博士請求論文審査要旨

情報セキュリティ大学院大学
情報セキュリティ研究科

論文題目　：　トラフィック分析技術を用いた不正アクセス抑止システム
申請者　　：　三村 守
審査委員会：　主査　教授　田中 英彦
副査　教授　小柳 和子
副査　教授　佐藤 直
副査　教授　松尾 和人

Ⅰ．論文内容の要旨

本論文は、「トラフィック分析技術を用いた不正アクセス抑止システム」と題し、９章からなる。近年、組織等の情報システムは組織内外からの様々な不正アクセスの脅威にさらされており、それに対応する情報セキュリティ対策が施されている。しかしながら、それらは主に権限奪取、不正実行および後処理の対策が殆どであり、そこに至る以前に施すべき対策の検討は少ない。一般に不正侵入は遠隔から対象情報システムの情報を収集し、それに基づいて脆弱性を探し、そこから行われるのが通例である。この研究は、そのような事前調査による情報収集を防止することによって情報セキュリティ対策とすることを検討し、その手法を詳細に考察したものである。

第１章は「序論」で、本研究の背景とねらい、目的、範囲、方針及び論文の構成についてまとめている。

第２章は「情報システムに対する情報収集の脅威」で、情報システムへの事前調査プロセスに着目し、外部からの脅威であるトラフィック分析技術と、内部の脅威である不正接続とについて検討し、本研究で対象とする脅威を明らかにしている。すなわち、トラフィック分析技術としては、TCP/IP ヘッダの内容を観察し、TCP/IP プロトコルの実装が OS 毎に差異があることを用いて OS の種類を特定する OS Fingerprinting と、メッセージのペイロードを走査せずに、パケット長や送受信タイミングに着目してアプリケーションやプロトコルを推定する技術を取り上げ、その脅威を分析している。不正接続に対しては、未承認機器が組織の情報システムに接続されることへの対策を取り上げ、従来のネットワーク監視システムでは検出が不可能な NAT による不正接続問題があることを明らかにしている。

第３章は「Anti OS Fingerprinting システムの提案と実装」で、ネットワークの経路上で対策を施すルータである Anti OS Fingerprinting システムを扱っている。従来の手法では、機器毎に実装する必要性があり、また、パッシブな OS Fingerprinting には無力という問題があったが、本章では、ネットワーク経路上で OS Fingerprinting を消去する汎用的な手法を提案している。送信パケットのみを対象に変換を実施するもので、変換は、ヘッダの Type of Service フラグ、パケット識別子、TCP オプション、Time to Live、ウインドウサイズなどへの対策からなる。論文では、これを実験ネットワーク上に実装し、代表的な OS Fingerprinting 手法による OS 推定を行った結果、それらが失敗し対策が有効であることを示している。しかし、パケットスループットが低下すること、traceroute が出来なくなること等、提案手法の限界を明示するとともに、Application Banner を用いる OS 推定手法対策、TCP シーケンス番号対策などの必要性を指摘している。

第４章は「トラフィックパターンを隠すトンネリングアプリケーションの試作」で、ネットワークトラフィックの挙動分析技術に対する対策として匿名通信技術を応用した対策を検討している。従来、幾つかの手法が提案されてきたが実装は個別に必要であった。この章では、ネットワーク経路上で集中して対策を施しパケット長と送信間隔を変える方式を

試作し、それを用いた実験を通して、挙動分析対策を施した VPN 実装のための指針を明らかにしている。

第5章は「トラフィックパターンを隠す VPN の開発」で、4 章で試作したアプリケーションを基に、暗号機能を付加した VPN アプリケーションを実装し、その性能を実験で確認している。信頼性を確保するために Session Control Transmission Protocol を用い、パケット長とタイミングを制御しており、実験の結果、本方式は多くのアプリケーションの動作には影響を与えず、パケットの損失が少なければスループットに殆ど影響は無いが、損失が大きい場合はかなりの影響があることなどを示している。

第6章は「能動的 NAT 検出手法の提案」で、従来の手法では検出できない NAT による不正接続を検出する手法を提案したもので、外部へ出るルータに検出システムを載せる手法である。パケットを監視し、送信元へトレースパケットを送信し能動的に IP ヘッダ内の Time To Live 値を取得して不正接続を検出する。トレースパケットに応答しないホストについては、そのホップ数をシステムに記録し、同一ホストの別パケットのホップ数と比較することで検出を行うもので、実装実験を行いその効果を確認している。

第7章は「能動型不正接続防止システムの開発」で、利用者にその存在を意識させない形での効率的な不正接続防止システムを検討したもので、6章で提案した能動的 NAT 検出手法を用い、検出した不正接続には、RST パケットを送信することでその TCP 接続を切断し、対象ホストの TCP 通信を無力化する方式を提案している。この方式は、既存の方式に比して、ローカル通信の検出は出来ないが、簡易に 1 か所の集中対策で可能という利点を有する。

第8章は「不正アクセス抑止システムの効果」で、この論文で提案した不正アクセス抑止システムの効果を総合的に確認するために、模擬システムを構築し現実の外部インターネットに接続して効果を検討したものである。抑止システムは、Anti OS Fingerprinting システム、トラフィックパターンを隠す VPN および能動型不正接続防止システムで構成され、それらの対策を施したシステムと、施さないシステムとを並列に動作させた結果、両者間には有意なるトラフィック量の差異が認められ、この提案システムが有効であることを示している。

第9章は「結論」である。

Ⅱ. 論文審査結果の要旨

これを要するに本論文は、インターネットに於ける大きな脅威として情報システムへの不正アクセス問題を取り上げ、対象システムへの侵入手段に関する事前調査活動に着目し、それを無力化することにより不正アクセスを抑止するシステムを提案し、実験によりその有効性を示したもので、情報学に貢献するところ少なくない。

よって、本論文は、博士（情報学）の学位請求論文として合格と認められる。

Ⅲ. 審査経過

本審査委員会は、平成 23 年 2 月 2 日に論文内容とこれに関連する事項について口述試問を行い、申請者が学位取得にふさわしい知見を持つものと判断した。