2001년 한국정보처리학회 추계 학술발표논문집 제8권 제2호

IPv6 기반의 전자상거래 보안 프로토콜의 진화

최정선, 김건웅, 박용식
목포해양대학교 해양전자·통신공학부
e-mail: light-wind@hanmail.net

Evolution of E-commerce Protocols in IPv6

Jung-Sun Choi, Geonung Kim, Ryoung-Sik Park
Faculty of Electronic & Communication Engineering,
Mokpo National Maritime University

요약

인터넷의 보급으로 전자상거래가 활성화 되고 있는 시점에서 무엇보다 중요한 것이 보안 문제인데, 현재의 인터넷에서 전자상거래와 관련하여 이용되고 있는 보편적인 보안 프로토콜이 SET와 SSL이다. IPv4의 여러 가지 한계를 극복하고자 진행되고 있는 IPv6에서 무엇보다도 주목할 점은 망 차원에서의 보안기능이 강화되고 있다는 점인데, 본 논문에서는 이러한 IPv6의 IPsec과 SET 그리고 SSL의 기능 및 역할을 고찰하고, 향후 차세대 인터넷에서의 전자상거래 관련 보안 프로토콜의 진화 방향을 제시한다.

1. 서론

최근 인터넷의 급속한 확산에 의하여 인터넷상의 전자상거래가 활발히 이루어지고 있다. 이러한 전자상거래 서비스의 실효성을 확보하기 위해서는, 전송되는 정보의 비밀성, 전송되는 정보가 변경되지 않았다는 보장과 전송자의 신분을 증명하고 사후 자신의 행위에 대한 부인 불가를 위한 서비스가 반드시 필요하다.

현재의 전자상거래 프로토콜인 SET(Secure Electronic Transaction)[1,2,3]나 SSL(Secure Socket Layer)[1,3,4]은 상대적으로 취약한 IPv4를 기반으로 하기 때문에, 보안에 관련된 서비스를 응용계층에서 제공하고 있다. 그러나 망 계층에서의 보안이 강화되는 IPv6[5,6,7]에서는 SET 와 SSL의 기능 변화가 필수적이다.

본 논문에서는, 먼저 2장과 3장에서 SET와 SSL의 기능과 동작을 살펴보고, 4장에서는 IPv6에서 제공되는 IPsec의 보안 서비스를 고찰하고, 이를 반영한 전자상거래 보안 프로토콜의 진화 방향을 제시한 후, 5장에서 결론을 맺는다.

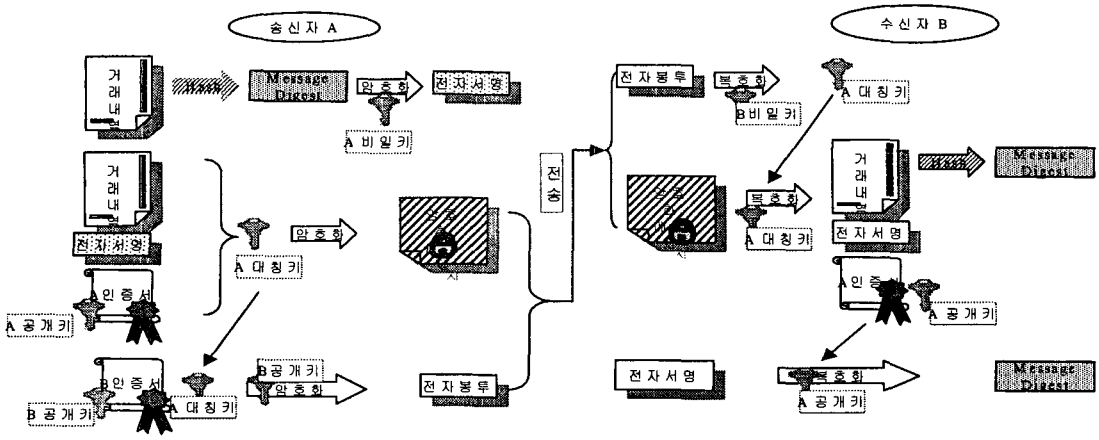
2. SET

SET는 인터넷을 이용한 전자상거래에서의 안전한 지급결제를 위하여 비자와 마스터카드사가 공동으로 개발한 신용카드지불을 위한 프로토콜이다. SET은 전자상거래시 안전한 지불을 위하여 고객과 판매자가 서로의 신분을 확인할 수 있는 인증에 관한 내용과 인터넷 상에서 메시지를 안전하게 주고받을 수 있는 암호화 기법에 관한 내용, 지불절차에 관한 내용을 담고 있다. SET의 동작은 크게 메시지의 암호화와 전자증명서 그리고 디지털 서명[8]으로 설명 할 수 있다

먼저 메시지의 암호화는 카드사용자의 계좌번호, 신용카드번호, 지불정보 등의 민감한 정보의 노출을 방지하기 위해 메시지를 암호화한다. 암호화 알고리즘[9]은 대칭키(비밀키-128bit) 방식이며, 키의 분배를 위해 RSA(공개키-1024bit) 방식을 사용한다. 여기서의 대칭키[9]는 거래 때마다 바뀌기 때문에, 세션키(session key)라고도 부르며, 키의 암호화와 복호화 방식이 같으므로, 카드사용자는 이 키의 보안에 힘써야 한다. (그림 1)은 SET의 메시지 처리 과정을 보이고 있다.

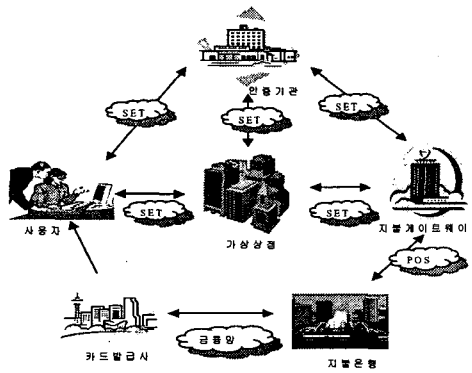
전자서명 기술[8]은 자신의 공개키를 외부에 공개한 후, 이를 이용하여 자신을 상대방에게 인증시키는 기술이다. 사용자의 공개키와 개인정보를, 믿을 수 있는 제3자가 보장해 주는 것을 공개키 인증이라고 하고, 이러한 역할을 하는 제3자를 인증기관(Certification Authority)이라고 한다. 인증기관이 발급한 사용자의

(그림 1)SET의 메시지 처리과정



공개키에 대해 보증하는 전자문서를 인증서(Certificate)라고 하며, 인증기관은 자신의 개인키로 사용자의 공개키 인증서를 전자서명함으로써, 사용자가 합법적인 사용자임을 증명하고, 인증서의 무결성을 보장한다. 이때, 거래 당사자들간의 인증을 위해 X.509를 기반으로 하는 인증서를 발급 받는다.

디지털 서명[8]은 메시지에 해쉬함수를 적용해서 나온 다이제스트(digest)를 비밀키로 암호화한 것이다. 수신측에서는 메시지에 해쉬함수를 적용한 결과와, 전송된 디지털 서명 값을 공개키로 복호화해서 얻은 결과가 동일하면 무결성이 입증된다. 거래 당사자가 모두 서명하는 이중서명방식을 사용함으로써 판매자가 신용카드 정보를 엿볼 수 없으며 은행은 어떤 물품을 구입하였는지 알 수 없게 한다.



(그림 2) SET와 전자상거래 구성 요소

(그림 2)는 SET의 구성요소와 전체 처리과정을 보이고 있다. 사용자는 상품을 구매하는 개인이나 기업이며, 카드 발급사는 사용자에게 신용카드를 발급해주고 그 계정을 관리하는 금융기관으로서 사용자의 적법성 확인을 수행한다. 판매자는 카드가맹점으로서 사용자에게 상품과 서비스를 제공한다. 지불은행은 판매자의 계정을 생성하고, 카드승인과 지불을 처리한다. 지불게이트웨이는 사용자의 카드번호를 보호해주며, 판매자들이 실시간으로 신용카드의 유효 여부를 확인할 수 있게 해주고, 지불은행과 인터넷 사이에서 인터페이스 역할을 하며 인터넷에서 받은 주문 정보를 번역하여 은행 처리 시스템으로 전달해준다.

SET의 처리 흐름을 보면, 사용자와 판매자, 지불 게이트웨이는 모두 인증기관으로부터 인증을 받아야 한다. 사용자가 판매자에게 제품구매를 원하면, 판매자는 인증기관을 통해서 사용자가 인증이 되었는지를 확인한다. 제품을 판매한 후에 판매자는 지불 게이트웨이에게 지불을 요구하는데, 이때에도 서로에 대한 인증을 인증기관을 통해서 하게된다. 이와 같이, 금융거래에 참여하는 모든 구성원의 신원 확인과 인증이 필요하고, 이를 인증기관에서 담당한다.

현재까지 SET는 구성요소간의 시스템적, 제도적 인프라의 구축이 미비하고 이를 적용하고자 하는 신용카드 회사들의 준비도 부족한 상태로, 앞으로 참여 주체간의 제도적 합의와 각종 기준이 마련되어야만 제기능을 다 할 수 있다[5]. 이러한 제반 요건이 갖추어진다면, SET는 인증, 이중 서명, 메시지의 비밀성 등 전자상거래의 요구되는 보안 조건을 모두 갖춘 지불결제 프로토콜로 사용이 가능할 것이다.

3. SSL

Netscape사에서 개발된 SSL은 서버와 클라이언트 사이에서, 인증되고 암호화된 통신을 위하여 일반적으로 사용되고 있다. SSL은 기본적으로 사용자의 인증 없

이 데이터 암호화를 위해서 개발되었는데 핸드쉐이크 계층(Handshake Layer)과 레코드계층(Record Layer)을 거쳐 작동된다.[2,10]

핸드쉐이크 계층에서는 클라이언트와 서버간에 인증서 교환, 상호 신원확인, 암호화에 사용될 대칭키를 교환하는 과정을 수행하고, 레코드 계층에서는 교환된 대칭키를 가지고 암호화된 소켓을 이용하여 데이터를 주고받는 과정을 수행한다.

SSL은 클라이언트와 서버간의 약정만 맞으면 개인정보의 제공 유무에 관계없이 거래를 개시할 수 있다는 장점이 있으나, 다음과 같은 문제점들이 존재한다. 먼저, SSL은 기본적으로 응용계층에서 수행하는 암호화 프로토콜이기 때문에, IP 스푸핑(IP Spoofing)의 해킹에 취약할 수 있다. 특히 개인정보와 지불정보가 서버에 전송되어야 하기 때문에, 통신망에 대한 해킹, 시스템 내부자에 의한 정보 유출 등으로 개인정보가 외부로 노출될 가능성이 많으며, 운영체제에서 직접 지원을 하지 않기 때문에, 애플릿(Applet)이나 액티브엑스 컨트롤(ActiveX Controller)등의 인터넷 응용프로그램의 보안을 지원하지 못한다. 또한, 인증서와 개인키가 기본적으로 PC에 저장되어 관리되기 때문에, 클라이언트의 이동성에 제약을 받는다.[3] 무엇보다도 SSL 방식에 의한 전자상거래 표준이 마련되어 있지 않기 때문에 쇼핑몰, 인터넷 뱅킹, 기타 정보보호 사이트의 암호화, 인증방식이 서로 상이하고, 따라서 사용자는 정보보호 사이트별로 인증서와 암호화 프로그램을 각각 설치하여야 하는 불편을 감수하여야 한다.

4. IPV6에서의 SSL, SET의 진화

IPv6는 IPv4의 문제점을 개선한 것으로 주소공간의 증가, 라우팅 능력의 개선, QoS에 대한 지원 등을 보강하였고 무엇보다도 보안과 인증 기능이 추가되었다. 보안 측면에서 보면 인증, 데이터의 무결정, 데이터비밀성, 접근제어, 데이터 근원인증, 제한적인 트래픽 흐름 비밀성이 지원된다.

IPsec에서는 인증헤더(AH: Authentication Header)와 ESP(Encapsulating Security Payload) 프로토콜을 통해 보안을 제공한다.[7,8]

인증헤더(AH)는 데이터의 근원지의 신원확인, 데이터의 무결성, 그리고 재연공격방지 서비스를 제공한다. 여기서 데이터의 무결성은 메시지 인증을 담당하는 코드에 의해 계산된 각 필드의 합산 값을 수신자가 확인함으로써 보장되고, 데이터의 인증은 인증시 필요한 키와 인증알고리즘을 SA(Security Associations)와 연계하여 지정하고, 지정된 알고리즘을 수행함으로써 보장되며, 재연방지는 AH에 있는 일련번호 이용하여 보장한다.[7]

ESP는 IP의 암호화된 정보를 전송하는 표준이며, 전송되는 데이터의 무결성을 검증하고, 전송의 비밀성을 제공한다. 암호화 알고리즘을 통하여 오직 송신자와 수신자만이 암호화 키 값을 갖게되고 그 외의 다른 네트워크 상의 노드들은 송·수신측이 전송하는 데이터를 해독할 수 없어 트래픽의 비밀성도 제공된다. 다음 <표 1>은 SET와 SSL, 그리고 IPsec에서 제공하는 보안 서비스를 비교해놓은 것이다

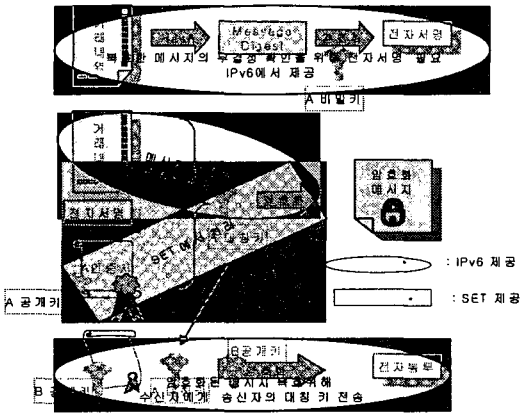
<표 1> 보안프로토콜별 비교

종류 / 서비스	SET	SSL	IPsec
인증	○	○	○
유효성 검증	○	×	×
비밀성	○	○	○
무결성	○	○	○
부인봉쇄	○	×	×
IP spoofing	○	×	○
재연공격 방지	○	○	○
트래픽 공격	×	×	○
암호 프로토콜	복잡함	보통	보통
프로토콜 처리속도	늦음	고속동작 가능	보통
보안위치	응용계층	전송계층과 응용계층 사이	IP 계층

SSL은 전송계층의 상위에서 인증과 기밀성 등의 보안서비스를 제공하는데 반해, IPv6은 망계층에 위치하여, 망 계층 상위의 모든 정보에 대해 보안서비스를 제공할 수 있으며, 터널모드 ESP를 사용하면, SET와 SSL에서 문제되었던 IP 스푸핑같은 공격도 막을 수 있다. 이렇듯 IPv6의 IPsec이 SSL보다는 인증, 기밀성, 트래픽 공격에 대한 보안 서비스가 우수하다. IPv6의 IPsec은 네트워크 규모가 방대하므로 키 교환 메커니즘을 정의하기가 어렵지만 이러한 키 분배 메커니즘이 정의되어진다면, 현 SSL이 가지고 있는 대부분의 문제점을 해결해 줄 것이라 생각된다.

SET는 전자상거래에서 처리되는 여러 처리 절차 중 카드만을 이용한 지급절차에 한하여 정의하고 있어 기존의 신용카드기반을 그대로 사용할 수 있고, IPsec과 SSL에는 없는 인증서 기능이 있다. 이러한 SET는 IPv6를 기반으로 하는 경우, 망계층에서 보안이 이루어지므로 다른 형태로 발전할 것이다. 특히, 키 분배

과정에서 SET의 인증부분을 담당하게 된다면, IPv6의 암호화에서 이용되는 개인키와 이와 대칭되는 공개키를 SET의 인증서에 적용 할 수 있을 것이다. 따라서 IPv6와 SET을 사용하면, 프로토콜 각각의 키 분배가 하나의 키 관리로 가능해진다.



(그림 3) IPv6기반에서 SET의 보안서비스

(그림 3)은 SET의 메시지 암호화 과정에서, IPv6를 기반으로 했을 때, IPsec과 SET가 담당해야 하는 영역을 나타낸 것이다. IPv6를 기반으로 전자상거래 환경이 구축되면, 현 SET의 전자서명 부분과 IPsec의 보안서비스만으로도 안전한 전자상거래가 가능하리라고 본다.

<표 2> 기반별 비교

IP기반	IPv4			IPv6		
종류 / 서비스	IPv4	SET	SSL	IPsec	SET	SSL
인증	×	○	○	○	-	-
유효성검증	×	○	×	×	○	-
비밀성	×	○	○	○	-	-
무결성	×	○	○	○	-	-
부인봉쇄	×	○	×	×	○	-
IP spoofing	×	○	×	○	-	-
트래픽 공격	×	×	×	○	-	-

<표 2>는 IPv4와 IPv6를 기반으로 했을 경우, SSL과 SET가 담당하는 보안 영역을 비교한 것이다. IPv6 기반으로 하는 경우, IPsec가 제공하는 모든 보안이 기본으로 제공된다는 의미가 되므로, 현재 SSL의 모든 서비스가 망 계층에서 제공되며, SET의 경우, 인증서(부인봉쇄 서비스) 기능을 제외한 모든 서비스가 망 계층에서 제공 가능하다.

5.결론

본 논문은 현 인터넷 기반의 전자상거래의 보안 프로토콜인 SET와 SSL을 살펴보고, 향후 IPv6를 기반으로 하는 차세대 인터넷에서의 진화 방향을 제시하였다. 결론적으로, IPv6의 IPsec을 기반으로 하는 경우, SSL은 보안 프로토콜로서의 유용성을 상실 할 것이라 생각되며, SET는 IPsec의 보안기능과 기존의 인증, 부인 봉쇄 서비스가 결합된 형태로 진화하리라 보여진다.

추후 이러한 IPsec의 적용을 위해 필수적인 키 교환 메커니즘과 키 관리 부분에 대해 연구를 계속할 예정이다.

참고문헌

[1]SET specific "Business Description", 1997.5
[2] 류종호, 염흥열, "전자상거래를 위한 전자지불시스템 동향" 한국통신학회지, 제17권 제10호, 2000
[3] 장준형, 배진수, 이경근, "인터넷 보안 프로토콜에 관한 고찰" 한국통신학회, Vol23 NO2 , 2001
[4] 김배현, 김석훈, 유인태, "차세대 인터넷을 위한 정보보안 방안" 한국통신학회, Vol23 NO2 , 2001
[5] Eric A.Hall, "Internet Core Protocols", pp.53-115, 한빛 미디어, 1999
[6] (주)니츠 보안기술연구팀, "인터넷 보안기술 I ", 동서, 2000
[7] Stephen A. Thomas "IPng and the TCP/IP Protocols Implementing the Next Genetation Internet", pp93-126, John Wiley&Sons, inc.
[8]http://www.kisa.or.kr
[9] William Stallings, "Network And Internetwork Security Principles And Practice", pp107-136, Prentice Hall, 1995 Black,
[10]http://ise.yonsi.ac.kr
[11]Uyless D. "Internet Security protocols Protecting IP Traffic", pp.157-170, Prentice Hall, 2000