동적 웹 페이지 변조 점검 시스템

김우년O* 김도환* 주미리* 박응기* 김상욱**
*국가보안기술연구소
{wnkimO, dkim, mrjoo, ekpark}@etri.re.kr
**경북대학교 컴퓨터언어/멀티미디어연구실
swkim@cs.knu.ac.kr

Dynamic Web Page Defacement Validation System

Woonyon KimO* Do hwan Kim* Miri Joo* Eungki Park* Sangwook Kim**
*National Security Research Institute
**Computer Languages/Multimedia Lab. Kyungpook National University

요 약

일반적으로 웹 페이지 변조 점검 시스템은 해시 코드를 이용한다. 해시 코드 방법은 웹 페이지의 민감한 변화를 즉시 찾아 낼 수 있는 장점이 있지만, 인터넷 포털이나 뉴스 사이트 등의 동적인 웹 페이지의 경우에 적용하기 어려운 단점이 있다. 본 논문에서는 인터넷 포털이나 뉴스 사이트 등과 같은 웹 페이지의 내용이 계속해서 변화하는 경우에도 적용할 수 있는 N-Gram 색인 기반의 웹 페이지 변조 점검 시스템인 웹 레이더 시스템을 제시한다. 웹 레이더 시스템은 정상적인 웹 페이지의 N-Gram 색인과 점검시에 생성한 N-Gram 색인을 비교하여 두 인덱스의 동일 N-Gram의 발생 비율 차이를 합한 값을 N-Gram 색인 거리로 정의하고 이 값을 이용하여 웹 페이지 변조를 확인한다. 본 논문에서 제시하는 웹 레이더 시스템은 구조화되지 않은 동적 웹 페이지의 변조를 원격에서 점검할 수 있다.

1. 서 론

웹 서버는 많은 공공 기관과 기업, 개인이 정보 제공, 제품 소개 및 판매 등의 다양한 목적으로 운영하고 있다[1]. 웹 서버는 서비스 특성상 외부에 정보를 제공해야 하기 때문에 외부에서 항상 접근 가능한 위치에서 운영된다. 이러한 특성으로 웹 서버 시스템의 취약점을 이용하여 웹 서버를 해킹하고 웹 페이지를 변조하는 해킹사고가 자주 발생한다[1]. 웹 페이지 변조 사고는 zone-h[6]에 따르면 매년 사고수가 증가 하고 있다. 이와 같은 홈 페이지 변조 사고는 조직이나 기업의 이미지 및 신뢰도에 영향을 끼치므로 웹 서비스가 지속적으로 제공되도록 해야 하며, 웹 서비스가 단절되더라도 그 시간을 최소가 되도록 해야 한다.

홈 페이지 변조에 대한 조기 탐지 방법은 웹 서버 호스트에서 점검하는 방법과 원격지에서 점검하는 방법이 있다. 웹 서버 호스트에서 점검하는 방법은 점검 도구가 웹 서버와 같은 호스트에 있기 때문에 웹 서버가 해킹을 당할 때 웹 페이지 변조를 점검하는 도구도 함께 해킹을 당할 위험이 있다. 따라서 원격지에서 웹 서버의 홈 페이지 변조를 점검하기 위한 방법이 필요하다. 일반적으로 웹 페이지의 변조를 점검하기 위한 방법은 해시 코드를 이용한다[2, 3]. 그러나 해시 코드는 정적인 웹 페이지의 경우에는 잘 적용되지만 인터넷 포털, 뉴스 사이트와 같이 웹 페이지가 동적으로 구성되는 페이지에는 적용하기 어려운 단점이 있다.

본 논문에서는 원격지에서 동적인 웹 페이지의 변조를 점검할 수 있는 웹 레이더 시스템을 제시한다. 웹 레이더는 동적 웹 페이지 변조를 점검하기 위하여 N-Gram 기반의 색인 거리를 이용한다. N-Gram은 하나의 긴 문자열에서 N개의 문자 단위 부분을 의미한다[4, 5]. N-Gram은 모든 문자열을 N개로 이루어진 작은 단위로 분해하기 때문에, 오류가 제한된 부분에만 영향을 끼치도록 하고 나머지 부분들은 영향을 받지 않도록 한다. 따라서 두 문자열에 대한 N-Gram 빈도수를 구하게 된다면, 두 문자열 사이의 유사성을 측정할 수 있다[5]. N-Gram 기반의 색인은 이러한 N-Gram을 이용하여 색인을 생성하고 생성된 두 색인의 발생 비율의 차이를 이용하여 두 페이지의 유사도를 판정한다. 이때, 발생 빈도가 낮은 내용들은 점검에서 제외하여 웹 페이지의 소규모 내용 변화에 대하여 적응할 수 있게 한다. 웹 레이더는 N-Gram 기반의 색인 거리를 활용하여 내용이 변화하는 뉴스 사이트, 인터넷 포털 사이트 등의 동적인 웹 페이지의 변조를 평가할 수 있다.

본 논문은 2장에서 관련연구에 대해서 설명하고, 3장에서 웹 레이더 시스템의 구조에 대해서 설명한다. 4장에서는 웹 레이더 시스템에서 웹 페이지의 변조 평가에 사용하는 N-Gram 색인 거리를 설명하며, 5장에서는 실험 결과를 설명한다. 마지막으로 6장에서는 결론 및 향후 연구 방향에 대해서 설명한다.

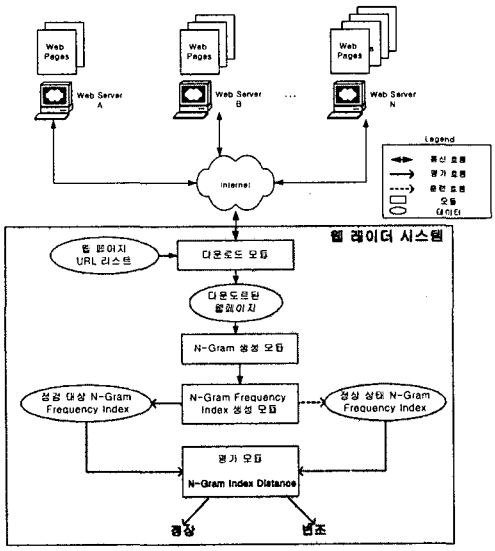
2. 관련연구

웹 서버 자체에서 페이지의 변조를 점검하기 위한 시스템으로는 Tripwire 사의 다양한 제품군이 있다. 이들 제품은 해당 서버에서 점검을 수행하며, 해시 코드 기반의 점검을 수행한다[7]. 대부분의 웹 페이지 변조 점검을 위한 방법으로는 해시 코드를 이용한 방법이 사용된

다[3]. 해시 코드를 이용한 방법은 크기가 큰 웹 페이지에 대한 변경 여부를 점검하는 좋은 방법으로서, CRC, MD5 또는 SHA와 같은 해시 함수를 이용하여 해시 값을 구한 후 새로운 페이지에 대한 해시 값을 비교하여 웹 페이지의 변조 유무를 검사한다[3]. 그러나 해시 코드를 이용하는 방법은 해시 함수의 특성상 동적 특성을 가진 웹 페이지에 대해서는 적용하기가 어려운 단점이 있다[3]. 해시 코드를 적용할 경우는 웹 페이지가 정적으로 항상 동일한 내용을 포함하고 있는 경우에 적합하며, 내용이 변경되는 웹 페이지에는 적용하기 어려운 단점이 있다.

3. 웹 레이더 구조

웹 레이더 시스템의 구조는 아래 (그림 1)과 같다. 원격지 웹 서버에 접속 후 해당 페이지를 다운로드하여 웹 페이지의 변조를 점검한다.



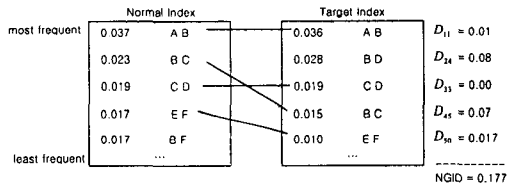
(그림 1) 웹 레이더의 구조

- 다운로드 모듈 : 점검 대상 웹 페이지 URL 리스트를 참조하여 해당 서버의 접속 상태를 확인하고 해당 페이지를 다운로드한다.
- N-Gram 생성 모듈 : 다운로드 된 페이지로부터 N-Gram을 생성한다.
- N-Gram Frequency Index 생성 모듈 : 생성된 N-Gram을 빈도수가 높은 것으로부터 정렬하여 특정 순위 이하의 것은 제거를 한다. 남은 N-Gram의 총 발생 빈도수로 각 N-Gram의 발생 확률을 구한다. 정상 상태 N-Gram Frequency Index는 정상적인 웹 페이지로부터 구한 색인이며, 점검 대상 N-Gram Frequency Index는 점검 시점에 구한 색인이다.
- 평가 모듈은 정상 상태의 색인과 점검 시점에 구한 색인을 비교하여 N-Gram 색인 거리를 구하여 평가한다.

4. N-Gram 색인 거리(N-Gram-based Index Distance)

본 장에서는 웹 레이더 시스템이 원격지에서 홈페이지의 변조를 평가하기 위해 사용하는 N-Gram 색인 거리(NGID)에 대하여 설명한다.

N-Gram 색인 거리는 두 웹 페이지의 유사도를 측정하기 위한 값이다. N-Gram 색인 거리는 두 웹 페이지에서 구한 각각의 N-Gram 발생 확률을 저장한 색인으로부터 생성한다. N-Gram 색인 거리는 기준이 되는 색인에서 평가 대상 색인의 차이를 합한 값으로 표현한다. 이 값은 두 웹 페이지가 어느 정도 서로 유사한지를 나타내는 값이다. 이 값이 작을수록 두 페이지의 유사도는 크고, 이 값이 클수록 두 페이지의 유사도는 작아지게 된다. 아래 (그림 2)는 N-Gram 색인 거리를 구하는 예이다. 정상적인 상태의 N-Gram 색인과 비교 시점에 구한 N-Gram 색인에서 동일한 N-Gram의 발생 비율의 차를 합한다. 예를 들어 <A B> 인 N-Gram의 경우 정상 상태와 비교 시점의 차이는 0.037-0.036 = 0.01이 된다. <B F> 인 N-Gram은 정상 상태에서만 발견되고 비교 시점에는 발견되지 않으므로 0.017-0 = 0.017이 된다. 이들 차이 값을 모두 합한 값이 N-Gram 색인 거리가 된다. N-Gram 색인 거리는 특정 기준값과 비교를 통해서 해당 웹 페이지가 변조되었는지를 결정하게 된다.



(그림 2) N-Gram 색인 거리 예

생성된 색인 거리를 이용하여 웹 페이지의 변조를 평가하는 방법은 평가 임계치를 이용한다. 구한 색인 거리가 평가 임계치보다 작거나 같은 경우는 해당 페이지가 정상적인 상태로 판정하고, 그렇지 않은 경우 변조 된 것으로 판정한다.

$$valid : \text{색인거리} \leq Threshold_{validation}$$

$$invalid : \text{색인거리} > Threshold_{validation}$$

5. 웹 레이더 시스템의 평가

본 장에서는 웹 레이더 시스템의 변조 점검에 대한 실험 결과를 설명한다. 해시 알고리즘을 이용한 방법과의 비교를 통해서 N-Gram 색인 거리 방법을 이용한 웹 레이더 시스템이 동적인 웹 페이지에 대해서 변조 점검을 수행함을 설명한다. 해시 코드 방법에서는 MD5 알고리즘을 이용하였으며 N-Gram 색인 거리의 평가 임계치는 0.1로 설정하였다. 평가 임계치는 웹 페이지의 특성에 따라서 각각 다르지만 일반적으로 10%의 내용 변화에 대해서 허용 가능하도록 설정한 경우에 좋은 결과를 나타내었다.

정상적인 웹 페이지에 대해서 변조로 판정하는 False Positive를 위한 실험은 실세계에 운영되는 웹 사이트를

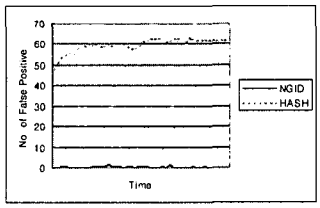
임의로 100개 선택 하였다. 표준 상태의 NGID와 해시 값을 각각의 웹 페이지에 대해서 구한 후 이 값을 30분 주기로 새로 구한 NGID와 해시 값과 비교하여 웹 페이지의 변경 여부를 결정한다.

실험 결과는 (표 1) 기관별 False Positive와 같다. 실험 결과 해시 코드를 이용하여 웹 페이지의 변조를 점검하는 것이 실세계의 웹 페이지에 적절하지 않다는 것을 알 수 있다. 웹 레이더는 MD5로는 평가할 수 없는 동적 웹 페이지에 대한 평가가 가능한 것을 알 수 있으며, 동적 웹 페이지를 점검하는 방법으로서 N-Gram 색인 거리가 해시 코드보다 효과적임을 알 수 있다.

(그림 3)은 시간에 따라서 해시 코드와 NGID의 False Positive의 변화를 나타낸 것으로서 해시 코드의 False Positive를 통해서 실세계의 웹 페이지의 내용이 지속적으로 변화하는 것이 많다는 것을 알 수 있다.

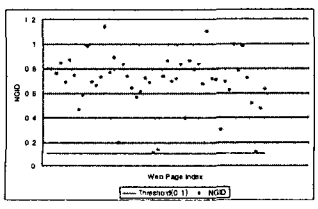
(표 1) 기관별 False Positive

기관	신문사	방송국	포털	공공기관	합계
선택 웹페이지 수	38	15	14	33	100
해시코드의 False Positive 수	29	14	12	8	63
웹 레이더의 False Positive 수	1	1	0	0	2



(그림 3) 시간에 따른 False Positive의 변화

변조된 웹 페이지에 대해서 변조되지 않은 것으로 판정하는 False Negative를 위한 실험은 실제 해킹당한 웹 페이지를 50개 선택하여 해킹당하기 이전 페이지와 해킹당한 페이지로부터 N-Gram 색인 거리를 구하여 웹 페이지 변조 결과를 평가하였다. 실제 해킹당한 웹 페이지이므로 해시 코드를 이용한 비교에서는 모두 변조된 것으로 평가되었다. 웹 레이더의 NGID를 이용한 방법에서는 (그림 4)와 같이 각각의 웹 페이지 별로 평가 임계치인 0.1 보다 크게 평가되었다. (그림 4)에서 보는 것과 같이 0.1에 가까운 것은 웹 페이지의 일부 내용만 변조한 경우이며, 1 이상의 것은 웹 페이지의 구조와 내용을 완전히 변조한 경우에 해당한다.



(그림 4) 50개의 해킹당한 페이지에 대한 NGID 값

6. 결론

본 논문에서는 원격지에서 동적으로 변화하는 웹 페이지의 변조를 점검하는 시스템인 웹 레이더 시스템을 설명하였다. 웹 레이더 시스템은 동적인 웹 페이지의 변조를 점검하기 위해서 N-Gram 색인 거리를 이용하였다. N-Gram 색인 거리는 기존의 해시 알고리즘으로서는 평가할 수 없었던 동적인 웹 페이지에 대해서 컨텐츠의 변조 점검을 가능하게 한다. 실험 결과와 같이 해시 코드를 적용한 변조 점검 방법은 실세계의 많은 웹 페이지가 동적인 속성을 가지고 있으므로 적용하기 어렵다는 사실도 확인할 수 있다. 그러나, 민감한 내용의 변조 점검에는 여전히 유용할 수 있다.

앞으로의 연구는 웹 레이더 시스템의 평가 척도인 평가 임계치가 현재 임의로 설정되어 있으므로 다양한 특성을 만족시키지 못하고 있다. 따라서 평가 임계치 값을 각각의 웹 페이지의 특성에 따라서 조절할 수 있도록 하기 위해서 학습 모델을 적용하여 좀 더 정확하게 웹 페이지의 변조 여부를 확인할 수 있는 방안에 대한 연구가 필요하다.

참 고 문 헌

[1] Dae-Sik Choi, Eul Gyu Im, and Cheol-Won Lee, "Intrusion-Tolerant System Design for Web Server Survivability," LNCS 2908, pp. 124-134. 2003.

[2] Feiyi Wang, Fengmin Gong, Chandramouli Sargor, "SITAR: A Scalable Intrusion-Tolerant Architecture for Distributed Services," Proceeding of the 2001 IEEE Workshop on Information Assurance and Security, pp. 38-45, June, 2001,

[3] Feiyi Wang, Raghavendra Uppalli, Charles Killian, "Analysis of Techniques For Building Intrusion Tolerant Server Systems," MILCOM 2003, Oct. 13-15, 2003.

[4] William B. Cavnar and John M. Trenkle, "N-Gram-Based Text Categorization," Proceedings of SDAIR-94, 3rd Annual Symposium on Document Analysis and Information Retrieval, pp.161-169, April, 1994.

[5] Woonyon Kim, Miri Joo, Eunyoung Lee, Dohoon Lee, Eungki Park, Sangwook Kim, "N-Gram-based Dynamic Web Page Defacement Validation," Pre-Proceedings of WISA-2004, The 5th International Workshop on Information Security Applications, pp.309-316, August, 2004.

[6] Web site,
http://www.zone-h.org/en/defacements.

[7] Web site,
http://www.tripwire.com