INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2005-2008

STUDY GROUP 17

TD 4068

English only

Original: English

Question(s): 6/17 Geneva, 7-18 April 2008

TEMPORARY DOCUMENT

Source: Editor

Title: Draft text of X.tb-ucr: Traceback Use Cases and requirements

This is a draft Recommendation that captures the result of discussing contributions on trace-back in April 2008 Q6/17 meeting.

The editor team for this draft consists of the following:

Tian Huirong, Richard Brackney, Gregg Schudel, Craig Schultz, and H. Y. Youm

Contributions are sought for the SG 17 September meeting to help refine the following:

1. Scope
2. Use cases
3. Focus on IP trace back or broader than layer 3.

Contact: Huirong Tian
CATR, MII
China

Tel:86-10-68094268
Fax:86-10-68034801
Email:tianhuirong@mail.ritt.com.cn

Appendix A

New work item proposal for the scenarios and requirements of IP trace-back

Abstract

In the previous September 2007 meeting of SG 17, it was said in Q6 meeting report that Q6 agreed Trace-back would be further studied within new Q6 for next SG period. To accelerate the research process of IP trace-back and attract more related contributions, we propose in this contribution to set up a new work item on it.

Discussion

In the current IP-based network, there is huge number of unwanted traffic such as DDos attacks, spams, worms and so on, and there are increasing e-crimes such as the loss of sensitive information and network fraud. And most of these attackers and criminals use spoofed IP addresses. However, as the IP network is a hop-by-hop packet forwarding network where the routers don't remain any informations of the packets forworded normally, the network itself hasn't the ability to find out the original IP address to counter these problems. At the same time, more and more important applications are carried over the IP network, and it becomes the basic requirement that the network would courage the users to use the network properly and have the ability to identify the root where the bad thing originated.

Thus, IP trace-back is the important mechanism to make users have the confidence to use their key applications over the IP network. Because it can provide the trace of the packets' source IP addresses, therefore with the deployment of IP trace-back technology, it can help to solve the problem mentioned above, such as:

- Help to fight against DDoS attacks, spams, worms and so on. For example, by tracing the DDos attack route back, the DDoS traffic could be blocked by the network router along the route.
- Provide technical supports to counter network crimes and trace back to the roots. This would deter criminals and reduce the volume of network crimes.
- Provide more reliable network environment and enhance the performance of the applications deployed over the IP traceable network.
- Others to be studied.

The discussion above shows that the IP trace-back technology is very important and need to be studied for the better traceability of the current IP network. However, the international standard which can provide a valuable guidance for the implementation of this area is still absent.

Proposal

Therefore, based on the above discussion, we think it is a proper time for ITU-T SG17 to launch the research of IP trace-back technology. And we propose to set up a new work item on the scenarios and requirements of IP trace-back.

Appendix B

Proposed a study skeleton for new work item about IP trace-back

Introduction

During SG 17 Geneva Sept. 2007 meeting, Q.6/17 has discussed the concept of Trusted IP Carrier Network and got the conclusion that further study of this concept was required. And Q.6/17 agreed that a new work item would be created based on the refinement of the proposed scope. This contribution proposes a refined scope which concentrates on IP trace-back, and makes a study skeleton for it.

Proposals

It is proposed that Q.6/17 uses the skeleton in the following appendix as the study baseline of the new work item we proposed.

Appendix C

Scenarios and requirements of IP trace-back

1 Scope

This document defines the scenarios and requirements of IP trace-back mechanism.

2 References

The following ITU-T Recommendations and other references contain provisions, which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published.

[TBD]

3 Definitions

<Contributor's note: Check in ITU-T Terms and definitions database under http://www.itu.int/sancho/index.html to make sure the term is not already defined in other recommendations. It could be more consistent to refer to such a definition rather than redefine it>

IP trace-back: to find out the origin of one or more IP packets.

4 Abbreviations and acronyms

<Include all abbreviations used in this Recommendation>

5 Conventions

<Describe any particular notation, style, presentation, etc. used within the Recommendation, if any>

6 Overview

IP trace-back is a name given to any method for reliably determining the origin of a packet on the Cyberspace. It is a critical ability for identifying sources of IP packets and instituting protection measures for the IP network.

However some natures of the IP network makes it difficult to realize this ablility. Firstly, IP network is a "dump network, smart end-system" network. It simplifies the core network transport functions and makes it focus on packets forwarding. Therefore, the routers in the IP network don't remain any packets forwording informations which are needed by packet tracing. Secondly, the lack of source IP address checking makes it easier than it should be for the attackers to spoof source addresses in the IP network. The trace-back problem is complicated because of these spoofed packets. Thirdly, there are numerious dymamic IP address and NAT widely used in the IP network. It becomes more serious now to find out the real sources of the IP packets in these two cases.

Moreover, IP network consists with massive networks which may belong to different carriers. Carrying out the trace-back mechenism across diverse networks will be a difficult task.

This document develops some use cases and requirements for the IP trace-back mechanism, and all of these obstacles mentioned above will be considered throughout this document.

Objectives

This clause describes the ultimate goal of IP trace-back. The focus is what should be achieved rather than identifying practical implementation steps.

<Contributor's note: following items are just for example, more materials and discussions are needed in the future.>

The objectives for IP trace-back:

- Any type of IP packets (including spoofed IP) can be traced backward to its origin.
- In order to ensure traceability, essential information of the originator should be logged by network.

Scenarios

This clause describes several application scenarios addressed by some requirements of this document.

<Contributor's note: following items are just for example, more materials and discussions are needed in the future.>

Most existing approaches to IP trace-back have been tailored toward DoS attack detection. Actually, there are many other application scenarios of IP trace-back. Different scenarios will face different network environments, and have different specific methods.

- Trace-back of malicious IP packets(e.g. DDOS attack)
- Trace-back for normal IP packets
- Trace-back of IP packets with dynamic address
- Trace-back of spoofed IP packets
- Trace-back across different management domains
- …

8.1 Trace-back of normal IP packets

8.2 Trace-back for malicious IP packets

8.3 Trace-back of IP packets with dynamic address

8.4 Trace-back of spoofed IP packets

8.5 Trace-back across different management domains

Requirements

This section specifies requirements of IP trace-back in terms of general and functional requirements.

<Contributor's note: following items are just for example, more materials and discussions are needed in the future.>

9.1 General Requirements:

- IP trace-back mechanism is required to be adapted to various network environments, such as different addressing (IPv4 and IPv6), different access methods (wire and wireless) and different access technologies (ADSL, cable, Ethernet) and etc.
- IP trace-back mechanism is recommended to take into account the influence/impact on performance, quality of service, usability, scalability and cost constraints on deployment of IP network.
- IP trace-back mechanism is recommended to be feasible over current and future IP network.
  - A good IP trace-back mechanism shouldn't make too many changes to the existing equipments and protocols.
  - A feasible IP trace-back mechanism should be able to be carried out with small amount of samples (e.g. IP packets) even with a single one.
  - …
- IP trace-back mechanism is required to be able to deal with the complex network topologies, for example, network with NAT or dynamic IP address assigning.
- Implementation of IP trace-back should not bring new security threats to the IP network.
- …

9.2 Functional Requirements

Edge network

- …

Core network