情報保護學會論文誌
第19卷 第6號, 2009. 12

보안 인증을 통한 ActiveX Control 보안 관리 모델에 관한 연구

박 성 용,† 문 종 섭‡
고려대학교 정보경영공학전문대학원

The Study on the Security Model for ActiveX Control Management through Security Authentication

Sung-Yong Park,† Jong-Sub Moon‡
Graduate School of Information Management & Security, Korea University

요 약

최근 국내는 전자정부·인터넷 뱅킹·포털 등 대부분의 웹 사이트에서 다양하고 동적인 온라인 서비스 제공을 위해 ActiveX Control을 개발·배포하고 있다. 하지만, 안전성이 검증되지 않은 ActiveX Control은 인터넷 사용자들에게 심각한 보안위협요소가 될 수 있다. 최근 이러한 취약한 ActiveX Control로 인한 해킹 사고가 급격히 증가되고 있음에도 불구하고, 개인 PC 보안의식에만 의존할 뿐 이에 대한 국가적인 보안정책이나 대책이 마련되어 있지 않다.

이에, 본 논문에서는 ActiveX Control 개발·배포·사용의 3가지 측면 모두에서 안전하고 효율적인 보안관리가 가능한 「보안인증을 통한 ActiveX Control 보안관리 모델」설계를 위한 기술적 방법론을 제안하고자 한다.

ABSTRACT

In recent years, to provide visitors with the various and dynamic services, many ActiveX Controls are developed and distributed in most of the web sites such as e-Goverment · Internet banking · Portal in Korea. However, unsecure ActiveX Controls may be critical security threats on Internet User. Although hacking incidents increase sharply for these vulnerable ActiveX Controls, there are not enough national security actions or policies.

Thus, in this paper we propose the technical method to design 'Security model for ActiveX Control Managemnet through Security Authentication' to be able safe and useful security management in three aspects of development · distribution · using.

Keywords: ActiveX Controls, ActiveX Control vulnerability, vulnerability attacks, Security Authentication

I. 서 론

우리나라는 세계적으로 우수한 초고속 정보통신 환경을 기반으로, 전자정부(E-Gov)·포털(Portal)·전자상거래(E-Commerce)·금융(Internet Banking) 등 웹을 통한 다양한 온라인 서비스를 제공하고 있으며, 이러한 온라인 서비스 제공시 기존의 정적인 HTML의 스크립트방식을 탈피하여 이용자들에게 보다 확장된 대화형의 동적인 서비스 제공을 위해 Microsoft社에서 개발한 ActiveX 기술을 사용하고 있다[1].

또한, 국내에서는 웹기반의 온라인 서비스 확대와 더불어, ActiveX 기술이 소프트웨어 산업의 하나의 성공적인 상업적 모델로 재평가되면서 세계적으로도 유례가 없을 만큼 그 사용범위가 날로 확대되고 있다.

하지만, 이러한 ActiveX 기술은 인터넷을 쉽고 편리하게 이용할 수 있게 하는 장점이 있는 반면, 취약

접수일(2009년 10월 13일), 게재확정일(2009년 11월 5일)
† 주저자, stardragon@korea.ac.kr
‡ 교신저자, jsmoon@korea.ac.kr

점이 존재할 경우 해당 프로그램을 설치한 모든 사용자 PC를 일시에 심각한 보안위협에 노출되게 하는 문제점 또한 내포하고 있다. 최근 들어 이러한 ActiveX Control 취약점을 악용한 해킹사고가 급격히 증가하고 있는데, 주로 해커들은 다수의 사용자가 접속하는 웹사이트에 취약점을 악용하는 악성 스크립트가 은닉된 웹문서를 게시하거나, 악성 프로그램을 정상 ActiveX Control 프로그램으로 위장하여 유포하는 수법으로, 서비스 이용자 PC內에 악성코드를 설치한 후, 개인정보·자료를 유출하거나 좀비 PC를 생성하는 등 해킹에 악용하고 있다.

이와같이, 국내 인터넷 환경에서 ActiveX 기술이 많은 보안적 문제점을 내포하면서도 그 사용범위가 급속히 증가되고 있는데 반해, 이에 대한 국가차원의 적절한 보안대책이나 체계적인 관리제도는 마련되어 있지 않다.

이에, 본 논문에서 ActiveX Control의 개발·배포·사용의 3가지 측면에서 보안적 위협요인을 사전에 차단·제거할 수 있고, 체계적인 통합관리가 가능한 '보안인증을 통한 ActiveX Control의 보안관리 모델'을 제안하고자 한다. 본 논문은 다음과 같이 구성되어 있다. 2장에서는 ActiveX Control의 개발·배포·사용상의 취약점 유형과 국내 사용현황과 문제점을 살펴보고, 3장에서는 ActiveX Control 취약점 검증 및 대응과 관련한 최근 연구 동향에 대해서 살펴볼 것이다. 4장에서는 본 논문에서 제안하는 보안인증 방식을 통한 ActiveX Control 보안관리 모델 설계를 위한 기술적 방법론을 제시하고, 5장에서는 기존 연구 모델과의 비교·평가 결과에 대해 설명하고자 한다. 마지막으로 6장에서는 결론을 맺는다.

II. 3가지 측면의 취약점 유형 및 국내사용 현황

2.1 개발자 측면

ActiveX Control 형태의 프로그램은 인터넷을 통해 배포되는 제품의 대중성과 실행파일 형태로 PC內에 설치되는 프로그램 동작 유형 특성상, 일반 응용프로그램 보다 더 강화된 보안성을 제고하여 개발되어야 함에도 불구하고, 국내에서는 대다수 개발업체의 영세성으로 인한 보안인력 부족 및 편의성 위주의 마케팅 수단, 그리고 MS社의 Internet Explorer가 국내 전체 웹브라우저 사용의 98%이상[4]을 차지하는 편중된 PC환경 등으로 인하여, 적절한 보안검증이 이루어지지 않은 수많은 ActiveX Control 제품들이 개발·배포되고 있다. 또한, 다수의 개발업체는 자사 제품에 보안취약점이 존재시에 상업적인 마케팅 전략 및 업체이미지 손상 등을 고려하여 취약점 내용을 외부에 공개하지 않거나, 즉각적인 보완패치버전 개발·배포 등의 적절한 보완대책 마련이나 조치가 미흡한 실정이다.

최근, 해외 해커들에 의하여 국내 ActiveX Control 형태의 동영상재생 프로그램이나 인터넷 뱅킹시 설치되는 공인인증서 관리 프로그램 등의 취약점을 악용한 해킹사고가 발생되고 있으며, 현재도 'milw0rm', 'secunia' 등 해외 취약점 공개사이트 등에서 국내 ActiveX Control 제품들에 대한 취약점 및 악용 공격코드(Exploit Code)가 공개되고 있는 실정이다.

[표 1] 국내 ActiveX Control 취약점 및 악용 해킹 사례

일시	사고 내용
09.7	MS社 윈도우즈 비디오스트리밍(MPEG2TuneRequest) ActiveX 취약점 악용, 국내 다수 PC 감염
09.7	Adobe社 Flash Player ActiveX 취약점 악용, 국내 다수 PC 감염
08.1	국내 oo커뮤니케이션 대표가 웹브라우저 사용시 특정 사이트로 접속을 유도하는 '툴바'와 '루트킷'을 포함한 악성코드를 ActiveX 형태로 포털 등을 통해 무단 배포, 1140만명의 PC감염
08.2	국내 oo소프트社 ActiveX 안티바이러스 제품 취약점 및 공격코드가 해외 취약점공개사이트(milw0rm, secunia)에 공개
07.10	국내 유명 멀티미더어재생기(곰플레이어) ActiveX 취약점 해외 보안사이트에 공개

2.2 배포자 측면

현재 온라인 서비스 제공 웹사이트들은 인터넷 방문자 대상으로 ActiveX Control 프로그램을 배포할 시에, 해당 설치파일을 서비스를 제공하는 동일한 웹서버나 관련 공개시스템에 저장하여 두고, 사용자들로 하여금 웹문서상에 설정된 프로그램 파일이 위치하는 URL경로를 통하여 해당 파일을 다운로드·업데이트하는 방식으로 ActiveX Control 프로그램을 관리하고 있다. 하지만, 만약 배포용 ActiveX Control 설치파일이 저장되어 있는 웹서버가 해킹이 되어 해당

설치파일이 해커에 의하여 악의적으로 변조되거나, 또는 웹문서상에 설정된 프로그램 설치경로가 해킹경유지에 존재하는 악성코드 위치경로로 변조된다면, 사용자들은 이를 인식하지 못한채 자신의 PC內에 악성코드를 설치하게 되는 상황에 직면할 수 있다.

실례로, 09년 7·7 DDoS 공격 관련 경찰청 사고조사 발표[5]에 따르면, 해커는 최초 악성코드 유포경로로 국내 인터넷 파일공유(웹하드)사이트를 이용하였는데, 보안이 취약한 해당 웹사이트를 사전에 해킹한 후, 서비스 이용자들에게 ActiveX Control 형태로 필수적으로 제공하는 파일공유 프로그램의 업데이트 경로를 통하여 악성코드를 유포하여, 수많은 좀비PC를 생성하였다는 조사 결과가 이러한 사실을 증명하고 있다.

2.3 사용자 측면

인터넷 사용자들은 하루에도 수많은 웹사이트에 접속하면서 방문사이트에서 배포하는 ActiveX Control 프로그램을 다운로드·설치하고 있는데, 정작 자신의 PC內에 어떤 프로그램이 설치되어 있고, 해당 프로그램이 어떠한 기능을 가지고 있으며, 또한 언제·어디서 설치하였는지 등의 프로그램 관련 정보를 인지하기가 어렵다. 또한, 사용자들은 자신의 PC에 설치되어있는 다양한 ActiveX Control 프로그램에 대한 취약 정보를 일일이 사전에 습득하기가 어렵기 때문에, 취약점이 존재하는 프로그램임에도 불구하고 이를 인식하지 못한채 설치·사용하게 되는 것이다.

최근 해커들은 이러한 PC內에 설치된 ActiveX 제품에 대한 관리적 어려움 및 인터넷 사용자들의 낮은 보안 의식을 악용하여, 방문자가 많은 웹사이트나 메일 등을 통하여 대량으로 악성코드를 유포하고 있다.

2.4 국내 사용현황 및 문제점

국내 전자정부나 주요 포털·게임 사이트 경우 단일 접속자가 수십만에서 수백만명에 육박하는데, 이러한 다수의 사용자가 이용하는 특정 ActiveX 제품 취약점을 악용한 해킹공격이 발생될 경우, 단시간에 대규모 사이버 침해사고로 발전되어 대량의 좀비 PC생성이나 주요 기관 전산망 마비 등 심각한 국가 사이버 위기상황이 도래할 수 있다.

현재 국내에서는 국가·공공기관에서 사용하는 정보보호제품에 한해서는 국가차원에서 평가·인증을 거쳐 안정성과 신뢰성을 보증하는 보안 관리체계가 마련되어 있으나, 민간·정부기관을 망라하여 다수의 사용자층을 보유하고 있는 ActiveX Control과 같은 일반 응용소프트웨어 경우에는 업체나 개인 사용자들의 보안의식에만 의존할 뿐, 국가차원의 안전성 검증이나 평가·인증 등의 보안 관리 시스템이 마련되어 있지 않다.

[표 2] 국내 PC 평균 ActiveX Control 설치개수(400~700개)

설치 경로	종류
웹(web)	인터넷뱅킹, 포털, 온라인게임 등
응용 프로그램(SW)	MS 오피스(60여개 이상) Adobe Acrobat, Quicktime Player
운영체제(OS)	Windows제품 : 200~300여 개

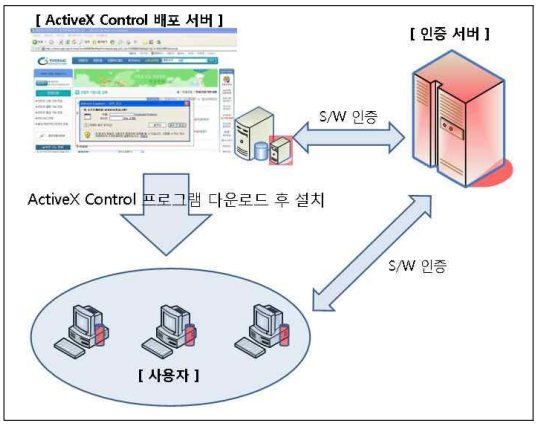
III. 관련 연구

최근 ActiveX Control의 보안위협과 관련된 연구로서 ActiveX 기술 기반의 소프트웨어에 대한 취약점 검사나 점검기법에 관한 연구[2]가 진행되고 있는데, 대부분 프로그램 개발논리나 실행코드(binary)에 대한 취약코드 탐지 방법론으로, 크게 '자동 업데이트 모듈·파일 접근(읽기/쓰기/삭제)·레지스트리 접근·프로세스 접근(실행/종료)' 등 총 4가지 분야로 구분하여 사용권한이 없는 ActiveX Control 제품에 의한 PC內 시스템 자원(파일, 레지스트리, 프로세스)에 대한 비정상정인 행위·접근을 사전에 탐지·차단하는 기술적 방법론에 대한 연구로 진행되고 있다. 그리고, 일부 연구 논문[3]에서는 사용자측 PC보안을 위해서, PC內에 설치된 특정 ActiveX Control의 실행 행위를 모니터링할 수 있는 특정 보안모듈(Security Agent)을 두고, 사용자가 특정 ActiveX Control 프로그램을 설치하기 前 단계에서는 보안스캐닝(Security Scanning)을 통하여 취약 여부를 확인하고, PC內에 설치된 후에는 해당 프로그램 실행 행위를 추적·관리하는 방식의 사용자 PC 보안 모델을 제시한 바가 있다.

하지만, 이러한 연구는 사전에 수많은 제품에 대한 취약점 등 세부 정보를 인지하고 있어야 가능하며, 일반 보안업체에서 국내외의 다양한 ActiveX Control 프로그램에 대한 취약점 등 세부정보를 수집·관리하기는 거의 불가능하다.

IV. 보안인증을 통한 ActiveX Control 보안관리 모델 설계 및 구현

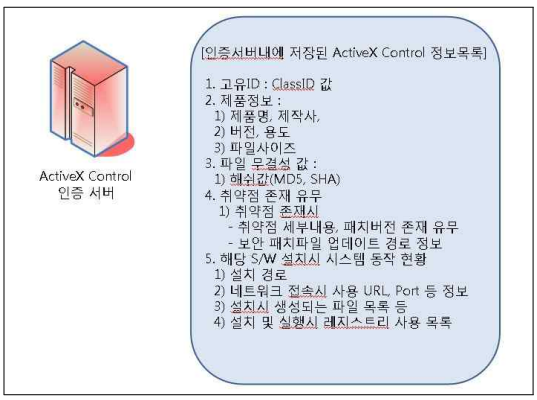
본 장에서는 인터넷 환경에서 ActiveX Control의 개발·배포·사용시 취약요인 사전탐지·제거 등 안전하고 효율적인 보안 관리가 가능한, 보안인증방식을 통한 ActiveX Control의 통합 관리모델 설계를 위한 기술적 방법론을 제안하고자 한다.



[그림 1] ActiveX Control 인증서버를 통한 보안관리 모델

4.1 ActiveX Control 보안인증 시스템

국내 다양한 ActiveX Control 프로그램에 대한 세부 정보 및 취약 정보를 하나의 시스템에 DB化하여 통합 관리하면서, '일반 사용자'나 '온라인서비스 제공기관'에서 자신들이 사용·배포하고 있는 특정 프로그램에 대한 보안정보(취약점 존재여부 등)나 프로그램 정보(프로그램 실행시 정상행위정보 등) 요청시, 해당 정보를 제공해줄 수 있는 별도의 'ActiveX Control 보안인증 서버'를 둘 수 있다.

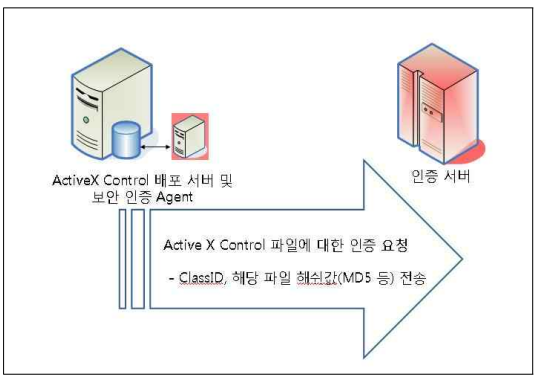


[그림 2] ActiveX Control 인증서버내 저장된 정보목록

'보안인증서버'는 국내외 다양한 ActiveX Control 제품의 프로그램 상세정보*(ClassID, ProgID, 제품명, 제작업체, 버전, 용도, 파일사이즈, 파일무결성값[Hash Value], 취약점 존재여부, 취약점 정보, 보안패치버전 존재여부, 프로그램 실행정보, 레지스트리·파일·네트워크 사용정보 등)*를 종합하여 DB저장·관리하고, 사용자나 서비스 제공기관으로부터 'ActiveX Control ClassID값'을 식별 인자로한 특정 프로그램에 대한 보안 인증요청시, 취약점 존재여부 등 보유하고 있는 프로그램 상세정보를 제공하는 방식으로 보안 서비스를 제공한다.

추가적으로, 보안인증 서버간의 통신패킷은 Unix·Window 등 다양한 이기종 시스템간의 범용적인 서비스 제공을 위하여 상호 보안인증 처리시의 '통신프로토콜'은 반드시 표준화 되어야 할 것이다. 또한, 이러한 인터넷을 통한 보안인증 처리방식은 불특정 다수의 사용자 대상으로 제공하는 공개 서비스 특성상, 악의적인 사용자에 의한 '프로그램 취약정보 수집' 등에 악용될 소지가 있기 때문에, 사용자나 온라인서비스 제공기관에서 인증서버에 보내는 보안인증 요청메시지는 반드시 '서명기법'을 통한 암호화 통신방식으로 전송하고, 보안 인증서버는 이를 검증하는 방식으로 신뢰된 사용자로부터의 인증요청에만 응답하는 인증체계로 구현되어야 할 것이다.

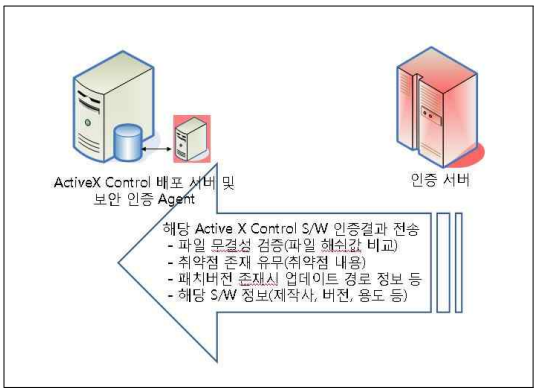
추가적으로, 보안인증서버는 수많은 사용자들로부터의 보안 인증요청시 접속 폭주에 따른 서비스 장애에 대비하여 부하분산(load balancing)서비스 및 캐싱을 통한 다중 서버 방식으로 운영되어야 할 것이다.



[그림 3] ActiveX Control 배포서버·사용자에서 인증서버로의 보안인증 요청정보

4.2 ActiveX Control 배포자와 인증서버간의 통신 설계

ActiveX Control 프로그램 설치파일을 웹사이트 등 공개시스템에서 저장·관리하는 '온라인 서비스 제공기관'은 배포용 설치파일에 대하여, 해커에 의한 악의적 변조 여부 확인 등 파일에 대한 실시간 보안관리가 필요하다. 이에, 온라인 서비스 제공기관은 배포파일이 저장된 시스템과 다른 별도의 시스템에 '보안인증 Agent'를 설치한다. 온라인 서비스 제공기관의 '보안인증 Agent'는 해당 웹사이트에 저장되어 있는 배포용 ActiveX Control 프로그램의 'ClassID'와 설치파일에 대한 '무결성값(Hash Value)'을 추출한 후, 해당 2개의 값을 인자로 ActiveX Control 보안 인증서버에 해당 제품에 대한 '보안인증'처리를 위한 인증 요청 메시지를 전송한다.

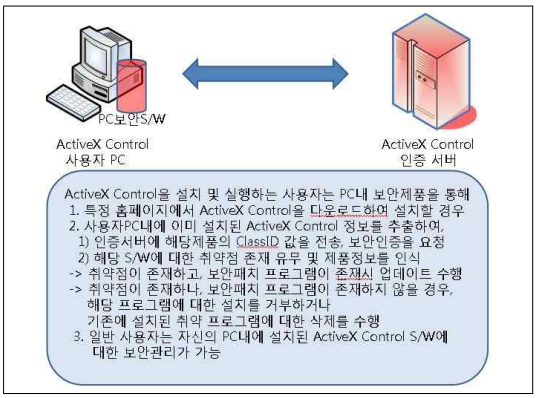


[그림 4] ActiveX Control 인증 서버에서 배포서버·사용자로의 보안인증 요청에 대한 인증 결과값 전송 정보

이에, 인증서버는 보안인증 Agent로부터 요청받은 값*(ClassID, Hash Value)*을 식별자로, 자신의 DB서버內에 저장되어 있는 해당 프로그램의 정상時의 무결성값*(Hash Value)*과 비교하여 변조 및 취약여부 등을 확인한다. 또한, 보안인증 요청결과 취약점이 존재하는 제품으로 판단될 경우, 취약점 세부 내용 및 패치버전 존재 여부와 패치버전이 존재할 경우 업데이트 설치경로 등의 추가적인 보안정보를 제공한다. 이러한 방식을 통하여, 온라 인서비스 제공기관은 이용자들에게 보다 안전하고 신뢰할 수 있는 서비스 제공 및 배포용 ActiveX Control 프로그램에 대한 실시간 보안관리가 가능하게 된다.

4.3 ActiveX Control 사용자와 인증서버간의 통신 설계

ActiveX Control를 배포하는 온라인서비스 제공기관은 인증서버와의 보안인증처리를 위해 별도의 보안인증모듈(Agent)를 사용하나, 일반사용자는 PC내에 설치되어 있는 안티바이러스 등 일반 PC보안제품에 보안인증 기능을 추가하여 인증서버와의 보안인증처리를 수행할 수 있다. 사용자는 특정 웹사이트를 통해 ActiveX Control을 설치할 시점에, PC보안제품내의 보안 인증모듈(Agent)이 해당 웹사이트에서 제공하는 ActiveX Control 프로그램의 고유 ClassID 값와 파일 해쉬값을 추출하여 인증서버에 전송하는 방식으로, 사용자 PC內에 설치전에 해당 프로그램에 대한 무결성 검증과 취약점 존재 유무 등을 확인할 수 있게 된다.



[그림 5] 사용자와 인증서버간의 보안인증 처리 방식

이러한 방식을 통해, 사용자는 취약한 ActiveX Control의 설치·사용에 대한 능동적인 보안대책을 수립할 수가 있고, 旣설치된 프로그램에 대해서도 수시적으로 보안인증 서버간의 통신을 통하여 취약점 존재 여부 및 프로그램에 대한 세부정보(제작업체, 기능·용도, 프로세스 정보 등)를 확인할 수 있게 된다. 또한, 사용자는 보안 인증서버로부터 전송 받은 특정 ActiveX Control 프로그램의 정상적 동작시의 상태정보*(관련 파일명·사이즈, 시스템 설치경로, 네트워크 사용時 URL·Port 등)*를 통하여, 취약점으로 인해 악용된 ActiveX Control 제품의 비정상적인 행위*(특정 네트워크 접속, 비정상적인 파일·레지스트리 접근 등 시스템 자원에 대한 생성·수정·삭제행위)* 발생시 실시간 탐지·차단이 가능하게 된다.

이러한 안티바이러스 등 일반 'PC보안제품'과 '보안인증서버'간의 '보안인증'처리를 수행하기 위해서, 각 PC 보안제품 개발업체는 자사의 보안제품內에 이러한 보안인증 기능을 수행하는 별도의 모듈을 추가로 개발하여야 하는데, 이러한 보안 인증모듈은 보안 인증서버를 관리하는 정부 또는 비영리기관에서 표준화된 인증모듈(SDK)을 개발하여 각 보안제품 개발업체에게 자사의 보안제품內에 포함시켜 적용가능토록 제공하는 것이 바람직할 것이다.

V. 제안방식과 기존연구와의 비교 및 평가

본 논문에서 제안한 보안인증 방식을 통한 ActiveX Control 관리모델은, 보안상 취약한 프로그램은 인증서버를 통하여 취약성이 외부로 공개되므로, 해당 프로그램을 도입하여 온라인서비스를 제공하고자 하는 기관이나 프로그램을 설치·사용하려고 하는 사용자측 모두로부터 외면을 받을 것이고, 또한 프로그램 개발업체는 업체 이미지 손상 등 상업적인 부분에서 손해를 입을 수 밖에 없을 것이다. 이로 인해, 개발측면에서는 최초 설계시부터 보다 보안성을 강화하여 제품을 개발하려고 할 것이고, 취약점 존재시에도 즉각적인 보완패치 제작·배포 등 능동적인 보완대책을 수립하려 것이다. 또한, 이러한 보안관리 모델은 ActiveX Control 형태의 악성코드에 의한 해킹사고나 애드·스파이웨어 등 악성코드 무단유포 등의 인터넷상의 각종 보안위협에 대해서도 근본적인 보안대책을 제공하여 준다. 하지만, 기존연구[3]에서 제안된 사용자 PC 기반의 보안모듈은 공개되지 않은 신규 취약점에 대해서는 사전탐지가 불가능한데, 이는 국내외 수많은 ActiveX Control 제품의 취약점에 대한 정보를 사전에 입수하기가 어렵기 때문이다. 또한, 이러한 PC 측면만을 고려한 보안모듈은 이미 일부 상용 보안제품에서 일부 기능이 구현이 되어 있는데, 대부분 자체 보유한 악성코드 탐지패턴(시그니쳐)이나 탐지기술에 의존하고 있어 최신 웜·바이러스 등의 악성코드 발생시에 완벽한 탐지·제거 등의 적절한 보안대책을 제공하지는 못한다.

하지만, 본 논문에서 제안한 '보안인증 방식을 통한 보안 관리모델'은 보안 인증서버(취약점 DB서버)內에 저장되어있는 특정 ActiveX Control 제품의 사전 정의된 프로그램정보(정상프로그램 실행시 상태정보)와의 비교·분석을 통하여 기존 안티바이러스 등 보안제품에서 탐지하지 못하는 악성코드의 비정상적인 행위에 대한 실시간 탐지·차단이 가능하다. 그리고 보안 인증 처리시의 통신 프로토콜은 표준화를 통하여 개발업체간의 공통된 보안 인증모듈 개발 및 이기종 시스템·보안제품간의 호환을 가능하게 한다. 또한, 특정 ActiveX Control 취약점을 악용한 대규모 사이버 침해사고 발생시에, 보안 인증서버를 통한 실시간 보안 위협경고(alert)를 통하여, '사용금지' 및 '프로그램 삭제' 등의 긴급 보안조치가 가능해진다.

[표 3] 기존 보안 모델과의 효율성 비교/평가

구분	기존 연구 보안모델	제안한 인증방식의 보안모델
취약점 관리	취약점 통합관리 불가능	다양한 제품에 대한 취약점 통합 관리가 가능
취약성 공개	불가능	인증서버를 통해 제품별 취약점 실시간 공개
서비스 범용성	불가능	인터넷을 통해 누구나 서비스 이용이 가능
백신 미탐지 악성코드 처리	불가능	사전정의된 정상행위와 비교 비정상행위 탐지·차단 가능
보안모듈 개발	업체마다 별도의 보안모듈 개발이 필요	표준화를 통해 공통된 보안모듈 개발 가능
기존 보안제품간의 호환성	불가능	표준화로 이기종 보안제품간 호환가능

VI. 결 론

현재 전자정부·인터넷뱅킹 등 국내 수많은 웹사이트에서는 다양한 온라인 서비스 제공을 위하여 ActiveX 기술을 사용하고 있으며, 특히 MS社 의존적인 국내 인터넷 환경에서 그 사용 범위가 나날이 확대되고 있다.

이에 본 논문에서는 신뢰받지 못하는 인터넷 환경에서 보다 안전한 ActiveX Control의 개발·배포·사용을 위한 보안대책을 제공하는 인증기반의 보안관리 모델 설계를 위한 기술적 방법론을 제안하였다. 이러한 보안 인증기반의 보안관리 모델은 비단 ActiveX Control 뿐만 아니라 다양한 웹 플러그인 제품도 포함하여 적용시킬 수 있으며, 더 나아가 응용소프트웨어 분야로 확대 적용하여 무분별한 소프트웨

어 복제에 대한 디지털 저작권 보호 등 소프트웨어 산업 전반의 질적인 발전과 더불어 해킹・악성코드로부터 안전한 사이버 세상을 구축하기 위한 보안대책 마련시 하나의 수단으로 이용될 수 있을 것이라 생각된다. 이에, 향후 이러한 인증기반의 소프트웨어 보안관리 모델을 구축하고 관리하기 위한 국가차원의 정책이나 제도 마련 등에 관한 심도있는 논의와 연구가 필요할 것이라 생각된다.

참 고 문 헌

[1] 국가정보원 국가사이버안전센터, "ActiveX Control 개발 보안가이드라인," 2008년 11월.

[2] 김수용, 손기욱, "ActiveX Control 취약점 검사 및 검증기법 연구," 정보보호학회논문지, 15(6), pp. 3-12, 2005년 12월.

[3] 김재현, "ActiveX 컨트롤의 보안모델 설계," 석사학위, 동국대학교 국제정보대학원, 2006년 2월.

[4] InternetTrend, http://trend.logger.co.kr

[5] MBC TV, "DDoS 공격 근원지는 국내 웹하드 사이트," http://imnews.imbc.com/replay/nwdesk/article/2398580_5780.html

[6] 전상훈, "게임 산업에서의 Vista(ActiveX) 파급효과와 보안의 이슈," 정보보호학회지, 17(2), pp. 57-65, 2007년 4월.

[7] 전병선, Microsoft Visual C++ 6.0 ATL COM Programming, 삼양출판사, pp. 297-298, 2001년 2월.

[8] Microsoft Corporation, "Introduction to ActiveX Controls," http://msdn.microsoft.com/en-us/library/aa751972(VS.85).aspx

[9] Micorsoft Corporation, "What is an ActiveX Control-Microsoft Security," http:// www.microsoft.com/protect/terms/activex.aspx

<著者紹介>

사 진

박 성 용 (Sung-Yong Park) 학생회원
2004년 3월 ~ 현재: 고려대학교 정보경영공학전문대학원 석사 수료
<관심분야> 시스템 보안, 해킹・악성코드, 취약성 분석

문 종 섭 (Jong-Sub Moon) 종신회원
1981년 ~ 1985년: 금성 통신 연구소 연구원
1992년 2월: Illinois Institute of technology 졸업(전산학 박사)
1993년 ~ 현재: 고려대학교 전자 및 정보공학부 교수
<관심분야> 생체인식, 침입탐지, 운영체제