発信源追跡のための ハイブリッドトレースバック方式の設計と実装

山田竜也† 池田竜朗†
森尻智昭† 才所敏明†

これまでに提案されていたインターネット環境における IP データグラムの発信源追跡の方式は、追跡者の意図に関わらず、追跡用データが生成者から一方的に送信されてくるという方式、すなわち受動的トレースバック方式が主流であった。しかし、この方式だけでは、効率的で詳細な発信源追跡が可能であるとは言えない。これに対して、本研究では送信者の意図を反映できるようなハイブリッドトレースバックアーキテクチャを提案する。さらに、このアーキテクチャを実現するにあたって必要な要素である能動的トレースバック方式の仕様と実装の概略について述べ、それを用いたときに考えられる発信源追跡のプロセスについても概説する。

The Design and Implementation of The Hybrid Traceback Scheme for Finding True Source of Packets

TATSUYA YAMADA,† TATSURO IKEDA,† TOMOAKI MORIJIRI† and TOSHIAKI SAISHO†

Conventional traceback protocols have been only considered to send traceback information from Generator to Tracer. We categorize them Passive Traceback Protocol. But their protocols are not helpful when Tracer wants to know who attacks them because of they do not reflect Tracer intention. Therefore we propose new tracebacking concept, Hybrid Traceback Scheme. In order to work well this scheme, a new protocl is required which is able to reflect Tracer intention and initiate tracebacking timely. Moreover, we introduce Active Traceback Protocol specification and some usage to enable Hybrid Traceback scheme, and describe some processes using it.

1. はじめに

インターネットの利用が広まるにつれて、(Distributed) Denial-of-Service 攻撃も頻繁に行なわれるようになってきており[1]、大規模なサイトに対する攻撃の事例も報告されている[2]。また日本においてもDSL☆などを用いた常時接続の利用者数が増加してきており[3]、これらの端末に対する攻撃やその端末を踏み台とした攻撃に対するセキュリティを講じる必要がある。

これに対するセキュリティ対策の一つに、攻撃パケットの発信源を特定し、攻撃の元から断つという手段が取り得る。しかし、現在のインターネットにおいては、ファイアウォールによってネットワークが分断されていたり、IP[4] アドレスの送信元の偽造が容易であったりすることにより、発信源の特定が困難であったり、特定できたとしても本来の攻撃者ではないという状態が起こり得る。したがって、正確な発信源の特定を可能にする技術、すなわち IP トレースバック技術が必要になってくる。

これに関して、これまでに具体的な実装として提案されているものに、Internet Engineering Task Force の itrace Working Group で標準化が行なわれている ICMP traceback (iTrace)[5] がある。これはパケットの経路上に位置するルータを通過するときに、ある一定の確率に基づいてパケットの追跡情報を生成するというものである。しかし、この方式には、利用者が発信源を追跡したいときに追跡できないばかりか、追跡したいパケットの種類を明示的に指定することができない、という問題点がある。

この iTrace に加えて、追跡者の意図を反映して発信源追跡を行なうための先行研究に 6) が存在する。

† 株式会社 東芝 SI 技術開発センター
Systems Integration Technology Center, Toshiba Corporation.

☆ Digital Subscriber Line

これは、簡単には、BGP☆1に iTrace のパラメータを調整するためのオプションを追加するというものである。しかしこれは BGP によってルーティングされているネットワークしか対象としていないため、ローカルネットワーク内での追跡には使用しづらいこと、また、iTrace のみにしか対応していないため機能拡張が容易ではないこと、などの問題点が依然として存在する。

これらの問題を解決するために、本研究では、従来型のトレースバック技術 (特に iTrace) と組合せて用いるハイブリッドトレースバック方式を提案し、それに必要なコンポーネントである能動的トレースバックの仕様とその運用方法について概説する。

本論文は以下のように構成される。2 章でハイブリッドトレースバック方式の概要について述べ、3 章で能動的トレースバックの仕様の概略について述べる。そして、4 章で本プロトコル仕様を用いた発信源追跡の典型的な動作について述べる。5 章でその運用に関して、6 章でセキュリティに関して、それぞれ検討を行ない、最後にまとめる。

2. ハイブリッドトレースバック方式

iTrace などに代表されるこれまでのトレースバック方式を、パケットの追跡者の意志に関係なく発信源追跡を行うものであることから、受動的トレースバック方式と呼び、これに対して、追跡者から要求が出たときに初めてトレースバックの処理を開始するという方式を能動的トレースバック方式と呼んでいる[7]。

受動的トレースバック方式だけではその性質上、発信源追跡の正確性や適時性、運用管理面において問題がある。そのため、この方式に加えて、本論文で提案する能動的トレースバック方式を組合せたものをハイブリッドトレースバック方式という概念の下で運用することを提案する。

ハイブリッドトレースバック方式は次のような効果をもたらすと考える。能動的トレースバック方式によって発信源追跡の開始地点を指定し、そこからの詳細な発信源追跡が可能となる。また、発信源追跡の開始時期を追跡者が任意に設定することが可能となるため、通常時に流通させなければならない受動的トレースバックによって発生するトラフィックを制御し減少させることが可能になる。

新たにハイブリッドトレースバック方式を実装・配備するためのコストについては、発信源追跡自体の機能はこれまでの受動的トレースバック方式をそのまま利用することが可能であるため、軽微であると考える。

3. 能動的トレースバックプロトコル

今回開発したプロトコルを Active Traceback Protocol (ATP)[8] と称し、の概要を以下に示す。

3.1 用語の定義

本稿で使用する用語を以下に示す。

Victim (D)DoS 攻撃などの被害を受ける機器など。

Generator 自身を通過するパケットについて、トレースバック用の識別子を付加したり、新たに追跡用データを含んだパケットを送信する機器。一般的にはルータを想定する。本プロトコル仕様においては ATP を受信・解釈する機能も備え、インターネット上、ローカルネットワーク上に多数存在すると仮定する。

Tracer Generator に対して実際に追跡要求を出す機器などを指し、一般に、Victim が所属する AS☆2内に存在する。IDS☆3などのようなネットワーク監視装置に実装されることが一般的と考えるが、Victim と同じ機器に搭載されても構わない。動作は Generator からの受動的トレースバックパケットを受信して攻撃を検知し、状況に応じて ATP を Generator に対して送信する。攻撃判断のアルゴリズムなどは本提案では検討しない。

Proxy Tracer 元の Tracer(Original Tracer と呼ぶ) からの依頼を受け、代理で能動的な追跡を実行する。想定される状況として、ファイアウォール内や NAT☆4 のように外部 AS に位置する Tracer からではネットワーク的にアクセスすることのできない位置から送信されてくる攻撃パケットの発信源を追跡することが考えられる。また、本仕様においては Proxy Tracer を再帰的に用いることが可能ではあるが、実際の運用を想定すると Original Tracer から Proxy Tracer への 1 段の代理追跡のみを可能とすることが現実的と考える。

3.2 プロトコルデザイン

受動的トレースバック方式において追跡情報を送信する方式は大きく二通りあった。通過するパケットの未使用ヘッダ内に分割した追跡情報を挿入する方式 (これをマーキング方式と呼ぶ) と、一つの追跡情報を通常のパケットとは別のパケットで送信する方式 (これをメッセージング方式と呼ぶ) である。

我々の提案する ATP は明示的に追跡情報の要求を

☆1 Border Gateway Protocol
☆2 Autonomous System
☆3 Intrusion Detection System
☆4 Network Address Transition

送信する必要があること、実装や配備のコストの面から既存の提案方式に沿ったものであることを重視したため、ICMP[9]、を基にしたメッセージング方式のプロトコルを作成することにした。

ICMP を基にした受動的トレースバック方式には iTrace が既に存在している。これは ICMP へのオプションとして定義されており、汎用性があることから本方式の基盤として採用とした。しかしながら、プロトコル仕様を iTrace へのオプションの追加として定義しているものの、特別に iTrace に依存してはいないため、単純に ICMP へのオプションとして実装することが可能である。

3.3 メッセージ形式

ICMP のメッセージフォーマット (図 1) の Message Body の中に Tag-Length-Value 形式で提案プロトコルのメッセージを格納する (図 2)。

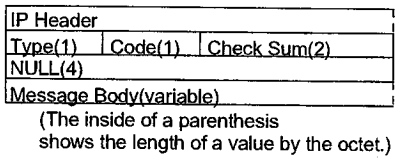

図 1 ICMP メッセージ形式

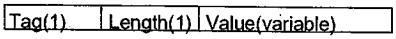

図 2 基本メッセージ構造

3.4 メッセージの種類

プロトコル仕様において定義したメッセージの種類とその概要について示す。

Begin Trace 能動的トレースバックを開始させる指示を Tracer から Generator に対して送信する。

End Trace Begin Trace によって開始された能動的トレースバックを停止させる指示を Tracer から Generator に対して送信する。

Deny Trace Tracer から送信された Begin Trace メッセージを拒否するために Generator から Tracer に対して送信する。

Capability Query Generator に実装されている受動的トレースバックプロトコルを問い合わせる。

Capability Reply Capability Query によって問い合わせを受けた Generator に実装されている受動的トレースバックプロトコルを回答する。

Delegate Active Trace Tracer から別の Tracer に対して能動的トレースバックの代理追跡を依頼する。依頼元を Original Tracer、依頼先を Proxy Tracer と称する。

Accept Delegation Proxy Tracer が Original Tracer からの追跡依頼を受理するときに送信する。

Deny Delegation Proxy Tracer が Original Tracer からの追跡依頼を拒否するときに送信する。

Trace Result Proxy Tracer によって行なわれた追跡結果を Original Tracer に返却するときに送信する。追跡結果は、追跡によって得られた IPv4/v6 アドレスである。

Passive Traceback ID 受動的トレースバックプロトコルを一意に識別可能な ID を示す。この番号割当は、将来的には IANA☆事項である。

Reason (Original) Tracer からの要求を拒否するときに、拒否する理由を人間に可読な文字列で記述する。

以下は既に iTrace の Internet-Draft 中で定義されていたものであるが、仕様上の相違から再定義したものを示す。

IPv6 Address 一つの IPv6[10] アドレスを示す。iTrace の I-D では二個一組であったため本プロトコル仕様には適合しなかった。

IPv4 Address 一つの IPv4 Address を示す。IPv6 アドレスと同様の理由による。

4. 運用プロセス

受動的トレースバック方式の Generator に対して ATP の一部を導入する必要があるため、本方式を用いたトレースバックには受動的トレースバックのみの運用よりも高度なオペレーションが必要となってくる。

本プロトコルは従来の受動的トレースバック方式に追加する形式で利用する。すなわち、日常の運用形態では受動的トレースバックメッセージのみがネットワーク上に流れており、Tracer がそれを監視している。あるとき、Tracer がパケットの発信源を追跡しようとするときに、適当な Generartor へ能動的トレースバックを実行し、さらにその結果に基づいて再帰的に能動的トレースバックを繰り返していくというものである (図 3)。

本アクティブトレースバックプロトコルを利用した

☆ Internet Assigned Numbers Authority

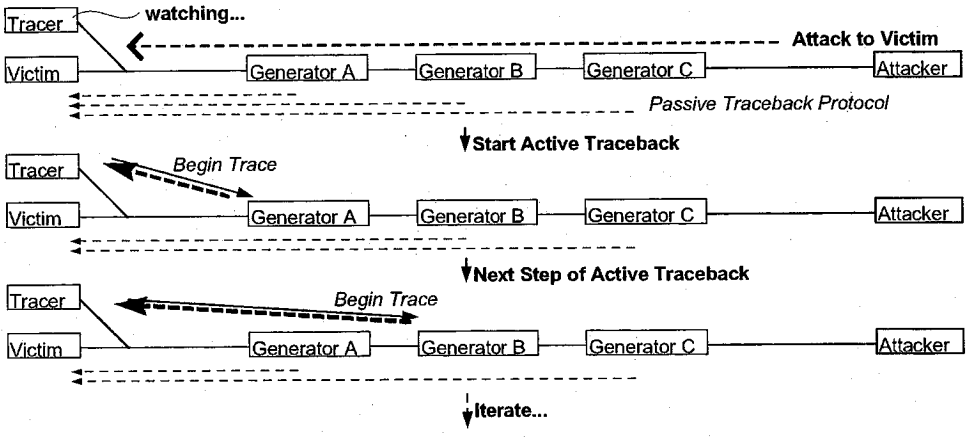

図 3　ハイブリッドトレースバック方式の運用形態

ハイブリッドトレースバック方式における発信源追跡の主な手順は、

- 要求-応答プロセス
- 能力調査プロセス
- 代理依頼-応答プロセス

の三種である。以降、これらについて示す。

4.1　要求-応答プロセス

これは本提案方式を使用するときの基本となるプロセスである。Tracer が定期的に受信している受動的トレースバック情報などについてさらに詳しい情報を知りたいときに、Generator に対して要求を送り、その結果を得るときに使用する (図 4)。

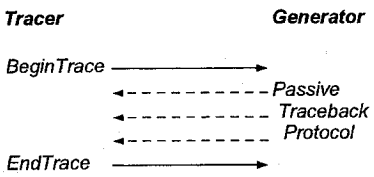

図 4　要求-応答プロセス

4.2　能力調査プロセス

Tracer が Generator の能力を調査するときに用いる。本提案で定義してあるのは Generator が実装している受動的トレースバックプロトコルを調査するためのメッセージであるが、任意に追加可能である (図 5)。

4.3　代理依頼-応答プロセス

元の Tracer からネットワーク的に到達できないネットワーク (例えば、ファイアウォールを超えたネットワーク) に対して発信源追跡を継続して行なうために、ネットワーク境界に位置している Tracer に対して代理の追跡を依頼するために使用する (図 6)。

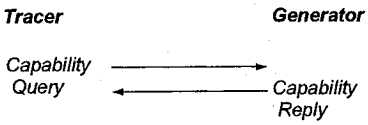

図 5　要求-応答プロセス

Proxy Tracer は Proxy Tracer が追跡依頼を出す Generator に対しては Original Tracer のように動作する。すなわち、Generator には Proxy Tracer と Original Tracer の区別がつかない。

5.　動作に関する考察

5.1　既存の受動的トレースバック方式に対する変更

これまでに提案されていた受動的トレースバック方式は、生成したトレースバックパケットの送信先を Victim としているものが主流である。このため、Generator が Tracer の宛先情報を知らないまま、ハイブリッドトレースバック方式を運用すると、Victim に到着する受動的トレースバックのパケットが増加してしまい、新たな攻撃の原因となる状況が考えられる。このため、Generator は能動的トレースバックによって生成される受動的トレースバックのデータを、Tracer 宛に送信できるように仕様・実装を改変する必要がある。

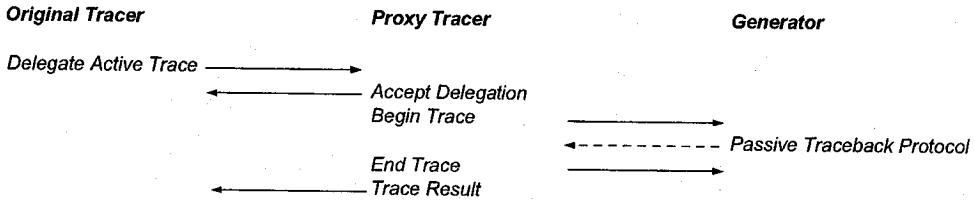

図 6 代理依頼-応答プロセス

さらに問題となるのは、マーキング方式を受動的トレースバック方式に選択した場合である。マーキング方式は通過するパケット中にトレースバック情報を埋めこむため、Victim 宛のパケット (攻撃中においてはその攻撃パケット) の中にしかその追跡データは存在しないことになる。実運用を想定すると、Victim が Tracer になることはあまり無いと考えているので、マーキング方式を使った場合に追跡情報の送信先を Victim とは異なる Tracer に変更可能にするための機構を設ける必要があるだろう。

5.2 停止条件

本プロトコル仕様では、受動的トレースバックメッセージの受信・解析を契機として Tracer が ATP を発信し、さらに詳細な追跡情報を新たな受動的トレースバックメッセージによって受信するという手順になっている。これによっても明らかなように、受動的トレースバック方式と能動的トレースバック方式を交互に繰り返し実施するとした場合、その探索の停止条件が明確ではない。しかし、本プロトコル仕様はパケット発信源追跡を効率的に、詳細に、行うことを目的としたものであり、自動化を目的としていない。したがって、本提案では、特に考慮しない。

しかしながら、直感的には、真の発信源に到達したとき、能動的トレースバックをサポートしないネットワーク機器に到達したとき、Layer3 対応ではないデバイスに到達したときに探索が終了すると考える。

5.3 ネットワーク負荷

能動的トレースバックプロトコルに関わるトラフィック増加を検討する。一回の能動的トレースバックパケットにより発生するデータは、基礎とする ICMP の仕様により IPv6 では最大 1280 オクテット、IPv4 では最大 576 オクテットである。そして、2 ノード間で行なわれる能動的トレースバックの各プロセスで交換されるメッセージは高々3 個である。したがって、標準的な管理回線に利用されるシリアルリンクの速度である 9600bps に対して、数秒程度で通信が完了できる。したがって、能動的トレースバックによって発生するネットワーク負荷はほとんどないと言える。

6. セキュリティに関する考察

6.1 パケット認証

本プロトコルは外部の Generator や Proxy Tracer に追跡パケットの生成を依頼する必要があるため、送受信パケットの認証機構は必須である。しかし、本プロトコル自身には認証機構を備えないため、別の方法で認証を行う必要がある。そのために、実際の運用では、本プロトコルの基盤とした iTrace の認証機構や、IPsec[11] などを用いることにする。

さらに、パケット認証に伴なう鍵交換を実施する必要もあるが、これについても本仕様では特に規定しない。しかしながら、最終的な運用形態を想定すると PKI☆によって行なうことになると考えている。

6.2 本方式による DoS 攻撃への考察

本プロトコル仕様では Tracer が Generator に命令して詳細な追跡パケットを生成させている。このため、以下では、ハイブリッドトレースバック方式によって Tracer と Generator に対する (D)DoS 攻撃が引き起こされる可能性を検討する。

Generator の場合。偽造された Begin Trace メッセージによって多量の受動的トレースバックメッセージを生成させられてしまう状況が考えられる。しかし、Generator のリソースに余裕が無いならば直ちに Deny Trace を発行することによって処理を拒否できるため、この問題は回避可能である。さらに、Begin Trace メッセージの検証に時間を要する可能性も考えられるが、同様に不要な追跡要求は拒否することが可能なため、これについても問題ない。

Tracer の場合。前提として、Tracer-Generator 間では相互認証が確立されており、かつ Tracer が Generator に対して指定した頻度で発生する受動的トレー

☆ Public Key Infrastructure

スバックメッセージを受信して処理することについては、Tracer の処理能力上の問題は発生しないと仮定する。このとき問題となるのは、第三者が偽造した (能動的、受動的) トレースバックメッセージに任意の認証情報を付加したメッセージを Tracer に送信し検証させてしまうことである。しかし、本プロトル仕様では通信に認証を伴うため、予め信頼関係が結ばれていない相手や Tracer が情報の取得を望んでいない相手とは基本的にトレースバック情報を交換しない。したがって、通信相手との認証情報の対応が取れていない時点で検証を中止することが可能であるため、偽造されたトレースバックパケットによる攻撃を防ぐことは十分に可能である。

7. 今後の予定

能動的トレースバックプロトコルやハイブリッドトレースバック方式について IETF に継続して提案し、標準化を目指す。また、仕様に従って PC ルータ上に実装し、実験ネットワークでの運用実験を行い、運用における課題の洗い出しや、仕様・実装のスケーラビリティの検証なども行なっていく。

8. ま と め

本研究では、ハイブリッドトレースバック方式の必要性について考察し、それに必要な能動的トレースバック方式のプロトコルについても概説した。また、能動的トレースバック方式を採用することによって発生する既存方式への変更点や運用時に考慮すべき事項についても指摘した。

謝辞 本研究は、通信・放送機構 (TAO) の委託研究テーマ「個人ユーザ向けの常時接続セキュリティ保護技術に関する研究開発」の一環として行なわれているものである。ここに記して謝意を表す。

参 考 文 献

1) D. Moore, G. M. Voelker, and S. Savage. Inferring internet denial-of-service activity. *10th USENIX Security Symposium*, 2001.
2) Computer Emergency Response Team. Cert advisory ca-2000-01 denial-of-serivce developements. http://www.cert.org/advisories/CA-2000-01.html, 2000.
3) 総務省. インターネット接続サービスの利用者数等の推移. http://www.soumu.go.jp/s-news/2002/020502_1.html, 2002.
4) J. B. Postel. Internet protocol. RFC791, 1981.
5) S. Bellovin, M. Leech, and T. Taylor. Icmp traceback messages. http://www.ietf.org/internet-drafts/draft-ietf-itrace-02.txt, 2002.
6) D. Massey, A. Mankin, C. L. Wu, X. L. Zhao, S. F. Wu, and W. Huang. Intention-driven icmp trace-back. Internet-Draft (Expired), 2001.
7) 大岸 伸之, 池田 竜朗, 森尻 智昭, and 才所 敏明. ハイブリッドスキームを利用した ip トレースバック技術. *SCIS2002*, 2002.
8) T. Yamada. Active traceback protocol. http://www.ietf.org/internet-drafts/draft-yamada-active-trace-00.txt, 2002.
9) J. B. Postel. Internet control message protocol. RFC792, 1981.
10) S. Deering and R. Hinden. Internet protocol, version 6 (ipv6) specification. RFC2460, 1998.
11) S. Kent and R. Atkinson. Security architecture for the internet protocol. RFC2401, 1998.