ＩＤＳ回避攻撃への対策手法について

2G－5

小林 信博、勝山 光太郎
三菱電機(株) 情報技術総合研究所

1. はじめに

近年、インターネットの普及に伴い、不正アクセスによる被害も増加の一途を辿っている。これに対して、企業や大学、公的機関等においてイントラネットを保護する為に、ファイアウォールを用いた外部からの侵入防止や、IDS(Intrusion Detection System) による内部への侵入の検出といった方策がとられている。IDS は、実現形態によりネットワーク型,ホストベース型の２種類、検知手法により MID(Misuse Intrusion Detection), AID(Anomaly Intrusion Detection)の２種類に分類される。現在主に導入されているのはネットワーク型 MID 方式の IDS であるが、これを回避する攻撃として挿入(Insertion)や回避(Evasion)等の方法が報告されている[1]。そこで本稿では、IDS 回避攻撃への対策として、能動的にネットワーク的な距離情報を取得し、これを利用する手法について提案する。本手法を用いることにより、従来の IDS と比較して false negative の割合を減少させることが可能であり、より安全なネットワークの実現に寄与するものと考える。

2. IDS 回避攻撃

IDS による検知を回避する攻撃方法の一つとして挿入がある。ネットワーク型 MID 方式の IDS による検知を回避する場合は、余分なパケットを挿入することで実現される。図１に IP パケットの TTL(Time to Live)を利用した挿入の例を示す。

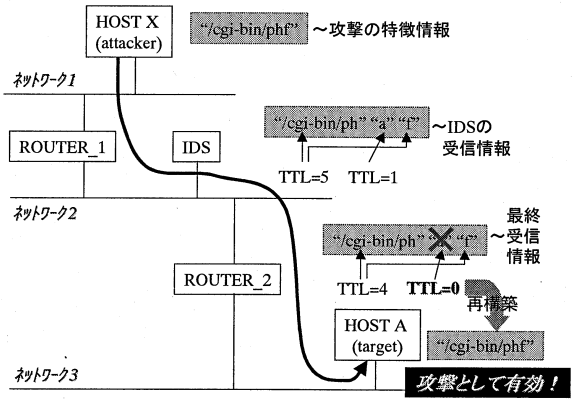

図 1　IDS 回避攻撃概念図

パケットが ROUTER を経由するごとに TTL 値は１つ減じられ、TTL=0 となると破棄される。そこで、攻撃者(attacker)である HOST X は、IDS の接続されたネットワーク２には到達するものの、目標(target)である HOST A の接続されたネットワーク３には不達となるように、TTL値 を操作した攻撃用のパケットを送信し IDS による検出を回避する。

3. 対策手法

従来の IDS はネットワークトポロジーを知らずに受動的なデータ収集のみを行っている為、前述の攻撃への対処が困難と考えられる。そこで今回は、パケットの宛先までのネットワーク的な距離(HOP数)を能動的に取得することで、問題解決を図る。パケットの宛先までの距離と TTL値 を比較することで、最終的にそのパケットがターゲットへ到達可能かどうかを判断する機能を追加する。そして、実際に宛先まで到達可能なパケットのみを入力情報として処理し、攻撃シグネチャと比較検証を行う。これにより、TTL を操作した挿入への対策を可能となる。

A proposal for intrusion detection system against insertion attack
Nobuhiro Kobayashi, Kotaro Katsuyama,
Information Technology R & D Center,
Mitsubishi Electric Corporation
5-1-1 Ofuna, Kamakura-shi, Kanagawa,
247-8501, Japan

3.1. システム構成

図２に攻撃対策の機能を付加したIDSのシステム構成を示す。新たに追加された部分は、パケットの宛先までのネットワーク距離を測定するネットワーク距離測定部とネットワーク距離測定用のパケットを送受信する測定パケット送受信部である。

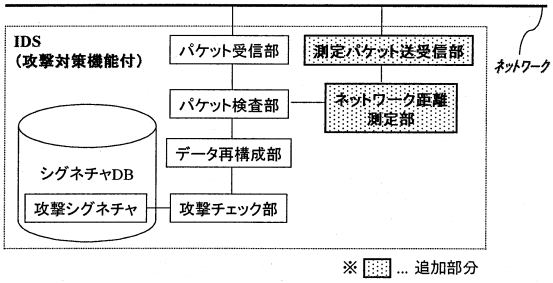

図 2　攻撃対策機能付 IDS

このシステムの動作について説明する。まずパケット受信部によりネットワーク上のパケットを受信し、パケット検査部へと渡す。次にパケット検査部がパケットから宛先アドレス取得し、ネットワーク距離測定部へと渡す。ネットワーク距離測定部は、受け取った宛先アドレスと TTL=1 を設定した ICMP エコー要求メッセージを測定パケットとして作成し、測定パケット送受信部からネットワークへ送信する。もしも、ICMP 時間超過メッセージがパケットの経由するルータから返送された場合は、TTL を１加算して再送する。そして、ICMP エコー応答メッセージを受信した場合に、その時点の TTL 値をネットワーク距離としてパケット検査部に渡す。パケット検査部は、パケットの TTL と測定したネットワーク距離を比較し、TTL が短い場合は不達パケットとして破棄し、それ以外のパケットをデータ再構成部に渡す。そして再構成されたデータが攻撃チェック部でシグネチャ DB に格納された攻撃シグネチャと比較され、攻撃かどうかの判断がなされる。

3.2. ステルス性の確保

従来から多くのネットワーク型 IDS は、パケットの宛先に関係なく受信動作を行うプロミスキャスモード(promiscuous mode)にて動作している。従って、他の機器との通信を全く行わずに、その存在を攻撃者から隠蔽すること(ステルス化)が可能となっている。しかし今回提案の方式では、ターゲットとなるホストまでのネットワーク距離を測定する際に通信が発生する為、このステルス性が失われてしまう。そこで、ネットワーク距離測定用のパケットに特別な変更を加える。

まず、IDS の接続されたネットワーク２に存在する別の機器のアドレスを予め与える。図１のようなネットワーク構成の場合には、ROUTER_1 のアドレスが利用可能である。そして、この ROUTER_1 のアドレスを、ネットワーク距離測定用パケットの送信元アドレスに設定してターゲットへ送信する。ターゲットからのリプライは、ROUTER_1 に返送されるが、同じくネットワーク２に接続された IDS では、プロミスキャスモードによりこのパケットを取得することができる。以上のような動作により、ステルス性を確保しつつ IDS 回避攻撃の対策が実現可能となる。

4. おわりに

本稿では、IDS に対する回避攻撃の一つである挿入への対策として、ターゲットへのネットワーク距離を測定し、これを元にパケットの再構築を行うことで偽装を発見する方法について述べた。そして、その対策を実現するシステムの構成と動作について説明を行った。また、ステルス性を確保する為に、同一ネットワーク上に存在する機器のアドレスを利用してネットワーク距離の測定を行う方法についても述べた。これにより、従来の IDS よりもネットワークの安全性を向上することが可能と考えられる。

今後は、システムの試作を行うと共に、評価を実施する予定である。

5. 参考文献

[1] T.H.Ptacek and T.N.Newsham, “Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection”, Secure Networks, Inc, Jan. 1998

[2] 武田 圭史,磯崎 宏、”ネットワーク侵入検知”、ソフトバンク パブリッシング株式会社、Jun. 2000