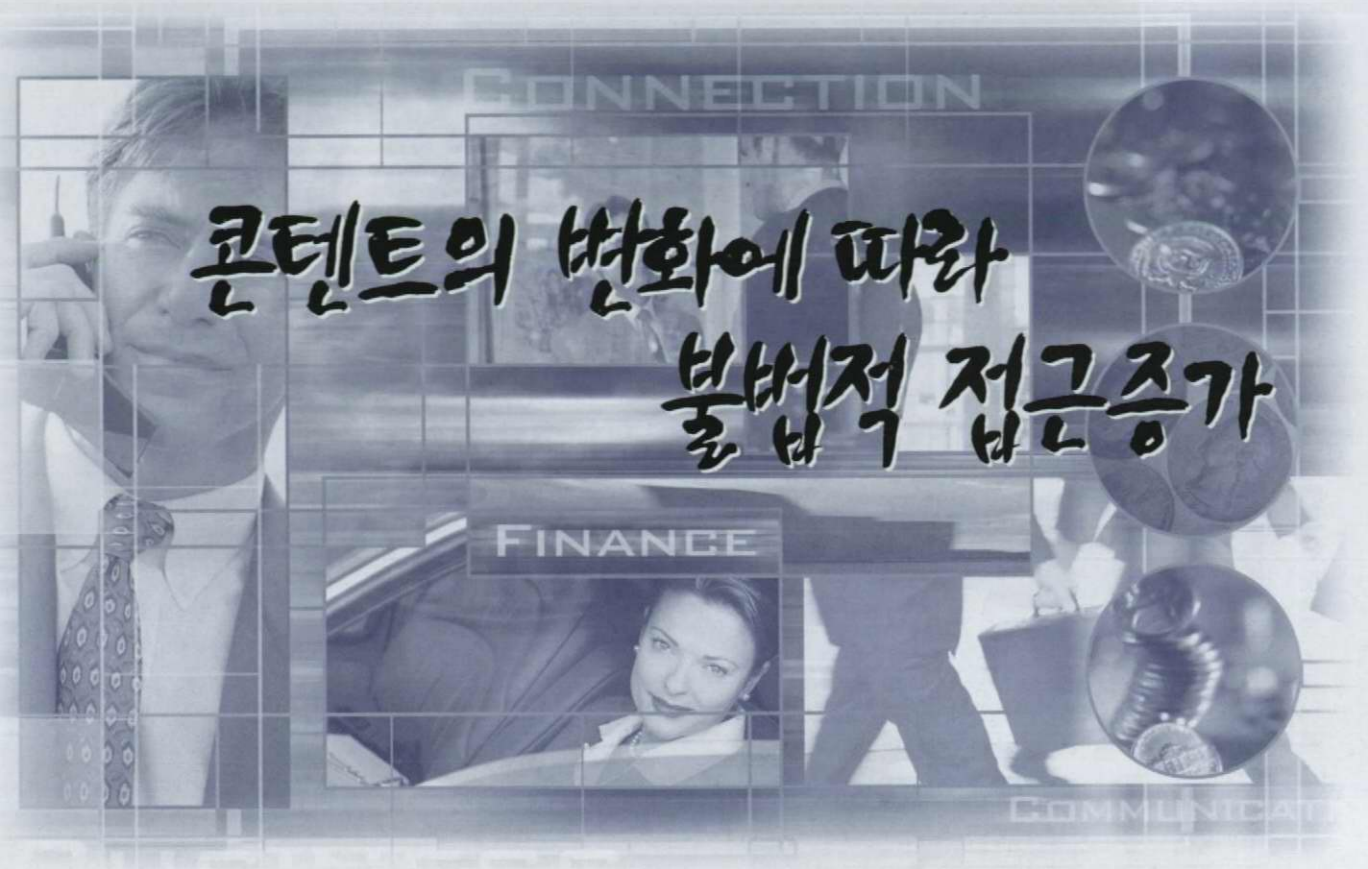


콘텐트의 변화에 따라 불법적 접근증가

인터넷 사용 인구의 증가와 사용 용도의 다양화로 인해서 초기 웹의 정적이고 단순함은 더 이상 사용자의 욕구를 충족시킬 수 없었다. 이러한 욕구는 웹 페이지가 동적이며 더욱 다양한 기능을 갖도록 요구하였으며 자바, Active-X Control 등의 기술을 이용한 Executable Content가 등장하게 되었다. 그러나 이것은 내부 정보 유출 및 파일 삭제 등의 컴퓨터자원에 대한 불법적인 접근의 위험성이 증가하고 있다. 이런 보안상의 취약점에 대해 살펴본다.

■ 이정효/ 한국정보보호센터
(jhlee@kisa.or.kr)

2000년대 디지털 문명을 대표하는 인터넷의 핵심에는 월드 와이드 웹(World-Wide Web, WWW, Web, W3)이 위치하고 있다. 하드웨어를 진정 가치 있게 하는 것은 그에 걸맞는 소프트웨어이듯이 네트워크의 네트워크인 인터넷의 가치를 더욱 높인 것은 월드 와이드 웹이었다.

1989년 스위스 CERN(Conseil Europeen pour la Recherche Nucleaire) 연구 센터의 Tim Berners-Lee에 의해 제안된 월드 와이드 웹은 이미지, 오디오, 비디오 자료 등의 멀티미디어를 포함한 통합형 인터넷 서비스로 현재 전문가 및 관련 연구자 뿐만 아니라 일반인들의 실생활에도 밀접히 다가와 상당한 편리함을 제공해 주는 유용한 도구로서 활

기초상식

간혹 웹(WWW)과 인터넷을 동일시하여 언급하는 경우가 있는데 분명히 웹은 인터넷과 다른 의미이다. 웹은 인터넷을 기반으로 하는 통신 시스템의 한 종류일 뿐인데 현재 인터넷을 기반으로 하는 통신 서비스를 대표하고 인터넷 기반 통신 시스템 중 가장 널리 알려져 있고 많은 사용자를 확보하고 있기 때문에 인터넷과 웹을 동일시하는 혼돈이 생기기 않았나 생각된다.

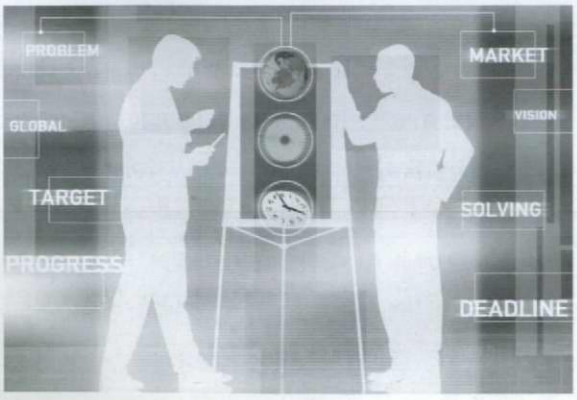
용되고 있다. 기존 명령어 방식의 인터넷 활용 도구에 비해 사용하기 쉽고 이해하기 쉬운 사용자 인터페이스를 갖춘 웹이 많은 사용자를 확보하는 것은 어려운 일이 아니었다.

웹의 인기를 급상승시키는데 중요한 역할을 한 것 중 웹 브라우저를 빼 놓을 수 없다. 1993년 미국 NCSA (National Center for Supercomputing Applications)의 Marc Andreessen과 Eric Bina에 의해 개발된 웹 브라우저 모자익(Mosaic)은 현재 가장 많은 사용자를 둔 넷스케이프 네비게이터(Netscape Navigator)의 효시가 되었다. 웹 브라우저는 웹에 대한 전문지식 없이도 웹을 충분히 활용할 수 있게끔 사용자의 직관(LOOK & FEEL)에 기반한 편리한 사용자 인터페이스를 제공함으로써 많은 인기를 누리게 되었다.

Executable Content 등장 배경

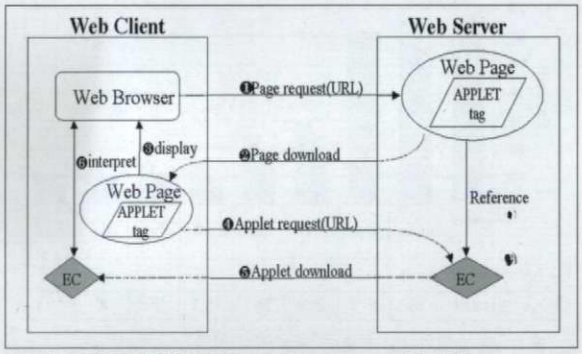
웹은 기본적으로 HTML(HyperText Markup Language) 언어로 작성된 웹 페이지를 서버와 클라이언트간에 HTTP(HyperText Transfer Protocol) 프로토콜을 사용하여 통신한다. 화상과 음성이 지원되는 웹 환경은 기존의 텍스트 방식 사용자로 하여금 많은 매력을 느끼게 하였다.

그러나 인터넷 사용 인구의 증가와 사용 용도의 다양화로 인해서 초기 웹의 정적이고 단순함은 더 이상 사용자의 욕구를 충족시킬 수 없었다. 이러한 욕구는 웹 페이지가 동적이며 더욱 다양한 기능을 갖도록 요구하였으며 자바, ActiveX Control 등의 기술을 이용한 Executable Content가 등장하게 되었다. 실행 가능한 코드를 원격지로 전송 후 실행시킬 수 있다는 개념으로부터 출발한 Executable Content는 정적인 웹에 한 차원 더 높은 기능을 부여하였고 다양한 표현력을 부가하였다. Executable Content의 도입으로 인해 정적인 텍스트와 화상 위주의 웹 페이지는 더욱 세련된 멀티미디어 환경으로 확장될 수 있다.



이러한 Executable Content 기술의 매력은 웹 서버와 클라이언트간의 강력한 상호작용과 더불어 웹 서버 제공자에게도 서버 시스템의 성능 감소 최소화와 네트워크 속도 향상 효과 등의 측면에서 많은 이점을 제공하고 있다. 또한 웹을 이용한 전자상거래 시장이 활성화되고 전자출판 시대가 본격적으로 개막될 경우 자바 또는 ActiveX Control 등의 기술을 이용한 Executable Content의 사용은 급격히 증가할 것으로 전망된다.

Executable Content에 대한 개략적인 이해를 돕기 위해 웹 페이지 상의 applet 전송 절차 및 동작 원리를 간략하게 설명하면 〈그림 1〉과 같이 나타낼 수 있다.



〈그림 1〉 웹 페이지상의 Executable Content 전송 절차

우선 클라이언트(웹 브라우저)측에서 웹 서버측의 해당 페이지를 요청①하게되면 웹 서버측의 해당 페이지가 클라이언트 시스템으로 전송(download)②된다. 전송된 웹 페이지는 웹 브라우저를 통해 그 내용이 표시③되고 전송된 웹 페이지 내의 애플릿 태그(applet tag)를 통해 웹 브라우저는 웹 서버상의 Executable Content를 요청④하게 된다.

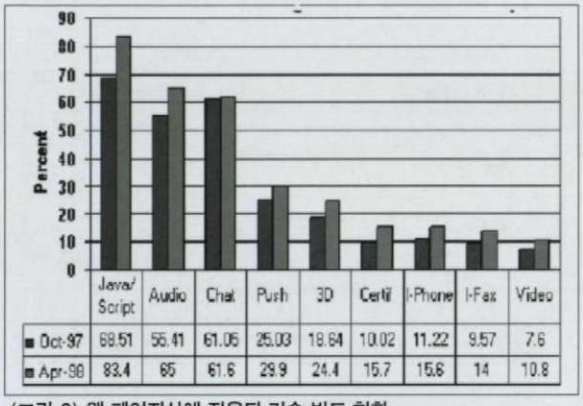
요청된 해당 Executable Content가 클라이언트 시스템으로 전송⑤되고 전송된 Executable Content는 클라이언트측의 해석기(interpreter)에 의해 해석⑥되어 특정한 기능을 수행하게 되는 것이다.

Executable Content 향후 전망

웹에 대한 더욱 다양하고 향상된 기능의 요구로 인해 웹은

동적이며 향상된 상호작용성을 추구하고 있다. 웹을 이용한 다양한 서비스를 지원하기 위해 Executable Content 기술은 급속히 발전하고 있으며 그 사용 빈도 또한 증가 추세에 있다.

GVU(Graphics, Visualization & Usability Center)에서 웹 사용자를 대상으로 조사한 결과에 따르면 웹 사용자 중 80% 이상의 사용자가 자바 및 자바스크립트를 사용해 본 경험이 있는 것으로 나타났다. 〈그림 2〉에서 보다시피 자바 및 자바스크립트를 사용한 경험이 있는 사용자 비율이 97년 68.51%에서 98년 83.4%로 15%의 높은 증가율을 보이고 있다. 이러한 증가세는 향후에도 자바 및 자바스크립트에 대한 수요 및 사용 빈도가 높아질 것이라는 전망을 가능하게 한다.



〈그림 2〉 웹 페이지상에 적용된 기술 빈도 현황

또한 GVU에서는 웹 사용자를 대상으로 향후 필수 불가결할 것으로 고려되는 인터넷 기술을 선정하는 조사를 하기도 하였다. 1997년도 GVU 조사결과 자바 및 자바스크립트 기술은 21.6%, 1998년도 조사결과에서는 29.7%로 높게 선정되었다. 물론 조사 대상 기술 분류에 있어서 범주가 맞지 않는 문제 등으로 조사 대상자로 하여금 몇 가지 혼동의 우려가 없지 않지만 웹 사용자들의 의식 속에 중요한 인터넷 기술로서 인정받고 있음을 증명하는 조사결과가 되었다. 이러한 결과를 토대로 GVU는 향후 가장 많은 사용 빈도를 보일 인터넷 기술로서 자바 및 자바스크립트를 꼽았다.

Executable Content 중 역시 중요한 비중을 차지하는 ActiveX는 원래 윈도우 운영체제만을 위한 기술로 개발되었고 MSIE(Microsoft Internet Explorer)에서만 동작하도록 설계되었으나, 영국의 앤컴패스(Ncompass)사와 같은 협력 개발업체(third party)에서는 유닉스 운영체제에서 동작되는 넷스케이프 네비게이터에서 ActiveX Executables를 실행시킬 수 있는 기술을 개발하기도 했다.

〈표 1〉 주요 인터넷 기술

	GVU9(1998)	GVU8(1997)	변동률(%)
E-mail	93.3	84.3	+9
WWW	90.6	88.7	+1.9
자바/자바스크립트	29.7	21.6	+8.1
Chat	23.9	22.3	+1.6
Audio	20.9	17.1	+3.8
Video	7.9	6	+1.9
Digital Signatures	7.1	5.2	+1.9
Internet Phone	6.5	4.7	+1.8
Internet Fax	6.1	4.3	+1.8
3-D	5.8	4.5	+1.3
Push	5.3	4.5	+0.8

그러나 불행히도 ActiveX는 자바와 달리 보안 모델이 없다. 대신 ActiveX에서는 인증코드(Authenticode) 기술을 이용하여 보안 문제에 대한 해결 방안을 제시하고 있으나 그러한 대응책으로는 인터넷에서 높은 보안성을 요구하는 웹 사이트에서 사용되기 힘들 것으로 전망된다.

Executable Content 보안에 대한 연구

자바 Applet 보안 취약성에 대한 연구 사례

자바 Applet 및 ActiveX Control 등의 Executable Content는 웹 사용자가 웹을 이용하는 동안 사용자 컴퓨터 내에서 실행코드를 수행하는 것을 허용함에 따라 사용자 컴퓨터 시스템의 내부 정보 유출 및 파일 삭제 등의 웹 사용자 컴퓨터 자원에 대한 불법적인 접근의 위험성이 내재되어 있다. 이러한 보안상의 취약점은 향후 전자상거래와 같은 웹을 이용한 응용 서비스의 활성화에 치명적인 걸림돌이 될 것이다.

이러한 Executable Content 기술이 개발되어 점차 그 사용 범위가 확대되어 감에 따라 Executable Content를 이용한 공격 기법에 대한 연구도 활발히 진행되고 있다. 〈표 2〉는 자바 애플릿을 이용한 공격에 대해 연구되어진 내용을 정리한 것이다.

이외에도 자바 및 자바스크립트 등의 Executable Contents를 이용하여 웹 사용자의 시스템에 대한 공격용 코드가 인터넷에 공공연히 발표되고 있는 실정이다. 아직

Executable Contents를 이용한 침해 사례에 대한 발표는 희소하지만 향후 Executable Contents의 사용 빈도가 증가함에 따라 침해 사례 또한 증가될 것으로 보인다.

〈표 2〉 자바 애플릿을 이용한 공격

취약점명	발표 일자	해당 브라우저	수정 버전	내용
Jumping the Firewall	96.1.	NN 2.0	NN 2.1	자바 통신 소프트웨어 취약점
Slash and Bum	96.3.	NN 2.01	NN 2.02	내부 클래스 참조의 취약점
Applet running Wild	96.3.	NN 2.01	NN 2.02	자바 바이트 코드 검사기와 자바 클래스 로딩 기법의 취약점
Casting Caution to the Wind	96.5.	NN 2.02 IE 2.0B2	NN 3.0B3 IE 2.0B2	자바 번역기(Interpreter) 응용 취약점
Tag-Team Applets	96.6.	NN 3.0B3	NN 3.0B4	자바 번역기(Interpreter) 응용 취약점
You are not my Type	96.6.	NN 3.0B5	NN 3.0B6	자바 배열 타입 응용의 취약점
Casting Caution to the Wind	96.7.	NN 3.0B5	NN 3.0B6	자바 번역기(Interpreter) 취약점
Big Attacks come in Small Packages	96.8.	IE 3.0B3	E 3.0B4	내부 클래스 참조의 취약점
Digital Sign	97.4.	Hot자바1.0 (JDK1.1.1)	Hot자바1.0 (JDK1.1.2)	디지털 사인 데이터베이스 취약점

자바 Applet 및 자바스크립트를 이용한 침해 유형 분석

자바 Applet 및 자바스크립트를 이용한 침해 유형을 일반적인 보안성 침해 유형에 준하여 분류할 수 있다. 보안의 목표인 비밀성(Secrecy, Confidentiality), 무결성(Integrity), 가용성(Availability) 침해 유형과 더불어 필자는 웹 특성을 고려하여 "사용상의 불편 및 사용자 불쾌감 유발 행위(Annoyance)"를 침해 공격의 한 유형으로 분류하고자 한다. 이러한 분류는 필자가 현재 진행중인 Executable Web Content 보안 관련 프로젝트 수행 중 코드 구현 수준에서 확인된 것으로 그 외의 공격 기법도 물론 가능함을 언급해 둔다.

비밀성(Secrecy, Confidentiality) 침해 공격

비밀성 침해 공격은 사용자 시스템의 자원을 불법적으로 획득하는 행위가 해당된다. 파일시스템, 프로세스/쓰레드, 메모리 등이 그 주요 공격 대상이 된다. 주로 사용자의 파일 시스템에 있는 사용자의 개인 정보 또는 시스템 정보를 유출하는 경우이다. 비밀성 침해 공격은 자바 Applet 및 자바스크립트를 이용한 침해 유형 중 가장 위험한 경우에 속한다고 할 수 있다. 인터넷의 활성화에 힘입어 온라인 뱅킹, 홈 트레이딩을 통한 주식거래 등이 도입됨에 따라 직접적으로 금전과 직결되는 주요 정보가 개인용 컴퓨터에 저장된 경우가 많다. 이러한 정보가 비밀성 침해 공격에 노출될 경우 아주 치명적인 결과를 낳을 수 있다.

〈표3〉 비밀성 침해 공격 유형

공격 유형	자바 Applet	자바스크립트
특정 디렉토리 존재 여부 확인	○	
특정 파일 존재 여부 확인	○	○
디렉토리 정보 획득		○
파일 데이터 획득		○
시스템 정보 획득	○	

무결성(Integrity) 침해 공격

무결성 침해 공격은 사용자 시스템의 자원을 불법적으로 수정 또는 변경하는 행위가 해당된다. 파일시스템, 프로세스/쓰레드, 메모리 등이 그 주요 공격 대상이 된다. 주로 사용자 파일시스템의 프로그램 또는 정보를 변경하거나 삭제하는 행위와 프로세스/쓰레드의 변경 및 강제 종료 등의 행위를 하는 경우이다.

가용성(Availability) 침해 공격

가용성 침해 공격은 사용자 시스템의 자원을 과도하게 사용하여 사용자의 정상적인 사용을 방해하는 행위가 해당된다. 파일시스템, 프로세스/쓰레드, 메모리, 중앙처리장치(CPU) 등 기타 입출력 장치가 그 주요 공격 대상이 된다. 가용성 침해 공격은 비밀성 침해 공격이나 기밀성 침해 공격에 비하여 쉽게 구현할 수 있기 때문에 그 코드의 개발 및 사용 빈도가 높다.

〈표 4〉 가용성 침해 공격 유형

공격 유형	자바 Applet	자바스크립트
파일시스템의 가용 공간 소멸*	○	
CPU 자원을 과도하게 소모	○	○
메모리 자원을 과도하게 소모	○	○

* 특정 버전(Netscape Communicator 4.05)에서만 적용됨

사용상의 불편 및 사용자 불쾌감 유발(Annoyance)

웹 사용자에게 수많은 윈도우나 프레임을 생성시켜 사용상의 불편을 끼치거나 원하지 않는 음향을 지속적으로 발생시키는 경우 시스템의 자원을 과다하게 소모하지는 않지만 사용자에게 불쾌감을 유발하는 경우가 이에 속한다. 이러한 기술은 자바 애플릿 및 자바스크립트 코드의 긍정적인 기능에

속하나 악의적으로 사용될 경우 사용자에게 부정적인 영향을 미칠 수 있다.

〈표 5〉 사용상의 불편함 및 불쾌감 유발 행위 유형

공격 유형	자바 Applet	자바스크립트
지속적인 윈도우 및 프레임 생성	○	○
지속적인 음향 발생	○	
재귀적 윈도우 생성으로 브라우저 사용 방해	○	○
원치 않는 사이트로의 이동	○	○

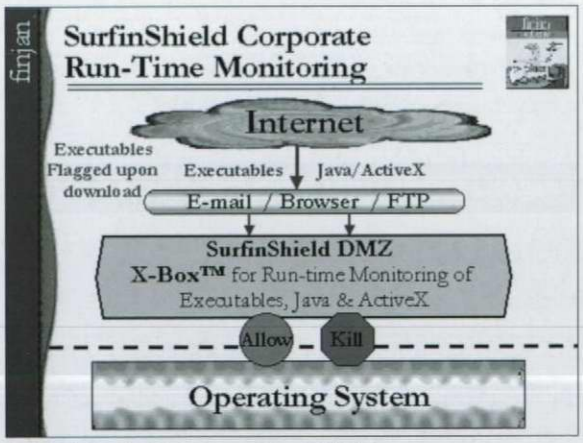
Executable Content 보안 솔루션

자바 applet, 자바스크립트 및 ActiveX Control 등의 Executable Content를 이용한 악성 코드 탐지 관련 기술 및 제품의 핵심은 유해 행위 판정 기술에 있다. 따라서 각 연구기관 및 업체에서는 자체적으로 개발한 판정 기술을 대부분 특허로 출원하고 있고 관련된 기술적 내용에 대한 자세한 언급을 회피하고 있다.

Finjan社 보안 솔루션 및 제품군

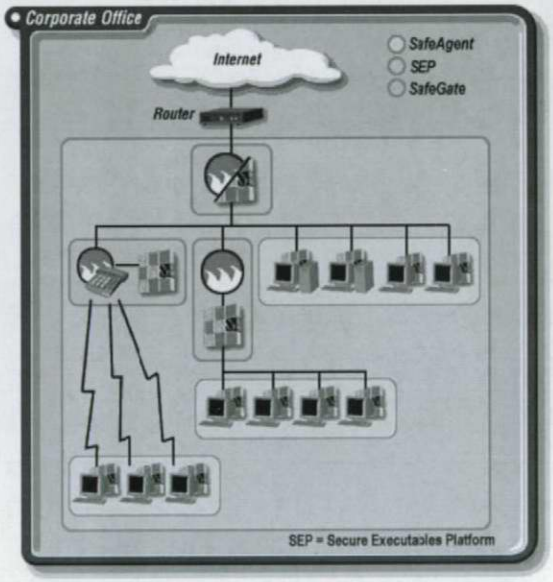
Finjan社는 Executable Content 보안 분야에서 가장 널리 알려진 업체로서 SurfinGate와 SurfinShield 두 종류의 보안 제품을 선보이고 있다. SurfinGate는 네트워크상의 Gateway 레벨에서 자바, ActiveX, 자바스크립트 기술을 이용한 유해 코드를 검색한다.

SurfinGate는 SurfinGate Server, SurfinGate Console 및 SurfinGate DataBase 세 개의 구성 요소로 되어 있다. SurfinGate Server는 HTTP 프록시 서버로 동작할 수 있으며, SurfinGate Console은 네트워크 상에 설치된 많은 SurfinGate Server에게 네트워크를 통해 전송되는 Executable Content를 통제하는 수단으로 사용된다. 그리고 SurfinGate DataBase에는 ASPs(Applet Security Profiles)와 사용자, 그룹 및 보안 정책에 따른 관련 정보 등이 저장된다.



〈그림 3〉 SurfinShield Corporate 동작 개요

시스템 보안 솔루션으로 개발된 SurfinShield 제품은 현재 SurfinShield 2.0 제품이 단종되고 SurfinShield Corporate 4.5 제품이 출시되었으며 SurfinShield Corporate의 동작 개요도는 〈그림 3〉과 같다. SurfinShield는 단일 시스템 내부에서 악성 코드를 X-Box라고 하는 DMZ(Demilitarized Zone)를 만들어 X-Box 내부에서 자바 등의 악성 코드가 동작하는 것을 확인 후 판정한다. X-Box와 관련된 기술은 특허 출원 중으로 Finjan사에서 자세한 언급을 하고 있지 않다.



〈그림 4〉 Security7 제품군의 통합 보안 솔루션

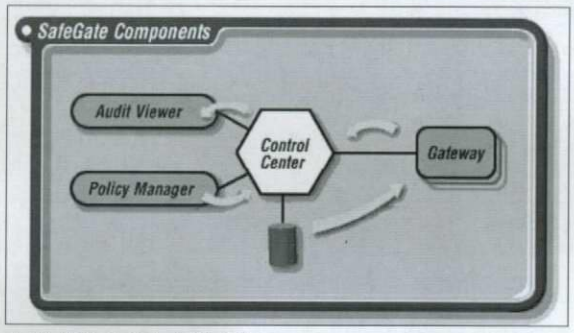
Citrix社 보안 솔루션 및 제품군

Citrix社에서 개발한 Digitivity CAGE는 보호 영역내의 클라이언트에서 요청된 모든 Executable Content가 firewall 외부에 존재하는 웹 서버(CageServer)에서 동작된다. 해당 이동코드의 동작 결과는 별도로 설계된 프로토콜에 따라 Executable Content를 요청한 각 클라이언트 시스템의 GUI를 통해 나타나게 된다.

Security7社 보안 솔루션 및 제품군

Security7社에서 발표한 보안 제품으로는 SafeGate와

SafeAgent 두 제품이 있다. 〈그림 4〉는 Security7社의 SafeGate와 SafeAgent를 이용한 통합 보안 솔루션을 보여준다. SafeGate 제품은 〈그림 5〉에서 보여지는 것처럼 Gateway 레벨의 보안 솔루션으로 시스템의 디바이스 드라이버 형태로 구현되어 있으며 프락시 서버에서 모든 HTTP 트래픽을 감시하고 분석된 HTTP 트래픽을 기반으로 Executable Content의 악성 코드 여부를 판정한다. 미리 설정된 Policy Manager의 보안 정책에 따라 Executable Content의 동작은 제어될 수 있다.

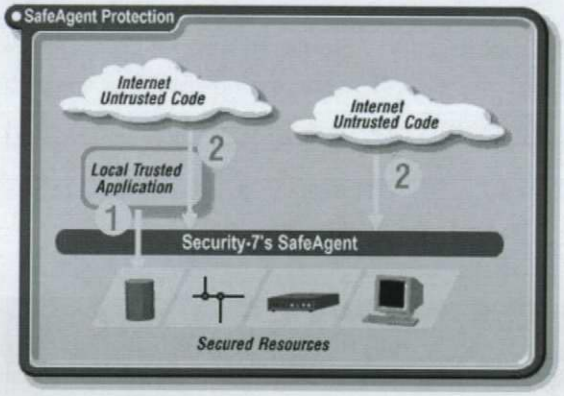


〈그림 5〉 SafeGate 구성 요소

SafeAgent 제품은 단일 시스템에 적용 가능한 독립형(StandAlone) 보안 솔루션으로서 워크스테이션이나 랩탑(Laptop), PC 등에 적용 가능한 제품이다. 〈그림 6〉에서 보다시피 워크스테이션이나 PC 등에 설치된 신뢰성 있는 응용 프로그램(Trusted Application)은 모든 시스템 자원에 대한 접근을 자유롭게 할 수 있지만 그 외 신뢰할 수 없는 응용 프로그램(Untrusted Application)이나 네트워크를 통해 전송된 신뢰할 수 없는 코드(Untrusted Code) 등은 시스템 자원에 대한 제한을 받는다.

중요한 데이터(sensitive data)와 신뢰성 있는 응용 프로그램은 "Secured Resources Zone"에 존재하게 되고 그 외 신뢰성 없는 응용 프로그램을 통해 중요한 자원에 접근할 경우 항상 사용자의 동의를 구하게 된다. 신뢰성 없는 응용 프로그램(Unknown Applications)과 executables는 별도로 격리되어 실행될 수는 있으나 시스템 자원에 대한 접근은 금지된다. 신뢰성 있는 응용 프로그램이라 할지라도 Executable Content에 대해 노출되는 경우 역시 중요 자원에 대한 접근 시에는 사용자의 동의를 구하게 된다.

Security7社의 행위 탐지 기술(프로세스 및 쓰레드의 동작 탐지)은 현재 특허 출원 중에 있어서 기술에 대한 자세한 언급을 회피하고 있으나 SafeAgent에 적용된 기법은 특별히 설정된 "Secured Resources Zone"에 중요 데이터와 신뢰성 있는 응용 프로그램을 설치하고 그 외의 응용 프로그램 및 Executable Content의 "Secured Resources Zone"에 대한 접근을 제한하는 것으로 분석된다.



〈그림 6〉 SafeAgent 구성 요소

eSafe社 보안 솔루션 및 제품군

eSafe社에서는 eSafe Protect GateWay, eSafe Protect Enterprise 및 eSafe Protect Desktop의 세가지 보안 솔루션을 제공하고 있다. eSafe社는 마이크로소프트 보안 솔루션 파트너로 대부분의 제품이 마이크로소프트 윈도우 계열 제품(Windows 3.x, Windows 95/98, Windows NT)을 지원한다.

eSafe Protect GateWay 제품은 네트워크를 통해 전송되는 Executable Content에 대해 침입 차단 시스템(Firewall) 차원의 보안 솔루션으로서 네트워크를 통한 Executable Content를 필터링하고 악성 코드를 검색한다.

eSafe Protect Enterprise 제품은 네트워크 서버 기반 솔루션 제품으로 네트워크 상의 시스템 변경 및 네트워크 자원의 불법적인 접근을 감시한다. 불법적인 감시를 위해 개선된 SandBox 모듈, anti-virus 모듈, personal firewall, 사용자 관리 및 특권 제한 기법 등이 적용되어 있다.

eSafe Protect Desktop 제품은 eSafe社 제품 중 가장 포괄적인 content 보안 제품으로 공격형 content 및 기타 유해한 코드를 탐지한다. Protect Desktop에서는 자체적으로 설계된 Sandbox를 통해 브라우저 내부의 악성 행위를 탐지하고 ACL(Access Control Lists)을 사용하여 자바, 자바스크립트 및 ActiveX 등의 Executable Content를 이용한 악성 행

위로부터 시스템 자원을 보호하고 있으며 역시 자체 설계된 Sandbox 모듈은 특허 출원 중이다.

Princeton Secure Internet Programming Team의 솔루션 및 제품

미국의 Princeton 대학교에서 개발한 자바Filter는 각 site별로 black-list와 white-list를 만들어 ClassLoader가 Applet을 load시키기 전에 험의가 있는 Applet의 동작을 제한한다. 실제로 Applet을 구동시키는 모듈이 Applet ClassLoader인데 자바Filter에서는 Applet ClassLoader를 변경하는 방식으로 구현되어 있다.

ACR(Advanced Computer Research)社 솔루션 및 제품

ACR社의 악성 Executable Content 탐지 관련 제품은 Secure4U로 브라우저 상의 모든 이벤트와 접근 요청이 되는 자원 감시를 통하여 악성 행위를 탐지하는 방식으로 구현되어 있다. Secure4U에서는 레지스트리, 시스템 디바이스, 파일 시스템, 네트워크 자원 및 IP 포트 등의 시스템 자원을 감시하고 브라우저에서 해당 시스템 자원의 요청을 탐지한다.

결론

지금까지 언급된 Executable Content를 이용한 침해 행위가 가능한 것은 웹 페이지에 더욱 다양한 기능성을 부여하기 위한 기술적 발전 과정에서 파생된 문제이다. 따라서 이러한 문제를 방지하기 위해서 새로운 기술, 즉 자바 애플릿 및 자바스크립트 등의 Executable Content를 브라우저에서 지원하지 않는 방법도 있다. 그러나 그러한 해결책은 불의 사용이 인류에 많은 이점을 안겨주지만 화재로 인한 위험 때문에 불의 사용을 금지하는 것과 같은 것이라 할 수 있다.

현재 인터넷 쇼핑몰이나 예약 시스템, 홍보 등의 인터넷 비즈니스는 웹을 중심으로 이루어지고 있다. 그런데 99년 7월 28일자 중앙일보 기사에 따르면 인터넷 전자상거래를 통해 제품 구입을 하지 않는 이유로 '보안사항을 믿을 수 없어'라는 응답이 14%에 달했다. 인터넷 비즈니스의 중요한 분야인 쇼핑몰 사업이나 전자상거래 분야의 활성화를 위해서는 이러한 불안 요소를 불식시키기 위한 효과적인 기술적 연구 및 개발 활동과 법적 대응책이 강구되어야 할 것이다.

News Line

시스코, IBM 네트워킹 기술 인수

시스코시스템즈와 IBM은 최근 IBM의 네트워크 지적소유권을 시스코가 인수하는 것을 포함하는 제휴를 발표했다. 이 제휴 내용에는 시스코와 IBM 글로벌 서비스의 전략적 관계 및 20억 달러 규모의 기술협정 등이 포함돼 있다.

이번 제휴로 시스코는 IBM이 강점을 나타내온 SNA 및 스위칭 관련 기술을 확보하게 됐으며, IBM은 사실상 네트워크 사업을 포기하는 것으로 알려졌다. 이에 따라 한국IBM의 네트워크 사업부도 기존 사용자에 대한 서비스 인력 이외의 인원을 타 부서로 재배치한 후 사업부를 폐지하는 수순을 밟게 된다.

시스코는 이번에 체결된 제휴에 따라 IBM의 라우팅 및 스위칭 기술의 지적 소유권을 인수하고, 양사는 솔루션 제공을 위한 공동 개발을 했으며, 시스코 인터넷 솔루션으로의 이행을 위해 네트워크 솔루션을 테스트하는 연구소 및 프로젝트 오피스를 설립할 예정이다.

시스코는 향후 5년간 IBM의 기술을 구매하는 협정을 체결하게 된다.

반면, IBM은 현 사용자들을 위해 라우팅 및 스위칭 제품에 대해 지속적인 기술지원을 제공하는 동시에 IBM의 판매 및 유통채널을 통해 시스템 네트워크 아키텍처, 토큰링 솔루션, 이더넷 어댑터를 지속적으로 제공하고 지원한다.

또한 시스코 제품을 사용하는 기업들은 IBM의 글로벌 서비스를 통해 네트워크 컨설팅과 디자인, 설치 및 유지보수 등의 지원을 받을 수 있다.

이를 위해 IBM 글로벌 서비스는 시스코 공인 기술력을 갖춘 전문가를 계속 양성할 계획이며, 시스코의 글로벌 지원 파트너 프로그램(골드 파트너 인증 프로그램)과 기술 협력 및 공동 판매 마케팅에 초점을 맞춘 시스코 음성 애플리케이션 파트너 특화 전략에 참여하게 된다.

한편, 시스코는 지난달 중순 대규모 사업자들을 위한 차세대 APPN(Advanced Peer-to-Peer Networking)인 SNA 스위칭 서비스(SNA Sw)를 발표했다.

SNA Sw는 APPN 아키텍처의 복잡함을 크게 단순화 한 것으로 시스코는 고객들에게 IBM의 인터네트워킹 장비와 함께 솔루션을 제공할 수 있게 됐다. SNA 스위칭 서비스는 IP 인프라를 구축하고 있는 대규모 사업자들이 SNA 애플리케이션과 장비에 대한 투자를 확장시킬 수 있도록 시스코에서 91년에 도입한 블루 로드맵 가운데 가장 최근에 발표된 솔루션이다.