불필요한 규제 및 제도 개선 '시급'

보안(security)은 다분히 군사적인 목적으로부터 시작되었다. 보안 기술의 발전도 전쟁을 통한 개선을 통하여 이루어져 왔다. 여기서는 이중에서 보안 기술에 대한 정리를 통하여 전자 상거래를 위한 보안 기술이 갖추어야 할 내용과 보안 기술의 미비에 따르는 문제점들을 나열하려고 한다.

김치권/한국휴렛팩커드 인터넷팀

목 차

1. 정보사회의 새 열꽃 인터넷
2. 인터넷 비즈니스의 단계적 구축
3. 인터넷 도입에 따른 IT 아키텍처의 변화
4. 정보유통을 위한 인터넷
5. 영원한 창과 방패, 보안 (이번호)
6. 네트워크상에서의 비즈니스
7. 인터넷의 통합관리 방안
8. 미리보는 인터넷의 미래

IT와 보안

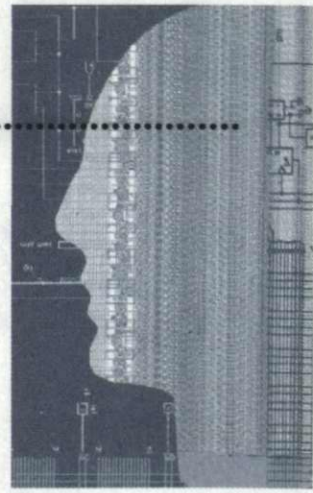
보안은 인터넷의 도입에 따라서 사람들의 관심을 받고 있는 분야가 되고 있다. 보안은 무엇이든 막을 수 있는 방패를 만드는 것을 목적으로 시행되지만 항상 이를 관통하는 창이 있어 왔다. 이러한 모순적인 양상은 보다 완벽한 솔루션을 위한 정반합의 관계로서 보안의 발전에 이바지하여 왔다. 즉, 보안은 만들어진 보안 시스템을 공격하는 방법을 개발하고 때로 실행하는 해커로 대표되는 창과 이를 막으려는 IT 관리자의 노력으로 개선되어 왔다.

인터넷이 교육적인 목적의 네트웍에서 상업적인 목적의 네트웍으로 변화함에 따라서, 인터넷을 기업망의 일부 또는 기업의 비즈니스를 위한 매체로서 사용하고자 하는 시도가 늘어가고 있다. 전자 상거래(Electronic Commerce)로 대표되는 이러한 새로운 시도는 지금 초기 도입과정을 거치고 있으며 해결해야 할 많은 문제를 가지고 있다.

첫번째로서 언급되는 것이 새로운 환경에 대한 사람들의 인식의 변화가 선행되어야 한다는 것이고, 두번째는 이를 뒷받침할 정치, 제도적인 지원체제가 갖추어 져야 한다는 점이며, 세번째로서 실제의 구현을 위한 기술적인 입장에서의 보안 기술의 정립이 해결되어야 한다.

본문은 이중에서 보안 기술에 대한 정리를 통하여 전자 상거래를 위한 보안 기술이 갖추어야 할 내용과 보안 기술의 미비에 따르는 문제점들을 나열하려고 한다. 보안(security)은 다분히 군사적인 목적으로부터 시작되었다. 보안 기술의 발전도 전쟁을 통한 개선을 통하여 이루어져 왔다.

보안의 일반적인 개념은 "위험과 불안 요소로부터 조직의 자산과 자원의 피해를 최소화하려는 모든 종류의 행동"이라고 할 수 있으며, 이러한 범주에서 보안은 자연재해, 인위적인 재해, 물리적인 파괴, 도난을 포함하여 광대한 범위를 포괄한다. 이러한 모든 분야의 보안에 대하여 언급하는 것은 본문의 방향과 맞지 않으므로, 앞으로의 내용은 IT에 대한 보안만으



로 한정하여 설명하도록 한다.

보안 관련 용어 정리

보안에 대한 설명을 하기 위해서 먼저 앞으로 사용될 보안 용어에 대하여 미리 설명이 필요한 것을 선별하여 정리하고자 한다. 보안의 기술에는 전문적인 용어가 많으므로 그 의미를 밝혀두는 것이 내용의 이해에 도움이 되리라고 생각된다. 또한, 보안 용어의 한글화에 대하여 여러가지 이견이 많으므로 이 글에서 사용되는 용어를 정의하는 것이 필요하다.

인증(authentication)

사용자의 자기 자신을 확인하는 단계 또는 그 기술로서 사용자의 식별자를 물어보는 과정과 식별자와 연결된 자기 자신의 특성을 확인하는 과정으로 이루어진다. 중대형 컴퓨터를 사용하기 위해서 우리는 컴퓨터에 접속하기 위하여 각자 계정 (account)과 비밀 번호(password)를 알고있어야 한다. 그래서, 로긴시에 계정 이름과 비밀 번호를 입력하여야 컴퓨터를 사용할 수 있다. 이러한 입력 과정을 인증이라고 한다.

컴퓨터 시스템에서 계정 이름과 비밀 번호는 각각 식별자와 특성을 나타낸다고 할 수 있다. 자기 자신을 증명하는 방법으로서 비밀 번호는 컴퓨터 입장에서 비교가 쉽다는 점에서 매력이 있지만 외부에 공개된다면 자기 자신의 증명으로서의 효력이 떨어진다는 점에서 취약점이 있다. 그러므로, 보안의 증대를 위하여 일부 시스템은 사용자의 개인적인 신상 정보를 사용하는 경우도 있다.

예를 들어, 인증을 위하여 시스템에 최초 등록시에 개인의 사적인 정보인 가장 좋아하는 색, 도시 등의 선호도 정보와 부모 또는 자식의 이름을 함께 입력받아서 인증시에 이를 확인하는 방법을 사용하는 경우도 있다. 또는 신체적인 정보를 사용하여 지문을 감식하거나 눈동자의 실핏줄 문양을 이용한 홍채 감식을 사용하는 시스템도 있다. 지문 감식과 홍채 감식은 첩보 또는 SF 영화에서 많이 등장하고 있는 인증 방법이지만 사용자 자신을 확인하는 유력한 방법이라는 점에서 앞으로 확산 가능성이 많은 시스템이기도 하다.

권한(authorization)

인증이 보안의 시작이라면 권한은 보안의 중심이다. 권한은 인증에 성공한 사용자가 전체 시스템에서 어느 부분까지 사용할 수 있는가를 한정하고 이를 검사하며 모니터링하는 것을 의미한다. 즉, 한 회사에서 일반 사원이 볼 수 있는 정보와 사장이 볼 수 있는 정보가 다른 것을 IT에 적용하기 위해서는 두 사용자의 권한을 다르게 배분하면 되는 것이다.

이러한 권한은 사용자의 계정 정보에 목록을 만들어서 관리하거나, 접근할 자원에 사용할 수 있는 사용자의 목록을 만들어 관리한다. 보안에 있어서 권한의 문제는 전자 상거래의 확산에 따라서 더욱 중요하여질 것이다.

인정(certification)

전자 상거래에 있어서 보안은 여러가지 위험요소를 해결할 수 있어야 한다. 위험요소는 전자 상거래에서 구매자와 판매자가 서로 직접 상면하지 않는다는 점에서 발생한다. 구매자의 입장에서 판매자의 신용을 확인하여야 하며 전달되는 금융정보-예를 들어 신용카드 번호나 통장 번호 그리고 비밀 번호,-를 제3자가 획득하더라도 읽어낼 수 없도록 하는 것이 필요하다.

판매자 입장에서도 구매자의 신용을 확인하고, 구매자가 상품을 획득한 후에 구매 사실 자체를 부인하는 경우의 공적인 증거를 위하여 부인 방지 방법이 필요하다. 이러한 양자의 불안요소를 해결하기 위한 방법으로 전자 상거래에서는 공신력이 있는 제3자가 각자를 보증하는 방법을 사용하는데 이를 인정이라고 한다.

실제 환경에서는 인정의 권한을 가지고 있는 CA(certificate authority)를 사용하여 구매자와 판매자의 신분을 확인하고 전달되는 비밀 정보를 보호하며, 서로의 구매 사실을 부인할 수 없게 하여 준다.

보안의 역사

컴퓨터 보안의 시작은 일반적으로 1988년 인터넷 웜(Internet worm)으로 부터 출발된다고 할 수 있다. 이 사건이 최초의 보안 사건은 아니지만, 그 피해와 영향은 이를 계기로 컴퓨터응급대응팀(CERT, Computer Emergency Response Team)의 발족을 촉진하였으며 비로서 체계적인 보안 문제가 대두되게 하였다.

인터넷 웜은 1988년 11월 2일에 발생하여 인터넷을 통하여 미국 전역

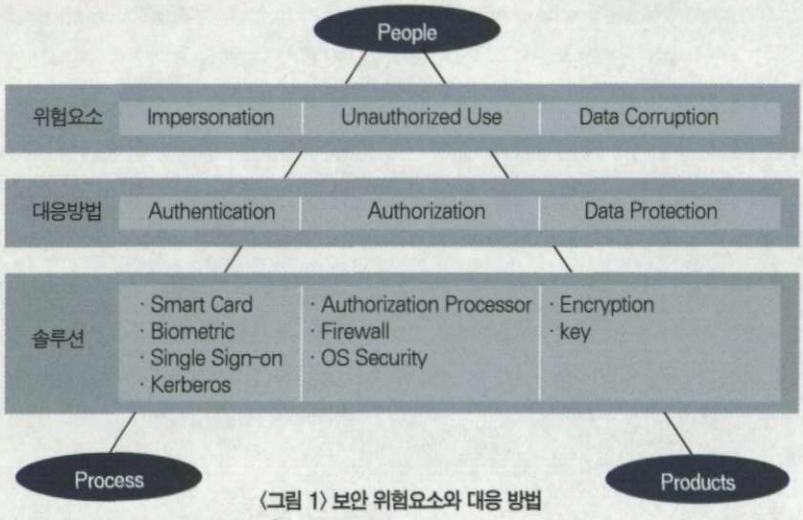
의 대학, NASA, 국방 기지, 연구소에 전파되었다.

인터넷 웜은 바이러스와는 달리 네트웍을 통하여 전파되며, 자기 자신이 완전한 프로그램으로서 다른 프로그램의 도움없이 독자적으로 실행된다. 추정된 피해 시스템은 600개에 이르며, 프로그램이 아무런 피해를 주지않도록 작성되었지만 인터넷 웜의 전파를 막기 위해서 시스템을 다운하거나, 네트웍 연결을 제거하면서 약 1만불에서 100만불의 손해가 발생하였다. 이 사건의 범인으로 미국 코넬 대학의 대학원생인 로버트 모리스 (Robert T. Morris)은 1990년 재판을 통하여 5년형을 선고받았다.

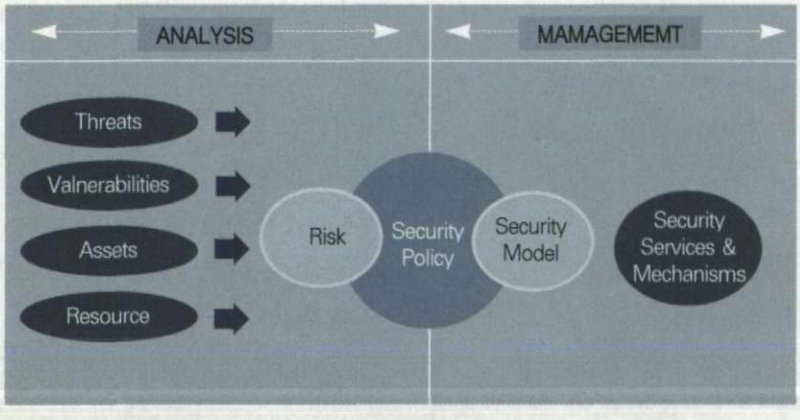
이 사건은 컴퓨터 보안을 전 사회에 선전하는 계기가 되었으며, 많은 보안관련 산업과 조직을 만들게 하였다.

1988년에 나온 책인 "뻐꾸기 알(The Cuckoo's Egg)"은 천문연구소 전산센터의 클리프 스톨(Cliff Stoll)이 서독의 한 해커를 추적하기 위하여 1년 동안 노력한 것에 대한 내용으로서 책자로서 나타난 해커의 이야기를 다루고 있다. 서독에 소재한 것으로 알려진 이 해커는 잡히지는 않았지만, 해커는 미국의 핵, 생물학, 화학 등의 국가 기밀에 대한 문건을 네트웍을 통하여 입수하고 소련의 KGB에게 넘겼다고 한다. 이일을 계기로 컴퓨터 보안은 국가 기밀의 보호를 위한 또 하나의 고려사항으로 등장하게 된다.

컴퓨터 보안이 이처럼 해커의 공격에 대한 대응으로서 발전하였으며, 새로운 대응 방법에 대하여 새로운 공격이 연구되는 관계를 통하여 현재에 이르고 있다.



〈그림 1〉 보안 위험요소와 대응 방법



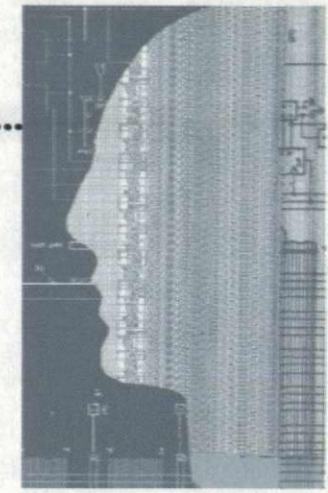
〈그림 2〉 보안의 구현 과정

보안의 위험 요소와 대응 방법

보안을 창으로 대표되는 위험 요소와 방패로 대표되는 대응 방법으로 나누어서 볼 때, 보안은 사용자들이 시스템을 바르게 쓸 수 있도록 하는 일련의 프로세스와 그를 뒷받침하는 제품으로 구성될 수 있다. 시스템 관리자가 고려하여야 하는 위험 요소로는 위장(impersonation), 불법 이용(unauthorized use), 자료 변조(data corruption)가 있다. 이에 대한 대응 방법으로 인증(authentication), 권한(authorization), 자료 보호(data protection)가 있다.

위장은 다른 사람의 신분으로 시스템을 속이는 것으로 계정 이름의 도용을 들 수 있다. 이를 방지하는 방법이 바로 인증이며 강력한 인증 솔루션으로는 스마트 카드, 생물학적인 방법 (지문, 홍채), 한번의 확인 만으로서 전체 시스템을 별도의 로긴 과정없이 사용할 수 있게하는 싱글사인온(single sign-on), 분산된 네트웍 환경에서 인증서비스를 제공할 수 있는 커버로스(kerberos)등이 있다.

불법 사용은 할당되어 있는 권한의 한계를 벗어나서 사용하는 것으로 기밀 정보에 대한 접근 문제에 관련된



다. 대응 방법으로는 명백한 권한을 배정할 수 있게 하는 시스템이 필요하며 운영체제, 네트웍, 애플리케이션 레벨에서 다양한 권한을 일관성있게 할당할 수 있는 솔루션이 필요하다. 운영체제 레벨에서는 시스템 시큐리티의 일부로서 권한 배정을 할 수 있으며, 권한 배정에 대하여 강력한 제한을 가지고 있는 시스템을 보안의 등급을 정의한 오랜지 북(orange book)에서는 B1등급 이상이라고 한다.

전자 상거래에서는 금전적인 정보의 전달이 주된 내용이므로 더욱 강력한 권한 제한이 필요하며 이를 위해서는 B1 등급 이상의 운영체제를 지원하는 것이 대두되고 있다. 네트웍 레벨에서의 권한 제한을 위하여 사용되는 것이 보안 방호벽(firewall)이며, 이는 네트웍을 통하여 접근하는 모든 서비스에 대하여 접근의 불가/허가를 정의할 수 있게 해준다.

보안 방화벽의 설치는 전자 상거래는 물론 인터넷 구축의 가장 기본적인 사항이다. 어플리케이션 레벨의 권한 배정을 위하여서는 개발자를 위한 API가 필요하며, 네트웍 환경에서 분산된 권한 제한을 할 수 있는 솔루션이 적당하다.

자료의 변조는 천원이 들어있는 통장을 천만원이 들어 있는 통장으로 바꿀 수 없게 하는 것이다. 변조 방지를 위한 자료 보호는 일반적으로 자료의 내용을 암호화하는 방법으로 구현된다. 암호는 저장된 자료의 내용을 해독할 수 있는 키(key)의 존재로서 권한이 부여된 사람에게만 전달된다. 기존의 암호화 방법은 암호를 생성할 때 사용하는 키와 해독할 때 사용하는 키가 같으므로, 암호에 사용된 키의 안전한 전달이 보안에 가장 중요한 요소가 되어 왔다.

그러나, 네트웍 환경에서 복잡한 관계를 구현하기 위해서는 각각의 연결 관계마다 별도의 키가 존재해야 하므로 N명이 참가하는 관계에서는 nC2 , 즉 n * (n-1) / 2 개의 키가 필요하다. 간단한 예로서 100명이 서로 비밀 정보를 주고 받을 경우에는 4,950개의 암호가 필요하게 된다.

이러한 단점을 개선하기 위해서 1976년 디피에(Diffie)와 헬만(Hellman)이 발표한 공개키(public key) 암호 방식은 이러한 단점을 뛰어 넘어 사용자 당 공개키와 개인키(private key) 2개의 암호를 할당한다. 개인키는 개인이 비밀스럽게 보관하고 공개키는 공개된 장소에 공표하는 구조로 운영되는 이 방법은 다수가 참가하는 경우에도 참가자 당 2개의 비밀키만을 필요로 한다는 점과 키의 분배가 비밀스럽지 않아도 된다는 점에서 전

〈표 1〉 위협의 예제와 설명

종 류	예 제	설 명
자연적/물리적인 위협	화재, 홍수, 전원 공급 중단	인위적인 방법으로 해결할 수 없는 자연 재해나 사고
의도적인 위협	해커, 내부 불만자	명백한 공격 의지를 가지는 인위적인 위협
비의도적인 위협	초심자의 실수, 잘못된 작동	무지나 오해에 의한 시스템이 위험에 빠지는 경우

〈표 2〉 취약점의 예제와 설명

종 류	예 제	설 명
물리적 취약점	시스템 파손, 장치 도난	침입자가 시스템에 물리적인 손상이나 강탈을 할 수 있는 여지로서 물리적인 출입문 관리등이 해결책이다.
자연적인 취약점	화재, 홍수, 지진, 번개, 전원 차단	인위적인 것이 아닌 자연 재해로 인한 위험
하드웨어와 소프트웨어 취약점	하드웨어의 이상 작동, 소프트웨어의 버그	모든 장비, 소프트웨어는 설계된 것 대로만 동작하지 않은 가능성이 있으며, 이로 인하여 항상 문제점에 대비하여야 한다.
매체 취약점	디스크에 남겨진 비밀 정보의 유출	저장매체에 쓰여진 정보는 지워서 없앤 경우에도 정보의 내용이 남겨져 있을 수 있다.
방사 취약점	통신 선로의 도청	모든 전기장치는 전자기파 방사를 하며, 이를 이용하여 전송되는 데이터를 도청할 수 있다.
통신 취약점	IP 스푸핑(spoofing)에 의한 불법적인 접속 허용	통신의 허가에 의하여 프로토콜의 취약점이나 버그를 이용하여 침입이 가능하다.
인간적인 취약점	시스템 관리자의 컴퓨터	범죄 시스템 관리자 또는 이용자의 의도적인 시스템 불법 사용

자 상거래를 위한 솔루션으로 이용되고 있다.

현재 전자 상거래에서의 자료 보호는 속도면에서 빠른 기존의 방법과 공개키의 방법이 적절하게 절충되어 사용되고 있다. 일반적인 방법은 서비스의 초기에는 강력한 보안 방법인 공개키 방법으로 접속하고 서로 공통으로 사용할 비밀키를 교환함으로써 실제 자료의 전송에는 빠른 속도의 기존 방법을 사용한다.

보안의 구현 과정

보안은 위험 요소를 분석하는 것에서부터 시작되며, 위험 분석(risk analysis)은 쉽게 얘기하여 우리를 공격할 수 있는 창의 종류와 공격 방법을 알아보는 것이다. 위험 분석은 취약점과 위협을 통하여 알아볼 수 있다. 취약점(vulnerabi-lity)은 시스템이 공격받을 수 있는 내재적인 가능성을 말한다. 리스크로 부터 보안정책을 결정하며, 이에 따른 보안 모델을 설계하고 관리하는 과정으로 보안의 전체를 나타낼 수 있다.

위협(threat)은 외부에 존재하는 위험을 의미하며 위험은 사람이거나 어떤 물건 또는 사건으로 구분할 수 있다.

위협에 있어서 중요한 점은 명백한 의도를 가지고 공격하는 해커등의 문제 뿐만 아니라, 교육 등의 미비로 발생할 수 있는 실수가 발생하지 않도록 준비하고 자연 재해나 사고에 대비할 수 있는 백업 솔루션을 장치하는 것이다.

취약점(vulnerability)은 위협과는 상반된 입장에서 시스템 자체의 문제를 의미하며, 위협과 취약점이 일치하는 경우에 보안의 위험이 발생하게 된다.

보안은 내재적인 취약점과 외재적인 위협으로 부터 자원(resource)와 자산(asset)을 보호하는 것이다. 그러나, 위에서 언급한 것처럼 취약점과 위협은 인위적인 방법으로는 해결할 수 없는 것도 있고, 인위적으로 가능하더라도 재정적이거나 기술적인 또는 제도적인 면에서 해결할 수 없는 것들이 존재한다.

그러므로, 각각의 취약점과 위협을 해결하는 방향이 필요하며 이를 보안 정책이라고 한다. 보안 정책은 보안을 해결하기 위한 비용효율적인 도구이며 보안 솔루션의 검증을 위하여 필요한 기준이 된다.

보안 정책은 조직의 성격이나 상황에 따라서 그 내용과 구체성에 차이가 있을 수 있으나, 보안 시스템의 구축을 위하여서는 반드시 작성되어야 한다. 보안 정책은 자원과 자산에 대한 언급이 필요하며 이러한 자원과 자산을 각각의 취약점과 위협으로 부터 보호하는 것의 여부를 명백하게 정의한다.

전자 상거래를 위한 보안

보안의 여러가지 방향에서 전자 상거래는 앞으로 우리가 좋던 싫던 참여할 수 밖에 없는 대세가 되고 있다. 전자 상거래를 위한 표준안이 이번 연도에 이루어 졌다. 바로 비자와 마스터의 공동 개발로 공표된 인터넷을 통한 카드 결제 솔루션인 SET가 금년 5월에 공개되었다.

SET은 Secure Electronic Transaction의 약자로서 안전한 인터넷 상의 트랜잭션 처리를 위한 표준이다. SET의 발표로 인하여 지금까지 각자 개발되어 왔던 많은 전자 지불 시스템들이 SET 표준을 준수하는 방향으로 선회하고 있다. SET 프로토콜의 작동 방식을 〈그림 3〉에서 살펴보자.

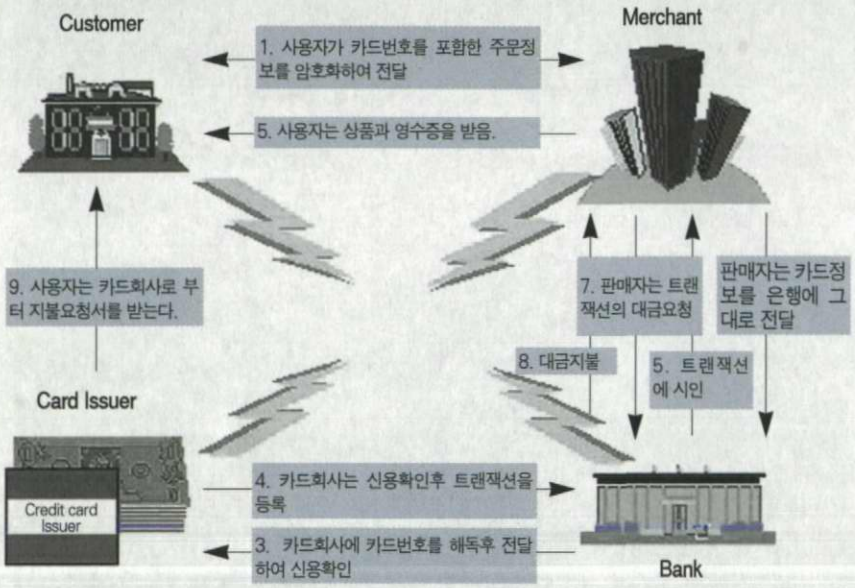
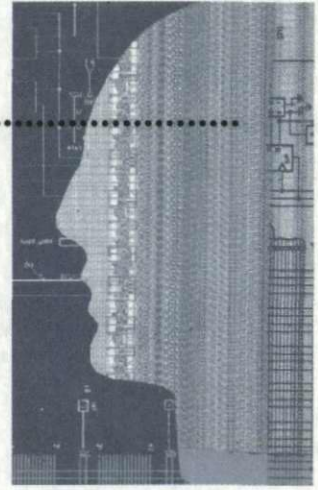
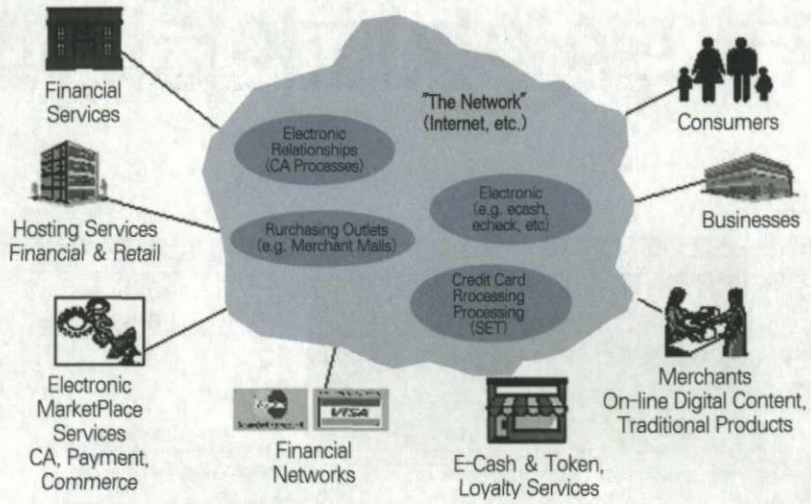


그림 3. SET의 동작 방식

이러한 SET 프로토콜의 안전한 작





〈그림 4〉 전자 상거래 환경

동을 위해서는 판매자와 구매자를 인정하기 위한 CA의 존재가 무엇보다도 중요하다. 전자 상거래를 위한 환경의 구축을 위해서는 공개된 신분증명을 위한 공개 CA의 존재가 무엇보다도 필요해진다.

국내의 전자 상거래의 활성화를 위하여서도 정부 및 공공단체에서 민간기업이 신뢰할 수 있는 CA의 구축이 가능하도록 제도 및 산업 환경의 선도에 앞장서야 될 것이다.

전자 상거래의 보안 문제를 해결하기 위한 또 하나의 중요점은 스마트카드를 사용한 인증 및 인정 시스템이다. 구매자와 판매자가 서로 신분을 확인할 명백한 솔루션이 없는 환경에서 스마트카드는 이를 해결하기 위한 강력한 솔루션이다.

마침 우리 정부는 전자주민증을 구상하면서 이의 매체로서 스마트카드를 고려하고 있다고 한다.

스마트카드의 기능을 보다 충실하게 살리기 위한 좋은 기회로서 스마트카드를 사용한 금융거래에 대한 솔루션의 개발과 정착이 필요한 시기이다. 스마트카드를 사용한 전자 상거래는 이미 유럽을 중심으로 활발히 앞서나가고 있으며, 이런 점에서 유럽공동체는 미국보다 활발한 전자 상거래 환경을 구축해 나가고 있다.

전자 상거래를 중심으로 한 앞으로의 네트웍 및 시스템 환경을 살펴보면 전자지불 시스템 과 인터넷 신용카드 결제 시스템, 사이버 쇼핑몰, 전자 관계 시스템 등을 중심으로 모든 서비스가 집중되어 제공될 수 있는 환경이 만들어질 것이다. 이러한 환경의 등장에 가장 활력소가 되는 것이 사람들을 안심시킬 수 있는 보다 개선된 보안 솔루션의 개발이다.

결론

국내의 상황도 이러한 산업의 동향을 따르기 위하여 정부와 기업이 함께 관련 문제를 해결해 나아가야 하는 위치에 있으며, 특히 보안 기술에 관한 문제는 미국의 보안 기술에 대한 수출통제법에 의하여 많은 제약을 받고 있는 상태이다. 이러한 미국 내의 제약은 전세계적인 전자 상거래의 정착을 앞당기는 데에 큰 지장을 주고 있다. 이에 대한 미국 내의 관련 법, 제도의 개선을 위하여 빌 클린턴 미대통령과 엘고어 미부대통령에 의해서 "A Framework for Global Electronic Commerce"라는 문건에서 미국 정책의 방향을 제시하고 있다. 이 문건은 전자 상거래의 주도를 민간업체에서 주체적으로 시장원리에 맞추어서 발전시키도록 권고하고 있으며 정부의 불필요한 제한 및 제도를 시급히 개선하도록 제시하고 있다.

정부의 수반으로서의 위치에도 불구하고 이렇게 정부의 역할을 제한하는 문건을 만들어낸 의도는 앞으로 세계가 전자 상거래에서 성공한 나라에 경제의 발전을 약속하리라는 믿음이 있기 때문이다. 이를 위하여 느린 정부의 대응보다는 활발한 시장 경제의 선택을 정부는 뒷받침하고자 하는 의지를 보이고 있다.

우리나라도 인터넷을 통한 무형의 자산에 대한 구매 및 판매에 있어서는 관세를 부과하지 않겠다는 과감한 결정을 내리는 등, 발빠른 행보를 취하고 있다. 미국과는 다른 보안 환경과 경제 환경을 가지고 있는 우리나라에 맞는 보안기술의 개발과 정착을 통하여 전자 상거래에 도약하는 것이 새로운 IT 환경을 맞는 우리의 자세일 것이다. 그러기 위한 조치로서 산업계에서 CA와 스마트카드의 도입을 적극적으로 추진해 나가야 할 것이다. DC