Journal of The Korea Society of Computer and Information
Vol. 17, No. 12, December 2012
www.ksci.re.kr
http://dx.doi.org/10.9708/jksci/2012.17.12.159

공개키 기반 인증체계의 사용이 클라이언트 시스템에 미치는 영향에 관한 연구

전 정 훈*

A study about the influence to the client system when using PKI-based authentication system

Jeong-Hoon Jeon *

요 약

공개키 기반(public key infrastructure)의 인증체계는 서비스 제공자와 사용자 모두에게 인증성과 보안성, 접근성, 경제성, 편의성을 제공으로 국내의 공공 및 민간 기업들은 웹 서비스의 인증방안으로 널리 사용되고 있다. 그러나 공개키 기반의 인증체계의 사용에 따른 여러 보안 취약 요인들이 나타나면서, 클라이언트 시스템의 안전성은 위협을 받고 있다. 따라서 본 논문은 공개키를 기반으로 하는 인증체계에 따른 취약 요인들을 사례연구 및 실험을 통해 분석함으로써, 향후 새로운 인증체계의 구축 및 성능향상을 위한 자료로 활용될 것으로 기대한다.

▸ Keywords : 공개키 기반, 인증서 기반의 인증, 엑티브 엑스 플러그 인, 보안 프로그램

Abstract

The authentication system of the PKI(public key infrastructure) provides the authenticity and security, accessibility, economic feasibility, and convenience to the service provider and users. Therefore the public and private companies in Korea widely use it as the authentication method of the web service. However, the safety client system is threatened by many vulnerable factors which possibly caused when using PKI-based authentication system. Thus, in this article vulnerable factors caused by using the PKI-based authentication system will be analyzed, which is expected to be the useful data afterwards for the construction of the new authentication system as well as performance improvement.

▸ Keywords : PKI-based, Certificate-based Authentication, ActiveX Plug-in, Security Program

• 제1저자 : 전정훈
• 투고일 : 2012. 10. 12, 심사일 : 2012. 12. 4, 게재확정일 : 2012. 12. 16.
* 동덕여자대학교 컴퓨터학과(Dept. of Computer Science, Dongduk Women University)

I. 서 론

최근 인터넷 보급이 확산되고, 웹을 통한 다양한 서비스들이 새롭게 등장함에 따라, 클라이언트들은 서비스 이용을 목적으로 적지 않은 개인 정보를 서비스 제공업체(Service Provider)들에게 제공하고 있다. 그리고 이러한 개인 정보는 서비스 제공업체의 마케팅 활용을 이유로 오남용 되고 있어, 온·오프라인의 구분 없이 사회적 문제로 이슈가 되고 있다. 특히 웹을 통한 정보 유출사고가 전체 보안사고 중, 높은 비중을 차지함에 따라, 보안의 필요성이 절실히 요구되고 있으며, 최근에는 웹 서비스에 대한 공격 증가로 인해 여러 대응 기술들 가운데, 인증기술에 대한 관심이 점차 높아지고 있다. 초기의 인증(authentication)기술은 아이디 및 패스워드를 이용한 단순 방식으로 여러 보안상의 취약점들을 갖고 있었다[1]. 그러나 이러한 기술들의 취약점들은 공개키(public key)암호를 응용한 공개키 기반(public key infrastructure)의 인증체계와 OTP(one time password), SSO(single sign on) 등과 같은 다양한 인증기술들을 등장시키는 계기가 되었다. 특히 공개키를 기반으로 하는 인증체계는 하나의 인증서만으로 관련 사이트의 로그인을 용이하게 하였고, ActiveX를 이용한 보안 프로그램의 배포 및 설치를 통해, 보다 편리하고 강력한 보안 서비스를 제공할 수 있게 하였다. 그러나 공개키 기반의 인증체계는 편의성과 보안성 제공이라는 측면에서 클라이언트들에게 긍정적으로 평가되고 있으나, 최근 공개키 기반 인증체계의 사용에 따른 보안 취약요인들이 나타나면서, 새로운 대체 인증기술의 개발 및 보완이 필요한 실정이다[2].

따라서 본 논문은 공개키 기반 인증체계의 사용으로 인한 보안 취약 요인들을 분석함으로써, 발생 원인과 클라이언트 시스템에 미치는 영향에 대해 알아보고, 이에 대한 대응 방안을 제안한다. 향후 이와 같은 연구가 새로운 웹 인증체계의 구축 및 기존 기술의 성능향상을 위한 자료로 활용될 수 있을 것으로 기대한다. 연구내용에 대한 논리적 근거를 위해, 논문의 Ⅱ장은 공개키 기반의 인증체계와 관련한 기술들에 대해서 알아보고, Ⅲ장의 공개키 기반 인증체계에 따른 취약 요인과 Ⅳ장의 취약 요인들이 클라이언트 시스템에 미치는 영향에 대해 분석하고, 이에 대한 대응 방안을 다루며, 마지막 Ⅴ장의 결론으로 논문을 마치도록 한다.

II. 관련 연구

2.1 공개키 기반의 인증체계

공개키 기반의 인증체계는 비대칭 키(asymmetric keys) 암호를 기반으로 키 생성 및 관리가 용이해 국내 행정 및 금융 기관, 민간 기업 등의 온라인 인증체계로 널리 사용되고 있다. 대표적인 비대칭 키 암호 알고리즘으로는 1977년 Ron Rivest와 Adi Shamir의 연구에 의해 체계화 된 RSA(Rivest and Shamir Algorithm)알고리즘이 있으며[3], 키 생성 및 관리의 용이함으로 국내 많은 웹 사이트에서 사용되고 있다[4]. 공개키 암호의 특징으로는 서로 다른 키를 이용한 암·복호화로 대규모 키 생성 및 관리에 용이한 장점을 갖고 있다. 그러나 암·복호화 속도가 느리고, 키 길이가 길어 암호 기능보다는 인증 키 생성에 주로 사용되며, 키 교환 시, 인터셉트(intercept) 공격에 취약해 보안 채널(secure channel)을 필요로 한다[5][6].

2.2 보안 채널

공개키 기반의 인증체계는 서비스 제공자와 클라이언트 간에 보안성 보장을 위해 보안 채널(secure channel)을 사용하고 있다. 보안 채널은 통신 양자 간에 전송되는 데이터에 기밀성(confidentiality)과 무결성(integrity)을 제공함으로써, 보다 안전한 통신을 가능케 하고, 신뢰성을 보장한다. 국내 공개키 기반의 인증체계는 이와 같은 보안 채널을 구축하는데 SSL (secure socket layer) 프로토콜을 사용하고 있으며, 브라우저를 통해 제공되고 있다. 특히 SSL은 세션상태의 보안성 제공과 브라우저와의 연동이 가능하고, 서비스 제공자들의 보안 채널 구축비용을 절감할 수 있다는 장점으로 인해, 국내 공개키 기반의 인증체계에 널리 사용되고 있다[6].

2.3 보안 프로그램

보안 프로그램은 공개키 기반의 인증체계를 사용하는 클라이언트의 보안성 강화에 사용되고 있으며, 그 종류로는 방화벽(firewall)과 백신(vaccine), Malware 제거, 로그 수집, 키보드 보안, 인증서 관리, SSL 등이 있다. 이러한 보안 프로그램은 공개키 기반의 인증체계를 사용하고자 하는 클라이언트들의 요청이 있을 경우, ActiveX를 통해 쉽게 설치할 수 있어, 국내 관련 사이트들에 널리 사용되고 있다. 그러나 최근 보안 프로그램은 다양성과 상호 호환문제 등으로 인해, 클라이언트 시스템의 안정성을 위협하는 요인이 되고 있다[2].

2.4 ActiveX

ActiveX는 Sun MicroSystems의 자바에 대응하기 위해, 마이크로소프트사에서 개발된 프로그래밍 기술의 하나로 'ActiveX 플러그인' 또는 'ActiveX Control'이라 부른다. ActiveX는 웹 브라우저를 통해 프로그램의 배포가 용이하고, COM(Component Object Model)을 기반으로 어떠한 언어로도 구현할 수 있다. 이러한 점 때문에 ActiveX는 국내 민간 기업이나 행정 기관의 웹 서비스와 관련한 프로그램 및 파일 등의 배포와 멀티미디어 지원 등에 사용되고 있으며, 특히 국내 공개키 기반 인증체계에 필요한 보안 프로그램의 배포에 널리 사용되고 있다[3]. 그러나 이러한 장점들과는 달리, ActiveX를 악용한 공격들이 점차 증가하고 있어, 이에 대한 검토 및 대응방안 마련이 필요한 실정이다[2].

III. 공개키 기반 인증체계의 사용에 따른 취약 요인

공개키 기반 인증 체계는 서비스 제공자와 사용자 모두에게 인증성과 보안성, 접근성, 경제성, 편의성 등을 제공하고, 효과적인 운영을 위해서 사용되고 있다. 그러나 클라이언트 시스템은 공개키 기반 인증체계의 사용에 따른 운영 및 관리와 보안 프로그램의 취약 요인들로 인해 보안성을 위협 받고 있다. 이러한 요인들을 표1로 요약하고, 이에 대해 소절에서 분석하도록 한다.

표 1 취약 요인들
Table 1. Vulnerable to factors

분류		요인
공개키 기반 인증체계의 사용에 따른	운영 및 관리상의 취약 요인	ActiveX의 사용이 클라이언트 시스템을 취약하게 하는 요인이 되고 있음.
		인증서 관리 부주의로 클라이언트 시스템을 취약하게 하는 요인이 되고 있음.
		결재 방식의 호환성 문제가 활성화에 장애 요인이 되고 있음
	보안 프로그램의 취약 요인	보안 프로그램의 사용상의 오류가 클라이언트 시스템을 취약하게 하는 요인이 되고 있음.
		보안 프로그램들 간의 불 호환이 클라이언트 시스템을 취약하게 하는 요인이 되고 있음.
		잘못된 탐지가 클라이언트 시스템을 취약하게 하는 요인이 되고 있음.
		잘못된 기본 설정이 클라이언트 시스템을 취약하게 하는 요인이 되고 있음.

3.1 운영 및 관리에 따른 취약 요인

3.1.1 ActiveX의 사용에 따른 요인

앞서 2.4절에서 언급한 바와 같이, ActiveX는 클라이언트 시스템에 대한 파일의 설치 및 배포가 용이하기 때문에 보안 프로그램의 배포 수단으로 널리 사용되고 있다. 그러나 ActiveX의 여러 보안 취약점들을 악용한 공격이 증가하면서, 최근 경계해야할 기술이 되고 있다[2]. 이에 대해, ActiveX의 기능에 따른 보안 취약점들을 표2를 통해 분석해 본다[7].

표 2. ActiveX의 관리자 권한
Table 2. Administrator privileges of the ActiveX

자원명	행위
파일	생성/삭제/읽기/쓰기
레지스트리	생성/삭제/읽기/쓰기
프린터	출력/스풀링
프로세스	실행/종료

표2의 ActiveX는 관리자 권한으로 파일과 레지스트리의 생성, 삭제, 읽기, 쓰기와 프로세스의 실행 및 종료가 가능하고, 프린터의 출력 및 스풀링에 대한 권한을 갖는다. 또한 ActiveX는 로컬 자원의 접근과 업데이트 기능에 필요한 권한 부여가 가능하여, 사실상 클라이언트 시스템의 모든 권한을 갖게 된다[8]. 이러한 이유로 인해, ActiveX는 공격자들에게 악성 프로그램 및 바이러스의 유포 등에 악용되고 있어, 클라이언트 시스템을 위협하는 요인이 되고 있다. 따라서 최근 ActiveX를 대신할 HTML5의 교체적용이 추진되고 있으나[2], 기존 ActiveX의 사용 분야가 매우 광범위하고, 추가 비용이 불가피하여 신속한 대응이 어려운 실정이다. 이에 대해 국내 ActiveX의 사용현황을 알아보기 위해, 행정 기관 및 민간 기업 별로 각각 100개 사이트를 조사한 자료를 분석해 본다[10].

표 3. 민간 및 행정 기관의 ActiveX 사용 비교
Table 3. ActiveX Usage

구 분		민간 100대 사이트	행정 기관 100대 사이트
ActiveX 사용 사이트 수(%)		86%	82%
총 ActiveX 사용 프로그램		338개	305개
사용 기능	결제 및 인증	41.1%	13.0%
	보안	22.5%	40.0%
	파일 처리	6.8%	3.3%
	웹 확장 문서	0.8%	0.7%
	멀티미디어 및 UI	22.4%	31.0%
	기타	5.0%	11.8%

표3의 조사 자료에 따르면, 국내 민간 기업과 행정 기관이 각각 86%, 82%의 사용률을 나타내고 있으며, 사용 기능으로는 '보안'과 '멀티미디어 및 UI' 기능이 가장 많이 사용되고 있는 것으로 나타났다. 또한 기능에 대한 용도들을 살펴보면, '보안' 기능은 개인 방화벽과 키보드 보안, 데이터 암호, 이메일 보안 등에 사용되고 있으며, '멀티미디어 및 UI' 기능은 동영상 재생과 음악 재생, 그래픽 처리, 그래픽 및 차트 표현, 웹 지도 등에 사용되고 있다[4]. 이러한 조사결과를 통해, 국내 웹 사이트들의 ActiveX에 대한 높은 의존도와 대체 기술의 적용에 많은 시간과 추가 비용의 소요가 불가피함을 알 수 있다. 다음은 국내 웹 사이트들의 ActiveX 사용 유무에 대한 민간 기업별 현황을 그림1을 통해 분석해 본다.

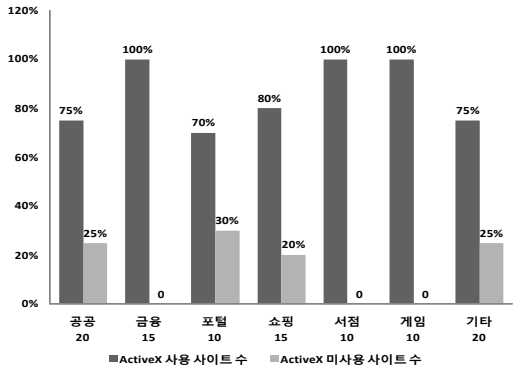

그림1 민간 100대 사이트 ActiveX의 사용현황
Fig. 1. 100 Sites Private Agencies use of ActiveX

그림1은 민간 기업 7개 분야(공공, 금융, 포털, 쇼핑, 서점, 게임, 기타) 100개 사이트에 대해 ActiveX 사용과 미사용을 조사한 것으로 금융 및 서점, 게임 분야에서 100%의 사용률을 나타냈고, 쇼핑과 공공에서는 각각 80%와 75%, 포털과 기타는 각각 70%와 75%를 나타냈다. 이와 같은 자료를 분석해볼 때, ActiveX의 사용률이 표2의 사용 기능에 따라 다양하게 나타나고 있으며, 특히 금융기관은 ActiveX의 취약성에도 불구하고 높은 사용률을 나타냄으로써, 보안 프로그램의 배포와 서점과 게임 포털, 쇼핑은 전자상거래 및 광고를 위해 사용되고 있음을 알 수 있다. 또한 공공 및 포털, 쇼핑 등의 미사용 사이트는 보안 프로그램의 미설치를 의미하는 부분을 내포하고 있어, 보안이 미흡함을 알 수 있게 한다[4]. 다음은 국내 웹 사이트들의 ActiveX 사용 유무에 대한 공공기관별 현황을 그림2를 통해 분석해 본다.

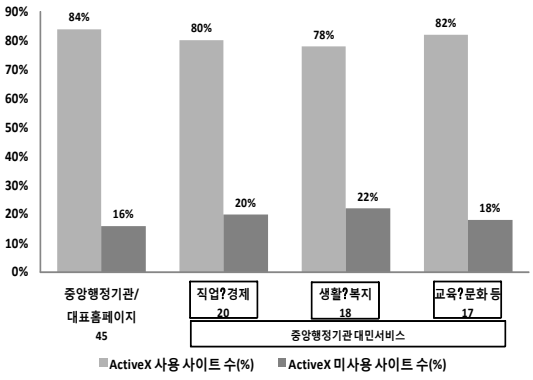

그림2 공공 기관 100대 사이트 ActiveX의 사용현황
Fig. 2. 100 Sites Public Agencies use of ActiveX

그림2는 행정 기관 4개 분야(중앙 행정 기관, 직업 및 경제, 생활 및 복지, 교육 및 문화) 100개 사이트에 대해 ActiveX의 사용과 미사용을 조사한 것으로 이들 분야 중, 중앙 행정 기관의 홈 페이지 보안이 84%로 가장 높은 사용률을 나타냈다[4]. 이와 같은 자료를 분석해 볼 때, 국내 공공 기관의 ActiveX에 대한 의존도가 비교적 높음을 알 수 있으며, ActiveX의 미 사용률은 보안성이 다소 미흡(ActiveX로 설치되는 보안 프로그램의 미설치)함을 반증해 준다. 결과적으로 앞서 3.1.1절에서 언급되었던 ActiveX의 취약성을 고려해 볼 때, 국내 웹 사이트의 보안성 문제가 매우 심각한 수준에 이르고 있으며, 이는 클라이언트 시스템의 위협 요인이 되고 있음을 알 수 있다. 이에 대해 ActiveX의 사용률을 높이는 요인으로 국내 민간 및 행정 기관의 정보 보호에 대한 인식 부족과 이에 따른 대응 기술 개발의 부진, 보안성을 고려하지 않은 무분별한 사용 등을 들 수 있다[10][11].

3.1.2 인증서 관리에 따른 요인

공개키 기반의 인증체계는 인증서를 발급하는 인증기관(Certificate Authority)과 등록기관(Registration Authority)을 필요로 하며, 국내 공인 인증기관으로는 금융결제원과 한국 정보인증, 코스콤, 한국 전자인증, 한국 무역정보통신 등이 있다. 인증기관은 인증서의 발급 및 갱신, 관리 등의 업무를 수행하며, 등록기관은 클라이언트로부터의 요청을 받아 등록 후, 인증기관에 통보한다. 그리고 클라이언트는 인증기관으로부터 인증서를 발급받아, 하드 디스크나 USB에 저장하여 사용한다. 그러나 공인인증서는 클라이언트의 관리 소홀로 인해, 크고 작은 사이버 범죄의 원인이 되고 있으며, 복제 및 분실, 도난 등의 다양한 취약성들을 포함하고 있다. 이에 대한 대응방안으로 공공 및 민간 기업들은 OTP나 보안

카드, 보안 토큰, 개인 비밀번호, 이체 비밀번호 등과 같은 2중, 3중의 개인 식별 인증방법으로 보완하고 있으나, 최근 제3자에 의한 인증서 재발급과 같은 취약점을 악용한 사고 사례들이 발생함에 따라, 공개키 기반 인증체계의 안전성을 위협하고, 클라이언트의 편의성을 저하시키는 요인이 되고 있다.

3.1.3 결제 방식의 호환성에 따른 요인

최근 전자 상거래는 인터넷의 활성화와 더불어 글로벌화가 급속히 진행되고 있는 가운데, 국내 기업들은 보다 쉽게 글로벌 시장으로 진출할 수 있게 되었다. 특히 카드 결제 시스템은 글로벌 결제 수단으로써, 전자 상거래를 가속화하는 촉매 역할을 하고 있으나, 국내 카드 결제 시스템은 해외 시스템과는 달리, 에스크로(Escrow)나 공인 인증서, 휴대폰 인증, 아이핀(I-PIN)등과 같은 인증방식들로 인해, 다양한 문제들이 발생하고 있다[12][13]. 이에 대해 국내·외 결제 방식을 표4를 통해 분석해 본다. 표4의 국내 결제 방식은 클라이언트의 고유 식별 정보를 요구하고 있어, 해외 이용고객들에게는 사용이 불가능하며, 결제 정보를 보호하기 위한 보안 프로그램의 사용이 불가피하다[2]. 그러나 해외 결제 방식의 경우, 간단한 카드정보만으로 결제가 가능하고, 이에 필요한 보안 채널의 구축은 브라우저에서 지원하는 SSL을 사용함으로써, 국내 보안 프로그램의 설치 방식과는 다르게 추가적인 프로그램의 설치 없이 사용이 매우 간단하다[13].

표 4. 국내·외 결제 방식
Table 4. Payment Domestic and Foreign

		요구정보
국내	안심클리닉	카드번호, 유효기간, 주민번호, CVC
	ISP 결제	카드번호, 유효기간, CVC, 비밀번호
	휴대폰결제	인증번호(임의의 문자열)
	IPIN	주민번호, 실명
	공인인증	주민번호, 실명(30만원이상시 사용의무화)
국외	PAYPAL	임의의 문자열(첫 거래 시 한번)
	일반결제	카드번호, 유효기간, CVC

따라서 이와 같은 결제 방식의 차이로 국내 기업들은 해외로부터의 결제를 위해 해외 결제 시스템의 사용이 불가피하며, 이에 따른 비용을 감수해야만 하는 상황이다. 또한 국내 스마트 기기의 사용이 증가하고, 애플리케이션 마켓 활용과 글로벌화가 활성화됨에 따라, 최근 인증 및 결제 관련 사고들이 발생하고 있어, 국내 결제 방식의 범용성과 호환성을 고려한 보완이 필요하다.

3.2 보안 프로그램으로 인한 취약 요인

3.2.1 보안 프로그램의 사용에 따른 요인

보안 프로그램은 서비스 제공자와 클라이언트 모두의 보안성을 보장하기 위한 프로그램으로써, 클라이언트가 해당 서비스에 접근할 경우, 자동으로 동작하고 종료하도록 하고 있다. 그러나 이러한 보안 프로그램들은 오동작 및 불 호환 등의 문제들로 인해, 클라이언트 시스템의 안정성을 위협하는 요인이 되고 있다. 이에 대해 보안 프로그램의 문제점들을 표5와 같이 사례별로 분석해 본다.

표 5. 보안 프로그램의 문제점
Table 5. Problems of Security Program

	사 례
사례1	동작 중이던 보안 프로그램이 종료되지 않는 경우
사례2	이전 보안 프로그램과 중복 동작하는 경우
사례3	보안 프로그램이 종료되지 않아, 수동 종료를 하려고 하여도 종료가 되지 않는 경우
사례4	시스템 트레이에 해당 보안 프로그램이 2개 이상 동작하는 경우
사례5	메모리상에서 보안 프로그램이 삭제되지 않는 경우
사례6	보안 프로그램과 전혀 무관한 사이트의 방문시 이전 보안 프로그램이 동작하는 경우

표5의 사례1과 3, 5의 경우, 프로세스의 종료가 불안정한 상황으로 다른 프로세스의 수행을 방해하거나 시스템을 종료시켜, 시스템의 안정성을 저하시킨다. 그리고 사례2와 4의 경우, 두 개의 프로세스가 동시에 동작하거나, 이전 프로그램의 프로세스만이 동작하는지 알 수 없으며, 실제 보안 기능을 수행해야 하는 보안 프로그램의 정상 동작을 보장할 수 없는 상황이다. 마지막으로 사례6은 이전 프로세스가 정상 종료되지 않은 채, 계속 동작함으로써 진행 중인 프로세스의 정상 동작을 방해하여, 시스템을 사용불능 상태에 놓이게 한다. 이러한 모든 상황들은 보안 프로그램의 정상 동작을 방해하거나, 클라이언트 시스템의 취약성을 증가시키는 요인이 되고 있다.

3.2.2 불 호환 문제에 따른 요인

공개키 기반 인증체계는 클라이언트 시스템의 보안성을 보장하기 위해 다양한 보안 프로그램과 함께 사용되고 있다. 이러한 보안 프로그램의 대부분은 방화벽과 백신, 악성 프로그램의 제거, 인증서 관리, 로그 수집, 키보드 보안 등과 같은 기능들로 구성하고 있다. 또한 보안 프로그램은 ActiveX를 이용해 클라이언트에게 배포되고 있으며, 이와 같은 편리한 점 때문에 국내 보안이 요구되는 행정 및 금융, 민간 등의 웹 서비스의 인증 방식으로 널리 사용되고 있다[4]. 그러나 이와 같은 보안 프로그램은 동일 개발업체에서 개발되었다 할지라도, 웹 사이트가 다르면 상호 호환되지 않고 있어, 보안 프로그램의 재설치 및 업그레이드를 반복해야만 하는 문제를 갖는

다. 이에 대해 표6을 통해, 국내 인터넷 뱅킹에 사용되고 있는 다양한 보안 프로그램을 분석해 본다.

표 6. 은행별 보안 프로그램의 사용 현황
Table 6. Usage of Security Program by Bank

국내은행	기능
K 은행	-공인인증서 보안 wizIN-dE -개인PC방화벽 nProtect-Netizen -키보드 보안 Secure KeyStroke -로그 수집기 nProtect-SecuLog
W 은행	-웹 보안 Softforum XecureWeb Control -개인방화벽 Ahnlab Online Security(AOS -키보드 보안 SoftSecurity TouchEn key keyboard Protector
H 은행	-키보드보안 Softcamp secure keystroke 4.0 -백신 Ahnlab MyV3 -개인 방화벽 Ahnlab My Firewall
N 은행	-웹 보안 Softforum XecureWeb Control -키보드보안 SoftCamp Secure KeyStroke -개인 방화벽 & 백신 Ahnlab Online Security
I 은행	-개인PC방화벽 nProtect-Netizen -웹 보안 Softforum XecureWeb Control

국내 은행들은 표6과 같이 자체 보안 정책에 따라, 다양한 종류의 보안 프로그램들을 사용하고 있으며, 이 중, 몇몇 보안 프로그램은 여러 인터넷 뱅킹 사이트들에서 빈번히 사용되고 있다. 또한 이와 같은 인터넷 뱅킹 서비스의 대부분은 안전한 서비스를 제공하기 위해, 보안 프로그램의 설치를 강제화함으로써, 클라이언트들에게 안전성과 편의성을 제공하고 있다. 그러나 이러한 보안 프로그램의 설치 방식은 다음과 같은 문제점을 갖게 된다. 클라이언트들은 여러 은행들과의 거래를 위해, 은행들마다 제공하는 보안 프로그램들을 설치해야 하는데, 동일 기능, 동일 제품의 보안 프로그램을 중복 설치해야하는 경우가 발생한다. 이는 클라이언트 시스템의 안정성을 위협하는 요인으로 소프트웨어적인 오류뿐만 아니라, 타사 보안 프로그램과의 불호환 등의 문제를 야기함으로써, 보안 프로그램의 설계 및 개발 시, 일관된 지침이나 표준 등의 마련이 필요하다.

3.2.3 오 탐지(wrong detection)에 따른 요인

보안 프로그램은 종류와 버전, 기능, 보안 정책 등에 따라 다양하며, 선택적으로 사용되고 있다. 그러나 이러한 보안 프로그램의 다양성은 보안 프로그램들 간의 오 탐지 문제를 야기 시키는 요인이 되고 있다. 이에 대해 보안 프로그램들 간의 오 탐지 문제를 간단한 실험으로 알아본다. 실험은 클라이언트 시스템에 해외 보안 소프트웨어(방화벽과 백신 기능을 포함한 PC방화벽)를 설치하고, 국내 인터넷 뱅킹의 초기 연결 시, 요구되는 보안 프로그램의 설치과정 중 발생하는 잘못된 탐지 오류를 캡쳐 하였다.

그림3은 해외 보안 프로그램이 국내 인터넷 뱅킹에 필요한 보안 프로그램의 설치과정을 비정상 동작 또는 파일로 간주하여 경고하고 있는 것을 보여주고 있다. 만약 클라이언트가 보안 프로그램의 설치 파일의 일부를 삭제할 경우, 보안 프로그램의 정상 동작을 보장할 수 없으며, 2차적으로는 시스템을 무방비 상태에 놓이게 하는 치명적인 위협 요인이 됨을 알 수 있다.

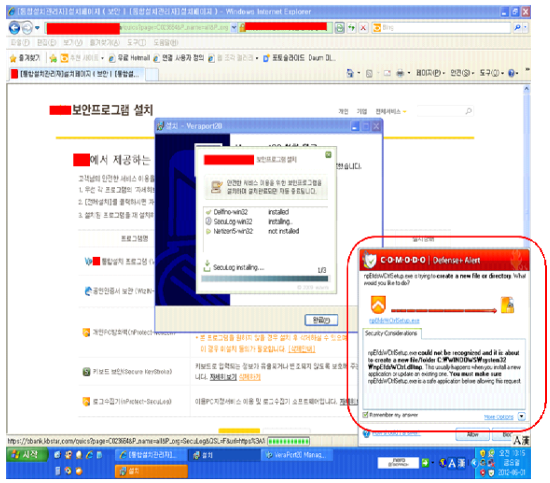

그림3 잘못된 탐색
Fig. 3. Wrong Detection

3.2.4 기본 설정에 따른 요인

보안 프로그램은 클라이언트의 로그인 시도가 발생할 경우, 설치 및 업데이트를 확인하고, 미설치 시, ActiveX를 통한 설치를 강제화 하고 있다. 이와 같은 설치 방법은 전문성이 요구되는 보안 프로그램의 설정과 관리에 있어, 클라이언트들에 의한 잘못된 설정으로 발생할 수 있는 2차 위협을 예방하는 측면에서 유용할 수 있다. 이러한 이유로 인해 대부분의 클라이언트들은 보안 프로그램의 설정에 대한 변경 및 확인보다는 사용에만 치중하는 경향이 매우 높으며, 보안 프로그램과 관련한 사이트들마다 설정을 변경하기 위한 매뉴얼이 제공되고 있지 않고 있어, 보안 프로그램의 기본 설정(default setting)은 클라이언트 시스템의 보안성을 보장하

는데 매우 중요한 요인임을 알 수 있다. 이에 대해 표7에서는 국내 은행별 보안 프로그램의 설정변경 가능 여부와 설정 매뉴얼의 제공 여부에 대해 조사하였다.

표 7. 설정 및 메뉴얼 조사
Table 7. Research of Configuration and Manual

국내 은행	설정 변경 가능 여부	설정 매뉴얼 유무
K은행	가능	없음
W은행	가능	없음
H은행	가능	없음
N은행	가능	없음
I은행	가능	없음

표7과 같이 국내 은행들의 보안 프로그램은 클라이언트가 직접 설정을 변경할 수 있도록 API(application programming interface)를 제공하고 있음에도 설정 매뉴얼은 제공되고 있지 않고 있어, 클라이언트가 직접 설정을 변경하기에는 어려움이 있으며, 설치 초기에 제공되는 기본 설정에 의존할 수밖에 없음을 알 수 있다. 따라서 이러한 상황에서 초기 설정이 잘못 설정 될 경우에는 클라이언트 시스템의 안전을 위협하는 요인으로써 작용할 수 있다. 이와 관련해, 보안 프로그램의 기본 설정으로 인한 문제를 간단한 실험을 통해 알아본다.

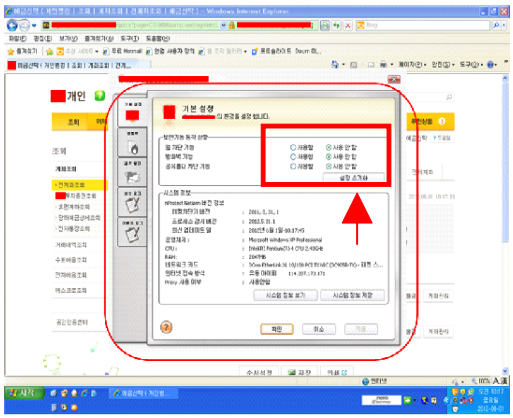

그림4 잘못된 기본설정
Fig. 4. Wrong Default Settings

실험은 클라이언트 시스템에 국내 은행의 인터넷 뱅킹을 초기 연결하였을 때, 인터넷 뱅킹에 필요한 보안 프로그램의 설치 후, 보안 프로그램의 기본 설정화면을 캡쳐 하였다. 그림4에서는 보안 프로그램의 주요 기능에 대한 기본 설정 화면으로 '웜 차단'과 '방화벽', '공유 폴더 차단' 기능들이 기본 설정 값으로 '사용안 함'이 설정되어 있는 것을 확인할 수 있다. 이러한 초기 설정은 클라이언트 시스템을 무방비 상태에 놓이게 하며, 2차적인 보안 문제를 유발시키는 위협 요인이 되고 있음을 알 수 있다.

IV. 취약 요인들이 클라이언트 시스템에 미치는 영향 분석 및 대응

본 절에서는 Ⅲ장의 공개키 기반 인증체계의 사용에 따른 취약 요인들이 클라이언트 시스템에 미치는 영향과 이에 대한 대응 방안을 제도적인 측면과 관리적인 측면으로 나누어 분석하고자 한다. 우선 제도적인 측면을 살펴보면, 공개키 기반 인증체계는 운영과 사용 주체의 범위가 광범위하고, 강제성을 포함하고 있는 만큼, 제도적인 측면에서의 분석이 요구되며, 이러한 취약 요인들로 표1의 '운영 및 관리상의 취약 요인'들을 꼽아 볼 수 있다. 이와 같은 요인들이 클라이언트 시스템을 취약하게 하는 원인에는 다음과 같은 상황들이 전제된다.

1) 대다수의 클라이언트가 공개키 기반 인증체계의 서비스에 대해 신뢰하고 있다는 점이다. 이는 공개키 기반 인증 체계의 운영 및 관리와 서비스 제공의 주체가 신뢰성이 높은 국가 기관 및 금융기관이 되고 있기 때문이다.
2) 공개키 기반 인증체계는 강제성을 포함하고 있다는 점이다. 이는 클라이언트들에게 선택의 여지가 없으며, 서비스의 사용을 위해서는 반드시 공개키 기반 인증체계를 사용해야만 한다.
3) 대다수의 클라이언트는 보안에 관한 전문적인 지식을 갖고 있지 않다는 점이다. 이로 인해, 인증 서비스에 대한 의존성이 매우 높고, 수동적이어서 취약 요인들에 대한 대응이 매우 어렵다.
4) 인증체계의 운영 및 서비스 제공 주체는 보안 체계의 일관성과 호환성이 매우 미흡하다는 점이다. 따라서 체계적인 관리가 운영되고 있지 않고 있다.

이와 같은 전제 상황들로 인해, 클라이언트 시스템은 다음과 영향을 받게 된다.

1) 클라이언트 시스템은 인증체계에 필요한 응용 기술 및 제도적 장치의 취약 요인이나 문제점으로 치명적인 피해를 상속받게 된다.
2) 보안 체계의 일관성 및 호환성 결여로 인해, 클라이언트 시스템은 다양한 보안 프로그램의 설치를 반복해야

하며, 보안 프로그램에 대한 신뢰성을 얻기가 어려울 뿐만 아니라, 시스템의 안정성 또한 보장할 수 없다.

3) 인증체계의 관리가 체계적으로 이뤄지고 있지 못하기 때문에 취약성 발견에 소요되는 시간이 증가함에 따라, 클라이언트 시스템의 취약성도 증가하게 된다.

다음으로 관리적 측면에 대해 살펴보면, 보안 프로그램은 개발업체가 다양하고, 이를 사용하는 서비스 주체 또한 정형화된 기준에 구속되지 않고, 선별하여 보안 기능을 사용할 수 있는 만큼, 관리적인 측면에서의 분석이 요구되며, 이러한 취약 요인들로 표1의 '보안 프로그램의 취약 요인'들을 꼽아 볼 수 있다. 이와 같은 요인들이 클라이언트 시스템을 취약하게 하는 원인으로 다음과 같은 상황들이 전제된다.

1) 대다수의 클라이언트들은 보안에 관한 전문적인 지식을 갖추고 있지 않아, 보안 프로그램의 필요성을 느끼지 못한다.
2) 보안 프로그램의 사용으로 얻게 되는 효율성보다는 서비스의 사용에 목적을 두는 클라이언트가 대다수이다. 따라서 서비스 주체들 또한 보안 프로그램의 설정 변경을 위한 매뉴얼 제공보다는 서비스 사용상에 오류에 대해서만 제공하고 있다.
3) 보안 프로그램은 개발업체와 기능이 다양하여, 서비스의 일관성과 호환성, 안정성을 보장하기 어렵다.
4) 서비스 제공 주체는 보안 프로그램에 관한 관리를 개발업체에게 위탁함으로써 체계적인 관리가 이뤄지고 있지 않고 있다.

이와 같은 전제 상황들로 인해, 클라이언트 시스템은 다음과 영향을 받게 된다.

1) 클라이언트 시스템은 서비스 제공 주체에 따라 보안 프로그램의 반복되는 설치를 해야만 한다.
2) 다양한 보안 프로그램으로 인해 호환성이 저하되고, 시스템의 오류를 유발한다.
3) 보안 프로그램의 위탁개발로 인해 관리의 체계성이 저하된다.
4) 클라이언트는 보안 프로그램 개발업체에 대한 의존성이 높아지고, 수동적인 설치 및 운영만을 하게 된다.

따라서 이와 같은 전제 상황들과 클라이언트 시스템에 미치는 영향들은 제도적인 장치 마련과 관리적인 체계가 필요함을 알 수 있다. 이에 대해 표8에서는 취약 요인들에 대한 대응방안을 알아본다.

표 8 취약 요인에 대한 대응 방안
Table 8. Countermeasures

	방 안
제도적 대응	.ActiveX의 대체 기술 마련 .I-PIN과 같은 인증 기술 사용의 활성화 .해외 결재방식과의 호환 인증체계 구축 .보안 지침 및 표준 마련
관리적 대응	.보안 운영 및 관리체계의 구축 .개발 지침 마련 .철저한 보안 점검과 모니터링 체계의 구축 .제3자 테스트

표8에서 제안하는 대응 방안은 제도적 대응과 관리적 대응 2가지로 나누어 볼 수 있으며, 이에 대해 알아보도록 한다. 첫 번째로 제도적 대응 방안을 살펴보면, ActiveX의 취약성에 대해 대체 기술의 개발과 전환이 제도적으로 이루어져야 한다. 그리고 ActiveX의 활용범위가 광범위한 만큼 제도적 장치를 통해 강제화함으로써, 대체 시간의 단축과 취약 요인의 경감을 효과를 기대할 수 있다. 또한 인증서 관리의 취약점을 보완하기 위해 새로운 대체 방안과 기술이 보완되기까지 I-PIN과 같은 강력한 인증체계의 사용의 의무화나 활성화가 요구되며, 해외 결재 방식에 있어서도 범용성을 포함한 국가적 차원에서의 제도적 보완이 필요하다. 이와 같이 제도적 대응이 필요한 취약 요인들은 민간 차원에서의 대응 방안 마련만으로 보완이나 수정되기 어렵기 때문에 국가적인 차원의 제도적 장치 마련이 필요하다. 두 번째로 관리적 대응을 살펴보면, 앞서 3.2절에서 언급되었던 취약 요인의 대부분이 공공 및 기업들의 운영 및 관리 체계의 미비 또는 미흡에서 기인하고 있어, 이에 따른 방안으로 보안 운영 및 관리 체계의 구축이 마련되어야 한다. 그리고 이에 대해 보안 지침 및 표준안과 같은 제도적 장치와 철저한 점검 및 모니터링을 통해 취약 요인의 경감과 대응을 기대할 수 있다. 결과적으로 공개키 기반 인증체계의 사용에 따른 취약 요인에 대응하기 위해서는 국가 차원의 제도적 장치의 마련과 민간 차원의 관리체계 구축 및 준수가 모두 필요하며, 무엇보다도 보안에 관한 높은 관심이 중요함을 알 수 있다.

V. 결 론

공개키 기반의 인증체계는 국내 행정 및 민간 기업들의 웹사이트에 사용되는 인증체계로 클라이언트와 서비스 제공자 모두에게 편의성을 제공하고, 보안 프로그램을 통해 통신 양자 간에 보안성을 보장한다. 그리고 보안 프로그램은 웹상에

서 ActiveX를 이용해 클라이언트의 시스템에 손쉽게 설치할 수 있어, 시간과 비용을 절감할 수 있다. 이러한 장점들로 인해, 국내 인터넷 뱅킹 및 공공, 민간 사이트에서 공개키 기반 인증체계를 널리 사용하고 있다. 그러나 공개키 기반의 인증체계는 인증서 및 ActiveX의 취약성과 보안 프로그램 및 결제시스템의 불호환성, 클라이언트 시스템의 안정성 위협 등 취약 요인들을 악용한 공격들이 증가하고, ActiveX에 대한 클라이언트의 신뢰성이 저하되고 있는 가운데, 이러한 요인들은 클라이언트 시스템에 치명적인 악영향을 미치고 있음을 확인할 수 있었다.

따라서 본 논문은 공개키 기반 인증체계의 사용에 따른 취약 요인들을 분석함으로써, 클라이언트 시스템의 안정성 및 보안성 보장과 공공 및 민간 기업들의 보안 체계적인 관리를 위해서는 제도적, 관리적 대응이 요구됨을 알 수 있었으며, 무엇보다도 공공 및 민간 기업들의 보안에 대한 자율적인 노력과 자각이 가장 중요함을 알 수 있었다. 마지막으로 이와 같은 연구가 향후 기존 인증체계 및 새로운 인증체계의 보안성 및 성능향상을 위한 자료로 활용될 수 있을 것으로 기대하며, 공개 키 기반 인증체계와 관련한 대체 기술개발 및 응용기술에 대한 연구와 제도적인 보안 체계의 구축 및 다양한 관련 연구가 지속적으로 이뤄져야 할 것이다.

참고문헌

〔1〕 Jeonghoon Han, "Analysis on Vulnerability of ID/PW Management Solution and Proposal of the Evaluation Criteria" Korea Information Processing Society Journal, vol 15, c, pp125-132, 2008.4.

〔2〕 Telecommunications Technology Association of Korea "HTML5 Techniques for ActiveX Replacement" Telecommunications Technology Associations 2011.12.22

〔3〕 Jeon Jeong Hoon 11others "Cryptography & Network Security 5th", pp.283-347, Green 2011.

〔4〕 Broadcasting and Communications Commission Press release 2012.4.2.

〔5〕 Adams & Lloyd "Understanding Public-Key Infrastructure" Macmillan Technical Publishing, 1999.

〔6〕 Richard E. Smith "Authentication" Addison-Wesley, 2002.

〔7〕 Kim Min Jea 4 others, "A Method for Vulnerability Analysis of ActiveX Modules for Internet Services using Fuzzing Techniques", Korea IT Industry Promotion Agency Conference vol.36, no.2(D). pp46-49, 2009.

〔8〕 National Cyber Security Center "'ActiveX controls' at installation hacking vulnerabilities for Web Services" NCSC-TR050017

〔9〕 ITSTAT "Proportion of Internet banking transactions" http://www.itstat.go.kr/stat/graphView.htm?mclass_cd=JB3&detail=4

〔10〕 Su Yong Kim, Ki wook Sohn "The Study of technique to find and prove vulnerabilities in ActiveX Control", National Security Research Institute Vol. 15, No 6, pp.3-12, 2005.12

〔11〕 Jeon Jeong Hoon, "A Study of the Performance Degradation Factors of An Internal Network", Korea Institute of Communications and Information Sciences Vol. 36, No. 1, 2011.1

〔12〕 Kim, Boo Hyun , Yeo, Jungsung , "An Analysis of the Use of Cellular-phone's micro payment" Consumer policy and education review, Vol. 5, No. 2, pp.63-79, 2009.6.

〔13〕 KIPA "Electronic Payment 2.0 Payment 2.0 Market Trends" 2008.8

저 자 소 개

전 정 훈

1999: 숭실대학교 컴퓨터공학과 공학사.
2000: 숭실대학교 일반대학원 컴퓨터공학과 공학석사.
2008: 숭실대학교 일반대학원 컴퓨터공학과 공학박사
현 재: 동덕여자대학교 컴퓨터학과 교수
관심분야: 네트워크 보안, 디지털 포렌식, 인증, 유무선보안,
Email : nerdrandy@dongduk.ac.kr