Journal of Korea Multimedia Society Vol. 7, No. 1, January 2004(pp. 91-97)

웹 컨텐츠 변경 탐지 시스템의 설계 및 구현

김영선†, 장덕철††

요 약

전자상거래는 컨텐츠를 통해 거래가 이루어지고 있는데 외부로부터 불법적 침입을 받을 수 있는 컨텐츠에 대한 보안이 절실히 요구되고 있다. 전자상거래 컨텐츠의 대한 침해 방지를 그동안 수동적인 형태의 보호에서 이제는 적극적인 형태의 보호 대책을 강구해야 한다. 그래서, 해커들의 불법적인 컨텐츠 침입에 대한 보호가 필요하다. 컨텐츠에 대한 침입이 발생함과 동시에 시스템에 대한 피해를 최소화하기 위한 컨텐츠 감시 기능을 제공하는 도구가 요구된다. 본 논문의 웹 컨텐츠 변경 탐지 시스템은 웹에 대한 개별적인 모니터링을 처리하여 소요되는 자원 및 인력의 손실을 방지하는데 있다. 그리고, 웹 환경의 컨텐츠 보안의 취약성과 정보 노출에 대한 문제점의 원인을 분석하여 컨텐츠의 빠른 지원을 제공한다. 이 시스템은 모니터링을 이용하여 컨텐츠 보안 취약성과 정보 노출을 보호하는데 그 목적이 있다.

Design and Implementation of Modified Web Contents Detection System

Young-Sun Kim†, Deog-Chul Jang††

ABSTRACT

As the electronic commercial transaction is being transacted by contents which can get an illegal intrusion from the outside, we sincerely require security for them. We must consider a protection countermeasure about intrusion from protection of the passive form to protection intrusion of the active one. So the security is required against hackers illegality intrusion into the contents. As soon as the intrusion happens about the contents, the tools providing the monitor of contents are required to minimize the damage to the systems. Modified web contents detection system in this paper prevents the loss of resources and manpower required through individually monitoring on the web. Also, this paper offers rapid support of security that it analyzes the weakness of contents security of the web environment and the cause of the problem with the leakage of information. So this system has the purpose of protecting the weakness of contents security and the leakage of information.

Key words: Web(웹), Contents(컨텐츠), security(보안), Monitoring(모니터링), Intrusion(침입), Hacking(해킹)

1. 서 론

전자상거래의 컨텐츠는 정보통신 네트워크를 통해 공급자와 수요자 사이에 있는 기존 유통 구조에서 중간 매체를 없앰으로써 수요자의 요구를 정확하게 파악하여 시간과 비용의 절감효과를 가져오고 있다. 컨텐츠는 전 세계적으로 그 활용이 확산되고 있으며, 제품의 생산 및 판매 등의 기업 활동과 기업이나 고객과의 관계를 개선할 수 있는 중요한 경영 수단으로 자리잡아 가고 있다. 급격히 늘어나고 있는 전자상거래의 컨텐츠 활성화는 상품의 판매와 대금의 지불 등의 다양한 정보서비스를 제공한다.

전자상거래는 사용이 편리하고 개인과 조직의 생

※ 교신저자(Corresponding Author) : 김영선, 주소 : 경기도 안양시 동안구 비산동 526-7(431-715), 전화 : 031)467-4996, FAX : 031) 467-4996
E-mail : yskim306@lycos.co.kr
접수일 : 2003년 2월 3일, 완료일 : 2003년 7월 9일
† 정회원, 대림대학 경영정보계열 조교수
†† 비회원, 광운대학교 컴퓨터과학과 교수
(E-mail : dcjang@daisy.kw.ac.kr)

산성을 향상시켜 주는 대신 서비스 제공자인 전자상거래의 정보시스템과 사용자의 개인 정보, 지불 정보에 대해 철저한 보안을 요구하고 있다.

컨텐츠는 인터넷과 같은 개방형 네트워크를 통해 거래가 이루어지고 있기 때문에 외부로부터 불법 침입은 물론이고, 지불 정보의 전송 중 패킷 조작에 의한 부정 사용, 타 사용자의 ID 도용 등 거래 시 발생할 수 있는 역기능에 대해 보안 대책을 강구하지 않으면 안 된다[1]. 따라서, 전자상거래를 구성하고 있는 컨텐츠의 보호가 절실히 요구되고 있는데 이것은 컨텐츠 모니터링 도구의 필요성을 요구하게 된다. 컨텐츠의 빠른 정보 전달과 지식의 공유는 보안 관리의 필요성을 크게 대두되게 하고 있다. 전자상거래 상에서 컨텐츠에 대한 정보 침해 방지의 수동적인 형태의 보호에서 적극적인 형태의 보호가 요구된다[2].

본 논문에서는 모니터링 도구를 이용하여 시스템에 대한 피해를 최소화하는데 있다. 기존 탐지 시스템에서는 컨텐츠에 대한 개별적인 모니터링을 이용하여 소요되는 자원 및 인력의 손실이 많아 이런 점을 해결하기 위한 연구 결과 본 논문에서는 침입 감시 도구로 모니터링 된 컨텐츠를 분석함으로써 컨텐츠에 대한 해커 침입을 감지하여 피해를 최소화하고 컨텐츠의 정보 흐름을 보호함으로써 전자상거래 접속의 보안 수준을 향상시킬 수 있었다.

본 논문의 구성은 2장에서는 관련 연구분야로 탐지기술과 모니터링 도구에 대한 설명과 3장은 탐지 시스템을 설계하고, 4장에서는 시스템을 구현했다. 5장은 시스템에 대한 성능 평가를 고찰했고, 6장에서는 결론을 내린다.

2. 관련 연구

2.1 웹 보안 서비스

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.

웹의 시스템 보안은 어플리케이션 개발자가 독자적으로 보안 솔루션을 개발하는 것이 일반적이어서 이에 대한 표준화는 진행되지 않고 있다. 그러나, 상호 운용성이 요구되는 네트워크 보안 부분에서는 TCP 계층 바로 위에서 보안 서비스를 제공하는 SSL (Secure Socket Layer)과 응용계층에서 보안 서비스를 제공하는 S-HTTP(Secure HTTP)로 나뉘어 표준화가 제공된다[3]. S-HTTP는 HTTP의 전송 능력을 그대로 유지하면서 전송되는 각각의 메시지에 대해 전자서명, 암호화, 인증과 같은 세 가지 전송을 보안 서비스로 제공한다[4]. 메시지에 대한 전자서명은 각 메시지에 전자서명이 추가되어 전송되며, 암호화는 원하지 않는 사람이 읽을 수 없도록 암호화를 통해 안전을 보장해 준다. 메시지 인증은 MAC (Message Authentication Code)를 사용하여 메시지 무결성 및 송신자 인증을 가능하게 한다.

2.2 침입탐지기술

네트워크와 컴퓨터를 통해 정보의 교환이 자유로워지고 정보의 이용 효율이 높아진 것은 정보가 그만큼 가치가 있는 것이며 정보가 손쉽게 자신의 의지와 상관없이 유통 될 수 있다는 것을 의미한다. 편리한 생활과 함께 개인과 기업의 정보 및 국가의 중요한 정보를 불법으로 취득하여 악용되는 경우가 크게 증가하고 있다. 다양한 해킹유형의 위협이 존재하고 있어 중요한 정보자산의 보호를 위한 보안시스템이 요구된다[8]. 침입탐지시스템은 이미 알려진 공격의 감시를 통해서 이상한 네트워크 활동을 찾아 경고 메시지를 보내고 침입 상황을 기록 보고하는 목적을 가지고 있다[5]. 또한 외부의 불법적인 침입을 사전에 탐지하여 사전 경보를 하여 초기 대응 기능을 갖춘 시스템을 통한 비정상적인 침입시도를 실시간으로 탐지, 경보하며 탐지된 침입 시도에 대해 실시간 대응한다. 현재 많은 연구들은 비정상행위 탐지 기술을 중심으로 이루어지고 있으나 매우 단순한 비정상행위 탐지 시스템이 사용되고 있다. 개별적인 사용자의 행위에 기반한 탐지기술보다는 일반적인 사용 시간,

네트워크 접속 수 등이 비정상행위 탐지를 위한 측정으로 사용하고 있다. 시스템이나 네트워크에서 발생하는 침입을 탐지하고 실시간으로 대응하는 보안시스템으로 컴퓨터 시스템의 비정상적인 사용을 탐지하고 이를 차단하는 시스템이고, 알려진 해킹 패턴이나 OS 취약성 등에 대비하고 이를 보완하는 시스템이다. 침입탐지시스템은 서버 침입탐지와 네트워크 침입탐지 등이 있다. 서버기반의 침입탐지는 서버의 내부에 상주하면서 불법 침입에 대해 감시하는 서버기반의 감시도구이다. 또한 파일 모니터링 기능을 이용하여 웹페이지의 변경이나 백도어, 트로이 목마 등과 같은 불법 침입을 검출한다. 의심스러운 침입을 검출하면 경보나 자동 대응책을 통해 피해의 확대를 방지한다. 네트워크 침입탐지는 네트워크를 통한 비인가 행위를 지속적으로 감시, 대응조치 한다.

2.3 침입 탐지 모니터링 도구

침입탐지 모니터링은 침입자의 행위를 모니터링하여 침입자의 이동 경로 상에 있는 호스트를 자신에게 복제함으로써 모니터링과 침입탐지, 침입대응 등을 할 수 있는 것을 말한다[6]. 공간적인 제약을 극복하고 지역적인 정보 수집과 분석으로 많은 보안 정보를 유지할 수 있다. 침입탐지 모니터링은 컴퓨터 사용에 대한 작업 현황을 모니터링하고 활용도를 분석하여 전사적 자원관리의 다양한 기능을 제공한다[9]. 또한, 전자우편을 통한 중요자료 유출 등을 모니터링하여 인터넷 사이트 접속현황, 차단 네트워크 접근제어 및 사용현황 등을 분석하기도 한다.

차단 모니터링은 이메일과 함께 정보 유출의 새로운 경로로 이용될 수 있는 각종 웹 메일을 모니터링하기도 한다. 그래서 침입방지 모니터링은 토탈 사이트들의 웹 메일을 통해 나간 내용과 첨부파일을 체크하여 악의적인 메일이나 사내의 기밀정보 유출에 대비하여 기업 내부 자료 유출을 방지한다. 침입방지 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. 또한, 사용자별로 차단 사이트를 차등 적용하기도 하고 시간대별 차단 정책을 적용하여 업무시간만 지정한 차단도 가능하다[7]. 차단 모니터링 방법은 사용자가 본 화면 그대로 모니터링하거나 게시판, 웹 메일 사이트에 uploading된 자료 및 첨부 파일 사본 저장 기능 등을 하기도 한다[10]. 하루에도 수백 개의 인터넷 사이트가 새로 생기고 없어지기도 하기 때문에 접속사이트 URL 및 컨텐츠 기록이 사이트 차단과 함께 필요하다. 개인 및 기업정보의 유출로 인한 피해 규모는 점차 증가되고 있으며, 이러한 시점에서 기업의 정보유출 위험성은 기업의 중요 정보를 보호하고, 안정된 시스템의 유지는 업무효율을 가져오고 정보보호 솔루션으로 부각되고 있다.

3. 웹 컨텐츠 변경 탐지 시스템의 설계

네트워크 상의 불법 침입은 해가 갈수록 증가하고 다변화되고 있다. 또한 인터넷의 발전과 더불어 네트워크의 시스템 상호간의 협력이 중시되고 있다. 악의적인 사용자들의 독창적이고 새로운 침입 방식의 개발은 침입탐지에 대한 어려움을 증가시키고 있다. 기존의 침입탐지 시스템들은 갈수록 다양해지는 침입에 대해 능동적으로 대처하는데 어려움이 따른다. 전자상거래 환경의 컨텐츠에 대한 효율적인 탐지 구조가 필요하게 되었다. 따라서 이를 고려한 새로운 형태의 탐지 시스템 구조를 제시하고자 한다. 그래서, 전자상거래 컨텐츠의 불법적인 침입에 대한 모니터링을 유지하고 시스템의 안전성을 갖춘 컨텐츠 감시 시스템 설계한다. 컨텐츠 보호를 위해 불법 해킹이나 바이러스로부터 시스템 자원의 손상을 막기 위한 관제를 실시하는 컨텐츠 침입 모니터링 시스템을 제시하고자 한다.

3.1 컨텐츠 침입 모니터링 시스템 구조

컨텐츠 모니터링은 침입자의 행위를 지속적으로 모니터링하여 컨텐츠 침입탐지를 분석하여 침입대응에 대처할 수 있도록 방법을 본 논문에서는 그림 1과 같이 제안한다.

컨텐츠 침입 모니터링 구성도의 그림 1에서 컨텐츠 분석은 전자상거래의 원활한 처리를 위한 기본적인 업무 분석을 파악하는 것이다.

3.1.1 컨텐츠 분석

웹메일 및 이메일의 사용과 사용자가 본 웹서핑화

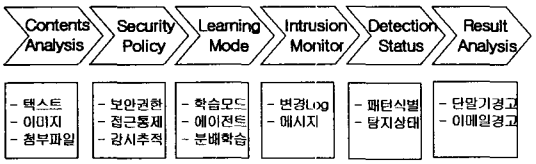


그림 1. 컨텐츠 침입 모니터링 구성도

면, 업로드된 웹 데이터, 인스턴스 메신저 사용 현황 등, 대부분의 웹 컨텐츠를 모니터링한 텍스트, 이미지, 메일의 첨부파일 등의 캡처링한 데이터를 DB에 저장한다. 웹사이트의 불법적인 위·변조를 검증하고 탐지하여 컨텐츠의 내용 점검 및 분석을 공유하여 침입에 대한 준비를 한다.

3.1.2 보안 정책

컨텐츠 분석을 근거로 시스템에서 정의된 보안 정책을 권한에 따른 접근 통제를 실시한다. 접근 통제를 위한 보안 레이블이 주체 및 객체에 대한 결합 표시, 객체 재사용, 감시 추적 등을 반영한다. 그리고, 시스템 저장 영역 내에 남아 있는 데이터가 없도록 모든 저장 영역을 우선적으로 재 할당하여 방문 차단 URL, 바이러스 탐지, 불법적인 컨텐츠 위·변조를 방지하도록 한다.

3.1.3 학습 모드

컨텐츠에 대한 불법적인 위·변조를 파악할 수 있는 기초 정보를 제공하는 것으로 컨텐츠 정보에 대한 학습 에이전트가 수행된다. 컨텐츠에 대한 각각의 학습 에이전트 파악은 학습모드에 전달되어 결합시킨다. 이것은 불법 침입 패턴을 연속적인 학습 에이전트를 통해 전달되어 불법 침입 패턴에 대한 빠른 분배 학습이 가능하게 한다.

3.1.4 침입 모니터링

컨텐츠에 대한 불법적인 위·변조를 학습모드를 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.

3.1.5 탐지 상태

컨텐츠에서 어떤 페이지에 오래 머무는지, 어떤 페이지를 인쇄하는지, 어떤 제품을 구매하는지 등과 같은 행동을 바탕으로 컨텐츠에 대한 적절한 정보 이용을 통해 컨텐츠의 패턴을 식별하는 탐지 상태를 표시한다.

3.1.6 결과 분석

사용자의 웹, 이메일 및 웹 메일, 인스턴스 메신저 등의 사용 현황을 실시간으로 모니터링하여 탐지된 상태를 근거로 데이터를 분석하여 경고, 지정 단말기 경고, 이메일 경고 등의 실시간 경고를 제공한다. 모니터링된 데이터를 차후에 다시 검색할 수 있도록 결과를 분석하여 기간별, 사용자별, 특정 단어 검색, 조건에 맞는 검색 결과를 요약 등의 검색을 제공한다.

3.2 컨텐츠 침입 모니터링 동작 모델

컨텐츠 모니터링은 전자상거래의 컨텐츠를 모니터링함으로써 컨텐츠의 침입 차단 정보를 수집한다. 컨텐츠의 메시지 형태로 전송되는 보안 정보들을 학습모드를 거쳐서 모니터링 관리기로 관리 또는 조작한다. 침입탐지 관리기는 모니터링 관리기로부터 전송되는 사용자의 웹, 이메일 및 웹 메일, 인스턴스 메신저 등의 사용 현황을 실시간으로 모니터링하고 모니터링된 모든 데이터를 분석하여 즉시 경고, 지정 단말기 경고, 이메일 경고 등의 실시간 경고를 제공하는 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 2의 설명으로 보안정책은 프로토콜 스택상 응용 계층 단계로 보안기능 요구사항인 신분확인, 접근통제, 무결성, 비밀성, 감사기록 및 추적, 보안관리

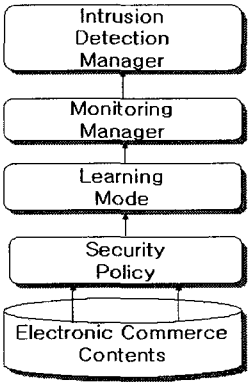


그림 2. 컨텐츠 모니터링 동작 구조

의 사항을 보안관련 데이터와 보안기능을 안전하게 유지하기 위한 기능이다. 학습 모드는 보안정책을 반영한 침입 패턴의 연속적인 학습을 위한 에이전트 구조이다. 침입 패턴에 대한 빠른 분배 학습이 가능한다. 모니터링 관리기는 시스템에 관한 취약점 정보를 파악하기 위해 공격하는 것을 침입시도라고 하는데 이런 침입 시도 공격에 대응과 컨텐츠 정보 유출 및 변경에 대한 컨텐츠 침입을 감시한다.

컨텐츠 모니터링 시스템 구성 요소는 침입 증상과 보안 정책에 따라 적절히 관제 처리된 기준 페이지(Base Page) 창과 변조 페이지(Modified Page) 창이 해당 페이지에 띄우고, 바뀐 내용에 해당하는 부분은 수정된 페이지 로그(Modified Page Log)창에 보일 수 있도록 나타난다.

4. 웹 컨텐츠 변경 탐지 시스템 구현

컨텐츠 모니터링 시스템 개발은 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 모니터링 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.

4.1 프로젝트 생성

파일 메뉴에서 새 프로젝트를 클릭한다. 프로젝트 이름과 프로젝트 위치를 설정하여 작업되는 프로젝트들이 저장할 위치를 만든다.

4.2 침입 모니터링 관제 사이트 지정

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.

4.3 침입 모니터링 서브 페이지 추가

프로젝트 창에서 추가된 사이트를 선택하고 오른쪽 마우스를 클릭하여 서브 페이지 추가를 하면 원하는 사이트 내의 서브 페이지 URL들이 나타나다. 서브 페이지에 원하는 사이트 내의 서브 페이지 URL들을 선택하면 된다.

4.4 침입 모니터링 관제 결과

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

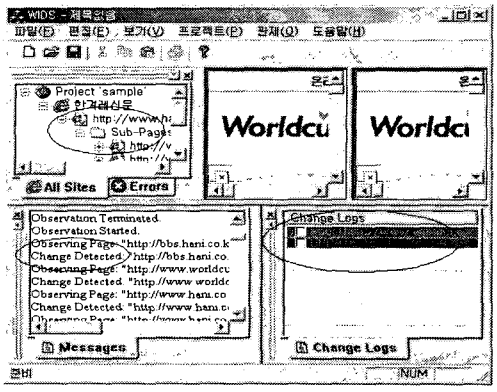


그림 3. 컨텐츠 침입 모니터링 결과

5. 컨텐츠 탐지 성능 평가

5.1 컨텐츠 모니터링 결과 분석

관제 옵션 설정 후 관제 메뉴에서 관제 시작하면, 설정된 관제 사이트와 서브 페이지들을 관제하기 시작한다.

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.

5.2 컨텐츠 모니터링 성능 분석

컨텐츠 모니터링 시스템은 Solaris에 Linux 운영체제이며, DBMS는 MySQL을 사용하고 J2EE를 이용하여 구현했다. 컨텐츠 침입탐지, 침입추적을 실시간으로 수행할 수 있어 각 컨텐츠에 대한 모니터링 정보, 침입추적 결과, 침입자에 대한 정보를 관리자에게 제공한다.

그림 4의 결과에서 변화패턴 무시하기는 Modified Log창에서 체크박스를 체크한 후 오른쪽 마우스를 선택하면 해당된 변화가 학습 패턴에 추가되어 이후의 관제에서 동일한 변화는 무시된다. 변화패턴 검출은 Modified Log창에서 체크박스를 체크한 후 오른쪽 마우스를 선택하면 해당된 변화가 학습 패턴에서 삭제되어 이후의 관제에서 동일한 변화는 검출된다. 심각한 변화로 분류는 해킹으로 의심되는 변화가 발생한 경우로 Modified Log창에서 체크박스를 체크한 후 오른쪽 마우스를 선택하면 해당된 변화는 프로젝트 창의 "Errors" Tab으로 이동되어 심각한 변화로 표시된다. 일반적인 변화로 분류는 해킹으로 의심되어 심각한 변화로 분류되었으나 해킹이 아닌 정상적인 변화로 판명된 변화는 Modified Log창에서 체크박스를 체크한 후 오른쪽 마우스를 선택하면 해당된 변화가 다시 일반적인 변화로 분류되어 프로젝트 창의 "All Sites" Tab으로 이동되어 표시된다. 아래 표 1은 기존의 침입탐지와 대응을 위한 시스템들의 항목을 제안된 시스템과 비교한 것이다.

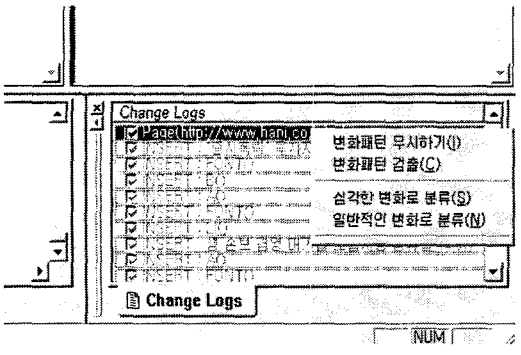


그림 4. 컨텐츠 모니터링 결과

기존의 침입대응 시스템은 host 또는 Network에 해당되는 것만 모니터링하는 경우가 많았지만, 본 제안 시스템은 침입에 대한 모니터링을 통해서 host와 Network을 동시에 실시간 감시하면서 컨텐츠를 보호하여 기존의 보안관리 시스템보다 침입에 대한 대응시간을 최소화할 수 있다.

6. 결 론

인터넷을 통해 전세계 정보를 쉽게 얻을 수 있고 전자상거래의 컨텐츠 활용으로 새로운 유통구조를 형성하고 있다. 또한, 끊임없이 연결되는 네트워크는 전세계 어디든지 접속을 할 수 있고, 이것은 정보 보호의 필요성을 요구하게 된다.

본 논문에서는 웹 환경에서의 보안 취약성과 정보 노출에 대한 문제점의 원인을 분석함으로써 컨텐츠 보안의 빠른 지원을 결정할 수 있고, 안정적인 컨텐츠 시스템을 이용할 수 있다. 또한, 모니터링된 정보를 이용하여 정보 보안 취약성과 정보 노출을 보호하는데 있다.

본 논문의 웹 컨텐츠 변경 탐지 시스템은 컨텐츠에 대한 불법적인 침입을 차단할 수 있는 모니터링을 수행한다. 이것은 컨텐츠의 불법 침입을 신속하고 능동적으로 대처할 수 있고, 침입에 대한 피해를 최소화할 수 있다. 컨텐츠 모니터링 도구는 웹에 대한 개별적인 모니터링을 통해 웹 메일이나 이메일, 메신저 등의 사용 현황을 실시간으로 탐지할 수 있어 기밀정보 유출을 대비한 기업의 정보를 보호할 수 있다. 또한, 컨텐츠 관리에 소요되는 자원을 효율적으로 활용

표 1. 침입대응시스템 성능 비교

구 분	IDES[2]	NSM[3]	USTAT[4]	제안시스템
탐지원리	anomaly	hybrid	policy	hybrid
탐지시간	realtime	realtime	realtime	realtime
측정대상	host	network	host	both
측정형태	passive	passive	passive	active
Data수집	distributed	centralized	centralized	distributed
보안관리	static	static	static	extensible

하고 컨텐츠 관리에 필요한 인력 손실을 방지할 수 있다. 본 논문의 컨텐츠 탐지 시스템은 안정된 웹 컨텐츠 사용으로 해킹이나 바이러스로부터 시스템을 보호 할 수 있다.

참 고 문 헌

[1] S. Garfinkel, G. Spafford, *Practical UNIX and Interent Security, 2nd Ed. Oreilly & Associates Inc.*, pp. 731-757, 2002. 11.

[2] T.F.Lunt, R.Jagannathan, R.Lee et al., "IDES: The enhanced prototype, A Real-time Intrusion Detection System," Technical report SRI-CSL-88-12, Computer Science Laboratory, SRI International, USA, October 1988.

[3] T.Hebelein, G.Dias, K.Levitt et al, "A Network Security Monitor," *Processing of the IEEE Symposium on Resaerch in Security and Privacy*, pp. 296-304, 1990,

[4] K. Ilgun, R. A. Kemmerer, and P. A. Porras, "State transition analysis: A rule based intrusion detection approach," *IEEE transactions on Software Engineering*, vol.21. no.3. pp. 181-199, march 1995.

[5] Martin Roesch, "Snort-Lighweught Instrusion Dectection for Networks," *USENIX LISA '99 Conference*, 1999.

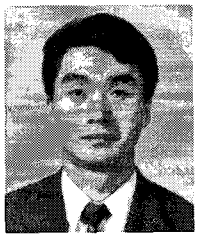
[6] Solar Designer, "Designing and Attacking Port Scan Decrction Tools," *Phrack magazine Vol .8* Issue 53. 1998.

[7] 서동일, 최병철, 손승원, 이상호, "해킹 기법을 이용한 내부망 보안 평가 방법", 정보처리학회 논문지 제9-C권 제3호, pp. 337-342, 2002. 6.

[8] 장희진, 김상욱, "자기확장 모니터링 기반의 침입자동 대응 시스템", 정보과학회논문지 제28권 제4호, pp. 480-497, 2001. 12.

[9] 유일선, 조경산, "네트워크 취약점 검색공격에 대한 개선된 탐지시스템", 정보처리논문지 제8-C권 제5호, pp. 543-550. 2001. 10.

[10] 박수진,박명찬,이새롬,최용락, "실시간 e-mail 대응 침입시도탐지 관리시스템의 설계 및 구현", 정보처리논문지 제9-C권 제3호, pp. 359-366. 2002. 6.



김 영 선

1985년 광운대학교 전자계산기공학과(공학사)
1997년 광운대학교 전자계산학과(이학석사)
2000년 광운대학교 컴퓨터과학과(박사과정 수료)
1987년~1993년 (주) LG-CNS 근무
2000년 (주) 컴텍크 코리아 연구소장 역임
2000년~현재 대림대학 경영정보계열 조교수
관심분야 : 멀티미디어, UML, DB, XML, 무선 인터넷, 보안

장 덕 철

1974년 고려대학교 대학원 경영정보학석사
1982년 고려대학교 대학원 경영정보학박사
1979년 광운대학교 전자계산소 소장
1981년~1982년 버클리대학교 객원교수
1993년~1997년 광운대학교 전산대학원 원장
1995년~1997년 광운대학교 이과대학 학장
1977년~현재 광운대학교 컴퓨터과학과 교수
관심분야 : 멀티미디어, Internet DB 정보검색, UML, XML, SMIL, E-Commerce