웹서버에서의 보안 기술

안 혜 연*, 은 창 선**
(*(주) 시큐어 소프트)

1. 서 론

많은 기업들은 상거래의 효율성을 통해 이익을 창출하려 하고 있으며 이러한 효율성은 웹이라는 매개체를 통해 극대화 될 수 있다. 비단 이러한 효율성은 기업에만 국한하는 것은 아니며 많은 공공 기관과 개인들에게도 적용될 수 있다. 그러나 웹을 통한 정보공유는 항상 긍정적인 면만을 가지고 있는 것은 아니며, 반대로 이것은 많은 기업들의 정보가 웹상에 노출될 수밖에 없다는 것을 의미하기도 한다. 웹 보안이 취약한 상황에서 웹 서비스를 시행하는 것은 오히려 해커들에게 더욱 더 많은 범죄기회와 새로운 해커들을 유인하는 원천을 제공하게 되어, 결과적으로 기업에 막대한 손실을 줄 수 있는 위험을 낳게 한다.

또한 요즘 활동하는 해커의 경향은 단순히 명성을 얻거나 신용카드 번호를 알아내는 단순사기에서 기업의 중요 정보를 빼내는 지능적인 사기로 점차 바뀌고 있으며 그 대상도 웹을 이용하고 있는 모든 기업, 기관들로 확대되고 있다. 이러한 해커들에 의한 공격은 주로 웹서버의 취약점을 통해 이루어지고 있으며, 이러한 취약점을 막기 위해 필요한 방안과 해결책 그리고 이와 관련된 동향을 이 글에서 제시하고자 한다.

2.웹서버의 보안상 취약점

일반적으로 웹서버에서의 취약점은 웹서버 자체의 구현상 취약점, CGI 관련 취약점, 그리고 웹서버 구성상의 취약점으로 구분할 수 있다.

웹서버 구현상의 취약점은 공개용 웹서버 또는 상용 웹서버 자체의 구현상 문제로 인하여 보안 취약점이 생기는 것을 뜻하며 이와 관련된 구체적인 예는 표 1과 같다.

CGI와 관련된 취약점은 외부의 사용자에게 호스트의 정보를 보여주거나 또는 사용자 입력 양식(Form)을 통해서 임의의 명령을 수행할 수 있는 취약점이 뜻하며 이와 관련된 구체적인 예는 다음과 같다.

표 1. 웹서버 구현상의 취약점

웹서버	취약점
Apache	쿠키를 이용하여 프로그램 스택을 덮어씀으로써 임의의 명령을 수행할 수 있는 취약점이 있고, 디렉토리의 내용을 리스팅하는 취약점이 있다.
IIS 3.0	특정 길이의 URL을 IIS 웹서버로 전송하여 웹서버를 정지시킬 수 있는 취약점을 가지고 있다.(memory buffer overflow)

표 2. 보안 취약점이 알려진 CGI 목록

nph-test-cgi	phf	php
finger	web-dist	wrap
view-source	jj	query
wwwcount	handler	guestbook
websendmail	campas	webgais
Glimpse	Stronghold	test-cgi
AnyForm	FormMail	Excite
pfdisplay	Info2www	htmlscript

마지막으로 웹서버 구성상의 취약점은 웹서버 구성의 잘못으로 인한 파일 접근 권한 획득, 디렉토리 내용 리스팅, 심볼릭 링크 등의 취약점을 의미한다.

이러한 취약점들을 막기 위한 일반적인 대응 방법들이 3절에서 다루어지고 있으며, 이들 취약점과 관련된 정보들은 보안관련 웹 사이트를 통해 얻을 수 있다.

3. 웹서버에 대한 보안대책

일반적으로 웹서버 보안 강화를 위한 대책은 크게 두 가지 관점에서 마련될 수 있다.

첫째는 웹서버 자체에 대한 보안 기능 강화로 웹서버에 SSL, TLS을 지원하여 웹상에 안전한 통신 채널을 제공하도록 하는 것이며 Keberos, Fortezza 등과 같은 여러 가지 인증 수단을 지원하고 이들에 대한 암호화 수준을 높여 사용자에 대한 접속 통제를 하는 것이다. 현재 출시되어 있는 대부분의 웹서버 제품들이 이를 지원하고 있다. 표[3]은 실제 웹서버 제품[1]에서 이용되고 있는 보안 항목들이다.

표 3. 웹서버에 구현되어 있는 보안 기능들[2]

보안 기능	IIS 3.0	Apache 1.1.3	Enterprise Server
Password/challenge-response authentication	OO	OO	OO
Supports SSL v.3	O		O
Access control handled by OS	O		
Access control handled by server		O	O
Access control handled by domain name	OO	OO	OO
Can control access to documents		O	O
Can control access to parts of documents	O		
Creates private certificates			O
Scripts or wizard for creating certificates	O	O	O

다른 하나는 웹서버의 취약점으로 알려진 부분들을 제거하거나 보완하여 웹서버의 보안취약점을 없애는 것이다. 이에 대한 취약점 및 해결책은 대부분 웹 상에 공개되어 있어, 웹서버 공급 벤더 홈페이지나 그 밖의 웹서버 보안관련 홈페이지에서 제공하는 대책에 따라 적절히 조치를 취함으로써 취약점 문제를 해결될 수 있다. 다음의 표가 그러한 예[3]이다.

표 4. 웹서버 구현상의 취약점 및 대응책

웹서버	취약점	대응책
NCSA 1.3	HTTPd 버퍼 오버플로우	패치 설치
Apache 1.1.1	쿠키 버퍼 오버플로우 Indexes 명령어 취약점	Apache 1.1.3 이상으로 업그레이드
IIS 3.0 (Windows NT 4.0)	URL 취약점	서비스팩 설치

표 5. CGI 관련 취약점 및 대응책

CGI	취약점	대응책
Nph-test-cgi 스크립트	Nph-test-cgi 취약점	소스를 수정, 제거
Perl 5.003 이하	Suidperl 버퍼 오버플로우	5.004로 업그레이드
Count.cgi 버전 2.3 이하	Count.cgi 버퍼 오버런	2.4로 업그레이드

표 6. 웹서버 구성상의 취약점을 이용한 해킹방법 및 대응책

해킹방법	취약점	대응책
SSI의 #exec 이용	SSI의 #exec 명령을 부주의하게 사용할 경우 외부에서 임의의 명령 시행 가능	웹서버 구축시 SSI를 사용하지 않음
입력 FORM 이용	Form의 email주소 입력부에 임의의 명령을 추가, 외부에서 임의의 명령 수행가능	입력부에서 email 주소만 받아들이도록 필터기능 추가

위에서 언급된 보안 대책들은 웹서버에 대한 일반적인 보안 대책이며 현재 사용 중인 특정 웹서버에 대한 취약점을 파악, 해결하기 위해서는 ISS Suite, SATAN, Ballista와 같은 상용 또는 무료 웹 보안 진단 소프트웨어를 이용할 수 있다.

이 밖에도 웹서버에 대한 보안 관리 소프트웨어를 이용하여 보안을 강화할 수 있는데, 현재 시장에 출시된 제품으로는 WebStralker-Pro, ForceField, Trusted Web 등이 있으며 이들 제품이 가지고 있는 주요 보안 기능으로는 데이터에 대한 무결성 점검, 접근제어, 침입/오용에 대한 모니터링 등이 있다.

4. 발전방향

가트너 그룹에 따르면 향후 웹서버에 대한 보안은 다음과 같은 두 가지 모델을 바탕으로 이루어질 것이라고 예측하고 있다. 이러한 예측은 웹서버 보안모델의 발전방향도 침입차단시스템의 발전방향과 유사할 것이라는 가정 하에 이루어진 것이다.

첫 번째 웹서버 모델은 웹 어플라이언스로, 웹 서비스라는 단일 업무 수행 목적을 위해 제작된 서버이다. 이 서버의 가장 큰 특징은 가전제품처럼 플러그를 꽂아 필요한 사항만 설정해 부면 바로 사용할 수 있다는 데 있다. 이러한 특징은 여러가지 면에서 이점을 가지게 되는데, 우선 웹서버와 OS 사이에서 일어나는 많은 보안 문제들을 제거해주며 또한 웹서버 설치나 관리 상의 어려움을 많이 경감시켜 줄 수 있다.

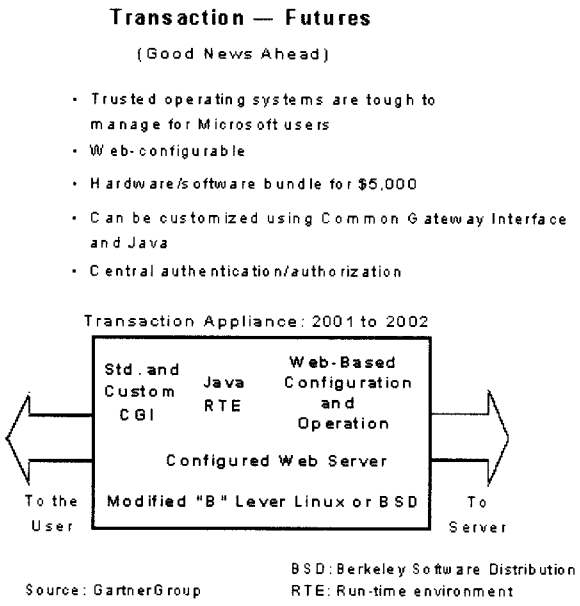

그림 1. 웹 어플라이언스

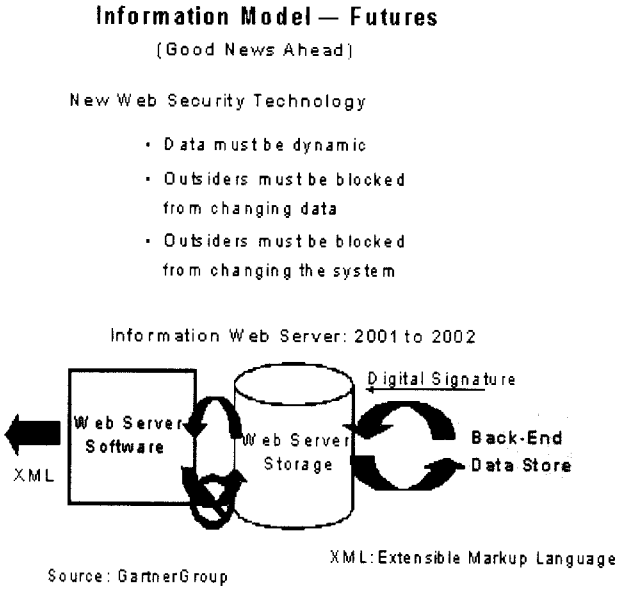

그림 2. 인포메이션 웹서버

웹 어플라이언스가 향후 갖추게 될 특성은 그림[1]로 요약될 수 있다.

제안된 또 하나의 모델은 인포메이션 웹서버로, 웹서버의 정보를 읽거나 읽을 수 있는 기능들만 제공하여 외부의 침입자에 의한 정보의 수정이나 시스템의 변경을 막을 수 있게 하는 웹서버 모델이다. 구체적으로 이것은 기존 웹서버 모델에 "메일박스" 모델을 적용한 것이며 웹서버와 데이터베이스의 연동 시 전자서명을 이용하여 추가적으로 보안 기능을 강화한 것이다. 이러한 특징으로 인하여 웹서버의 사용은 보안에 대한 전문적인 지식이 없는 웹 관리자들도 보안에 대해 신경 쓰지 않고 웹서버를 설치, 구성, 운영할 수 있게 만들 것이다.

이 두 가지 모델 중 첫번째 모델은 로우-엔드 시장을 점유하게 될 것이고, 두번째 모델은 하이-엔드 시장을 점유하게 될 것이라고 가트너그룹은 예측하고 있다.

5. 결 론

웹 관련 서비스는 대부분 불특정 다수를 대상으로 오픈해서 서비스를 제공해야 하므로 침입차단시스템으로 완벽한 접근제어를 하기에는 무리가 따른다. 따라서 외부에 어느 정도 노출될 수 밖에 없기 때문에 이에 대한 자체적인 보안은 필수적이라 할 수 있다. 이를 위해서는 일차적으로 웹서버에 대한 취약점 정보를 수집, 취약점을 계속 해결해 나가야 하며 이와 동시에 웹서버 공급업자에 의해 제공되는 추가적인 보안 기능을 제공 받아 설치하여 웹서버의 보안 기능을 강화해야 한다.

끝으로 이 글에서는 웹서버 보안과 직접 관련된 부문만을 언급하고 있지만 웹에 대한 보안은 웹서버 자체에만 국한되지 않는다. 웹 보안을 위해서는 사용자와 웹서버사이에 two-factor 인증이나 암호화된 채널을 사용해야 하며 웹서버에 이용되는 오퍼레이팅 시스템을 B-level 이상의 시스템으로 이용해야 하는 등의 추가적인 보안이 필요하다.

참고문헌

[1] "Enterprise Management Update: Web Security Outlook From 2000 to 2005", M.Zboray, GartnerGroup, 2000.1
[2] "Secure Commerce Via the Web", M.Zboray, GartnerGroup, 1998.3
[3] "CEO and CIO Alert: Web Security ? Sin in Haste, Repent at Leisure", M.Zboray, GartnerGroup, 1999. 6
[4] "Security Enemy No.1: Active Web Pages", M.Zboray, GartnerGroup, 1999.11
[5] "웹 환경 구축 및 운영을 위한 보안 관리 지침서(안)", 한국전산원, 1997.12
[6] "웹서버 안전 운영 대책", CERTCC-KR, 1998.7
[7] "Internet Information Services Features",
[8] "아파치 보안",
[9] The World Wide Web Security FAQ ,
[10] Summury of Features , PC Magazine,

저 자 소 개

안혜연(安惠妍)

1981년 이화여대 수학과 졸업. 1983년 동 대학원 수학과(전산전공) 졸업(석사). 1994년 메사츄세츠주립대학 전기전산기공학 졸업(공박). 1982년 12월-1987년 6월 한국데이타통신주식회사. 1994년 5월-1999년 12월 삼성 SDS(주). 2000년 1월-현재 (주)시큐어소프트 연구소장. 관심분야 : 보안컨설팅, 무선인터넷서비스, 인증서비스

은창선(殷暢鮮)

1999년 서울대 화학과 졸업. 2000년 5월-현재 (주)시큐어소프트 근무. 관심분야 : 보안컨설팅, 무선인터넷서비스

1. Netcraft Web Server Survey (2000.8)에 따르면 현재 웹서버 시장 점유율은 apache, IIS, Enterprise Server가 각각 60%, 20%, 7% 정도인 것으로 조사되었다.
2. 이 자료는 1007년 PC magazine 자료로서 현재 나온 최신 버전과 차이가 있을 수 있다.
   예를 들어 Apache 웹서버의 경우, 최신 버전은 1.3.12로서 SSL이 지원 가능하다.
3. 아래의 예는 하나의 단순한 예로 이와 관련된 최신 자료는 웹사이트 등을 통해 얻을 수 있다.