정상 스크립트 패턴에 기반한 비정상 스크립트 탐지

백성규* 위규영
아주대학교 정보통신공학대학원
(shalom34, kbweel@ajou.ac.kr)

Abnormal Scripts Detection based on Normal Scripts Patterns
Sung-Kye Baek* Kyu-Bum Wee
Graduate School of Information and Communication, Ajou University

요 약
본 논문은 악성 스크립트를 탐지하는 새로운 방법을 제안한다. 정상 스크립트 패턴을 기반으로 정상 패턴을 정의함으로써, 정상 패턴에서 벗어나는 경우에 악성이라고 판단한다. 또한 새로운 악성 스크립트가 생성되는 경우에도 탐지가 가능하다는 장점을 가지고 있다.

1. 서론
악성 스크립트는 스크립트 언어로 작성된 언어로 하며, 1994년 12월에 최초로 발견되었다. 악성 스크립트의 경우는 대체로 인터넷을 통해 전파되는 것이며, VBS(Visual Basic Script)나, VBS는 독특한 사용법이 가능하며, 동적 실행이 가능하며, 자주복제, 메인코드 변경, 그리고 파일 수정 등의 기능들을 가지고 있어서 많은 피해를 입히고 있는 실정이다.

그리나 현재 나와 있는 기법은 대부분 오류발견(misuse detection)에 중점을 두어 악성 스크립트를 탐지할 수 있는 방법을 제안하고자 한다.

제 2장에서는 기존 대중 기법에 대해서 설명한다. 제 3장에서는 시스템 개요와 구조에 대해서 설명한다. 제 4장에서는 정보 검색(information retrieval) 기법과 같은 탐지 시스템에 K-Nearest Neighbor의 적용에 대해서 설명한다. 제 5장에서는 실증 결과 및 향후 연구 방향에 대해서 설명한다.

2. 기존의 대응 기법
2.1 패턴 비교 방법
적자 바이러스 프로그램들이 바이러스를 탐지하기 위해 이용하는 방법으로 악성 스크립트의 시그니처(Signature)를 이용한 대응 기법이다.

2.2 단락 시스템을 이용한 방법
인체 단락 원리를 응용한 디지털 단락 시스템 대응 기법이다.

2.3 신경망
악성 스크립트의 시그니처(Signature)를 신경망을 이용하여 새로운 시그니처(Signature) 패턴을 생성하여

패턴 비교하는 대응 기법이다.

2.4 기타 악성 코드 탐지 기법
2.4.1 대중에 취항한 패턴을 분석하는 방법
대중에 취항한 패턴을 메일서비스에서 분석하여 악성 여부를 판단하는 방법이다. 대부분의 악성 코드의 패턴이 복잡한 형태로 되어 있기 때문에, 악성 코드에 대한 방해가 있다.

2.4.2 네트워크 호출을 통해 분석하는 방법
악성 스크립트가 네트워크에서 전파될 때 네트워크에 사용될 악성 스크립트가 없는 네트워크의 경우보다 증가한다. 이러한 네트워크의 호출을 관찰하여 악성 호스트, 악성 네트워크를 판전하는 기법이다[7].

3. 시스템의 개요와 구조
3.1 시스템의 개요
3.1.1 실시간 스크립트 호스트의 모니터링을 통해 스크립트가 실행되기 전에 해당 스크립트의 악성 여부를 판단하여 실행을 차단하는 것을 목적으로 한다.

3.1.2 정상 스크립트와 대상 스크립트의 중요도를 계산하기 전에 주석 제거와 스크립트 등의 기능을 나누는 전처리를 하게 된다. 전처리 후에는 각 function들이 하드 스크립트와 같이 처리한다.

3.1.3 악성 여부의 판단은 보유하고 있는 정상 스크립트의 패턴과 탐지 대상이 되는 스크립트의 유사 정도를 근거로 한다. 단 여기서 정상 스크립트와 악성 스크립트를 그대로 사용하는 것이 아니라, 기능별로 나누어서 악성 여부를 결정하게 된다.

3.1.4 탐지 대상은 압호화된 스크립트를 제외한 스크립트를 실행 대상으로 한다.
본 시스템은 그 기능에 근거하여 네 부분으로 구성된다.

3.2.1 아랫부분은 중요도 계산을 위해 keyword list 생성하는 부분이다. 수집되어 있는 정상 스크립트와 악성 스크립트들에서 정상 스크립트에는 많이 나오고 악성 스크립트에는 적게 나오는 keyword들과, 악성 스크립트에 많이 나오며 정상 스크립트에는 적게 나오는 keyword들을 keyword list로 정리하게 된다. 정상 스크립트와 악성 스크립트들은 좀 더 정확히 구분하기 위함이다. 본 논문에서는 100개의 keyword list를 선택하였다.

3.2.2. 위쪽 맨 bú분은 다른 수집된 정상 스크립트로부터 중요도 벡터를 계산하는 부분이다. 정상 스크립트의 불필요한 주석을 제거하고, function 별로 나누어 별도의 스크립트로 취급하는 전처리 과정을 거치게 된다. 그 후에 keyword list에 있는 keyword 별로 중요도를 계산하여 저장한다.

3.2.3 오른쪽 위부분은 스크립트 호스트를 모니터하는 부분으로 대상 스크립트가 스크립트 호스트에 의해 실행되기 전에 가로채아 오른쪽 아랫부분으로 전달하게 되고, 유사도를 계산하여 정상 판단 여부에 따라 실행 여부를 결정하게 된다.

3.2.4 오른쪽 중간부분은 대상 스크립트의 정상 여부를 판단하는 부분으로 불필요한 주석을 제거하고, function 별로 나누어 별도의 스크립트로 취급하는 전처리 과정을 거치게 된다. 대상 스크립트의 function 별로 매치된 keyword의 중요도를 구하고, 미치지 않은 정상 스크립트의 중요도 벡터를 이용하여 유사도를 계산한다.

4. 정기 검색 기법의 점입 단계 시스템 적용

4.1 정기 검색 기법

4.1.1 중요도

\[
\text{weight}(i,j) = \begin{cases} 
(\text{tf}_{i,j}) \log \left( \frac{N}{\text{idf}_{i}} \right) & \text{if } \text{tf}_{i,j} \geq 1 \\
0 & \text{if } \text{tf}_{i,j} = 0
\end{cases}
\]

수식1 중요도 계산식

i : 단어의 인덱스
j : 문서의 인덱스
N : 전체 문서의 개수
\text{tf}_{i,j} : i번째 단어가 j번째 문서에 나타난 횟수
\text{idf}_{i} : i번째 단어가 N개의 문서 중에 나타난 단어의 개수

키워드 리스트의 기여도를 이용하여 정상 스크립트와 호스트에서 실행되어지지 않 대상 스크립트의 중요도를 계산하게 된다.

4.1.2 유사도

\[
\text{cos}(q,d) = \frac{\sum_{i=1}^{n} q_i d_i}{\sqrt{\sum_{i=1}^{n} q_i^2} \sqrt{\sum_{i=1}^{n} d_i^2}}
\]

q : 질의어
\text{d} : 문서
n : 매칭 단어 수
q_i : 질의어에서 매칭된 단어의 중요도
\text{d}_i : 문서에서 매칭된 단어의 중요도

정상 스크립트의 중요도를 기반으로한 결과 감시된 스크립트의 유사도를 위의 식을 이용하여 구한다[5,6].

4.2 K-Nearest Neighbor 기법의 적용

build the training normal data set D; for each script X in the test data do for each script D_i in training data do calculate cos(X, D_i); if cos(X, D_i) equals 1.0 then X is normal; exit; find k biggest scores of cos(X, D); calculate sim_avg for k-nearest neighbors; if sim_avg is greater than threshold then X is normal; else X is abnormal;

그림2 Pseudo code for detection of abnormal Scripts

감시대상 스크립트와 정상 스크립트간의 유사도를 모두 구한 후에 유사도 값이 큰 순서대로 K개의 유사도 값의 평균값을 기준값으로 사용한다. 그 평균값이 threshold 값보다 크면 normal로, 작으면 abnormal로 판단하게 된다[3].
5. 실험 결과 및 향후 연구

5.1 데이터

<table>
<thead>
<tr>
<th>종류</th>
<th>스크립트의 개수</th>
<th>전처리 후 스크립트의 개수</th>
</tr>
</thead>
<tbody>
<tr>
<td>profiling</td>
<td>정상 VBS</td>
<td>352</td>
</tr>
<tr>
<td>test</td>
<td>정상 VBS</td>
<td>40</td>
</tr>
<tr>
<td></td>
<td>정상 VBS</td>
<td>40</td>
</tr>
</tbody>
</table>

표 1. dataset

dataset의 종류는 크게 profiling과 test로 나누며, profiling에 사용된 것과 test에 사용된 것은 서로 다른 것입니다. 정상과 비정상을 나누는 기준은 기존의 백신 프로그램을 사용하였다고[1,2].

5.2 실험 결과

![ROC curve diagram](image)

[그림3] Performance of kNN classifier method expressed in ROC curves

5.3 결과 및 논의

위의 실험에서는 threshold값을 둔 개를 이용하여 실험하였고, 그림3의 결과로 볼 때, 정상 스크립트의 패턴을 이용하여 비정상 스크립트 탐지도 충분히 가능하다고 볼 수 있고, K값의 선택이 중요한 요소임을 알 수 있다.

그러나 K-Nearest Neighbor 알고리즘을 적용하였