Journal of The Institute of Electronics and Information Engineers Vol.52, NO.11, November 2015 http://dx.doi.org/10.5573/ieie.2015.52.11.164
ISSN 2287-5026(Print) / ISSN 2288-159X(Online)

논문 2015-52-11-17

컨텐츠 보안 침입 탐지 시스템 설계 및 구현

(Design and Implimentation of Intrusion Detection System on Contents Security)

김 영 선*, 서 춘 원**

(Young Sun Kim© and Choon Weon Seo)

요 약

인터넷 사용이 보편화되면서 웹을 통한 광고, 사이버 쇼핑, 인터넷 뱅킹 등 다양한 서비스가 네트워크를 이용하여 제공되면서 웹 보안에 대한 필요성이 증가하고 있다. 또한, 시스템을 다양한 유형의 해킹 위협과 외부의 불법적인 침입으로부터 정보자산의 보호를 위한 보안시스템을 요구하게 된다. 본 논문의 웹 침입 탐지 도구는 웹에 대한 개별적인 모니터링을 통해 소요되는 자원 및 인력의 손실을 방지할 수 있도록 하여 보안 수준을 향상시켜는 것이다. 웹 보안 시스템은 웹 환경에서의 보안 취약성과 정보 노출에 대한 문제점의 원인을 분석하고 보안의 빠른 지원을 결정하기 위해서 모니터링을 이용하여 정보 보안 취약성과 정보 노출을 보호할 목적으로 보안 시스템을 설계하고자 한다.

Abstract

As Internet use is widespread advertising through the Web, shopping, banking, etc. As the various services offered by the network, the need for Web security is increasing. A security system for the protection of information assets and systems against various types of external hacking threats and unlawful intrusion will require. Intrusion Detection Tool of the paper web will have is to increase the security level, to prevent the loss of resources and labor spent by the individual monitoring of the web. Security intrusion detection system analyzes the cause of the problem of the security vulnerability and exposure of the information on the Web. Using a monitor to determine a fast support of security is to design a security system for the purpose of protecting the information security vulnerability and exposure information.

Keywords : Contents, Security, Intrusion Detection

Ⅰ. 서 론

컴퓨터 시스템은 인터넷이 접목됨으로써 시스템에 대한 불법 침입, 중요 정보 유출 및 변경에 대한 보안과 컴퓨터 바이러스 등의 공격으로부터 시스템을 보호할 대책을 가지고 있어야 한다. 해커들은 이러 자동화된 보안 도구을 이용하여 침입하고자 하는 시스템의 보안 취약점 정보 및 공격대상을 찾는다. 침입 후에 탐지를 하는 방법보다는 침입을 하기 위해 사전에 미리 해보는 침입시도탐지를 적극적으로 예방할 필요가 있다. 인터넷 및 전자상거래 환경 속에서 경쟁력을 확보하기 위해서 기업은 많은 변화를 하고 있다. 가속화되는 전자상거래 영역의 확대는 기업 시스템, 어플리케이션 및 데이터가 인터넷 커뮤니티에 접근하기가 더욱 쉽다는 것을 의미한다. 전자상거래는 안전성, 거래 정보 보안, 고객 데이터 보안 및 신속한 액세스가 가능해야 한다. 본 논문의 웹 침입 방지 도구는 웹에 대한 개별적인 모니

* 평생회원, 대림대학교 세무회계과
(Dept. of Tax & Accounting, Daelim University)
** 평생회원, 김포대학교 컴퓨터네트워크과
(Dept. of Computer Network, Kimpo University)
©Corresponding Author(E-mail: yskim306@daelim.ac.kr)
Received ; September 4, 2015 Revised ; September 20, 2015
Accepted ; October 28, 2015

터링을 통해 소요되는 자원 및 인력의 손실을 방지할 수 있도록 하여 보안 수준을 향상시켜는 것이다. 웹 환경에서의 보안 취약성과 정보 노출에 대한 문제점의 원인을 분석하고 보안의 빠른 지원을 결정하기 위해서 모니터링을 이용하여 정보 보안 취약성과 정보 노출을 보호하는데 있다.

Ⅱ. 관련 연구

2.1 웹 보안

최근 인터넷 사용이 보편화되어 웹을 통한 광고, 사이버 쇼핑, 인터넷 뱅킹 등 다양한 서비스가 네트워크를 이용하여 제공되면서 웹 보안에 대한 필요성이 강조되고 있다. 대부분의 인터넷 쇼핑몰 사용자는 구매에 대한 지불 방법으로 신용카드를 사용하는데, 이 때 신용카드 번호와 개인 정보가 불법적으로 제3자에게 유출되거나 위조 및 변조될 가능성이 커지고 있다. 이러한 문제점은 인터넷의 TCP/IP와 웹 프로토콜인 HTTP가 데이터에 대한 보안 서비스를 제공하지 않는데 있다. 이에 따라 인터넷을 이용하여 전송된 데이터에 대해 무결성, 기밀성, 사용자 인증, 부인봉쇄, 접근통제, 보안감사 등의 보안 서비스를 제공함으로써 안전하고 편리한 인터넷 환경을 구축하기 위해서 노력이 활발히 진행되고 있다. 웹 보안의 시스템 보안은 어플리케이션 개발자가 독자적으로 보안 솔루션을 개발하는 것이 일반적이어서 이에 대한 표준화는 진행되지 않고 있다.

2.2 침입 탐지 모니터링 도구

침입 탐지 모니터링은 침입자의 행위를 모니터링하여 침입자의 이동 경로 상에 있는 호스트를 자신을 복제함으로써 모니터링과 침입탐지, 침입대응을 하는 영역까지를 말한다. 공간적인 제약을 극복하여 지역적인 보안 정보 수집과 분석으로 많은 보안 정보를 유지할 수 있다. 침입 탐지 모니터링은 컴퓨터 사용에 대한 모든 작업 현황을 모니터링하고 활용도를 분석하여 전사적 자원관리의 다양한 기능 제공한다. 침입 방지 모니터링은 포탈사이트들의 웹 메일을 통해 나간 내용과 첨부파일을 체크하여 악의적인 메일이나 사내의 기밀정보 유출에 대비하여 기업 내부 자료 유출을 방지한다. 침입 방지 모니터링 기능으로 비업무용 사이트는 리스트 목록을 통해 차단하고, 관리자가 지정 사이트 목록을 통한 차단을 하기도 한다. 또한 증권사별로 독자적으로 쓰는 포트도 차단하고 파일을 전송할 수 있는 FTP, Telnet 등의 접속을 차단한다. 차단 결과에 대한 접속 시도 기록 등을 모니터링하기도 한다. 그리고 사용자별로 차단 사이트를 차등 적용하기도 하고 시간대별 차단 정책을 적용하여 업무시간만 지정한 차단도 가능하다. 모니터링은 기간별 증감 및 시간에 따른 네트워크 사용 변화를 쉽게 파악할 수 있고 이런 네트워크 정보를 통하여 현재 네트워크에서 일어나는 상황을 쉽게 파악할 수도 있다. 하루에도 수백개의 인터넷 사이트가 새로 생기고 없어지기도 하기 때문에 접속사이트 URL 및 컨텐츠 기록이 사이트 차단과 함께 필요하다. 접속 사이트 로그 저장을 통한 다양한 항목별 검색 및 키워드 기반 검색 기능으로 접속 사이트 URL 기록 및 실시간 모니터링을 한다.

Ⅲ. 침입 탐지 시스템 설계

네트워크 상에서의 불법 침입은 해가 갈수록 증가하고 다변화되고 있다. 또한 인터넷의 발전과 더불어 네트워크의 시스템간의 상호협력이 중시되고 있다. 악의적인 사용자들에 의한 독창적이고 새로운 침입 방식의 개발은 침입 탐지에 대한 어려움을 증가시키고 있다. 기존의 침입 탐지 시스템들은 갈수록 다양해지는 침입에 대해 능동적으로 대처하는데 어려움이 따른다. 전자상거래 환경의 컨텐츠에 대한 효율적인 탐지 구조가 필요하다. 따라서 이를 고려한 새로운 형태의 침입 탐지 시스템 구조를 제시하고자 한다.

3.1 컨텐츠 보안 도구 구성

네트워크 기반에서 컨텐츠 보안 감시는 침입자의 행위를 지속적으로 모니터링하여 컨텐츠 침입탐지를 분석하여 침입대응에 대처할 수 있도록 하는데 있다.

컨텐츠 보안 도구 구성도 그림 1에서 컨텐츠 분석은 전자상거래의 원활한 처리를 위해서 기본적인 업무 분석처리를 파악하는 것이다. 웹사이트의 불법적인 위변

그림 1. 컨텐츠 보안 도구 구성
Fig. 1. Content Security Configuration Tool.

조를 검증하고 탐지하여 컨텐츠의 내용 점검 및 분석 서비스를 공유하여 침입에 대한 준비를 한다. 이것을 근거로 보안 정책을 수립하여 방문 차단 URL, 바이러스 탐지, 불법적인 컨텐츠 위변조에 방법을 모색한다. 컨텐츠에 대한 불법적인 위변조를 파악하기 위해서 학습모도를 통해서 탐지한다. 설정된 관제 사이트에 대한 관련 메시지와 변경 Log를 확인한다. 기존 페이지와 변조 페이지 창에 해당 페이지를 띄우고 바뀐 부분을 확인하여 위험에 능동적 예방과 대처를 한다.

3.2 컨텐츠 보안 도구 동작 모델

컨텐츠 감시 도구는 전자상거래의 컨텐츠를 모니터링함으로써 컨텐츠의 침입 차단 정보를 수집한다. 컨텐츠의 메시지 형태로 전송되는 보안 정보들을 모니터링 관리기로 관리 또는 조작한다.

침입 탐지 관리기는 모니터링 관리기로부터 전송되는 보안 정보들을 분석하여 컨텐츠의 침입을 탐지한다. 침입 대응은 컨텐츠 분석 결과 대응 전략에 따라 침입 대응을 수행하며 또 다시 메시지 형태로 적절한 대응을 한다.

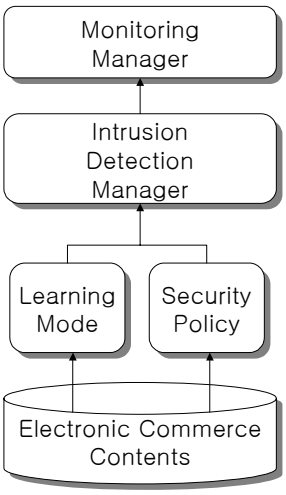

그림 2. 컨텐츠 보안 도구 동작 구조
Fig. 2. Operating structure of Content security.

3.3 컨텐츠 보안 도구 알고리즘

시스템에 관한 취약점 정보를 파악하기 위해 공격하는 것을 침입시도라고 하는데 이런 침입 시도 공격에 대응과 컨텐츠 정보 유출 및 변경에 대한 컨텐츠 보안 도구 알고리즘은 다음과 같다.

```
DectectStatus CheckAttack(CPacket* cmtPacket)
{
if(IsSourceHostList(cmtPacket);
{ // Check same Packet
      if (cmtTime-srcHost -> UpdateTime)
      { // Normal Time Check
       if(srcHost-> Connect > SCAN_MAX)
        // attack detect
          return DetectNormalAttack ;
       else
          // increase connect
      else
     {
       InitHost(srcHost, cmtPacket);
     }
  }
 else
  if (IsSourceHostListFull())
      RemoveOldHostSourceHostList();
      // create host
  }
 return Normal;
}
```

그림 3. 컨텐츠 보안 도구 알고리즘
Fig. 3. Content security tools, algorithms.

Ⅳ. 컨텐츠 보안 시스템 구현

컨텐츠 보안 감시 탐지된 정보는 침입 증상에 따라 보안 정책에 따라 적절한 관제 처리된 기준 페이지 창과 변조 페이지 창이 해당 페이지에 뜨고, 바뀐 내용에

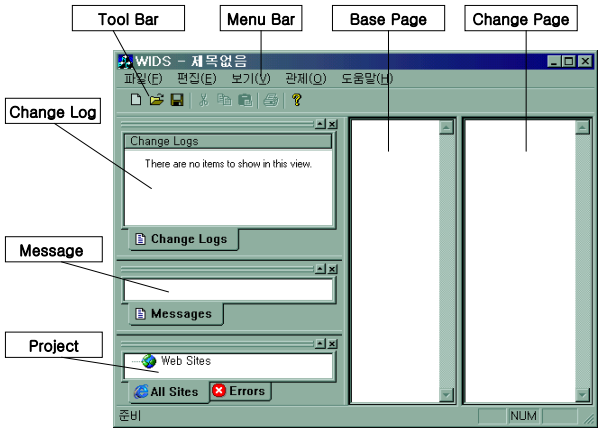

그림 4. 침입 탐지 시스템
Fig. 4. Intrusion Detection System.

표 1. 침입 탐지 시스템 도구 설명
Table 1. Intrusion Detection System Tool Description.

창 설명	기능
메뉴바 (Menu Bar)	여러 가지 작업에 필요한 각종 메뉴들의 모음
도구모음	기본적 도구들의 아이콘의 형태로 표시
프로젝트 창	감시 도구를 이용해 만든 프로젝트의 구성을 보여주는 창
기준 페이지 창	바뀌기 전 기준이 되는 페이지를 보여주는 창
변조 페이지 창	바뀐 후 페이지ffm 보여주는 창
메시지 창	현재 진행 상황을 보여주는 창
Chang Log 창	관재 중 발생된 Change Log를 보여주는 창

해당하는 부분은 Change Log창에 보일 수 있도록 나타난다.

4.1 침입 탐지 시스템 개발

침입 탐지 시스템에 불법 침입, 중요 정보의 유출 및 변경, 컴퓨터 바이러스 및 서비스 거부 공격 등의 문제를 해결하기 위한 방법으로 컨텐츠의 안전성을 확보할 수 있다. 컨텐츠 보안 시스템을 실행할 때 프로젝트를 만들어서 프로젝트가 저장할 위치를 지정한다. 이때 지정된 위치의 디렉토리 밑에 해당 이름으로 디렉토리가 생성된다. 프로젝트가 창에 생성된 프로젝트를 선택하고, 관제할 사이트를 추가하면 해당 사이트 이름과 메인 페이지 URL를 입력하여 관제한다. 또한 특별한 페이지를 추가할 때는 서브 페이지 추가를 하여 관제를 할 수 있다.

가. 침입 감시 관제 사이트 지정

파일 메뉴에서 새 프로젝트를 클릭한다. 프로젝트 이름과 프로젝트 위치를 설정하여 작업되는 프로젝트들이 저장할 위치를 만든다. 프로젝트 창에서 생성된 프로젝트를 선택하고 관제 사이트 추가를 클릭하여 프로젝트 메뉴에 관제 사이트를 추가한다. 원하는 사이트 이름과 메인 페이지 URL을 입력하면 프로젝트 창에 관제 사이트가 추가된 것을 볼 수 있다. 프로젝트 창에서 추가된 사이틀르 선택하고 오른쪽 마우스를 클릭하여 서브 페이지 추가를 하면 원하는 사이트 내의 서브 페이지 URL들이 나타나다. 서브 페이지에 원하는 URL's를 클릭하면 된다.

나. 침입 감시 관제 결과

관제 메뉴에서 관제를 시작하여 설정된 관제 사이트와 서브 페이지들을 관제한다. 관련 메시지와 Change Log들은 해당 창에 확인할 수 있다. 관제를 확인하기 위해서 관제를 중지 시킨후 Change Log창에 표시된 log들을 클릭하면, 기준 페잊 창과 변조 페이지 창에 해당 페이지가 나타난다. 변경된 내용에 대하여 표시가 되면 확인을 한다.

4.2 침입 탐지 시스템 결과 분석

관제 옵션 설정 후 관제 메뉴에서 관제 시작을 클릭하여 관제를 시작하면 관제가 다음과 같은 상태가 나타난다. 관제 주기에 따라 Thead의 작업 상태를 파악할 수 있다.

관제 후에 관제 메뉴에서 관제 정지를 클릭하면 관재 결과 분석이 나타난다. 관제 결과 분석의 Observation Count에 표시되는 내용은 해당 페이지의 관제 정지까지 관제된 횟수와 전체 관제된 것에 대한 비율을 %로 표시한 것이다.

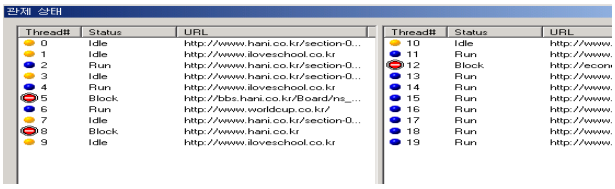

그림 5. 침입 탐지 시스템 상태
Fig. 5. Intrusion Detection System Status.

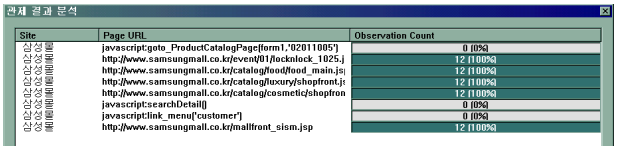

그림 6. 침입 탐지 시스템 결과 분석
Fig. 6. Intrusion detection systems analyze results.

V. 결 론

네트워크를 통하여 전세계 정보를 쉽게 얻을 수 있고 컴퓨터를 통하여 기존에 수 십 시간에서 길게는 수 개월이 걸리던 정보의 가공을 몇 초, 몇 분이면 간단하

게 끝낼 수 있게 되었다. 끊임없이 연결되는 네트워크는 현재의 위치에서 전세계 어디로든지 접속을 할 수 있고, 이것 정보의 보안이라는 개념을 확장시켰다. 전자상거래의 확대는 시스템과 어플리케이션 및 데이터가 인터넷 커뮤니티에 접근하기 쉽다는 것을 의미한다. 이것은 전자상거래의 어플리케이션, 네트워크, 호스팅 인프라스트럭쳐, 서버 및 데스크탑을 노리는 바이러스 침입, 무단 액세스, 서비스 공격 거부, 다양한 형태의 침입 증가에 대한 위험 속에 직면하고 있다. 그래서 다양한 보안 위협 및 침입에 대한 관리와 대응이 필요로 하게 된다.

본 논문의 웹 침입 방지 도구는 웹에 대한 개별적인 모니터링을 통해 소요되는 자원 및 인력의 손실을 방지할 수 있도록 하여 보안 수준을 향상시켜는 것이다. 웹 침입 방지 도구는 모니터링되는 웹을 분석하여 해커 침입을 방지하고 피해를 최소화하는데 그 목적이 있다. 향후 인터넷 해킹방지에 효율성을 갖는 논문으로 다양한 해킹 방지에 활용될 수 있을 것으로 사료된다.

REFERENCES

[1] H. Jang and S. Kim, “A Self-Extension Monitoring for Security Management,” Proceeding of the 16th Annual Computer Security Applications Conference, pp.196-203, December 2000.
[2] S. Garfinkel, G. Spafford, Practical UNIX and Interent Security, 2nd Ed. Oreilly & Associates Inc., pp.731-757, 2002. 11.
[3] Hyundong Lee and Mokdong Chun, “Context-Aware Security System for Cloud Computing Environment”, joural of the Institute of Electronics and Information Enginerrs, Vol.47 CI. pp.19-27. November 2010.
[4] Moon-Goo Lee, “Secured Verification of Intrusion Prevention System Security Model Based on CPNs”, joural of the Institute of Electronics and Information Enginerrs, Vol.48 CI. pp.76-81. May 2011.
[5] Sunghee Woo, “A Study on Security Capability of IDPS”, joural of the Institute of Electronics and Information Enginerrs, Vol.49 CI. pp.9-11. July 2012.

저 자 소 개

김 영 선(평생회원)
1985년 광운대학교 컴퓨터공학과 학사 졸업
1997년 광운대학교 전산과 석사 졸업
2004년 광운대학교 컴퓨터과학과 박사졸업
1987년~1993년 (주) LG-CNS 근무
2000년~현재 대림대학교 세무회계과 교수
<주관심분야 : 웹보안, 보안 정보관리, 모바일 컨텐츠, 멀티미디어>

서 춘 원(평생회원)
1988년 광운대학교 전자공학과 학사 졸업
1990년 광운대학교 전자공학과 석사 졸업
1997년 광운대학교 전자공학과 박사 졸업
2000년~현재 김포대학교 컴퓨터네트워크 교수
<주관심분야 : 패턴인식, 영상처리, 스테레오 비젼 시스템, 보안정보 관리>