JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 20, No. 2 : 289~298 Feb. 2016

국내 공인인증서(NPKI)와 국제 표준(SSL/TLS) 기반의 안전 인터넷 거래 비교 분석

박승철*

A Comparative Analysis of NPKI and SSL/TLS for Secure Internet Transactions

Seungchul Park*

School of Computer Science and Engineering, Korea University of Technology and Education, Chungnam 31253, Korea

요 약

지난 10년간 공인인증서 인프라(NPKI-National Public Key Infrastructure) 기반의 우리나라 안전 인터넷 거래 환경은 급속하게 발전하여 왔지만, 한편으로는 폐쇄적인 방식으로 동작하는 NPKI 기반의 인터넷 거래 환경으로 인해 개방성과 호환성 측면에서 여러 가지 문제점들도 노출되어 왔다. 인터넷 거래의 활성화를 위해서는 이러란 문제점들이 가까운 시일 내에 해결될 필요가 있고, 웹 기반 안전 인터넷 거래의 국제 표준인 SSL/TLS 기반으로의 전환이 해결책이 될 수 있을 것으로 받아들여지고 있다. SSL/TLS 기반의 안전 인터넷 거래로의 전환은 현재의 NPKI 기반의 인터넷 거래의 장점을 잘 유지하면서 추진되어야 할 것이다. 본 논문의 주된 목적은 NPKI기반의 인터넷 거래와 SSL/TLS 기반의 인터넷 거래의 장단점을 구체적으로 비교분석하여, SSL/TLS 기반의 NPKI 구현의 기본 아이디어를 파악하는 데 있다. 그런 다음 분석 결과를 바탕으로 현재의 NPKI 기반의 인터넷 거래의 장점을 잘 유지하면서 NPKI 기반 인터넷 거래 환경을 SSL/TLS 기반의 인터넷 거래 환경으로 전환하기 위한 방안을 제시하고자 한다.

ABSTRACT

Though, thanks to NPKI(National Public Key Infrastructure), the Korean secure Internet transaction environment has been rapidly grown in the last decade, it also faces with several problems, which need to be solved in near future, mainly resulted from the lack of openness and compatability of the NPKI-based environment which is operating in a closed way. It is believed that those problems of the NPKI can be solved when it is implemented to be based on the SSL/TLS, an international standard for web-based secure Internet transactions. The transition to the SSL/TLS-based NPKI needs to be performed so that the advantages of current NPKI are well maintained. The purpose of this paper is to comparatively analyze the NPKI and the SSL/TLS so as to give basic idea of implementing the current NPKI to be based on the SSL/TLS. The analysis will show not only how the SSL/TLS-based NPKI can improve current NPKI but also how the advantages of current NPKI can be maintained by the SSL/TLS-based NPKI.

키워드 : 공인인증서, NPKI, SSL/TLS, 안전 인터넷 거래

Key word : Public Certificate, NPKI, SSL/TLS, Secure Internet Transaction

Received 03 November 2015, **Revised** 01 December 2015, **Accepted** 15 December 2015

*** Corresponding Author** Seungchul Park(E-mail:scpark@koreatech.ac.kr, Tel:+82-41-560-1492)
School of Computer Science and Engineering, Korea University of Technology and Education, Chungnam 31253, Korea

Open Access http://dx.doi.org/10.6109/jkiice.2016.20.2.289 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

공인인증서(public certificate)는 특정 공개키(public key)가 인증서에 기술된 신원 정보에 해당하는 사용자의 소유임을 공인기관(certification authority)에서 인증하는 문서이다[1]. 공인인증서 발급 과정에서 공인인증서의 소유자는 인증서의 공개키에 대응하는 자신의 개인키(private key)를 생성하여 특정 장소(예, PC, USB, 또는 하드웨어 토큰)에 비밀로 유지하고, 발급된 공인인증서는 해당 소유자의 공개키가 필요한 사용자(예, 서비스 제공자)에게 제공된다.

1999년 7월부터 시행된 전자서명법에 근거하여 도입되기 시작한 인증서는 2002년부터 국가에서 인정하는 인증기관이 발급하는 공인인증서를 사용하는 국가공개키 인프라(NPKI-National Public Key Infrastructure) 체계로 전환되어 현재에 이르고 있다. NPKI 공인인증서의 공개키를 입수한 사용자는 실제 데이터 암호화에 사용되는 대칭키(symmetric key)를 공개키로 암호화하여 공인인증서 소유자에게 안전하게 전달할 수 있고, 공개키 소유자의 전자서명(digital signature)을 해당 공개키로 검증할 수 있다. 그리고 공인인증서의 신원 정보(identity information)가 정확함을 인증기관에서 보증하므로 공인인증서에 대응되는 개인키를 인증 토큰(authentication token)으로 사용할 수 있다. NPKI 공인인증서는 2014년 말 현재 30,536,707개가 발급되어 인터넷 뱅킹, 전자상거래 지급결제, 정부조달, 전자입찰, 온라인 증권거래, 전자 무역 및 통관 등에서 광범위하게 사용되는 데서 알 수 있듯이, 우리나라 인터넷 거래에서 매우 중요한 인프라를 형성하고 있다[2].

NPKI 기반의 안전 인터넷 거래 환경은 우리나라에서 자체적으로 개발된 SEED 대칭키 암호화 기법과 잘 알려진 RSA 공개키 암호화 기반의 전자서명, 그리고 서비스 제공자들이 자체적으로 정의하는 거래 절차에 근거하여 구현된다[3]. NPKI는 다른 나라에서 유래를 찾을 수 없을 정도로 인터넷 거래의 활성화에 크게 기여해 왔다. 그러나 인터넷 거래 환경의 변화에 따라 NPKI 기반의 안전 인터넷 거래 환경에 대한 개선 요구사항도 지속적으로 증가해 왔다. NPKI에 대한 개선 요구사항은 공인인증서 관리 편의성 추구에 따른 보안 문제(PC 또는 USB에 저장된 공인인증서의 복제 공격 가능성)와 웹 응용 형태로의 구현으로 인한 웹 메모리 컨텐트 조작(MITB, Man-In-The-Browser) 공격 가능성 문제[4, 5] 등도 있지만, 대부분의 개선 요구사항은 국제 표준과 다른 자체적인 NPKI 구현 방식으로 인한 웹 브라우저와의 호환성 결여와 그에 따른 사용자 불편, 그리고 개방성 부족에 따른 보안 신기술 적용 지연 등과 관련되어 있다[2, 6].

대부분의 외국의 경우 국제 표준인 SSL/TLS[7] 기반의 안전 인터넷 거래 환경을 제공하고 있다[8]. SSL/TLS 기반 안전 인터넷 거래의 경우 통신 세션 설정 시에 서버에 의해 사용자(클라이언트)를 인증하는 대신, 사용자 ID/패스워드 또는 OTP 기반의 별도의 사용자 인증 기능을 통신 세션 설정 후 웹 응용 차원에서 구현한다. 현재 사용되고 있는 모든 표준 웹 브라우저들이 SSL/TLS 표준을 지원하므로 SSL/TLS 기반의 인터넷 거래는 호환성 확보에 매우 유리하다. 그리고 국제 표준인 SSL/TLS는 기술 발전에 맞춰 표준 기관에 의해 지속적으로 개선되고 검증되므로 개방성 확보뿐만 아니라 보안성 제고에도 유리한 측면이 있다. 따라서 향후 우리나라 인터넷 거래 환경이 호환성과 개방성을 확보하여 글로벌 인터넷 거래 환경으로 발전하기 위해서는, 중장기적으로 현재의 NPKI 기반의 안전 인터넷 거래 환경을 국제 표준인 SSL/TLS 기반으로 전환할 필요가 있다. NPKI 환경의 SSL/TLS 환경으로의 전환은 현재 NPKI의 장점을 유지하며 SSL/TLS을 통해 NPKI 환경의 문제점을 해결하는 방향으로 이루어지는 것이 바람직할 것이다. 본 논문은 NPKI 기반의 인터넷 거래 절차와 SSL/TLS 기반의 거래 절차를 비교 분석함으로써 NPKI 기반 인터넷 거래 환경의 장점을 파악하고, SSL/TLS 기반으로의 전환을 통해 NPKI 환경의 문제점들을 어떻게 개선할 수 있는 지에 대해 논하고자 한다.

Ⅱ. NPKI 기반 안전 인터넷 거래 절차

2.1. 인증과 키교환

Fig. 1은 NPKI 기반의 가장 전형적인 안전 인터넷 거래인 인터넷 금융 거래 절차의 예를 보이고 있다[3].

NPKI 인터넷 금융 거래는 서버 인증, 사용자 인증과 세션키 교환, 금융정보 조회, 금융 거래 등의 순서로 이

루어지는 것이 일반적이다. 만약 NPKI 기반의 인증 서비스만 필요한 인터넷 거래의 경우 서버 인증과 사용자 인증 절차만 구현되고 나머지는 생략된다. 우리나라에서 인터넷 거래 절차 진행을 위한 메시지 교환 절차는 별도의 표준 프로토콜 없이 서비스 제공자의 서비스 요구에 따라 자체적으로 정의되는 프로토콜을 사용한다. 즉, 인터넷 거래를 위한 별도의 표준 프로토콜을 사용하지 않고 HTTP의 웹 응용 프로그램(클라이언트, 서버)으로 개발된다.

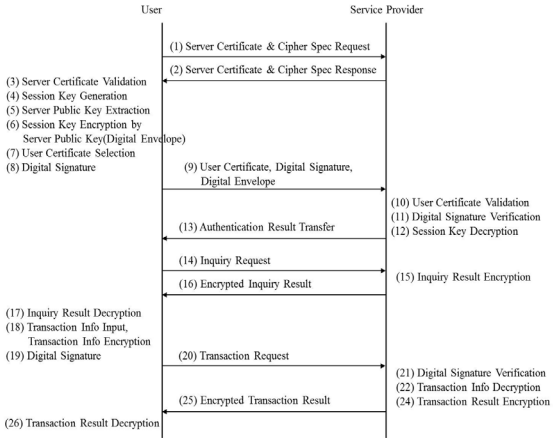

Fig. 1 Typical Example of NPKI-based Secure Internet Transaction

인터넷 거래는 클라이언트 응용 프로그램이 웹 브라우저를 통해 웹 서버 응용 프로그램에게 서버 인증서 및 암호 사양 요청 메시지를 전송함으로써 개시된다. 서버 응용 프로그램은 자신의 공인인증서와 자신이 지원하는 암호 사양(해시 알고리즘, 공개키 암호알고리즘, 대칭키 알고리즘 등)을 클라이언트 응용 프로그램에게 응답한다. 우리나라 인터넷 거래에는 SHA-1 해시 알고리즘, RSA(Ronald Rivest, Adi Shamir, and Len Adleman) 공개키 암호화 알고리즘, 그리고 우리나라에서 자체적으로 개발된 SEED 대칭키 암호화 알고리즘이 사용되고 있다[3]. 서버 인증서 및 암호사양 응답 메시지를 수신한 클라이언트 응용 프로그램은 서버 인증서를 검증함으로써 서버를 인증한다. 서버 인증서 검증은 인증서 유효기간 확인, 인증서에 포함된 인증기관 서명 확인, 폐기 여부 확인 절차를 포함하여 이루어진다. 서버 인증서 확인이 웹 브라우저가 아닌 클라이언트 프로그램에 의해 자체적으로 이루어지므로 서버 인증에 대한 웹 브라우저 알림 표시에 대한 별도의 표준이 존재하지는 않는다.

서버 인증이 완료되면 클라이언트 응용 프로그램은 서버가 제안한 대칭키 암호화 알고리즘(SEED)에서 사용할 일회용 세션키(session key)를 생성한다. 그리고 세션키를 서버 인증서에 기술된 서버 공개키를 사용하여 공개키 암호화 알고리즘(RSA)으로 암호화한다. 서버의 공개키로 암호화한 세션키를 전자봉투(digital envelope)라 한다. 즉, NPKI는 실제 데이터 암호화를 위한 세션키 교환을 전자봉투 방식으로 수행한다. 그리고 클라이언트 응용은 서버 응용 프로그램에 대해 사용자 인증을 수행하기 위해 사용자의 공인인증서를 선택하고, 패스워드로 개인키를 입수하여 교환된 메시지와 연계된 사용자 인증용 전자서명을 생성한다. 마지막으로 사용자의 공인인증서, 전자서명, 그리고 전자봉투가 서버 응용 프로그램에게 전송된다. 즉, NPKI 기반의 인터넷 거래에서는 보안 세션 설정 과정에서 사용자의 전자서명 요청을 통한 사용자 인증이 이루어진다.

서버 응용 프로그램은 유효기간 확인, 인증서에 포함된 인증기관 서명 확인, 폐기 여부 확인 등을 통해 사용자 공인인증서를 검증하고 사용자의 공개키를 확보한다. 이 때 사용자의 공캐키는 전자서명 검증키 역할을 수행한다. 즉, 사용자의 전자서명을 공인인증서의 공개키로 복호화함으로써 전자서명을 검증한다. 전자서명 검증이 완료되면 서버에 의한 사용자 인증이 성공적으로 완료되게 된다. 그런 다음 서버 응용 프로그램은 클라이언트 응용 프로그램과 암호화 통신에 사용할 세션키를 확보한다. 세션키는 서버의 공개키로 암호화된 전자봉투를 서버의 개인키로 복호화함으로써 확보된다. 그리고 서버 응용 프로그램은 사용자 인증 결과를 담은 메시지를 클라이언트 응용 프로그램으로 전달함으로써 인증과 키교환 절차를 완료한다.

2.2. 조회 및 거래

인증과 키교환 절차가 완료되면 클라이언트 응용 프로그램은 조회 요청 메시지를 전송하여 거래 정보를 조회할 수 있다. 조회 요청 메시지를 수신한 서버 응용 프로그램은 조회 결과를 SEED 알고리즘으로 암호화하여 클라이언트 응용 프로그램에게 전송한다. 클라이언트 응용 프로그램은 암호화된 조회 결과를 복호화하여 출

력한다. 인터넷 금융 거래는 송금계좌, 수신계좌, 이체 금액, 계좌비밀 번호 등을 입력하고, 안전한 거래를 위한 추가적인 인증 수단 선택과 선택된 수단에 따른 인증 정보를 입력함으로써 수행된다. 금융 거래는 일반적으로 거래를 요청하는 예비거래와 거래내역을 확인하고 인증하는 본거래로 이루어진다. 클라이언트 응용 프로그램은 거래 요청 정보를 SEED 암호화 알고리즘으로 암호화하여 전달하되, 본거래 내역 인증은 사용자 전자서명으로 수행한다. 본거래 내역 인증은 웹 브라우저상에서 사용자의 거래내역 확인, 공인인증서의 개인키 추출, 그리고 거래내역에 대한 전자서명 생성으로 이루어진다. 본거래 내역에 대한 전자서명은 거래 인증(transaction authentication) 외에 사용자에 대한 부인방지(non-repudiation) 서비스를 추가적으로 제공한다. 우리나라 인터넷 금융 거래에서 공인인증서 기반의 전자서명을 통한 사용자 인증 외에 거래내역 인증을 위한 추가적인 인증 수단은 보안 요구사항에 따라 다르게 사용될 수 있다.

Table. 1 Authentication Methods and Security Classes for NPKI

Authentication Method	Security Level	Transaction Limit
OTP + Certificate	Level 1	100M won/time, 5 times/day
HSM Certificate + Security Card		
Security Card + Certificate + 2ch Authentication		
Security Card + Certificate + Handphone-based Transaction Info Notification	Level 2	50M won/time, 5 times/day
Security Card + Certificate	Level 3	10M won/time, 5 times/day

Table 1은 금융 당국에서 정의한 보안등급별 인증수단과 보안 등급에 따른 금융거래 한도 규정을 보이고 있다. 추가적인 인증은 공인인증서와 개인키 유출 상황에 대응하고, 공인인증서 기반의 인증 후 세션 하이재킹(session hijacking) 공격을 방어함으로써 인터넷 금융 거래의 보안을 강화한다. 전자서명과 함께 SEED로 암호화된 거래 요청 정보를 수신한 서버 응용 프로그램은 인증과정에서 수신한 사용자의 공인인증서의 공개키를 사용하여 서명을 검증한다. 검증 결과 이상이 없으면 키교환 과정에서 클라이언트 응용 프로그램과 공유한 세션키를 사용하여 거래정보를 복호화하여 금융 거래를 수행한다. 그리고 거래결과는 세션키로 SEED 암호화하여 클라이언트 응용 프로그램에게 전달하고, 클라이언트 응용 프로그램이 거래결과를 처리함으로써 인터넷 금융 거래는 완료된다.

Ⅲ. SSL/TLS 동작 절차

3.1. 보안 역량 협상

SSL/TLS는 1995년 Netscape에 의해 클라이언트-서버 프로토콜(예, HTTP)의 보안 서비스 제공을 위해 SSL(Secure Socket Layer)로 개발된 이후, IETF (Internet Engineering Task Force)에 의해 국제 표준 TLS(Transport Layer Security)로 개편되어 2008년 8월 버전 1.2까지 공표되어 사용되고 있다[7]. Fig. 2는 SSL/TLS의 동작절차를 보이고 있다.

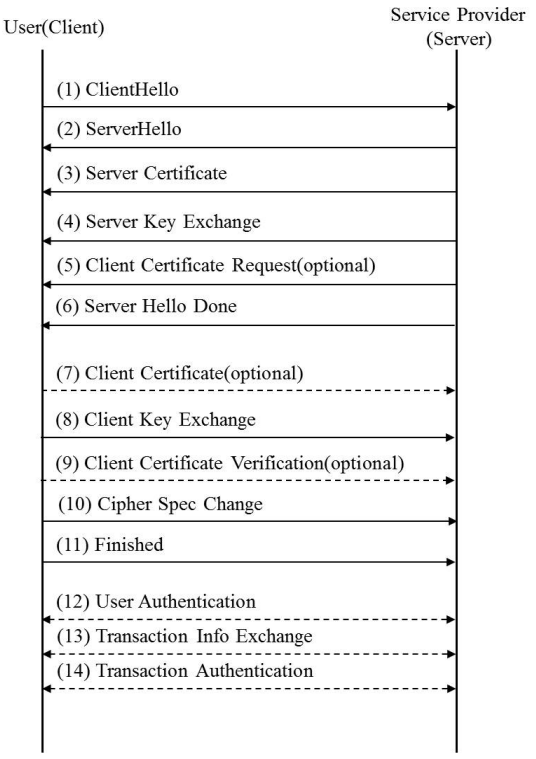

Fig. 2 Operation Procedure of SSL/TLS

첫 번째 단계에서 클라이언트와 서버는 핸드세이크 프로토콜의 헬로 메시지(ClientHello, ServerHello) 교환을 통해 키교환 알고리즘, 전자서명 알고리즘, 메시지 인증 알고리즘, 암호화 알고리즘, 압축 알고리즘 등 보안 역량 협상(security capability negotiation)을 수행한다. SSL/TLS는 NPKI가 지원하는 서버의 공개키를 사용하는 RSA 기반의 키교환 알고리즘뿐만 아니라, 필요할 때마다 임시적인 세션키 교환을 보장하는 DHE (Ephemeral DH), ECDHE(Elliptic Curve DHE) 등의 키 교환 알고리즘을 지원한다. 메시지 인증 알고리즘은 공유 비밀키(shared secret key)와 MD5 또는 SHA-1/SHA-256/384 해시 알고리즘 기반의 메시지 인증 알고리즘을 지원한다. 그리고 암호화 알고리즘은 3DES, AES 등을 지원하고, 2008년에 공표된 TLS 1.2에서는 국내 암호 기술인 SEED도 지원하고 있다. 클라이언트와 서버는 보안 역량 협상 과정에서 통신 세션의 목적에 부합하는 적절한 알고리즘들을 선택한다.

3.2. 서버 인증과 키교환

보안 역량에 대한 협상이 완료되면 서버는 자신의 인증서를 클라이언트에게 전달함으로써 클라이언트로 하여금 서버를 인증하게 하고, 서버의 공개키를 획득하게 한다. 서버 인증을 위한 인증서는 서버 사이트에 대한 신원 확인 방법에 따라 도메인 검증(DV, Domain Validation) 인증서와 확장 검증(EV, Extended Validation) 인증서로 구분되어 사용되고 있다. 서버 인증서를 전송한 후 서버는 협상된 키교환 알고리즘에 따라 세션키를 생성하는 데 필요한 서버 키교환 메시지를 클라이언트에게 전달한다. 클라이언트가 세션키를 생성하여 서버의 공개키로 서버에게 전달하는 RSA 방식의 키교환 알고리즘을 선택한 경우 서버 키교환 메시지 전송은 불필요하다. 키교환 과정에서 서버가 클라이언트를 인증할 필요가 있는 경우 서버는 클라이언트 인증서 요청 메시지를 보낼 수도 있다. 그러나 현재 대부분의 SSL/TLS 기반의 인터넷 거래에서 인증서 기반의 클라이언트 인증을 지원하고 있지 않으므로 이 과정은 생략된다. 서버 인증 및 키교환 단계는 ServerHelloDone 메시지 전달로 완료된다.

3.3. 클라이언트 인증과 키교환

서버가 인증서를 요청한 경우 클라이언트는 자신의 인증서를 서버에게 전달한다. 즉, SSL/TLS도 NPKI와 같이 인증서 기반의 클라이언트(사용자) 인증 기능을 선택적으로 제공하고 있다. 그러나 대부분의 SSL/TLS 기반의 인터넷 거래에서 인증서 기반의 클라이언트 인증을 지원하고 있지 않으므로 이 과정은 생략된다. 클라이언트 키교환 메시지의 내용은 선택된 키교환 알고리즘에 따라 달라진다. RSA 키교환 알고리즘의 경우 키를 생성하는 데 필요한 완전한 예비 마스터 비밀(pre-mater secret) 정보를 포함한다. DHE와 ECDHE 키교환 알고리즘의 경우 세션키 생성에 필요한 매개변수들이 전달된다. 클라이언트는 서버의 주소로 서버를 접속하므로 인증서에 포함된 인증 대상 정보(이름, IP 주소, URL 주소 등) 확인을 통해 서버를 인지할 수 있지만, 클라이언트에 접속하는 과정이 없는 서버는 클라이언트 인증서를 수신하더라도 클라이언트를 인지할 추가적인 방법이 필요하다. 이를 위해 클라이언트는 이전에 보낸 모든 핸드세이크 메시지들에 대해 해시 함수를 적용한 결과를 자신의 개인키로 서명한 클라이언트 인증서 입증 메시지를 전송함으로써, 자신이 전송한 인증서의 공개키에 대응되는 개인키를 소유하고 있음을 서버에게 증명한다. 즉, SSL/TLS가 인증서 기반의 클라이언트 인증을 지원하는 경우, 클라이언트 전자서명 확인을 통해 클라이언트를 최종적으로 인증하게 되는 것이다. 보안 역량 협상과 인증, 그리고 키교환 결과에 따라 확정된 보안 사양은 암호사양 변경 메시지를 통해 적용이 개시되고, 클라이언트가 Finished 메시지를 전송함으로써 보안 세션의 설정이 완료된다.

3.4. 안전 인터넷 거래

SSL/TLS 세션 설정이 완료되면 클라이언트와 서버 간에 교환되는 모든 거래 정보에 대한 기밀성(confidentiality), 무결성(integrity), 그리고 메시지 인증성(message authenticity)이 보장된다. 그러나 일반적으로 세션 설정 과정에서 클라이언트 인증이 이루어지지 않으므로, 인터넷 거래를 수행하기 전에 서버는 사용자에 대한 인증 작업을 별도로 수행하여야 한다. 사용자 인증은 ID/패스워드 기반으로 이루어지는 것이 일반적이다. 그러나 인터넷 거래에 대한 인증 요구 수준에 따라 OTP(One-Time Password), 챌린지/응답(challenge / response) 등에 기반의 거래 인증이 추가되는 것이 일반적이다[8].

Ⅳ. 비교 분석

4.1. 표준과 프로토콜 구조

Table 2는 NPKI와 SSL/TLS에 대한 비교 결과를 요약하여 보이고 있다.

Table. 2 Comparison of NPKI and SSL/TLS

Items	NPKI	SSL/TLS
Standard	Proprietary	International Standard
Protocol Architecture	Transaction over NPKI over HTTP	Transaction over HTTP over SSL/TLS
Sever Authentication	Public Certificate-based	EV-Certificate-based
Client Authentication	Public Certificate + Digital Signature	- (optional)
Encryption Algorithm	SEED	3DES, AES, SEED, etc.
Key Exchange Algorithm	RSA	RSA, DHE, ECHDE, etc.
Non-repudiation	Digital Signature	-

SSL/TLS가 국제표준화기구에 의해 개발되고 유지 및 관리되는 국제표준으로 정의된 반면, NPKI 기반의 인터넷 거래 절차는 별도의 표준으로 정의된 대신 감독기관이 제공하는 지침(예, [3])에 근거하여, 서비스 제공자들이 거래 절차를 정의하여 구현하는 비표준 방식으로 사용되고 있다. 개방형 표준화기구인 IETF는 정해진 절차에 따라 SSL/TLS를 위해 새로운 보안 기술들을 지속적으로 수용하고 검증하고 있다. 그러나 NPKI는 공개된 표준화 기구가 없고 새로운 기술 도입이 감독 기관과 인터넷 거래 서비스 제공자의 판단에 의존하는 폐쇄적인 구조로 운용된다. 단일 감독 기관 또는 인터넷 거래 서비스 제공자는 새로운 기술의 평가와 적용 능력을 갖추기가 쉽지 않기 때문에, 기존 인터넷 거래 환경 유지에 치중할 수밖에 없고 문제가 생기면 보완하는 수동적인 방식을 취할 수밖에 없는 것이 일반적이다. 따라서 NPKI가 SSL/TLS에 비해 새로운 기술에 대한 개방성이 취약할 수밖에 없다. 폐쇄적인 구조는 개방성 취약뿐만 아니라 보안성 측면에서도 심각한 문제를 야기할 가능성이 높다[6]. 즉, 개방된 환경에서 많은 전문가들에 의한 인터넷 거래 절차에 대한 보안성 검증 기회가 없이 자체적으로 보안성을 검증하기 때문에, 보안성 검증의 강도가 상대적으로 약할 수밖에 없는 것이다. SSL/TLS 기반의 인터넷 거래는 'SSL/TLS상의 HTTP상의 인터넷 거래(Transaction over HTTP over SSL/TLS)'의 프로토콜 구조로 구현된다. 현재 모든 표준 웹은 SSL/TLS를 지원하므로 SSL/TLS 인터넷 거래는 표준 웹만 사용하는 응용 형태로 구현될 수 있다. 반면 NPKI 기반의 인터넷 거래는 'HTTP상의 NPKI상의 인터넷 거래(Transaction over NPKI over HTTP)'의 프로토콜 구조로 구현되고, 표준 웹이 지원하지 않는 NPKI의 기능들은 웹 확장 플러그인 프로그램 형태로 구현된다. NPKI의 경우 대부분의 서비스 제공자들이 마이크로소프트사가 인터넷 익스플로러를 위해 개발한 ActiveX 프로그램으로 플러그인을 제공해오고 있고, 이것이 다른 웹 브라우저들과의 호환성 결여 문제의 원인이 되고 있다.

웹 응용 기반의 인터넷 거래는 웹 메모리상의 거래 정보를 조작하는 MITB(Man In The Browser) 공격에 노출될 수 있다[4, 5]. NPKI 기반의 인터넷 거래의 경우 거래 정보를 HTTP상의 NPKI에서 암호화하기 때문에 HTTP하의 SSL/TLS에서 암호화하는 경우에 비해 좀 더 빨리 암호화할 수 있고, 따라서 웹 메모리 노출 범위가 축소되어 NPKI가 상대적으로 MITB 공격에 대한 방어에 유리하다. [5]는 실제로 MITB 공격 방어를 위해 확장E2E 암호화를 적용하여, 입력장치로부터 입력된 거래 정보를 최대한 빨리 암호화함으로써, NPKI에 대한 MITB 공격을 방어하도록 권고하고 있다. 거래 정보 암호화가 HTTP하의 SSL/TLS에서 이루어지는 SSL/TLS 기반 인터넷 거래의 경우 웹 브라우저 대신 별도의 안전장치를 통한 거래인증 도입 등 MITB 공격 방어에 보다 세심한 주의가 필요하다.

4.2. 서버 및 클라이언트 인증

NPKI와 SSL/TLS 모두 인증서를 통해 서버를 인증하는 것은 동일하다. 그러나 SSL/TLS이 표준 웹의 일부이므로 SSL/TLS 서버 인증은 표준 웹 브라우저를 통해 이루어지지만, NPKI 서버 인증은 NPKI를 구현한 웹 응용 프로그램에 의해 이루어지는 차이가 있다. SSL/TLS 기반의 웹 브라우저에 의한 서버 인증은 인증 결과를 표준 사용자 인터페이스를 통해 표시할 수 있는 장점이 있다. 특히, 글로벌 인증기관과 웹 브라우저 업체들이 연합된 CAB 포럼(CA/Browser Forum)에서 제시

한 확장 검증(EV) 방식[9]으로 발급된 인증서에 의해 서버를 인증한 웹 브라우저는, 동일한 사용자 인터페이스를 통해 인증 결과를 보다 분명하게 표시한다. 이로써 사용자가 서버의 진위를 보다 쉽게 파악할 수 있게 하여 피싱 사이트 접속에 의한 피해 예방을 보다 용이하게 한다. NPKI 공인인증서에 의한 서버 인증은 서비스 제공자의 NKPI 응용 프로그램을 통해 자체적으로 이루어지고, 웹 브라우저가 인증 결과를 표시하는 표준 인터페이스는 결여되어 있다. 따라서 SSL/TLS에 비해 사용자에 의한 피싱 사이트 인식에 어려움을 초래할 수 있다.

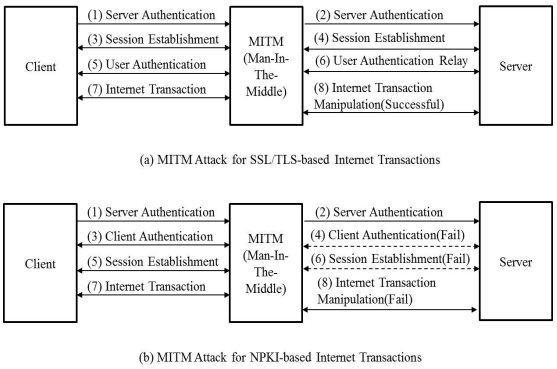

Fig. 3 Comparison of MITM Attack for SSL/TLS and NPKI-based Transactions

인증서에 의해 서버 인증을 수행하는 경우에도 인증 결과 표시에 대한 사용자의 무관심, 정상적인 인증서를 가진 피싱 사이트를 이용한 피싱 공격 등으로 인해, 사용자는 중간공격자의 사이트에 접속하여 민감정보를 공격자에게 노출할 수 있다. 이 경우 중간공격자가 사용자를 대신하여 서버에 접속한 후 사용자와 서버간의 거래를 자신에 유리하도록 조작하는 중간자공격(MITM attack, Man-In-The-Middle attack)을 수행할 수 있다. Fig. 3의 (a)에서 보는 것처럼 클라이언트 인증이 없는 SSL/TLS의 경우 피싱 공격으로 사용자가 공격자 사이트를 접속하도록 속여 클라이언트가 공격자 사이트와 세션을 설정하기만 하며, 서버는 클라이언트 인증을 요구하지 않으므로 중간 공격자가 사용자를 대신하여 서버와 정상적인 세션을 쉽게 설정한다. 즉, 사용자-중간 공격자-서버 간의 연계 세션 설정이 이루어진다. 이후 중간 공격자는 사용자와 서버간의 별도의 사용자 인증 정보(예, OTP)를 중계함으로써 중간 공격자는 서버에 대한 사용자 인증 과정을 통과하고, 인터넷 거래 정보 조작을 통해 중간자 공격에 성공하게 되는 것이다.

NPKI 기반의 인터넷 거래의 경우 서버 인증이 성공한 후 반드시 전자서명에 의한 사용자 인증을 요구한다. 전자서명은 세션 설정 과정에서 교환하는 메시지들과 연계되어 생성된다. 따라서 중간 공격자가 피싱 공격을 통해 사용자가 자신의 사이트에 접속하여 사용자-중간 공격자 간의 세션을 설정하도록 유도하더라도, 사용자의 개인키를 알 수 없는 중간 공격자는 서버에게 사용자의 전자서명을 대신 생성할 수 없다. 그리고 사용자의 전자서명은 사용자와 중간공격자 사이트 간에 교환된 메시지와 연계되어 생성된다. 따라서 사용자의 전자서명이 중간공격자에 의해 서버에게 중계되더라도 도착한 사용자 전자서명은 서버가 중간공격자와 교환한 메시지와 무관하게 생성되었으므로, 서버는 정상적인 전자서명이 아님을 인지할 수 있게 된다. 결과적으로 중간공격자는 서버와 세션 설정을 할 수 없게 되어 사용자-중간 공격자-서버 간의 연계 세션 설정은 실패하게 된다. 따라서 사용자와 서버간의 거래 정보 조작을 통한 중간자 공격을 수행할 수 없게 되는 것이다.

4.3. 암호 및 키교환 알고리즘

SSL/TLS는 세션을 통해 교환되는 정보의 암호화를 위해 3DES, AES 등 다양한 알고리즘을 지원하고, 필요에 따라 새로운 알고리즘을 지속적으로 추가하고 있다. 반면 NPKI의 경우 대부분 자체적으로 개발된 SEED 알고리즘을 통한 암호화를 지원한다. SEED 알고리즘은 AES 등과 같이 충분히 안전한 것으로 증명이 되고 있고, TLS 1.2에 의해 표준 암호 알고리즘의 하나로 채택되었다. 그러나 SEED는 우리나라를 제외한 나머지 국가에서 거의 사용되고 있지 않고, 표준 웹 브라우저에 의해 지원이 되지 않는 문제가 있다. 따라서 NPKI의 암호화 기능이 여전히 ActiveX등을 사용한 웹 확장 플러그인 형태로 구현되어야 한다.

NPKI 기반의 인터넷 거래에서 키교환은 클라이언트 응용 프로그램이 서버의 공개키로 세션키를 암호화하여 서버에게 전달하고, 서버는 자신의 개인키로 세션키를 복호화하는 RSA 방식으로 이루어진다. 따라서 NPKI에서 서버의 공개키와 개인키는 세션키 교환에 필

요한 롱텀키(long-term key)가 되고, 서버와 인터넷 거래를 수행하는 사용자들의 모든 세션키는 롱텀키인 서버의 개인키에 의해 복호화될 수 있다. 이것은 만약 서버의 개인키가 공격자에게 노출되는 경우 서버와 거래한 모든 사용자의 거래 내역에 관한 정보가 공격자에게 노출될 수 있음을 의미한다. 이 문제를 전방향 비밀성(forward secrecy) 미보장 문제라 한다[10]. 서버에 의한 전방향 비밀성 미보장은 인터넷 거래 과정에서 생성된 사용자 프라이버시 정보가 추후 심각하게 침해될 가능성이 있음을 의미한다. 2011년부터 Google은 Gmail 서비스 등 중요 서비스에 대해 SSL/TSL 기반으로 전방향 비밀성을 보장하고 있고, 2013년 11월부터 Twitter도 전방향 비밀성을 지원하고 있다.

SSL/TLS는 RSA 방식 외에도 롱텀키와 무관하게 세션키를 생성하는 DHE와 ECDHE와 같은 다양한 키교환 알고리즘을 지원한다. DHE와 ECDHE의 경우 서버의 개인키가 노출되더라도 서버와 교환된 이전의 세션키들이 노출되지 않으므로 SSL/TLS는 전방향 비밀성을 보장할 수 있다.

4.4. 전자서명과 부인방지

NPKI는 사용자 인증뿐만 아니라 거래인증 단계에서 사용자의 전자서명을 서버에게 전송한다. 전자서명은 기본적으로 자신의 행위(예, 거래정보 전송)에 대한 부인을 방지할 수 있는 부인방지 기능을 제공하므로, NPKI는 서버가 사용자의 거래 사실 부인을 방지하기 위한 별도의 기능 구현을 불필요하게 한다. 반면 사용자의 전사서명 대신 OTP 등을 통해 거래인증을 수행해야 하는 SSL/TLS의 경우 사용자의 거래 사실 부인방지를 위한 별도의 기능을 구현할 필요가 있다. [11]은 TTP (Trusted Third Party)에 의존하는 OTP 기반의 부인방지 프레임워크를 정의하고 있다.

Ⅴ. 국내 NPKI 기반 인터넷 거래 환경 개선 방향

NPKI 기반의 인터넷 거래와 SSL/TLS 기반의 인터넷 거래의 비교분석 결과를 토대로, 현재 우리가 사용하고 있는 NPKI 기반의 거래 환경은 다음과 같은 방향으로 개선될 필요가 있음을 알 수 있다. Table 3은 이를 요약하고 있다.

Table. 3 Future Enhancement of NPKI-based Transactions

Items	Current	Future
Protocol Architecture	Transaction over NPKI over HTTP	Transaction over HTTP over SSL/TLS
Sever Authentication	Public Certificate-based	EV-Certificate-based
Client Authentication	Public Certificate + Digital Signature	SSL/TLS Client Authentication(Public Certificate + Digital Signature)
Encryption Algorithm	SEED	3DES, AES, SEED, etc.
Key Exchange Algorithm	RSA	RSA, DHE, ECHDE, etc.
Non-repudiation	Digital Signature	Digital Signature
Defense for MITB Attack	E2E + Transaction Authentication	Security Token-based Transaction Authentication

- SSL/TLS상의 HTTP상의 인터넷 거래(Transaction over HTTP over SSL/TLS) 프로토콜 구조로 전환 : 새로운 보안 기술 수용에 대한 개방성을 높이고, 개방된 환경에서의 보안성 검증 기회를 확대하며, 표준 웹 환경과의 호환성 제고를 위해 현재의 폐쇄적인 NPKI 프로토콜 체계는 국제 표준 프로토콜 체계로 전환하는 것이 바람직하다.
- 확장 검증 방식 인증서(EV-Certificate) 기반의 서버 인증으로 전환: 위조 사이트를 통한 피싱 공격을 보다 효과적으로 방어하기 위해서는, 자체적인 공인 인증서를 서버 인증에 적용하는 것 보다는 표준 웹 브라우저의 사용자 인터페이스와 잘 통합된 확장 검증 방식 인증서(EV-Certificate)를 서버 인증에 사용하는 것이 바람직하다.
- 공인인증서와 디지털 서명 기반의 클라이언트 인증 유지 : SSL/TLS는 클라이언트 인증을 선택 사양으로 정의하고 대부분의 SSL/TLS 기반의 인터넷 거래는 사용자 인증서 인프라 구축의 어려움으로 인해 클라이언트 인증을 지원하지 않고 있다. 클라이언트 인증이 결여된 SSL/TLS는 중간자 공격(MITM)에 취약하므로 향후 SSL/SSL 기반의 인터넷 거래 환경으로 전환하더라도, 현재 잘 구축된 공인인증서 인프라(NPKI)를 활용하여 SSL/TLS의 클라이언트 인증을 필수로 적용하는 것이 바람직하다.

- SSL/TLS의 다양한 표준 암호 알고리즘 체계로 전환 : 새로운 암호 기술 수용에 대한 개방성을 높이고 표준 웹과의 호환성을 높이기 위해, 현재 자체적인 SEED 암호 알고리즘 전용 체계에서 SSL/TLS의 다양한 표준 암호 알고리즘 체계로 전환하는 것이 바람직하다.
- SSL/TLS의 다양한 키교환 알고리즘 체계로 전환 : 현재 NPKI 기반의 인터넷 거래에서 지원하는 RSA 기반의 키교환 메카니즘의 치명적인 전방향 비밀성(forward secrecy) 미보장 문제를 해결하기 위해서는, RSA뿐만 아니라 전방향 비밀성을 보장하는 DHE, ECDHE 등을 지원하는 SSL/TLS의 다양한 키교환 알고리즘 체계로 전환하는 것이 바람직하다.
- 디지털 서명 기반의 거래 인증 유지 : SSL/TLS 프로토콜 체계로 전환하더라도 공인인증서 기반의 디지털 서명을 통한 거래 인증을 유지함으로써, NPKI 기반 인터넷 거래의 부인 방지 기능을 계속 지원하는 것이 바람직하다.
- 외부 보안 토큰을 통한 거래 인증 체계로 전환 : SSL/TLS 프로토콜 체계로 전환 시에 더욱 우려되는 MITB(Man-In-The-Browser) 공격을 효과적으로 방어하기 위해, 웹 브라우저와 독립적으로 동작하는 안전한 보안 토큰 상에서 거래 인증이 수행되는 체계로 전환하는 것이 바람직하다.

Ⅵ. 결 론

NPKI는 우리나라의 안전 인터넷 거래 환경을 세계에서 유래를 찾을 수 없을 정도로 빠르게 활성화시켜왔다. 그러나 NPKI는 폐쇄적인 구조로 운영되어 왔기 때문에 새로운 보안 기술에 대한 개방성 부족과 표준 웹과의 호환성 부족 등의 문제도 함께 안고 있다. NPKI의 개방성과 호환성 문제는 국제 표준인 SSL/TLS로의 전환을 통해 해결될 수 있다. 본 논문은 NPKI의 장점을 유지하며 SSL/TLS로 전환하는 방법을 제시하기 위해 NPKI와 SSL/TLS를 비교분석하였다. 이를 통해 NPKI를 SSL/TLS 기반으로 전환할 경우 개방성과 호환성 문제 해결뿐만 아니라, 서버 인증 강화를 통한 피싱 공격 방어 역량 강화와 DHE 및 ECDHE 키교환 알고리즘 적용을 통한 전방향 비밀성 보장도 기대할 수 있음을 보였다. 그러나 NPKI 환경을 SSL/TLS 기반으로 전환할 경우, SSL/TLS의 클라이언트 인증 결여로 인한 MITM 공격에 대한 취약성 문제, 전자서명 결여로 인한 부인방지 기능 미흡 문제, 그리고 높은 MITB 공격 가능성 문제 등에 대한 해결 방안이 함께 제시되어야 함을 알 수 있었다. 다행히 SSL/TLS가 인증서 기반의 클라이언트 인증을 선택적으로 제공하므로 NPKI의 공인인증서를 활용하여 SSL/TLS의 클라이언트 인증과 전자서명 기능은 쉽게 활성화할 수 있다. 그러나 NPKI를 SSL/TLS 기반으로 전환하는 경우 확장E2E를 활용한 MITB 공격 방어는 불가능하다. 따라서 NPKI를 SSL/TLS 기반으로 전환하는 경우 HSM(Hardware Security Module) 등 거래서명을 할 수 있도록 보완한 확장된 하드웨어 토큰을 도입하고, 웹 메모리 대신 하드웨어 토큰에서 거래인증을 안전하게 수행하게 함으로써 MITB 공격을 방지할 수 있는 방안 등을 추가적으로 강구할 필요가 있음을 알 수 있다.

REFERENCES

[1] RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, IETF, May 2008.

[2] Y. K. Song, “Lessons of Public Certificate-related Debates and A Policy-direction Proposal for Future Digital Transactions,” *KDI FOCUS*, no 51, March 2015.

[3] Financial Security Institute, “A Management Guide for Financial Part Encryption Technologies,” Jan. 2010.

[4] Y. J. Maeng, D. O. Shin, S. H. Kim, D. H. Nyang, and M. K. Lee, “A Vulnerability Analysis of MITB in Online Banking Transactions in Korea,” *Internet and Information Security*, vol 1, no. 2, pp. 101-118, Nov. 2010.

[5] Financial Services Commission, “Integrated Solutions for Enhancement of Financial Transaction Security,” Press Release, July 2013.

[6] H. S. Kim, J. H. Huh, and R. Anderson, "On the Security of Internet Banking in South Korea," Oxford Univ. Computing Laboratory, CS-RR-10-01, Oct. 2010.

[7] RFC 5246, *The Transport Layer Security(TLS) Protocol Version 1.2*, IETF, Aug. 2008.

[8] S. Kiljan, K. Simoens, D. D. Cock, M. V. Eekelen, and H. Vranken, "Technical Report : Security of Online Banking

Systems," Technical Report of Open Universiteit, Feb. 2014.

[9] CA/Browser Forum, *Guidelines For The Issuance And Management Of Extended Validation Certificates Version 1.5.5*, March 2015.

[10] Wikipedia, Forward Secrecy[Internet]. Available : https://en.wikipedia.org/wiki/Forward_secrecy.

[11] X.1156, *Non-repudiation Framework based on One-Time Password*, ITU-T, June 2013.

박승철(Seungchul Park)

1985.2 : 서울대 계산통계학과 졸
1987.2 : KAIST 전산학과 석사
1996.8 : 서울대 컴퓨터공학과 박사
ETRI 연구원, 한국IBM, 현대전자 네트워크연구소장, 현대네트웍스(주) 연구소장 역임,
현재 한국기술교육대학교 컴퓨터공학부 교수
※관심분야 : 컴퓨터 네트워크, 멀티미디어통신, 네트워크 보안