게이트웨이형 웹 애플리케이션 방화벽 보호프로파일에 관한 연구

한국시스템보증 ▌윤 여 웅*
충북대학교 ▌이 상 호**

1. 서 론

인터넷은 다양한 형태의 서비스를 제공함으로써 사용자에게 많은 편리성을 제공하나 공격자에 의한 불법적인 자료 접근, 개인정보 유출 등의 다양한 취약점도 발생되고 있다. 이러한 취약점을 막기 위하여 침입차단시스템, 침입탐지시스템 등 다양한 정보보호제품들이 사용되고 있으며, 2002년부터 CC(Common Criteria) 기준을 도입하여 국제수준의 신뢰된 정보보호제품을 공급하고 있다.

최근 많은 애플리케이션이 웹을 기반으로 구축되고 있고 웹의 활용도가 증가함에 따라 웹 애플리케이션 취약점을 이용한 공격이 증가하고 있다. 웹 애플리케이션 공격이 증가하여 OWASP(Open Web Application Security Project)는 웹 애플리케이션 및 서비스의 보안을 이해하고 향상시키기 위하여 가장 심각한 10가지 웹 애플리케이션 보안 취약점을 발표하여 최소한의 대처를 권고했다.

정보보호업체는 웹 애플리케이션 공격을 방어할 수 있는 다양한 정보보호제품을 개발하고 있다. 이러한 정보보호제품 중의 하나가 게이트웨이형 웹 애플리케이션 방화벽이며 대부분의 제품이 OWASP에서 권고한 10가지 취약점에 대해 대처하고 있다.

보호프로파일은 ISO/IEC 15408 국제공통평가기준인 CC 평가를 위하여 특정 정보시스템 사용자가 요구하는 구현에 독립적인 IT 보안요구사항의 집합이며, 개발된 보호프로파일을 이용하여 정보보호제품에 대한 평가·인증을 보다 쉽게 받을 수 있다. 그러나, 현재 게이트웨이형 웹 애플리케이션 방화벽에 대한 보호프로파일이 개발되지 않아 평가준비에 어려움을 겪고 있다.

따라서, 본 연구에서는 OWASP 10대 취약점에 대응할 수 있는 게이트웨이형 웹 애플리케이션 방화벽 보호프로파일을 위한 보안환경, 보안목적, 보안기능요구사항을 제안하였으며, 게이트웨이형 웹 애플리케이션 방화벽 평가를 준비하는 업체에게 활용될 수 있을 것이다.

2. 관련연구

2.1 보호프로파일 개발

보호프로파일은 특정 정보시스템 사용자가 요구하는 구현에 독립적인 IT 보안요구사항의 집합이며, 개발자는 제시된 요구사항을 기반으로 정보보호제품에 대한 보안목표명세서를 쉽게 작성할 수 있다[1~3]. 그러나, 보호프로파일 없이 보안환경, 보안목적, IT 보안요구사항을 작성할 수 있는 정보보호업체는 많지 않으며, 작성할 수 있다하더라도 사용자의 요구사항을 분석해야 하며, 이를 토대로 보안목표명세서를 작성해야 하므로 많은 시간과 비용이 소요된다. 이러한 개발자의 어려움을 해소시켜주기 위하여 특정 정보보호제품에 대한 보호프로파일이 개발·보급되고 있으며,

표 1 연도별 개발된 PP 수

연도	1998	1999	2000	2001	2002	2003	2004	2005	2006
개발된 PP 수	11	9	17	16	8	10	6	21	9

표 2 제품군별 개발된 PP 수

제품군	안티 바이러스	생체 인식	데이터 베이스	침입차단 시스템	침입탐지 시스템	접근 제어	공개키 관리	스마트 카드	VoIP	가상 사설망	무선 랜	기타
개수	2	3	5	8	9	7	22	28	1	3	2	17

* 정회원
** 종신회원

표 3 웹 애플리케이션 10대 취약점

구 분	특 징
입력값 검증 부재	웹 애플리케이션이 웹요청을 처리하기 이전에 적절한 검증을 누락시키는 취약점
취약한 접근통제	인증된 사용자만이 허용된 작업을 수행하도록 통제하지 못하는 취약점
취약한 인증 및 세션관리	계정토큰과 세션토큰을 적절히 보호하지 못하는 취약점
크로스 사이트 스크립팅 취약점	웹 애플리케이션이 다른 사용자의 브라우저를 공격할 수 있는 도구로 사용되는 취약점
버퍼 오버플로우	웹 애플리케이션이 사용자의 입력값을 적절히 점검하지 못하는 취약점
삽입 취약점	취약한 웹 애플리케이션을 통해 다른 시스템에 악성코드를 전송할 수 있는 취약점
부적절한 에러처리	일상적인 운용과정 중에 발생하는 에러 상황에 대해 적절한 처리가 되지 않는 취약점
취약한 정보저장 방식	정보나 인증관련 토큰을 보호하기 위해 부적절하게 암호화하는 취약점
서비스 방해 공격	웹 애플리케이션 자원을 고갈시켜 정당한 사용자가 서비스를 사용하지 못하는 취약점
부적절한 환경 설정	부적절한 환경설정이 서버를 안전하지 않은 상태로 만드는 취약점

최근까지 개발되어 보급된 연도별 PP 수와 제품유형별 PP 수는 표 1, 2와 같다[4~9].

현재까지 알려진 웹 관련 보호프로파일은 3가지가 있다[10~12]. "U.S. Government Protection Profile Authorization Server for Basic Robustness Environments v1.0"은 개발이 완료되었고 인증서버 제품에 대한 보안기능 및 보증 요구사항을 명세하였으며, 웹서버, 데이터베이스, 애플리케이션 서버 등의 IT 자원으로의 접근통제를 지원한다. "U.S. Government Protection Profile for Web Servers in Basic Robustness Environments v0.61"은 개발 중에 있으며 모든 웹 서버에 대한 최소한의 보안 요구사항을 명세하였다. "Web Browser Protection Profile v0.5"는 개발이 보류되었으며, 다양한 웹 서버의 저장된 정보를 검색하고 웹 서버 접근을 위한 웹브라우저에 대한 최소한의 보안요구사항을 명세하였다.

2.2 웹 애플리케이션 취약점

웹 애플리케이션 취약점은 OWASP에서 발표한 10가지 취약점이 잘 알려져 있으며, 폼필드 변조, 쿠키변조, 크로스 사이트 스크립팅, SQL 삽입 등의 공격을 포함하며, 주요 특징은 표 3과 같다[13].

2.3 웹 애플리케이션 정보보호제품

웹 애플리케이션 정보보호제품은 웹 해킹 등으로부터 웹 애플리케이션을 보호하는 전용솔루션으로 침입방지시스템(IPS : Intrusion Prevention System)이 탐지할 수 없는 웹 관련 공격들에 대해 방어한다. 웹 애플리케이션 방화벽, 웹 취약성 스캐너, 애플리케이션 소스코드 검사 도구 등이 개발되고 있으나 웹 애플리케이션 방화벽이 대부분을 차지하고 있다.

웹 애플리케이션 방화벽은 분석해야 할 데이터를 어디로부터 얻느냐에 따라 네트워크 기반과 웹서버 기반으로 구분할 수 있으며, 네트워크 기반의 방화벽이 게이트웨이형 웹 애플리케이션 방화벽이다. 게이트웨이형 웹 애플리케이션 방화벽은 웹 서버로 접근하는 모든 HTTP 또는 HTTPS 네트워크 트래픽을 분석하므로 웹 서버의 종류와 무관하게 보호를 할 수 있다. 웹서버 기반 웹 애플리케이션 방화벽은 웹 서버가 제공하는 API를 기반으로 웹 서버의 플러그인 형태로 설치된다.

일반적으로 게이트웨이형 웹 애플리케이션 방화벽은 긍정 보안모델(Positive Security Model)과 부정 보안모델(Negative Security Model)을 혼합하여 구현된다. 긍정 보안모델은 안전하다고 정의한 것만 허용되고 나머지는 모두 거부되며, 방화벽의 앞부분에 위치하여 등록된 URL에 대한 접근통제 등을 수행한다. 부정 보안모델은 위험하다고 정의된 것만 거부되고 나머지는 모두 허용하는 보안모델로써 긍정 보안모델을 통과한 웹 트래픽에 대해서만 검사를 수행하며 비정상적인 패턴의 침입탐지 등을 수행한다.

국내에서 개발된 게이트웨이형 웹 애플리케이션 방화벽은 ASROC R4, WEB Insight, WEBFRONT, WAPPLE-SECURITY Gateway, nProtect WebFirewall 등이 있으며, OWASP의 취약점에 대해 대응하는 것으로 알려져 있다[14~18].

따라서, 최근 주로 개발되고 있는 게이트웨이형 웹 애플리케이션 방화벽에 대한 보호프로파일이 개발되지 않아 본 연구에서 제안하고자 한다. 제안되는 보호프로파일은 OWASP에서 발표한 10가지 취약점을 방어할 수 있도록 작성되었으며, 본 연구에서 제시된 보안환경, 보안목적, 보안기능요구사항을 게이트웨이형 웹 애플리케이션 방화벽 평가를 준비하는 업체가 활용할 수 있을 것이다.

3. 게이트웨이형 웹 애플리케이션 방화벽 보안환경

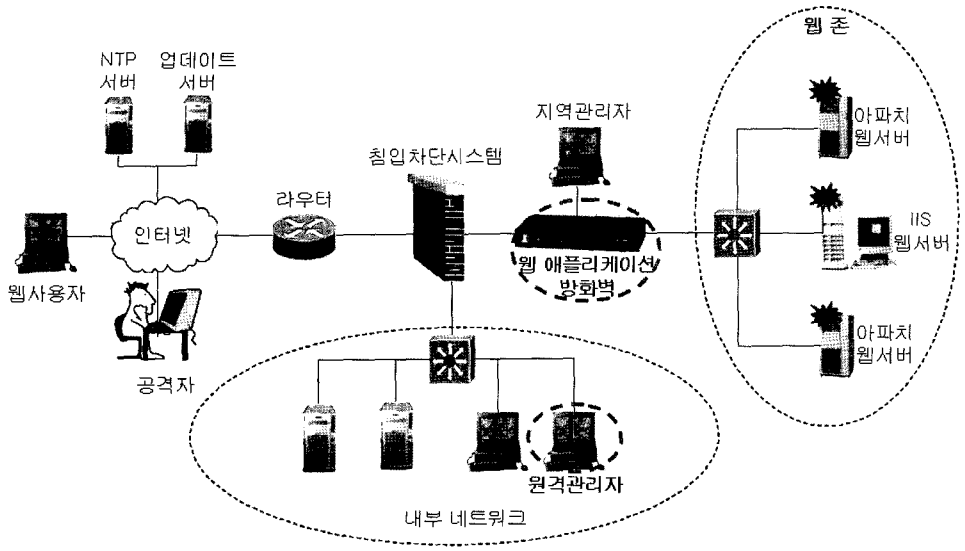


그림 1 일반적인 운영환경

게이트웨이형 웹 애플리케이션 방화벽 보안환경은 방화벽에 대한 운영환경 분석을 기반으로 가정사항, 보안위협, 조직의 보안정책을 명세하였다.

3.1 운영환경

게이트웨이형 웹 애플리케이션 방화벽의 운영환경은 그림 1과 같은 구조를 가지며, 공격자의 불법적인 접근 등으로부터 웹서버에 존재하는 중요 데이터를 보호한다.

웹사용자, 공격자, 시간동기화를 위한 NTP(Network Time Protocol) 서버, 최신의 탐지 시그니처를 유지하기 위한 업데이트 서버는 인터넷에 연결되어 있고, 아파치 또는 IIS 웹서버 등은 웹 존에 위치한다. 최신의 탐지 시그니처는 중요한 TSF 데이터이므로 안전하게 송수신되어야 한다. 웹 애플리케이션 방화벽의 보안관리를 위한 원격관리자는 내부 네트워크에 위치하며, SSL(Secure Socket Layer)을 통하여 안전하게 통신한다.

게이트웨이형 웹 애플리케이션 방화벽은 침입차단시스템 뒷단에 위치하며 웹 존 내의 다양한 웹서버로 유입되는 또는 웹서버로부터 유출되는 모든 HTTP/HTTPS 패킷에 대한 정보흐름을 통제한다. 유입되는 정보흐름 통제 시 성능적인 부분을 고려하여 긍정 보안모델과 부정 보안모델을 혼합하여 수행한다. 긍정 보안모델을 통하여 허용된 트래픽만을 통과시키고 통과된 트래픽에 대해 부정 보안모델을 적용하여 공격에 대한 추가적인 탐지를 한다. 또한, 웹 애플리케이션 방화벽은 유

표 4 가정사항

가정사항	설 명
A.물리적보안	TOE는 인가된 관리자만이 접근할 수 있는 물리적으로 안전한 곳에 위치한다.
A.유일한연결점	TOE는 네트워크 상에 설치될 때 네트워크를 인터넷과 웹 존으로 분기해주며, 인터넷과 웹 존 간의 모든 통신은 TOE를 통해서만 이루어진다.
A.신뢰된관리자	TOE를 관리하는 인가된 관리자는 악의가 없으며, TOE 관리를 위하여 적절히 교육 받았고, 관리자 지침에 따라 관리를 수행한다.
A.보안유지	네트워크 구성 변경, 호스트의 증감, 서비스의 증감 등으로 내부 네트워크 환경이 변화할 때, 변화된 환경과 보안정책을 즉시 TOE 운영정책에 반영하여 이전과 동일한 수준의 보안을 유지한다.
A.안전한외부서버	TOE의 보안기능을 위해 TOE에게 신뢰된 시간과 최신의 탐지 시그니처를 제공하는 업데이트 서버와 NTP 서버는 안전하다.
A.SSL프로토콜	TOE는 원격지 관리자와의 안전한 채널을 형성하기 위해 SSL 프로토콜을 사용한다.
A.운영체제보강	TOE에 의해 필요하지 않은 운영체제 상의 서비스나 수단 등을 제거하는 작업과 운영체제 상의 취약점에 대한 보강 작업을 수행하여 운영체제에 대한 신뢰성과 안전성을 보장한다.
A.SSL인증서	SSL 인증서는 SSL 통신을 위하여 미리 생성되어 TOE에 저장되고 안전하게 관리된다.
A.TIME	TOE는 RFC 1305를 따르는 NTP 서버 또는 OS로부터 신뢰할 만한 Timestamp를 제공받는다.
A.원격관리자	원격관리자는 안전하고 신뢰된 내부 네트워크에 위치한다.

표 5 보안위협

보안위협	설 명
T.가장	위협원은 인가된 관리자 또는 웹사용자로 가장하여 TOE 또는 웹서버에 접근할 수 있다.
T.고장	위협원은 TOE의 고장 등을 발생시켜 TOE가 웹사용자에게 정상적인 서비스를 제공하지 못하게 할 수 있다.
T.기록실패	위협원은 다량의 보안관련 이벤트를 발생시킴으로써 저장공간을 소진시키고 TOE가 보안관련 사건을 기록하지 못하게 할 수 있다.
T.불법서비스접근	위협원은 웹서버의 허가되지 않은 서비스에 접근을 시도하여 웹 서버가 제공하는 중요 정보를 불법적으로 획득할 수 있다.
T.서비스과다요청	위협원은 웹 서버에서 제공하는 웹 서비스를 과다하게 요청하여 정상적인 웹사용자가 웹 서비스를 제공받지 못하게 할 수 있다.
T.우회접근	위협원은 TOE의 보안기능을 우회하여 TOE 또는 웹서버에 접근할 수 있다.
T.인증우회	위협원은 웹 서비스 요청 시 허가되지 않은 SQL 구문 삽입 및 버퍼 오버플로우 공격을 통하여 정상적인 인증 과정을 거치지 않고 웹 서버의 관리자 권한을 획득할 수 있다.
T.유해프로그램삽입	위협원은 웹 서비스 요청 시 스크립트나 실행 파일을 삽입하여 중요 정보를 불법적으로 획득할 수 있다.
T.정보변조	위협원은 웹 서비스 요청 시 폼필드를 변조하여 웹 서버의 오동작을 유발하거나 쿠키를 변조하여 타인의 권한을 획득할 수 있다.
T.암호화된정보	위협원은 웹 서비스 요청 정보를 암호화하여 TOE가 해석하지 못하도록 할 수 있다.
T.중요정보획득	위협원은 정상적인 웹 요청을 통하여 웹 서버가 부주의하게 관리하고 있는 중요 정보를 획득할 수 있다.
T.오정보제공	위협원은 웹 서버가 공격으로부터 변조된 잘못된 정보를 웹 클라이언트에게 제공하도록 할 수 있다.
T.비정상적인웹요청	위협원은 비정상적인 웹 서비스 요청을 통하여 허용되지 않은 웹 서비스에 접근할 수 있다.
T.새로운취약점공격	위협원은 웹 존에 위치한 TOE 또는 TOE 운영환경의 새로운 취약점을 악용하여 공격할 수 있다.

입되는 정보흐름통제뿐만 아니라 웹서버로부터 유출되는 주민등록번호, 신용카드정보 등과 같은 중요정보에 대해 추가적인 정보흐름통제를 수행한다.

3.2 가정사항

서술된 운영환경을 토대로 게이트웨이형 웹 애플리케이션 방화벽에 대한 보호프로파일은 표 4와 같이 10가지의 가정사항이 도출되었다.

3.3 보안위협

게이트웨이형 웹 애플리케이션 방화벽에 대한 보호프로파일은 OWASP의 알려진 취약점과 운영환경을 기반으로 표 5와 같이 14가지의 보안위협을 도출하였다.

3.4 조직의 보안정책

게이트웨이형 웹 애플리케이션 방화벽은 운영하는 조직에 따라 보안정책이 상이할 수 있으나 아래 표와 같이 일반적으로 적용가능한 2가지 보안정책을 도출하였으며, 조직 특성에 따라 보안정책을 추가할 수 있다.

4. 게이트웨이형 웹 애플리케이션 방화벽 보안목적

본 연구에서는 앞서 도출된 가정사항, 보안위협, 조직의 보안정책을 기반으로 표 7과 같이 TOE에 대한 보안목적을 도출하였다.

5. 게이트웨이형 웹 애플리케이션 방화벽 보안기능요구사항

본 연구에서는 앞서 도출된 보안목적을 기반으로 표 8과 같이 TOE에 대한 보안기능요구사항을 제안하였다. 또한, 각 보안기능요구사항을 통하여 구현되어야 할 게이트웨이형 웹 애플리케이션 방화벽이 제공해야 하는 보안기능을 간략히 서술하였다.

표 6 조직의 보안정책

조직의 보안정책	설명
P.감사	보안과 관련된 모든 행동에 대한 책임을 추적하기 위해 보안관련 사건은 기록 및 유지되어야 하며, 기록된 감사데이터는 검토되어야 한다.
P.안전한관리	인가된 관리자는 관리지침에 따라 안전한 방법으로 TOE를 관리해야 한다.

표 7 TOE 보안목적

보안목적	설명
O.가용성	TOE는 우발적 또는 외부 공격에 의해 고장이 발생 시 최소한의 보안기능을 유지하여 정상적인 서비스를 제공해야 한다.
O.감사	TOE는 보안과 관련된 행동의 책임추적이 가능하도록 보안관련 사건을 기록 및 유지해야 하며, 기록된 데이터를 검토할 수 있는 수단을 제공해야 한다.
O.관리	TOE는 TOE의 인가된 관리자가 TOE를 효율적으로 관리할 수 있는 관리수단을 안전한 방법으로 제공해야 한다.
O.식별	TOE는 TOE에 접근하고자 하는 관리자와 웹서버로 접근하는 웹사용자를 식별해야 한다.
O.인증	TOE는 식별 후 TOE 또는 웹서버에 접근을 허용하기 전에 관리자 또는 웹사용자를 인증해야 한다.
O.TSF데이터보호	TOE는 TOE에 저장된 TSF 데이터를 인가되지 않은 노출, 변경, 삭제로부터 보호해야 한다.
O.서비스접근제어	TOE는 웹 서버의 허가되지 않은 서비스에 접근하여 중요 정보를 획득하려는 불법적인 접근을 차단해야 한다.
O.서비스과다요청 차단	TOE는 TOE를 통과하는 패킷 중 웹 서비스에 대한 과다한 요청을 차단해야 한다.
O.인증우회차단	TOE는 정상적인 인증 과정을 거치지 않고 웹 서버의 관리자 권한을 획득하려는 허가되지 않은 SQL 구문 삽입 및 버퍼오버플로우 공격을 차단해야 한다.
O.유해프로그램 삽입차단	TOE는 중요 정보를 불법적으로 획득하려는 웹 서버로의 스크립트 삽입 또는 실행 파일 업로드를 차단해야 한다.
O.정보변조차단	TOE는 웹 서버의 오동작 또는 타인의 권한을 획득하려는 폼필드 또는 쿠키 변조를 차단해야 한다.
O.암호화된정보처리	TOE는 웹 서버로 전송되는 암호화된 패킷을 해석하여 유해성 여부를 판별하여야 한다.
O.중요정보노출차단	TOE는 웹 서버의 부주의한 관리로 인한 중요 정보의 노출을 차단해야 한다.
O.오정보제공차단	TOE는 웹 서버가 변조된 오정보를 웹사용자에게 제공하는 것을 차단해야 한다.
O.비정상적인웹 요청차단	TOE는 웹사용자의 비정상적인 HTTP 메서드, HTTP 헤더 또는 URL을 가진 웹 요청을 차단해야 한다.
O.학습	TOE는 보안정책에 의해 차단된 웹사용자의 요청 패킷에 대한 정보를 학습하는 기능을 제공해야 한다.
O.최신시그너처갱신	TOE는 업데이트 서버로부터 최신의 시그너처를 주기적으로 업데이트해야 한다.

표 8 TOE 보안기능요구사항

보안기능 클래스	보안기능 컴포넌트	보안기능 클래스	보안기능 컴포넌트
보안감사	FAU_ARP.1(보안 경보)	식별 및 인증	FIA_AFL.1(인증 실패 처리)
	FAU_GEN.1(감사 데이터 생성)		FIA_ATD.1(사용자 속성 정의)
	FAU_GEN.2(사용자 신원 연관)		FIA_UAU.1(인증)
	FAU_SAA.1(잠재적인 위반 분석)		FIA_UAU.7(인증 피드백 보호)
	FAU_SAR(감사 검토)		FIA_UID.1(식별)
	FAU_SAR.3(선택가능한 감사 검토)	보안 관리	FMT_MOF.1(보안기능 관리)
	FAU_SEL.1(선택적인 감사)		FMT_MSA.1(보안속성 관리)
	FAU_STG.1(감사 증적 보호)		FMT_MSA.3(정적 속성 초기화)
	FAU_STG.3(감사 데이터 손실 예측시 대응행동)		FMT_MTD.1(TSF 데이터 관리)
	FAU_STG.4(감사 데이터의 손실방지)		FMT_SMF.1(관리기능 명세)
			FMT_SMR.1(보안 역할)
암호지원	FCS_CKM.1(암호키 생성)	TSF 보호	FPT_AMT.1(추상기계 시험)
	FCS_CKM.2(암호키 분배)		FPT_FLS.1(장애시 안전한 상태 유지)
	FCS_CKM.4(암호키 파기)		FPT_RVM.1(TSP 우회불가성)
	FCS_COP.1(암호 연산)		FPT_SEP.1(보안기능 영역분리)
사용자 데이터 보호	FDP_IFC.1(1)(부분적인 정보흐름통제(1))		FPT_STM.1(신뢰할 수 있는 타임스탬프)
	FDP_IFC.1(2)(부분적인 정보흐름통제(2))		FPT_TST.1(TSF 자체 시험)
	FDP_IFC.1(3)(부분적인 정보흐름통제(3))	자원활용	FRU_FLT.1(오류에 대한 내성 : 부분적용)
	FDP_IFF.1(1)(단일 계층 보안속성(1))		FRU_RSA.1(최대 할당치)
	FDP_IFF.1(2)(단일 계층 보안속성(2))	TOE 접근	FTA_SSL.3(TSF에 의한 세션 종료)
	FDP_IFF.1(3)(단일 계층 보안속성(3))	안전한 경로/채널	FTP_ITC.1(TSF간 안전한 채널)

(1) 보안감사

TOE는 보안관련 사건에 대해 감사기록하며 잠재적인 보안위반 사건에 대해서는 경보를 전송한다. 다량의 감사기록을 발생시킬 수 있으므로 관리자가 감사기록되는 보안관련 사건을 선택할 수 있으며 기록된 감사데이터를 검토할 수 있다. 또한, TOE는 저장된 감사데이터를 보호하고 손실을 방지하기 위하여 손실예측 시 대응행동을 수행하며 감사 저장소가 포화인 경우 손실을 방지한다.

(2) 암호지원

TOE는 웹사용자와 웹서버간 전송되는 트래픽 중 웹서버의 보호를 위하여 암호화된 HTTPS 트래픽에 대해 복호화한 후 유해성을 판별해야 한다. 이를 위해 TOE는 암호키를 생성하고 분배하며 파기할 수 있는 능력을 가져야 하며 분배된 암호키를 이용하여 복호화한다.

(3) 사용자 데이터 보호

TOE는 웹서버로 유입되는 HTTP/HTTPS 트래픽에 대하여 긍정 보안모델에 대한 정책(FDP_IFC/IFF.1(1))과 부정 보안모델에 대한 정책(FDP_IFC/IFF.1(2))이 요구된다. TOE는 긍정 보안모델의 허용 정책을 기반으로 설정된 정책과 일치하는 경우 트래픽을 통과시키며 허용되는 정책과 일치하지 않는 트래픽을 거부하고 거부된 정책은 학습된다. 또한, 긍정보안모델을 통과한 트래픽에 대해서 부정 보안모델의 거부정책과 일치하는 트래픽은 거부되며 일치하지 않는 트래픽은 모두 통과된다. TOE는 유입되는 트래픽뿐만 아니라 웹서버로부터 유출되는 HTTP/HTTPS 트래픽에 대하여 추가적인 정보흐름통제(FDP_IFC/IFF.1(3))가 요구되며, 주로 주민등록번호와 같은 중요 개인정보가 유출되는 것을 차단한다.

(4) 식별 및 인증

TOE는 안전한 보안관리를 위하여 TOE로 접속하려는 관리자와 웹서버로 접속하려는 웹사용자에 대해 식별 및 인증기능을 수행해야 한다. TOE는 관리자 및 웹사용자의 연속적인 인증 실패에 대해 적절히 처리해야하며 인증이 진행되는 동안 인증 피드백을 보호해야 한다.

(5) 보안관리

TOE는 주어진 관리자별 역할 및 권한에 따라 인가된 관리자에게 보안기능, 보안속성, TSF 데이터를 관리할 수 있도록 보안관리 기능을 제공하여야 한다.

(6) TSF 보호

TOE는 TOE 보안정책을 우회하는 것을 방지하고 보안기능 간 영역을 분리한다. 또한, 초기 시동 시 또는 주기적으로 하부추상기계 시험을 수행하고 신뢰할 수 있는 타임스탬프를 제공하며 TSF 및 TSF 데이터에 대해 무결성을 점검한다.

(7) 자원활용

TOE는 하드웨어적인 결함 또는 소프트웨어적인 결함과 같이 설정된 오류에 대해서 적절히 대처할 수 있어야 하며, 웹서버로 접속하려는 요청 세션에 대해서 적절히 통제할 수 있어야 한다.

(8) TOE 접근

TOE는 오랫동안 연결된 세션은 취약할 수 있으므로 인가된 관리자에 대한 보안관리 세션과 웹사용자의 웹서비스 요청 세션에 대해 종료할 수 있어야 한다.

(9) 안전한 경로/채널

TOE는 TSF와 원격의 신뢰된 IT 제품인 업데이트 서버 간, TSF와 원격관리자간에 안전한 통신을 제공해야 한다.

6. 보호프로파일 검증

보호프로파일 검증은 크게 3부분으로 구성하였다. OWASP에서 권장하고 있는 10대 취약점이 보안위협에 반영이 되었는지를 검증하고, 도출된 보안환경을 보안목적이 모두 만족하는지와 도출된 보안목적이 보안기능요구사항을 모두 만족하는지를 검증한다.

6.1 OWASP 취약점과 보안위협간 검증

표 9는 OWASP에서 권장하고 있는 10대 취약점과 도출된 보안위협간 상관관계를 나타낸 것이며, 모든 10대 취약점에 대하여 보안위협이 매핑된 것을 확인할 수 있다.

부적절한 에러처리 취약점은 웹서버가 요청에 대한 처리를 잘못하여 불필요한 정보가 제공될 수 있으므로 웹 애플리케이션 방화벽이 허용된 입력값만을 받아들이도록 해야하며 T.불법서비스접근, T.인증우회, T.정보변조, T.비정상적인웹요청과 매핑된다. 부적절한 환경 설정 취약점은 웹 존내에 있는 웹 서버의 잘못된 설정으로 인하여 인증 우회, 서비스 불법 접근, 과다요청 허용 등의 취약점이 발생될 수 있으며 T.가장, T.불법서비스접근, T.서비스과다요청, T.우회접근과 매핑된다.

표 9 OWASP 취약점과 보안위협간 상관관계

OWASP 취약점	보안위협
입력값 검증 부재	T.인증우회, T.정보변조, T비정상적인웹요청, T.오정보제공
취약한 접근통제	T.불법서비스접근
취약한 인증 및 세션관리	T.가장, T.우회접근
크로스 사이트 스크립팅 취약점	T.정보변조
버퍼 오버플로우	T.인증우회
삽입 취약점	T.인증우회
부적절한 에러처리	T.불법서비스접근, T.인증우회, T.정보변조, T.비정상적인웹요청
취약한 정보저장 방식	T.암호화된정보
서비스 방해 공격	T.고장, T.서비스과다요청
부적절한 환경 설정	T.가장, T.불법서비스접근, T.서비스과다요청, T.우회접근

6.2 보안환경과 보안목적간 검증

표 10은 보안환경과 보안목적간 상관관계를 나타내며, 도출된 TOE 보안목적은 모든 보안위협에 대해 대응하고 서술된 조직의 보안정책을 만족하였다.

6.3 보안목적과 보안기능요구사항간 검증

표 11은 보안목적과 보안기능요구사항간 상관관계를 나타내며, 도출된 TOE 보안기능요구사항은 TOE에 대한 보안목적을 모두 만족하였다.

7. 결 론

본 연구에서는 웹 애플리케이션 취약점을 분석하였고 현재까지 개발된 보호프로파일과 정보보호제품을 조사하였다. 이러한 조사를 통하여 국내에서는 게이트웨이형 웹 애플리케이션 방화벽이 주로 개발되고 있으나 평가를 위한 보호프로파일이 존재하지 않음을 확인하였다. 이를 토대로 본 연구에서는 게이트웨이형 웹 애플리케이션 방화벽에 대한 보호프로파일에 필요한 보안환경, 보안목적, 보안기능요구사항을 제안하였다.

제안된 보안환경은 게이트웨이형 웹 애플리케이션 방화벽의 운영환경에 대한 분석을 통하여 10개의 가정사항, 14개의 보안위협, 2개의 조직의 보안정책을 도출하였으며, 이러한 보안환경을 만족시키기 위한 TOE에 대한 보안목적과 정의된 보안목적을 만족시키기 위한 TOE 보안기능요구사항을 제안하였다. 또한, 웹 애플리케이션 취약점 분석으로부터 TOE 보안기능요구사항까지 정확히 정의되었는지를 검증하기 위하여 OWASP 취약점과 보안위협간 상관관계, 보안환경과 보안목적간 상관관계, 보안목적과 보안기능요구사항간 상관관계 분석을 통하여 정확히 정의되었다는 근거를 제시하였다.

본 연구는 OWASP에서 권장한 10대 취약점에 대응할 수 있는 게이트웨이형 웹 애플리케이션 방화벽을 개발하고 평가를 준비하는 정보보호업체에게 활용될 수 있을 것이다.

표 10 보안환경과 보안목적간 상관관계

보안환경 \ 보안목적	O.가용성	O.감사	O.관리	O.식별	O.인증	O.TSF 데이터 보호	O.서비스 접근제어	O.서비스 과다요청 차단	O.인증우회 차단	O.유해프로그램 게시차단	O.정보변조 차단	O.암호화된정보 처리	O.중요정보 노출차단	O.오정보 제공차단	O.비정상적인웹요청 차단	O.학습	O.최신 그너처 갱신
T.가장		X		X	X												
T.고장	X					X											
T.기록실패	X	X															
T.불법서비스접근							X									X	
T.서비스과다요청								X									
T.우회접근				X	X												
T.인증우회									X							X	
T.유해프로그램삽입										X						X	
T.정보변조											X						
T.암호화된정보												X					
T.중요정보노출													X				
T.오정보제공														X			
T.비정상적인웹요청															X		
T.새로운취약점공격																	X
P.감사		X															
P.안전한관리			X														

표 11 보안목적과 보안기능요구사항간 상관관계

보안목적 / 보안기능 요구사항	O. 가용성	O. 감사	O. 관리	O. 식별	O. 인증	O. TSF 데이터 보호	O. 서비스 접근 제어	O. 서비스 과다 요청 차단	O. 인증 우회 차단	O. 유해 프로그램 게시 차단	O. 정보 변조 차단	O. 암호화된 정보 처리	O. 중요 정보 노출 차단	O. 오정보 제공 차단	O. 비정상적 인 웹 요청 차단	O. 학습	O. 최신 시그너처 갱신
FAU_ARP.1		X															
FAU_GEN.1		X															
FAU_GEN.2		X															
FAU_SAA.1		X															
FAU_SAR.1		X															
FAU_SAR.3		X															
FAU_SEL.1		X															
FAU_STG.1		X															
FAU_STG.3	X	X															
FAU_STG.4	X	X															
FCS_CKM.1												X					
FCS_CKM.2												X					
FCS_CKM.4												X					
FCS_COP.1												X					
FDP_IFC.1(1)							X					X				X	
FDP_IFC.1(2)									X	X	X				X	X	
FDP_IFC.1(3)													X	X			
FDP_IFF.1(1)							X					X				X	
FDP_IFF.1(2)									X	X	X				X	X	
FDP_IFF.1(3)													X	X			
FIA_AFL.1					X												
FIA_ATD.1				X													
FIA_UAU.1					X												
FIA_UAU.7					X												
FIA_UID.1				X													
FMT_MOF.1			X														
FMT_MSA.1			X														
FMT_MSA.3			X														
FMT_MTD.1			X														
FMT_SMF.1			X														
FMT_SMR.1			X														
FPT_AMT.1						X											
FPT_FLS.1	X																
FPT_RVM.1							X										
FPT_SEP.1							X										
FPT_STM.1		X															
FPT_TST.1						X											
FRU_FLT.1	X																
FRU_RSA.1								X									
FTA_SSL.3			X														
FTP_ITC.1			X														X

참고문헌

[1] ISO/IEC 15408 Standard, Common Criteria for Information Technology Security Evaluation Version 2.3, 2005.

[2] ISO/IEC TR 15446, Guide for the production of Protection Profiles and Security Targets, 2004.

[3] Shoichi Morimoto and Jingde Cheng, Patterning Protection Profiles by UML for Security Specification, CIMCA-IAWTIC '05, 2005.

[4] CC Portal, http://www.commoncriteriaportal.org/public/expert/index.php?menu=8

[5] CCEVS(Common Criteria Evaluation and Validation Scheme), http://niap.bahialab.com/cc-scheme/pp/index.cfm

[6] CESG(Communications-Electronics Security Group), http://www.cesg.gov.uk/site/iacs/index.cfm?menuSelected=1&displayPage=19

[7] CSE(Communications Security Establishment), http://www.cse-cst.gc.ca/services/common-criteria/protection-profiles-e.html

[8] DCSSI(Central Information Systems Security Division), http://www.ssi.gouv.fr/en/confidence/pp.html

[9] BSI(Bundesamt für Sicherheit in der Informationstechnik), http://www.bsi.de/ cc/pplist/pplist.htm

[10] NIAP, U.S. Government Protection Profile Authorization Server For Basic Robustness Environments v1.0, 2005.6.

[11] NIAP, U.S. Government Protection Profile for Web Servers in Basic Robustness Environments v0.61, 2004.12.

[12] NIAP, Web Browser Protection Profile v0.5, 2001.4.

[13] OWASP(Open Web Application Security Project), The Ten Most Critical Web Application Security Vulnerabilities, 2004.

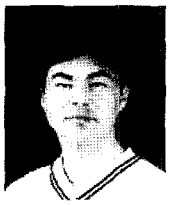
[14] ASROC R4, http://www.dualsecure.co.kr/dual/asrocr418.html

[15] WEB Insight, http://www.monitorapp.com/product/web.htm

[16] WEBFRONT, http://www.piolink.co.kr/korea/product/main2.asp

[17] WAPPLESECURITY Gateway, http://www.pentasecurity.com/korean/product2_1_ wapplesecurity.html

[18] nProtect WebFirewall, http://www.inca.co.kr/products/webfirewall.html



윤 여 웅

1996. 2 한남대학교 컴퓨터공학과 졸업(공학사)
1998. 2 한남대학교 대학원 컴퓨터공학과 졸업 (공학석사)
2000. 10~2006. 9 한국정보보호진흥원 선임연구원
2000. 3~현재 충북대 전기전자컴퓨터공학부 전자계산학과 박사수료
2006. 12~현재 한국시스템보증 평가팀장

관심분야 : 정보보호제품 평가, Security Testing, Network Security
E-mail : ywyun@kosyas.com

이 상 호

1976 숭실대학교 전자계산학과 졸업
1981 숭실대학교 전자계산학과 졸업(MS)
1989 숭실대학교 전자계산학과 졸업(PHD)
1976. 1~1979. 5월 한국전력 전자계산소
1981. 6~현재 충북대학교 전기전자컴퓨터공학부 교수

관심분야 : Protocol Engineering, Network Security, Network Management, Network Architecture
E-mail : shlee@chungbuk.ac.kr