International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series X
Supplement 10
(09/2011)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

ITU-T X.1205 – Supplement on usability of network traceback

ITU-T X-series Recommendations – Supplement 10

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

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

Supplement 10 to ITU-T X-series Recommendations

ITU-T X.1205 – Supplement on usability of network traceback

Summary

This supplement to Recommendation ITU-T X.1205 provides an overview of traceback for responsive measures to certain network issues within a single or a more complex array of service providers. Traceback may assist in discovering ingress points, paths, partial paths or sources of problematic network events. This information may aid service providers in mitigating such events.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X Suppl. 10	2011-09-02	17

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

Compliance with this publication is voluntary. However, the publication may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the publication 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 publication is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication 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 publication development process.

As of the date of approval of this publication, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this publication. 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

Supplement 10 to ITU-T X-series Recommendations

ITU-T X.1205 – Supplement on usability of network traceback

1 Scope

This supplement to Recommendation ITU-T X.1205 provides an overview of traceback capabilities that may be useful in responding to network incidents where some knowledge of the source(s) of those incidents is necessary for effective cybersecurity responsive measures. It includes descriptions and usability considerations of traceback.

Traceback, as described in this supplement, may be in conflict with laws and regulation (e.g., secrecy of telecommunications or data protection/privacy) in some countries or regions, and therefore cannot be applied in those countries or regions. Implementers and users of the described mechanisms shall comply with all applicable national and regional laws, regulations and policies.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This supplement uses the following terms defined elsewhere:

3.1.1 domain [b-ITU-T M.3010]: A set of managed resources subject to a common management policy.

3.1.2 event [b-ITU-T M.2140]: An instantaneous occurrence that changes the global status of an object. This status change may be persistent or temporary, allowing for surveillance, monitoring, and performance measurement functionality, etc. Events may or may not generate reports, may be spontaneous or planned, may trigger other events, or may be triggered by one or more other events.

3.2 Terms defined in this supplement

This supplement defines the following term:

3.2.1 traceback: A technique 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.

4 Abbreviations and acronyms

ADSL	Asymmetrical Digital Subscriber Line
DDoS	Distributed Denial of Service
IP	Internet Protocol
IPv4	IP version 4
IPv6	IP version 6
NAT	Network Address Translation

5 Conventions

None.

6 Traceback introduction

IP-based incidents, especially attacks on network infrastructure, have increased dramatically in number and complexity. End users, service providers, and network operators are all adversely affected by such attacks.

In order to deal with these attacks, traceback has been developed and evolved over some years. Traceback attempts to discover information about the attack source(s) for the purpose of pursuing remediation measures. For example, when DDoS attacks occur, network providers along the attack path may be able to detect and mitigate DDoS traffic at ingress points with the help of traceback.

Traceback has evolved from network operational tools that have long existed and been included as part of network management systems and products. Indeed, the basic traceroute tool is provided with almost every computer and network element operating system. When combined with directory systems such as WHOIS, some basic traceback capabilities can be created. These, and other techniques, are examples of the type of traceback used by service providers. This supplement does not describe such techniques, but rather the usability considerations of traceback.

Clauses 7 and 8, and corresponding subclauses, describe the overview and usability consideration of traceback.

7 Possible traceback capabilities in networks

7.1 Source identification

A service provider seeking to uncover the source of a problematic network event may use traceback immediately after the incident has been identified. In the scenario in which the service provider has made appropriate investment in, and configuration of, core and edge routers based on the applied traceback mechanisms, operators may be able to uncover at the edge router or the incoming physical port the source of the problematic network event. Source identification may help operators stop the problematic network event or mitigate its impact.

7.2 Ingress point identification

A network operator, who operates a region/domain (having multiple links to adjacent regions/domains), may use traceback to identify the set of affected links from a particular network incident. The ability to narrow down the number of affected links may help operators expedite the investigation and, when necessary, mitigation procedures.

7.3 Partial path identification

If traceback is both deployed and possible across multiple regions/domains, it can be used to uncover a partial path of widespread attacks. While source identification across multiple regions/domains may be difficult under partial traceback deployment, some applications of traceback may be able to identify the partial path or multiple paths of a problematic network event, thus helping mitigation procedures across multiple regions/domains.

8 Potential applications of traceback

8.1 Application to DDoS attacks

DDoS attacks are characterized by large amounts of traffic from multiple sources destined for particular network end resources to render that resource unavailable to the intended users. Figure 1 shows a typical DDoS attack scenario. The target of the DDoS attack is the victim served by Domain/region 1. The DDoS attack not only affects the victim, but also the resources within Domain/region 1. The attack traffic comes into Domain/region 1 from Domain/region 2 and Domain/region 3, which belong to different network providers.

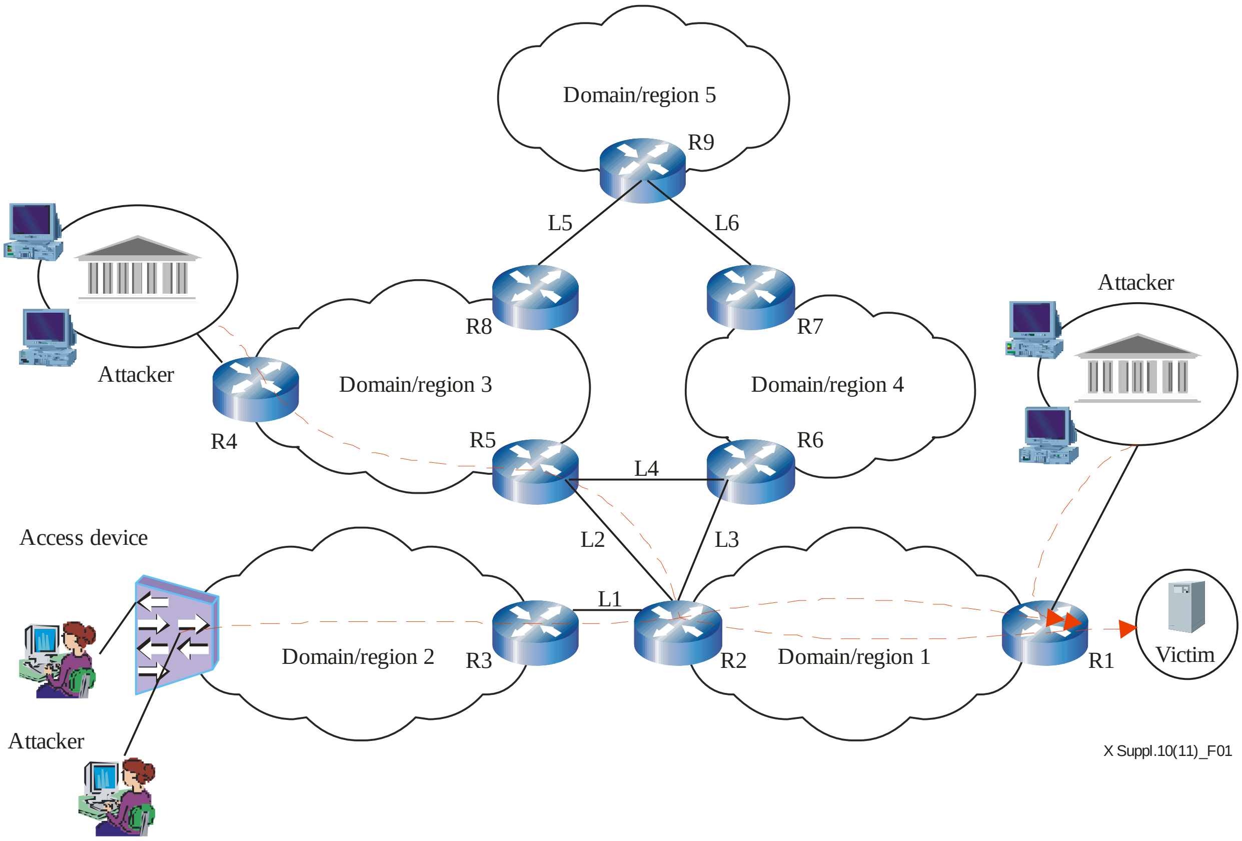

Figure 1 – Typical DDoS attack applications

In a DDoS attack, the victim expects the network provider to block the attack traffic before it reaches him, as this type of attack typically attempts to overwhelm the network resources (bandwidth) of the connection circuit between the victim and the provider. Because DDoS attacks can be comprised of hundreds or thousands of sources, or more, sending attack packets, it is difficult to identify the source of all such packets. Traceback is useful in this case not for identification of the sources, but rather for identification of the ingress points and partial paths within the provider network where the DDos attack can best be mitigated. Traceback, in this case, helps network providers to determine the ingress edge router and affected high value links.

In the DDoS scenario in Figure 1, the quick solution is dropping DDoS traffic at edge router R1. But if the attack traffic has reached R1, there has already been a great deal of unwanted traffic flooding the network and other network elements within Domain/region 1, which wastes network bandwidth and platform resources. Therefore, by using traceback within Domain/region 1, operators can determine specific ingress points from other providers; namely Domain/region 2 and Domain/region 3, but not Domain/region 4. The Domain/region 1 may wish to engage in cooperative traceback with Domain/region 2 and Domain/region 3 providers, to enable pushing mitigations even further towards attack sources to protect interconnection points. Then there will be several better solutions, such as dropping the DDoS attack traffic by R4, the access device of Domain/region 3, and by R5, the peering router between Domain/region 1 and Domain/region 3, for example.

Various factors may affect traceback. There may be various network environments, such as networks with IPv4 and IPv6 addresses, networks with different access techniques (e.g., ADSL, cable and Ethernet), and so on. In addition, the attacker may be using packets with spoofed source addresses, may be located behind NATs, and/or may have its IP address assigned dynamically. Traceback must consider all of these various network environments.

8.2 Application to misconfiguration issues

Many network and application issues are caused by misconfiguration. In such situations, operators might find such misconfiguration problems with the help of traceback after problematic network events have occurred.

8.3 Application to routing issues

A domain/region always has several links to adjacent domains/regions. The routing path could be managed based on policies to provide a differentiated service, to load-balance network traffic, etc. Therefore, if it is found that traffic from the source domain/region to the destination domain/region does not follow existing policies, operators may utilize traceback to identify the path of packets and determine where routing problems exist. For example, in Figure 1, there are several paths from Domain/region 5 to Domain/region 1, and all the traffic from the former to the latter is expected to traverse through L2 based on routing policy. Thus, when L5 is down, upon receiving packets through L2, operators in Domain/region 5 could use traceback to find out the routing issues by ascertaining that all packets were transferred through "L6->Domain/region4->L4->L2".

Bibliography

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

[b-ITU-T X.1231] Recommendation ITU-T X.1231 (2008), *Technical strategies for countering spam*.

[b-ITU-T M.2140] Recommendation ITU-T M.2140 (2000), *Transport network event correlation*.

[b-ITU-T M.3010] Recommendation ITU-T M.3010 (2000), *Principles for a telecommunications management network.*

[b-ITU-T X. Suppl. 8] ITU-T X-series Recommendations – Supplement 8 (2010), *ITU-T X.1205 – Supplement on best practices against botnet threats.*

[b-Majumdar] Majumdar, Saugat; D. Kulkarni, C. Ravishankar (2011). *DHCP Origin Traceback in Ethernet Switched Networks*. 12th International Conference on Distributed Computing and Networking (ICDCN 2011), Bangalore, India, January 2011. <http://people.bu.edu/kulkarni/icdcn2011.pdf>

[b-Hazeyama] Hazeyama, Hiroaki; Y. Kadobayashi, D. Miyamoto and M. Oe (2006). *An Autonomous Architecture for Inter-Domain Traceback across the Borders of Network Operation*. IEEE Computer Society 2006, Proceedings of the 11th IEEE Symposium on Computers and Communications. Cagliari, Sardinia, Italy. pp. 378-385.

[b-Belenky] Belenky, Andrey; Nirwan Ansari (2007). *On deterministic packet marking.* Computer Networks: The International Journal of Computer and Telecommunications Networking, Vol. 51 (Issue 10): pp. 2677-2700.

[b-Rayanchu] Rayanchu, Shravan K.; Barua, Gautam (2004). *Tracing Attackers with Deterministic Edge Router Marking (DERM).* First International Conference on Distributed Computing and Internet Technology, Bhubaneswar, India. vol. 3347, pp. 400-409.

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, 2012