International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series X

Supplement 10

(01/2014)

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
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.

Supplement 10 to ITU-T X-series Recommendations

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

Summary

Supplement 10 to the ITU-T X-series of Recommendations 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	Unique ID*
1.0	ITU-T X Suppl. 10	2011-09-02	17	11.1002/1000/11341
2.0	ITU-T X Suppl. 10	2014-01-24	17	11.1002/1000/12160

* 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 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 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 the traceback.

Traceback, as described in this supplement, may be in conflict with laws and regulation (e.g., secrecy of telecommunications or data protection and/or 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

This Supplement uses the following abbreviations and acronyms:

ADSL Asymmetric 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 the 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 was developed, and it has now evolved for several years. Traceback attempts to discover information about the attack source(s) for the purpose of pursuing remediation measures. For example, when a distributed denial of service (DDoS) attack occurs, network providers along the attack path may be able to detect and mitigate DDoS traffic at the ingress points with the help of traceback.

Traceback has evolved from network operational tools that have existed for a long time and it has been included as part of the 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 [b-IETF RFC 3912], 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 describe the overview and usability considerations 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 that operates a region/domain (with multiple links to adjacent regions/domains) may use traceback to identify the set of links affected by a particular network incident. The ability to narrow down the number of affected links may help operators expedite the investigation and, when necessary, apply 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, in support of the 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 that originates in multiple sources and is destined to particular network end resources. It is sent with the intention of rendering the targeted resources 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.

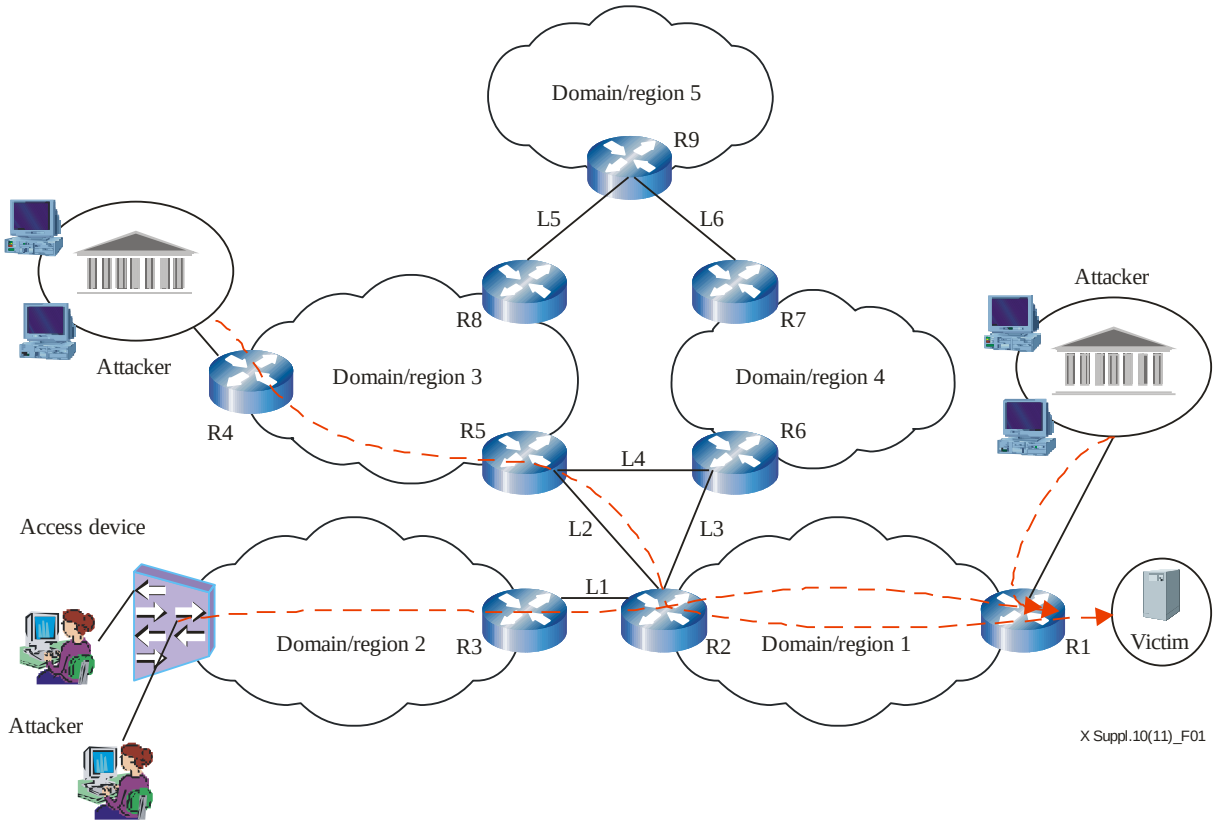

Figure 1 – Typical DDoS attack applications

As DDoS attacks typically attempt to overwhelm the network resources (bandwidth) of the connection circuit between the victim and the provider, the victim expects that the network provider will block the attack traffic before it reaches the targeted resources. Because DDoS attacks can involve 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's 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. Domain/region 1 providers 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. There are, then,

several better solutions, like for example, dropping the DDoS attack traffic at R4, the access device of Domain/region 3, and at R5, the peering router between Domain/region 1 and Domain/region 3.

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., asymmetric digital subscriber line (ADSL), cable and Ethernet), etc. In addition, the attacker may be using packets with spoofed source addresses, may be located behind network address translations (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 the 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, if L5 is down, upon receiving packets through L2, operators in the Domain/region 5 could use traceback to find out the routing issues by ascertaining that all packets were transferred through "L6 → Domain/region 4 → L4 → L2".

Appendix I

Overview of traceback mechanisms research

This appendix provides an overview of traceback mechanisms, including taxonomy and fundamental operations of the key traceback mechanisms. The appendix also specifies the criteria for classifying the traceback mechanisms, provides a comparison of various traceback mechanisms according to the criteria and describes basic security requirements for traceback mechanisms.

NOTE – Traceback mechanisms, as described in this appendix, may be in conflict with the laws and regulations (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 should comply with all the applicable national and regional laws, regulations and policies.

I.1 Abbreviations and acronyms

This appendix uses the following abbreviations and acronyms:

AAM Advanced and Authenticated packet Marking

AS Autonomous System

DDoS Distributed Denial of Service

DGA Data Generation Agent

DLL Distributed Link List

DPM Deterministic Marking Mechanism

GRE Generic Route Encapsulation

HMAC Hashed Message Authentication Code

ID Identifier

IDS Intrusion Detection System

IPSec Internet Protocol Security

ISP Internet Service Provider

PPM Probabilistic Packet Marking

RID Real time Inter-network Defence

SCAR SPIE Collection And Reduction

SPIE Source Path Isolation Engine

STM SPIE Traceback Manager

TCP Transmission Control Protocol

TR Tracking Router

TTL Time To Live

VPN Virtual Private Network

I.2 Classification of traceback mechanisms

Traceback is defined as 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 purpose of applying mitigation measures. Traceback mechanisms are classified

according to three criteria: connection method, response way and deployment location of the traceback module.

In the first criterion, i.e., the connection method, the mechanisms are classified into transmission control protocol (TCP) connection traceback or IP traceback. TCP connection traceback makes use of the characteristics of the TCP connection such as a connection-oriented connection. This way mainly uses the characteristics of the TCP connection chains for traceback. On the other hand, since IP operates in the connectionless mode, IP traceback should make use of logs in the victim system or transit network node and trace the attacker's location using the log information.

In the second criterion, i.e., the response way, the mechanisms are classified either as passive methods or active methods. In passive methods, the traceback is initiated when the victim system detects the attacks, and should be completed while the attack is still in progress. In active methods, the transit network element records the relevant information for traceback as the packets are forwarded and the stored traceback-related information is used to construct the attack path back to the source of the attack. Currently, many companies are making efforts to develop active preventive systems to block in real time the attempt of hacking itself.

In the third criterion, i.e., the deployment location of traceback module, the mechanisms are classified as either network-based traceback or host-based traceback, according to the location where a traceback module is installed or deployed. In network-based traceback, the traceback module can be installed in the server, router, gateway or other devices forming the physical communication path from the attacker to the victim system when the packets pass through the network. In host-based traceback, the traceback module can be installed in each host of the networks providing traceback with information.

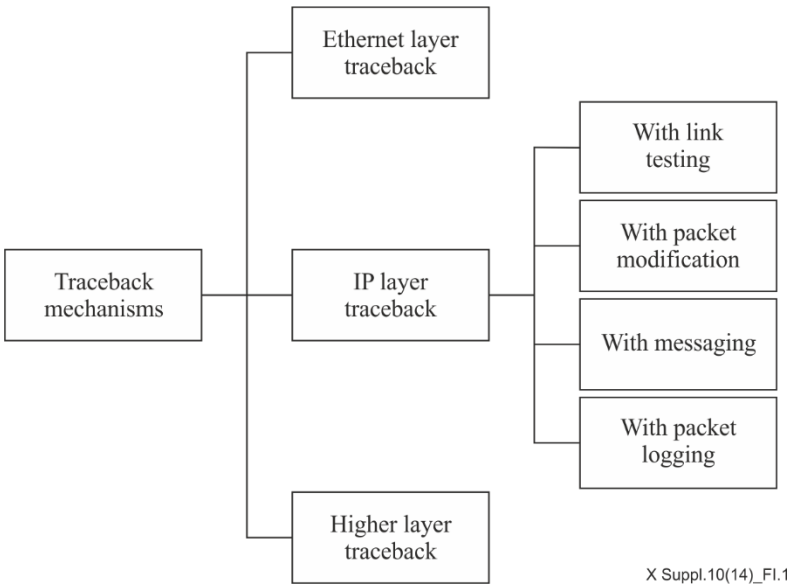

Figure I.1 – Classification of traceback mechanisms according to the connection method

This clause specifies the criteria for classifying the existing traceback mechanisms: a layer implementing traceback mechanism and an action type of each network element.

Figure I.1 illustrates the classification of traceback mechanisms based on two architectural choices: the layer implementing the traceback mechanism and an action type of the traceback element.

Choice of layer: Layer where the traceback mechanism is implemented – Traceback mechanisms are classified into Ethernet layer traceback, IP layer traceback or higher-layer traceback, depending on the layer in which the traceback mechanism is operating. Most traceback mechanisms fall under the

IP layer traceback category, which is further categorized according to the following choice of action type.

Choice of action type: Action type of the traceback element – Traceback mechanisms are classified into four categories depending on the action type of each network element: link testing [b-Stone], modification of packets [b-Savage] and [b-Song], messaging, and logging packets [b-Snoeren-1]. Link testing traceback tests links between routers; packet modification traceback modifies packets at a network element, i.e., a router, to for example mark or encapsulate packets; packet messaging traceback sends messages, e.g., ICMP messages from routers to victims; and packet digesting traceback stores audit logs of the forwarded packets at the routers to support tracing attack flows.

I.3 IP layer traceback mechanisms

This clause describes the basic operations of major existing traceback mechanisms for each category of the IP layer traceback mechanisms.

I.3.1 Traceback with link testing

The controlled flooding mechanism works by generating a burst of network traffic from the victim's network to the upstream network segments and observing how this intentionally-generated flood affects the intensity of the incoming attack traffic. Using a map of the known Internet topology around the victim, these packet floods are targeted specifically at certain hosts upstream from the victim's network; they iteratively flood each incoming network link on the routers closest to the victim's network. From the changes in the attack traffic's frequency and intensity, the victim can deduce the incoming network link on the upstream router and repeat the same process on the router one level above.

I.3.2 Traceback mechanism with overlay network

This type of traceback mechanism forwards packets to a certain network point, where they are monitored in the network. It can be applicable to an autonomous system (AS) domain.

Overlay network-based traceback mechanism (so-called CentreTrack): An overlay network-based traceback mechanism introduces a tracking router (TR), a special type of router connected to the edge router either physically or virtually with an IP tunnel, called generic route encapsulation (GRE) tunnel, in a network [b-Stone]. All TRs should optionally be connected to a central TR via the IP tunnels, creating a total overlay network. If an attack is detected, a victim node sends the traceback-related information to the TR which then uses the information to construct the attack connection chain. The malicious traffic is routed through the overlay network via the dynamic routing protocol.

IP traceback with Internet protocol security (IPSec): This mechanism [b-Chang] is configured on the assumption that the complete network topology is known to the system. What follows is the underlying principle, i.e., if there is an IPSec security association between an arbitrary router and the victim, and the attack packets detected are authenticated by the association; the attack is originated on some device further than this router. If the packets of the attack are not authenticated by this security association, the attack is originated on some device between this router and the victim. By establishing these security associations, it is possible to identify a single router or a group of routers where the attack was initiated.

I.3.3 Traceback with packet modification

The traceback mechanisms in this category modify, append and/or encapsulate packets at routers. Those modified packets are analysed at the host node which is usually a victim node. The major schemes are described below.

Probabilistic packet marking: The probabilistic packet marking mechanism is characterized by inserting traceback data into the IP packet to be traced, thus marking the packet on its way through the various routers on the network to the destination host (Figure I.2). Packets are marked with

probability of 1/25. The marked packet stores information about only one link in the attack path. In other words, probabilistic packet marking (PPM) is a traceback method that inserts the router's information for the packet that passes the router along the attack connection chain so that the victim host can construct the attack path taken by the traffic using the ICMP packet, even if an attacker uses the spoofed IP address instead of the active IP address.

Deterministic marking mechanism (DPM): In the deterministic marking mechanism, only the ingress router on the attack path marks every packet passing through it with its router IP address [b-Belenky03], enabling a victim to identify packets traversing the same paths through the Internet on a per packet basis, regardless of the source IP address spoofing. It also uses the 16-bit identification field and reserved 1-bit flag field. The IP address is split into two halves of 16 bits each and a randomly chosen segment is marked in the identifier (ID) field in the IP header. The 1-bit flag is used to inform the victim which fragment is marked in the identifier (ID) field, i.e., "0" indicates the first half of the IP address and "1" indicates the second half. As a merit of this mechanism, a network can implement it without revealing its internal network topology.

Advanced and authenticated packet marking (AAM): As an enhanced variant of the PPM scheme [b-Song], AAM was designed keeping in mind avoiding the problem of spurious packet markings generated in PPM when a router is compromised. There are two variants: an algorithm for advanced marking and an algorithm for advanced and authenticated marking scheme. This scheme also uses the 16-bit ID field in the IP header which is split into an 11-bit edge field and a 5-bit distance field. In the algorithm for advanced marking scheme, as in the PPM, each router marks the packets probabilistically. If a router chooses to mark, each router writes, instead of just its address, the hash of its IP address in the 11-bit edge field of the IP header and sets the 5-bit distance field to zero. Otherwise, a non-marking router checks if the packet has already been marked by an upstream router. If the answer is positive, the router overwrites the edge field with the exclusive Or (XOR) of hash of its IP address with old content and increments the distance field count. Otherwise, the router just increments the distance field count. In the algorithm for advanced and authenticated marking scheme, each router in the network is assumed to share with the victim the secret key and use it for generating a message authentication code such as the hashed message authentication code (HMAC) [b-IETF RFC 2104] to authenticate the markings of a router. Each router applies the HMAC function (rather than a plain hash function) to its IP address to authenticate the validity of the markings. Thus, AAM provides strong authentication of router markings. Such authenticated marking prevents the generation of spoofed marking by any compromised router.

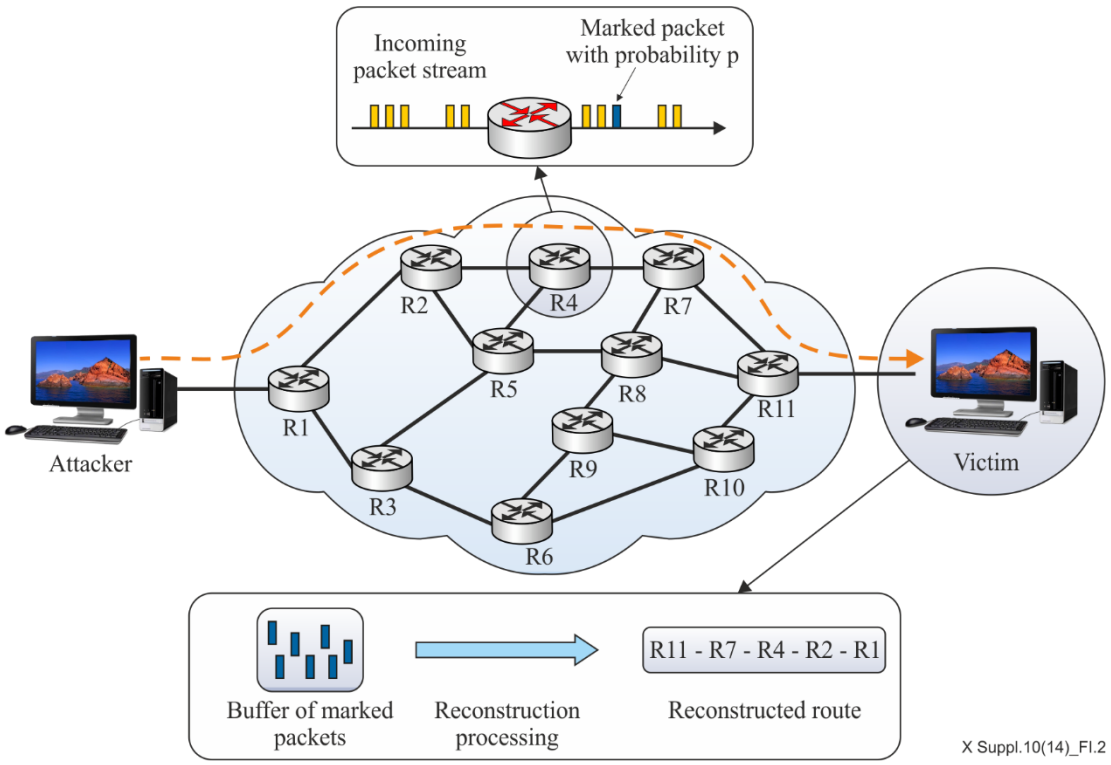

Figure I.2 – Probabilistic packet marking

I.3.4 Traceback with messaging

In the case of traceback with messaging, routers probabilistically send messages that are best described by ICMP traceback [b-Heo].

ICMP traceback: This scheme determines the full path of the attack. In case of ICMP traceback (Figure I.3), (iTrace), the router residing in the connection chain creates one ICMP packet for a certain number of packets passing through it on the way to a victim node,for example, only one ICMP packet per 20 000 packets. The ICMP packet generated is then forwarded to the victim node. All the gathered ICMP packets are used to determine the connection chain to the victim node at the destination node. The iTrace message itself consists of the next and the previous hop information and a time stamp. The iTrace message of an ICMP packet includes the traceback information such as the IP address of a router residing in the connection chain in the ICMP payload. The initial value of the time to live (TTL) field is set to 255 when creating an iTrace message. The TTL field is then used to identify the actual path of the attack.

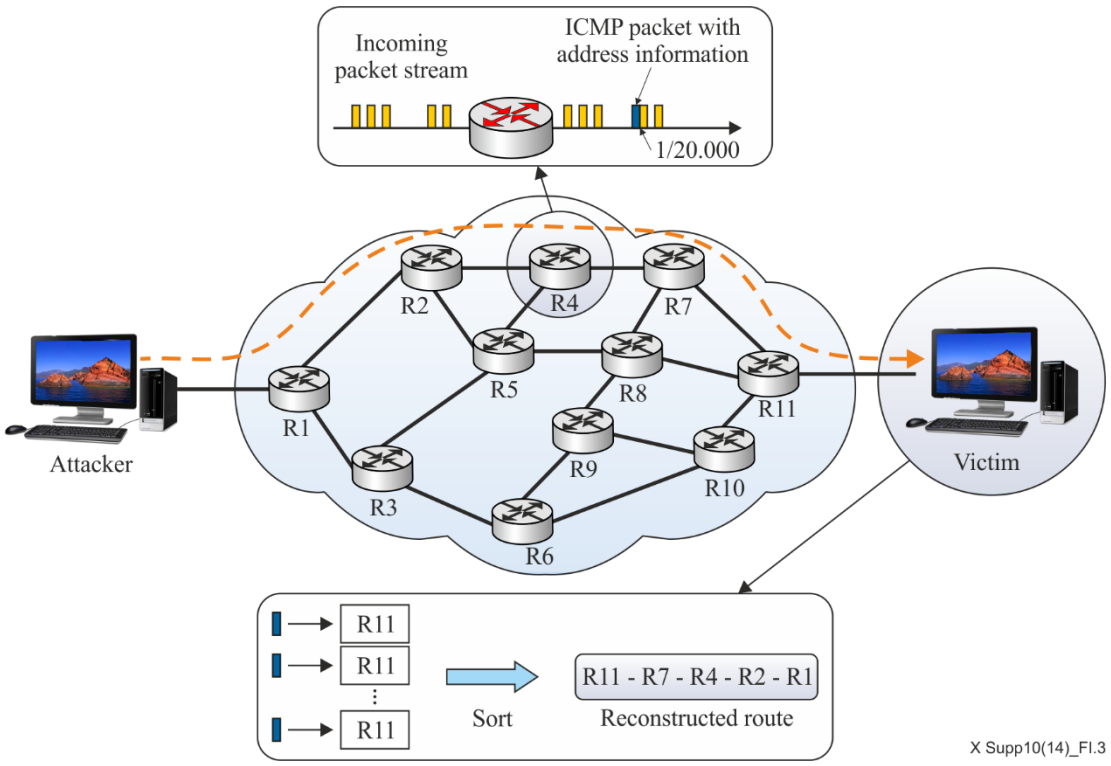

Figure I.3 – ICMP traceback

I.3.5 Traceback with packet logging

In the case of traceback with packet logging, probabilistically or deterministically categorized routers store audit logs of the forwarded packets to support tracing attack flows. Victims consult upstream routers to reconstruct the attack paths. The major schemes are described below.

IP logging: IP logging is designed to identify the true source of a particular IP packet. IP logging requires that the intermediate routers log the passage of all IP packets. To consider packet transformation, IP logging is based on the invariant portions of 20-octet IPv4 header and the first eight octets of the payload. Therefore, IP logging uses an invariant portion of the IP header. Note, however, that IP logging requires a large amount of memory to store the 28-octet packet information. In order to reduce the storage size, instead of storing the entire 28-octet packet information, hashing is done to it, followed by Bloom filter processing [b-Bloom]. By such further refinement, the scheme reduces the memory storage requirement in the router to 0.5% of link bandwidth per unit time. It also maintains privacy and prevents eavesdropping of legitimate traffic stream.

Hash-based IP traceback: This approach is introduced in [b-Snoeren-2]. The scheme is officially called source path isolation engine (SPIE). In the hash-based traceback, every router captures partial information of every packet that passes through the router to be able, in the future, to determine if that packet passed through it. In this scheme, such routers are called data generation agents (DGAs). DGA functionality is implemented on the routers. The network is logically divided into regions. In every region, SPIE collection and reduction (SCAR) agents connect to all DGAs, and they are able to query them for the necessary information. The SPIE traceback manager (STM) is a central management unit that communicates with the intrusion detection systems (IDSs) of the victims and SCAR.

As packets traverse the network, digests of the packets are stored in DGAs. In this scheme, constant fields from the IP header and the first eight octets of the payload of each packet are hashed by several hash functions to produce several digests. Digests should be stored in a space-efficient data structure called Bloom filter, which reduces storage requirements by several orders of magnitude. When the given Bloom filter is about 70 % full, it is archived for later querying and another one is used.

I.3.6 Hybrid traceback type

The hybrid type combines the packet marking type, messaging type or packet logging type. Although several types of such hybrids are logically available, only the combination of packet marking type and packet logging type are developed further for practical reasons.

Hybrid mechanisms employing packet marking and logging: A hybrid scheme was proposed to record network path information partly at routers and partially in packets [b-Gong]. This mechanism introduces the distributed link list (DLL) concept, which seeks to keep track of a subset of routers involved in forwarding a certain packet by establishing a temporary link between them in a distributed manner. DLL is based on a "store, mark and forward" approach. A fixed-size marking field is allocated in each packet. Any router that decides to mark the packet stores the current content of the marking field (written by the previous marking router) in a special data structure called the marking table maintained at the router. The router generates an ID for that packet to index its marking information in the marking table, marks the packet by overwriting the marking field by its own IP address, and then forwards the packet as usual. Any router that decides not to mark the packet just forwards it.

I.3.7 Inter-AS traceback

To construct global-scale traceback beyond AS, different administration policies and regulations among countries and organizations need to be considered. Practically, it is hard to assume that all network domains adopt and deploy a single traceback mechanism. Moreover, some ASs may wish to conceal detailed information on the traceback mechanism that is deployed. Inter-AS traceback mechanisms can be used to address these issues. Inter-AS traceback uses the communication between autonomous systems and it may allow them to implement arbitrary traceback mechanisms based on the policies. With this type of mechanism, different network operators may not implement a single traceback mechanism on all the routers provided one representative router implements the inter-AS traceback scheme; their own traceback mechanisms are implemented to conceal information on this traceback of the outside.

AS-level single packet traceback: [b-Korkmaz] combines the SPIE mechanisms and the concept of AS SPIE. The scheme utilizes the BGP attribute to understand the network topology. A victim wishing to trace the attack path back to the attack source should send inquiries to the routers implementing the traceback mechanism level by level.

Real time inter-network defence: There is a need for inter-AS communication that facilitates traceback information exchanges between different autonomous systems. A standard real time inter-network defence (RID) message format defined in both [b-ITU-T X.1580] and [b-IETF RFC 6045] can be used so that the traceback information can be exchanged on a timely basis [b-IETF RFC 6045]. A set of incident coordination messages necessary to communicate cybersecurity event, including traceback request and scenario, is described between the relevant network entities.

I.4 Comparison of traceback mechanisms

I.4.1 Strengths and weaknesses of the existing traceback mechanisms

Table I.1 describes the strengths and weaknesses of the existing traceback mechanisms in each category.

Table I.1 – Strengths and weaknesses of several traceback mechanisms

Category	Strength	Weakness
Link testing	• Compatible with existing protocols. • Easy to implement.	• Attack should last long enough for successful trace. • Can handle big flows only. • Flow characterization needed.
Packet modification	• Allows post-attack analysis. • No need for flow characterization.	• Requires modification to the existing protocols. • Can handle big flows only. • Requires upstream router map. • Unable to handle IPSec and virtual private network (VPN)
Messaging	• Compatible with the existing protocols. • Allows post-attack analysis. • No need for flow characterization. • Need for network configuration change.	• Can handle big flows only. • Public keys of router required.
Packet logging	• Compatible with the existing protocols. • Allows post-attack analysis. • No need for flow characterization. • Can trace single packet. • No network topology changes.	• Resource-intensive in terms of processing and storage requirement.

Appendix II

Comparison of traceback mechanisms based on criteria and taxonomy

This appendix describes the comparison results of the existing typical traceback mechanisms according to some of the criteria, as shown in Table II.1.

Table II.1 – Comparison of criteria according to taxonomy

Taxonomy		ISP involvement	No. of packets required	Memory requirement		Processing overhead		Ability to handle DDoS attacks	Misuse by attacker	Knowledge of network topology
				Network	Victim	Network	Victim			
Traffic monitoring	Controlled flooding	High	Large	None	None	High	None	Poor	Yes	Yes
	Input debugging	High	Large	None	None	High	None	Poor	Yes	No
Packet marking	PPM	Low	Large	None	High	High	High	Good	Yes	No
	DPM	Low	Large	None	High	High	High	Good	Yes	No
	AAM	Low	Large	None	High	High	High	Good	No	Yes
Packet messaging	iTrace	Low	Large	Low	High	High	High	Poor	Yes	No
Packet logging	Hash-based	High	1	High	None	High	None	Good	No	No
Overlay network	CenterTrack	High	1	Low	None	High	None	Good	Yes	No
Hybrid	Hybrid	High	Large	Medium	Medium	High	Low	Good	Yes	No

To summarize the comparison results, the packet marking type requires high processing overhead to the network node, but low Internet service provider (ISP) involvement. The packet messaging type requires high processing overhead to the victim node but does not require knowledge of the network topology. Packet logging has no processing requirement to the victim node but requires high ISP involvement. The overhead network type requires change of routing by the network. Therefore, an ISP administrator needs to select the appropriate traceback mechanisms taking into account its network capabilities and environments.

Bibliography

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

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

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

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

[b-IETF RFC 2104] IETF RFC 2104 (1997), *HMAC: Keyed-Hashing for Message Authentication*.

[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 3912] IETF RFC 3912 (2004), *WHOIS Protocol Specification*

[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-Belenky03] Belenky, Andrey, and Ansari, Nirwan (2003), *IP Traceback With Deterministic Packet Marking*, IEEE Communication letter, Vol. 7, No. 4, April.

[b-Belenky07] 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-Bloom] Bloom, Burton H. (1970), *Space/time trade-offs in hash coding with allowable errors*, *Communications of the ACM* 13 (7), pp.422-426.

[b-Chang] Chang, H.Y., Narayan, R., Wu, S.F., Vetter, B.M., Wang, X., Brown, M., Yuill, J.J., Sargor, C., Jou, F., and Gong, F. (1999), *Deciduous: Decentralized Source Identification for Network-based Intrusions*, 6th IFIP/IEEE International Symposium on Integrated Network Management.

[b-Gong] Gong, C., and Sarac, K. (2008), *A More Practical Approach for Single-packet IP Traceback using Packet Logging and Marking*, IEEE Trans. Parallel Distribution System, October.

[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-Heo] Heo, J., Hong, C., and Kang, M. (2007), *Lightweight IP Traceback Mechanism on IPv6 Network Environment*, Journal of the Korea Institute of Information Security and Cryptology Vol. 17, No. 2, pp. 93-102.

[b-Korkmaz] Korkmaz, T., *et al.*, (2007), *Single Packet IP Traceback in AS-level Partial Deployment Scenario*, International Journal on Securing Network.

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

[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-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.

[b-Savage] Stefan Savage, David Wetherall, Anna Karlin and Tom Anderson, (2000), *Practical Network Support for IP Traceback,* SIGCOMM'00, pp. 295-306, August.

[b-Snoeren-1] Snoeren, Alex C., Partridge, Craig, Sanchez, Luis A., Jones, Christine E., Tchakountio, Fabrice, Schwartz, Stephen T. Kent, and Strayer, W. Timothy (2002), *Single-Packet IP Traceback*, IEEE/ACM Transactions on Networking, Vol. 10, No. 6, pp. 721-734.

[b-Snoeren-2] Snoeren, A.C., Partridge, C., Sanchez, L.A., Strayer, W.T., Jones, C. D., Tchakountio, F., and Kent, S.T. (2001), *Hash-Based IP Traceback*, BBN Technical Memorandum No.1284, 7 Feb.

[b-Song] Song, D.X., and Perrig, A. (2001), *Advanced and Authenticated Marking Scheme for IP Tracebackm*, In Proc. of IEEE INFOCOM Conference.

[b-Stone] Stone, R. (2000), *Centertrack: An IP Overlay Network for Tracking DoS Floods*, Proc. of 9th USENIX Security Symposium, Denver, Colorado, August, pp. 199-212.

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