4E-04

WAFの動的選択によるコスト上昇を抑えた検知範囲拡充手法の検討

寺本 泰大† 岸 寿春† 永渕 幸雄† 小山 高明† 北爪 秀雄†
†日本電信電話株式会社 NTT セキュアプラットフォーム研究所

1 はじめに

近年，Webサイトに対するサイバー攻撃によって，機密情報の流出，Webサイトの不正改竄，サービスのダウン等様々な被害が続出している．サイバー攻撃の被害を受けると，システムの復旧および被害状況の確認や利用者に対する補償によって多大な損害を被る可能性があるため，攻撃を未然に防ぐ事が重要である．

サイバー攻撃からWebサイトを守るための製品として，WAF (Web Application Firewall) が存在する．WAFは主にWeb (L7のHTTP) を対象としたFirewallであり，一般的なL4レイヤーまでを対象としたFirewallと比較し，HTTPリクエストの入力パラメーターを分析する事が可能である．

しかし，WAFは全ての攻撃を検知することは出来ずに攻撃を見逃す事があり，どの攻撃を見逃すかは製品毎に異なる．我々は，市中WAF製品2製品に対して攻撃試験を行う事により，攻撃の見逃しには製品毎に特徴がある事を確認した．

つまり，複数の製品を同時に利用する事により，製品の攻撃見逃しを削減する事が可能である．しかし，単に複数製品を同時に利用した場合，1リクエストあたりの利用製品数が増大し，製品台数に応じて機器コストがリニアに上昇する問題がある．

そこで，本稿では，HTTPリクエストを分析し，リクエスト毎に複数のWAF製品の中から攻撃の検知のために必要なWAF製品のみを動的に選択し，1リクエストあたりの製品の平均利用台数を削減する事により，検知率を向上させつつも機器コストのリニアな上昇を抑える手法について提案し，評価実験を行った．

2 提案手法

本章では，複数WAFによって検知漏れを削減する場合における，課題および解決手法について検討を行う．

複数のセキュリティ製品を用いた研究や技術として，SIEM[1] 等が存在し，複数機器を用いる事により，検知性能が向上するという事が示されている．一方，複数機器を同時利用する場合，利用台数に応じて機器コストが上昇するという課題が存在する．しかし，SIEM等の研究では固定的な構成においての複数機器の検知結果を用いて検知性能を向上させる事を目的としており，機器コストについては研究対象とはされておらず，またログやアラートといった事後の結果のみを用いているため，利用機器数を減らす事は困難である．

本研究では，上記課題の解決のために，ログだけでなく入力通信 (本研究ではHTTPリクエスト) を評価対象に加え，HTTPリクエストパターンから各WAF製品の検知結果を予測し，攻撃検知が可能と推定されるWAFのみに選択的にリクエストを振り分ける事により，1リクエストあたりの同時利用WAF台数を削減する方式を提案する．

図1のように，複数のWAF製品の中から攻撃判断に必要なWAFのみを選択する事で，複数台数のWAFを利用した場合の検知率を維持しつつ，全体のWAFの使用率 (コスト) 削減を実現する事が出来る．

例えば，毎秒100リクエストを処理可能なWAFが2台存在した場合，2台を同時利用すると毎秒処理可能なリクエスト数は100リクエストであるが，常に最適な機器1台を選択する事が可能ならば，毎秒最大200リクエストを処理可能となる (WAF選択装置の性能が十分にあると仮定した場合)．特にデータセンターやIaaS等の複数テナントがWAFを利用するような環境においては，WAFを共有し，テナントごとに必要な機器を動的に選択して利用する事により，1リクエストあたりの利用WAF台数を大幅に削減可能であると考えられる．

本研究では，リクエストから機器を動的に選択するために，機械学習を用い，HTTPリクエストとWAFの検知可否を学習する事により，新たなリクエストに対してWAFが攻撃として検知するかどうかのスコアリングを行う．出力スコアが一定の閾値を越えたもの，つまり検知可能であると判断したWAFの組み合わせだけリクエストを振り分ける．

本研究では機械学習の識別器として，SVM (Support Vector Machine) [2] および文字列カーネルであるSubsequence String Kernel(SSK) [3] を用いた．

3 評価実験

本研究では，市中WAF2製品 (製品A, 製品Bとする) を用いて評価実験を行った．各製品の検知ルールは共に推奨シグネチャセットを利用し，純粋な検知率の測

†Yusuhiro Teramoto †Yukio Nagafuchi †Toshiharu Kishi †Takaaki Koyama †Hideo Kitazume
†NTT Secure Platform Laboratories, NTT

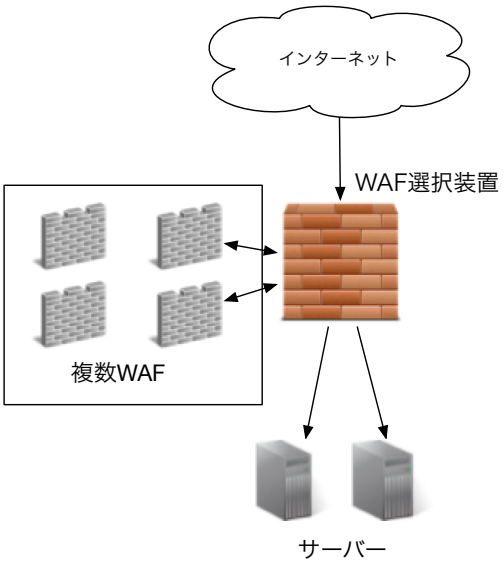

図 1: 最適 WAF 選択

定のために，プロファイリングや誤検知の学習は行わなかった．評価対象は，検知率と 1 リクエストあたりの平均機器使用数とし，誤検知率については評価対象外とした．

また，評価実験を行うための試験用データセットとして，脆弱性情報サイトである Exploit Database [4] から，識別器の訓練用として 1 製品のみが検知可能な攻撃 200 件ずつ (合計 400 件)，評価実験試験用として上記 400 件を含まない攻撃 1000 件の攻撃 1400 件を無作為に抽出した．

表 1 は，本研究で提案する動的機器選択を行わなかった場合の検知率である．動的に機器選択を行わない場合，常に固定的な構成においてリクエスト処理を行う．表 2 は，閾値を変化させ動的機器選択を行った場合の検知率である．動的に機器選択を行った場合，2 台の製品のうち 1 台以上の製品を用いてリクエストの攻撃判定を行う．

動的機器選択を行った場合，

表 1: 検知率 (機器選択無)

製品	A	B	A+B
平均機器数 (台/req)	1	1	2
検知率 (TPR[%]])	85.1	85.0	90.6

表 2: 検知率 (機器選択有)

閾値	0.0	0.4	1.0	∞
平均機器数 (台/req)	1.0	1.1	1.4	2.0
検知率 (TPR[%]])	89.6	90.0	90.4	90.6

4 考察

評価実験の結果常に単一の機器を選択した場合についても，常に一つの機器を利用した場合と比較し，検知率が 4.5〜4.6%向上し，機器選択アルゴリズムの効果がある事を確認した．また，閾値を変化させ，複数機器への振り分けを許容する事で，1 リクエストあたりの平均機器使用台数 1.4 台 (2 台同時利用の 70%のコスト) で 90.4%の機器選択精度となり，2 台同時利用時の 90.6%と比較し 0.2%の差の検知率を実現した．本研究によって用いたデータセットは，脆弱性情報サイトより無作為に抽出した攻撃であるため，既知の攻撃に対しては同等の検知性能があると考えられる．以上により，WAF コストを上昇を抑制しながら，複数台数の WAF 同時利用に近い検知率を実現可能である事を示した．

5 まとめ

本研究では，複数台の WAF を選択的に利用する事で，WAF の同時利用台数を抑えながらも，検知率を向上させる方式について提案を行った．さらに脆弱性情報サイトから攻撃情報を抽出する事で，データセットを作成し，機器選択アルゴリズムの評価を行い，提案方式の効果を確認した．

本稿では市中 WAF2 製品を用いた場合の検知率について測定を行ったが，今後は 3 台以上の WAF を用いた場合，市中製品と比較し低コストであるが検知性能も低いオープンソース WAF を用いた場合についても評価を行う予定である．また，本稿では対象外としていた誤検知率についても今後評価を行う予定である．

参考文献

[1] 針生 剛男, 秋山 満昭, 青木 一史, “進化するマルウェア等によるサイバー攻撃の検知・解析・対策技術”, NTT 技術ジャーナル 2012, pp.13-17, Aug. 2012.

[2] Bernhard E. Boser, Isabelle Guyon, Vladimir Vapnik, “A Training Algorithm for Optimal Margin Classifiers”, COLT 1992, pp.144-152, Jul.1992

[3] Huma Lodhi, Craig Saunders, John Shawe-Taylor, Nello Cristianini, Christopher J. C. H. Watkins, “Text Classification using String Kernels”, Journal of Machine Learning Research 2002, pp.419-444

[4] OffensiveSecurity Exploits Database: https://www.exploit-db.com/