論 文 内 容 の 要 旨

博士論文題目

Studies on Interconnection Architecture for Traceback Systems in Practical Network Operations

氏　　名 櫨山 寛章

(論文内容の要旨)

Although many traceback techniques have been proposed and several network domains become using traceback systems in their network operation, locating the true source of attack traffic across the Internet is still difficult. Difficulties of traceback across the Internet are derived from these two issues as follows; the difference of the requirements for traceback systems according to the situation, and the fear of operational violation using an inter-domain traceback techniques.

In order to achieve an automated inter-domain traceback trial, we studied an interconnection architecture for traceback systems. We designed InterTrack as an interconnection architecture. Based on the phased tracking stages and the modularization of traceback systems, Intertrack covers requirements along with the situation to track attack traffic without any operational violation. We also proposed Ingress Port based traceback and a layer 2 extension of Hash-based IP traceback as interconnection techniques for tracking packets from the layer 3 networks to the layer 2 networks and locating the source nodes of packets in layer 2 networks.

Our proposals can achieve a traceback architecture which can track traffic on multiple layers across the Internet. Through discussion and evaluations with prototype implementations, we clarified the feasibility of our proposals.

氏　名	櫨山 寛章

（論文審査結果の要旨）

本論文は，パケット，トラフィックの転送経路の追跡技術であるトレースバック技術の連携機構に焦点を当てている．既存のトレースバック技術の研究の問題点は，各ドメインの内部情報の漏洩やドメイン間での権限の逸脱，異なる方式間の連携機能の欠如や回避攻撃の対応への困難さであり，それらの問題点により実運用におけるドメイン間トレースバックの実現は難しいとされていた．しかし，本論文では異なるトレースバックシステム間を連携させるトレースバック技術連携機構によりそれらの問題を解決している．本論文の主な成果は以下に要約される．

1. 現在のルーティングオペレーションにおけるドメイン間の境界とそれに付随する運用上の境界を分析し，ドメイン間でのトレースバック情報の伝達や運用におけるトレースバックシステムに対する要件と，その要件に対する既存のトレースバック研究の問題点を明らかにし，トレースバック技術の連携機構の必要性を示した．
2. 現在のルーティングオペレーション境界と運用上の信頼関係を基にし，ドメイン間トレースバックを実現するためのトレースバックシステム連携機構を提案した．連携機構により各ドメインごとにトレースバックシステムの運用範囲を分割でき，ドメイン間トレースバックの運用に各ドメインの運用ポリシーの適用が行え，情報漏洩，権限の逸脱を防ぎつつドメイン間トレースバックを実現可能できる．また，各ドメインのトレースバックシステムをモジュールとして連携させることでトレースバックシステムの導入や新技術への移行がドメインごとに独立して行え，単一ドメインで様々なトレースバック技術を用いて追跡が行えるを示した．
3. ドメイン内部に存在するパケットの送信ノードの特定をより詳細に行うために，レイヤ 3 ネットワーク上でのトレースバックシステムとレイヤ 2 ネットワーク上でのトレースバックシステムの連携方式を提案した．これにより，異なるレイヤでのトレースバック技術を連携させることで，より詳細な追跡が行えることを示した．

以上のように，本論文は実ネットワーク運用に沿う形でより詳細なドメイン間トレースバックの実現を目指し，ドメイン間やレイヤ間でのトレースバックシステムの連携機構，連携技術の提案を行った．さらに，モデル化や実装による追跡時間の評価により有効性を示し，トレースバックシステムの実用化における問題点の説明と問題に対する研究の方向性を示した．本論文は学術上だけでなく，今後のインターネット上での追跡技術を実現するための新しいアプローチとしてもその貢献度は大きいといえる．よって本論文は博士（工学）の学位論文としてふさわしいものと認める