The Journal of Korean
Institute of CALS/EC
Vol. 4, No. 2, September 1999

SET기반 전자상거래의 보안위협요소 분석 및 대응 방안에 관한 연구

김상균*, 강성호**

A Study on the Security Vulnerabilities and Defense Mechanism for SET-based Electronic Commerce

Sangkyun Kim, Sungho Kang

Abstract

In order to construct a successful electronic commerce system, three main essential factors must be satisfied to obtain the best effective outcomes. The three main essential factors are as follows : economic factor, effectiveness factor and convenient factor. In order to understand the role of these three factors, one must have some insight knowledge about security to assist him to implement these three factors in his construction of an electronic commerce system. This paper analyses a implementation mechanism of security systems based on the SET 1.0 standard for electronic commerce systems, thus providing an effective plan for the construction of a security system in the SET-based electronic commerce field. This paper helps to analyse the elements of security vulnerabilities in the SET 1.0 standard implementation and also helps to understand the SET 1.0 protocol.

Key Word : *SET-based Electronic Commerce, Security System, Security Vulnerabilities*

* 연세대학교 인지과학 산업시스템공학 전공
** 연세대학교 기계전자공학부

1. 서론

컴퓨터와 네트워크의 등장과 발전만큼이나 인간의 생활상에 있어서 단기간에 많은 변화를 가져온 요인도 드물다. 이러한 변화의 선상에서 근래 들어 가장 많은 화젯거리를 쏟아내고 있는 것이 전자상거래 시스템의 등장 및 발전 양상이다. 대부분의 변화 요소가 그렇듯이 전자상거래 시스템의 등장 또한 단순히 컴퓨터와 네트워크의 발전에 기인한 결과물은 아니다. 전자상거래 시스템의 등장은 인간 본연의 심리적 욕구, 기술적 발전, 인프라의 성장, 경제적 원리, 제도적 변화, 문화적 변화 및 신 산업의 창출 등 다각적인 요소가 복합적으로 작용하여 이루어진 결과물이다.

전자상거래에 대해서는 구구한 해석들이 존재하지만 가장 일반적인 것으로 받아들여지는 것은 북미의 AIAG(Automotive Industry Action Group)에서 언급한 것이다. AIAG는 전자상거래를 '거래 당사자간 비즈니스 관계의 효과성 증진을 위하여 진보된 정보기술의 지원을 받아 비즈니스 비전을 가능하게 하는 것'이라고 정의했다[Lynch, 1996]. 결국, 전자상거래의 대상은 상품의 선별, 상품 주문, 상품 인도 , 사후지원 및 대금지불 등 상거래 활동 일부 또는 전부를 포함한다[Wayner, 1997]. 이러한 전자상거래는 백화점이나 전문 상점에서 상품들을 판매하는 것처럼 인터넷이라는 가상공간에서 다양한 상품을 거래하는 사이버 쇼핑몰과 자동화된 국제간 거래인 사이버 무역, 사이버 대금 결제와 사이버 은행/증권과 같은 사이버 금융 및 사이버 광고/마케팅 등의 분야로 각각 구분할 수 있다. 이러한 분야 중에서 상업적으로 가장 활발하게 활용되고 있는 분야가 바로 사이버 쇼핑몰이고 이것이 본 논문에서 논하고자 하는 SET (Secure Electronic Transaction)가 포함하고 있는 전자상거래 시스템, 협의의 전자상거래 시스템이다.

SET기반의 전자상거래 시스템을 구현함에 있어 가장 큰 걸림돌로 작용하는 것이 SET시스템의 통신기반을 이루는 인터넷이 안고 있는 보안상의 문제점이다. 개방을 목표로 개발된 인터넷이 안고 있는 최대의 문제점인 보안상의 결함을(신용카드, 계좌번호, 비밀번호 등의 정보 누출 가능성) 뛰어넘어 고객이 안심하고 인터넷상의 지불 수단을 이용하여 상품을 구매하기 위해서 보안문제의 해결이 선결되어야 한다[Wayner, 1997].

본 논문에서는 전자상거래 시스템, 그 중에서도 근래 들어 경제성과 가용성 측면에서 최고의 시스템으로 시장에서 입지를 굳혀가고 있는 SET기반의 전자상거래 시스템에 대하여 파악하고, 본 시스템이 지니고 있는 보안상의 위협요소를 분석하며, 이에 대한 대응 메커니즘의 구현을 통한 시스템의 구축 및 활용방안을 제시하고자 한다.

2. SET 시스템에 대한 분석

2.1 SET의 역할 및 동작

2.1.1 SET의 개요

전자상거래에서 주요 위치를 차지할 각 이해집단은 새롭되 새롭지 않은, 다시 말해 기존 상거래 양식에서 크게 벗어나지 않은 전자상거래 양식을 선호하고 있다. 즉, 효용성을 중시하는 경제 원리에 충실한 전자상거래 시스템만이 새로운 시장에서 주도권을 잡을 수 있

다는 것이다. 이는 보안성이나 구축비용 및 운영비용 등에 대한 해결은 기본적이고 그러한 바탕 위에서 기존 상거래 양식의 단점을 보완한 형태의 가장 구태의연한 시스템이 승산이 있다는 것이다.

다기종 시스템간의 경쟁기간은 이와 같은 요건을 충족시켜줄 누군가를 기다려온 혼란기와 같았다. 그리고 이러한 혼란기를 청산하기 위하여 나타난 것이 바로 SET이다. SET의 탄생시기는 세계적인 신용카드 서비스 회사인 Visa사와 MasterCard사가 신용카드용 전자상거래의 공동 표준 개발을 발표한 1996년 2월 1일로 잡을 수 있다[http 5]. 발표 당시부터 GTE, IBM, Microsoft, Netscape Communications, SAIC, Terisa Systems, Verisign과 RSA Data Security와 같은 시스템 및 정보보안과 관련된 굴지의 기업들이 SET의 손을 들어주는 탄생에서부터 이미 그 성장 가능성은 예견되어 있었다. 이러한 탄생 배경을 살펴 볼 때 오늘날 각 상점에서 신용카드 단말기가 연결되어 있고, 해당 단말기를 통해 물품을 구매하는 것이 일반화된 것과 같은 양상으로, 조만간에 SET 기반의 전자상거래 시스템, 즉, 인터넷을 통해 물품을 검색하고, 전자지갑을 통해 신용카드를 사용하여 온라인으로 물품을 구매하는 상거래 양식이 보편화될 것은 자명한 것이다.

SET의 주요한 특징을 살펴보면 <표 1>과 같다.

SET은 전자상거래 시스템 보안의 필수요소인 정보의 기밀성, 결제 정보의 무결성, 카드 사용자의 인증 및 상점에 대한 인증, 상호 호환성에 대해서 보안성 및 안전성을 보장해 준다.

구체적으로 살펴보면 정보의 기밀성, 결제정보의 무결성, 카드 사용자의 인증 및 상점에 대한 인증부분에 대해서는 SET의 Business Description(버전 1.0)에서 제시하는 'Purpose of Secure Electronic Transaction'에서 나타나며, 마지막 부분인 상호 호환성은 'Market Acceptance'에서 제시한 '기본의 클라이언트 프로그램에 대하여 새로운 전자지불 기능을

<표 1> SET 프로토콜의 주요 특징

항 목	설 명
시스템의 구성 메카니즘	▷ 인터넷 신용카드 지불 시스템
주요 특징	▷ 개방형 프로토콜 표준 ▷ 모든 시스템 개발자들이 사용할 수 있음
익명성에 대한 보장	▷ 부분적으로 보장됨
부가적인 하드웨어	▷ 필요 없음
부가적인 소프트웨어	▷ 각각의 시스템공급자가 제공하는 Wallet소프트웨어 또는 하드웨어 사용
기타 요구사항	▷ 신용카드
제한사항	▷ 없음
암호화 방식	▷ 공개키 암호화 방식, 비밀키 암호화 방식 ▷ 전자 서명, 이중 서명, 인증

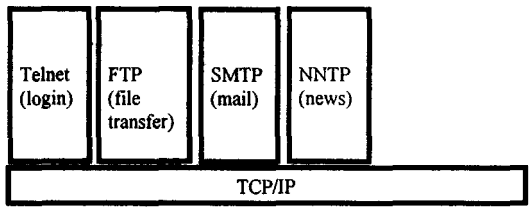
플러그인 할 수 있도록 한다.'라는 부분을 고려해보면 쉽게 알 수 있다[VISA, 1997-1] .

SET은 위와 같은 보안성의 확보를 위해 높은 비도를 보장해주는 공개키 암호화 방식, 비밀키 암호화 방식, 전자서명, 이중서명, 인증 등의 다양한 암호화 기법을 사용한다. 그러나 SET이 지닌 보안성의 의미는 단순히 암호화 알고리즘 자체가 지닌 높은 비도가 아니라 알고리즘을 운영하는 프로토콜의 결실성과 강력한 전자 서명 기법을 포함한 치밀한 보안 구조 설계에 기인한다. 또한 SET은 지역에서부터 시작해서 전세계적으로 커나갈 수 있는 CA의 모델을 제시해준다. 즉, 시스템의 적용 범위가 궁극적으로 전세계화 된다는 가정 하에서 시스템이 설계된 것이다. 익명성에 대해서 SET은 부분적인 보장만 해주고 있는데, 이는 SET이 기본적으로 실세계의 신용카드 시스템을 인터넷을 통하여 온라인화한 것이기 때문이다. 하지만, 개선된 부분도 존재한다. SET의 경우에는 거래정보를 다루는 상점과 금융기관에 대해서 상점의 경우에는 고객의 계좌정보를 은닉해주고 금융기관의 경우에는 고객의 구매정보를 은닉해준다.

SET에 대한 이해를 위해 가장 먼저 생각해 볼 문제는 무엇보다 SET의 역할에 대한 것이다. 간략하게 말하자면 SET은 전자상거래에 있어서 거래정보의 기밀성, 지불정보의 무결성, 상점과 카드소지자에 대한 인증의 세 가지 요소를 충족하는 것을 기본 역할로 하고 있다. 또한, 이러한 기본 요소를 바탕으로 경제성의 원리에 입각하여 소비자 및 서비스를 제공하는 상점이나 금융기관의 입장에서 가장 효율적인 방법으로 전자상거래 시스템을 구축, 운용하도록 하는 것이 SET의 목표이다[VISA, 1997-1].

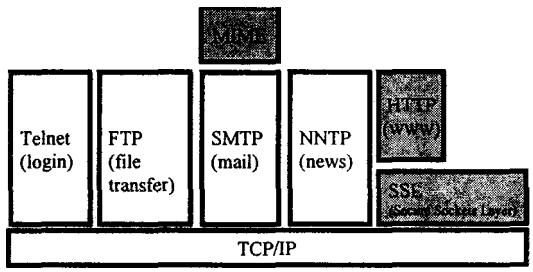
2.1.2 인터넷 프로토콜에 대한 SET의 위상

기존의 인터넷에 대한 고려를 배제하고 단순히 새로운 상거래 시스템의 등장이라는 측면도 물론 중요하지만, 기존의 인터넷 상 서비스 프로토콜로부터의 확장이라는 측면에서도 SET은 특별한 의미를 갖고 있다. 기존의 인터넷 프로토콜은 등장시기를 생각해 볼 경우 대략 <그림 1>과 같이 파악된다.



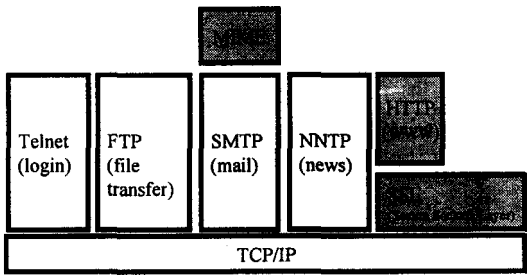
<그림 1> 인터넷 프로토콜의 초기구조

<그림 1>은 보안이라는 측면에 대한 고려가 전혀 개입되지 않은 것이다. 그러나 인터넷의 규모가 확대되면서 자연스럽게 보안에 대한 요구가 증대된 것은 당연스러운 것이고 그 결과 현재 대다수의 인터넷 사용자가 가장 친밀하게 느끼고 있는 <그림 2>와 같은 형태의 환경으로 그 프로토콜이 발전된 것이다.



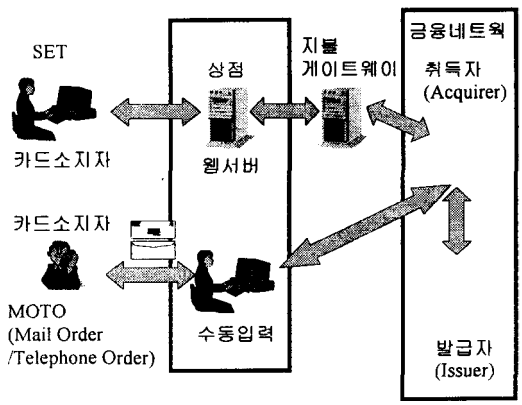
<그림 2> 보안기능이 추가된 인터넷 프로토콜의 구조

<그림 2>의 상황에서 SET은 많은 부분에서 독자적인 보안 메카니즘을 새롭게 구현했지만 기본적 기존의 SSL방식을 이용할 수 있도록 개발되었다. 이는 <그림 3>과 같이 파악된다.



<그림 3> 인터넷 프로토콜상에서 SET의 위상

MOTO(Mail Order/Telephone Order) 시스템과 비교할 경우 구매자와 상점과의 통신 및 상점과 금융기관간의 통신 방법에 인터넷을 도입하고 그것에 안전성을 부여한 것이라고 생각할 수 있다. 기존에 우편이나 전화를 통해서 물건을 주문하던 방식을 벗어나서 상점의 웹서버에 접속한 후 물품의 주문을 온라인으로 처리하는 것이고, 상점의 경우에는 구매요청에 따라서 기존의 폐쇄된 금융네트웍을 통해서 처리되던 이체처리를 지불게이트웨이를 통해서 처리하는 것으로 <그림 4>와 같은 형태로 볼 수 있는 것이다.



<그림 4> SET의 기본적 동작

2.1.3 SET의 의의

SET의 의의는 다음과 같다. 첫째, 표준화된 스펙상에서 시스템과 망을 구축하지 않았을 경우 발생하는 양 시스템간의 연동시의 재투자에 대한 부담을 제거하기 위해서이다. 둘째, 경쟁관계에 있는 양사간의 전략적 협업을 통해 새로운 비즈니스의 창출을 수월하게 하기 위함이다. 시스템에 대한 보안이라는 측면을 기본으로 하여서 위와 같은 사업적인 성과를 거두기 위하여 양업체가 가장 심혈을 기울인 부분이 바로 상호호환성의 문제이다. 이 부분에 대한 기본 방침은 이러하다.

첫째, SET에 대한 모든 스펙을 세부적으로 정형화된 형태로 공개하여 별개의 시스템 개발업체에 의해서 제작된 각각의 시스템간에 연동성을 확보한다. 둘째, 인터넷 상의 신용카드 거래 스펙에 대한 모든 자료를 무상으로 공개하며, 동시에 저작권에 대한 사용 제한을 두지 않는다. 셋째, SET과 관련된 제품의 수출이 규제되지 않도록 하여 SET의 국제적인 확산을 촉진한다. 넷째, 기존의 표준안들을 최대로 활용하여 기존에 존재하는 서브시스템에 대한 응용성을 극대화한다. 다섯째, 시스템의 운영체제와 하드웨어적인 특성에 의존하지 않도록 한다[http 2].

2.1.4 SET의 역할

일반적으로 전자상거래는 다음과 같은 아홉개의 프로세스로 나뉘어진다[VISA, 1997-2].

가. 물품검색 : 본 단계는 카드소지자가 물품에 대한 검색을 수행하는 단계이다. 인터넷을 통한 전자상거래에서 일반적으로 생각해 볼 수 있는 것처럼 웹브라우저를 통해서 수행하는 것도 가능할 것이고, 기존의 MOTO시스템에서와 마찬가지로 소책자형태의 물품카다록이나 물품정보가 담긴 CD-ROM 등을 통해서 검색하는 것도 가능하다.

나. 구매할 물품 선택 : 앞 단계의 검색을 통해서 단품단위로 자신이 구매할 물품을 선택하거나 또는 장바구니와 같은 개념을 통해서 자신이 구매할 물품의 군을 형성하는 과정이다.

다. 구매 요청 : 구매할 물품의 목록 및 단위가격과 전체가격, 운반비용 및 세금 등을 모두 포함한 주문서를 제시한다.

라. 지불방식 선택 : 상기의 구매요청에 대한 지불방식을 선택한다. SET스펙은 지불방식으로 구매자가 신용카드를 선택했을 경우에 적용된다.

마. 상점에게 구매와 지불에 대한 정보 전송 : 구매요청과 지불정보가 구매자에 의해 상점에게 전송된다. 구매 및 지불정보는 모두 인증을 득한 구매자에 의해 전자서명이 되어서 전달된다.

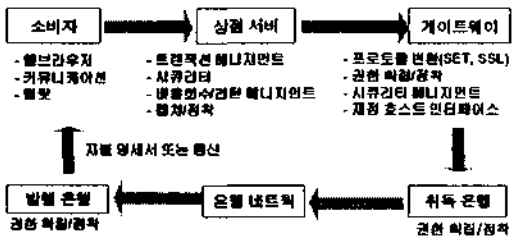
바. 카드에 대한 인증 : 구매자로부터 넘겨받은 정보를 바탕으로 상점은 구매자가 거래하는 금융기관에게 구매자에 대한 인증을 수행한다.

사. 구매 요청 승인 : 상기의 인증결과를 바탕으로 하여서 상점은 구매의뢰자에게 물품의 구매에 대한 확인을 해준다.

아. 물품의 배달 : 상점은 상기에서 확인된 결과에 따라서 구매자에게 해당하는 물품을 배달하거나 또는 서비스를 제공해준다.

자. 수금 : 상점은 구매자가 거래하는 금융기관을 통해서 물품대금을 수금한다.

상기와 같은 전자상거래의 프로세스 중 SET은 '마, 바, 사, 자'의 프로세스에 대해서만 관여한다. 이러한 상황도 구매자가 지불수단으로 신용카드를 선택했을 경우에만 해당하는 것이고 SET은 위의 프로세스 중 여타의 상황에 대해서는 개별적인 시스템 특성에 따라서 임의로 구성하도록 하고 있다. SET를 통한 구매의 프로세스는 <그림 5>와 같이 정리된다[통상산업부, 1997].



<그림 5> SET을 통한 상거래 프로세스

즉, SET은 다음의 사항들에 대해서는 관여하지 않는다[VISA, 1997-1].

가. 물품 검색과 배달에 요구되는 프로토콜 및 방식

나. 물품의 주문시 요구되는 주문서의 항목 및 세부양식

다. 신용카드를 제외한 방식의 지불방식

라. 금융기관들이 신용카드를 발급해주고 거래상점에 대한 신용을 승인하는 과정

마. 구매자, 상점, 지불게이트웨이 등의 시스템

에 저장되는 정보에 대한 보호

바. 구매자, 상점, 지불게이트웨이 등의 시스템에 대한 해킹방지 대책

2.2 SET의 구성요소 및 메커니즘

SET의 전자상거래 운용환경은 시스템 측면에서 다음과 같은 컴포넌트들로 구성되어 있다[VISA, 1997-1] .

가. 카드소지자(구매자) : 카드사에 의해서 카드를 발급 받은 구매자로서 인증기관을 통해서 거래 승인을 득한 사람을 의미한다.

나. 상점(서비스 제공자) : 유형의 물품을 판매하거나 또는 특정 정보(예, 주식거래, 논문정보 등) 및 특정 서비스(예, 온라인 컨설팅, VOD 서비스 등) 등을 일정 금액의 대가를 받고 판매 또는 제공하는 업체를 의미한다.

다. 발행은행 : 개개의 카드소지자에게 카드를 발급해주는 기관을 의미한다.

라. 취득은행 : 상점으로 유입되는 구매관련 지불정보를 취합하여 처리해주는 금융기관을 의미한다.

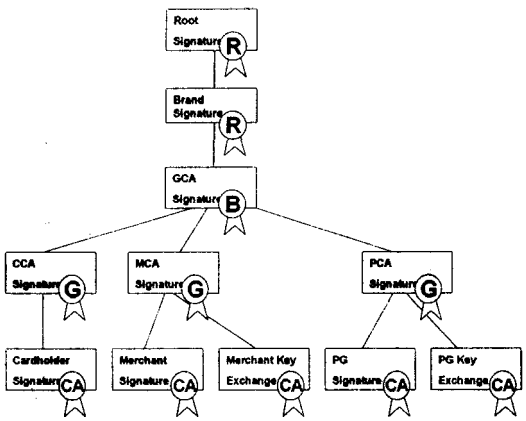
마. 지불게이트웨이 : 취득기관을 지원하여 상점들에게 전자상거래 서비스를 제공해주는 기관으로서 취득기관에게 이체 처리내역에 대한 인증을 수행한다.

바. 신용카드회사 : 하나의 통합적인 전자상거래 서비스를 제공하는 신용카드 기관

사. CA(인증기관) : 하나의 신용카드회사나 복수의 신용카드회사에 대해서 각각의 카드소지자, 상점 및 지불게이트웨이에 대한 인증을 생성하고 분배해주는 관리기관

여기서 우리가 주의 깊게 살펴볼 것은 CA에 대한 것이다. 다른 시스템은 동일 선상에서 여타의 시스템과 연동되는 반면에 CA는 수직적인 관리체제를 통해서 각각의 CA가 관리되는 모습을 갖고 있다. 이렇듯 구성한 이유는 SET에서 가장 핵심적으로 준수되어야 할 것이 보안에 대한 사항이고 또한 보안에 대해서 주도적인 책임이 바로 CA에 주어지기 때문이다.

CA는 최상단의 루트CA에서 부터 시작하여 맨 하단의 CCA(Cardholder CA), MCA (Merchant CA), PCA(Payment Gateway CA) 까지 다단계의 구조를 가진다. 루트CA는 스스로 자신을 인증함과 동시에 하단의 신용카드사에 대한 인증을 수행해준다. 루트CA로 부터 인증된 신용카드사(Brand CA)는 하단의 지역 CA(Brand Geo-political CA)에 대한 인증을 수행해주고 지역 CA는 일정지역내에 존재하는 CCA, MCA, PCA에 대한 인증을 수행해준다. CCA는 카드소지자에 대한 인증을 수행해주며, MCA는 상점들에 대한 인증을 수행하고 PCA는 지불게이트웨이에 대한 인증을 수행한다. 즉, 이와 같은 복잡한 연결고리를 통해 체계적인 보안성을 유지한다. CA는 <그림 6>과 같은 형태의 수직구조로 관리된다[VISA, 1997-2] .



<그림 6> CA의 구성 체계

상기와 같은 구조상에서 SET에서 처리되는 인증 방식은 <표 2>와 같이 정리된다.

<표 2> SET의 구성요소별 인증방식

인증대상	전자 서명	키 암호화	인증, CRL 서명
카드소지자	*		
상점	*	*	
지불게이트웨이	*	*	
카드소지자CA	*	*	*
상점CA	*	*	*
지불게이트웨이CA	*	*	*
신용카드사의 지역CA	*		*
신용카드사CA			*
루트CA			*

3. 보안 위협요소의 분석

3.1 SET스펙 자체의 보안 위협 요소

SET는 근본적으로 SET자체의 목표설정이라는 부분에서 실세계의 시스템에 적용시 보안상의 위협요소로 작용할 수 있는 몇가지 문제점들을 안고 있다. 첫째, SET스펙을 살펴보면 SET와 주변 시스템의 연계성을 프로토콜에 대한 부분만으로 한정짓고 있다. 프로토콜이란 말의 의미자체가 일종의 통신규약일 뿐이라는 데서 문제가 발생한다. 이는 즉, 통신중에 생기는 여러 문제점에 대해서는 SET이 암호화를 기반으로한 방법들을 통해서 문제를 해결하지만, 트랜잭션을 처리하는 다수의 시스템 자체에서 발생할 수 있는 시스템 레벨의 공격에 대해서는 별다른 대안책을 제시하고 있지 못하다는 것이다. 결국, 프로토콜에 대한 표준안만을 제시하는 것보다는 일종의 스펙으로서 프로토콜을 포함함과 동시에 시스템 레벨의 공격방법에 대한 대비책과 함께 포용하는 것이 좋을 것이다. 결과적으로 SET가 지향하는 프로토콜이 지니는 본질적 특성상 보안상의 문제점이 위협요인으로 작용한다. 둘째, SET는 개발업체와 서비스제공자들에게 표준화된 규격을 제시하고 있는 것이 사실이다. 반면, SET는 통신 부분을 제외한 시스템 레벨의 구현 및 운용에 대해서는 어떠한 규격도 제시하고 있지 않다. 실제로 소프트웨어 개발업체들이 통신부분에 대한 표준안만을 가지고 표준화된 제품을 만든다는 것은 매우 어려운 일이다. 클라이언트레벨의 보안 메커니즘에 대해서 스펙에서 규정하지 않고있는 문제로 인하여 소프트웨어 제조업체별로 사용방식이나 내

부 메커니즘이 매우 상이한 형태의 클라이언트 모듈이 등장하게 될 것이다. 물론, 이러한 부분에서 제조업체 마다 서로 상이한 특징을 갖게될 것이고, 이것이 제품을 차별화 시킬 수 있는 요소가 되겠지만, 이러한 부분에서 카드소지자, 시스템 도입업체 또는 기관이 잘못된 제품을 선택하여 운용하게 될 경우에는 심각한 보안위협이 잠재된 전자상거래 시스템이 구현될 수 밖에 없다.

SET는 시장에 대한 조속한 확장을 위하여 모든 소프트웨어, 시스템 제조 및 공급업체가 동일선상에서 SET관련 시스템의 구현에 접근할 수 있도록 특정 단위 시스템에 대해서는 규약화를 배제하고 있다. 이러한 접근방식의 근본취지는 모든 제조업체가 동등한 조건에서 관련 제품의 상품화에 접근할 수 있도록 하려는 것이지만, 이로 인하여 세부적으로 정의되지 않은 단위 시스템의 규격에 대하여 각각의 제조업체가 독자적인 방식으로 시스템을 구현하는 과정에서 보안상의 위협요소가 발생한다. 첫째, SET는 근본적으로 개방을 목적으로 하고 있다. 즉, 규약정립의 주체에 의해 정립된 모든 규격 내용을 소프트웨어와 시스템 개발업체에게 철저히 공개하고 있다. 이를 통해 실용화, 상용화된 시스템이 조속히 나올 수 있도록 하기 위함이다. 하지만, 이부분에서 문제가 발생한다. SET스펙을 수용한 시스템을 상용화하는데 있어, 실제 개발과정을 생각해 볼 때 Point-to-Point에 대한 시스템 설계방침 뿐만 아니라, End-to-End 형태의 시스템에 대한 설계방침 또한 요구된다. 그러나, SET의 경우는 규약정립의 주체가 민간기업인 상태에서 규격 내용을 정립하는 과정에서 End-to-End형태의 시스템 개발업체의 손을 들어주는 형상이 될 수 있다는 우려 때문에 Point-to-Point에 대한 시스템 설계방침만을 제시하고 있다[VISA, 1997-1] . 결국 이 부분에 대한 스펙 또는 규약이 명확시 되지 않은 상태에서 여러 제조업체로부터 시스템들이 독자적으로 개발될 경우에는 제조업체가 상이한 시스템간의 상호 연동시 현재 스펙에서 표방하는 것 이상으로 추가적인 비용과 작업이 소요될 것이다. 물론, 이부분에서 상호호환성 테스트가 지속적으로 이루어지고 있기는 하지만 아직까지는 많은 문제점이 남아있는 것으로 파악되며, 이 부분에 대한 문제점을 해결하고자 단순한 메커니즘으로 해당 시스템을 구현할 경우 보안상에 치명적인 위협요소가 발생한다. 둘째, 상대방의 정보를 인증하는 과정에서 SET는 일반 카드소지자의 경우도 해당자가 소유하고 있는 전자지갑이 SET에서 규정한 정확한 메커니즘을 통해 연산을 수행하고 결과치를 나타낸다고 가정하고 있다. 즉, 메커니즘자체에 대한 무결성의 보장에 대한 메커니즘은 존재하지 않는다. 이는 통신의 양주체가 사용하는 클라이언트 소프트웨어가 변조되지 않았다는 가정하에서만 성립되는 것이다. 따라서, 보안상의 문제점을 생각해본다면 클라이언트 소프트웨어가 자체적으로 변조에 대한 방지책을 갖고 있어야만 한다.

SET는 규약의 범위 설정에 따른 문제점을 알고 있다. 첫째, SET는 전송되는 데이터의 기밀성 보장에 대한 메커니즘에 대해서만 규약하고 있다[VISA, 1997-2] . 하지만, 스펙자체가 전송에 대해서만 기밀성을 보장해준다는 것은 실제로 운영되는 시스템을 놓고 생각해 볼 때 매우 위험스런 일이다. 즉, 데이터가 전송되는 송수신 시스템 자체에 대한 정보보안

이 요구된다. 일 예로 송수신 시스템에 대한 침입차단 시스템, DB접근 제어 시스템 및 서버 측에 대한 관리자 인증 시스템 등이 필수적으로 요청된다. 둘째, SET는 기본적으로 프로토콜을 위한 스펙이다[VISA, 1997-1] . 따라서, 실질적인 시스템의 구현에 대한 부분은 규약의 범위에서 배제되어 있다. 즉, 시스템의 설계 기술과 그에 대한 검증에 대한 부분은 제외되어 있다. 이러한 부분이 일반적인 시스템공학의 범주와 선진국을 중심으로 시행되고 있는 시스템에 대한 보안성 평가 및 인증제도 등을 통해 상당부분 해결되기는 하지만, SET을 위해 소요되는 단위시스템들이 기존의 소프트웨어, 시스템과 메커니즘적으로 차별화된 요소가 많다는 점을 고려해 볼 때 이러한 부분에서 SET가 규약화를 배제하고 있다는 것이 보안상의 위협요소로 작용된다. 셋째, SET는 지역의 단위 시스템 공격에 대한 대응 메커니즘을 제시하고 있지 않다[VISA, 1997-2]. 즉, 지역의 단위 시스템 상에서 카드번호, 만기일 및 비밀번호 등의 정보보안에 대한 방안이 요구될 것이다. 넷째, 상대측 시스템과 통신을 수행하기 위해서 SET의 단위 시스템은 자체적으로 비밀키를 생성한다[VISA, 1997-2]. SET에서는 생성된 비밀키의 적용방식에 대해서만 규약화 되어 있다. 즉, 비밀키를 생성하는 과정에서 생길 수 있는 문제점과 생성된 키가 시스템내부에서 처리되는 과정에서 발생할 수 있는 도청공격 등에 대해서는 대응 메커니즘이 제공되고 있지 못하다. 이 경우 단위 시스템에 설치된 TSR형태의 도청 소프트웨어에 의해서 해당정보가 쉽게 도청되고 악용될 수 있다. 따라서, 단위 시스템에 대해서 TSR 프로그램을 통한 공격에 방어할 수 있는 대비책이 요구된다. 그렇지 못할 경우 비밀키의 생성과정에 대해서 보안성이 확보된다해도 시스템 상에 저장된 정보가 저장매체에서 읽어들여지는 과정에서 TSR프로그램을 통해 간단하게 도청될 수 있다. 다섯째, 앞서 언급한 것과 유사한 문제점으로 공개키와 개인키의 생성과 응용에도 보안상의 문제점에 대한 대응 메커니즘은 제시하고 있지 못하다[VISA, 1997-2]

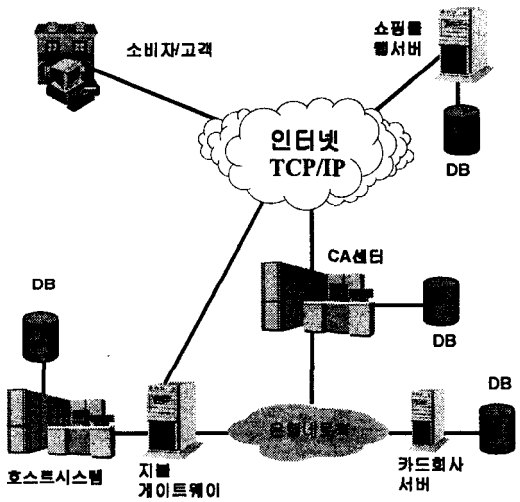
이 부분에서도 역시 두 개의 키쌍에 대한 보안대책이 확보되지 못하고 있다. 이는 앞서 언급한 것과 유사한 공격법을 통해 키가 유출된 경우 전송정보 및 인가자에 대한 위변조가 발생할 소지가 있다. 여섯째, 카드소지자는 본인의 단말기에 일반 제조업체를 통해 배포된 전자지갑 소프트웨어를 통해 신용카드 번호, 카드 말소일과 비밀번호를 포함한 각종정보를 CCA의 요청에 의해 입력하게 된다[VISA, 1997-2]. 하지만, 이 경우에 대해서도 클라이언트 레벨의 RAM버퍼 스누핑, 키보드버퍼 스캔, 가상메모리 스누핑 등의 공격법에 대한 대응 메커니즘이 정립되어 있지 못하다. 따라서, 침해자에 의해서 상기의 정보가 도청될 경우 위변조와 연결될 수 있는 보안상의 위협요소가 존재한다.

3.2 시스템 구성상의 보안위협요소

앞장에서 기술한 내용들을 바탕으로 SET 전자상거래의 전체 시스템을 구성하면 <그림 7>과 같다.

SET스펙은 인터넷상의 트랜잭션에 대한 보안성만을 확보해주는 것이다. 따라서, SET 기반의 인터넷 전자상거래 시스템 상에서는 SET이 보호해주는 인터넷기반 트랜잭션 처리

부분을 제외한 부분들에서 보안상의 위협요소가 발생한다. 소비자 또는 고객이 사용하는 시스템에 대한 보안위협은 크게 전자지갑 프로그램의 비밀번호 유출, 거래내역 저장정보에 대한 참조, 위변조 및 시스템 설정 정보에 대한 위변조 위협의 세 가지로 나뉘어진다.



<그림 7> SET기반의 전자상거래 시스템 구성도

첫째, 전자지갑 프로그램의 비밀번호 유출 위협은 키보드 스니핑 공격, 트래이 목마를 통한 침투 및 TSR형태의 감시 프로그램 작동을 통해서 발생할 수 있는 문제점이다. 둘째, 거래내역 저장정보에 대한 참조 및 위변조 위협은 트래이 목마를 통한 침투, TSR형태의 감시 프로그램 작동 및 저장정보에 대한 불법적 위변조를 통해서 발생할 수 있는 문제점이다. 셋째, 시스템 설정정보에 대한 위변조 위협은 트래이 목마를 통한 침투와 설정정보에 대한 불법적 위변조를 통해서 발생할 수 있는 문제점이다.

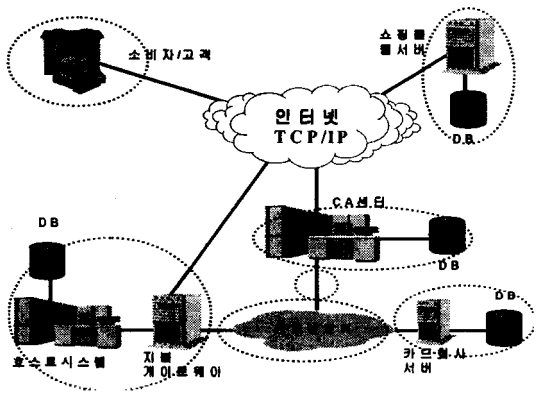
상점의 서버 및 DB에 대한 보안위협은 크게 상점서버에 대한 파괴, 상점서버에 대한 임의적 오동작 유도 위협 및 상점 서버내부의 DB에 저장된 고객, 거래 내역 정보에 대한 참조 및 위변조 위협의 세 가지로 나뉘어진다. 첫째, 상점서버에 대한 파괴 위협은 시스템 정지와 시스템의 성능저하를 목적으로한 공격행위에 의해 발생할 수 있다. 둘째, 상점서버에 대한 임의적 오동작 유도 위협은 소비자, 고객에 대한 거래거부와 물품 또는 서비스 정보에 대한 파괴 및 변조를 목적으로한 공격행위에 의해 발생할 수 있다. 셋째, 상점 서버내부의 DB에 저장된 고객 및 거래내역 정보에 대한 참조, 위변조 위협은 소비자, 고객 정보에 대한 불법적 참조와 거래내역에 대한 참조, 임의적 위변조를 목적으로한 공격행위에 의해 발생할 수 있다.

은행의 지불게이트웨이 및 DB에 대한 보안위협은 크게 지불게이트웨이에 대한 파괴위협, 지불게이트웨이에 대한 임의적 오동작 유도 위협 및 지불게이트웨이 DB에 저장된 거래정보에 대한 참조, 위변조 위협의 세 가지로 나뉘어진다. 첫째, 지불게이트웨이에 대한 파괴 위협은 지불게이트웨이 정지, 지불게이트웨이의 성능 저하를 목적으로한 공격행위에 의해 발생할 수 있다. 둘째, 지불게이트웨이에 대한 임의적 오동작 유도 위협은 CA, 상점서버 또는 카드회사와의 통신 불능 유도를 통해 발생할 수 있다. 셋째, 지불게이트웨이 DB에 저장된 거래정보에 대한 참조 및 위변조 위협은 거래내역 정보에 대한 임의적 위변조를 통한 거래내역 삭제, 추가를 통해 발생할 수 있다.

카드회사의 서버 및 DB에 대한 보안위협은 카드회사의 서버에 대한 파괴 위협, 카드회사의 서버에 대한 임의적 오동작 유도 위협 및 카드회사의 서버 DB에 저장된 승인 및 지불정보에 대한 참조, 위변조 위협의 세 가지로 나뉘어진다. 첫째, 카드회사의 서버에 대한 파괴 위협은 카드회사 서버의 정지, 카드회사 서버의 성능 저하를 목적으로한 공격행위에 의해 발생할 수 있다. 둘째, 카드회사의 서버에 대한 임의적 오동작 유도 위협은 지불게이트웨이와의 통신 불능 유도를 목적으로한 공격행위에 의해 발생할 수 있다. 셋째, 카드회사의 서버 DB에 저장된 승인 및 지불정보에 대한 참조 및 위변조 위협은 거래자 정보에 대한 불법적 참조를 통한 신용내역의 위장사용과 거래내역 정보에 대한 임의적 위변조를 통한 거래내역 삭제 및 추가를 통해 발생할 수 있다.

인증센터의 서버 및 DB에 대한 보안위협은 인증센터의 서버에 대한 파괴 위협, 인증센터의 서버에 대한 임의적 오동작 유도 위협 및 인증센터의 서버 DB에 저장된 인증정보에 대한 참조, 위변조 위협의 세 가지로 나뉘어진다. 첫째, 인증센터의 서버에 대한 파괴 위협은 인증센터 서버의 정지와 인증센터 서버의 성능 저하를 목적으로한 공격행위에 의해 발생할 수 있다. 둘째, 인증센터의 서버에 대한 임의적 오동작 유도 위협은 상점서버 또는 지불게이트웨이와의 통신불능 유도를 목적으로 한 공격행위에 의해 발생할 수 있다. 셋째, 인증센터의 서버 DB에 저장된 인증정보에 대한 참조 및 위변조 위협은 인증 정보에 대한 불법적 참조를 통한 신용내역의 위장사용과 인증 정보의 위변조를 통한 허위의 상점, 지불게이트웨이 및 카드회사 서버의 상점을 통해 발생할 수 있다.

은행네트워크의 통신에 대한 보안위협으로 대표적인 것이 통신내역에 대한 불법적 도청 행위이다. 이를 통해서 공격자, 침해자는 시스템 구성도상에서 앞서 분류된 보안위협요소를 바탕으로 SET스펙을 통해 보안성이 확보된 부분과 보안위협요소가 존재하는 부분을 분류하면 <그림 8>과 같다.



<그림 8> SET기반의 전자상거래 시스템에 대한 보안위협요소

지불게이트웨이와 카드회사간의 통신내역 도청을 통하여 개인 신용정보를 불법적으로 획득하고자 한다. <그림 7>에서 제시한 본 구성도에서 점선으로 표시된 부분은 SET스펙 자체만으로 보안위협요소가 제거되지 못한 부분 즉, 보안상의 위험성이 존재하는 부분이고, 그외의 부분은 보안위협요소가 SET스펙에 의하여 제거된 부분 즉, 안전한 부분이다.

4. 보안시스템의 구축 방안

4.1 단위 보안 시스템의 설계

<그림 8>에서 제시된 것과 같은 각각의 시스템 또는 네트웍이 갖고 있는 보안상의 문제점을 해결하기 위해서는 <표 3>과 같은 단위시스템들이 소요된다. 각각의 시스템에 대한 기능은 다음과 같다.

<표 3> SET보안을 위한 단위 시스템

시스템명	기 능
보안감사 시스템	서버 및 클라이언트 시스템에 존재하는 OS, 네트웍 및 어플리케이션상의 보안 취약성 또는 문제점을 자동으로 진단 및 보고해주는 시스템[ISS, 1997]
침입탐지 시스템	외부망에 존재하는 불법적 침입자에 의한 서버시스템 침입 시도 또는 침입내역을 자동으로 감지, 시스템 관리자에게 통보 및 대응해주는 시스템[http 3]
개인단말 보안 시스템	클라이언트시스템의 보안성을 확보해주는 프로그램. 기억장치에 대한 스푸핑 방지, 키보드 스캔방지, 비밀번호 덤프 방지, 기밀정보 암호화/복호화, 시스템에 대한 일시잠금, 시스템에 대한 무결성 점검 등의 기능을 보유[http 1]
침입차단 시스템	서버시스템에 대한 공격행위, 제한된 서비스 또는 시스템에 대한 불법적 접근 등을 방지해주고 해당내역을 저장 및 통보해주는 시스템[http 6]
암호화 통신 시스템	주요 서버간의 모든 통신 내역을 자동으로 암호화/복호화하여 주는 시스템[Atkins, 1996]
DB보안 시스템	DB에 대한 접근제어 및 DB에 저장된 내역에 대한 무결성과 기밀성을 유지해주는 시스템[http 4]

4.1.1 보안감사 시스템

보안감사 시스템은 서버시스템에 존재하는 보안 결함 요인들을 자동으로 점검해주며 이에 대한 해결책을 DB에 기초하여 제시해 줄 수 있어야 한다. 또한, 점검 내역과 제시된 해결책에 대하여 가용성이 뛰어난 리포팅 기능이 제공되어야 한다[ISS, 1997].

4.1.2 침입탐지 시스템

침입탐지 시스템은 일반적으로 침입자에 대한 실시간 탐지기능, 침입자 발생시 해당 사항을 관리자에게 즉각 알릴 수 있는 통보기능, 감시내역을 자동으로 저장하여 사후관리에 활용할 수 있는 기능 및 내부 시스템의 접근 내역에 대한 실시간 감시기능이 포함되어야 한다[http 3].

침입탐지 시스템은 다음과 같은 주요 기능 요소를 포함해야 한다. 첫째, 침입자에 대한 실시간 탐지기능은 세분화된 침입패턴 DB를 보유하고 이를 통해서 침입패턴에 대한 자동화된 감지가 구현되어야 한다. 둘째, 침입자 발생시 해당 사항을 관리자에게 즉각 통보할 수 있는 기능은 호출기 및 전자우편을 통하여 통보와 경보메시지를 전할 수 있어야 한다. 셋째, 감시내역을 자동으로 저장하여 사후관리에 활용할 수 있는 기능은 로깅내역에 대한 백업을 지원하고 로깅내역에 대한 자동요약 및 선택적 출력기능을 포함해야 한다. 넷째, 내부시스템에 대한 접근 내역을 실시간으로 감시하는 기능은 현재 내부시스템에 연결된 전체 커넥션에 대해서 문자와 그림정보 형태로 각종 요소에 의해서 자동정리 및 통계화가 가능해야 한다.

침입탐지 시스템은 침입분석기와 침입탐지기의 이원화된 구조로 설계된다. 침입분석기는 침입탐지기를 통해 수집된 패킷 정보를 바탕으로 침입여부를 판단하고 그에 대한 대응을 수행하는 서버 프로그램, 특정한 경우를 제외하고 한 대만 설치되도록 한다. 침입탐지기는 각각의 호스트에 탑재되어 호스트에 송수신되는 패킷을 수집하여 침입분석기에게 보내주는 에이전트 프로그램으로 보호하려는 내부 호스트의 수에 따라서 각각의 호스트마다 설치되도록 한다.

침입탐지 시스템은 앞서 언급한 내역을 바탕으로 200여가지 이상의 기본적 침입패턴에 대한 탐지, 인공지능 및 신경회로망을 응용한 하이브리드 형태의 침입탐지, 관리자에 대한 암호화 인증 기능, 시스템에 대한 보안관리 기능 및 네트웍 사용 내역에 대한 감사기록, 관리 기능 등이 요구된다.

4.1.3 개인단말 보안 시스템

개인단말의 보안을 위한 시스템은 다양하고 강력한 암호화 알고리즘을 통한 PC정보보안 기능과 거래내역 정보에 대한 참조 및 위변조를 방지할 수 있는 기능, TSR형태의 도청공격에 대한 대응 기능을 포함해야 한다. 이를 위해서 개인 및 그룹 단위의 파일 암/ 복호화 기능, 키보드 스누핑 방지 기능, 무결성 점검 기능 및 시스템 잠금 기능 등이 포함되어야 한다.

4.1.4 침입차단 시스템

침입차단 시스템은 기본적으로 다음과 같은 설계 사상을 바탕으로 구현되어야 한다. 첫째, 침입차단 시스템은 사용자의 계정정보, 시스템의 신분정보 및 보안레이블에 기초한 정보들을 바탕으로한 접근제어 기능을 포함해야 한다[정보통신부, 1998]. 둘째, 시스템의 관리자에 대한 강력한 암호화 인증 기능을 포함해야 한다. 이를 통해 위급 상황 발생시 시스템의 원격관리가 지원될 수 있어야 한다[정보통신부, 1998]. 셋째, 다양한 해킹기법에 대한 대응 메커니즘이 내부적으로 포함되어 있어야 한다[Atkins, 1996].

4.1.5 암호화 통신 시스템

암호화 통신 시스템은 내부적으로 크게 키관리 기능과 암/복호화 기능의 두가지로 나뉘어 진다. 첫째, 키관리 기능은 암/복호화에 소요되는 비밀키를 자동으로 생성, 분배, 저장 및 파기할 수 있는 메커니즘을 확보하고 있어야 하며, 이러한 메커니즘은 자체적으로도 내부적 처리과정에 대한 보안

성을 가져야 한다. 둘째, 암/복호화 기능은 키관리 기능을 통해 생성된 비밀키를 통해서 대량의 데이터를 고속으로 암/복호화 할 수 있는 기능을 의미하는 것으로, 높은 비도의 암호화 알고리즘을 다양하게 지원할 수 있도록 시스템이 구축되어야 한다.

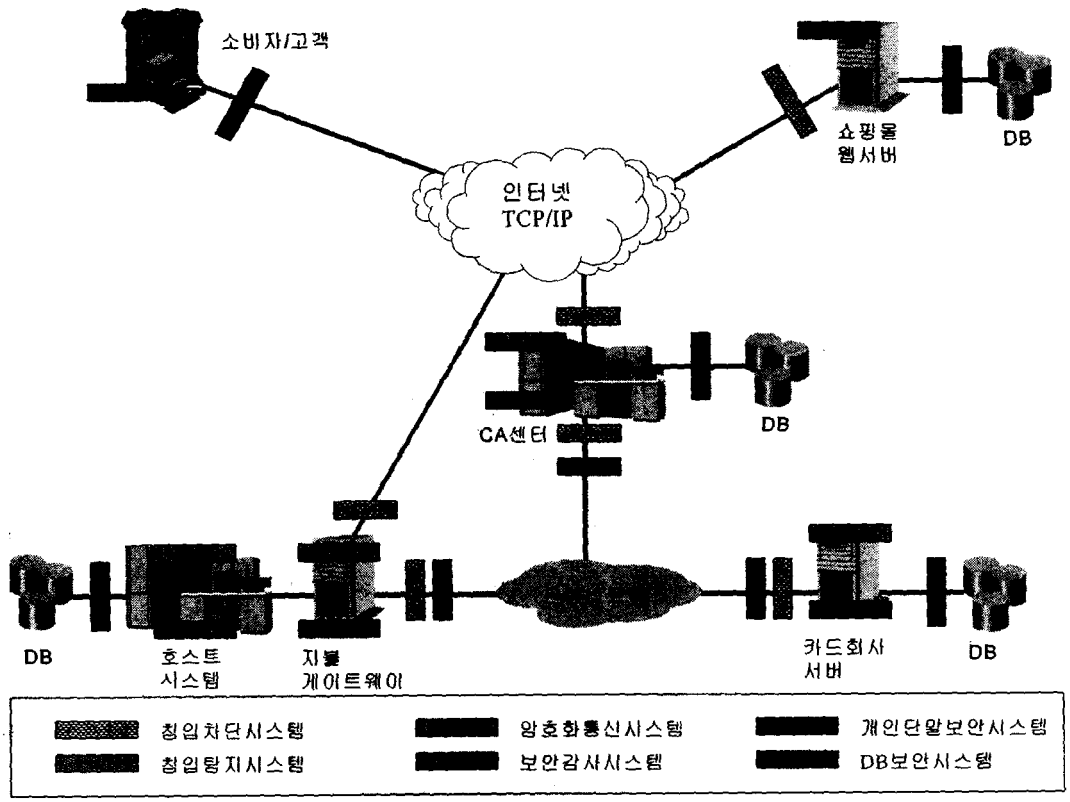
4.2 전체적 보안 시스템의 구축

앞장에서 분석한 보안위협요소에 대해서 앞절에서 제시한 단위 보안 시스템의 구성요소를 바탕으로 제시한 보안위협에 대한 대응 메커니즘은 <표 4>와 같다.

<표 4> SET보안위협요소에 대한 대응 메커니즘의 구성

보안위협요소 \ 보안메카니즘 구성요소		보안감사 시스템	침입탐지 시스템	개인단말 보안 시스템	침입차단 시스템	암호화 통신 시스템	DB 보안 시스템
소비자, 고객의 시스템	전자지갑 프로그램의 비밀번호 유출			●			
	거래내역 저장정보에 대한 참조 및 위변조	●					
	시스템 설정정보에 대한 위변조	●		●			
상점의 서버 및 DB	상점서버에 대한 파괴		●		●		
	상점서버에 대한 오동작 유도	●	●		●		
	DB에 저장된 고객, 거래내역 정보에 대한 참조 및 위변조				●		●
은행의 지불 게이트 웨이 및 DB	지불게이트웨이 파괴		●		●		
	지불게이트웨이 오동작 유도	●	●		●		
	거래정보에 대한 참조 및 위변조				●		●
카드 회사의 서버 및 DB	카드회사의 서버에 대한 파괴		●		●		
	카드회사의 서버 오동작 유도	●	●		●		
	승인 및 지불정보에 대한 참조 및 위변조				●		●
인증센터의 서버 및 DB	인증센터의 서버 파괴		●		●		
	인증센터의 서버 오동작 유도	●	●		●		
	인증정보에 대한 참조 및 위변조				●		●
은행 네트워크	통신내역에 대한 도청	●				●	

<그림 7>에서 제시한 SET전자상거래의 기본적 구성에 대하여 <표 4>에서 제시한 보안 메커니즘을 반영하면 <그림 9>와 같은 시스템이 구축된다.



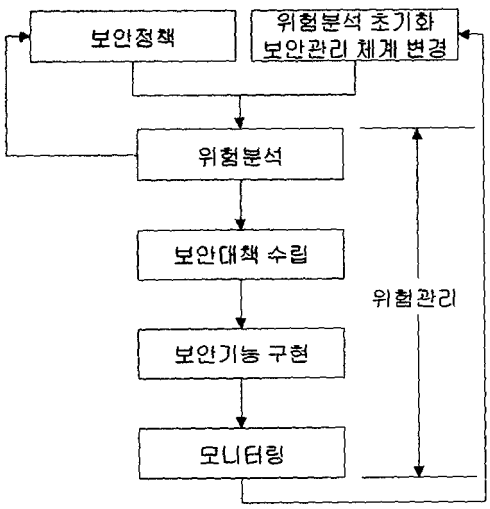
<그림 9> SET기반 전자상거래를 위한 보안 시스템의 구축도

5. 보안시스템 관리 및 운영 방안

5.1 전체적 관리 및 운영 방안

5.1.1 보안관리의 개념

보안시스템 관리의 목적은 여러 위협으로부터 자산을 보호하며 안정된 서비스를 제공할 수 있도록 하는 것이다. <그림 10>은 보안시스템 관리의 흐름을 나타낸 것이다.



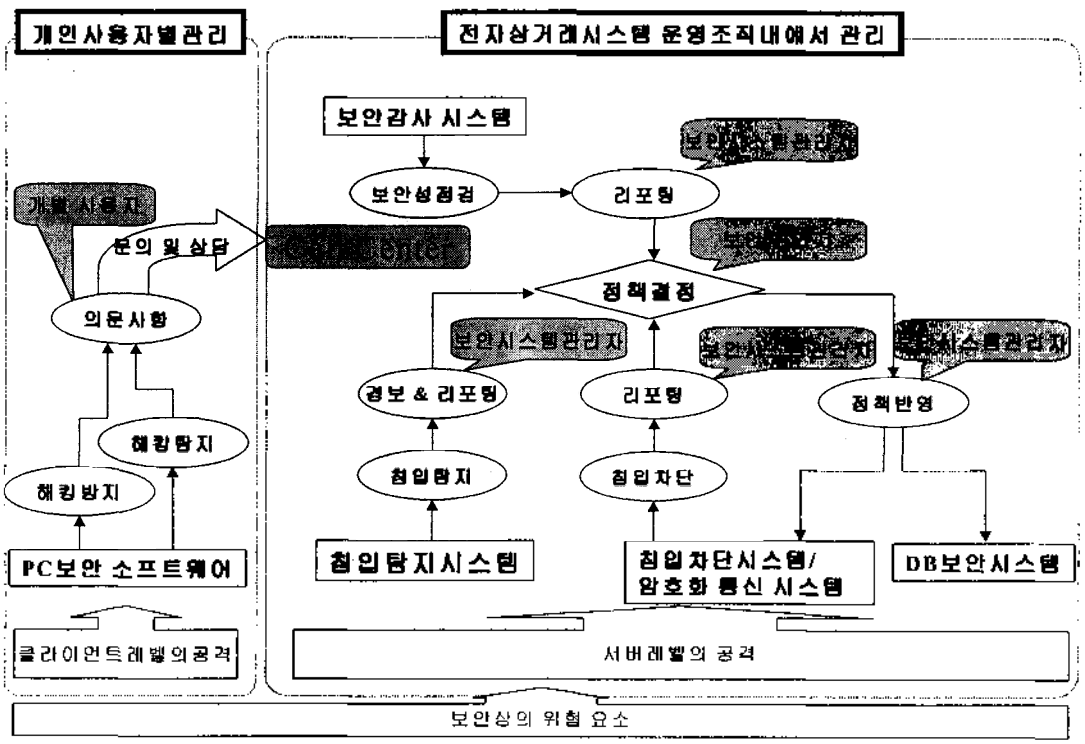
<그림 10> 보안시스템 관리의 흐름

이에 따른 보안관리의 구성요소는 다음과 같다.

가. 위험분석 : 시스템의 위험정도를 평가한다.
나. 보안정책 : 보안관리의 기본방향, 범위 및 보안 목표 수준을 규정한다.
다. 보안대책수립 : 보안수준 향상을 위한 대책을 수립한다.
라. 보안기능구현 : 보안기능을 설정, 구현한다.
마. 감사 및 모니터링 : 보안기능이 추가된 상태의 시스템 보안상황을 모니터링한다.
바. 보안사고 응급조치 : 보안사고의 응급조치는 <그림 10>의 흐름도에는 명기되어 있지 않다. 이는 응급상황 발생시 보안시스템 관리를 담당하는 모든 관련자가 소집되어 해당되는 문제점을 최단시간내에 해결하고 대응할 수 있도록 하는 절차를 의미한다.

5.1.2 전체적 관리 방안의 수립

5.1.1에서 살펴본 보안관리의 개념을 통하여, 3장에서 제시한 SET기반의 전자상거래 시스템에 대한 보안 시스템의 전체적 관리는 <그림 11>과 같이 도식화 할 수 있다. 즉, 5.1.1에서 살펴본 기본 개념을 바탕으로 위험에 대한 분석과 초기정책의 설정 및 보안기능 구현은 본 논문에서 제시한 방법론을 따른다. 일단 시스템이 가동에 들어가면 각각의 단위시스템에서 제공되는 리포팅 기능과 보안감사 시스템



<그림 11> SET기반 전자상거래를 위한 보안 시스템의 전체적 관리 방안

의 감사기능을 통해 감사 및 모니터링을 수행하여 새로운 위험요소를 파악하고 이에 따라 새로운 보안정책 및 보안대책을 수립하여 보안기능에 반영시킨다. 보안에 대한 관리는 크게 개인 사용자별 관리와 전자상거래 시스템 운영조직내 관리의 두 분류로 나눠어진다. 개인 사용자의 경우는 전자지갑과 함께 배부된 소프트웨어를 통해 기본적 보안 문제를 해결하며 유사시 상거래 운영조직의 콜센터를 통해 문제를 해결하도록 하는 것이다.

추가적으로 <그림 11>과 같이 구성된 보안 시스템 및 관리 체계하에서 주기적으로 시스템 납품업체 또는 외부의 전문 감리업체를 통해서 보안시스템에 대한 전반적 성능 및 문제점에 대한 보안감사를 받도록 한다.

5.2 내부적 관리 및 운영조직의 구성

클라이언트레벨의 보안은 개별 사용자가 PC보안 소프트웨어를 바탕으로 자체적으로 해결하며 문제점 및 문의사항 발생 시 중앙의 콜센터를 통해 문제를 해결한다.

서버레벨의 보안은 전자상거래시스템을 중앙에서 운영하는 사업자가 별도의 조직을 구성하여 관리하도록 한다. 이를 통상 보안조직이라고 명명하는데 이의 구성은 보안 관리자, 보안시스템 관리자 및 콜센터로 이루어진다. 서버레벨의 보안을 위하여 구성된 보안조직은 유기적인 관계를 유지하며 각자의 영역에서 시스템의 보안과 관련된 업무를 담당한다. 일반적으로 앞서 명시한 보안조직은 기존 조직의 전산관련 조직에서 해당자의 업무특성을 파악하여 선별하도록 한다. 일반적 기업, 기관의 경우 이러한 보안조직이 별도의 전산관련 업무를 담당하면서 본 업무를 겸임하게 되는 경우가 많은데, 이는 매우 위험한 관리 방식이다. 보안조직은 해당 시스템의 관리나 정책 수립 및 고객 상담 등을 위하여 지속적으로 전자상거래 시스템 보안에 대한 정보수집, 분석 및 파악을 병행해야 한다. 따라서, 보안조직은 여타의 전산관련 업무와 겸임되지 않도록 업무영역을 명확하게 설정해주는 것이 효과적이다. 보안조직의 담당업무 및 이에 대한 처리방식은 다음과 같다.

5.2.1 보안관리자

보안관리자는 1인의 책임자급으로 설정한 후에, 실질적인 정책결정의 역할은 하부에 위치한 보안 시스템 관리자들과의 협의 하에 진행하도록 하는 것이 효과적이다. 보안관리자는 전사적으로 인터넷을 포함한 보안정책을 수립하고 이를 각각의 보안 시스템에 적용 가능한 형태의 정책으로 수립하는 역할을 담당하며, 보안 시스템 관리자를 통해서 보고되는 보고서를 통하여 보안상의 취약점을 파악하여 즉시 조치를 취하거나 필요시 세부지침을 수립하여 보안 시스템 관리자에게 전달한다. 또한, 일단 보안이 온라인으로 적용되고 결과가 보고서로 출력되면 보안 관리자는 내용을 검토한 후 새로운 지침을 만들거나 강화하여 이를 또 다시 시스템에 반영하고 그 결과를 분석하여 대안을 작성하는 등 일련의 작업을 되풀이하여 전자상거래 시스템의 보안이 강화될 수 있도록 한다.

5.2.2 보안 시스템 관리자

보안 시스템 관리자는 보안시스템 각각의 구성요소에 대하여 독립적으로 설정하거나, 또

는 복수개의 시스템을 1인이 관장하도록 할 수 있다. 보안 시스템 관리자는 보안 시스템의 설치 및 문제 발생 시 이에 대한 대응 역할을 수행하며 새로운 버전의 도착 시 버전 업그레이드 작업 등을 수행한다. 또한, 보안 시스템을 관리하며 해당 보안시스템에서 발생하는 이벤트에 대한 로깅을 취압, 출력 및 정리하여 리포팅하고, 보안 관리자와의 긴밀한 협의 하에 보안 관리자가 작성한 보안 관련 내용을 보안시스템에 적용한다.

5.2.3 콜센터

콜센터는 전자상거래 시스템을 이용하는 고객의 규모에 따라서 1인이상 복수명으로 구성된 전체적 상담조직을 의미한다. 콜센터는 PC보안 프로그램에 대한 설치, 운용 및 문제해결에 대한 대고객 상담을 담당한다. 운영하는 전자상거래 망의 규모가 상대적으로 커진 경우, 일반적 내용에 대한 상담과 답변은 CTI(Computer Telephony Integration)시스템을 통하여 해결하도록 하는 것이 효율적이며, 상담원이 이에 부가적으로 CTI시스템을 통해 해결할 수 없는 세부사항에 대한 상담과 답변에 응하도록 한다. 또한, 콜센터의 상담조직은 인터넷 및 전자상거래 시스템의 전반적 사항에 대한 개괄적 이해와 이의 사용 및 활용에 있어서 발생할 수 있는 보안상의 문제점과 그에 대한 예방법 및 대응방안에 대한 세부적 지식을 습득하고 있어야 한다.

6. 결론

현재 시점에서 가장 안전한 전자상거래용 프로토콜의 표준으로 자리잡은 것은 Visa사와 MasterCard사의 주도하에 정립된 SET이다. 실제로 SET는 기존에 여러 기업, 연구기관 및 단체에서 제시했던 전자상거래 메커니즘에서 진일보하여 전자상거래시 보안측면에서 발생할 수 있는 대다수의 문제점에 대한 대응 메커니즘을 내재하고 있다. 하지만, SET는 말 그대로 일종의 프로토콜이며, 프로토콜 자체가 가질 수 밖에 없는 한계성을 극복하고 있지는 못하다. 즉, 시스템 측면에서의 보안상 문제점에 대한 파악과 이에 대한 대응 메커니즘을 제시하고 있지는 못하다.

이와 같은 전제하에서 본 논문은 SET 1.0 자체에 대하여 파악하고, 파악된 내용을 바탕으로 표준집 자체에 포함된 내용들의 보안상 문제점을 분석하였으며, 실제적인 운용 시스템의 모델을 정립하고 그에 따른 보안상 위협요소를 분석하여, 이러한 내용들을 바탕으로 하여 보안상의 위협에 대한 대응 메커니즘을 설계하고 그에 따른 시스템의 구축 및 관리, 운영 방안을 제시하였다.

대응 메커니즘의 구현에서 제시한 단위 시스템들은 PC보안 소프트웨어, 침입탐지 시스템, 침입차단 시스템, 암호화 통신 시스템, DB 보안 시스템 및 보안감사 시스템으로, 이에 대해서는 현재 대다수의 시스템이 실용화단계에 도달해있고, 또한 지속적인 개량과 발전이 이루어지고 있다. 실질적으로 본 논문에서 제시한 보안 시스템을 구축하기 위하여 세부적 단위 시스템을 선별할 경우에는 각각의 제조업체마다 상이한 제품의 기능 및 성능상의 특성을 면밀히 살펴보아야 할 것이다. 본 논문에서는 이러한 부분에 대한 내용이 배제되어 있으나, 본 사항에 대한 판단은 도입 기관, 기업별로 본 논문에서 제시한 기본적 사상의 범주내

에서 무리없이 수행할 수 있을 것으로 사료된다.

본 논문에서 제시한 SET 1.0 전자상거래시스템에 대한 보안 시스템은 실질적 운용모델에 대한 분석을 통하여 설계된 시스템으로, SET 1.0을 기반으로한 가상쇼핑몰의 효과적 운영과 가상쇼핑몰 상에서 발생할 수 있는 각종 범죄행위를 예방하고 효과적으로 대처하기 위한 근간으로 자리매김할 수 있을 것이다.

참고문헌

[정보통신부,1998] 정보통신부, *정보통신망 침입차단 시스템 평가기준, 평가 지침서*. 1998.

[통상산업부,1997] 통상산업부, *전자상거래와 보안기술*. 1997.

[Atkins, 1996] Derek Atkins, *Internet Security Professional Reference*, New Riders. 1996

[http 1] Graham Information Security and Management Service, *PC Workstation Security*, http://www.onthenet.com.au/~grahamis/IGGPCSec.html

[ISS, 1997] Internet Security Systems, *Internet Scanner SAFEsuite*, 1997

[Lynch, 1996] Daniel C. Lynch, Leslie Lundquist, Digital Money, John Wiley&Sons. 1996.

[http 2] SET Secure Electronic Transaction LLC, *Open Vendor Meetings and Overviews*, http://www.setco.org/download.html

[http 3] Aurobindo Sundaram, *An Introduction to Intrusion Detection*, http://www.acm.org/crossroads/xrds2-4/intrus.html

[http 4] Shekhar Swamy, *Database Security*, http://www.cs.rpi.edu/~swamy/adb/security/db_future_work.html

[VISA, 1997-1] VISA and MasterCard, *SET Securre Electronic Transaction Specification, Book 1 : Business Description, Version 1.0*. May 1997.

[VISA, 1997-2] VISA and MasterCard, *SET Securre Electronic Transaction Specification, Book 2 : Programmer's Guide, Version 1.0*. May 1997.

[http 5] VISA, *SET Secure Electronic Transaction at Visa*, http://www.visa.com/cgi-bin/vee/nt/ecomm/set/main.html?2+0

[http 6] John Wack, *Introduction to Firewalls*, http://www.telstra.com.au/pub/docs/security/800-10/node30.html

[Wayner, 1997] Peter Wayner, *Digital Cash*, 2nd Edition, AP Professional. 1997.

저자소개

김상균

1996년 중앙대학교 제어계측공학과 공학사
1998년 연세대학교 산업공학과 공학석사
1998년 (주)사이버게이트인터내셔널 기술이사
현 재 연세대학교 인지과학 산업시스템공학전공 박사과정
관심분야 전자상거래

강성호

1986년 서울대 제어계측공학과 공학사
1988년 The University of Texas at Austin, Electrical and Computer Engineering, M.S.
1992년 The University of Texas at Austin, Electrical and Computer Engineering, Ph.D.
현 재 연세대학교 공과대학 기계전자공학부 조교수
관심분야 Testing and Design for Testability, CAD for VLSI, ASIC Design