侵入検知システムの高速化手法について

3H－03

大越 丈弘、藤井 誠司、勝山 光太郎
三菱電機株式会社 情報技術総合研究所

1．はじめに

近年、システムの脆弱性が次々と発見され、それと同時に侵入検知システムが検知しなくてはならない不正アクセス手法が急激に増加してきている。不正アクセス手法が増加の一途をたどり侵入検知システムの検知処理が増大するため、パケットを取りこぼし、不正なパケットを処理できず攻撃を検知しない問題が発生する。いかにパケットを取りこぼすことなく全パケットに対して検知処理を実施できるか、侵入検知システムの高速化が重要な課題となっている。

本稿では、侵入検知システム（Intrusion Detection System、以降、IDS と略記）の高速化手法として、検知する不正アクセス手法を絞り込むことによって高速化を実現する手法について報告する。

2．分析手法

どの不正アクセスも、次に示す2つの分析方法で検知が可能である。

2.1 シグニチャ検知

攻撃パケットの特徴表す情報をパターンマッチングすることにより検知する。もっとも一般的な分析手法である。例えば、メールサーバへのバッファオーバフロー攻撃の検知であれば以下の条件に合致するかを分析する。すなわち、パケットの tcp ヘッダ部にある送信先ポート番号が 25（smtp）、tcp のデータ部にある smtp コマンドの引数が128バイトより長いかをチェックする。チェックする個所は特定しておらず、パケットの種類、ポート番号、文字列等、不正アクセス手法によってさまざまである。

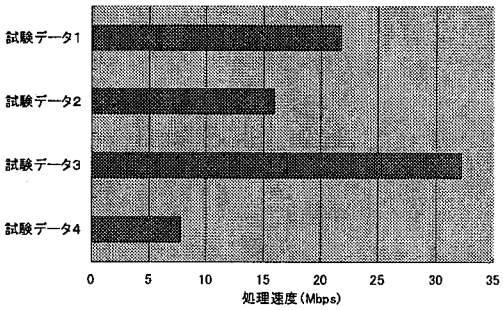
2.2 統計的検知

攻撃の中には、大量のパケットを集中的に流すことでサービスの可用性を低下させ、時にはサービス提供を不能とするのもある。そのような攻撃は、パケット自体は規格に則った正しいものであるため、上述のシグニチャをパターンマッチングする方法では検知できない。この場合、特定のパケットが特定の期間に集中しているかを察知することにより、攻撃が行われているかを推定しなくてはならない。

2.3 高速化の必要性

我々は、以前の研究において IDS を試作し性能測定を実施した[1]。そのときの測定結果を以下に示す。

表 性能測定結果



環境：PentiumIII 500MHz,128MB,NT4.0SP5
試験データ 1：expn　xxx...x(expn　の後に 128 文字)
試験データ 2：expn　zzzzz
試験データ 3：get　yyy...y(get　の後に 1024 文字)
試験データ 4：get　www...w(get　の後に 1023 文字)

Method to improve the process performance of IDS(Intrusion Detection System)
Takehiro Okoshi, Seiji Fujii, Kotaro Katsuyama
MITSUBISHI ELECTRIC CORPORATION,5-1-1 Ofuna, Kamakura, Kanagawa 247-8501, Japan

従来のシステムにおけるパケット分析機能は、将来の不正アクセスの増加を考慮して、容易に分析ロジックを組み込むことができることを優先し上述のシグニチャ検知の処理を一部共通関数化した。そのため、パケットによっては、冗長な処理の繰り返し等、性能を劣化させることが判明した。

したがって、ネットワークの負荷があがると，パケットを取りこぼす可能性があり、チェックされてないパケット（取りこぼしたパケット）の中に攻撃パケットが含まれ、攻撃を検知できない可能性が十分に考えられた。分析処理の高速化が不可欠となった。

3．高速化手法の検討

高速化を検討するにあたり、データ構造・ロジックの見直しといったことも検討項目として考えられた。しかし、上述の IDS が将来の攻撃に対応する処理の追加を容易にすることを優先していたことから、我々は他の方法を検討した。

そして、ターゲットとなるホスト及びネットワークシステムが提供するサービスが限られていることから、必ずしもすべての攻撃を検知する必要がないことに着目し、ネットワーク負荷に応じて検知する項目を動的に絞ることを検討した。その結果、以下のような攻撃項目テーブルとパケット監視機能を新たに設けることにした。

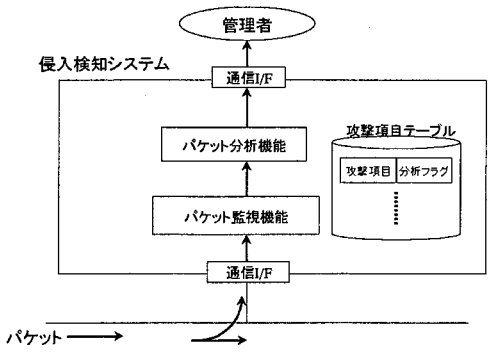


図 全体構成図

3.1 攻撃項目テーブル

本設計では、各不正アクセス手法に関する攻撃項目に、分析処理をする/しないを表す分析フラグを付加することとした。なお、分析フラグはユーザが動作環境に応じて設定するものとする。

3.2 パケット監視機能

パケット監視機能において、単位時間あたりのパケット数、データ量等のパケット量を監視することとする。

3.3 パケット分析機能

パケット分析機能では、パケット監視機能でカウントした受信パケットの量が、あらかじめユーザによって設定された閾値を越えた場合は、攻撃項目テーブルに列挙されている全攻撃項目を検知処理するのではなく、分析フラグで指定された項目だけを処理することとする。

4．今後の評価及び検討課題

今後は、上述した高速化手法を実現して、パケットの取りこぼしが発生するか否か本手法による効果を検証しなくてはならない。また、ネットワーク負荷により検知項目の絞り込みが行われ、検知しない項目があったとしても、実運用に影響がないかを実際に運用して有効性を検証しなくてはならない。

5．終わりに

本稿では、ネットワークの負荷に応じて検知する項目を動的に絞ることによって、IDS を高速化する手法について説明した。

参考文献

[1]藤井他、“侵入検知システムの検知性能の評価”、情報処理学会第 61 回全国大会論文集、5D-01、2000.