アセンブラ命令ペアの出現頻度に基づく バッファオーバーフロー攻撃の検知に関する研究

Detection of Buffer Overflow Attacks Based on Frequency of Assembler Instruction Pairs

南後 吉秀 / 法制・倫理分科会 / 中央大学

Abstract

Buffer overflow attacks are attacks that cause unauthorized access to the system and occur when data exceeding the allowable range is sent to the secured memory area. It is important to consider countermeasures against unknown attacks, due to the development of attacks that evade existing methods and the occurrence of risks in embedded software. In this research, we analyze the frequency by focusing on the order of assembler instruction sequences, and propose a method to detect buffer overflow attacks based on the similarity.

1. 研究背景

・ネットワーク上でのサイバー攻撃の増加
　バッファオーバーフロー攻撃がその原因の1つ
・バッファオーバーフロー (Buffer Overflow)
　―良く知られているセキュリティホールの一種
　―DoS攻撃やDDoS攻撃の原因

2. 研究目的

　インテルx86アーキテクチャ環境下におけるアセンブラ命令列の解析，および類似度の比較を通して，バッファオーバーフロー攻撃を検知する．

3. 代表的な既存手法：侵入検知システムの利用

・シグネチャマッチング方式が用いられている．
　→パターンマッチングによる攻撃検知
・シグネチャの中身は?
　―セキュリティホールに対する攻撃パケットの固有な部分
　―攻撃の根幹をなすシェルコードと呼ばれる部分の特徴的な部分に関わるもの
・なぜダメか?
　―未知のセキュリティホールを検知できない．
　―シェルコードのパターンが無数に作成可能であるため，すべての攻撃の検知が原理的に不可能である．
　―導入時の設定が難しい．

4. 本研究での提案手法

・攻撃コードに頻出するアセンブラ命令への着目
　int命令・lea命令・mov命令・pop命令・push命令・xor命令の6つに着目する．
・近傍を考慮したアセンブラ命令ペア頻度解析
　アセンブラ命令で構成されたコードを行数nの数列{A(n)}とみなす．(前後K個の命令に着目)
　A. sが1からnである間，以下を繰り返す．
　　a. 基準命令A(s)を決める．
　　b. tがs-Kからs+Kである間，1≦t≦nかつ t≠sを常に保ちつつ，以下を繰り返す．
　　―t<sの時，A(t)→A(s)としてカウント
　　―t>sの時，A(s)→A(t)としてカウント
　B. ペアごとの出現率を算出する．
・出現頻度ベクトルの導入・指標の算出
　i：テストデータにおける出現頻度ベクトル
　a：攻撃学習データにおける出現頻度ベクトル
　b：正常学習データにおける出現頻度ベクトル
　として，以下の内積およびコサイン尺度を算出する．
　　i・**a**，**i**・**b**，cos(**i**, **a**)，cos(**i**, **b**)
・類似度に基づいた攻撃検知
　テストデータについて，以下の判断基準により攻撃か否かを判断する．
　　cos(**i**, **a**) > cos(**i**, **b**)：攻撃データ
　　cos(**i**, **a**) ≦ cos(**i**, **b**)：正常データ

5. 結果・考察・今後の課題

検知実験で使用したデータ
攻撃データ：Exploit Database のシェルコード20個
正常データ：Linuxのコマンド20個

	提案手法	Snort (1)	Snort (2)
攻撃データ	20 / 20	20 /20	0 / 20
正常データ	18 / 20	0 / 20	20 / 20

誤検知が発生した正常データ2個は攻撃データの特徴に類似

特徴抽出のやり方を見直す必要があるのでは?
例
・頻度解析の際のKの値を変えてみる．
・着目対象のアセンブラ命令を変えてみる．