5E-4

SVMを用いたWAFへの異常検知機能の実装と評価

伊波靖† 高良富夫‡
† 沖縄工業高等専門学校メディア情報工学科 ‡ 琉球大学工学部情報工学科

1 はじめに

近年，様々な分野においてWebアプリケーションの利用が増える一方で，Cross-Site Scripting（XSS）攻撃やSQLインジェクション攻撃による情報漏えいなどの深刻な被害が報告されている [1]．Webアプリケーションをそれらの攻撃から守る方法の一つに，Web Application Firewall(WAF) の使用があるが，WAFは，未知の入力値検査に問題を抱えている．そこで我々は，WAFの入力値検査にSVMを利用し，False Positiveを低減させながらも，未知の攻撃を検知出来る手法を提案し，実験によりその有効性を示した [2]．本研究では，我々が提案した手法をApacheのモジュールとして実装し，性能を評価するためにApacheの標準的なWAFであるModSecurityとの比較実験を行い，その結果から有効性を議論する．

2 Web Application Firewall(WAF)

WAFとは，Webアプリケーションを含むWebサイトと利用者の間で交わされるHTTPによる通信を検査し，攻撃などの不正な通信を自動的に遮断するソフトウェア，もしくはハードウェアである．本研究では，WAFの機能の中でもXSSやSQLインジェクションの脆弱性対策の基本となる入力値検査の問題について考える．パターンマッチングに基づくWAFでは，ホワイトリストとブラックリストが用いられる．入力値検査におけるホワイトリストは，入力可能なパラメタ全てを設定することが難しく，また手間もかかる上，設定漏れの可能性もある．一方，ブラックリストは，既知の攻撃であれば問題ないが，未知の攻撃に対しては攻撃を見逃す検知漏れの可能性がある．

Apache用のWAFとしてはModSecurityが広く利用されている．ModSecurityは，Apacheのモジュールとして動作し，正規表現等により記述されたルールに基づいてパターンマッチングを行うオープンソースのWAFである．

3 Support Vector Machine(SVM)

SVMは統計的学習理論に基づく新しい2クラスのパターン認識手法であり，ニューラルネットワークなどの従来法と比較して汎化能力が高い点と最適解が求まる点に特徴があり，学習に用いていないデータに対しても高い識別率を示す．SVMがこのような特徴を示すのは，その学習に認識誤りと汎化性能の両面から最適化が行われ，これが2次の凸計画問題として定式化されているため最適解を求める事ができるためである [3]．

SVMは学習の最適解として求められた分離超平面による線形識別を行っているが，学習用データを線形分離することが不適切な場合，学習データを元のパターン空間からより高次のパターン空間に非線形写像を行い高次元空間で分離超平面を構築し線形識別を行う．

4 SVMを用いたWAFへの異常検知機能の実装

4.1 提案手法

我々のこれまでの研究においてWAFの入力値検査にSVMを利用する手法を提案した．具体的には，ホワイトリストとブラックリストから得られたN-gramとN-gramの共起頻度をSVMに与えるデータの特徴ベクトルとし，あらかじめ作成した学習用データを用いてSVMを学習させ，2クラスのパターン識別器を構成する．次に，このパターン識別器により入力値の異常検知を行うものである．

4.2 Apacheのモジュールとしての実装

本研究では我々が提案したSVMを利用する異常検知手法をApacheのモジュールとしてLIBSVMを用いて実装した．予めSVMへ学習データを与えて構築したSVMのモデルデータをモジュールの初期化処理において読み込みパターン識別器を構成する．Apacheへのhookには，ap_hook_access_chekerを用いることで，ユーザからの全てのリクエストをモジュールで受け取ることが可能となる．hook関数において受け取ったリクエストデータ内のqueryデータをN-gram法により特徴ベクトル化しSVMによるパターン識別機で異常検知を行う．

5 評価実験

5.1 実験用データセット

ブラックリストのデータとしてXSS，SQLインジェクションを合わせて3200個用意し，1600個を学習用，1600個を評価用データとした．また，ホワイトリストのデータは，Webアプリケーションに入力されると考えられるデータを名前，住所，メッセージ，電話番号，パスワードの5つのカテゴリーに分類し，合わせて2600個用意し，1300個を学習用，1300個を評価用データとした．なお，名前，住所，メッセージについては，日本語と英語のデータ両方を用意した．

Implementation and Evaluation of anomaly detection Using SVM for WAF.

†Yasushi IHA (yasuc@okinawa-ct.ac.jp)
‡Tomio TAKARA (takara@ie.u-ryukyu.ac.jp)
†Department of Media Information Engineering, Okinawa National College of Technology
‡Department of Information Engineering, University of The Ryukyus

表 1: 予備実験結果

	ブラックリスト	ホワイトリスト	総合
学習用データ	100%	100%	100%
評価用データ	99.5%	99.77%	99.62%

表 2: 評価実験結果

	ブラックリスト	ホワイトリスト	総合
学習用データ	100%	100%	100%
評価用データ	99.69%	99.69%	99.69%

表 3: ModSecurity による実験結果

	ブラックリスト	ホワイトリスト	総合
学習用データ	87.31%	60.92%	75.48%
評価用データ	87.44%	52.46%	71.76%

表 4: 処理能力の評価実験結果

	ブラックリスト	ブラックリスト
SVM WAF	1.268ms	1.288ms
ModSecurity	1.296ms	1.258ms

5.2 予備実験と結果

実装したモジュールの性能実験を行う前に SVM による認識性能を確認するために予備実験を行った．実験に使用した SVM は LIBSVM であり，カーネルには線形カーネルを用い，Solver Type は C-SVM を用いて実験を行った．また，特徴ベクトルの N-gram には N=2 の bi-gram を用いた．LIBSVM に学習データを与え SVM のモデルを構築した後，学習データと評価用データを用いて実験を行った．

実験の結果を表 1 に示す．実験結果から，未知のパターンに対しても高い識別率が確認できた．また，正常なパターンを異常なパターンとして誤認識する割合も低いことが確認できた．

5.3 識別性能の評価実験と結果

予備実験において学習データを与えて構築したモデルを用いて，実装したモジュールの評価実験を行った．また，比較のために同じデータを用いて ModSecurity でも同様の実験を行った．

実験の結果を表 2 に示す．実験結果から，予備実験同様に未知のパターンに対する高い識別率と正常なパターンを異常なパターンとして誤識別する割合が低いことが確認できた．また，予測結果の評価尺度の一つである F 値は 0.997 と高い値となった．

次に，ModSecurity の結果を表 3 に示す．ModSecurity のルールの設定はデフォルトの状態で行ったため，識別率が低く誤識別率が高くなっている．このことから，ModSecurity の場合は，運用に際して，細かいチューニングが必要であると考えられる．

5.4 処理能力の評価実験と結果

実装したモジュールの処理能力を評価するために，Apache に付属する Apache Bench(ab) ツールを用いて実験を行った．ab は同時接続数とリクエスト数及び URL を指定することによりリクエストを発生させ，接続時間・処理時間・待ち時間などの統計を取得することで Apache の性能を測定することができる．実験は，ブラックリストおよびホワイトリストから任意に選択したパターンを 10 種類を用いて，ab の URL に選択したパターンを与えることで平均処理時間を計測した．

実験の結果を表 4 に示す．表の値は 1 リクエストあたりの平均処理時間である．実験結果から，SVM を用いた WAF は，ModSecurity とほぼ同等の処理能力であることが分かる．しかし，ModSecrity は正規表現に基づいたパターンマッチングを行っているため，今後パターンが増加したり，複雑になるとさらに速度の低下が起こると予想される．SVM を用いた WAF の場合は，プログラムのチューニングにより処理能力が向上する可能性がある．

6 まとめと今後の課題

本研究では，我々が提案した WAF の入力値検査に SVM を利用する異常検知手法を Apache のモジュールとして実装した．性能を評価するために行った実験から，False Positive を低減させながらも，未知の攻撃を高い識別率で検知出来ることを示した．また，ModSecurity との比較実験において処理能力は同等であることを示した．今後の課題としては，実環境における性能評価と SVM のさらなる検知性能向上が挙げられる．

謝辞

本研究は科研費 23500106 の助成を受けたものである．

参考文献

[1] 情報処理推進機構，JPCERT コーディネーションセンター，“ ソフトウェア等の脆弱性関連情報に関する届出状況 [2011 年第 3 四半期（7 月～9 月）] ” (2011).

[2] 伊波靖, 高良富夫:SVM を用いた WAF の検知機能の提案, 情報処理学会第 73 回全国大会講演論文集 pp.445–447 (2011).

[3] Cristianini, N. and Shawe-Taylor, J.: サポートベクターマシン入門，共立出版 (2005).