Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79. This document may not be modified, and derivative works of it may not be created, and it may not be published except as an Internet-Draft.

This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html
Abstract

This memo reports a field trial of Inter-Domain Traceback Operation in Japan as a proof of concept on IP packet traceback. This field trial was carried out with 15 commercial ISPs and one traceback control center which was a mediator among participated ISPs.

Table of Contents

1. Introduction................................................3
2. Operational Models and Configurations.......................3
   2.1. Operational and Legal Requirements for Traceback Systems.3
   2.2. The Operational Model in this field trial.............5
   2.3. The configurations of this field trial...............13
      2.3.1. Participates......................................13
      2.3.2. Traceback systems................................13
3. The summary of the experiments............................14
   3.1. System Performance....................................15
   3.2. Validation of management system, and operational efficiency16
   3.3. System Adaptability....................................18
4. Security Considerations.....................................19
5. IANA Considerations..........................................19
6. Summary........................................................19
7. References....................................................20
   7.1. Normative References..................................20
   7.2. Informative References................................20
8. Acknowledgments..............................................21
1. Introduction

We had a field trial of inter-domain IP traceback operation with fifteen ISPs in Japan with their real network environments, from May to the end of August in 2009. In this memo, we briefly report this field trial. The details of the evaluation results have been reported in [Wakasa2010].

2. Operational Models and Configurations

While formulating an operation model of an inter-domain traceback, we identified following 5 assumptions;

1) Establish a traceback control facility.

2) Collect traceback data at all times.

3) Operational costs are treated as something to be resolved separately.

4) Legal charges are not expected to be initiated by the control facility.

5) With respect to judging whether or not there is an attack, we expect that judgment criteria will be created separately.

According to these assumptions, we designed traceback systems and the operational model.

2.1. Operational and Legal Requirements for Traceback Systems

According to our survey of commercial ISPs regarding their legal requirements, to operate in a legitimate manner an automatic traceback is allowed to trace only packets necessary for an incident response. Also, the requirements for implementing lawful traceback have been identified through investigation of various countries’ related laws, and from the results of a survey of Japanese ISP’s opinions, these are summarized as follows;

(1) No destruction of data for communications, etc.

Traceback systems should have affinity for all kinds of packets. Also, the deployment of a traceback system must not destruct some kind of communication, cause an excessive increase in traffic or cause damage to network equipment.
(2) Guaranteeing privacy of communications

To guarantee privacy of communications, acquired information for tracing, such as an IP header or payload information must be converted into hash values, with only those hash values to be recorded or exchanged.

(3) Access restricted to only those conducting traces

Authentication must be carried out to ensure that the data acquired for the purpose of tracking cannot be accessed by individuals other than those responsible for conducting traces.

(4) Restriction of usages

Traceback system should be used as a supportive tool for incident responses. As an incident response such as a DDoS attack, acts in pursuit of lawful business must be applied, and a traceback implemented.

(5) Protection of traceback data prior to the outbreak of an incident

Access to the traceback data acquired in advance for the purpose of tracking must be restricted until the outbreak of a specific incident.

(6) Obligation of confidentiality in the shared use of data

The shared use of the traceback data acquired for the purpose of tracking must be limited to only those ISPs involved in the coordination process.

(7) Information disclosure through appropriate methods

Details that can be disclosed from among the results of traceback must be disclosed through the appropriate methods.

(8) Obligation of confidentiality for those conducting traces

Those conducting traces must accept obligations of confidentiality with regard to the data acquired as a result of traces.
(9) Development and application of security and privacy policies

The security policies and privacy policies of each ISP must be developed and applied.

The details of these operational and legal requirements are written in [Wakasa2009].

2.2. The Operational Model in this field trial

To satisfy these requirements, the process of carrying out traceback is divided into automatic traceback phase and incident response phase, shown in Figure 1 and Figure 2. In the automatic traceback phase, an inter-domain traceback is carried out by traceback systems in second order. On the other hand, in the incident response phase, the operators of related ASs carry out an inter-domain traceback as a part of an incident response in ten-minutes order.

The automatic traceback is composed of four components as follows;

(i) Attack detection

An Intrusion Detection System (IDS) is installed to detect attack packets as shown in Figure 2. As described in Figure 2, Traceback Client (TC) converts an alert from IDS to a traceback request message. Each request message contains hash values of attack packets up to 60 entries. Due to the legal requirement (2), the packet information on a request message must be the hash value of an issued packet. The hash encoding method in the field trial was reported in [Kai2009].

(ii) Traceback System (TB System) to record AS communication packets

The TB systems in Figure 2 are based on hash-based traceback scheme reported in [Kai2009]. Each TB system generates hash values based on the header portion of packets that pass through the boundaries linking ASs with other ASs, and temporarily stores these hash values in memory.

(iii) Controller to identify the passage of attack packets

To exchange traceback information among ASs, we employed InterTrack [InterTrack] as the controller component of the
automatic tracing. When the passage of an attack packet has been
confirmed, the ITM (Inter-domain Traceback Manager) requests
execution of a traceback recursively to an adjacent AS ITM, and
posts the traceback results to the database (TB event Database in
Figure 1.).

An end-to-end traceback result is summarized as full or partial
AS path(s) from source AS to Destination AS(s) and the status of
each AS. The variations of the status of an AS in this field
trial were follows;

``Destination’’ :

The AS would be the destination of issued packets. Actually,
the issued packets were recorded in TB systems as the incoming
direction to the AS.

``Source’’ :

The AS would be the source of issued packets. Actually, the
issued packets were recorded in TB systems as the outgoing
direction from the AS.

``Transit’’ :

The AS would be located in the forwarding AS path of the
issued packets. Actually, the issued packets were recorded in
TB systems as both the incoming direction and outgoing
direction on the AS.

``Translated’’ :

Some translation of the issued packets would be occurred in
the AS. In this field trial, ‘’Translated’’ AS was the
reflection point of a DNS reflection attack. Actually,
‘’Translated’’ status was given when the traceback system for
DNS reflection attacks returned hash value(s) of a DNS request
packet which were paired with the hash value of the issued DNS
reply packet.

``Unknown’’ :

In this status, the issued packets were recorded on TB systems,
but, TB systems did not distinguish any direction of the
issued packets.

``Not Found’’:
TB systems did not have any records about the issued packets.

The message forwarding strategy of an ITM on the field trial was as follows: The ITM on the current AS forwards a request message to only upstream adjacent ASs if the TB system on the current AS distinguishes the AS status except for ‘’Unknown’’ and ‘’Not Found’’. When the TB system returns ‘’Unknown’’ or ‘’Not Found’’ status, the ITM executes a flooding routine, that is, the ITM on the current AS forwards the request message to all adjacent ASs except for the AS which forwarded the request message to the current AS. Each request message has a unique identifier. If an ITM receives a duplicated request message by the flooding routine on other ASs, the ITM stops forwarding the request message, and returns a reply message as ‘’reached’’. Also, a request message has ‘’Time To Live’’ field, whose value is decreased along with traversed AS hops. If the value of ‘’Time To Live’’ reaches to zero, an ITM stops further forwardings.

(iv) Database to store traceback results

End-to-end traceback results are managed in a database (TB event Database in Figure 1). This database can be available by AS operators through a trouble ticket system on the control facility (TB control center). The TB control center is a mediator of the incident response among ASs, managing the TB event Database and the TB trouble ticket system, and playing the role of an agent to notify incidents and response results to the related ASs.
Figure 1 The Operation Model in the field trial.
In the automatic traceback phase, the trigger of an inter-domain automatic traceback is an alert from the IDS on the victim AS or the victim customer. From the alert, the Traceback Client (TC) generates a request message and submits the request message to the ITM on the victim AS. The inter-domain automatic traceback of a submitted request is carried out according to the procedure drawn in Figure 3.
If some application layer traceback system is installed in related ASs, the automatic traceback will be carried out along with the procedure in Figure 4. An application traceback system replies the translated information of a packet, for example, the reflection by a DNS query, the address transition by NAT or NAPT, etc.. The application traceback system also replies a hash value of the pre-translated packet.
Figure 4 Flow chart of an automatic tracing with an application traceback
In the incident response phase, damage reports are submitted from the operator of victim AS to the TB trouble ticket system on the TB control center, and a request to confirm the circumstances of the attack will submitted to the AS from which the attack originated through the trouble ticket system. According to the opened ticket, the TB Control Center mediates between the ‘‘Source’’ AS and ‘‘Destination’’ AS. If the issued traceback result does not contain ‘‘Source’’ AS, the TB Control Center contacts to other related ASs such as ‘‘Transit’’ ASs. The flow chart of the incident response phase is show in Figure 5.

```
```

Figure 5  Flow chart of an incident handling
2.3. The configurations of this field trial

In this section, we describe the configurations of this field trial.

2.3.1. Participates

With the cooperation of fifteen ISPs and three research centers, we conducted this field trial. The fifteen ISPs were located in different prefecture across Japan: Hokkaido, Tohoku, Hokuriku, Kanto, Kansai, Chugoku, Shikoku, Kyusyu, and Okinawa. The EventDB and the ticket system were hosted in another data center. The TB control center was located in Tokyo. The three research centers participated as customers.

2.3.2. Traceback systems

At each ISP we installed one controller device, multiple probes, one PC for accessing the database and one attack simulation server. In total, we placed 35 probes in ISPs environments. The number of probes in each ISP was between one and four, and included the environment at the AS borders of each AS on IPv4 networks.

A controller device contained an ITM daemon of InterTrack [InterTrack] and a TB probe manager daemon [Kai2009]. ITM daemons and TB probe manager daemons exchanged traceback information in several XML messages. The XML messages were defined in InterTrackMessage.xsd [InterTrackSource]. A TB probe manager daemon and TB probes exchanged traceback information in an original protocol.

The TB probes were an enhanced hash-based IP traceback system [Kai2009], and an application layer traceback system to cover DNS reflection attack scenarios. One of enhanced hash-based IP traceback probes was hardware based probe catching up with 10 Gbps Ethernet. Others were software based probes which can make hash values of packets upto 300 Mbps.

To keep anonymity of each packet, the packet information was hash values of packets. The hash function we employed was an enhanced bloom filter described in [Kai2009]. A hash table on each TB probe was refreshed in 4.0 seconds interval. The false positive rate was 0.083 in 20 bit-length hash values on 890 Mbps traffic as a measured
The false positive rate can be reduced by employing more longer hash values, for example, the false positive rate was 0.00000578 in 26 bit-length hash values on 445 Mbps traffic as a measured value.

Each attack simulation server had TC daemon of InterTrack [InterTrack], Snort IDS daemon [Snort], simulative attack tools based on libnet [libnet]. The attack simulation servers were used either a victim host or an attacker host. The TC on each attack simulation server requested with 20 bit length hash values of 60 different packets in every 2 seconds, if the Snort captured attack packets. This request interval was derived from the performance of the EventDB server. In DNS reflection attack scenarios, a bind 9 daemon and an application traceback daemon ran on the attack simulation servers.

The controller, TB probes and the attack simulation server in each ISP were inter-connected on an isolated layer 2 network. All controllers and EventDB established TCP connections over another VPN.

We tested several variations of the peering topology among ITMs: a cascade topology, a full-mesh topology, a partial-mesh topology along with the BGP peering topology. The message forwarding strategy was a hybrid strategy. On the hybrid strategy, an ITM forwards a request to only upstream neighbors when the TB system distinguished the upstream neighbors, in other cases, the ITM floods requests to all neighbors except for the issuer neighbor.

To cover the communication overhead through the trouble ticket system, a live chat system was settled in the TB control center. We applied an access control rule to the live chat system as same as that of the TB trouble ticket system. Through the live chat system, operators actively confirm the current status of an incident response.

3. The summary of the experiments

Here, we report the summary of the experiments on this field trial. The field trial was carried out from May to the end of August in 2010. Totally, we had 13 times of demonstration experiments of incident responses with traceback along with 9 attack scenarios. The details of the experiments are described in [Wakasa2010].
3.1. System Performance

Results of the field trial confirmed the performance of the traceback system, including information about processing time and fault detection rates that can be expected in the real Internet environment of fifteen ISPs. We used 20 bit-length hash values. With more ISPs and larger scale Internet environment, the performance of the traceback system would still be only a few seconds of processing time, and the detection failure rate under 1 %. The reasons of detection failure were, i) the recording loss caused by high traffic load on an ISP where a software-based TB system was deployed, ii) the issued packets were forwarded through an AS border where a TB system was not deployed due to the limitation of the facility of an ISP.

Here, we summarize the processing time for each automatic tracing. In the full mesh topology among ITMs, all automatic traceback trials were completed in less than 1 second. Also, we measured such round trip time of an automatic traceback trial in the 13 hops cascade topology. In the cascade topology, most automatic traceback trials were finished in 3 seconds, the maximum was 4 seconds.

Also, we measured the time spent for an incident response, that is, the actual consumed time for the flow chart of Figure 5. We had 13 demonstration experiments of the traceback operation along with 9 attack scenarios, which included a single simulated DoS attack, multiple simulated DDoS attacks, a simulated DNS reflection attack, actual attacks reported by a honeypot system, and so on. The details of attack scenarios were described in [Wakasa2010]. The average time to spend an incident handling, from receiving a damage report of a customer to the closing of the ticket, was about 40 minutes, the minimum was 11 minutes, the maximum was about 1 hour.

The demonstration experiments in the field trial identified the following three issues about traceback systems:

i) How to cooperate with different traceback systems?

We tried to cooperate between traceback systems with slightly different technologies, but failed to trace simulated attacks because of differences in system parameters, operational rules, and network environments. In future, we should consider what is necessary to achieve automatic cooperation among multiple traceback groups, or cooperation among traceback systems based on different technologies.
ii) How to decide the best values of system parameters?

The best values of following many parameters must be agreed for each traceback system:

a) Type of topology and mode of traceback request transmission in InterTrack.

b) Hash parameters in the probe, and where to install each software probe or hardware probe in the ISP environment.

c) Upper limit of fault detection rate and packet loss rate.

d) Transmission rate to send the traceback request.

We should analyze the relationship among each parameter to be able to make the best decision about the target network environments.

iii) How to design the topology of InterTrack.

Because there were very few adjacent ASs among the fifteen ISPs participating in the demonstration experiments, we designed the topology of InterTrack as connecting each ISP completely, and the traceback requests were sent to all other ISP as same as broadcast. We should design future traceback systems so ISPs are independently able to update InterTrack and other parameters, this may achieve fairness, greater efficiency and widespread adoption of traceback systems.

3.2. Validation of management system, and operational efficiency

We examined traceback operation considering the following two factors. The first factor is the validation of the management system, which is required to follow legal requirements. The second factor is the efficiency of traceback operation from view point of ISPs operators.

i) Validation of management system

The management system for the demonstration experiments was required to have many check points for each process to satisfy
legal requirements, and the traceback operation is controlled on a step-by-step basis, traceback operators are required to record every operation on a check sheet. We analyzed the operational records from the viewpoint of following factors, and confirmed the validation of the management system.

a) Only few complex operational processes spent too much time and negatively impacted some experiments.

b) Even during exception handling, there were only a few instances when operational time increased for both the victim and attack ISP.

c) Operation time increased only occasionally when incidents occurred.

d) The time taken for operations in all situations was consistent across all the participating ISPs.

ii) Operation efficiency from view point of ISPs operators

Operators need to be aware that they may need to stop current operations and quickly switch attention to a higher priority incident. Some operators found it difficult to make the right decision in such situations because of lack of experience or skills. The traceback operation must provide support for such situations.

We analyzed the operation record from the view point of following factors, and confirmed the operational efficiency from view point of ISPs operators.

a) Our results showed that operation time was consistent among ISPs.

b) Among different experiments, operation time was exceeded when an ISP requested many operations simultaneously.

c) When high priority incident occurred, an ISP stopped the traceback operation. After the incident finished, the operator
was successfully able to continue the traceback operation after restart.

d) The traceback control center sent almost 60 messages to each ISP for help during the experiments, and ISPs reacted to these messages on and average of 20 occasions

3.3. System Adaptability

In a large-scale environment, it is not possible to avoid many types of incomplete situation when conducting a trace. In the demonstration experiments the following examples of incomplete situations were recognized.

i) The traceback operation was stopped by a higher priority incident.

ii) Experiments to cooperate with other traceback systems were conducted without detailed prior discussion.

iii) Could not install probes to all links of some ISPs.

iv) Could not make hash completely in probes at some ISPs because of the too much traffic.

v) Could not send traceback requests over 60 times in a 2 second period because of system restrictions.

vi) Could not install the traceback system to all ISPs.

The traceback system and operation were able to adapt to these incomplete situations to some extent. About issue i), prior training of ISPs operators and good operation procedures, documentation and check sheets were found to be good solutions. About issues iv) and v), the new search engine has provided a solution, searching multiple hash values with one click. About issues iii) and vi), general improvements to the traceback operation provide a solution.
4. Security Considerations

When the widely adaption of the inter-domain traceback or the standardization of the inter-domain traceback, we should consider the following items;

(i) The traceability of the inter-domain messaging
(ii) Authentication and Authorization among ITMs
(iii) Encryption of the communication channel among ITMs
(iv) Policy enforcement scheme
(v) Abuse of the inter-domain traceback

This memo is just an informational draft to report the result of a field trial of an inter-domain traceback operation. The discussion of each security issue is out of scope on this memo.

5. IANA Considerations

This document does not require any IANA action.

6. Summary

In this memo, we introduced the results of a field trial of an inter-domain packet traceback operation conducted with fifteen ISPs in Japan in 2009 using simulated and real attacks.

Through the results of this field trial we have gained a great deal of knowledge about following three factors. i) traceback system performance. ii) traceback operational efficiency and the management system’s validation. iii) traceback system’s adaptability against incomplete situations. And we have been able to begin to identify issue that will help to achieve widespread adaption.

When the traceback system achieves widespread adoption, a larger scale traceback control center and more efficient management system will be required. When the traceback system achieves widespread adoption in a real network environment, 24 hours/7days operation will be necessary, and updates of the management system would be required. For the operational efficiency, problems with the traceback system or mistakes by operators should be minimized by steady efforts on a day-by-day basis. Strengthen of monitoring and redundancies of the traceback system and promoting automatic operation will be necessary.
We should find a solution to tracing attacks with large scale ISPs in Japan and overseas. To install the traceback system into larger ISPs we must resolve the problems of cost. Because overseas ISPs would very likely install different types of traceback system, we must resolve how to cooperate with different technical and operational systems. Practically we must resolve how to trace attacks where few ISPs have installed the same traceback system, and many other ISPs have not installed any traceback system.

7. References

7.1. Normative References

7.2. Informative References

[Snoren2001]

[Wakasa2009]

[Wakasa2010]

[Hazeyama2006]

[Kai2009]
8. Acknowledgments

This research is a part of "Research and Development into Traceback technology on the Internet" sponsored by the National Institute of Information and Communications Technology since Fiscal 2005. Finally, we would like to express our deep gratitude to many ISPs and research centers that provide active cooperation with our field trial.

This document was prepared using 2-Word-v2.0.template.dot.
Authors’ Addresses

Hiroaki Hazeyama
Nara Institute of Science and Technology
Takayama 8916-5, Ikoma, Nara, Japan
Phone: +81-743-72-5216
Email: hiroa-ha@is.naist.jp

Ken Wakasa
Japan Data Communication Association
Minato-ku, Tokyo, Japan
Phone:
Email: secretariat@telecom-isac.jp

Keisuke Takemori
KDDI R&D Laboratories
Fujimino-city, Saitama, Japan
Phone:
Email: takemori@kddilabs.jp