，如Java和Flash脚本，因此它们可被用于伪造协议互动。因此，CYBEX端点应避免托管和运行来自不可信任渠道的软件，包括来自网站的软件。如果由于特定应用具有无歧视性质而无法对其它CYBEX端点执行上述工作，则需要对持续出现的风险进行衡量和控制。

6.4 传送和会话层方面的考虑

由于CYBEX端点需要保护通信信道的完整性，因此，鼓励使用TCP或SCTP [b-IETF RFC 4960]。此外，CYBEX端点的实施方还应通过繁复多样的手段防止拒绝服务攻击的发生，如通过SYN cookies [b-IETF RFC 4987]和其它分布式拒绝服务（DDoS）对策[b-Mirkovic]进行。实施者可进一步通过传输控制协议（TCP）认证方案[b-IETF RFC 5925]和流控制传输协议（SCTP）认证组块[b-IETF RFC 4895]所定义的信息认证代码加强通信信道的完整性。

[b-IETF RFC 5062]阐述了针对SCTP的已知威胁及其对策。为最大限度地降低反射攻击[b-Paxson]的风险，不应使用用户数据报协议（UDP）。

为实现通信的保密性，鼓励使用TLS（传输层安全协议）[b-IETF RFC 5246][b-IETF RFC 3436]。如果认为保障端点身份十分必要，则鼓励使用扩展认证证书（EVCERT）[b-EVCERT]。

参考资料

[b-ITU-T X.1205] Recommendation ITU-T X.1205 (2008), *Overview of cybersecurity.*

[b-ITU-T X.1541] Recommendation ITU-T X.1541 (2012), *Incident object description exchange format.*

[b-ITU-T X.1544] Recommendation ITU-T X.1544 (2013), *Common attack pattern enumeration and classification.*

[b-ITU-T X.1580] Recommendation ITU-T X.1580 (2012), *Real-time inter-network defense.*

[b-Bortz] Andrew Bortz, Adam Barth and Alexei Czeskis, Origin Cookies: Session Integrity for Web Applications, W2SP 2011.

[b-CSP] W3C, Content Security Policy 1.0.
http://www.w3.org/TR/CSP/

[b-EVCERT] CA/Browser Forum, *Guidelines for the Issuance and Management of Extended Validation Certificates*, Ver. 1.3.

[b-IETF RFC 2616] IETF RFC 2616 (1999), *Hypertext Transfer Protocol* – HTTP/1.1.

[b-IETF RFC 3080] IETF RFC 3080 (2001), *The Blocks Extensible Exchange Protocol Core*.

[b-IETF RFC 3436] IETF RFC 3436 (2002), *Transport Layer Security over Stream Control Transmission Protocol*.

[b-IETF RFC 4895] IETF RFC 4895 (2007), *Authenticated Chunks for the Stream Control Transmission Protocol*.

[b-IETF RFC 4960] IETF RFC 4960 (2007), *Stream Control Transmission Protocol*.

[b-IETF RFC 4987] IETF RFC 4987 (2007), *TCP SYN Flooding Attacks and Common Mitigations*.

[b-IETF RFC 5062] IETF RFC 5062 (2007), *Security Attacks Found Against the Stream Control Transmission Protocol (SCTP) and Current Countermeasures*.

[b-IETF RFC 5246] IETF RFC 5246 (2008), *The Transport Layer Security (TLS) Protocol Version 1.2*.

[b-IETF RFC 5925] IETF RFC 5925 (2010), *The TCP Authentication Option*.

[b-IETF RFC 6265] IETF RFC 6265 (2011), *HTTP State Management Mechanism*.

[b-IETF RFC 6455] IETF RFC 6455 (2011), *The WebSocket Protocol*.

[b-IETF RFC 6797] IETF RFC 6797 (2012), *HTTP Strict Transport Security*.

[b-Kissner] Lea Kissner and Dawn Song, *Privacy-Preserving Set Operations*, CRYPTO 2005.

[b-Mirkovic] Jelena Mirkovic and Peter Reiher, *A Taxonomy of DDoS Attack and DDoS Defense Mechanisms*, ACM SIGCOMM Computer Communication Review, 34(2), April 2004.

[b-Paxson] Vern Paxson, *An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks*, ACM SIGCOMM Computer Communication Review, 31(3), July 2001.

[b-SOAP] W3C, *Simple Object Access Protocol*.
SOAP Version 1.2 Part 1: Messaging Framework (2007).
SOAP Version 1.2 Part 2: Adjuncts (2007).

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
2014年，日内瓦