主題

안전한 전자상거래를 위한 보안기술 개발 방향

전자통신연구원 이주영, 김경범, 손승원

차 례

요 약

최근 빠른 속도로 확산된 인터넷 사용은 전자상거래와 인터넷 사업의 필수 인프라인 정보보호에 관한 관심을 고조시키고 있다. 전자상거래를 이용함에 있어 불안전성은 구조적인 문제, 발달된 해킹기술, 보안에 관한 사용자 인식 부족 등 여러 가지가 문제에 기인한다. 본 논문에서는 전자상거래에서 발생할 수 있는 위협 및 취약 요소들과 그에 따른 보안 요구사항을 살펴보고 이에 대한 솔루션으로서 연구, 개발되고 있는 정보보호 기술을 소개하고자 한다. 그리고 각 솔루션들에 남아있는 과제들을 정리해 봄으로써 전자상거래를 위한 정보보호 기술이 앞으로 나아갈 방향을 제시해 보고자 한다.

Ⅰ. 전자상거래와 보안

최근 컴퓨터 시스템의 성능 향상과 더불어 빠른 속도로 확산된 인터넷 사용은 전자상거래에 대한 관심을 고조시키고 있다. 시장전문 조사 기관인 IDC(International Data Corporation)는 전 세계적으로 전자상거래 규모가 지난 1998년 504.3억 달러에서 2003년에는 1조 3,173억 달러에 달할 것으로 전망하고 있다. 특히 국내 인터넷 및 전자상거래 현황에 대한 IDC의 조사를 살펴보면 인터넷 이용자 중에서 최근 3개월 동안 인터넷을 통해 물건을 구입한 경험이 있는 전자상거래 이용자 수는 지난 1998년 국내 인터넷 이용자수의 9.7%에 해당하는 17만 명에서, 1999년 17.5%인 58만 명, 그리고 향후 2003년에는 47.6%인 486만 명에 이를 것으로 전망하고 있다. 이렇게 인터넷 상에서 전자상거래가 부각됨에 따라 인터넷 사업의 필수 인프라인 정보보호에 대한 요구가 절실해 지고있다. Cyber Dialogue의 American Internet User Survey(AIUS)에 따르면 전자상거래를 하는데 있어서 가장 큰 장애요인은 정보보호에 대한 불신과 프라이버시의 침해 문제이며 전자상거래 사이트에

개인정보보장 정책의 공표가 온라인 쇼핑몰 재방문 결정에 중요한 요인이 되는 것으로 나타났다[1].

전자상거래를 이용함에 있어 불안전성은 여러 가지 문제에 기인한다. 우선 인터넷 그 자체만으로는 구조적으로 안전한 정보체계가 될 수 없다는 사실이 보편적으로 알려져 있으며 최근 다양하고 발전된 해킹기술은 사용자의 인터넷에 대한 불신을 가중시키고 있다. 또한 PC 운영체제는 바이러스나 다른 악의적 소프트웨어들에 대한 안전성을 거의 제공하지 않고 있다. 이와 더불어 정보유출에 대한 걱정에 비해 보안 인식에 대한 사용자의 인식이 매우 낮음도 간과할 수 없는 요인이다. 이러한 문제들은 현재 전자상거래의 발전에 걸림돌이 되고 있다. 하지만 전자상거래는 기존의 오프라인 거래에서 제공할 수 없는 시간과 공간 상의 많은 장점을 지니고 있기 때문에 전자상거래로의 흐름은 지속적으로 이루어질 것으로 전망된다. 따라서 불안전한 환경에서 안전한 전자상거래를 하기 위해서는 거래선간의 상거래 트랜잭션이 글로벌 공공 네트워크에 걸쳐 일어날 수 있도록 하는 거래선의 신원 보장과 트랜잭션의 내용이 가로채이거나 조작되지 않는다는 보장을 제공하기 위한 기술, 정책, 인프라를 제공이 필요하다.

본 논문에서는 전자상거래에서 발생할 수 있는 위협요소나 취약성 문제들과 그에 따른 보안 요구사항을 살펴보고 이에 대한 솔루션으로서 제안되고 있는 정보보호 기술을 소개하고자 한다. 그리고 각 솔루션들에 남아있는 과제들을 정리해 봄으로써 안전한 전자상거래를 위한 정보보호 기술이 앞으로 나아갈 방향을 제시해 보고자 한다.

Ⅱ. 전자상거래의 취약 요소들과 보안 요구사항

전자상거래에서 발생할 수 있는 위협요소나 취약성 문제들을 살펴보기 위해 한 구매자가 인터넷을 이용하여 상품을 구입하는 상황을 고려해 보도록 한다. 우선 구매자는 ISP(Internet Service Provider)를 통하여 네트워크에 접속하여야 한다. 그리고 구매하고자 하는 제품을 판매하는 판매점의 웹 사이트에 접속한 후 원하는 물건을 검색하고 그에 대한 주문을 할 수 있다. 주문한 물건에 대한 대금을 지불하기 위해서 사용자는 자신의 카드 정보 및 개인 신상정보를 입력해야 한다. 이때 구매자는

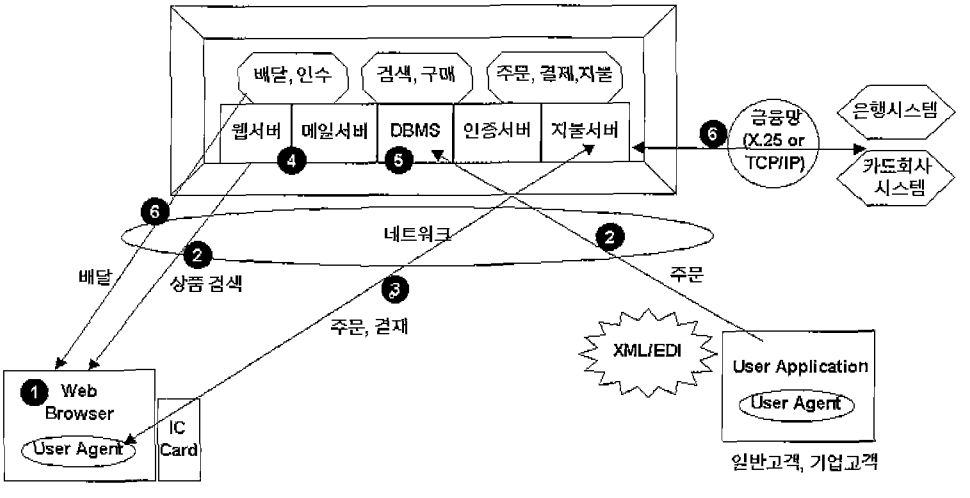

그림 1. 전자상거래 과정과 그에 따라 발생할 수 있는 보안 취약점

자신의 정보가 외부에 노출되거나 변경되지 않고 안전하게 판매자에게 전달되기를 원할 것이다. 구매자의 정보를 받은 판매자는 이 사용자가 카드의 소유자가 맞는지, 사용 가능한 카드인지 등 구매자가 보낸 정보의 정확성에 대한 확인을 한 후에 구매 물품을 보내게 된다. 그리고 거래가 이루어진 후에는 구매자는 자신이 물품 대금을 지불했다는 것과 판매자는 사용자가 구매요청을 했다는 거래 사실을 확인함으로써 구매자의 계좌로부터 물품대금을 인출 받게 된다. 위와 같은 시나리오를 바탕으로 그림 1에 나타난 것처럼 보안상의 취약점을 분석할 수 있다.

(1) 브라우저 소프트웨어의 취약성

현재 브라우저는 보안상 많은 헛점들을 지니고 있다. 따라서 판매자가 구매자의 웹브라우저를 통해서 구매자의 컴퓨터 내에 수록된 정보를 부당하게 수집해 이용할 수 있다.

또한 악의적 의도를 품은 프로그래머가 고의로 사용자의 웹브라우저를 제어할 수 있는 방법을 알아낼 수도 있다. 이를 이용해서 사용자의 컴퓨터를 재포맷하거나 사용자의 은행계좌나 신용카드 정보, 비밀번호 등 중요한 정보를 빼낼 수 있는 소프트 웨어를 다운로드 할 수 있다.

(2) 프라이버시 침해

구매자가 입력한 개인정보 정보는 언젠가 다른 목적을 위해 사용될 수 있다. 예를 들면 개인정보를 빼낸 사람이 사용자의 신뢰를 얻기 위해 그 정보를 사용할 수 도 있고 메일주소가 원하지 않는 메일링 리스트에 등록됨으로써 스팸메일을 지속적으로 받을 수도 있다.

(3) 액티브 컨텐츠에 대한 위험

사용자들이 거래를 위해서 등록한 정보들이 인터넷을 통해 전달되는 동안 신용카드 번호와 같은 중요한 정보들이 제3자에게 노출될 수 있다.

(4) 웹 서버 취약성

경쟁업체의 의도적인 조작으로 인해 웹사이트가 서비스불능 상태에 놓이거나 로봇 에이전트를 이용해 재고량이나 가격정보가 유출될 수 있다. 다른 사용자의 카드정보를 이용한 부당 사용자가 거래를 시도할 수 있다.

(5) 데이터베이스 위협

중요한 데이터를 보관하고 있는 데이터베이스는 매력적인 공격 대상이 된다. 해커나 크래커가 시스템의 데이터베이스나 웹사이트에 침입해 주문정보를 변경하게 되면 상인은 발생한 문제를 처리하기 위해서 상품의 반송, 반환에 따른 비용을 부담해야 할 뿐 아니라 고객의 신뢰를 잃을 수 있다.

(6) 거래부인

전자상거래 과정에서 구매자는 자신이 주문한 제품을 받지 못하거나 물건이 잘못 배달될 수 있다. 판매자의 경우 자신이 납품한 물건에 대해 구매자가 인수 사실을 부인함으로써 대금을 받지 못하는 문제가 발생할 수 있다.

상거래에서 발생할 수 있는 이러한 문제들은 기존의 오프라인 거래에 있어서도 존재해 왔다. 하지만 인터넷과 웹을 통한 상거래에서는 이 위험성들을 확대된다. 인터넷에서는 사용자들이 익명으로 행동할 수 있고 이러한 익명성을 기반으로 쉽게 타인에 대한 공격을 취할 수 있기 때문이다. 따라서 앞서 기술한 위협요소와 취약성을 해결하고 안전한 전자상거래를 하기 위해서는 다음과 같은 요구사항이 충족되어야 한다.

(1) 인증 (Authentication)

인증은 전자상거래 취약요소 (1), (3), (4), (5)에 대한 솔루션을 제공한다. 판매자들은 고객들의 신분이 맞는지 적어도 구매하기에 적합한지를 인증해야 한다. 만약 고객이 신용카드 번호를 사용할 경우 판매자는 고객이 이 신용카드를 사용하는 검증된 사용자인지를 확인할 필요가 있고 고객은 상인의 정체, 즉 자신이 말하는 진짜 상인인지를 확인할 필요

가 있다. 또한 전자상거래에 사용되는 시스템에 대한 접근 권한을 적절하게 제어할 수 있도록 사용자 인증이 필요하다.

(2) 상호 프라이버시

개인정보가 그 목적지에 도달한 이후에 개인적인 것으로 남아 있는다고 확신할 수 있도록 프라이버시 침해(2)에 대한 해결이 필요하다. 금융거래 참여자는 유출된 거래 내역은 불법 거래를 위한 정보를 제공할 수 있기 때문에 대부분의 경우 세부사항을 기밀로 하여 프라이버시를 보호해야 한다. 이를 위해서 신용카드 번호화 고객정보는 판매자 사이트에 안전하게 저장되어야 하고 고객과 판매자는 어떻게 판매자가 고객의 정보를 사용할 수 있는지에 대해 합의를 해야 한다. 또한 고객과 판매자는 어떻게 가격과 가용성 같은 판매자 정보를 고객이 사용할 수 있는지에 대해서도 합의해야 한다.

(3) 무결성 (Integrity)

전자상거래 과정에서 고객과 판매자가 상호 신뢰를 하는 것이 중요하다. 상거래 및 개인정보가 한쪽에서 다른 쪽으로 정확하게 전송되며 지불 거래와 관련된 약정들을 상대가 모르게 수정하지 않는다고 확신할 수 있어야 한다. 이를 위해서 원격지에서 전송된 메시지가 위, 변조되지 않았음을 증명할 수 있는 방법을 제공함으로써 개방된 인터넷을 통해 전달되는 액티브 컨텐츠에 대한 위험(3)을 방지해야 한다.

(4) 기밀성 (Confidentiality)

네트워크를 통해 전송되는 메시지를 송신자 및 적법한 수신자를 제외한 제3자는 볼 수 없도록 하는 기능과 로컬 시스템에서 안전한 저장, 그리고 기밀 데이터의 적절하게 사용하도록 제한 할 수 있는 방법이 필요하다. 이는 전자상거래 취약요소 (3)과 (5)의 솔루션이 될 수 있다.

(5) 거래부인봉쇄 (Non repudiation)

안전한 전자상거래를 하기 위해서는 취약요소 (6)이 해결되어 고객과 판매자 양측은 합의한 어떤 것도 부인하지 못한다는 확신을 가져야 한다. 따라서 메시지를 송수신한 경우 해당자가 송수신에 대한 행위를 부인할 수 없도록 하여 합의를 한 어느 한쪽이 동의안에 서명한 장본인이 아니라고 주장하는 것을 미연에 막을 수 있어야 한다.

Ⅲ. 안전한 전자상거래를 위한 보안 기술 요소

안전한 전자상거래를 수행하기 위해서는 기반기술, 전자상거래를 수행하는 과정에서 발생할 수 있는 보안위험성을 고려하여 설계된 지불기술 그리고 데이터가 전송되는 네트워크를 보호할 수 있는 기술이 적절하게 적용되어야 한다. 그림 2에 앞서 기술한 전자상거래의 취약 요소들과 그에 따른 요구사항을 해결하기 위한 정보보호 기술들을 제시하였다. 본 절에서는 이들 중 핵심이 되는 몇 가지 요소들에 대해 살펴보기로 한다.

1. 지불수단 요소

(1) 전자지불

전자지불은 전자상거래를 도모하기 위해 개발된 신기술의 유용한 모델이자 인프라가 되고 있다.

전자지불의 목적은 구매자나 판매자 모두가 안전하고 신뢰할 수 있는 가치 이전의 방법을 제공하고자 하는 것이다. 전자지불 시스템은 신용카드로부터 시작하여 네트워크형 전자화폐로 발전하고 있다. 전자화폐는 종류에 따라 크게 가치저장형, 지불지시형, 네트워크형 이 세가지로 분류된다. 이 중 네트워크형은 화폐의 가치를 인터넷과 같은 네트워크를 통해 주고받는 것으로서 실세계에서 사용되고 있는 화폐형식을 그대로 모방해 실세계의 사용방법과 특성을 같게 만들기 위한 것이다. 대표적인 예가 네덜란드의 Digicash사에서 발행하는 Ecash, 캘리포니

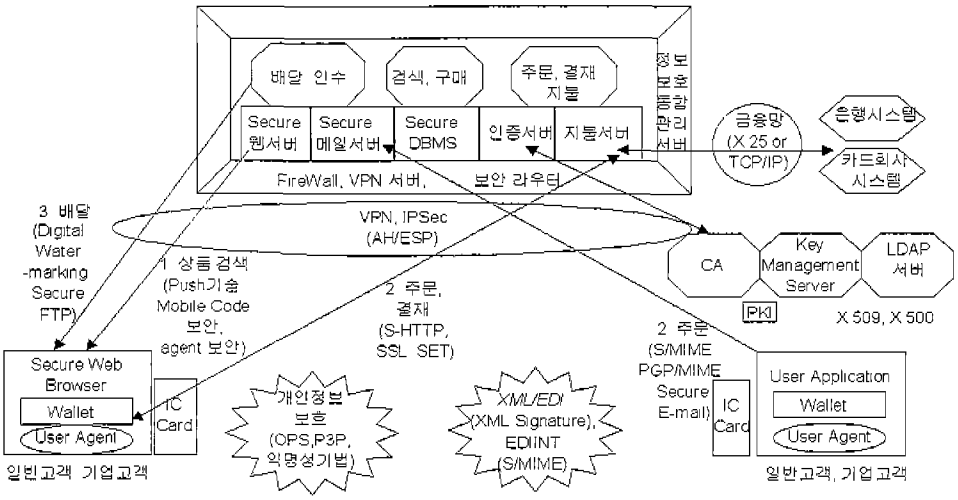

그림 2. 전자상거래 시스템 구성요소별 보안기술

아 대학에서 개발 중인 Netcash 등이 있다[2].

앞으로 전자상거래를 위한 지불기술에는 현금의 기능을 하는 시스템 뿐 아니라, 수표와 지로를 전자 발행하는 시스템도 등장할 것이며 또한 고객과 기업이 지불 및 신용카드를 이용할 수 있도록 고안된 방식도 생길 것이다. Giga에 따르면 현재 가장 많이 이용되는 지불수단은 지불카드(98년 99%, 2002년 90% 예상)이며, 그 다음으로 전자수표, 지로, 전자화폐(1998년 1%미만, 2002년 2~5 예상)가 그 뒤를 잇고 있다[2]. 하지만 현재 전자상거래를 위해 널리 활용되고 있는 지불기술 인프라는 없으며 최근 들어 발표되는 무수한 솔루션들 중 몇몇 지불기술들이 주도적인 입지를 차지하고 있다. 그리고 여러 관련 기술업체, 금융기관, 신용카드 회사 들은 서로 상이한 기술과 표준을 제공하고 있으며 구축이나 활용면에서 상이한 단계에 놓여 있다.

(2) SET

최근 널리 쓰이는 지불방식들은 SSL을 이용하여 정보를 보호하고 있다. 그러나 SSL을 이용할 경우에는 신용카드나 직불카드의 번호와 같은 중요 정보들이 사용자의 의지와 상관없이 여러 경로로 노출될 수 있으며 또한 거래 당사자들의 인증수단이 취약하다는 단점이 있다. 이를 보완하기 위해 등장한 것이 SET(Secure Electronic Transaction) 프로토콜이다.

SET 프로토콜은 부정 방지를 위해 상인이 지불카드의 인증된 수신자임을 보증하고 구매자가 지불카드의 인증된 사용자임을 보증하는 등 양측이 지불과정에 신뢰를 추가하도록 고안되었다[3]. 그러나 SET은 판매자가 고객의 신용카드 번호에 접근하는 것을 허용하지 않기 때문에 고객의 신상명세서 작성, 분쟁해결, 배상 같은 프로세스들이 복잡하다는 문제를 가지고 있다.

(3) 스마트카드

스마트카드는 플라스틱 카드에 마이크로 칩을 내장하고 있으며 그 안에 정보를 수록하고 내장된 마이크로 프로세서와 함께 응용 프로그램을 수행할 수 있다. 전자 보증서, 암호키 등을 스마트카드에 저장함으로써 신원인증 카드, 전자화폐, 신용카드 등으로 사용될 수 있다[2]. 현재 유럽이 스마트카드 산업의 선두를 차지하고 있으며 세계 시장의 90%를 차지하고 있다. 스마트카드를 주도하는 회사는 Gemplus, Schlumberger 및 Mondex USA 등이 있으며 최근 motorola도 본 분야에 참여하였

다. 스마트카드는 지불시스템 및 전자화폐 시스템이 발전함에 따라 그 중요성이 부각될 것으로 예상된다.

또한, 스마트카드의 보안성을 강화하기 위하여 사용자의 패스워드보다 안전하고 쉽게 변하지 않는 특징을 갖고 있는 생체 인식 기술의 접목도 최근 활발히 시도되고 있다. 예를 들어, 스페인에서는 스마트카드에 지문 정보를 저장하여 주민증과 의료 서비스에 활용하는 TASS 프로젝트를 수행중에 있으며, Gemplus에서는 스마트카드에 저장된 지문 정보가 인식 처리를 위해 단말기로 전송될 때 외부로 누출되는 위험을 최소화하기 위하여 지문 정보 저장뿐 아니라 인식 처리까지도 스마트카드에서 수행하는 Match-on-Card 기술을 개발 중에 있다.

(4) S/MIME

디지털 시대에 전자우편은 가장 보편적인 통신 수단으로 자리를 잡았다. 하지만 전자우편은 별다른 데이터 암호화 과정이 없이 직접 파일을 전송하기 때문에 보안성 면에서 취약하다. 침입자들은 전자메일이 통과하는 지점에 그들의 소프트웨어를 설치한 후 신용카드 번호 혹은 이름 등을 키워드로 이용하여 선택적으로 정보를 수집할 수 있는 것으로 알려져 있다. 따라서 정보보호 서비스가 제공되지 않는 전자메일의 사용은 전자상거래 이용 시 매우 위험하다. 전자우편 보안서비스는 편지 내용을 암호화해 정보 유출이나 정보 검열, 무단 해킹에서 벗어나 안전한 전자우편 송수신 체제를 갖는 것을 목적으로 한다.

현재 전자메일에 정보보호 서비스를 제공하는 기술은 S/MIME과 Open PGP가 대표적이며 시장 석권과 표준채택을 위해 경쟁 중에 있다. S/MIME은 RSA Data Security에 의해 개발되었으며 Netscape 및 Microsoft가 그들의 브라우저에 사용하고 있다[7]. Open PGP는 IETF에 의하여 워킹그룹이 결성되었다. S/MIME은 X.509 보증서를 사용하는 반면 Open PGP는 자체 개발한 보증서를 채택하고 있다.

2. 사용자 인증 요소

(1) 전자서명

전자서명(digital signature)은 개인의 고유성을 주장하고 인정 받기 위해서 전자적 문서에 서명하는 방법으로 신뢰성과 무결성 확보를 목적으로 한다. 이는 서명 방법에 따라 메시지 복원형 전자서명과 메시지 부가형 전자서명으로 나눌 수 있다[4]. 메시지 복원형의 경우 RSA와 같이 공개키로 암호화하고 비밀키로 복호화 하거나, 비밀키로 암호화하고 공개키로 복호화 해도 본래의 메시지가 복원되는 서명 방식이다. 이 방법은 기존의 공개키 암호 시스템을 이용하기 때문에 별도의 전자서명 프로토콜이 필요하지 않다는 장점이 있는 반면 메시지를 일정한 크기의 블록으로 나누어 그 각각의 블록에 대해서 서명을 해야 하므로 서명의 생성이나 검증과정에서 많은 시간이 소요되는 단점을 가지고 있다.

메시지 부가형의 경우 임의의 길이로 주어진 메시지를 해쉬알고리즘을 이용하여 일정한 길이로 압축하고 해쉬한 결과를 서명자의 비밀키를 이용해 전자서명한 후 메시지에 덧붙여 전송하는 방식을 사용한다. 서명에 대한 검증은 수신된 메시지를 해쉬한 결과와 전자서명을 공개키를 이용해 복호화한 값을 비교함으로써 이루어진다. 이 방법의 경우 메시지 이외에 전자서명을 따로 전송해야 하므로 전송량이 약간 늘어나는 단점이 있지만 메시지의 길이에 상관없이 단 한번의 서명생성 과정만 거치게 되므로 효율적이다.

전자서명은 서명자 이외의 다른 사람이 생성할 수 없기 때문에 위조가 불가능하며 각 사용자에게 유일한 개인키로 서명을 하기 때문에 서명자가 누구인지 확인할 수 있어 서명자인증 기능을 제공한다. 그리고 해쉬결과를 비교하는 과정을 거쳐 서명한 문서의 내용이 변경되었는지를 확인할 수 있다.

(2) PKI

앞에서 기술한 공개키 기반 전자서명은 사용 시에 몇 가지 문제를 고려해야 한다. 공개키가 공개된 장소에 등록되어 있기 때문에 항상 위, 변조에 대한 문제 존재하고 자신이 획득하고자 하는 공개키가 누구의 공개키인지를 확인할 수 있는 수단이 별도로 존재해야 한다는 것이다. 이러한 문제를 해결하기 위해서 사용자의 공개키를 그 사용자의 개인정보와 함께 믿을 수 있는 제3자가 보장해주는 공개키 인증 방법이 제안되었다.

PKI(Public Key Infrastructure)는 공개키 암호기술이 널리 활용될 수 있도록 하는 근본 기술과 제도적 틀로서 공개키 암호시스템을 사용하는 정보보호 응용분야의 효율성과 안전성을 높이기 위하여 구축되었다[5]. PKI는 신뢰성 있는 인증기관에 의한 공개키 인증서를 기본으로 하여 사용자 공개키를 안전하게 전달하는 방법과 신뢰 있게 관리하기 위한 수단을 제공한다. 이 외에도 암호화된 메일, 지불 프로토콜 등 다양한 인터넷 보안 응용을 가능케 하기 위한 바탕을 제공하며 신분 및 권한 확인, 프라이버시 보호, 전자서명, 부인방지 등의 보안 서비스 가능하게 한다.

아직까지 PKI는 인증서의 취소 및 그 유효성을 검사하는 메커니즘이 완전하지 않기 때문에 향후에는 PKI의 관리 및 정책분야의 중요성이 강조될 것이다. 공개키 기반구조 시장은 2000년에 가장 주목받을 보안섹터 중 하나로 꼽히고 있으며 2000~2002년 동안 연평균 63% 성장할 전망으로 이 부분을 주도하는 기업은 점유율 30%이상을 차지하는 Entrust Technology사이다.

(3) 생체인식 기술

생체인식을 통한 보안은 한 마디로 개인의 신체적 특성을 인증화해 보안성을 높인다는 데 초점이 맞춰져 있다. 개인의 신체적 특징은 태어나서 죽을 때까지 변하지 않으며 신체적 특징이 일치하는 사람은 없다는 것을 전제로 하며 패스워드 등 소프트웨어 방식의 사용자 인증보다는 한층 강화된 보안성을 가지고 있다는 점이 생체인식 보안의 가장 큰 장점이다[6]. 생체인식에 이용되는 신체적 특징은 최근 가장 활발히 상용화가 이뤄지고 있는 지문을 비롯해 손바닥 형상, 얼굴, 홍채와 망막, 손등의 정맥, DNA에 이르기까지 다양하며 음성이나 서명 같은 것도 포함된다. 생체인식 기반 보안은 초창기에 출입 통제 분야에 주로 활용됐으나 최근에는 인터넷이나 전자상거래와 맞물려 개인 신원을 확인하는 인증 시스템으로 활용 범위를 넓어지고 있다.

3. 네트워크 보안 요소

(1) 방화벽

방화벽(Firewall)은 인터넷과 같은 공중망으로부터 기업의 네트워크에 불법적으로 접근하는 것을 막기위한 도구이며 안전한 인터넷 연결을 위한 필수 요소이다. 기업 네트워크 내의 호스트들은 서로를 신뢰한다는 가정 하에 시스템이 구축되기 때문에 내부 네트워크 자체의 보안 요구사항은 외부 호스트들이 내부 네트워크에 접근하려 할 때의 보안 요구사항과는 다르다. 이러한 보안 요구사항의 차이점을 해결하기 위해서 내부시스템과 외부시스템을 구분하여 관리함으로써 보안성을 부여하는 시스템이 방화벽이다[7]. 방화벽의 장점은 내부 네트워크 자체의 보안조치가 인터넷 보안과 분명히 구분된다는 점이며 단일 지점에서 모든 기능을 제공하기 때문에 관리가 편하다는 점이다. 하지만 회사 내에서의 전자상거래 이용 시 커다란 장애물이 되고 있다. 기업 내의 사사로운 인터넷 사용이 늘어감에 따라 방화벽 정책은 더욱 강화되는 추세이다. 이를 피하기 위해 모뎀을 사용하는 경우가 있는데 이는 사내 네트워크 보안에 치명적인 약점이 될 수도 있다.

(2) 가상사설망

가상사설망(Virtual Private Network)은 인터넷과 같은 공중망을 사용하되 전용선을 사용할 때

와 같은 QoS와 인터넷에서의 보안기능을 제공하는 것을 목표로 한다. 가상사설망은 터널링 기술을 이용하여 구축된다. 터널링 기술은 전용망 환경에서 점대점으로 회선을 연결한 것과 같은 효과를 위해 두 종단사이에 가상적인 터널을 형성하는 것이며 현재 IETF의 IPsec워킹그룹이 네트워크 계층의 터널링 프로토콜로 제안한 IPsec이 표준으로 자리잡아가고 있다. IPsec은 인터넷망에서 보안문제인 인증, 무결성, 기밀성, 리플레이 방지 등의 기능을 제공하기 위해 만들어진 것으로 가상사설망 터널링을 위한 보안서비스 제공에 적절하다[8]. 이러한 가상사설망은 네트워크에서 임대되는 값비싼 사설망을 대체할 수 있으며 기업 대 기업 또는 본점 대 분점 등을 안전하게 연결하는 익스트라넷의 구축을 용이하게 해준다.

Ⅳ. 안전한 전자상거래를 위한 기반 구조 및 보안 플랫폼

지금까지 안전한 전자상거래를 위해 필요한 보안기술 요소에 대해 소개하였다. 이 기술들을 기반으로 하지만 더 신뢰할 수 있는 환경을 제공하기 위해 각각의 서비스들을 포함할 수 있는 구조와 이러한 서비스들을 적절하게 비즈니스 과정과 결합하는 메커니즘 제공할 필요가 있다. 현재 IBM의 SEMPER와 HP의 Plaesidium이 전자상거래를 위한 보안 플랫폼을 제안하고 있다. 하지만 아직까지 이 문제에 대한 표준이 없고 연구도 부족한 상태이다.

1. SEMPER (Secure Electronic Marketplace for Europe)

SEMPER는 European Commission에 의해 제안된 ACTS (Advanced Communication Technologies and Services) 연구개발 프로그램의 일부분으로서 European Commission 및 20여 개의 유럽업체로부터 지원을 받아 1995년부터 3년간 수행된 프로젝트이다. SEMPER프로젝트가 추구하는 목적은 인터넷과 같이 안전하지 않은 공중망을 통한 전자상거래에서 발생할 수 있는 모든 문제점들에 대한 전체적인 해결방안을 제시하자는 것으로 전자상거래에서 발생할 수 있는 극히 부분적인 영역들만을 해결할 수 있는 현 상황에서 안전한 전자상거래를 이룩할 수 있는 기반구조를 제공하겠다는 것이다. 그림 3은 TCP/IP 프로토콜처럼 계층구조를 이루고 있는 SEMPER의 아키텍쳐이다[9].

SEMPER 아키텍처에서 각 서비스 계층블록은 하나의 프레임워크로 설계하고 있는데, Business applications는 메일, 주문, 소매와 같은 특정 비즈니스 과정을 구현한다. Commerce 계층은 Business application들이 공통적으로 필요한 기능을 쉽게 이용할 수 있도록 하는 빌딩 블록을 제공한다. 이 공통 블록은 익명성과 같이 모든 단계를 통해 강화되어야 할 안전성 요구사항을 충족시키기 위해서 중요하다. Exchange 계층은 전자상거래에 참여하는 모든 구성 요소들 간에 정보가 신뢰성 있게 유통되는 것에 책임을 진다. 여기서 신뢰성있는 정보의 유통이란 구성요소들간에 미리 약속된대로 정보가 교환되는지 여부를 의미한다.

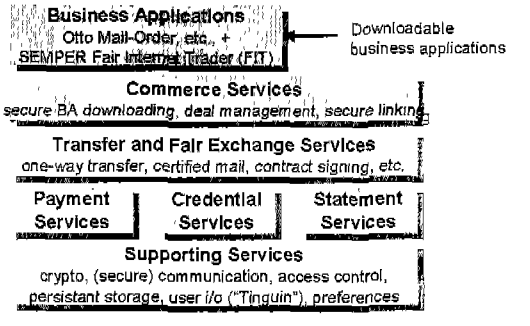

그림 3. SEMPER의 서비스 구조

Transfer 계층은 전자상거래의 구성요소들간에 필요한 정보를 해당 프로토콜에 의거하여 송수신하는 역할을 담당한다. Payment, Credential, Statement 서비스 계층은 지불서비스와 인증서 사용 및 관리, 그리고 모든 종류의 암호화되고 인증된 문서의 전송을 지원한다. 최하위에 있는 Supporting 계층은 상위 계층들을 위한 지원기능을 하며 암복호화, 전자서명 및 키 생성 등의 기능을 담당하는 암호화 서비스, 사용자들에게 사용되는 네트워크의 세밀한 기술적 내용을 감추어주는 역할을 하는 통신 서비스, 보증서, 서명된 문서, 각종 키, 거래 기록 등 장기간 보관되어야 하는 정보를 관리하는 아카이브 서비스, 다양한 서비스들에 대하여 사용자들이 일관성있게 선택사항을 정할 수 있도록 하는 선택사항 제공서비스 등을 제공한다.

SEMPER는 전자상거래에서 필요로 하는 안전성 서비스들을 위한 개방형의 확장가능한 구조를 설계하고 프로토타이핑하고 있지만 SEMPER에서 제안한 각 계층블록들이 가장 유용한 기초적 서비스 블록인지에 대한 의문이나 지적재산권 등 아직 다루지 않은 영역들은 어떻게 포함시켜야 하는지 등이 문제로 남아있다.

2. Plaesidium

HP에서 제안하고 있는 Plaesidium은 안전한 전자상거래를 지원하기 위해 총체적인 솔루션과 제품을 제공하고 있다. 그림 4에 Plaesidium의 서비스 구조가 나타나 있다. Plaesidium은 전자상거래에 필요한 요구사항을 Data privacy, Personalization, User Account Integrity, Application and System Integrity, 그리고 Network Integriry로 구분하여 각 카테고리를 위한 솔루션을 제공하고 있다. Plaesidium의 경우 SEMPER에서처럼 각 계층이 서로간에 순서적인 연계성을 가지고 있는 것은 아니지만 다양한 보안 솔루션들을 제공함으로서 전자상거래 보안을 하고자 하는 사용자들이 선택한 보안 솔루션들을 쉽게 통합할 수 있도록 하고 있다.

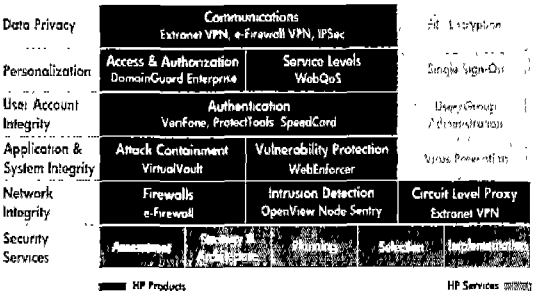

그림 4. Plaesidium의 서비스 구조

V. 보안기술 전개방향

전자상거래 과정 중 발생할 수 있는 위협요소와 취약성을 해결하기 위한 많은 정보보호 기술들이 제안되어 왔다. 하지만 신뢰할 수 있는 전자상거래를 수행하기 위해 아직까지 연구되어야 할 과제들이 남아있다.

첫째, PKI는 고객 인증, 판매자 인증, 거래 부인봉쇄 등의 보안 서비스를 위한 토대를 제공함으로서 공개키 기반의 많은 솔루션들의 핵심이다. 하지만 광역 전자상거래를 위한 시스템이 대규모의 PKI를 필요로 하는 경우에 경험이 별로 없기 때문에 운영시 안전성과 서비스의 유용성에 대한 문제가 발생할 수 있기 때문에 이에 대한 연구가 필요하다[9]. 또한 인증서를 폐지하는 방법에 대해 여러 가지 제안이 존재하지만 완벽하지 않다. 가장 안전한 접근방식은 항상 온라인 검증을 요구하는 것이지만 항상 가능한 솔루션은 아니다. CRL(Certificate Revocation List)과 같은 대안들은 비싸고 효력 발생 시까지의 지연시간이 문제가 될 수도 있다.

둘째, 안전성 시스템에 대한 기존의 사용자 인터

페이스는 너무 기술 기반적이다. 많은 인터넷 사용자들이 전자상거래를 위한 보안의 중요성은 인식하고 있지만 실제 사용 시 보안이 적절히 이루어지고 있는지, 보안정책을 결정하는 경우에 어떤 사항을 선택해야 하는지에 대해 파악하기 어렵다. 따라서 사용자가 보안 정보를 쉽게 점검할 수 있는 사용자 지향의 인터페이스의 개발이 중요하다. 이를 위해 보안정책을 쉽게 추상화 시키고, 정책을 결정하기 위한 사용자와의 인터렉션의 수를 줄이며 현재 제공중인 보안 서비스를 가시화하는 방법을 사용할 수 있다.

셋째, 신뢰할만한 컴퓨팅 베이스가 부족하다. 현재 대부분의 전자상거래 시스템은 PC 운영체제와 표준 웹 브라우저, CGI그리고 자바 스크립트 같은 언어 사용에 의존하고 있지만 이것들이 안전하지 못하다는 것은 보편적으로 알려져 있다. 즉 충분하게 안전하고 상업적인 OS나 좀 더 안전하고 물리적 공격에 잘 견딜 수 있는 사용자 디바이스가 필요하다.

넷째, 지금까지 기술해 온 안전한 전자상거래를 위해 필요한 모든 서비스들을 커버할 수 있는 구조와 안전하게 이러한 서비스들을 비즈니스 과정과 결합하는 메커니즘 제공 필요하다[9]. 대부분의 전자상거래 관련 안전성 연구는 전자 지불 시스템이나 디지털 서명 같은 기본적인 빌딩 블록에 초점을 두고 있다. 그러나 단순한 안전한 스텝이 불안전한 과정으로 결합하는 경우가 많다. 따라서 하나의 비즈니스 과정이 정확하고 안전한지 여부를 결정할 수 있도록 포괄적이고 안전한 과정을 제공할 필요가 있다. 이에 대한 해결책으로서 전자상거래를 위한 몇 가지 보안 플랫폼 프로토타입이 제안되어 있다. 하지만 아직까지 그에 대한 표준화작업과 연구가 부족한 실정이다. 따라서 이 문제에 대한 지속적인 관심이 필요하며 특히 국내 전자상거래 환경에 적합한 프로토타입의 개발도 이루어져야 한다. 이때 개별단계에 대한 보안 뿐 아니라 이들을 연결하는 처리 과정과 무선 미디어를 이용한 전자상거래에 대한 보안도 고려해야 한다. 이에 덧붙여 개발된 전자상거래 시스템의 안전성에 대한 평가기준과 기술이 필요하다.

Ⅵ. 결 론

지금까지 본 논문에서는 전자상거래 과정에서 발생할 수 있는 보안 취약점을 살펴보고 안전한 전자상거래를 지원하기 위한 정보보호 기술들을 살펴보았다.

전자상거래를 도모하기 위한 인프라로서 지불기술은 지난 20여년동안 전자상거래 관련 문제의 주요 목표로 연구되어 많은 솔루션들이 나와있다. 이러한 성과로 전자지불과 관련된 문제점들은 대부분이 해결되었고 현재 프로토콜의 표준화, 어플리케이션 상에서의 통합 등의 과제가 남아있다.

인증기술은 거래 당사자간의 신뢰를 바탕으로 하는 전자상거래를 활성화하기 위해서 무엇보다 선결되어야 할 분야이다. 과거에 인증서버나 하드웨어 토큰을 이용한 인증방법에서 현재는 PKI를 기반으로 한 전자서명 기술과 인증서를 통해 인증이 이루어지고 있다. 그리고 향후 1~2년 뒤에는 스마트카드가 인증서와 더불어 사용자 인증을 위해 사용될 것이고 생체인식을 기반으로 하는 인증방법도 계속적인 연구를 거쳐 도입될 것이다.

실질적으로 정보의 전송이 이루어지는 네트워크는 방화벽이나 VPN 서비스를 이용한 보안이 주류를 이루고 있다. 그 중 VPN은 IPsec을 기반으로 하여 적은 비용으로 양질의 서비스와 보안기능을 제공하기 때문에 계속적인 발전이 기대되는 분야이다. 특히 우리나라가 보유한 CDMA나 ATM기술과 VPN의 연계가 차세대 VPN으로 이루어질 전망이므로 향후 인터넷 개발에 적극 참여하기 위해서 국내 VPN 기술의 확보가 필요하다.

지금까지 언급한 기술 이외에도 앞으로 안전한 전

자상거래를 위한 정보보호 기술은 다양하게 지속적으로 발전할 것이다. 이와 더불어 이러한 기술들을 적절하게 도입함으로 각각의 안전한 기술 스텝들로부터 안전한 전자상거래를 위한 과정을 만드는 방법에 대한 연구가 연계되어야 하며, 무엇보다도 사용자들의 안전성 위험과 문제들, 그리고 기존 솔루션들의 한계에 대한 충분한 인식이 필요하다.

※참고문헌

[1] American Internet User Survey, "E-commerce", http://www.cyberdialogue.com/resource/data/ecom/index.html#data, 1999.

[2] E-Business technology forecast, price-waterhouse-Coopers, 1999.

[3] L. Loeb, *Secure Electronic Transactions*, Artech House Publishers, 1998.

[4] S. Garfinkel, *Web Security & Commerce*, O Reilly, June, 1997.

[5] 이재일, "전자상거래의 인증체계 이해", 정보보호21C, pp34~40, Oct. 1999.

[6] A.Jain, L.Hong, S.Pankanti, "Biometric identification," Communications of The ACM, Vol.43, No 2, p. 90-98. Feb. 2000.

[7] 김상춘, 이종태, "안전한 전자상거래를 위한 정보보호 기술에 대한 연구," Nov. 1999.

[8] 정태명, "VPN의 현황과 발전동향," 정보보호21C, pp92~97, Oct. 1999.

[9] G. Laciste, "SEMPER: A security framework for the global electronic marketplace," IBM France, Aug. 1997.

[10] HP, "HP Plaesidium: Authorization server," white paper, Hewlett-Packard Co, 1998.

[11] M. Waidner, "Open issues in secure electronic commerce," IBM Research Report, Oct. 1998.

이 주 영

1997년 덕성여대 전산학과 졸업
1999년 연세대학교 컴퓨터과학과 석사
2000년~현재 전자통신연구원 연구원 재직
관심분야 : 전사상거래 보안, 정보보호기술

김 경 범

1981년 인하대학교 전자공학과 학사
1983년 인하대학교 대학원 전자공학과 석사
1983년~2000년 한국전자통신연구원 책임연구원
2000년~현재 (주)한국에이아이소프트 상무이사, 전자계산기 기술사
관심분야 : 정보보호, 전자상거래, 인터넷 비즈니스

손 승 원

1984년 경북대학교 전자공학과(공학사)
1994년 연세대학교 산업 대학원 전자공학과(공학석사)
1999년 충북대학교 대학원 전자공학과(공학박사)
1991년~현재 한국전자통신연구원 정보보호기술연구본부 정보보호응용연구부 부장/책임연구원
관심분야 : IC Card, Biometry, Network Security