Vol.2020-MPS-127 No.17
2020/3/2

アセンブラ命令遷移グラフを用いたバッファオーバーフロー攻撃検知手法の提案

小林 勇希[1]　松田 健[2]　園田 道夫[3]　趙 晋輝[1]

概要：バッファオーバーフロー攻撃は，プログラムで用意された領域を超えるデータを送ることで本来想定していない領域を上書きし，情報を不正に操作する攻撃である．侵入検知システムにおいて既知の攻撃の特徴を利用するシグネチャマッチング方式等が研究されてきたが，シェルコードのパターンが無数に作成可能であることから全ての攻撃の検知は難しい．本研究では，バッファオーバーフロー攻撃を解析し，攻撃に含まれるシェルコードのアセンブラ命令遷移に着目した遷移グラフを作成し攻撃データに特有なグラフ形状を求め、それを活用した攻撃検知手法の提案を行う。

1. 序論

近年，急速なインターネットの普及に伴いインターネットを標的にしたサイバー攻撃も増加傾向にある．バッファオーバーフロー攻撃は不正アクセスを引き起こすサイバー攻撃の一種であり，今まで様々な対策手法が提案されてきたが，それらをすり抜ける攻撃の登場などにより近年においても攻撃による被害が多数発生している．

本研究では，攻撃に使用されるシェルコードをはじめとしたアセンブラ命令の命令遷移情報を用いた遷移グラフを作成し，それらのグラフ形状やグラフ特徴量を利用することで，バッファオーバーフロー攻撃を検知する手法の提案を行い，攻撃データを用いた検知実験の結果に対する考察を行った．

2. 既存の対策手法と従来研究

よく知られた既存手法として攻撃特徴を登録したデータベースとパケットの比較による検知が存在するが，誤検知が発生しやすく，また未知データの検知ができない問題がある．

従来研究においては，北條ら [1] の手法は検知できるシェルコードの種類が限られることやシミュレーションを実装する手間が問題であり，Zhao ら [2] の手法はコードの命令の順序によって検知できない問題があり，南後ら [3] の手法は誤検知の問題などがある．

3. 提案手法

本研究で提案する手法は，攻撃に使用されるシェルコードをはじめとしたアセンブラ命令の命令遷移情報を用いた遷移グラフを作成し，それらのグラフ形状やグラフ特徴量を利用することで，バッファオーバーフロー攻撃を検知することを目的とする．

3.1 命令遷移の出現頻度の算出

遷移グラフを作成するための前準備として，それぞれのコードにおけるアセンブラ命令遷移の出現頻度を求める．

3.2 遷移グラフの作成

本研究で作成する遷移グラフは頂点がアセンブラ命令，辺が命令遷移を意味する．本研究では遷移グラフを 2 種類作成し，いずれも攻撃コード，正常コードに対応した 2 つの遷移グラフを作成する．

3.2.1 力指向グラフの作成

力指向グラフ描画アルゴリズムは，力学モデルを使用したグラフ描画手法を用い，グラフの頂点と辺に対し仮想的な力を割り当てて力学的エネルギーが安定する状態をグラフとして表す．

3.2.2 格子グラフの作成

この方法では攻撃コードと正常コードで出現したアセンブラ命令を列挙し，それぞれにおいて出現頻度が高い命令遷移ほど中心に位置するように格子状に頂点を配置する．

3.3 格子グラフを用いた攻撃コード検知実験

本研究では，3.2.2 で作成した格子グラフを拡張して用いることで，新たに用意した攻撃コードの命令遷移情報を攻撃格子グラフと正常格子グラフのそれぞれに適用し，グラフ特徴を比較する実験を行う．格子グラフの拡張として，攻撃・正常コードの格子グラフそれぞれに対して，どちらか片方でしか現れていない命令を，現れていない方のグラフへ頂点として追加し，グラフから辺を削除した頂点の並びを用いる．

新たな格子グラフを作成したら，各実験データごとに

[1] 中央大学
[2] 長崎県立大学
[3] 情報通信研究機構

グラフ特徴量を比較する．ここで，本研究で使用するグラフ特徴量 F は，(a,b) を始点が a，終点が b である辺として，実験データにおける辺集合を E，辺の出現頻度を $freq(a,b)$，辺を構成する 2 頂点間の距離を $dist(a,b)$，辺を構成する各頂点のグラフ中心からの距離を $C(a)$，$C(b)$ とすると以下の式で表される．

$$F = \sum_{(a,b)\in E} freq(a,b)dist(a,b)(C(a)+C(b))$$

この特徴量はグラフが中心に集約するほど小さくなるため，2 種類の格子グラフで比較したときに，攻撃格子グラフの特徴量のほうが小さくなるデータを攻撃コードであると判断する．

4. 実装結果

本研究では，攻撃コードとしてシェルコードデータベースの exploit db に存在するシェルコード 20 個，正常コードとして自作 C プログラム 4 個の命令遷移情報を使用した．

4.1 命令遷移の出現頻度の算出

表 1 に攻撃・正常コードにおける出現頻度上位 5 つの命令遷移を示す．

表 1 アセンブラ命令出現頻度上位 5 遷移

攻撃コード			正常コード		
遷移元	遷移先	頻度	遷移元	遷移先	頻度
push	push	0.108	mov	mov	0.157
push	mov	0.106	mov	callq	0.068
mov	push	0.074	push	mov	0.037
push	pop	0.068	call1	mov	0.034
mov	int	0.065	mov	push	0.030

4.2 遷移グラフの作成

グラフの辺は出現頻度によって色付けを行い，頻度が高いものは赤色，低いものは青色に着色している．

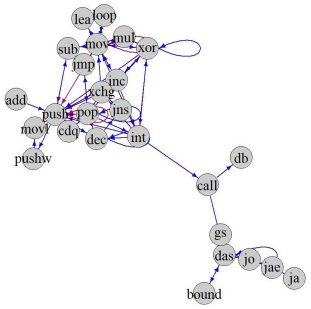

図 1 攻撃コードの力指向グラフ

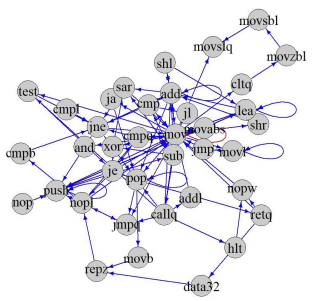

図 2 正常コードの力指向グラフ

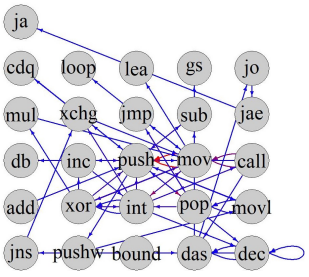

図 3 攻撃コードの格子グラフ

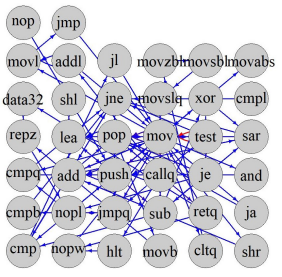

図 4 正常コードの格子グラフ

4.3 格子グラフを用いた攻撃コード検知実験

実験結果を表 2 に示す．また実験結果のうち，例としてデータ 1 に対応する遷移グラフを図 5, 図 6 に示す．

表 2 攻撃検知実験結果

データ	特徴量		攻撃判定
	攻撃格子グラフ	正常格子グラフ	
1	4.2709	9.8125	攻撃
2	4.0217	11.8696	攻撃
3	5.1350	11.6483	攻撃
4	5.1348	7.6133	攻撃
5	5.1578	10.1187	攻撃

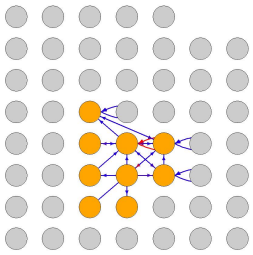

図 5 データ 1：攻撃格子グラフ

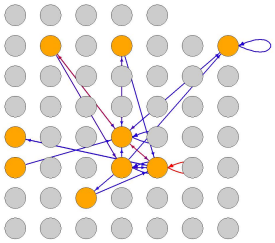

図 6 データ 1：正常格子グラフ

5. 考察

検知実験において 5 つの攻撃コードに対していずれも正しい攻撃判定をすることができた．しかし，本研究で使用した格子グラフにおいては，攻撃コードと正常コードにおいて重要な役割を占める push 命令と mov 命令がいずれもグラフの中心近くに存在してしまっていたため，特徴量における差異が小さいものとなっていた．また，検知実験で使用したデータ 4 においては特徴量の差が他の攻撃データと比較して小さく，誤検知の発生する恐れのあるデータであったことがわかる．

6. 結論

本研究の提案手法による命令遷移の出現頻度とグラフ形状の特徴を取り入れた特徴量を使用することで，検知実験において攻撃コードを正確に判定することができたが，グラフ作成の際に問題となる点がいくつか現れた．今後の課題として，攻撃コードと正常コードに出現する命令群の更なる調査，攻撃検知に使用する格子グラフにおけるより正確な特徴量が現れる頂点配置の方法の提案，同一命令間の遷移に焦点を当てたグラフ特徴量の作成が挙げられる．

参考文献

[1] 北條 孝佳，佐久間 英夫，種茂 文之: シェルコード解析による不正アクセス検出手法，情報処理学会研究報告 2003-CSEC-23，2003.

[2] Ziming Zhao, Gail-Joon Ahn: **Using Instruction Sequence Abstraction for Shellcode Detection and Attribution**, 2013 IEEE Conference on Communications and Network Security, 2013.

[3] 南後吉秀，松田健，園田道夫，趙晋輝: アセンブラ命令の出現頻度に着目したバッファオーバーフロー攻撃の検地とその考察，情報処理学会第 79 回全国大会，2017.