ネットワーク侵入検出手法の比較と脅威に応じた動的な検出

4T－6

武田 圭史†　溝江宏真†　武藤 佳恭††

1．はじめに

従来のアクセス制限、暗号化、認証を中心とした静的なセキュリティ技術を補完するものとして、能動的にシステム上の問題の発生を検出し通報等必要な処理を行う動的なセキュリティ機構が必要と考えられる。機器及びネットワークに対する不正なアクセス・操作を探知し、管理者あるいはユーザに警報を発し対応を促す機能を持つものとして侵入検出システム(Intrusion Detection System)が提案されている。[1]

本研究では侵入検出システムに応用可能な手法及び対象データについてのサーベイと比較を実施し、その結果を踏まえた上で複数のアプローチを脅威の状態に応じて動的に切り替えるシステムを提案する。

2．侵入検知手法と入力データ

ここでは検出に使用される「検出手法」、「入力データ」、「アーキテクチャ」の３つの観点から侵入検出を考える。

2.1 検出手法

*異常(anomaly)検出*の手法では、正常な運用時の状態をプロファイルとして記録、学習、あるいは初期値として定義し、運用状態の異常値を検出することで不正アクセスを発見する。[2]

*不正(misuse)検出*ではあらかじめ定義された不正なコマンド・セット等の文字列をシグネチャ(signature)として登録しておき、これを検出することで不正アクセスの判定を行う。[3]

それぞれ以下の特徴があると言われている。[4]

(1)異常検出(anomaly detection)
- 未知の攻撃手法を検出可能
- 緩やかにプロファイル・データを推移をさせることにより判定値に影響を与えることが可能
- 高い false positive rate

(2)不正検出(misuse detection)
- 既知の攻撃手法のみ検出可能
- シグネチャ情報の蓄積・更新が必要
- 低い false positive rate

2.2 入力データ

システムへの入力データとして、オペレーション・システム及びアプリケーションが生成するログ・データ、ネットワーク上のパケットデータ及びトラフィック情報、ファイルの更新情報、機器の設定情報などを用いることができる。特殊なものとしては、プログラムが使用するシステム・コールのシークエンス[5]や、システムの状態遷移パターンを入力とする研究も行われている。[6]

各入力データの特性は以下のとおりである。

(1)ログ・データ

システムあるいはアプリケーションによって生成されるログファイルを解析する。
- 新規または独自にデータを取得する必要がない。
- データ遅延によって事後検出になってしまう可能性がある。
- データ改竄の可能性がある。

(2)パケット・データ及びその統計

ネットワークのトラフィックを監視する。
- 要求される処理量と速度が大きい。
- ホストに限定されない情報が入手可能
- ネットワーク上の配置位置が限定される場合がある。

(3)ファイル情報

侵入時に置き換えや改竄をされる可能性のあるファイル・コマンド等の更新状況を監視する。
- 目的に応じた対象ファイルの指定が必要
- 正当な書き換えとの区別が困難

(e.g. 各種設定ファイル、パスワードファイル)

(4)機器設定情報

侵入時に変更される可能性のある機器設定情報を監視する。
- 検出可能な情報及び不正操作が限定される。

(e.g. Sniffer に対する NIC の promiscus mode)

2.3 アーキテクチャ

検出モジュールの配置と対象については、単一のホストに配置対象とするホスト・ベースと、対象ネットワーク上に配置されネットワーク及び接続機器を監視対象とするネットワーク・ベースに分類される。[7]

(1)ホスト・ベース
- 保護対象は当該ホストに限定される。
- 侵入により無効化される可能性がある。

A comparison of intrusion detection methodologies and a dynamic intrusion detection based on threats.

Keiji Takeda, Hiromasa Mizoe, Yoshiyasu Takefuji
Keio University.5322 Endoh Fujisawa Kanagawa 252,Japan
† 慶應義塾大学　政策・メディア研究科
†† 慶応義塾大学　環境情報学部

(2)ネットワーク・ベース

ネットワーク上の複数の機器あるいはネットワーク自体を対象に含む。

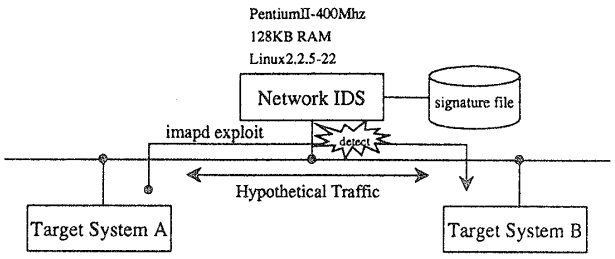
・対象範囲を広く、効率に優れる。

・パフォーマンス、スケーラビリティー、ロバストネスにおいて問題がある場合がある。

3. 実装と評価

試作したシステムでは単一ホストによるネットワーク監視部[8]及び各ホストにおけるホスト監視部を組み合わせて使用する。各ホスト部はログ・データ及びファイル情報の異常検出及び不正検出を行う。ホスト監視部での異常検出を受け、ネットワーク部がパケットの監視を開始する。ネットワーク監視部はネットワークの上流に位置し対象ネットワークに向けられたパケット上の不正シグネチャ検出を行う。前項にあげた手法、対象、アーキテクチャを組み合わせることでシステム資源を無駄に消費することなく効果的な侵入の検出が可能と考える。最終的には定義されたシグネチャの検出をもって警報を発することから不正が無いにも関わらず警報を発するfalse positive rate を低く押さえることができ、利用者のシステムに対する信頼を高めることができる。ただし未知の攻撃に対するfalse negativeの危険性がある。

実験はネットワーク部の性能について、外部から遮断されたネットーワーク上に監視対象となる2台のホスト及びこれらを監視するネットワーク・ベース監視ホストを設置し実施した。TCP プロトコルによる人為的な負荷としてランダムなテキストを含んだトラフィックを対象ホスト間で通信させ、検出するべき侵入行為としてimapd サーバのバッファ・オーバフローを目的とした攻撃プログラムをホストの一台に用意、対応するシグネチャを監視項目に登録した。計測の目的は大量のトラフィックの中からシグネチャ検出が可能であるかを確認することであり、結果は図のとおりとなった。今回の実験では、発生させる人為的な負荷トラフィックに限界があったために、機能上の限界値を測定することはできなかった。しかし、ネットワーク監視部は測定値の全てのパケット内容をモニタしており、実運用下での帯域幅値には監視不要なトラフィックが多く含まれることから、監視ホスト数によっては、十分なパフォーマンスが得られることが分かる。



TCP Monitor Traffic : 556.3 Kbps (limit unknown)

Simultaneous TCP Connections: 11 (limit unknown)

Attack Number: 100 (0.5 / sec) (limit unknown)

Detection Rate: 100%

図. 実験結果

4. まとめ

ネットワーク侵入検出のための手法、対象データ、及びアーキテクチャを整理分析するとともに、これらを動的に切り替えることで効率的な検出を行うシステムのを提案した。実運用下における評価及び、異常検出部の実装による未知の攻撃に対する対処能力の向上が今後の課題である。

5. Reference

[1]Amoroso, EG. Intrusion Detection : an introduction to Internet surveillance, correlation, trace-back, traps, and response. Intrusion.Net Book : Sparta, NJ. 1999.

[2]Denning, DE. An intrusion-detection model. IEEE Transactions on Software Engineering. Vol. SE-13. No2. pp. 222-32. 1987.

[3]Kumar, S. "Classification and Detection of Computer Intrusions." Department of Computer Sciences, Purdue Universit Ph.D. Dissertation. 1995.

[4]Ghosh, AK., J. Wanken, and F. Charron. Detecting anomalous and unknown intrusions against programs. Proceedings 14th Annual Computer Security Applications Conference. IEEE Comput. Soc. pp. 259-67. 1998.

[5]Forrest, S., S. A. Hofmeyr, and A. Somayaji. Computer immunology. Communication of the ACM. vol.40, no.10pp.88-96. vol.40, no.10pp.88-96. 1997.

[6]Shieh, S. and Gligor, VD. On a pattern-oriented model for intrusion detection. IEEE Transaction on Knowledge and Data Engineering. vol.9. no.4 pp.661-7. 1997.

[7]Schepers, F. Network-versus host-based intrusion detection. Information Security Technical Report. Elsevier Science. Vol3, No.4. 1998.

[8]武田圭史, Packet Monster - A Packet Monitor, 1999 http://www.sfc.keio.ac.jp/~keiji/ids/pakemon/