国 际 电 信 联 盟

ITU-T X.1210

(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

网络空间安全 – 网络安全

用于互联网协议网络的源码安全故障排除机制概述

ITU-T X.1210 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	
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.1210 建议书

用于互联网协议网络的源码安全故障排除机制概述

摘要

ITU-T X.1210建议书介绍了针对安全问题的源码安全故障排除机制以及故障排除机制的挑选标准和基本安全导则。

互联网协议网络中源码故障排除安全问题涉及用来发现有关造成网络故障事件的进入点、路径、半路径或一个或多个数据包来源的技术信息的技术。这些技术通常用来实施缓解措施。

历史

版本	建议书	批准	研究组	唯一ID*
1.0	ITU-T X.1210	2014-01-24	17	11.1002/1000/12043

* 如欲访问本建议书，请在网页浏览器的地址栏输入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

ITU-T X.1210 建议书

用于互联网协议网络的源码安全故障排除机制概述

1 范围

本建议书概要介绍了源码安全故障排除机制以及故障排除机制的评估标准和基本安全导则。

本ITU-T建议书的实施者和用户须遵守所有适用的国家及区域性法律、法规和政策。

2 参考文献

无。

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 服务拒绝[b-ITU X.800]：防止授权接入资源或拖延时间紧迫的操作。

3.1.2 安全域[b-ITU-T T.411]：遵循同一安全政策的一批资源。

3.1.3 威胁[b-ITU-T X.800]：破坏安全性的潜在可能。

3.2 本建议书定义的术语

无。

4 缩写词和首字母缩略语

本建议书使用以下缩略词和首字母缩略语：

AS 自治系统

BGP 边界网关协议

DoS 服务拒绝

ICMP 互联网控制消息协议

IP 互联网协议

IPFIX IP流信息出口

IPv4/v6 互联网协议第4版/第6版

ISP 互联网服务提供商

RID 实时网间防御

TCP 发射控制协议

5 惯例

无。

6 源码安全故障排除机制概述

排除互联网协议（IP）网络中的源码安全问题一般包括一个用来稳妥确定可能承载或未承载发送者的正确IP地址的一个或多个IP包的来源或正在引发安全问题的路径或部分路径的技术及/或管理过程。

源码安全故障排除机制可在诸如网络路由器或主机等网元的帮助下实时确定此类安全问题事件的物理或逻辑位置。

下文探讨了IP网络中的安全问题排除机制。

6.1 使用链路测试进行的源码安全故障排除

故障排除可从最靠近受害者的路由器开始，并以互动的方式测试上游链路直至互联网服务提供商能够确定哪一条是承载违规业务流量的链路。理想的状态是，该程序在上游路由器循环反复直至确定安全问题来源。

这项技术假设安全问题在故障排除程序完成之前一直不断出现。因此，这项技术不适用于事后发现的攻击、间或进行的攻击或针对安全故障排除调整了其行为的攻击。

输入调试是链路测试机制的一种实施方式。很多路由器已具备这项功能，可以使管理员确定具体数据包的传入网络链路。如路由器操作者了解攻击业务的具体特性（被称为“攻击签名”），则可以在路由器上确定传入网络链路。

6.2 使用重叠网进行的源码安全故障排除机制

黑洞机制[b-IETF RFC 3882]是一项利用攻击流量分析隧道的操作技术，可在能够到达目的地/被攻击自治系统（AS）的攻击的所有可能切入点处实施。使用边界网关协议（BGP）[b-IETF RFC 4271]，目的地为被攻击/目标主机的业务流量可能受到黑洞攻击，即脱离网络或重新路由至特殊路径（隧道），使设备得以捕获该业务进行分析并在之后予以丢弃。

6.3 使用探测进行的源码安全故障排除

互联网协议第4版（IPv4）[b-IETF RFC 792]和互联网协议第6版（IPv6）[b-IETF RFC 4443]的互联网控制消息协议（ICMP）无论在现在还是未来都是最为有效的IP网络故障排除机制之一。包括ping和traceroute命令在内的多种工具可与基于ICMP的通用操作系统捆绑在一起开展端到端的或链路层面的故障排除。

6.4 使用登录和取样进行的源码安全故障排除

流取样可以作为解决IP网络安全问题的一项有效的故障排除机制。运营商可使用sFlow [b-IETF RFC 3176]、NetFlow [b-IETF RFC 3954]或IP流信息出口（IPFIX）[b-IETF RFC 5655]，同时兼顾部署路由器所支持的流取样标准。

6.5 自治系统的源码安全故障排除

面对遍布自治系统的大规模安全问题，运营商可以依靠基于探测的故障排除工具（见第6.3节）以及互联网上提供的在线监测程序（例如Looking Glass [b-LG]）予以解决。将来，

运营商也许能够通过实时网间防御（RID）[b-IETF RFC 6045]等手段，简化自治系统中更为先进的故障排除工具的信息交流。

7 源码安全故障排除机制的基本安全导则

源码安全故障排除的基本安全导则包括如下内容：

- 源码安全故障排除机制应该具备可扩展性、稳健性和可复原性。
- 源码安全故障排除机制应在多个域内部署运行，每个域均由负责任的安全管理员管理（即自治系统间故障排除）。
- 源码安全故障排除机制应通过以下两种部署模式之一进行实施：集中部署模式或分布部署模式。
- 源码安全故障排除机制应提供有关造成网络事件的进入点、路径、半路径或一个或多个包来源的发现技术信息，以便实施缓解措施。
- 为了选择适合的源码安全故障排除机制，应根据第8节描述的标准评估故障排除机制。
- 跨自治系统的源码安全故障排除机制界面应确保在不同安全域间交换的信息的保密性、数据来源认证和完整性，同时还可确保故障排除机制的可用性。

8 评估源码故障排除机制的标准

可用于评估故障排除机制的标准如下所述：

- 互联网服务提供商（ISP）的参与程度：ISP管理员在详细说明故障排除时ISP的参与程度。多数故障排除机制的假定前提是，ISP提供有限设施以便实现故障排除。理想的故障排除方案仅需要较低程度的ISP参与。
- 故障排除需要的数据包数量：一旦发现安全问题，管理员用来确定安全问题来源的数据包数量。
- 部分部署的有效性：在单个ISP内部分部署故障排除方案时故障排除的有效性。有效性在从无法排除故障到可产生有意义的识别的范围内变化。
- 故障排除的处理开销：中介网元或潜在受害主机的处理开销量。可将中介网元或受害主机的处理开销控制在最低水平的理想故障排除方案更为可取。
- 带宽增加水平：排除故障所需要的额外流量。理想的故障排除机制应使带宽增加限制在最低水平或无增加。
- 内存需求：网元或专用故障排除服务器所需要的附加内存。网元不需要额外内存，而增加专用服务器的内存是可以接受的。理想的故障排除机制需要有限地增加专用服务器的内存，但不增加网元内存。

- 故障排除稳健性：故障排除机制即使在参与故障排除的部分网元受到破坏时也能产生有意义的绩效成果的能力。破坏由网元配置不当或软件补丁不合适造成。
- 可扩展性：增加单一网元时需在其它网元上进行的附加配置量。可扩展性代表了扩展故障排除方案的方便性。如只有新增网元需要配置，则可扩展性良好，如增加单一网元需要对其它网元进行全面配置，可扩展性则较差。理想的故障排除机制应具有可扩展性。
- 实施故障排除所需功能数量：实施故障排除方案所需要的附加功能数量。
- 处理大规模全网安全问题的能力：故障排除方案体现出来的在确定全网安全问题方面的能力。理想的故障排除方案应能确定所有安全问题，包括分布式服务拒绝（DDoS）攻击。
- 排除变形数据包的能力：故障排除方案即使在数据包变形的情况下仍能确定问题来源的能力。数据包变形意味着数据包在转发过程中被修改。网络地址翻译便属于一种常见变形，在该过程中多个或一个数据包的来源和/或目的地地址发生了变化。

参考资料

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

[b-ITU-T T.411] Recommendation ITU-T T.411 (1993), *Information technology – Open Document Architecture (ODA) and interchange format: Introduction and general principles*.

[b-IETF RFC 792] IETF RFC 792 (1981), *Internet Control Message Protocol*.

[b-IETF RFC 3176] IETF RFC 3176 (2001), *InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks*.

[b-IETF RFC 3882] IETF RFC 3882 (2004), *Configuring BGP to Block Denial-of-Service Attacks*.

[b-IETF RFC 3954] IETF RFC 3954 (2004), *Cisco Systems NetFlow Services Export Version 9*.

[b-IETF RFC 4271] IETF RFC 4271 (2006), *A Border Gateway Protocol 4 (BGP-4)*.

[b-IETF RFC 4443] IETF RFC 4443 (2006), *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*.

[b-IETF RFC 5655] IETF RFC 5655 (2009), *Specification of the IP Flow Information Export (IPFIX) File Format*.

[b-IETF RFC 6045] IETF RFC 6045 (2010), *Real-time Inter-network Defense (RID)*.

[b-LG] BGP Looking Glass, http://www.lookinglass.org/

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