2W-09

ハニーポットへの攻撃に対するNIDS検知反応を利用したシグネチャの自動チューニング

大橋 宗治 †　長谷川 皓一 ††　山口 由紀子 †††　嶋田 創 †††

† 名古屋大学工学部電気電子情報工学科　†† 名古屋大学情報戦略室　††† 名古屋大学情報基盤センター

1 はじめに

インターネットでは様々な脅威が存在し、一般的なセキュリティ対策のひとつとしてシグネチャをベースとしたネットワーク型侵入検知システム（NIDS）が広く使われている。しかしシグネチャの数は膨大であり適切に設定することは難しく、日々変化する攻撃の傾向にも対処する必要があるため運用コストが高い。本研究では複数のハニーポット及び、これに対する攻撃観測用 NIDS 環境を構築し、得られた統計データをもとに運用中の NIDS のシグネチャチューニングを行う手法を提案する。

2 既存システムとその課題

IDS とはネットワークに流れるパケットを監視し、不正アクセスを検知し管理者へ通知するシステムである。本研究では、シグネチャとしてあらかじめ定義された不正パターンと監視対象のパケットとのパターンマッチングにより不正アクセスを検知するシグネチャ型 NIDS（以下、IDS）を用いる。IDS は一般的なセキュリティ対策である一方で、監視対象のパケットに対し個々のシグネチャとパターンマッチングを行うため、通信量の多い環境下ではパフォーマンスの低下に伴うパケットロスを引き起こす可能性がある。そのため、環境に応じたシグネチャのチューニングを行う必要があるが、一般的にシグネチャの数は膨大であり、これらを適切に設定することは難しい。また、日々変化する攻撃の傾向にも対応する必要があるため IDS は専門的な知識なしでチューニングすることは困難とされている。

これに対し、パターンマッチング処理の高速化に着目した研究 [1] やマルチコア上でのシグネチャ割当によるレイテンシ削減手法 [2] など、IDS の処理性能の向上に多くの研究がなされている。本研究では、シグネチャの自動チューニングにより既存システムの課題解決を目指す。

An Automated Tuning Method for NIDS Signature based on NIDS Alerts of Attack on Honeypots

Shuji OHASHI† Hirokazu HASEGAWA†† Yukiko YAMAGUCHI††† Hajime SHIMADA†††

†Graduate School of Information Science, Nagoya University

††Information Strategy Office, Nagoya University

†††Information Technology Center, Nagoya University

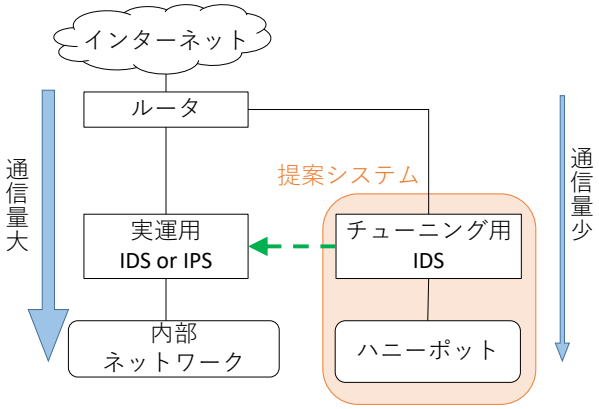

図 1: 提案手法

3 提案手法

本研究では実際に発生している攻撃の傾向を分析し、これを IDS に反映させることでチューニングを行う手法を提案する。提案システムの構成図を図 1 に示す。運用中のネットワークと同条件のセグメントを用意し、攻撃収集用のハニーポットおよび、これに対する攻撃を分析するためのチューニング用 IDS を設置する。

一般的にハニーポットのログは分析が難しく、ここから有用な攻撃情報を抽出し IDS のシグネチャを作成、選択することは困難である。そのため、ハニーポットでは攻撃の収集のみを行い、チューニング用 IDS により攻撃の分析を行う。ネームサーバに登録されていないハニーポットは、一般的にそれらがされている実運用サーバよりも通信量は少ないため、チューニング用 IDS は実運用 IDS よりも負荷が少なく、多くのシグネチャを適用させることができると考えられる。そこで、チューニング用 IDS には多くのシグネチャを適用させておき、ここで得られた統計データをもと選別されたシグネチャセットを実運用 IDS に反映させる。

4 検証実験

図 2 に示す実験環境を構築し、提案システムの検証を行った。IDS にはオープンソースの IDS である Suricata 4.03[1]、ハニーポットには低対話型ハニーポットであ

[1]Suricata Open Source IDS/IPS/NSM engine https://suricata.org

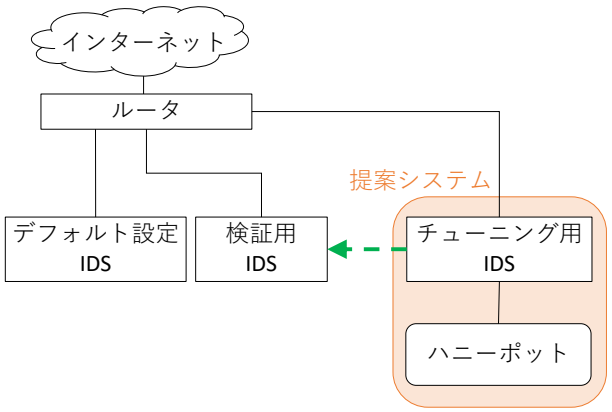

図 2: 実験環境

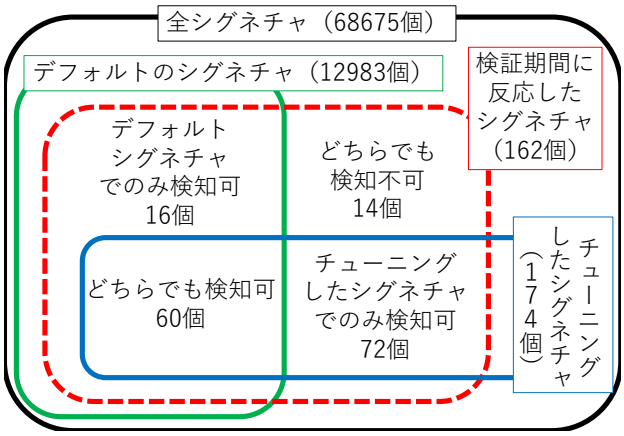

図 3: 実験結果

る T-pot、Glastopf、cowrie、dionaea の 4 種類を使用した。これらのハニーポットでは 22(ss)、42(nameserver)、80(http)、443(https)、5060(sip)、8081(blackice-icecap)、9200(wap-wsp) のポートに対する攻撃を待ち受けるよう設定した。

チューニング用 IDS では Suricata で使用することのできる公式のシグネチャセットである Emerging Threat rules[1] と Snort VRT rules[2] を用いる。これらのうち実験段階において最新である Emerging Threat rules（12/21 更新, version.8796）と Snort VRT rules（snortruless-snapshot-29110）に含まれる約 7 万個のすべてのシグネチャを使用する。今回の実験では、この約 7 万個のシグネチャから一定期間ハニーポットに対して行われた攻撃への検知反応を示した全てのシグネチャを抽出し構成したシグネチャセットを適用した検証用 IDS をチューニング済み IDS として設置した。比較対象として、デフォルト設定の Suricata を設置した。デフォルト設定では約 1 万個のシグネチャが適用されていた。

5 実験結果

2017 年 12 月 23 日から 26 日までの期間において、チューニング用データの収集を行った。ここで得られた結果をもとにチューニングを行った検証用 IDS、デフォルト設定 IDS、およびチューニング用 IDS を 12 月 27 日から 29 日までの検証期間に稼働させ、3 台の検知結果を比較した。

図 3 に実験で得られたシグネチャの個数の関係を示す。まず、デフォルト設定のシグネチャ数 12983 個に対し、チューニングを行った結果 174 個に減少しており、約 98.7%の削減をしている。次に、検証期間において反応を示した 162 個のシグネチャに対し、チューニングした IDS では 132 個が検知され、見逃し率は約 18.5%であった。対して、デフォルト設定では 76 個が検知され、見逃し率は約 53.1%であり、チューニングにより 34.6 ポイントの見逃し率の改善が見られた。また、各シグネチャに定義された全 3 段階の攻撃の危険度に着目すると、デフォルト設定により検知できなかった 86 個のシグネチャのうち、21 個のシグネチャは最も危険度の高いものであった。一方で、チューニングされたシグネチャセットで検知できなかった 30 個のうち、最も危険度が高いものは 2 個のみであったことから、実際の攻撃の傾向に即したチューニングが行えたと考えられる。

6 おわりに

本研究では、ハニーポットと IDS を用いたシグネチャの自動チューニング手法を提案した。実験環境において検証した結果、デフォルト設定のシグネチャセットと比較して少数のシグネチャセットで危険な攻撃の見逃し率を抑えたチューニングを行うことが可能であった。今後は、より精度を向上させるため、検証用の IDS で検知されたシグネチャのみならず、これに関連するシグネチャを取り入れるといった検討を行っていく。

参考文献

[1] 林經正ほか, ”Snort を用いた侵入防止システムの構築と侵入検知処理高速化の検討, ” 情報処理学会研究報告, 2003-CSEC-021, pp.59-64, 2003.

[2] 山田正平ほか, ”不正侵入検知システムにおけるマルチコア上でのシグネチャ割当によるレイテンシ削減手法, ” 情報処理学会研究報告, 2014-ARC-209, No.2, pp.1-8, 2014.

[1]EMERGING THREATS https://rules.emergingthreats.net
[2]Snort https://www.snort.org