6S-08

潜在曲線を用いた着色による SQLインジェクション攻撃の特徴の可視化

藤岡 あやか[I], 松田 健[II], 園田 道夫[III], 趙 晋輝[IV]

中央大学 理工学部 情報工学科

静岡理工科大学 総合情報学部 コンピュータシステム学科

サイバー大学 IT総合学部

概要

近年インターネットサービスが社会的に重要度を増す一方，サイバー攻撃による被害が問題となっている.中でも SQL インジェクション攻撃は簡単に仕掛けることができ，かつ経済的利益に繋がるデータを窃取できるため増加傾向にあり対策が必要とされている．本研究では潜在曲線モデルを応用し入力文字列に攻撃特徴と正常特徴に着色を行い，計算的に攻撃か正常かの判断が難しい入力文字列を可視化によって攻撃検出を支援する方法を提案する.

1. はじめに

インターネットの普及によって様々な情報の管理・運用が容易になったことに伴い，システムの脆弱性を狙ったサイバー攻撃の被害が問題となっている．その攻撃方法の一種である SQL インジェクション攻撃は簡単に仕掛けることができ,かつ経済的利益に繋がるデータを窃取できるため増加傾向にあり,対策が必要とされている.

SQL インジェクション攻撃の対策は,時間的,費用的な面において現実的とされる既存のアプリケーションを大きく変更せずにすむ対策としてゼータ分布や N-gram 解析，機械学習によって入力データから攻撃を自動検知する手法が考案され，実用性も示されている[1][2]．しかしながら誤検知の問題は残っており攻撃か正常かの判断を全て自動化することは難しい．そこで解決策として本研究では入力文字列に含まれる記号に着目し,潜在曲線モデルを応用し攻撃特徴と正常特徴に色付けを行い，計算的に攻撃か正常かの判断が難しい入力文字列を，着色した画像として表現する可視化によって攻撃検出を支援する方法を提案する.

2. 事前知識

この章では本研究の考察で必要となる知識について簡潔にまとめることにする.

2.1 SQLインジェクション攻撃

SQL インジェクション攻撃とは web 上のアプリケーションを狙った攻撃の一つで，悪意のある利用者が web 上の入力欄に不正な文字列を入力することで，データベースの書き換えや情報の取得という不正な操作ができてしまう．この攻撃は入力文字列に記号が多く含まれることが特徴であるが, 入力文字列の記号だけに着目すると誤検出が多くなることが分かっている[1][2].

2.2 潜在曲線モデル

潜在曲線モデルとは構造方程式モデリングのひとつであり, 各個体から経時的に反復測定した横断的なデータを表現する観測データの変化の様子について個々と集団の変化の傾向を同時に分析する手法である.

2.3 攻撃特徴記号

本研究では学習用データの全ての攻撃文を対象に各記号の含有率を調べ, そのうち下の表に示される最も含有率の高い上位 6 つの記号を攻撃特徴記号とみなして着色の対象とした.

表 1

SP	‘	;	)	.	(

3. 提案手法

本研究では入力文字列に含まれる特徴記号に色付けを行い, 計算的に攻撃か正常かの判断が難しい入力文字列を着色した画像として表現する可視化によって攻撃検出を支援する方法を提案する.

特徴の着色は文献[4]の手法を応用し, 潜在曲線モデルを利用することで以下のように実現した. 各入力文字列の特徴記号の含有率の変動を分析し二次関数に当てはめることによって導き出した値を着色濃度として利用する. 具体的には,攻撃の場合は二次関数の最大値に RGB 値の R の 255,

Visualization of the Features of SQL Injection Attacks by Coloring Using the Potential Curve

Ⅰ Fujioka Ayaka , Chuo University

Ⅱ Matsuda Takeshi , Shizuoka Institute of Science and Technology

Ⅲ Sonoda Michio , Cyber University

Ⅳ Chao Jinhui , Chuo University

最小値に R の 0 を対応させ，正常の場合は二次関数の最大値に B の 255，最小値に B の 0 を対応させている．

潜在曲線モデルの計算は以下のように行っている．入力文字列ごとに変化していく 6 つの特徴記号の含有率 y を二次曲線$y = a_1x^2 + a_2x + a_3$に当てはめる潜在曲線モデルを考えるために、以下のモデルを定義する．

$$y = a_1^{(i)}x_i^2 + a_2^{(i)}x_i + a_3^{(i)} + \varepsilon \quad (1)$$

ここで ε は平均 0, 分散 $\sigma^2 > 0$の正規分布に従う誤差項である．観測データに外部から影響を与える変数をモデルの持つパラメータ$a_1^{(i)}, a_2^{(i)}, a_3^{(i)}$と関連を持たせることで表現するため，以下の式を定義する．

$$a_1^{(i)} = b_{11}t + b_{21} \quad (2)$$

$$a_2^{(i)} = b_{12}t + b_{22} \quad (3)$$

$$a_3^{(i)} = b_{13}t + b_{23} \quad (4)$$

本研究ではパラメータ$a_1^{(i)}, a_2^{(i)}, a_3^{(i)}$を最尤推定法で計算し，これらの結果に再び最尤推定法を適用し$b_{11}, b_{21}, b_{12}, b_{22}, b_{13}, b_{23}$を求める．

4. 結果と考察

文献[5]の情報を元に作成した攻撃ジェネレータによって生成された攻撃文と正常文に対して着色画像を作成したところ，以下のような結果が得られた．

図 1 攻撃文の着色結果

図 2 正常文の着色結果

画像は基本的に 1 行が 1 入力文字列に対応しているが，文字数の長い入力文字列は右端で折り返しているため複数行に及んでいる．

出力結果から，正常文と攻撃文では文字数全体に対して着色量に違いが確認でき，また着色された色も若干ではあるものの正常文はより青に近い色に着色され，攻撃文はより赤に近い色で着色されていることが確認できる．

5. まとめ

本研究では，入力文字列に含まれる特徴記号に色付けを行い，入力文字列を着色した画像として可視化することによって計算的に攻撃か正常かの判断が難しい入力文字列の判定を支援できることを確認した．

発展的課題として挙げられるのは，同様の可視化を XSS 攻撃などの別の攻撃に対応することが挙げられる．

謝辞

今回の研究を進めるにあたりデータや数々のご指導をいただいた松田健先生，園田道夫先生，趙晋輝先生，そして趙研究室の皆様に深く御礼申し上げます．

参考文献

[1] Oosawa,T, et al. (2014) “SQL injection attack detection method using the approximation function of zeta distribution”

[2]佐野綾子ら(2014)「SQL インジェクション攻撃に含まれる文字の出現頻度とその関連性の解析による攻撃検出方法の提案」

[3] 潜在曲線モデルの解説 – 行動統計科学研分野 <http://bm.hus.osakau.ac.jp/~kano/research/application/gasshuku02/LCA.pdf>(最終閲覧 2014/12/21)

[4] 松田健 (2014) 「潜在曲線モデルを用いた能動的学習態度の推定」 情報処理学会研究報告

[5] SQL Injection Cheat Sheet <http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>(最終閲覧 2014/12/21)