シグネチャの H/W 検索を考慮したインライン型 IDS の開発(1)

貞包 哲男† 原田 道明† 永嶋 規充†
三菱電機株式会社 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より、ネットワーク不正侵入の問題が大きくなっている。それに伴い、外部から内部ネットワークへの攻撃を検知する IDS の重要性が高まっている。その中でも、攻撃を検知するだけでなく、攻撃パケットを破棄できるインライン型 IDS が、防御方法として非常に有効である。しかしながら、インライン型 IDS では、ユーザトラフィックの性能低下を抑えてリアルタイムにパケットを中継する必要があるため、ホスト型 IDS より高速な処理が必要となる。

今回、筆者らはシグネチャの検索において H/W での高速化について着目した方式を提案し、提案した方式が有効であることを検証するためにインライン型 IDS のプロトタイプを F/W で開発した。

２．シグネチャ

IDS では、入力されたパケットと攻撃パターンをルール化したシグネチャとをパターンマッチングして、攻撃を検出する。シグネチャのひとつのルールの書式を次に示す。

アクション プロトコル 送信元 IP 送信元ポート -> 宛先 IP 宛先ポート （ルールオプション列）

括弧までの前半部分をルールヘッダと呼び、ルールヘッダは、ルールが実施すべき行動(アラート通知、中継、破棄等)と監視すべきプロトコルと送信元、宛先の IP アドレス、ポート番号で構成されている。なお、IP アドレスはマスクにより範囲指定することができる。

ルールオプションには、そのルールをマッチさせるための詳細な条件（各プロトコルのヘッダのオプションや、ペイロード部分に含まれる文字列パターン等）を記述する。

Development of In-Line Intrusion Detection Method for Hardware Accelerated Signature Matching, Part 1

†Tetsuo SADAKANE, Michiaki HARADA, Norimitsu NAGASHIMA,
Information Technology R&D Center, Mitsuishi Electric Corporation 5-1-1 Ofuna, Kamakura, 247-8501 Japan

３．課題

インライン型の IDS では外部ネットワークから入ってくるパケットをすべてのシグネチャに対してリアルタイムに検査する必要があるため、高速な検知処理が必要である。特にルールオプションに記述される文字列パターンのマッチングは非常に処理負荷が大きい。したがってルールヘッダで条件が一致しないルールは、ルールオプションを処理しないようにルールの絞込みを行った方がよい。

F/W で IDS を実現している snort[1]では、プロトコルごとにヘッダオプションのリストを作成して、同じ条件はルールをまとめるような処理を行って検索時間の短縮を行っている。しかしながら、ルールヘッダの検索に全体の約 15%程度の処理時間がかかっていることが報告[1]されているように、F/W での処理には限界がある。

本発表では、ネットワーク装置で高速にパケットを振り分けるために用いられている CAM(Content-Addressable Memory)を使用して、検査する必要があるシグネチャの絞込みを高速に実現する方式を提案する。

4．構成

本システムの構成を図 1に示す。

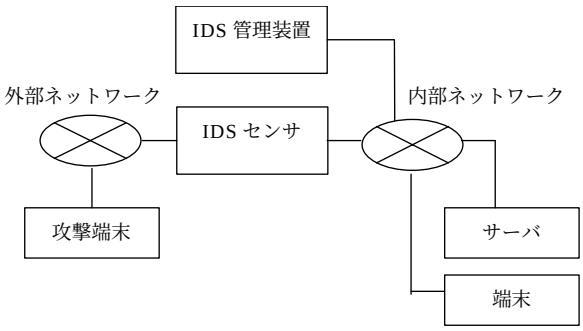

図1 インライン型 IDS の構成図

IDS 管理装置では、アラートの収集、シグネチャの登録処理の他に、シグネチャから CAM に登録するフォーマット（CAM フィルタ）に変換し IDS センサに送信する。IDS センサでは、シグネチャの他に CAM フィルタの登録を行い、外部ま

[1] snort™は米国 SourceFile INC.社の登録商標

たは内部ネットワークから入力されるパケットを検査し、中継する。

5．提案方式

図 2に IDS センサの検知処理の概要を示す。

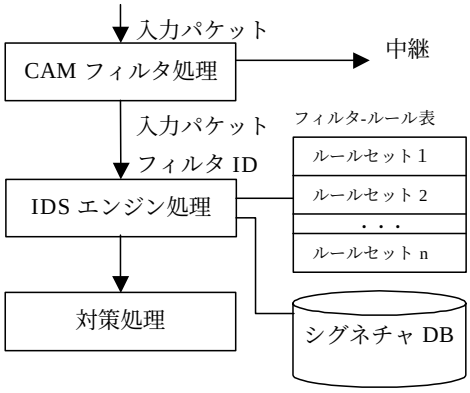

図2　検知処理の概要図

CAM フィルタ処理は入力されたパケットの IP アドレス・ポート番号・プロトコルの情報をもとに、CAM によって登録された内容と一致するものを検索し、最初にヒットしたフィルタの ID を入力パケットと一緒に IDS エンジン処理に渡す。フィルタ ID を受け取った IDS エンジン処理では、フィルタ-ルール表を用いてフィルタ ID からそのパケットで検査すべきルールセットを特定する。このシグネチャの絞込みの処理を行うことによって、IDS エンジンの処理負荷を少なくする。IDS エンジンは検査すべきルールのみをシグネチャ DB より取り出して、ルールオプションの検査を行う。最後にルールと一致して攻撃を検知した場合はパケットの破棄等の対策処理を行う。

5.1 CAM フィルタ

IDS 管理装置でのシグネチャの変換フォーマットについて説明する。シグネチャのルールヘッダをそのまま CAM に登録してしまうと、送信元と宛先の IP アドレスが範囲指定できるため Multi-Match が発生する可能性がある。その場合 CAM の検索に時間かかると共に IDS エンジン処理が複数回実行されることになり処理が煩雑になる。この問題を解決して、CAM を First-Match で検索できるように以下のような手順で CAM フィルタを生成する。

（1） プロトコルと宛先、送信元 IP アドレスとポート番号の範囲が他のルールと重なりがあるものは、重なりの部分で範囲を分割し、新しい CAM フィルタを生成する。
（2） プロトコルと宛先、送信元 IP アドレスとポート番号が同じ範囲、または含まれるものは、そのルールを追加する。
（3） 包含関係にあるルールは、範囲が狭いものを順に並べる。

以下のようなルールＡ、Ｂのシグネチャ(ルールオプションは省略)での CAM フィルタの生成の例を示す。

ルールＡ：alert TCP 10.74.10.0/24 any -> any 80
ルールＢ：alert TCP any any -> 192.168.12.0/24 80

表1　CAM フィルタの生成例

filter ID	proto	Src IP	Src Port	Dst IP	Dst Port	Rule
1	TCP	10.74.10.0/24	any	192.168.12.0/24	80	A,B
2	TCP	10.74.10.0/24	any	any	80	A
3	TCP	any	any	192.168.12.0/24	80	B

① ルールＡ、Ｂでは IP アドレスの範囲が重なっているため、重なりの部分を分割して新しいフィルタを生成する。
② 新しく生成したフィルタはルールＡ,Ｂに含まれているため Rule にはＡ,Ｂを追加する。
③ 新しく生成したフィルタはルールＡ、Ｂに含まれているため、それらよりも小さい順番に配置する。

表 1の filterID から Dst Port までの内容を CAM フィルタとして CAM に登録し、filterID と Rule の部分をフィルタ-ルール表として IDS センサに登録しておくことにより、CAM の検索で First-Match が可能となり IDS エンジンで検査するシグネチャの集合を特定することができる。

６．まとめ

本発表では、入力パケットに対して CAM を用いて高速に検査すべきシグネチャを絞り込む方式について述べた。

今回はプロトタイプとして CAM の部分を F/W で実装したため、実際の CAM を用いた構成で提案方式の評価を進めたい。

参考文献

[1] Mike Fisk and George Varghese, “Applying Fast String Matching to Intrusion Detection”, UCSD TR CS2001-0670.
[2]「シグネチャの H/W 検索を考慮したインライン型 IDS の開発(2)」原田 道明他、情報処理学会第 66 回全国大会
[3] Snort:The Open Source network Intrusion Detection System, http://www.snort.org