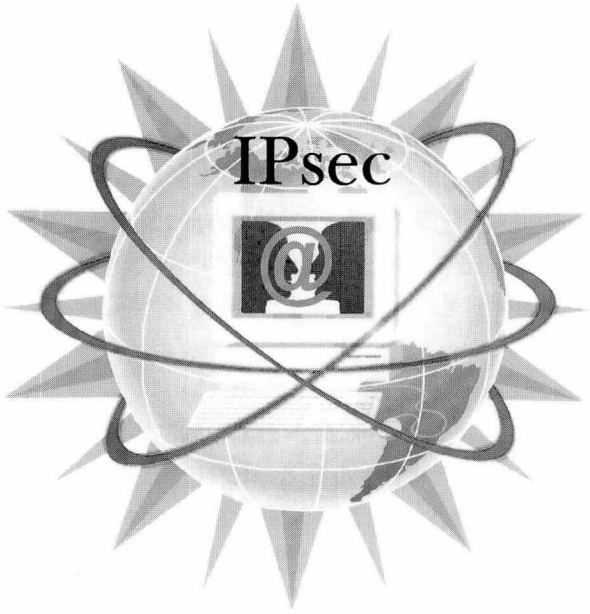
차세대 인터넷에서의 정보보호

이종태, 손승원, 조현숙 / 한국전자통신연구원 정보보호기술연구본부



서론

1970년 초반, 미국 DARPA에 의해 개발된 인터넷은 넷스케이프라는 응용 프로그램이 소개된 이후 그 활용도가 급속히 증가하여, 현재 전자상거래 및 전자정부의 실현을 위한 발판이 되고 있다. 이제 인터넷은 일반인에게도 편리할 뿐만 아니라 불가결한 문명의 이기로 여겨지고 있음에도 불구하고 정보보호에 대한 필요성이 절실하게 요구되는 이유는 무엇일까? 한 마디로 인터넷은 정보의 노출에 대해 무방비 상태의 통신 인프라라고 할 수 있기 때문이다. 현재도 컴퓨터에 대한 크래킹 및 바이러스 등에 의한 피해 사례가 끊임없이 보도되고 있다. 그 중에서도 CIH 바이러스와 야후, CNN등이 피해를 입은 서비스거부 공격등은 사회적으로 큰 파장을 일으킨 사건으로 기억되고 있다.

인터넷은 그 효용성에도 불구하고 정보보호 관점에서 볼 때, 근본적으로 여러 가지 문제점을 안고 있다. 최근에 자주 등장하는 분산 서비스 거부 공격같은 경우도 인터넷이 갖고 있는 문제점이 드러난 한 예에 불과하다. 문제점을 분석하기 전에 먼저 인터넷을 구성하고 있는 요소를 살펴보면 이는 근본적으로 호스트라고 할 수 있다. 그리고 이 호스트는 하드웨어와 소프트웨어로 이루어져 있고 호스트간의 네트워킹을 위한 링크가 존재한다. 하드웨어 부분은 모니터나 본체로 부터의 전자파 방출에 따른 원격 도청외에는 실제적으로 문제시 되지 않고 대부분의 인터넷 취약점은 바로 소프트웨어와 링크상에 잠재되어 있으며 〈표.1〉은 인터넷 취약점을 공격하는 대표적인 크래킹기법들을 보여주고 있다.

링크상의 문제점을 살펴보면, 우리가 많이 사용하는 LAN 환경에서는, 크래커가 자신의 PC를 LAN

<표1> 인터넷에서의 주요 크래킹 기법

구 분	크래킹 기법
전자 우편	Spam Mail
	Email Bomb
서비스 서버 공격	Smurf 공격
	ICMP 공격
	Syn Flooding
	Ping 공격
web 서버 공격	Phf Bug 공격
	Php Bug 공격
	Teat-cgi 공격
스 니 퍼	

구 분	크래킹 기법
네트워크 응용서버 공격	Named 공격
	Imapd 공격
	Popd 공격
	Identd 공격
	Innd
스캐너	Post Scan
	Mscan
ID도용	
맥 오리피스	
크래킹 도구	
바이러스	

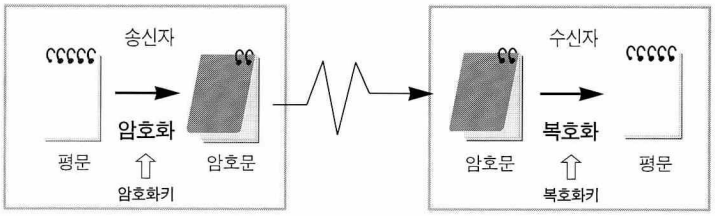
에 접속시키면 전송되는 데이타를 전부 읽어낼 수가 있으며 패킷 데이터의 내용을 위 · 변조시켜 재전송할 수도 있다. 그 다음은 운영체제를 포함한 소프트웨어 문제점으로서, 개발자가 예상하지 못한 비정상 상태가 발생하였을 때 적절한 대응을 하도록 하는 코드가 구현되어 있지 않기 때문에 나타나는 경우다. 그래서 프로그램 소스코드가 잘 알려져 있는 리눅스 경우에, 크래커들은 그러한 헛점을 종종 이용하게 되어 크랙킹 사고가 발생되는 것이다.

현재 사용중인 인터넷에서는 취약점 모두를 일시에 제거할 수는 없다. 넷스케이프는 SSL(Secure Socket Layer)이라는 정보보호기술을 적용하고 있고 전자상거래는 SET(Secure Electronic Transaction), 전자우편은 S-MIME(Secure Multipurpose Internet Mail Extension)을 사용하는 등, 각 응용서비스별로 정보보호기술을 적용하고 있으며 그러한 유형의 제품들이 많이 개발되어 있다. 그러나 현 인터넷을 대체할 차세대 인터넷에는, 모든 응용서비스에 대해 일관된 방식으로 정보보호 서비스를 제공하기 위해 IPsec(Internet Protocol Security)이라는 새로운 프로토콜이 추가되어 있어 인터넷을 근본적으로 안전한 인프라로 만들 뿐만 아니라 사용자가 편리한 도구로 활용할 수 있을 것이다.

암호 알고리즘

정보보호 기술에서 가장 근간이 되는 핵심요소는 암호 알고리즘이다. 암호기술은 평문을 해독 불가능한 형태로 변형하거나 또는 암호화된 통신문을 해독 가능한 형태로 변환하기 위한 방법을 연구하는 기술이다. 이는 데이터가 전송되는 중에 패킷 절취나 도 · 감청을 불가능하게 만들기 위한 것이다. 송신자는 수신자에게 평문을 암호화하여 그냥 보아서는 이해할 수 없는 암호문으로 변형하여 전송하고 수신자는 이를 복호화하여 본래의 평문으로 복원한다. 〈그림.1〉에서 보는 바와 같이 암호화와 복호화의 조작 원리를 암호 알고리즘이라 하며, 암호 알고리즘에 의한 변환을 제어하는 요소를 키라 한다.

현대 암호 알고리즘은 크게 스트림 암호 알고리즘, 블록 암호 알고리즘으로 분류할 수 있으며, 키 관리



<그림1> 암호와 복호의 개념

측면에서는 대칭키 암호 알고리즘과 공개키 암호 알고리즘으로 분류할 수 있다. 〈표.2 참조〉 스트림 암호 알고리즘은 키를 알고리즘에 주입하여 무한 수열로 평문을 암호화하는 것이며, 블록 암호 알고리즘은 고정된 크기의 입력 블록에 고정된 크기의 출력 블록으로 변형하는 암호 알고리즘으로, 블록내의 데이타는 키의 영향을 받는다. 또한, 대칭키 암호 알고리즘은 송신자와 수신자가 동일한 키에 의하여 암호화 및 복호화 과정을 수행하는 것으로, 이는 키를 안전하게 전송하고 관리해야 하는 어려움이 있어 암호화와 복호화 과정에서 서로 다른 키를 사용하는 공개키 암호 알고리즘이 등장하게 되었다. 또한, 임의의 길이의 입력을 받아 일정한 길이의 출력을 만들어 내는 해쉬 알고리즘이 있는데 이는 서명과 인증, 무결성에 이용된다.

대칭키 암호 알고리즘은 일반적인 데이터 암호화와 데이터 무결성 응용에 사용되고 공개키 암호 알고리즘은 계산 수행 속도의 문제로 인해 서명, 키관리 등에 이용되고 있다. 이 중 현재 가장 많이 이용되고 있는 암호 알고리즘은 대칭키 알고리즘인 3DES와 공개키 알고리즘인 RSA이며 해쉬 알고리즘은 SHA-1이다. 그러나, DES의 암호학적인 안전도 문제 즉, 작은 키 길이 등의 문제로 인해 DES를 대치하는 새로운 미국 표준 알고리즘인 AES가 표준화된 상태이고, 키 길이와 성능면에서 RSA보다 우수한 타원곡선 암호 알고리즘에 대한 관심도 증가하고 있다. 이러한 알고리즘들이 인터넷 정보보호를 위해 사용되고 있으며, IPsec에서도 적용되도록 표준화되어 있다.

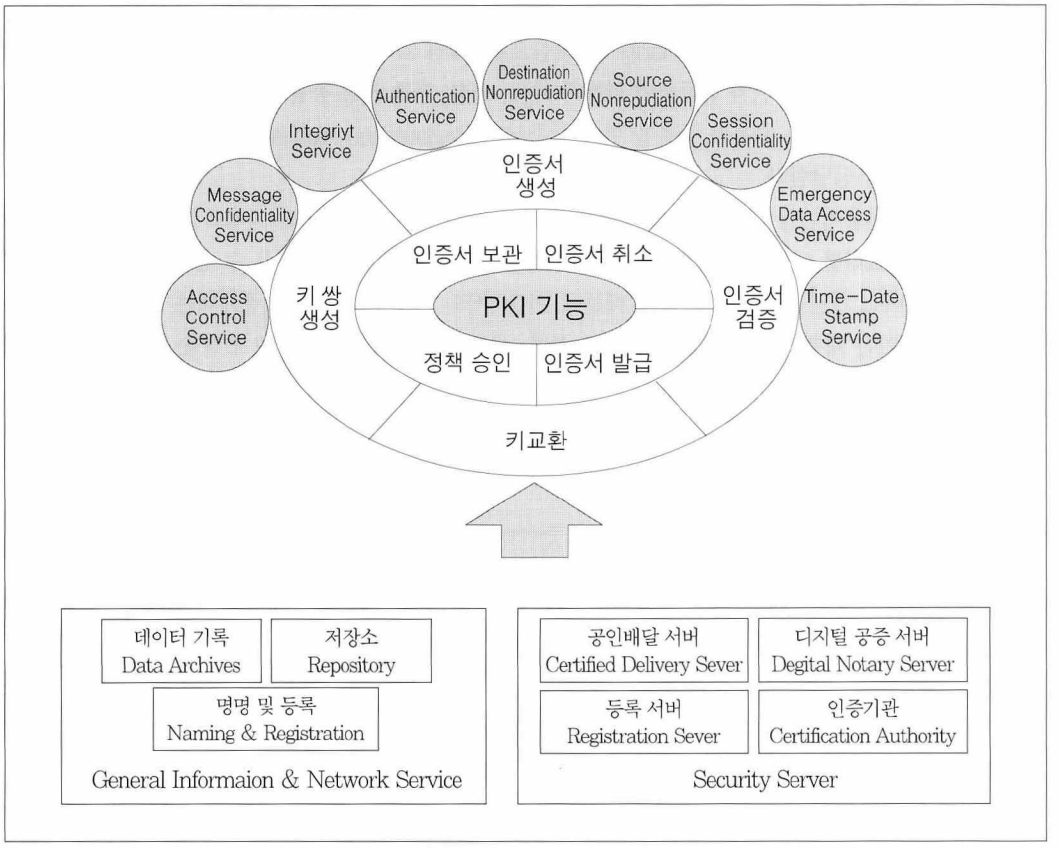
<표2> 암호 알고리즘의 종류

분 류	종 류
대칭키 암호알고리즘	DES, FEAL, BLOWFISH, SAFER, IDEA, RC5, SKILPJACK, CAST, 3DES, AES
공개키 암호알고리즘	RSA, RABIN, ELGAMAL, ECC
해쉬 알고리즘	MD4, MD5, SHA-1, RIPE-MD, HAVAL

IETF의 정보보호 연구 활동

IPsec은 국제 인터넷 표준화 단체인 IETF(Internet Engineering Task Force)에서 연구되고 있는 정보보호기술이다. 이미 IETF는 1994년 인터넷의 당면한 가장 중요한 과제 중의 하나가 "보안 문제"라는데 합의하였고 1993년부터 작업을 시작하여 현재 상당한 진전을 이루고 있다. IPsec은 기본적으로 인터넷을 통해 송수신되는 데이터에 대해 암호 및 인증서비스를 제공하여, 각종 응용 서비스를 보호하고자 하는데 목적이 있다. SSL이나 SET과 다른 점은 현재 우리가 사용하고 있는 TCP/IP를 교체하여야 한다는 점이다.

IPsec의 특징은 다음 몇 가지로 요약될 수 있다. 정보보호 서비스가 IP 계층에서 제공됨으로서 기존의 응용 소프트웨어에 대한 변경을 요하지 않아, 일반 인터넷 사용자에게는 투명한 상태로 처리된다. 응용계



<그림2> PKI의 전체적인 개념도

층 및 트랜스포트 계층의 모든 프로토콜에 공통된 정보보호 서비스를 제공할 수 있기 때문에, 한 호스트 내에서는 일관된 방식의 정보보호 서비스 설정이 가능하다. 또한 특정 알고리즘이나 인증 방식에 국한시키지 않으면서 새로운 정보보호 기술 수용이 용이한 구조를 갖고 있어 국내 암호 기술 적용도 쉽게 이루어질 수 있다. 현재 IPsec이 가장 활발하게 적용되고 있는 가상사설망 분야에서는, IPsec을 대기업 네트워크에 적용시 확장성 및 호환성을 해결할 수 있는 유일한 정보보호 프로토콜로 여기고 있다.

공개키 기반구조

IPsec과 관련하여 현재 인터넷 정보보호에서 가장 큰 이슈로 등장하고 있는 분야가 공개키기반구조(PKI : Public Key Infrastructure)이다. 공개키기반구조를 쉽게 설명하면, 사이버스페이스에서 각 개인에게 개인별 사이버 인감를 발급해 주는 체계라고 할 수 있다. 모든 전자문서에는 개인이 서명을 한다거나 도장을 찍을 수가 없다. 만약 서명을 그림 파일로서 첨부할 수 있을지라도 크래커는 쉽게 서명을 위조할 수 있을 것이다. 좀 더 기술적으로 이야기하게 되면, PKI는 네트워크 상에 연결된 각 사용자 및 메시지에 대한 인증 기능을 제공하기 위하여, 공개키 알고리즘 방식을 이용하는 인증 기반 구조이다. PKI는 인증서를

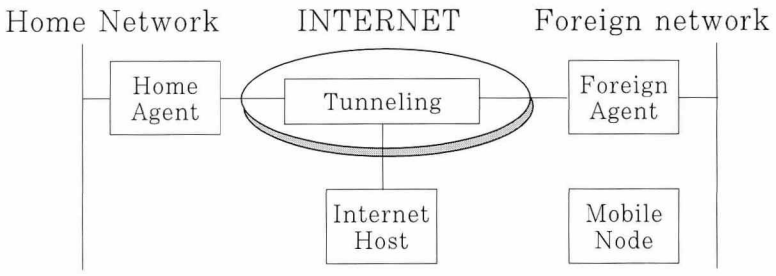
발급하는 인증기관(Certificate Authority)을 중심으로 〈그림 2〉에서와 같이 공개키 값의 효율적이고 안전한 유통을 위해 사용되는 전자 인증서의 발행과 획득, 조회, 검증 기능 등을 수행할 수 있도록 한다. 일반적으로 인증서를 요청하는 사용자 등록을 위해 등록서버(Registration Authority)를 두며 인증기관은 인증서 발급업무만을 담당한다.

PKI에서는 인증기관들에 대한 구성 체계를 통하여 인증서에 대한 관리의 최적화를 도모할 수 있다. 즉, CA간의 신뢰 고리를 어떻게 형성하는가에 따라 해당 PKI의 특성을 결정 지을 수 있다. X.509가 X.500의 디렉토리 서비스 개념을 근간으로 하기 때문에 PKI에서의 가장 기본적인 인증체계는 체계성과 정렬성에 초점을 두고 있는 계층적 구조를 갖고 있기도 하다. 이외에도 체계의 자율성에 초점을 두고 있는 네트워크 구조와 이 두 구조의 장 · 단점을 수용한 혼합형 구조가 있다. 국내에서도 이미 정보보호센타에 루트 CA서버를 두어 독자적으로 국가 인증 체계를 구축하고 있다. IPsec은 PKI를 절대적으로 필요로 하고 있으며, PKI는 전세계적인 Global PKI를 향하여 계속 발전할 것으로 보인다.

이동 인터넷 정보보호

현재 우리가 사용하고 있는 인터넷에서는, 모든 PC에게 유일한 IP 주소가 주어져 있으며, 그 IP 주소는 각 네트워크의 관리자에 의해 관리되고 있고, 다른 네트워크로 이동할 경우 동일한 IP 주소를 사용할 수 없도록 되어 있다. 이는 마치 각 집주소가 살고 있는 지역과 연계되어 있어 이사를 할 경우 다른 집주소를 가져야만 하는 경우와 같다. 그러나 통신이 글로벌화 되어 있는 추세에서 노트북을 갖고 이동할 경우, 네트워크 경계를 넘어설 때마다 IP 주소를 변경하는 것은 매우 불편할 것이다.

이러한 불편을 없애기 위해, 차세대 인터넷에서는 현 인터넷을 개선시켜 이동 컴퓨터에게 유일한 IP 주소를 제공하고, 어느 위치에서라도 이동 컴퓨터의 데이터를 효과적으로 전달하고 받을 수 있도록 하는 이동 IP를 제안하고 있다. 〈그림 3〉에서와 보인 바와 같이 각 네트워크는 에이전트를 두어 MN(Mobile Node)에 대해서 HA(Home Agent) 혹은 FA(Foreign Agent)으로서의 역할을 담당하고 있다. 데이터 전달 과정만을 간단히 살펴보면, HA는 MN이 자신과 같은 네트워크에 있으면 도착한 데이타를 바로 전달해 주고, Foreign 네트워크에 있으면, 데이타를 FA에게 전달한다. FA는 HA로부터 받은 데이타를 MN에 전달시켜 주게 된다.



<그림3> 이동 IP 구조

그러나 이동 IP는 몇 가지 정보보호 관점에서 문제점을 갖는다. MN이 데이타를 전송할 때 발신지 IP주소를 자신의 home address로 하기 때문에 발생하는 IP 주소 위장공격 문제, MN이 전송하는

데이타와 방화벽과의 충돌 때문에 발생하는 문제, MN이 foreign 네트워크로 이동할 때 발생하는 MN 인증 문제, 통신 비밀성 등의 문제가 있다. 이러한 정보보호 관련 문제점들은 IPsec을 이용하여 해결이 가능할 것으로 본다.

이동 IPsec에 대한 연구는 아직 초기단계이며 이동 IPsec에 대한 연구 논문과 초기문서가 일부 발표되었으나, 아직 완성된 표준 규격이나 이동 IPsec을 위한 제품은 없는 실정이다. 현재 Cicso System, SSH, MOEBIUS, NIST 등의 외국의 일부 업체에서 이동 IP와 IPsec 통합을 위한 준비 작업이 진행중이다.

멀티캐스팅 정보보호

차세대 인터넷에서 나타날 중요한 서비스는 멀티캐스팅 서비스일 것이다. 현재 인터넷은 근본적으로 항상 둘만의 통신 채널을 설정하도록 설계되어 있다. 이를 유니캐스팅이라고 한다. 그래서, 한 세션의 보호를 위해서는 비밀키도 오직 두 참여자만이 가질 필요가 있었다. 그러나 화상회의, 원격지 교육, 방송 등과 같은 여러 분야에서 멀티캐스팅 서비스 제공을 위한 연구가 활발해 짐에 따라 통신의 대상도 수천명이 참여할 수도 있는 멀티캐스팅 그룹으로 확장되었다. 멀티캐스팅 서비스를 위해서는 그룹이외의 사용자가 데이터를 볼 수 없도록 데이터가 암호화될 필요가 있다. 이를 위해서 동일한 비밀키를 모든 그룹원에게 배포하여야 한다.

멀티캐스트 그룹은 세션이 진행 되는 도중에 그룹원이 탈퇴하거나 새로 참여하여 동적으로 변하게 된다. 이렇게 그룹이 변함에 따라 탈퇴한 그룹원이 서비스를 받지 않게끔 그룹키는 재분배되어야 하는데, 그룹원의 수가 증가하게 되면 그룹키를 재분배하는데 장시간이 걸리게 된다. GKMP, Iolus등 여러 가지 효율적인 그룹키 분배 알고리즘이 제안되어 왔으며, 현재 IPsec에서도 그룹키 관리를 수용하기 위한 연구가 진행중에 있다.

결 론

IPsec은 지금까지 성공적인 인터넷 표준 중의 한 분야로 언급되고 있다. 이러한 사실은 대부분의 가상사설망 장비 제조 업체들이 기존의 L2TP, PPTP등의 프로토콜을 지양하고 IPsec을 채용하고 있음을 보아도 알 수 있다. 그러나 IPsec이 가상사설망의 주요 기능으로서 또는 다른 응용 소프트웨어에서 널리 사용되기 위해서는 PKI의 보급이 선결되어야 한다. 최근 IETF에서는 IPsec의 좀더 빠른 보급을 위해서 키관리 및 PKI의 미성숙에 따른 문제점을 보완하기 위해 새로운 연구그룹들이 만들어 지고 있다. 앞으로 차세대인터넷 진입을 위해서는 이동 IP의 수용, 그룹키관리, AES를 포함한 다양한 알고리즘의 수용, 성능개선 등의 문제점이 해결되어야 할 것으로 보인다. 이제 IPsec은 단순히 구현 차원을 넘어서 실제 필드에서 적용되었을 때 나타나는 여러 가지 문제들이 보완되면, 조만간 IPsec 사용이 급속히 확산될 것으로 보인다.