5K-7

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

氏　名　　佐野　綾子[I]，　松田　健[II]，　園田　道夫[III]，　趙　晋輝[IV]
所　属　　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

1. はじめに

SQL インジェクション攻撃とは,アプリケーションのデータベース問い合わせの際に SQL 文の一部をそのパラメータとして不正に与えることにより,データベース内の情報を参照したり,改ざんしたりする攻撃である.この攻撃に対する現状の対策として，主にブラックリスト・ホワイトリスト方式を用いて攻撃を検知するという手法がとられているが,新たな攻撃が開発されると対応に遅れが生じたり,攻撃でない文字列も攻撃と判定したりすることなどの欠点もあり対策としては十分でないといえる.

そこで本研究では，既知の攻撃はもちろん，未知の攻撃も正しく検知することを目的として,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手法を提案した.SQL インジェクション攻撃に含まれる文字同士の関連性を調べるために，自然言語処理でよく利用されている Ngram 解析を利用した．また，Ngram 解析の結果から条件付き確率を算出し，
その値を用いて入力された文字列が攻撃かどうか判別する．実験の結果，攻撃文字列,通常文字列，共に高い確率で正しく検知することに成功した.

2. SQL インジェクション攻撃の例

SQL インジェクション攻撃の分類は例えば，文献[1]で行われているが，ここではその中からいくつかの SQL インジェクション攻撃の例を紹介する.

以下の攻撃は常に真となる論理式が挿入されているところを特徴とする攻撃である.

' or 1=1--

この攻撃はログイン認証を回避するために用いられる.

;DROP members --

この攻撃は，任意に悪意のある SQL 文を追加することで，例えばデータベースにある情報を削除するためなどに用いられる．SQL インジェクション攻撃にはその他多くの攻撃手法が存在するが，文献[2]などによって SQL インジェクション攻撃にはある特定の文字や記号が多く含まれることが指摘されている．そこで本研究では,SQL インジェクション攻撃に含まれる記号や文字に着目し，それらの関連性について調べ，攻撃を検知する手法を提案する.

3.提案手法

本研究では，Ngram 解析とベイズの定理を利用し,テストデータが攻撃,正常のどちらである可能性がより高いかを判定する方法を提案する.以下，そのための準備を行う．ただし，N が 3 の場合から，攻撃検知の精度が悪化する傾向にあったため，本研究では N=2 として扱うことにする.

提案する攻撃検知法は以下の通りである.

SQL injection attack detection method by the frequency analysis
I Sano Ayako, Chuo University
II Matsuda Takeshi, Shizuoka Institute of Science and Technology
III Sonoda Michio, Cyber University
IV Chao Jinhui, Chuo University

Copyright ©2014 Information Processing Society of Japan.
All Rights Reserved.

(1) 正常と攻撃の訓練データを準備する
(2) 正常データを 2gram 解析し，得られた文字片ごとの出現回数を数え，正常データに対しそれらの文字列片が出現する確率を P(N)とする
(3) 攻撃データにも(2)と同様の作業を行い，攻撃データに対して 2gram 解析の結果得られた文字列片が出現する確率を P(A)とする．
(4) P(N|S)を入力文字列 S が正常である確率，P(A|S)を S が攻撃である確率と定義し，以下の式からこれらの値を算出する．

$$P(N|S) = \frac{P(S|N)P(N)}{P(S)}$$

$$P(A|S) = \frac{P(S|A)P(A)}{P(S)}$$

ここで P(S|N)や P(S|A)は 1gram 分析の場合は内部ベイズと同様の方法で計算し，2gram 分析の場合は，文字列 S を文字列片に分解したあと，その前後の出現頻度をもとに条件付き確率を計算して計算することとする．なお，文字列 S に関する分布 P(S)は，訓練データに依存しすぎてしまうのを防ぐため，事前知識として特徴的な文字片の出現確率を調整するために利用した．

5. 実験結果

前章で提案した攻撃検知手法の有効性を確認するため，初めに 100 個の正常訓練データと 100 個の攻撃訓練データを用意し，P(N)と P(A)の値を算出した．次に，試験用のデータを以下の通り準備し，前章の(4)式を計算することで試験用データの検知を行った．

【正常データ】
DataA：試験用正常データ集合 A（1000 個）
DataB：試験用正常データ集合 B（1000 個）

【攻撃データ】
Data1：試験用攻撃データ集合 1（1000 個）
Data2：試験用攻撃データ集合 2（1000 個）

上記４つのデータ集合に対し，以下の 4 パターンの解析を試みた．その結果を図１，２に示す．

a.テストデータから記号のみを抽出し,1gram 解析を行う
b.テストデータの内アルファベットと記号を抽出し,1gram 解析を行う
c.テストデータから記号のみを抽出し,2gram 解析を行う
d.テストデータの内アルファベットと記号を抽出し,2gram 解析を行う

Normal	DataA	DataB	平均
a	74.6	72.3	73.45
b	80.5	79.9	80.20
c	82.1	82.5	82.3
d	92.7	93.8	93.25

図１　試験用正常データ集合の検知率(単位:%)

Attack	Data1	Data2	平均
a	97.6	98.2	97.94
b	98.6	96.1	96.58
c	95.2	96.8	96.11
d	97.4	96.9	96.83

図２　試験用攻撃データ集合の検知率(単位:%)

以上の結果から,1gram 解析を行った場合，正常検知では，記号だけを用いて特徴抽出を行うより，アルファベットを混ぜて特徴抽出を行う方がより確実に検知できるが，攻撃検知では若干検知精度が悪化するという結果が得られた．一方で，2gram 解析を行った場合，正常検知，攻撃検知ともにその検出率が向上することがこの実験では確認することができた．この結果は，SQL インジェクション攻撃を検知するには，文字列に含まれる記号だけを見るよりも，その記号の前後に出現する記号や文字との関連性を用いて攻撃を検知する方がより確実に攻撃検知できる可能性があることを示していると考えられる．

参考文献

[1] Kumar, P and Pateriya, R.K."A survey on SQL injection attacks, detection and prevention techniques" International Conference on Computing Communication & Networking Technologies,pp.1-5, 2012
[2]Takeshi Matsuda, Feature of SQL Injection Attacks and Zeta Distribution, FIT2013.

Copyright ©2014 Information Processing Society of Japan.
All Rights Reserved.