International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1210

(01/2014)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Cyberspace security – Cybersecurity

Overview of source-based security troubleshooting mechanisms for Internet protocol-based networks

Recommendation ITU-T X.1210

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	**X.1200–X.1229**
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1210

Overview of source-based security troubleshooting mechanisms for Internet protocol-based network

Summary

Recommendation ITU-T X.1210 provides source-based security troubleshooting mechanisms for security issues, as well as selection criteria and basic security guidelines of troubleshooting mechanisms.

Source-based troubleshooting security issues in Internet protocol-based networks involve techniques used to discover technical information concerning the ingress points, paths, partial paths or sources of a packet or packets causing a problematic network event, generally for the purposes of applying mitigation measures.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1210	2014-01-24	17	11.1002/1000/12043

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Page

Recommendation ITU-T X.1210

Overview of source-based security troubleshooting mechanisms for Internet protocol-based network

1 Scope

This Recommendation provides an overview of source-based security troubleshooting mechanisms, evaluation criteria and basic security guidelines of troubleshooting mechanisms.

Implementers and users of this ITU-T Recommendation shall comply with all applicable national and regional laws, regulations and policies.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 denial of service [b-ITU X.800]: The prevention of authorized access to resources or the delaying of time-critical operations.

3.1.2 security domain [b-ITU-T T.411]: The set of resources subject to a single security policy.

3.1.3 threat [b-ITU-T X.800]: A potential violation of security.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AS	Autonomous System
BGP	Border Gateway Protocol
DoS	Denial of Service
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IPFIX	IP Flow Information export
IPv4/v6	Internet Protocol version 4/version 6
ISP	Internet Service Provider
RID	Real-time Inter-network Defence
TCP	Transmission Control protocol

5 Conventions

None.

6 General overview of source-based security troubleshooting mechanisms

Troubleshooting source-based security issues in Internet protocol (IP)-based networks generally involves a technical and/or an administrative process for reliably identifying the source of an IP packet or of IP packets that may or may not carry the correct IP address of the sender, or the paths or part of paths that are inducing security issues.

Source-based security troubleshooting mechanisms can be used to identify the physical or logical location of such security issue events in real time with the help of network elements such as routers or hosts in the network.

Troubleshooting mechanisms for security issues in IP-based networks are discussed below.

6.1 Source-based security troubleshooting with link testing

Troubleshooting can start from the router closest to the victim and interactively test its upstream links until the Internet service providers can determine which one of them is being used to carry the offending traffic. Ideally, this procedure is repeated recursively on the upstream router until the source of the security issue is identified.

This technique assumes that a security issue remains active until the completion of the troubleshooting procedure. As such, this technique is inappropriate for attacks that are detected after the fact, for attacks that occur intermittently, or for attacks that modulate their behaviour in response to security troubleshooting.

Input debugging is one implementation of the link testing mechanism. This is a feature that already exists on many routers allowing the administrator to determine incoming network links for specific packets. If the router operator knows the attack traffic's specific characteristics (called "attack signature"), it is then possible to determine the incoming network link on the router.

6.2 Source-based security troubleshooting mechanism with overlay network

A black-holing mechanism [b-IETF RFC 3882] is an operational technique that utilizes a sinkhole tunnel which is implemented at all possible entry points from which attacks can pass into the destination/attacked autonomous system (AS). Using the border gateway protocol (BGP) [b-IETF RFC 4271], traffic destined for the attacked/targeted host can be black-holed, i.e., dropped from the network, or re-routed to a special path (tunnel) where a device can capture the traffic for analysis and then drop the traffic.

6.3 Source-based security troubleshooting with probing

Internet control message protocol (ICMP), for both Internet protocol version 4 (IPv4) [b-IETF RFC 792] and Internet protocol version 6 (IPv6) [b-IETF RFC 4443], has been and will continue to remain one of the most useful troubleshooting mechanisms for IP-based networks. A number of tools, including ping and traceroute, come bundled with common operating systems that employ ICMP to conduct end-to-end or link-level troubleshooting.

6.4 Source-based security troubleshooting with logging and sampling

Flow sampling can be a useful troubleshooting mechanism for security issues in IP-based networks. Operators may use sFlow [b-IETF RFC 3176], NetFlow [b-IETF RFC 3954] or IP flow information export (IPFIX) [b-IETF RFC 5655] while taking into account supported flow sampling standards in deployed routers.

6.5 Source-based security troubleshooting across autonomous systems

In large-scale security issues that span across autonomous systems, operators can rely on troubleshooting tools based on probing (see clause 6.3) and online probes that are available on the Internet, e.g., Looking Glass [b-LG]. In the future, operators may be able to facilitate information exchange for more advanced troubleshooting tools across autonomous systems, e.g., by using real-time inter-network defense (RID) [b-IETF RFC 6045].

7 Basic security guidelines of the source-based security troubleshooting mechanisms

The basic security guidelines of source-based security troubleshooting are provided as follows:

- The source-based security troubleshooting mechanisms should be designed to be scalable, robust and resilient.
- The source-based security troubleshooting mechanisms should be deployed and operated across multiple domains each of which is managed by a responsible security administrator (i.e., inter-AS troubleshooting).
- The source-based security troubleshooting mechanisms should be implemented into one of two types of deployment models: a centralized deployment model or a distributed deployment model.
- The source-based security troubleshooting mechanisms should provide discovering technical information concerning the ingress points, paths, partial paths or sources of a packet or packets causing a problematic network event, generally for the purposes of applying mitigation measures.
- In order to select a suitable source-based security troubleshooting mechanism, the mechanisms should be evaluated according to the criteria described in clause 8.
- The interface of source-based security troubleshooting mechanisms across autonomous systems should provide confidentiality, data origin authentication and integrity of the information exchanged between the various security domains and may provide availability of the troubleshooting mechanism.

8 Criteria for evaluating source-based troubleshooting mechanisms

Criteria which can be used to evaluate troubleshooting mechanisms are specified as follows:

- Degree of Internet service provider (ISP) involvement: The degree of ISP involvement when troubleshooting is specified by an ISP administrator. Most troubleshooting mechanisms assume that ISPs provide limited facilities to enable troubleshooting. An ideal troubleshooting scheme would require a low level of ISP involvement.
- Number of packets required for troubleshooting: The number of packets used by an administrator to identify the source of the security issue once the security issue has been detected.
- Effectiveness of partial deployment: The degree of effectiveness of troubleshooting when the troubleshooting schemes are deployed partially within a single ISP. The effectiveness varies from inability to producing meaningful identification.
- Processing overhead for troubleshooting: The amount of processing overhead at the intermediate network element or a potential victim host. An ideal troubleshooting scheme with minimal processing overhead for the intermediate network element or victim host would be preferred.
- Degree of bandwidth increase: The additional amount of traffic required for troubleshooting. A desirable troubleshooting mechanism should have minimal or no increase of additional bandwidth.
- Memory requirement: The amount of additional memory required on the network elements or a dedicated troubleshooting server. Additional memory on the network element would be undesirable, whereas additional memory on dedicated servers is tolerable. An ideal

troubleshooting mechanism would require a limited amount of additional memory at the dedicated server but no additional memory at the network element.

- Robustness of troubleshooting: The capability of the troubleshooting mechanism to produce meaningful performance results even if some network elements involved in troubleshooting have been subverted. Subversion occurs due to errors arising from the misconfiguration of the network element or an improper software patch.
- Scalability: The amount of additional configuration performed on the other network elements required to add a single network element. This indicates how easily the troubleshooting scheme can be expanded. Scalability is considered to be good if only the newly added network element requires configuration and is considered to be poor if adding a single network element requires the complete configuration of the rest of network elements. An ideal troubleshooting mechanism should be scalable.
- Number of functions needed to implement troubleshooting: The amount of additional functions required to implement the given troubleshooting scheme.
- Capability to handle massive network-wide security issues: The ability of the troubleshooting scheme to reflect how well the troubleshooting scheme can identify network-wide security issues. An ideal troubleshooting scheme should identify any security issues, including distributed denial-of-service (DDoS) attacks.
- Capability to troubleshoot transformed packets: The ability of the troubleshooting scheme to identify the source of problems even when the transformation of packets occurs. Packet transformation means packet modification when packet forwarding occurs. A common transformation is network address translation, where the source and/or destination address of the packets or packet are/is changed.

.

Bibliography

[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/

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2014