第 XIV 部

IP トレースバック・システムの研究開発

第 14 部
IP トレースバック・システムの研究開発

第 1 章　はじめに

2005 年度における traceback ワーキンググループの活動の報告を述べる。本ワーキンググループは、IP トレースバック技術全般の研究を取り扱うワーキンググループである。IP トレースバックとは、パケットの通過した経路を特定する技術で、さまざまな方式や実装が存在し、不正アクセスへの対策手法として実用化が進んでいる。一方、種々の IP トレースバックシステムを相互接続し、インターネット上で横断的な IP トレースバックを実現するための運用アーキテクチャが必要とされている。

第 2 章　2005 年度の活動内容

2005 年度においては、各種 IP トレースバックシステムが連携して、インターネット上で横断的な IP トレースバックを実現するために必要なアーキテクチャの議論を行った。種々の既存提案などの調査や議論を行った結果、インターネット上で IP トレースバック実現するアーキテクチャである「Intertrack」を提案した。Intertrack は、異なる運用組織単位において、各種 IP トレースバックシステムの相互接続するしくみを提供し、かつ、これらの IP トレースバックシステムを効率よく運用することで、インターネット全体での IP トレースバックを実現する。Intertrack の概要や概念については、次章において、まとめる。

第 3 章　InterTrack: A federation of IP traceback systems across borders of network operation domains

On an attack tracking across ASes, the operational cost on the transfer of the tracking information to other network domains, the misuses of traceback systems to steal sensitive information or to comsume resources on ASes, and the risks of depending on a specific traceback technique are issued. To solve these issues, we propose InterTrack, an autonomous architecture for tracking attacks across borders of ASes and for providing a foundation to combine detection, traceback and protection (Fig. 3.1).

InterTrack runs a preliminary investigation of an attack path across Autonomous Systems (ASes) to find attack-source ASes, while at the same time concealing sensitive information of each AS. In parallel with the preliminary investigation, InterTrack can run a deep inspection on each suspected AS for detecting attacker. InterTrack can also trace an attack even if the attack come across different address spaces through some address translators (e.g. a NAT router or a 6to4 tunnel).

Such parallel investigations are brought by three characteristics of InterTrack: the separated tracking stages along with routing domains, the independence of the inside tracking from each other network domain, and the interconnections between different traceback systems through several messages which contain the tracking information. Due to these three characteristics, each tracking stage not only can employ different traceback systems according to their properties, but also can replace its traceback technique to another feasible one regardless of other stages or other domains. Furthermore, these three characteristics

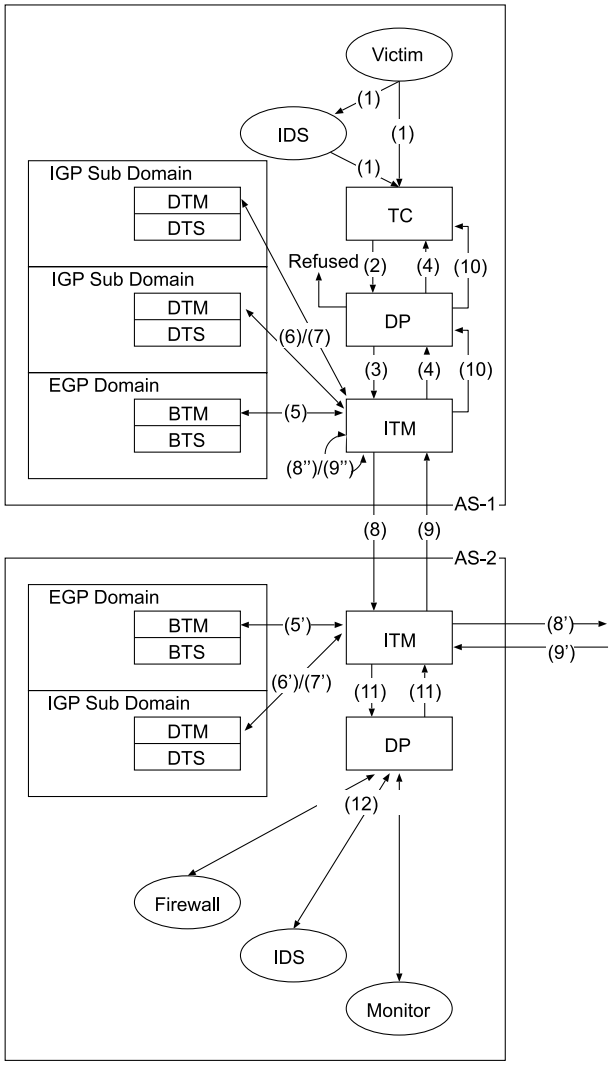

Fig. 3.1. Procedures of an attack tracking on InterTrack

allow each network domain to apply its own operational policy to each attack tracking request.

Because InterTrack can cooperate with detection systems and protection systems shown as Fig. 3.1, we predict that InterTrack will expedite the recent attack tracking and protecting in practice, and will become a deterrent against network attacks.

3.1 Attack Tracking on InterTrack

An attack tracking on InterTrack is composed of four stages: *the tracking initiation stage*, *the border tracking stage*, *the intra-AS tracking stage* and *the inter-AS tracking stage*. The tracking initiation stage is for access control and for making decisions to trace attacks along with operational policies. The Border tracking stage and the inter-AS tracking stage are for a preliminary investigation of an attack across ASes. In the intra-AS tracking stage, InterTrack seeks more detailed attack paths or detects attacker nodes.

The InterTrack architecture is constructed of these components as follows; Inter-domain Tracking Manager (ITM), Tracking Client (TC), Decision Point (DP), Border Tracking Manager (BTM), Border Tracking System (BTS), Domain Tracking Manager (DTM) and Domain Tracking System (DTS). Fig. 3.1 shows the procedures of tracking on InterTrack.

ITM is a mediator of attack tracking on each AS, and a coordinator of each AS on the inter-AS tracking stage. TC is an interface between InterTrack and detection systems. In the tracking initiation stage, DP controls accesses from detection systems through TCs, protection systems and InterTrack, and ITM decides whether or not ITM starts tracing along with operational policies or situations. In the border tracking stage, BTM traces attacks by running a BTS on EGP domain for preliminary investigation on each AS and for collecting evidences to decide next actions. DTM is a manager of an IGP sub-domain on an AS. In the intra-AS tracking stage, a DTM inspects an IGP sub-domain network by a DTS for detecting and isolating attacker nodes. BTS is a traceback system specified to grasp the state of an AS and upstream neighbor ASes on an attack path. On the other and, DTS is a traceback system for detecting a detail attack path or investigating the true IP/MAC address of an attacker node. Because the border tracking and intra-AS tracking on an AS are independent from those of other ASes, both BTS and DTS can be replaced to another feasible traceback system by each AS regardless of traceback techniques on other network domains.

3.1.1 Tracking Initiation Stage

First, on behalf of a victim node, a network operator or a detection system such as IDS inputs the headers and the payload of an issued attack into a TC (Fig. 3.1(1)).

Second, the TC tries to connect to a DP on the AS and to send a tracking request with the frame dump (Fig. 3.1(2)). When a DP receives a connection request from a TC, the DP authenticates the TC, establishes a session with the TC, and forwards the tracking request to the paired ITM with a time stamp (Fig. 3.1(3)). If the DP cannot process the authentication of the TC, then, the DP refuses the connection between the TC. Also a DP controls the interval of tracking requests from TCs because an attack tracking over the Internet consumes several resources on each AS. Through the access control by DPs, InterTrack can prevent ASes from misuses of traceback systems: steeling topologies or consuming resources by numerous continuous requests, for example.

Third, when an ITM receives a tracking request from the paired DP, the ITM assigns a tracking ID to the tracking request. The ITM forwards the tracking ID to the TC through the paired DP (Fig. 3.1(4)), and starts tracking the issued attack.

3.1.2 Border Tracking Stage

After the tracking initiation stage, the ITM asks the paired BTM to examine the state of AS for the attack and to get evidences for deciding next actions (Fig. 3.1(5)). When a BTM receives a tracking request from the paired ITM, the BTM picks up parameters from the tracking request, inputs these parameters into a BTS and runs the BTS to track the attack on borders of EGP domain on an AS.

By running a BTS, a BTM examines the state of the AS about the issued attack. The variations of the state of an AS are shown in Fig. 3.2. Each variation is as follows;

- *Refused*: an AS refuses to follow the attack tracking because of an operational policy (Fig. 3.2(a)).
- *Unknown*: an AS is in unknown condition due to the lack of a tracking method or some troubles (Fig. 3.2(b)).
- *Busy*: an AS is busy because of treating other tracking requests (Fig. 3.2(c)).
- *Wait*: an AS is now tracking but needs much more time to get a tracking result (Fig. 3.2(d)).
- *Not Found*: an AS is not included in the attack path (Fig. 3.2(e)).
- *Attacker*: an AS has one or more attacker nodes inside the AS (Fig. 3.2(f)).
- *Infected*: an AS receives the attack from one or more attacker nodes inside the AS (Fig. 3.2(g)).

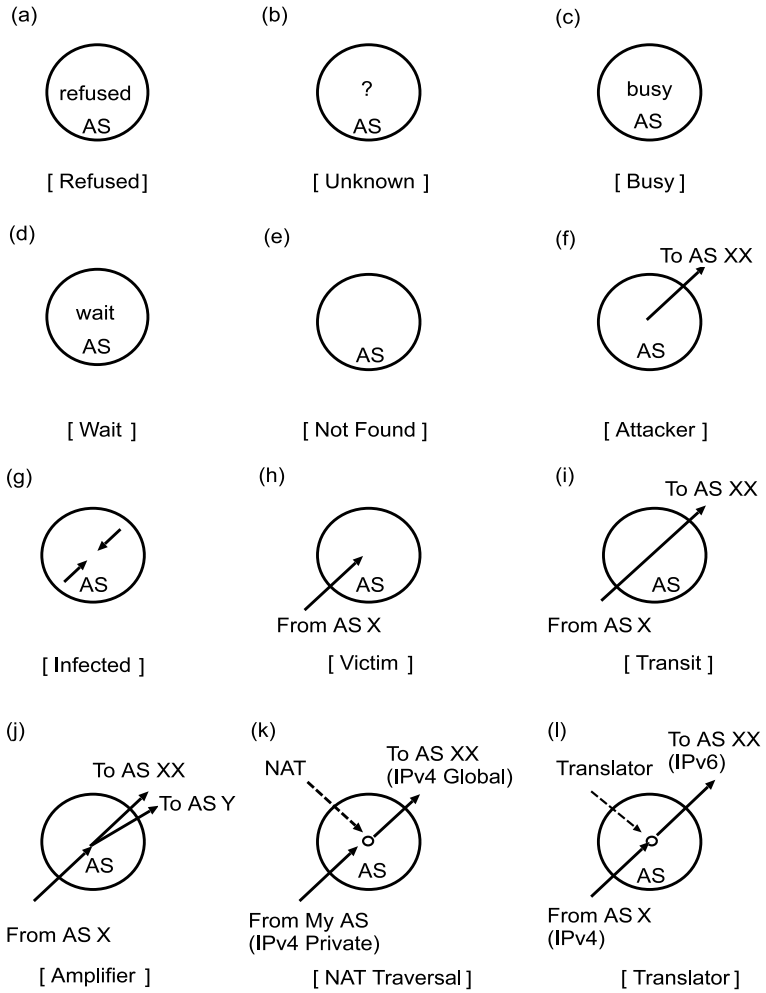

Fig. 3.2. Variations of state of an AS on an attack

- *Victim*: an AS is just the victim of the attack (Fig. 3.2(h)).
- *Transit*: an AS just forwards the attack (Fig. 3.2(i)).
- *Amplifier*: an AS not only forwards the attack but also amplifies the attack by one or more attacker nodes inside the AS (Fig. 3.2(j)).
- *NAT Traversal*: an AS forwards the attack from a private network used inside the AS (Fig. 3.2(k)).
- *Translator*: an AS forwards the attack through a translator such as 4to6 tunnel (Fig. 3.2(l)).

From (a) to (d) in Fig. 3.2 are error status, therefore, the ITM replies an error message to the issuer ITM or the paired DP.

(e) to (h) in Fig. 3.2 are basic state. If the state of the AS is *Not Found*, the ITM notifies the issuer about the tracking result (Fig. 3.1(9)). When BTM replies *Attacker* state, the ITM sends a reply message to the issuer for notifying that the attack is raised from this AS. In *Attacker* state, the ITM also transitions into an intra-AS tracking stage, that is, it queries DTMs on each sub-domain of the AS to examine details of the attack in parallel. *Infected* state shows that the victim on the AS is attacked by the attacker nodes inside the same AS. In this state, the ITM starts intra-AS tracking. The ITM starts an inter-AS tracking, and forwards the tracking request with its ID to ITMs on suspicious neighbor ASes when the result of border tracking is *Victim*.

From (i) to (l) of Fig. 3.2 are state about some

transit AS for an attack flow. *Transit* is the case where an AS simply forwards attack packets which came from another AS. In *Amplifier* case, an AS not only forwards attack packets from another AS but also sends attack packets generated by attacker nodes inside its own network. In these two cases, the ITM forwards the tracking request to each ITM on each suspicious neighbor AS. Also, the ITM runs an intra-AS tracking when the ITM is in the *Amplifier* state.

(k) and (l) of Fig. 3.2 are the cases where the attack comes through an address translator. *NAT Traversal* state shows an AS forwards an attack which comes through a NAT router in a private network managed by the AS. In the *Translator* case, an AS translates the address spaces of the attack packets by a 4to6/6to4 tunnel on the AS. In these address translation cases, the ITM adds the information about the address translation reported by the BTM into the tracking request, transitions its managing address space to another one, and starts the border tracking on the another address space (Fig. 3.1(8″) and (9″)).

3.1.3 Inter-AS Tracking Stage

An inter-AS tracking is a recursive border tracking on each AS included in an attack path. When an ITM receives a request to follow an inter-AS tracking from a neighbor ITM, the ITM runs border tracking and decides next actions. If the border tracking result shows some of the incoming cases (Fig. 3.2(h)–(l)), the ITM forwards the tracking request with its ID. The recursive forwarding of the tracking request across ASes is continued by ITMs on the attack path until the tracking request arrived in the *Attacker* state AS or an AS reports one of error state (Fig. 3.1(8), (8′) and (8″)). On replying the tracking request, each ITM generates a reply message with its state shown in Fig. 3.2, puts the reply message with the results from neighbors into a reverse AS path, prunes the reverse AS path along with the operational policy on each AS, and replies the pruned reverse AS path to the issuing neighbor (Fig. 3.1(9), (9′), (9″)).

A forwarded tracking request message includes the ITM path which contains each ITM's ID on the forwarding path like the path record of BGP. Therefore, if a loop occurs, each ITM can recognize the loop by the ITM path record on the tracking request message. When a loop happens, the ITM discards the tracking request. After some time period has been spent and a time out occurs, the issuer ITM judges that the neighbor ITM discarded the tracking request or some trouble happened. Also, a tracking request message contains a value of Time-To-Live (TTL) field that can prevent endless loops.

When the original issuer ITM receives reply messages from all of issued neighbor ITMs, merge the inter-AS tracking result with the result of an intra-AS tracking on its own AS, and replies the tracking result to the issuing TC through the paired DP (Fig. 3.1(10)).

3.1.4 Intra-AS Tracking Stage

The intra-AS tracking stage is aimed to seek and isolate attacker nodes inside an AS. Basically, the results of intra-AS tracking are not disclosed to other ASes through InterTrack. The reason of information hiding is as follows; an intra-AS tracking is more detailed inspection to track a true attack path on an AS or to get the true IP/MAC addresses of attacker nodes, and a result of an intra-AS tracking is likely to contain some sensitive information such as a topology described in router hops like **traceroute**. Although the details of intra-AS tracking are not disclosed, a reverse AS path reported by an inter-AS tracking is sufficient to find ASes which can filter out the attack efficiently.

When an ITM starts an intra-AS tracking, the ITM forwards the tracking request to each DTM on each IGP sub-domain of the AS with a tracking request (Fig. 3.1(6), (6′)). Each DTM searches attacker nodes by DTS, and replies the traceback result to the ITM. By distributing an actual tracking to several DTMs along with IGP

sub-domains, different organizations on an AS can manage the DTM on each IGP sub-domain and can apply its local policy on reporting tracking results.

After receiving all reply messages from each DTM or the time out interval has come (Fig. 3.1(7), (7′)), the ITM aggregates these reply messages into a tracking tree which shows a detail path to the attacker nodes inside the AS, and stocks the tracking result into the paired DP (Fig. 3.1(11)). Then, the DP can generate a new filter rule from the tracking result, and can export some filter rules or tracking results themselves to other detection systems (e.g. IDS or Net-Flow) to start another tracking, or to some protection systems such as firewall or filter functions of a router or a switch to isolate attacker nodes from the network (Fig. 3.1(12)).

3.2 Future Work

We have presented the summary of InterTrack, a federation of IP traceback systems across borders of network operation domains. We have already developed a prototype implementation of the InterTrack components and a BTS based on some hash digest scheme. We predict that InterTrack can trace an attack even when different traceback techniques are employed in each BTS or DTS. Now, we are trying to develop another BTS and DTS implementations based on sampling methods; we will evaluate the traceability of InterTrack with different traceback techniques in near future.

第 4 章　まとめ

2005 年度において、本ワーキンググループでは、intertrack の提案と実装を進めた。これをふまえて、2006 年度においては、各種 ISP などとの協力し、実際のインターネットにおける運用を通じて、その有効性を検証する予定である。