韓國 컴퓨터情報學會 論文誌
第12卷 第1號, 2007. 3.

2007-12-1-2-7

통합보안관리 에이전트를 확장한 웹 어플리케이션 공격 탐지 연구

김 성 락*

A Study of Web Application Attack Detection extended ESM Agent

Sung-Rak Kim *

요 약

웹에 대한 공격은 웹 서버 자체의 취약점 보다 웹 어플리케이션의 구조, 논리, 코딩상의 오류를 이용한다. OWASP에서 웹 어플리케이션 취약점을 10가지로 분류하여 발표한 자료에 의하면 웹 해킹의 위험성과 피해가 심각함을 잘 알 수 있다. 이에 따라 웹 해킹에 대한 탐지능력 및 대응이 절실히 요구된다. 이러한 웹 공격을 방어하기 위해 패턴 매칭을 이용한 필터링을 수행하거나 코드를 수정하는 방법이 있을 수 있지만 새로운 공격에 대해서는 탐지 및 방어가 어렵다. 또한 침입탐지시스템이나 웹 방화벽과 같은 단위보안 제품을 도입할 수 있지만 운영과 지속적인 유지를 위해서는 많은 비용과 노력이 요구되며 많은 탐지의 오류를 발생한다. 본 연구에서는 웹 어플리케이션의 구조와 파라미터 입력 값에 대한 타입, 길이와 같은 특성 값들을 추출하는 프로파일링 기법을 이용하여 사전에 웹 어플리케이션 구조 데이터베이스를 구축함으로서 사용자 입력 값 검증의 부재에 대한 해결과 비정상적인 요청에 대해 데이터베이스의 프로파일 식별자를 이용하여 검증하고 공격 탐지가 가능하다. 통합보안관리시스템은 현재 대부분 조직에서 도입하여 운영하고 있으며 일반화 되어있다. 그래서 통합보안관리시스템의 보안 감사 로그 수집 에이전트에 웹 어플리케이션 공격 탐지 기능을 추가한 모델을 제시함으로서 추가 단위보안제품을 도입하지 않고서도 웹 어플리케이션 공격을 탐지할 수 있도록 하였다.

Abstract

Web attack uses structural, logical and coding error of web application rather than vulnerability to Web server itself. According to the Open Web Application Security Project (OWASP) published about ten types of the web application vulnerability to show the causes of hacking, the risk of hacking and the severity of damage are well known. The detection ability and response is important to deal with web hacking. Filtering methods like pattern matching and code modification are used for defense but these methods can not detect new types of attacks. Also though the security unit product like IDS or web application firewall can be used, these require a lot of money and efforts to operate and maintain, and security unit product is likely to generate false positive detection. In this research profiling method that attracts the structure of web application and the attributes of input parameters

• 제1저자 : 김성락
• 접수일 : 2007.2.14, 심사일 : 2007.2.18, 심사완료일 : 2007. 2.28.
* 오산대학 컴퓨터정보계열 부교수
※ 본 논문은 오산대학 산업기술연구소의 학술비지원금에 의한 연구실적물 임

such as types and length is used, and by installing structural database of web application in advance it is possible that the lack of the validation of user input value check and the verification and attack detection is solved through using profiling identifier of database against illegal request. Integral security management system has been used in most institutes. Therefore even if additional unit security product is not applied, attacks against the web application will be able to be detected by showing the model, which the security monitoring log gathering agent of the integral security management system and the function of the detection of web application attack are combined.

▸ Keyword : ESM, Intrusion Detection, Web Application

Ⅰ. 서 론

최근 웹 사이트의 해킹이나 금전적인 이득을 목표로 한 정보유출 시도 등 웹에 대한 공격이 급증하면서 웹 어플리케이션 보안의 중요성이 증가하고 있다. 웹 어플리케이션의 해킹은 전통적인 해킹기법에 비해 상대적으로 취약한 공개 소스 기반의 웹 어플리케이션 해킹으로도 진행되고 있다. 웹 페이지 변조에서부터 명의도용, 개인 신상 정보 유출 등 다양한 방식의 위협에 노출되어 있다[1][2][3][4]. 일반적으로 웹 어플리케이션은 운영체제 및 데이터베이스 시스템과 상호 동작하기 때문에 운영체제의 명령 수행이나 사용자 및 트랜잭션 정보와 같은 의도하지 않은 중요 정보의 노출 등이 발생할 수 있다. 특히 SQL 인젝션 공격 등은 웹 인터페이스를 통해 데이터베이스의 중요 정보를 노출시킬 수 있는 위협으로 많이 알려져 있다. 웹 어플리케이션에 대한 공격은 웹 서버 자체의 취약점을 이용하는 것이 아니라 특정 목적으로 작성된 웹 어플리케이션의 구조, 논리, 코딩상의 오류를 이용하는 것이다[1]. 웹 어플리케이션에 대한 보안 취약점과 관련하여 OWASP(Open Web Application Security Project)에서는 2004년 웹 어플리케이션 취약점을 10가지로 분류하여 발표였고 2007년 새로운 버전의 10가지 취약점을 작업중에 있다[1]. 이러한 웹 공격을 방어하기 위해 패턴 매칭을 이용한 필터링을 수행하거나 코드를 수정하는 방법이 있을 수 있지만 새로운 공격에 대해서는 탐지 및 방어가 어렵다[2]. 또한 웹 방화벽과 같은 단위보안 제품을 도입할 수 있지만 많은 비용과 노력이 요구된다. 기존의 통합보안관리시스템의 경우를 보면 웹 로그에 특정 문자열이 있는지 검사하여 공격을 탐지하는 패턴 매칭 기법을 이용하거나 특정 HTTP의 상태 코드값에 대한 발생빈도를 검사하는 정도이다[5][6].

본 연구에서는 웹 어플리케이션의 구조와 파라미터 입력값에 대한 타입, 길이와 같은 특성 값들을 추출하는 프로파일링 기법을 사용하여 사전에 웹 어플리케이션의 구조를 데이터베이스로 구축함으로서 비정상적인 요청의 경우 구축된 데이터베이스의 프로파일 식별자에 의해 탐지가 가능하다[7][8][9]. 프로파일링 데이터 수집은 웹 서버 로그를 이용하므로 기존 통합보안관리시스템에서 별도의 추가 비용이 없을 뿐만 아니라 웹 어플리케이션에 대한 비정상적인 요청의 탐지율을 증가시킬 수 있다.

Ⅱ. 관련 연구

1. 통합보안관리시스템

통합보안관리시스템의 정의는 전사적인 차원에서 일관된 정책을 가지고 정보보호시스템을 통합적으로 관제 및 운영, 관리함으로서 보안관리 업무의 효율화와 보안성 향상을 극대화 시킬 목적으로 사용되는 통합적인 보안관리 시스템을 말한다. 또한 네트워크에 산재한 정보보호시스템들을 통합 콘솔로 관리하고 유사한 보안 정책을 갖는 보안시스템 간에 정책을 통일시켜 전체적인 보안성을 향상 시키는 통합시스템이라고도 한다. 결과적으로 이기종 정보보호시스템의 효율적 운영(정책관리, 침해대응, 이벤트 통합관리/분석)등을 통한 사전적 사고예방을 목적으로 하며 넓게는 IT자산 인프라에 대한 가용성, 무결성, 보안성을 보장하기 위한 위험관리라고도 볼 수 있다[6][10][11].

일반적으로 3-tier 형태로 구현되어 있으며, 단계별 관리에 의해 2-tier 나 4-tier 형태를 갖기도 한다. 구현방법에 따라 구조만 다를 뿐 처리방법은 비슷하다. 3-tier 형태의

구조를 살펴보면 정보보호시스템들과 이기종 장비에서 이벤트를 실시간으로 수집해오는 에이전트, 중앙에서 통합적으로 에이전트의 이벤트를 DB에 저장/분석 하는 매니저, 그리고 사용자가 GUI 환경에서 보안정책을 설정하고 이벤트를 분석할 수 있는 콘솔처럼 3가지로 구성되며 (그림 1)과 같다.

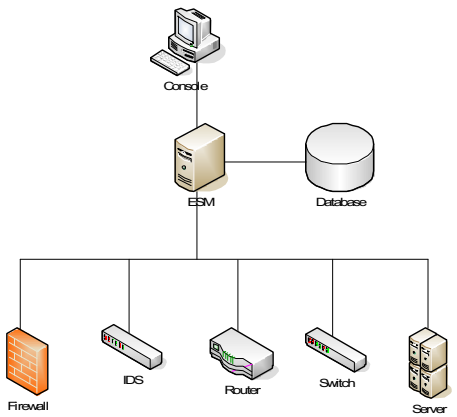

그림 1. 3-tier 통합보안관리시스템 구조
Fig. 1 Architecture of 3-tier ESM

현재 상용화되어 있는 통합보안관리 시스템들의 기능을 정리해보면 〈표 1〉과 같다. 즉 단위보안시스템에서 발생된 보안감사 이벤트들을 실시간 수집, 분석하여 보안경보를 발령하고 대응할 수 있다. 스팸메일 필터링제품, PC 보안제품, 문서 보안제품, 웹 어플리케이션 방화벽 등 정보보호관련 제품이 최근 몇 년간 다양하게 개발되었고 조직의 정보보호를 위해 도입되고 있다. 하지만 수많은 정보보호 제품을 한정된 인원으로 운영, 관리하고 침해사고 대응을 용이하게 하기 위해서는 통합보안관리시스템의 도입이 필연적이라 할 수 있다. 제안한 시스템에서는 다양한 이기종의 보안감사 이벤트를 수집하는 수집에이전트에 웹 어플리케이션 공격을 탐지할 수 있도록 설계하였다.

표 1. 통합보안관리시스템 기능명세
Table. 1 Function Specification of ESM

구분	기능설명
관리 및 운영 방안	Console의 Client/Server형 또는 웹 형태로 GUI 지원
	관리대상 시스템의 파일 무결성 점검 기능
	관리자별/운영자별 등급제한으로 인한 그룹관리 기능
	운영자 등급별 ESM 접속 사용 기능 제한
	동일한 이벤트에 대한 운영자별 선택적 모니터링
	ESM 사용자 접속 및 작업이력 관리 기능
	DB로 저장되는 이벤트 보관주기 설정 및 자동 백업
	에이전트 기능 추가 또는 Upgrade시 자동 Patch 기능
이벤트 수집	관리대상시스템과의 다양한 통합방법 (API, SNMP Trap, Syslog, Log File) 제공
	필요한 이벤트 만을 필터링 할 수 있도록 구현
통합 관제	Real-Time 모니터링 및 침입 분석 기능
	각 시스템별 이벤트의 하나의 창에서의 모니터링
	이기종 이벤트간 실시간으로 직관적인 방법 (Drag & Drop)으로 상호 연계 분석
	의심스러운 사용자, 서버에 대한 특별관리 (Black List DB)
	이기종 IDS의 서로 다른 위험도 평가에 따른 정형화된 기준 제시
	Real-Time 알림/경보(Notice/Alert) 기능
	Sound, E-mail, SMS 등 다양한 방법으로 경보제공
	위험 등급관리에 의한 Threshold 지정 및 경보기능
상호 연계 분석	하나의 보안장비에서 발생하는 패턴의 이상 징후 분석, 실시간 상호연관성 분석 기능
	탐지된 이상 징후를 실시간으로 운용자에게 알릴 수 있는 Alert 기능
	조합할 수 있는 Correlation-Rule 수의 무제한 적용
	Correlation Rule의 운용자에 의한 쉬운 추가 및 변경
리포팅	시스템 Resource 사용량 및 가동상태 통계보고서
	블랙리스트 대응보고서 등의 침해대응 운영보고서
	보고서의 사용자 정의 및 스케줄링에 의한 자동생성
기타	관리대상시스템에 Agent가 탑재될 경우, 데이터 송수신의 암호화 및 비암호화 통신 지원

2. 프로파일 기반 침입탐지시스템

침입탐지기술은 악의적인 공격에 대한 침입을 탐지하기 위한 중요한 기술로 네트웍상의 트래픽을 모니터링하며 시스템에 침입하려는 시도나 분산 서비스 거부 공격과 같은 시도를 탐지한다[5]. 네트웍 보안기술은 네트웍 트래픽을 모니터링하고 분석하며, 침입패턴을 인식하여 보안경보를 발생시킨다. 이 과정에서 침입패턴을 인식할 수 있는 방법으로 시그너처(Signature) 방식과 프로파일(Profile)을 기반으로 하는 방식이 있다. 시그너처 방식이 정확한 탐지와 실시간 분석이 가능하여 많이 사용되었으나 웹 어플리케이션 공격에 대해서는 적용하기 어렵다. 왜냐하면, 웹 어플리케이션 공격은 다양한 원인과 변형된 특성들을 가지고 있어서 기존 시그너처 방식처럼 특정 패턴을 찾기 어렵다. 프로파일 기반의 침입탐지시스템은 정상행위를 기준으로 이와 상반되는 행위를 침입으로 간주하는 방법이다. 즉, 프로파일 탐지기법은 공격행위가 정상행위와 다르다는 점을 가정한다. 프로파일은 네트웍 트래픽에 대한 데이터 마이닝, 감사 데이타 분석을 통한 통계적 분석, 그리고 운영체제 시스템 콜을 이용한 시퀀스분석으로 나누어진다[7][8].

제안 시스템에서는 감사 데이타 분석을 이용한 통계적인 분석으로서 웹 어플리케이션 요청 값의 파라미터 정보를 분석하고 데이터 타입, 허용 가능한 문자열, 입력 값의 길이

등을 학습한다. 그리고 정상행위 프로파일을 생성하고 이와 비교하여 웹 어플리케이션 공격을 탐지한다.

3. 웹 어플리케이션 공격탐지 연구

3.1 웹 어플리케이션 방화벽

일반적으로 '웹 방화벽' 이라 부르는 웹 어플리케이션 방화벽은 어플리케이션 계층 분석 기술로 침입탐지시스템이나 침입방지시스템이 탐지할 수 없는 웹 관련 공격들을 방어할 수 있다. 웹 어플리케이션 방화벽은 분석해야 할 자료를 어디에서 얻는 지 여부에 따라 네트워크 기반과 웹 서버 기반으로 나눌 수 있다[12]. 네트워크 기반은 네트워크를 지나는 http/https 트래픽을 분석하므로 웹 서버의 종류와 상관없이 보호가 가능하다는 장점이 있는 반면, 웹 서버 기반은 웹 서버가 제공하는 API를 기반으로 구현돼 IIS (Internet Information Server)나 아파치 웹 서버의 플러그인 형식으로 탑재된다[13].

일반적으로 웹 어플리케이션 방화벽은 포지티브 시큐리티 모델(Positive Security Model)과 네거티브 시큐리티 모델(Negative Security Model)을 혼합해 구현된다. 포지티브 시큐리티 모델은 안전하다고 정의된 것만 허용하고 나머지는 모두 금지하는 보안 모델이며 반면에 네거티브 시큐리티 모델은 위험하다고 정의된 것만 거부하고 나머지는 모두 허용하는 보안 모델이다. 이러한 웹 보안기능을 수행하기 위해 웹 애플리케이션 방화벽은 웹 서버와 웹 브라우저 사이에 인라인(In-line) 방식 등으로 구성된다. 인라인 방식 구성은 일반적인 방화벽과 같이 라인 중간에 웹 애플리케이션 방화벽이 들어가는 형식으로 구축되며, 사용자가 웹 어플리케이션 방화벽의 존재를 인식하지 못하는 네트워크 투명성을 제공하며 별도로 네트워크 구성을 변경할 필요가 없다. 그러나 웹 방화벽에 문제가 생길 경우 웹 서비스 자체에 영향을 준다. (그림 2)는 웹 방화벽을 네트웍에 도입하여 단위보안제품과 함께 침입을 탐지할 수 있는 구성을 보여준다. 즉, 방화벽은 서비스 거부공격등을 차단하고 침입방지시스템은 웜을 차단하고 웹 방화벽에서는 웹 관련 주요공격을 탐지하고 차단한다.

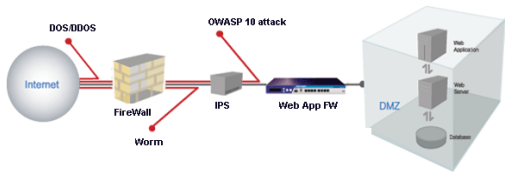

그림 2. 웹 어플리케이션 방화벽
Fig. 2 Web Application Firewall

3.2 통합보안관리시스템 웹 로그 분석 방법

통합보안관리시스템은 다양한 이기종 단위보안제품들의 로그를 자동으로 수집하여 분류하고 정규화, 필터링 과정을 거쳐 분석한다. 웹 로그의 경우 웹 서버의 종류에 상관없이 다음과 같이 2가지 기준으로 분류하여 공격을 탐지한다[6].

첫 번째 방법으로 웹 프로토콜인 http의 상태코드에 따라 초당 몇 번의 이벤트가 발생되었는지를 기준으로 공격을 판단할 수 있다. 상태코드 값은 IETF의 RFC 2616에 정의되어 있다.

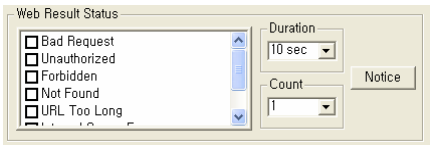

그림 3. 상태코드 설정
Fig. 3 Configuration of Web Status Code

두 번째 방법으로 사용자가 직접 문자열을 입력하여 특정 문자열의 로그가 발생할 경우 공격으로 탐지하여 경보를 발령할 수 있다.

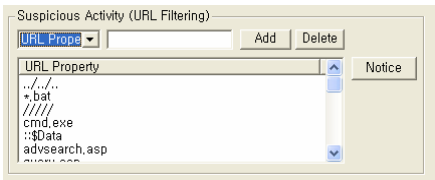

그림 4. 의심스러운 문자열 설정
Fig. 4 Configuration of Suspicious Activity

위 두 가지 방법으로는 특정이벤트에 대해서는 정확히 탐지할 수 있지만 예측할 수 없는 다양한 조건에 대해서는 탐지가 어렵다.

III. 제안시스템 구조

1. 웹 어플리케이션 공격탐지 에이전트 설계

ESM 에이전트는 관리대상 장비의 시스템 감사로그 및 보안 감사로그를 수집한다. 이때 수집한 로그를 처리하기 용이한 형태로 정규화하고 필터링 하게 된다. 그리고 동일한 형태의 로그가 지정 시간 동안 여러 번 반복되어 발생할

경우 축약을 한다. 수집된 데이터들을 암호화하여 ESM 매니저에 전송한다.

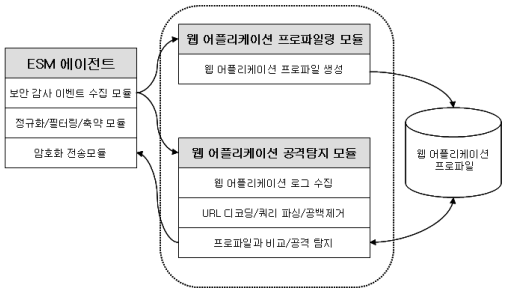

그림 5. 제안시스템 구조
Fig. 5 System Architecture of a proposition

제안시스템에서는 웹 어플리케이션에 대한 입력 값 검증을 하고 비정상 입력 탐지성능을 향상시키기 위해 (그림 5)와 같이 설계하였다. 추가된 모듈로는 웹 어플리케이션 프로파일링 모듈과 공격탐지모듈이며 웹 어플리케이션 프로파일을 생성한다. 웹 방화벽과 같은 단위 보안제품을 설치할 경우 추가 장비 및 별도의 독립 모듈을 기존 웹 서버 모듈에 추가하여야 한다. 그래서 웹 방화벽에 문제가 발생하면 웹 서비스에 치명적인 영향을 준다. 제안한 시스템은 운영중인 웹 서비스에 전혀 지장을 주지 않고 ESM 에이전트의 확장 모듈로 추가하여 탐지 성능을 개선할 수 있었다.

웹 어플리케이션 프로파일링 모듈은 처음 웹 어플리케이션이 개발 완료되었거나 웹 어플리케이션이 수정되었을 경우 실행되어질 수 있다. 즉, 웹 서버에 정상적인 요청을 하고 생성된 웹 서버 로그를 ESM 에이전트가 수집하고 웹 어플리케이션 프로파일링 모듈에 전달한다. 프로파일링 모듈은 웹 서버 요청 쿼리를 분석하여 프로파일을 생성한다. 이때 생성된 프로파일은 포지티브 시큐리티 모델을 적용하였다. 즉, 정상적인 경우에 대한 프로파일이다. 또한 프로파일 데이터 수집을 웹 서버 로그로부터 생성하기 때문에 프록시 형태의 구조가 필요 없다. 웹 어플리케이션 공격탐지 모듈은 프로파일 생성 이후, 실 운영에서 웹 어플리케이션의 비정상적인 요청에 대하여 입력값을 검증하고 공격을 탐지한다. 수집된 웹 서버 요청 URL 내에 유니코드 지원을 위해 인코딩된 데이터는 URL 디코딩 과정을 통해 변환한다. 공백 문자를 모두 제거함으로 프로파일 레코드와 비교하는데 용이하도록 하고 쿼리를 분석하고 공격을 탐지한다.

2. 웹 어플리케이션 프로파일링 기법

웹 어플리케이션 프로파일은 웹 어플리케이션의 구조를 파악하여 이를 데이터베이스화하는 것이다. 즉, (그림 6)과 같은 사용자 요청 데이터를 분석하여 (그림 7)과 같은 프로파일 데이타를 생성하게 된다. 사용자 요청은 '?' 문자로 구분되며 뒤쪽에 파라미터 변수와 값이 '=' 문자를 통해 대응된다. 웹 어플리케이션 프로파일링 모듈은 레코드 구성에 각 파라미터 변수를 연결하여 프로파일 레코드의 구분자인 ID 값을 구성한다.

http://hostname/cgi-bin/test.cgi?p1=v1&p2=v2&p3=v3&....pn=vn 과 같은 사용자 요청이 있을 경우 요청에 대한 ID 값은 /cgi-bin/test.cgi-p1-p2..pn 으로 구성하였다. 그리고 해당 ID 에 대응되는 파라미터 테이블들을 구성함으로서 비정상적인 요청을 탐지한다.

그림 6. 웹 어플리케이션 요청 정보
Fig. 6 Request information of web application

(그림 6)은 프로파일을 생성하기 위하여 TeleportPro 프로그램을 이용한 요청정보의 일부내용이다[14]. 이 프로그램은 웹 페이지의 링크를 전체 탐색하여 복제할 수 있으며 정상적인 요청에 대한 프로파일을 생성할 수 있다. 본 연구에서 제안한 모듈들 중에서 웹 어플리케이션 프로파일링 모듈에서 처리한 결과 값은 (그림 7)과 같다. 다양한 정상적인 요구들에 대하여 ID 값을 기준으로 프로파일을 생성하고 해당 ID 별로 파라미터 값들을 연결하였다. 이때 파라미터의 순서, 종류, 최대 길이 값을 정리하였다. 이 값은 입력값 검증에 이용된다. (그림 7)은 웹 어플리케이션의 프로파일 내용이다. 라인의 첫 글자가 # 으로 시작되는 부분은 주석이며 ID로 시작되는 라인은 프로파일에 대한 ID와 상세 프로파일에 대한 개수가 정의된다. "ID=/gmboard/bbs/idpass_find.php-db;1;' 내용에서 ID 는 /gmboard/bbs/idpass_find.php-db 이며 구분자(;)의 다음 숫자 1은 상세 프로파일내용의 개수 이며 다음 상세 라인의 수이다. SEQ-TYPE-LEN=0;105;40; 은 명칭=순차번호;타입;길이의 형식으로 설정되어 있다. SEQ-TYPE-LEN 은 사전에 정의된 구분자이다. 다음 숫자 0 은 순차번호 이며

0부터 시작된다. 다음 숫자 105 는 메타문자로 사전에 정의된 코드를 의미한다. 다음숫자 40은 입력값의 최대 길이를 의미한다. 다시 정리하면 첫 번째 프로파일의 ID 는 /gmboard/bbs/idpass_find.php-db 이며 메타문자로 구성되며 입력값은 1개 이며 최대 40 자 까지 입력가능하다.

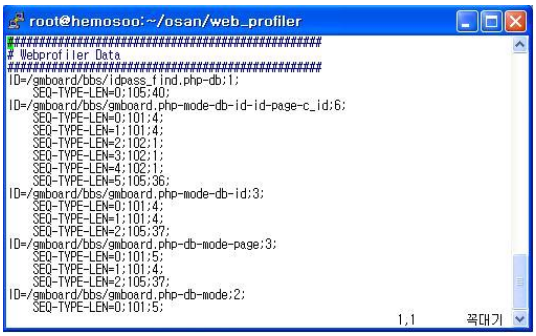

그림 7. 웹 어플리케이션 프로파일 내용
Fig. 7 Description of web application profile

프로파일의 파라미터값을 분석한 값 중 종류는 5가지로 분류하여 정의하였다. 즉 해당 파라미터값에 알파벳값이 입력되어야 하는데 특수문자가 입력된다면 비정상 입력으로 처리될 수 있다. 코드번호 101은 알파벳 대소문자로 구성된 문자로 정의하였고 코드번호 102는 1에서 0까지 숫자로 구성된 문자열로 정의하였다. 코드번호 103은 알파벳과 숫자의 혼합된 형태로 정의하였고 104번은 파일명에 사용가능한 문자열로 정의 하였다. 코드번호 105번은 모든 문자들을 통합한 형태로 정의하였다.

```
#define T_ALPHA  101    /* 알파벳 ( A-Za-z ) */
#define T_NUMBE 102    /* 숫자  (1-0)    */
#define T_ALNUM 103  /* 알파벳과 숫자 (A-Z a-z 1-0) */
#define T_FICHA  104    /* 파일명에 사용가능한 문자열 (A-Z a-z
1-0 /_+-)  */
#define T_META  105    /*  그 외 문자 */
```

3. 비정상공격 탐지 방법

본 연구에서는 웹 어플리케이션 입력값 검증을 통하여 공격을 탐지할 때 3가지 유형으로 나누어 탐지하였다. 첫 번째로 프로파일 식별자에 의한 공격탐지이다. 두 번째는 파라미터 변수 값의 타입에 의한 공격탐지 이다. 세 번째 방법은 파라미터 변수 값의 입력 값 길이에 의한 변화 탐지이다.

프로파일 식별자에 의한 탐지방법은 사용자의 입력 요청값이 프로파일 레코드에 존재하지 않을 경우 비정상 요청으로 간주하고 공격으로 판단한다. 공개소스기반의 대부분 웹 어플리케이션은 코드내의 내부변수들을 사용자가 직접 입력하는 공격이 가능하며 프로파일링기법으로 정상적인 조합에 대해서만 정의를 했기 때문에 새로운 변수가 URL에 입력되는 경우 탐지할 수 있다.

파라미터 변수값의 타입에 의한 공격탐지 기법은 사용자 입력 요청의 파라미터 변수값의 타입을 정의하여 사용한다. 알파벳 또는 숫자로 만 입력되는 파라미터에 대하여 특수문자 등이 입력될 경우 비정상 입력으로 판단하여 공격으로 탐지할 수 있다. 파라미터 변수값의 길이에 의한 공격탐지 기법도 사용자 입력요청의 파라미터 변수값의 최대 입력값을 정의하여 사용한다. 최대 길이 이상의 입력값이 들어올 경우 공격으로 탐지할 수 있다. 다음은 파라미터 입력 값의 예이다.

정상적인 입력

http://192.168.192.192/gmboard/bbs/gmboard.php?mode=view&db=free&id=

비정상적인 입력

http://192.168.192.192/gmboard/bbs/gmboard.php?mode=http://192.168.192.1/hack/test.php&db=free&id=

http://192.168.192.192/gmboard/bbs/gmboard.php?mode='or'1'='1&db=free&id=

Ⅳ. 성능평가

본 연구에서 구현한 웹 어플리케이션 공격 탐지 에이전트는 레드햇 리눅스 9.0에서 구현하였으며 Apache 웹 서버를 대상으로 시험하였다. 프로파일 데이터는 웹 로그 파일을 읽어서 프로파일 레코드를 생성하였다. 시험에 사용한 웹 어플리케이션은 〈표 2〉와 같은 공개용 웹 어플리케이션을 이용하였다.

표 2. 구현 및 성능 평가 환경
Table. 2 Environment of performance test

구현 환경	Red Hat Linux release
웹 서버	Apache/2.0.40
컴파일러	gcc version 3.2.2
시험용 웹 어플리케이션	phpBB 2.09
	gmBoard v1.5
	ZeroBoard 4.1

성능평가 방안은 첫 번째 방법으로 프로파일 비율을 분석한다. 웹어플리케이션 프로파일링 후 생성된 프로파일 레코드 수와 사용자 입력에 해당되는 웹 로그 건수를 비교하여 프로파일 비율을 분석한다.

두 번째 방법으로 통합보안관리시스템에서 탐지하는 공격탐지 건수, 즉 패턴비교에 의한 탐지와 프로파일에 의한 공격탐지 건수를 비교하였다.

1. 프로파일링 시험

정상적인 요청에 대한 프로파일링 시험은 3장에서 언급한 바와 같이 TeleportPro 프로그램을 이용하였고, 정상적인 요청을 하였을 경우 웹 로그에 남아있는 로그 개수와 프로파일링 모듈을 통해 생성된 프로파일 ID의 수를 비교하였다.

표 3. 프로파일 비율
Table. 3 Profile ratio

웹 어플리케이션	웹 로그 개수 (요청수)	프로파일 레코드수	프로파일 비율(%)
phpBB2	188	6	3.19 %
gmBoard	278	35	12.59 %
ZeroBoard	425	58	13.65 %

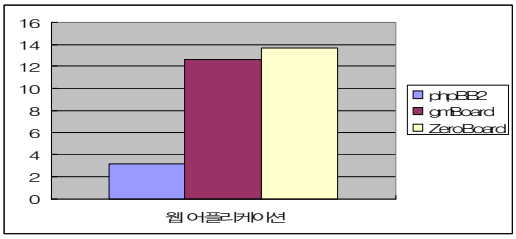

그림 8. 웹 어플리케이션 프로파일 비율
Fig. 8 Ratio of web application profile

프로파일 레코드 수는 웹 어플리케이션마다 웹 페이지 링크를 따라 생성된 것으로 해당 어플리케이션의 구조와 링크 수에 따라 차이가 있을 수는 있지만 결과적으로 요청수가 크게 늘어나도 프로파일의 레코드 수는 크게 증가하지 않게 된다. 또한 국내외 공개용 웹 어플리케이션을 대상으로 시험하였지만 〈표 3〉과 같이 웹 로그 개수가 증가하여도 프로파일 비율은 크게 증가하지 않는다. 정상적인 웹 어플리케이션에 대한 요청은 정형화 되어 있기 때문에 프로파일 기법으로 분류하여 비정상 요청을 탐지하는 방법이 효과적인 방법임을 유추할 수 있다.

2. 비정상 요청 탐지 시험 및 분석

비정상적인 요청을 탐지할 수 있는 성능을 비교하기 위해 비정상 요청 생성프로그램으로Acunetix 웹 취약점 스캐너 프로그램을 이용하였다[15]. 웹 어플리케이션 스캐너를 이용하여 웹 어플리케이션을 스캔 후 발생한 요청을 ESM 에이전트와 본 연구에서 제안한 웹 프로파일 탐지모듈이 각각 어느 정도 탐지할 수 있는지를 측정하였다. 웹 어플리케이션 스캐너는 OWASP에서 정의한 10가지 취약점에 대하여 종합적으로 취약점을 찾아내기 위하여 취약한 입력 값 등을 자동으로 입력하므로 시험도구로서 적합하다. 시험 내용은 Acunetix 웹 취약점 스캐너가 제공하는 여러 가지 스캔 방법 중 5가지 스캔 방법을 각각 나누어 적용한 후 전체 웹 서버 로그 건수와 제안시스템의 탐지 건수 그리고 기존 ESM 에이전트방식에서 탐지한 탐지 건수를 측정하여 서로 비교하였다.

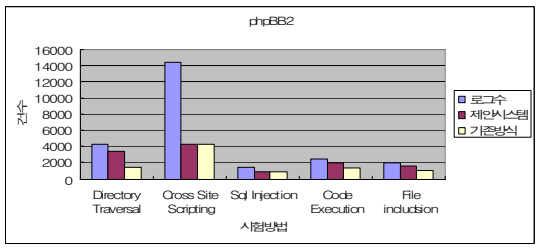

그림 9. phpBB2 웹 어플리케이션에 대한 공격 탐지 건수 결과
Fig. 9 Attack Detection Result of phpBB2 Web Application

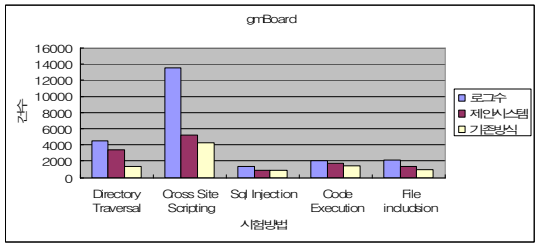

그림 10. gmBoard 웹 어플리케이션에 대한 공격 탐지 건수 결과
Fig. 10 Attack Detection Result of gmBoard Web Application

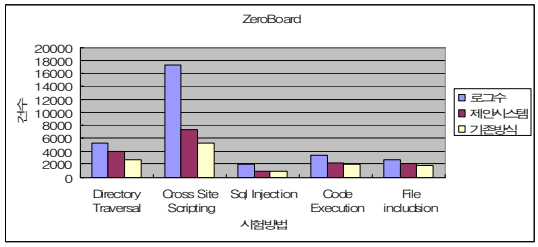

그림 11. ZeroBoard 웹 어플리케이션에 대한 공격 탐지 건수 결과
Fig. 11 Attack Detection Result of ZeroBoard Web Application

전체 실험 결과를 요약하면 제안 시스템이 기존 문자열 비교 방식에 비해서 탐지건수가 증가함을 알 수 있다. 웹

스캐너의 스캔, 즉 발생한 로그 대부분이 공격이기 때문에 건수가 증가하는 것은 그만큼 탐지성능이 개선된 것임을 알 수 있다. 공격 방법중 Sql 인젝션 시험방법에서는 거의 비슷한 탐지성능을 보인다. 왜냐하면 기존방식은 특정문자열 즉, SQL 키워드가 있으면 공격으로 탐지하기 때문에 스캔 내용을 대부분 공격으로 탐지한다. 실제 운영시 오탐 가능성이 매우 높다. 그러나 제안한 시스템은 SQL 키워드와 상관없이 특수문자 및 문자의 타입으로 공격을 결정하기 때문에 정확한 탐지를 할 수 있다. 그 외 디렉토리 이동공격(Directory Traversal), XSS(Cross Site Scripting) 공격, 코드실행(Code Execution) 공격, 파일삽입(File Inclusion) 공격에서 기존 방식보다 우수한 결과를 보였다.

V. 결 론

본 연구에서 제안한 모델은 웹 어플리케이션의 구조를 프로파일화하여 비교함으로써 공격의 오탐을 줄이고 탐지성능을 향상시킨다. 웹 어플리케이션의 경우 정형화된 형식을 통해 지정된 페이지를 요청하도록 구성하고 있기 때문에 프로파일 기반의 탐지방법이 효과적이다. 또한 통합보안관리시스템의 로그수집 에이전트에 웹 어플리케이션 공격을 탐지할 수 있도록 확장함으로써 추가 단위보안제품을 도입하지 않아도 되는 비용절감의 효과가 있다.

향후 연구로는 통합보안관리시스템의 다양한 단위보안제품의 감사로그와 상호연관지어 분석할 수 있는 알고리즘을 연구하고 탐지 및 대응능력을 향상시킬 수 있는 연구가 필요하다.

참고문헌

〔1〕 Jeffry R. Williams, "The Ten Most Critical Web Application Security Vulnerabilities", OWASP, 2004.

〔2〕 Christopher Kruegel, Giobanni Vigna, William Robertson, "A multi-model approach to the detection of web-based attacks", Computer Networks:Vol48, No.5, pp.717-738, Aug, 2005.

〔3〕 Mark Curphey, Joel Scambray, Erik Olson, "Improving Web Application Security : Threats and Countermeasures", Microsoft Corporation, 2003.

〔4〕 Robert Auger, Ryan Barnett, "Web Application Security Consortium : Threat Classification Version 1.0", Web Application Security Consortium(www.webappsec.org), 2004.

〔5〕 김성락, "상호연관성 분석을 이용한 웹서버 보안관리 시스템", 한국컴퓨터정보학회 논문지, 제 9권 4호, pp.157-165, 2004. 12.

〔6〕 (주)이글루시큐리티, " http://www.igloosec.co.kr"

〔7〕 윤영태, 류재철, 박상서, 박종욱, "프로파일기반 웹 어플리케이션 공격탐지 및 필터링 기법", 한국정보처리학회논문지C, 제 13-C권 제1호, pp.19-25, 2006, 2.

〔8〕 박채금, 노봉남, "웹 어플리케이션 보안을 위한 프로파일 기반 탐지시스템 설계", 한국정보처리학회 추계학술발표대회 논문집 제12권 제2호, pp.1055-1058, 2005, 11.

〔9〕 차병래, 박경우, 서재현, "이상 침입탐지를 위한 베이지안 네트워크 기반의 정상행위 프로파일링", 한국컴퓨터정보학회 논문지, 제 8권 1호, pp.103-113, 2003, 3.

〔10〕 어울림정보기술(주), "http://www.oullim.co.kr"

〔11〕 (주)제이컴정보, "http://www.jcsi.co.kr"

〔12〕 (주)모니터랩, "http://www.monitorapp.com/kr/"

〔13〕 Shreeraj Shah, "Defending Web Services using Mod Security (Apache)", NetSquare, 2004.

〔14〕 TelephortPro, "http://www.tenmax.com/telport/pro/home/htm"

〔15〕 Acunetix "http://www.acunetix.com/"

저 자 소 개

김 성 락

1984년 울산대학교 전자계산학과 (학사)

1989년 한양대학교 산업대학원 전자계산학전공(석사)

2003년 수원대학교 대학원 전자계산학과(박사)

1996년~현재 : 오산대학 컴퓨터정보계열 부교수

〈관심분야〉 웹보안, 웹프로그래밍, 동영상편집 등