通信情報保護學會誌
第5卷 第4號, 1995. 12

ISDN 정보보호 시스템 구조 연구

김 봉 한*, 이 선 우*, 정 기 현**,
신 기 수**, 강 철 신***, 이 재 광*

1. 서 론

현대 사회를 일컬어 정보화 사회라고 한다. 정보화 사회에서는 사회의 주체가 되는 정보를 컴퓨터의 디지털 기술과 통신의 전송 기술의 발달로 인하여 보다 더 정확하고, 신속하게 전송할 수 있게 되었다. 그러나, 사용자의 필요 및 요구에 따라 전송되는 정보는 텍스트 정보, 화상 정보, 음성 정보 등 그 종류가 다양해지고 전송매체도 다양하게 되었다. 따라서, 이러한 모든 종류의 정보를 통합적으로 전송할 수 있는 전송시스템의 필요성에 따라 개발된 새로운 통신망이 종합 디지털 전산망인 ISDN(Integrated Services Digital Network)이다. ISDN은 기존의 전화망, 텔렉스망, 디지털 데이터를 통합하여 디지털 처리할 수 있도록 표준화된 인터페이스를 통하여 다양한 형태의 음성, 비음성 정보 서비스를 동시에 제공할 수 있다.[1]

ISDN은 음성 및 비음성 정보 서비스를 통합하여 종합적으로 제공할 수 있도록 하나의 회선을 통하여 회선 교환망 및 패킷 교환망의 가입자 통신망이 디지털 방식으로 공통 접속을 제공하며, 통신망 내의 데이터베이스 등과 같은 정보 자원들을 공유할 수 있도록 해준다. 그러나, 모든 정보가 디지털 형태로 전송되고 통신망 접속이 개방성을 갖기 때문에 중요 정보 자원에 대한 위협이 날로 증가하게 된다. 또 최근의 통신망에 대한 정보의 침해 사례가 계속 늘어가고 있고 지능화되어가고 있는 실정이다. 따라서, 기존의 통신망과 연동 또는 통합하여 다양한 정보 서비스를 제공하는 ISDN에서의 사용자 중요 정보 자원의 취약성에 따른 불법적인 침입자에 의해 우연 또는 의도적인 침해 위협에 대한 대책이 절실히 요구되는 실정이다. 이를 위해서 종합 디지털 정보망인 ISDN에서는 사용자-망 인터페이스가 디지털화된 음성 및 비음성 정보들을 효율적으로 보호할 수 있는 정보보호 구조 및 프로토콜이 필요하다.

본 논문에서는 NIST의 컴퓨터 시스템 실험실에서 통합된 OSI, ISDN, 정보보호 프로그램 후원하에 작성된 특별 발간 500-189를 중심으로 ISDN 시스템 구조와 프로토콜에 대하여 정보보호 위협과 이를 해결하기 위한 정보보호 서비스, 효율적인 정보보호 서비스를 제공하기 위한 정보보호 시스템 구조와 필요한 프로토콜에 대하여 기술하였다.

* 한남대학교 공과대학 전자계산공학과
** 한국전자통신연구소
*** 한남대학교 공과대학 전자공학과

2. ISDN 정보보호 위협, 환경 및 서비스

2.1 ISDN 정보보호 위협

ISDN에서는 초기 ISDN 음성-중심 네트워크와 현재의 ISDN에서 필요한 정보보호 서비스에 대한 연구도 계속되어 왔으나 사용자 통신 정보에 대한 비밀유지를 보호하기 위한 체계적인 방법이 아직 없을 뿐아니라 침입자의 가로채기, 내용 알아내기, 통신 내용 변경이나 위조 등이 비교적 쉽게 발생할 수 있다. 그래서 ISDN에서는 네트워크 자체에서의 여러가지 유형의 불법적인 행위에 대해 매우 취약한 실정이다. 그리고 네트워크 사용자의 인증을 위한 효과적인 방법인 표준안이 아직 없는 실정이다.

이전의 공중 아날로그 전화망은 네트워크 제어를 위하여 in-of-band 신호방식을 사용하였지만, 현재의 공중망에서 교환기간의 정보는 out-of-band 신호방식으로 변환하여 전송되기 때문에 불법적인 행위를 어느 정도 줄일 수는 있다. ISDN에서 이 out-of-band 신호방식은 별도의 16kbps 디지털 D 채널을 이용하여 로컬루트와 사용자 터미널간의 제어 정보 전송에 사용하고 있다. 그러나 이 정보 전송이 ISDN 공중망에서의 불법적인 행위로 부터 안전하다고 할 수는 없다. ISDN이 공중망으로서 광범위하게 사용될 때 ISDN 터미널-대-네트워크 신호방식은 침입자의 불법적인 공격에 대한 위협을 받을 수 있어서 정보보호에 매우 취약하다. 또 사용자는 D 채널을 통하여 X.25 패킷 서비스를 받을 수 있는데, 이 D 채널을 통한 X.25 시스템에 침입할 가능성이 있다면 정보보호에 대한 노출은 더욱 커지게 된다. 따라서 ISDN에서의 정보보호 서비스에 대한 필요성은 더욱 더 커지고 있다.[11]

ISDN에서는 다음과 같은 정보보호 위협이 발생할 수 있다.

1) 서비스의 부인
2) 네트워크를 이용한 사용자 데이터 침입
3) ISDN을 이용한 사용자 시스템 침입
4) 네트워크를 이용한 불법적인 행위
5) ISDN 통신에서의 비밀유지 정보에 대한 침입
6) 통신 내용의 수정

여기서 서비스의 부인 공격에는 CPE(Customer Permises Equipment), 네트워크 링크와 교환기에 대한 물리적인 손상도 포함되며, 또 실제 침입자에 의한 공격은 아니지만 우연한 사고와 재해도 서비스 정보 손실의 원인이 될 수 있다. 교환기에 대한 공격은 교환 소프트웨어에 침입하여 사용자 호출을 전용하여 특정 사용자에게 피해를 주거나 교환기 자체를 사용하지 못하도록 하여 회선 사용을 못하게 할 수 있다.

또 ISDN에서는 사용자 데이터 뿐만아니라 사용자의 호출(call)에 대한 기록을 안전하게 관리하여 이 정보를 일반 사용자에게는 안전하게 비밀이 보호되어야 한다. 만약 침입자에 의해 네트워크 시스템이 침입을 당하면 침입자가 이 정보를 얻을 수 있다. 그래서 데이터 뿐만 아니라 시스템 관리 정보도 알아내어 네트워크 운영에 커다란 영향을 미칠 수도 있다.

그리고 최근에는 전화망이 불법적인 행위의 주요 도구 중의 하나로서, 이를 이용한 여러가지 불법적인 행위가 있을 수 있다. 전화를 이용한 불법적인 행위에는 개인 신용 기록, 법적인 기록, 전화번호 등의 비밀유지 정보를 알아내는 것이다. 현재 ISDN 전화선을 허가없이 도청하는 것은 불법으로 되어있다. 그리고 최근에 이용자수가 급격히 늘어나고 있는 셀룰러나 무선전화도 정보보호에 매우 취약하다. 따라서 ISDN에서 정보보호 서비스는 절대적으로 필요하다고 할 수 있다.

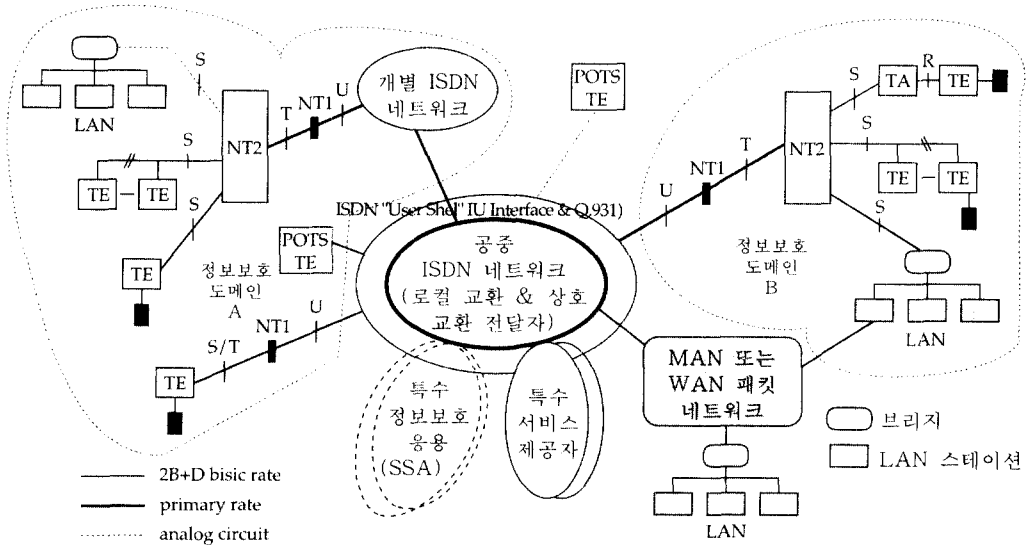
2.2 ISDN 정보보호 환경

[그림 1]은 ISDN에서 정보보호 서비스를 제공해야 하는 환경을 나타내고 있다. ISDN 정보보호의 시작은 사용자로서, 이 사용자는 정보보호가 필요한 사람, 기관 엔티티, 또는 사람이나 엔티티에 대한 컴퓨터 처리 활동일 수 있다. 사용자는 특정 선로나 터미널에 대해 제한을 받을 수 있고, 받지않을 수도 있다. 또 사용자는 이동성이 많아서 지리적으로 넓은 범위의 거래를 위하여 간단한 전화기를 사용한다면, 일반 ISDN 전화에서의 사용자에 대한 신뢰할 수 있는 인증은 매우 중요한 문제가 된다.

사용자는 ISDN 터미널 장비(TE: Terminal Equipment)를 이용한다. TE는 음성 전화, 자동응답기, 통합 음성/데이터 터미널 팩시밀리, 자동 텔레머신과 같은 특정 터미널이 될 수 있다. 대부분의 경우에 TE는 ISDN 인터페이스 장치 또는 카드 등을 통하여 ISDN 망과 연결된 장치이다. TE가 컴퓨터인 경우 사용자는 사람 또는 기관 엔티티를 위한 대리인으로서 역할을 수행하는 컴퓨터 프로세스가 된다. TE는 ISDN 망과 직접 연결되거나 ISDN 공중망과 순서에 따라 연결된 PBX와 연결될 수 있다. ISDN 용어에서 PBX는 네트워크 단말장치 2 또는 NT2가 된다. 일괄적으로, TE와 NT2 장치를 사용자 댁내 장치(CPE)라고 한다.[5]

공중망은 망에 대한 불법적인 행위와 서비스 가용성(availability)에 대한 위협으로 부터 보호되어야 한다. 따라서 망 서비스 제공자는 이에 대한 보호 서비스를 반드시 제공해야 한다. 또 서비스 제공자는 고객 서비스 기록에 대한 비밀유지를 해야 한다. 공중망은 매우 다양하기 때문에 사용자-대-사용자 정보보호인 비밀보호와 인증에 대해서 완전한 보장을 기대할 수 없다. 그리고 현재는 정보보호 프로그램을 강요하거나 관리할 수 있는 기관이 없는 실정이다.

특수 서비스 또는 텔레서비스인 응용층 서비스가 ISDN을 통하여 사용자에게 제공되고 있다. 이 특수 서비스에는 디렉토리 서비스



[그림 1] ISDN에서의 정보보호 환경

(X.500), 패킷 메시지 처리 서비스(X.400)를 포함한 여러가지 응용 서비스가 있다. X.400과 같은 텔레서비스는 일반 응용 서비스에 정보보호 서비스를 통합시킬 수 있다. 특수 서비스 제공자는 키 관리같은 정보보호 응용을 제공하게 된다. 여기서 정보보호 중심 응용은 특수 정보보호 응용(SSA:Specialized Security Application)이라고 한다. 그리고 특수 서비스에 추가해서 패킷 처리기는 공중망의 한 부분으로서 패킷 서비스를 제공하는 망 교환기에 통합할 수 있다. 독립된 패킷망은 로컬 교환기로 연결될 수 있다. 따라서 안전한 망에 포함된 다양한 패킷망 서비스는 로컬 교환기를 통하여 액세스될 수 있다.

서로 다른 정보보호 영역에 있는 사용자는 ISDN 망을 통하여 서로 통신하게 되는데, 공중 ISDN에는 사설 ISDN 망이 연결될 수 있고, 그리고 LAN, MAN, WAN 등의 여러가지 데이터망은 게이트웨이를 통하여 공중 ISDN 망과 연결된다. 아날로그 전화 서비스는 공중망에서 계속해서 제공될 것이다. ISDN을 통한 사용자-대-사용자 정보보호는 CPE에서 필요하게 된다. CPE에서 적용된 정보보호 해결책은 ISDN 뿐만 아니라 모든 통신에서 이루어져야 한다.

2.3 ISDN 정보보호 서비스

ISDN 정보보호 서비스는 OSI 정보보호 서비스와 ECMA 138에서 정의한 정보보호 서비스를 기본으로 한다.[13]

2.3.1 무결성 서비스

무결성 서비스는 무결성 체크값(ICV: Integrity Check Value)에 의해서 디지털 데이터를 위하여 제공되는데, 이 ICV는 개별(private) 또는 비밀 키에 의해 암호화되므로 침입자는 패킷을 수정하고 수정된 패킷의 ICV를 계산해 낼 수는 있지만 다시 ICV를 암호화할 수는 없기 때문에 패킷의 변경을 검색할 수 있다. 그리고 ICV에 타임스탬프 필드를 추가하면, 연결 재생 공격을 막을 수 있다. 또 ICV의 범위 내에 순서 번호 필드를 포함시켜서 완전한 연결 무결성으로 확장할 수 있다.

2.3.2 부인 봉쇄 서비스

메시지는 메시지 발신자만 알고있는 개인 비밀 키로 패킷이나 메시지의 ICV를 암호화하는 방법으로 사인(서명)될 수 있다. 만약 메시지가 날짜와 시간을 가지고 있으면, 수신자는 도착 시간을 조사해서 메시지의 서명된 사본을 가지고 발신자 증명을 이용하여 부인-봉쇄를 할 수 있다.

배달자 증명에 의한 부인 봉쇄의 목적은 수신자가 메시지를 받았으면서도 받지 않았다고 부인하는 것을 방지하고, 배달자 증명에 의한 부인 봉쇄는 만약 수신자가 받은 메시지에 서명하고 그것이 타임스탬프와 함께 발신자에게로 돌아온다면 가능해진다. 이 메카니즘은 완전한 해결책은 아니다. 왜냐하면 수신자가 그 메시지를 받아서 읽었음에도 불구하고, 수신의 확인을 위한 서명을 거절할 수 있기 때문이다. 만약 전자 통신이 등기우편 또는 프로세스 서버를 대신하려면, 수신자의 협력이 필요없는 메카니즘이 요구된다.

2.3.3 비밀유지 서비스

비밀유지는 종단-대-종단 암호화, 망의 완전한 물리적 보호, 또는 데이터가 지나가는 각 서브망이나 링크가 암호화 또는 물리적 수단에 의하여 보호되는 데이터 경로를 통한 안전한 라우팅에 의하여 제공된다.

암호화의 비용이 거리에 따라 증가하는 것이 아니기 때문에, 암호화는 ISDN과 같은 WAN에서 비밀보호를 보증하기 위한 중요한 메카니즘이 된다. 암호화는 OSI 모델의 어떤 계층에라도 위치할 수 있으며,(ICV와 적당한 메시지 순서 번호와 결합하여) 비밀유지와 무결성 서비스를 제공한다.

암호 알고리즘은 다음과 같이 두개의 일반적인 클래스로 분류된다.

(1) 대칭(Symmetric) 혹은 비밀(Secret) 키 알고리즘: 여기에서 송신측과 수신측 모두 같은 비밀 키를 사용한다. DES와 Fast Data Encipherment Algorithm FEAL-8이 그 예인데, 이 알고리즘들은 계산상으로 효율적이다. 그리고 DES는 보안성에 대한 신뢰를 받고 있다. 다만 대칭 키 알고리즘에서의 가장 어려운 점은 비밀 키 관리의 어려움이다.

(2) 공개 키와 개별 키 두가지를 다 사용하는 공개(Public) 키 알고리즘: 가장 일반적인 것은 평문은 공개 키로 암호화 되고, 개별 키로 복호화되거나, 개별 키로 암호화되고, 공개 키로 복호화되는 것이다. 어떤 경우에는 이 알고리즘은 송신측과 수신측이 안전하지 않은 링크 상에서 비밀 키를 안전하게 교환하게 해준다. Diffie-Hellman 알고리즘과 Rivest, Shamir, Adleman (RSA) 알고리즘이 현재까지 알려진 것 중에서 가장 우수한 알고리즘들이다. 이 두 알고리즘은 다른 알고리즘들과 마찬가지로 그들의 속도를 제한하는 큰 수의 지수 계산, 집중적인 계산 처리 등을 요구한다. 이 두 알고리즘을 깨는 것은 수학 분야에서 집중적으로 연구되어 온 어려운 문제, 즉 이산 로가리즘 문제와 매우 큰 숫자의 인수분해 문제 등과 거의 대등하게 어렵다고(비록 증명되지는 않았지만) 믿어지고 있다.

그리고, 대칭 키와 공개 키 암호화 방법이 각각의 장점을 살려 한 시스템에서 결합될 수 있다. 예를 들어서 X.25 암호화 시스템에서 공통 비밀 DES 세션 키를 유도해 내기 위하여 Diffie-Hellman 알고리즘을 사용하고, 인증과 서명을 위해서는 RSA 알고리즘을 사용할 수 있다.

2.3.4 인증 서비스

디렉토리 인증을 위한 주요 골격은 ISO/IEC 9594-8이며, OSI 인증 골격 초안 [JTC1 1]은 OSI를 위한 인증 골격 초안을 제공한다. 디렉토리 응용(X.500)은 디렉토리 정보 베이스(DIB)에서 이름 붙여진 대상들에 관한 속성 정보를 위해 저장 장소를 제공한다. 디렉토리는 디지털 서명 장치 메카니즘을 제공하는데, 이 메카니즘은 사용자가 인증서 발급기관에 의해서 DIB내에 위치한(사용자의 공개 키를 포함하는) 정보들을 확인하도록 해준다. 디렉토리의 주요 정보보호 특징은 사용자들과 그들의 공개 키들 간의 안전한 매핑(mapping)을 제공하는 것이다.

ISO/IEC 9594-8은 두 클래스의 인증을 정의하는데, 하나는 단순 인증(Simple Authentication)이고 또 다른 하나는 강력한 인증(Strong Authentication)이다. 단순 인증 절차는 사용자에게 알려진 비밀 키에 의존한다. 사용자 A의 이름과 패스워드가 타임 스탬프 및 난수와 함께 B로 전달된다. 패스워드는 단방향 해쉬함수에 의해 보호된다. 예를 들어서, 단순 인증 방법에서는, A는 타임스탬프, 난수, A의 식별 이름들로 구성된 인증자를 B에게 보낸다. 이들 보호된 파라미터들은 처음 3개의 파라미터들과 A의 비밀 패스워드로부터 단방향 해쉬함수에 의해 생성된다. B는 보호 파라미터들을 만들기 위하여 A의 패스워드의 로컬 사본을 액세스 하여 A로부터 받은 보호

파라미터들과 비교한다.

ISO/IEC 9594-8은 ISDN 인증에 기초를 둔 디렉토리의 기반을 제공한다. ISDN 사용자는 특별한 TE로 한정될 수 있는데, 이 경우에는 인증 처리, 키, 패스워드 등이 TE에 저장된다. TE에 대한 액세스는 물리적으로 제어되거나, 사용자가 TE를 인증할 수 있거나, 혹은 물리적인 토큰의 소유자가 사용자의 인증을 위하여 TE에게 요구함으로써 원격 TE들을 인증한다. 이같은 방식에서는 ISDN이 보통 OSI 인증에 추가로 별도의 장치를 둘 필요가 없다.

그러나, ISDN 사용자는 특별한 터미널의 사용으로 한정되지 않는다. 그들은 어떤 ISDN 전화 터미널이라도 사용할 수 있으며, 그것으로 부터 인증을 받기를 원한다. 터미널을 위한 보다 좋은 인증 서비스가 없을 경우 Calling line ID 부가(supplimentary) 서비스가 인증을 위해 사용될 것이다. 이 서비스는 비록 사업자 측면에서는 유용하지만(예를들면 전화가 왔을 때 고객 기록의 자동 검색), 각 개개인의 인증 수단으로는 믿을 수 없다. 더구나 개개인은 그들의 집에 있는 전화가 아닌 다른 어떤 터미널로부터라도 서비스를 액세스할 수 있기를 원한다.

2.3.5 액세스 제어 서비스

통신망 자체는 데이터를 저장하지 않기때문에, ISDN과 같은 통신망의 관점에서의 액세스 제어는 분산 컴퓨터 시스템만큼 복잡하지는 않다. ISDN 정보보호를 위해서는 망 액세스, 터미널 또는 CPE 액세스, 그리고 망 데이터베이스 액세스의 3가지 관점에서 생각할 수 있다.

ISDN 액세스 제어는 '사용자가 망을 사용할 권한이 있는가?', '혹은 망에서 어떤 특수 서비스를 받을 권한이 있는가?' 이다. 예를 들면, '사용자가 장거리 전화, 국제 전화, 또는 안전한 전화를 사용할 권한이 있는가?' 이다. ISDN PBX를 설치할 경우, PBX는 사용자 액세스 제어 체크를 요구한다. 표준 규격이 PBX에서의 이같은 서비스를 위하여 꼭 필요하지는 않지만, 이것에 대한 표준 규격이 없으면 터미널 상호 교환 능력은 부실하게 된다. 가장 간단한 해결 방법은 터미널에 대해 액세스 특권을 제어하는 것이다.

터미널은 내부 액세스 제어 및 외부 액세스 제어 방법을 가질 수 있다. 내부 액세스 제어는 '사용자가 터미널로부터 어떤 특별한 형태(전화 등급 및 수신처)의 전화를 할 수 있는가?' 이며, 외부 액세스 제어는 '전화를 거는 사람이 이 터미널을 사용할 권한이 있는가?' 이다. 외부 액세스 제어는 표준안이 없어도 터미날에 구축될 수 있다. 즉, 토큰 또는 패스워드가 터미널을 사용할 때 요구될 수 있다. 그러나 내부 액세스 제어는 표준안을 요구한다. 현재 유일하게 표준화된 ISDN 서비스는 Calling line ID 부가 서비스이다. 터미널들(또는 PBX들)은 명확하게 허가된 것 이외의 어떤 번호로 부터 call을 받아 들이는 것을 거절한다. 이것은 강한 인증이 구축되어있지 않을 경우에 강한 액세스 제어보다도 더 좋은 메카니즘이다.

망 데이터베이스(PBX에 의해 관리되는 데이터베이스 포함)에 대한 액세스 제어는 필수적이다. 전화 통화 내력에 대한 데이터베이스는 비밀 사항이며, 비인가된 사용자가 이를 액세스하는 것을 막아야 한다. 망의 관리, 유지보수, 그리고 라우팅을 위해 유지되는 데이터베이스는 비인가된 수정으로부터 보호되어야 한다. 침입자가 이를 수정하거나 망의 운영을 붕괴할 수 있기 때문이다.

2.3.6 ISDN을 위한 ECMA-138 정보보호 서비스

ISO 7598-2의 5가지 정보보호 서비스 외에, ECMA 138에서 소개된 개념을 ISDN 서비스

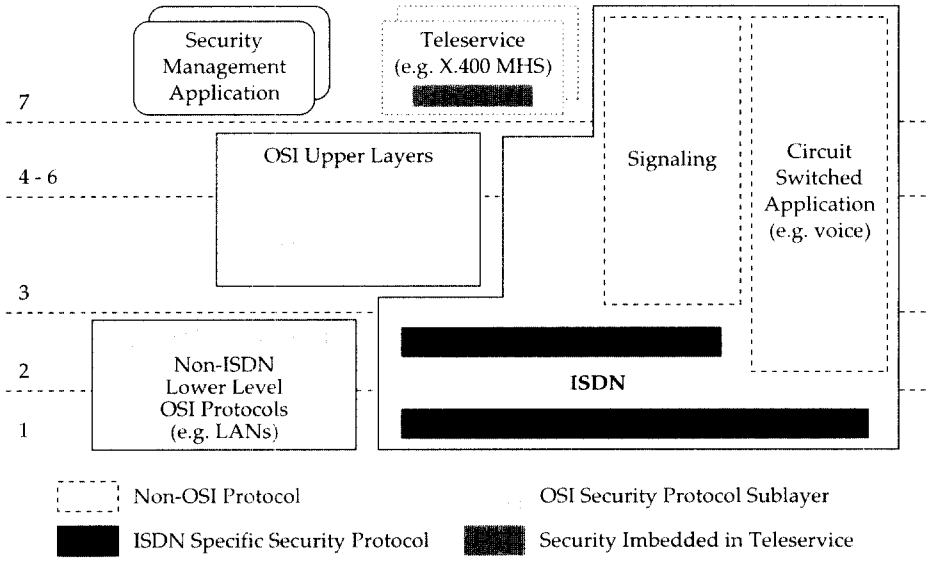
에 확장하는 것은 매우 유용하다. ECMA 138은 분산 컴퓨터 시스템에서의 인증과 액세스 제어를 다루고 있으며, 정보보호 속성 서비스와 내부 도메인 서비스뿐만 아니라 Privilege Attribute Certificates(PAC)의 개념을 기술하는데, 이것은 액세스 제어와 인증을 위한 액세스 방법을 제공한다.

ECMA는 공개 키를 사용하여 정보보호 속성에 디렉토리 증명서(Directory Certificates)를 추가한 PACs로 확장하였다. ECMA 138은 서로 다른 정보보호 영역간의 상호 작용을 고려하였다. 그리고 정보보호 속성 서비스를 요구하고 라벨된 객체들에 대한 속성을 변환하거나 대응시키는 정보보호 속성 서비스(SAS: Security Attribute Service)와 영역들간에서 PAC를 변환하고, 이를 다시 봉인하는 내부도메인 서비스를 가정한다.

일반적으로 ECMA 정보보호 개념은 ISDN에서 두 가지 특정 문제를 응용할 수 있다. 하나는 ISDN 망 데이터베이스 액세스 제어이고, 또 하나는 내부도메인(Interdomain) 정보보호 상호 작용이다.

3. ISDN 정보보호 프로토콜과 응용

ISDN 정보보호를 위한 일반적인 구조는 [그림 2]와 같이 정보보호 프로토콜과 정보보호 응용들로 구성된다. 이 구조는 정보보호 서비스들의 구현을 위한 것으로 정보보호 프로토콜은 트랜스포트층 또는 그 아래 계층들에서 수행되는 대등-대-대등 프로세스를 의미한다. 정보보호 프로토콜은 비밀유지, 무결성, 그리고 데이터가 교환되는 동안 정보보호 라벨링(labeling)을 제공한다. 정보보호 응용은 정보보호 프로토콜을 지원하는 응용 계층에서의 프로세스들이다. 정보보호 응용의 기능은 인증(authentication), 액세스 제어, 그리고 정보보호 속성 등의 기능을 포함한다. 정보보호 응용은 믿을 수 있는 특수한 서비스 응용 또는 제3자를 요구할 수 있다. 정보보호 응용은 안전한 연결, 또는 종료되는 과정에서 요청되어진다.



[그림 2] ISDN/OSI 정보보호 구조

3.1 정보보호 프로토콜

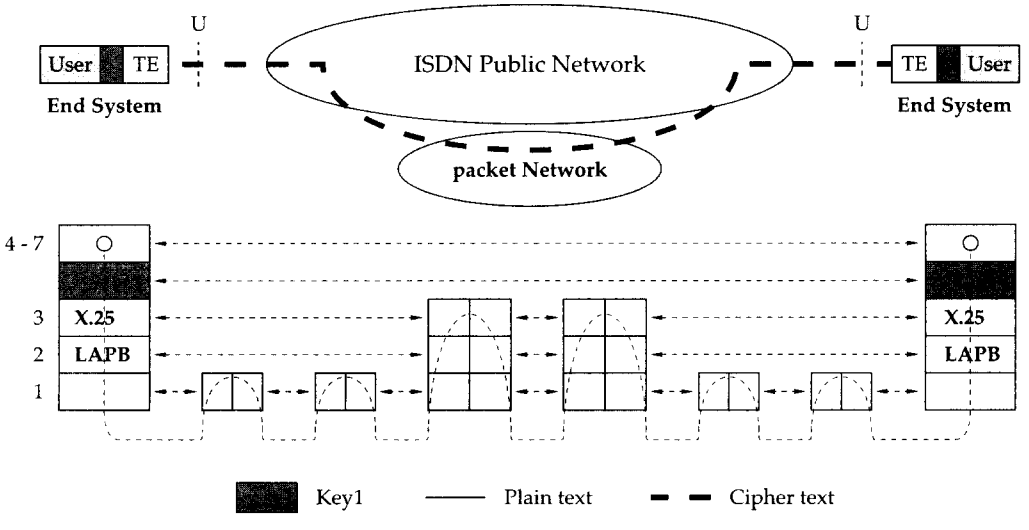
정보보호 프로토콜의 종합적인 기능은 안전한 데이터의 교환이다. 정보보호 프로토콜의 첫번째 기능은 무결성이며, 두번째로 중요한 기능은 비밀유지이다. 비록 비밀유지가 안전한 라우팅에 의해 제공된다 하더라도, 무결성과 비밀유지는 보통 암호 기술로 구현된다. 또한, 정보보호 라벨은 정보보호 프로토콜에 의해 제공되며 정확한 키의 사용은 패킷 단위의 인증 수단을 제공한다. 일반적으로 인증, 엑세스 제어, 키 관리, 공증같은 기능들은 주로 정보보호 관리 응용으로 구현된다.

3.2 ISDN에서의 정보보호 프로토콜

SDNS는 ISDN의 3, 4 계층들에서 OSI와 DoD 프로토콜 스택들과 함께 사용되기에 적합한 정보보호 프로토콜들을 정의한다. ISDN이 OSI(또는 DoD1) 프로토콜 스택의 한부분으로 사용될 때 이 프로토콜들은 ISDN과 연합되어 적합한 ISDN 상에 존재한다. 이 프로토콜들은 OSI 표준 정보보호 프로토콜의 개발을 위한 시작점을 제공할 것으로 기대된다.

[그림 3]은 ISDN의 계층 3과 계층 4에 위치한 특정한 SDNS 프로토콜의 위치를 보여주고 있다. OSI 패킷 데이터 스택들이 네트워크 계층 연결의 일부를 제공하는 ISDN을 사용하는 곳에서는, SP4와 같은 트랜스포트 정보보호 프로토콜은 강력한 종단-대-종단 비밀유지 서비스를 제공할 수 있다. [그림 3]은 패킷망을 위한 B채널 연결을 보여주고 있다. 이것은 D 채널 패킷 사용자 데이터 서비스에서도 같은 방법으로 적용된다. [그림 3]에서 패킷망은 로칼 오피스 교환기의 패킷 핸들러(packet handler)에 의해 구현될 수 있으며, 혹은 회선 교환을 통하여 도달될 수 있는 독립된 망으로 구현될 수 있다. 그러므로, 패킷망은 LAN 또는 완전히 ISDN으로부터 독립된 다른 망일 수 있다.

U 인터페이스점을 감시하는 침입자는 네트워크 계층 헤더를 평문으로, 그리고 트랜스포트 PDU를 암호문으로 볼 수 있다. 네트워크 헤더와 주소가 평문이고 패킷의 크기와 빈도



[그림 3] 트랜스포트 계층 단-대-단 부호화

수가 명확하기 때문에 트래픽의 분석은 매우 쉽다.

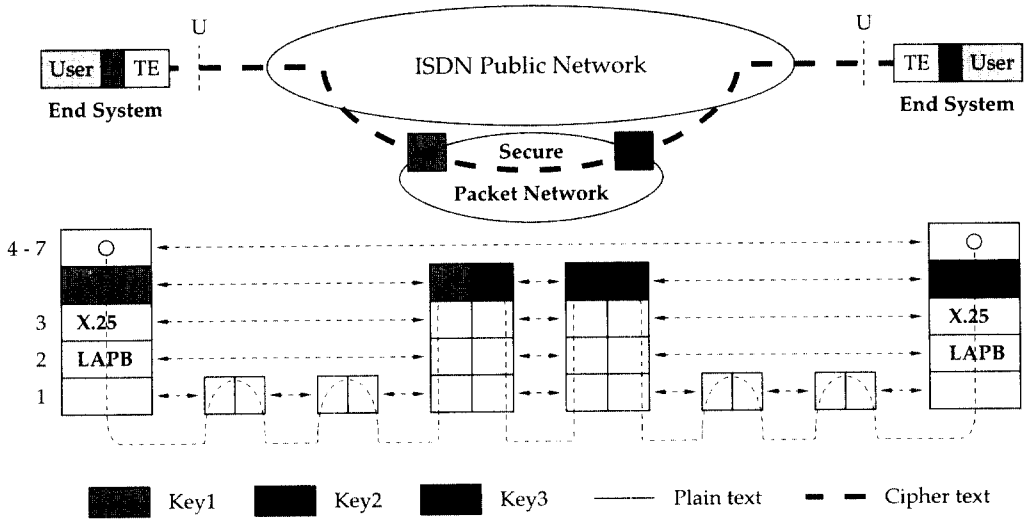
SP3 프로토콜들도 다양한 방법으로 ISDN 상에서 사용될 수 있다. [그림 4]는 서브 망 간의 B 채널 데이터를 암호화하는 네트워크 계층 암호화 방법을 보여주고 있다. 이 방법은 수신처에 관계없이 안전한 패킷 통신을 위하여 단지 하나의 키가 사용되기 때문에, 터미널들을 위한 키 관리가 단순하다는 장점이 있다. 그러나, 적어도 패킷 교환기 내에는 red data가 존재하기 때문에 패킷망을 믿을 수 있어야만 된다는 단점이 있다.

[그림 5]는 SP3 프로토콜의 좀 더 일반적인 사용 예를 보여주고 있다. [그림 5]에서 두 개의 SP3 프로토콜을 포함하는 X.25 게이트웨이가 블랙 공중망을 통하여 두 개의 red LAN을 연결한다. 여기서는 게이트웨이들이 모든 목적지 게이트웨이를 위한 키를 관리해야 한다. 공중망을 통한 게이트웨이간에 암호를 이용한 정보보호가 제공된다.

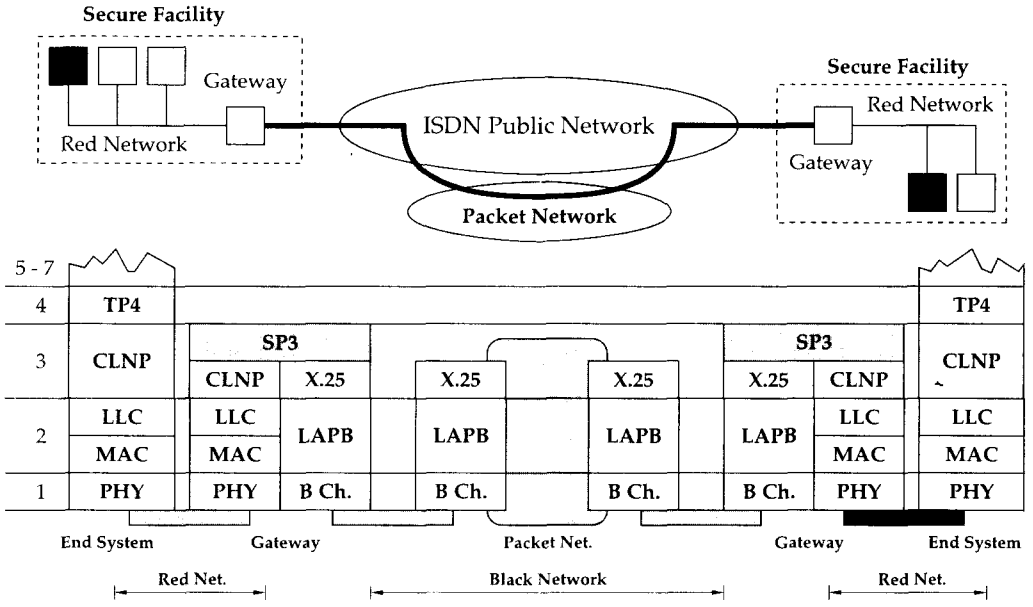
ISDN을 위한 네트워크층 암호화의 단점은 트래픽이 많을 때 안전한 게이트웨이가 병목점이 될 수 있다는 것이다. X.25를 위한 프로토콜 처리는 망 성능에 제한을 가져오며, SP3 프로토콜은 프로세싱 부하를 증가시킨다. 만약 프레임 릴레이 안전 게이트웨이가 사용되어진다면, 정보보호 프로토콜 처리는 게이트웨이의 성능에 상대적으로 더욱 큰 영향을 미치게 된다. 그리고 물리적으로 에러 복구가 의도되어진 종단 시스템의 트랜스포트층으로부터 정보보호 프로토콜을 분리한다.

3.3 ISDN용 정보보호 프로토콜

정보보호 프로토콜은 OSI 참조모델의 모든 계층에서 가능하며, X.400 MHS와 같은 응용에서도 응용 자체에 암호를 이용한 정보보호가 가능하다. 이것은 ISDN을 포함한 여러 망을 통해 접속되는 서비스에 대한 정보보호를 제공할 것이다. 선택된 필드의 비밀유지는 표현층에서 제공되며, 트랜스포트층과 네트워크층 SP3의 윗부분과 SP4 프로토콜은 OSI 정보보호 프로토콜 구축을 위한 기반을 제공한다. 적합한 상위 계층 OSI 정보보호 프로토콜이



[그림 4] 망 계층 패킷 부호화(1)



[그림 5] 망 계층 패킷 부호화(2)

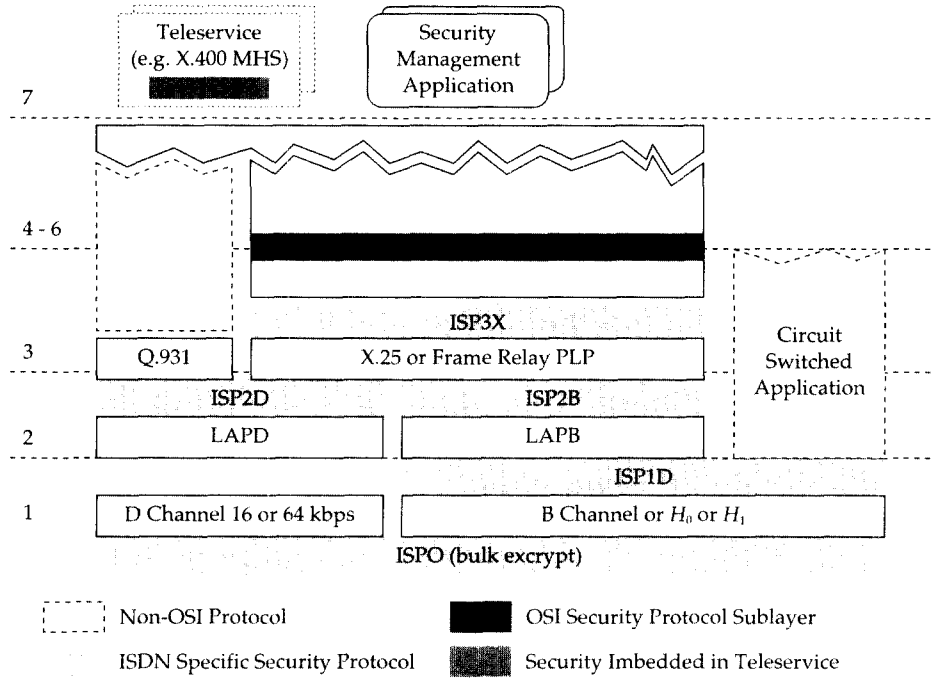
이용될 경우에는, 트래픽 흐름의 비밀유지를 제공하는 것을 제외하고는, ISDN을 위한 특별한 정보보호 프로토콜은 필요하지 않다. 그러나, 음성이나 비디오같은 많은 ISDN 응용은 OSI 프로토콜들에 의하여 제공되지 않는다. OSI가 아닌 데이터 트래픽들도 ISDN 공중망에 의하여 전달된다. 이 같은 경우에는 적당한 ISDN 정보보호 프로토콜들이 필요한 정보보호를 제공할 수 있다.

[그림 6]은 ISDN 정보보호 프로토콜이 위치할 수 있는 다양한 위치들과 암호화, 비밀유지, 그리고 무결성을 위한 프로토콜의 가능한 위치를 나타낸다. 여기서 ISDN 정보보호 프로토콜들은 이름과 ISPnx에 의하여 식별된다. 여기에서, n은 그 프로토콜이 속하는 OSI 계층의 번호를 나타내고, x는 X.25의 특정 프로토콜, 혹은 B 채널, D 채널 프로토콜을 의미한다.

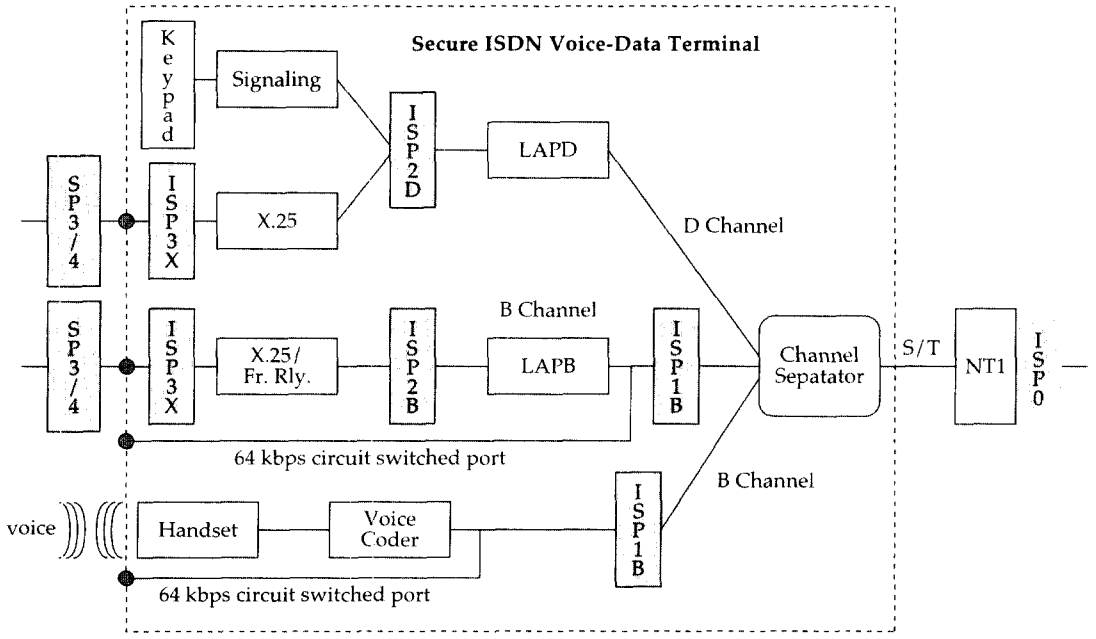
[그림 7]은 안전한 ISDN 음성-데이터 터미널의 블록다이아그램을 나타낸다. 이 그림에서 각 프로토콜은 터미널내에서 구현될 수 있음을 알 수 있다. 또한, [그림 8]은 ISDN 교환기 또는 패킷 핸들러에서 각 프로토콜이 구현됨을 보여주는 블록다이아그램이다.

ISP3X 프로토콜은 X.25(혹은 프레임릴레이)에 적용되는 게이트웨이-대-게이트웨이 프로토콜이다. 비록 이것은 비밀유지와 인증 서비스를 제공하지만, 이것의 중요한 목적은 X.25 게이트웨이 또는 터미널로부터 다른 X.25게이트웨이 또는 터미널까지 상위 계층과 독립적으로 연결하여 무결성을 제공하는 것이다. 만약 모든 트래픽이 적합한 SP3 또는 SP4 프로토콜을 사용할 경우, ISP3X 프로토콜을 반드시 사용하여야 할 이유는 없지만, ISP3X 프로토콜은 서로 다른 프로토콜 환경에서 상위 계층 프로토콜과 관계없이 정보보호를 수행한다.

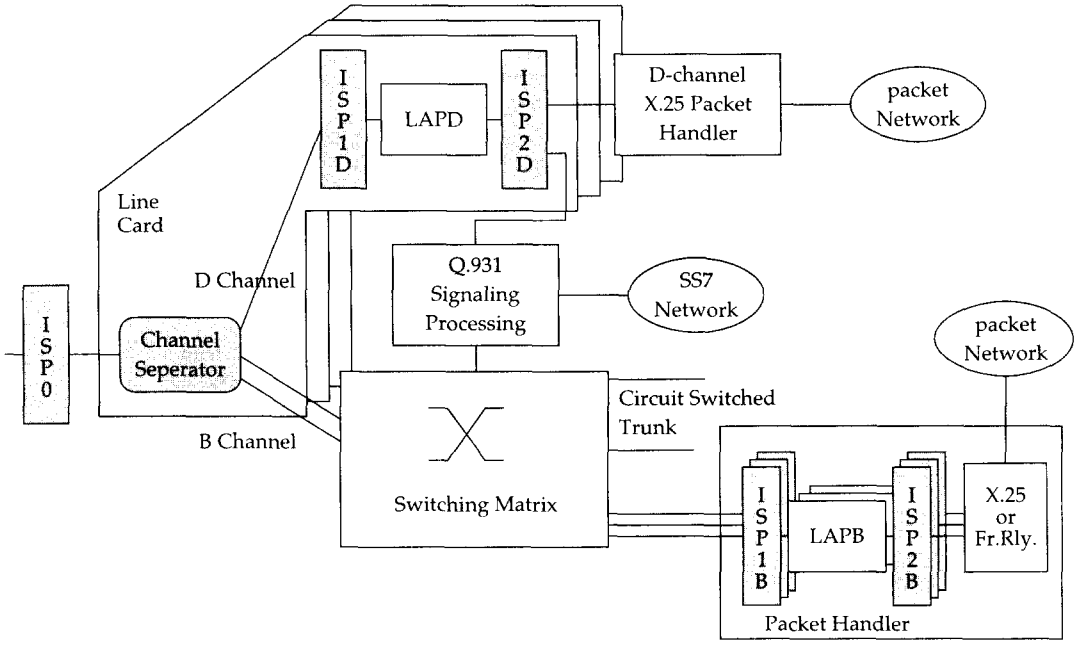
ISP2B와 ISP2D 프로토콜은 LAPB 또는 LAPD 링크 계층 프로토콜 바로 상위에 존재한다. 이들은 링크 계층 프로토콜이기 때문에, 교환기(ISP2B) 또는 패킷 핸들러(ISP2D)의



[그림 6] ISDN 정보보호 프로토콜



[그림 7] 안전한 ISDN 터미널 블록다이아그램

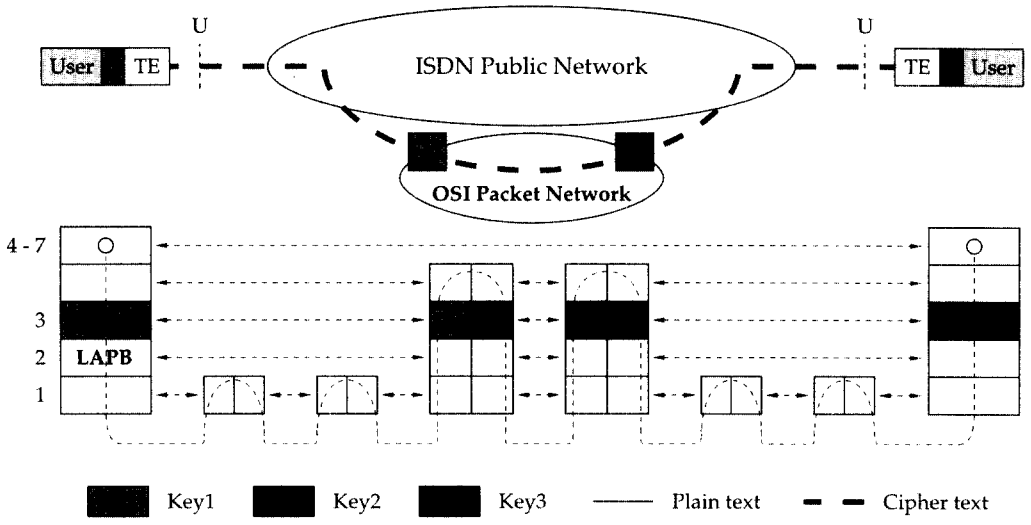


[그림 8] 안전한 ISDN 교환기 블록다이아그램

라인카드상에 구현된다. D 채널이 B 채널의 호 연결을 위해 사용될 때, ISP2B 프로토콜은 목적지 주소 트래픽 흐름의 비밀유지를 제공한다. 그러므로 U 인터페이스를 감시하는 침입자는 호 연결이 되는 것을 알수는 있으나, 정확한 수신처는 어디인지 알 수 없다. 정보보호 기능을 갖는 라인 카드의 대체는 비교적 쉽지만, 기존의 교환기를 이용하여 키 관리를 하기는 어렵다. 그러나, 이 문제를 라인 카드나 TE로 한정하고 일상의 교환 관리 기능을 배제하는 자동 키 관리 개념을 이용하면 가능할 것이다. 이것은 이 레벨의 정보보호 기능을 제공하지않는 교환기에서 안전한 라인 카드의 대체를 허용한다.

[그림 9]와 같이 ISP2B 프로토콜은 패킷 핸들러내에 구현될 수 있다. 중요 장점은 트래픽 흐름 비밀유지를 제공하는 것이다. 즉, X.25 호출 요구, incoming call, 그리고 DTE 주소를 가진 X.25 제어 패킷을 보호할 수 있다. 따라서 DTE와 패킷 핸들러간에 비연결 무결성과 비밀유지가 제공된다. B 채널을 통하여 DTE와 DTE간에 X.25가 직접 사용될 경우에는, ISP2B 프로토콜이 DTE-대-DTE 비밀유지를 제공한다. 그러나 이 경우에는 ISP2D에 목적지 주소 비밀유지 기능이 제공되어야 한다. LAPB 프로토콜에 의하여 허가되는 패킷의 정보보호 헤더와 트레일러의 오버헤드는 문제점을 가지고 있다. 보다 큰 패킷을 수용하면서 X.25의 페이로드(payload)를 유지하려면 LAPB의 수정이 요구된다.

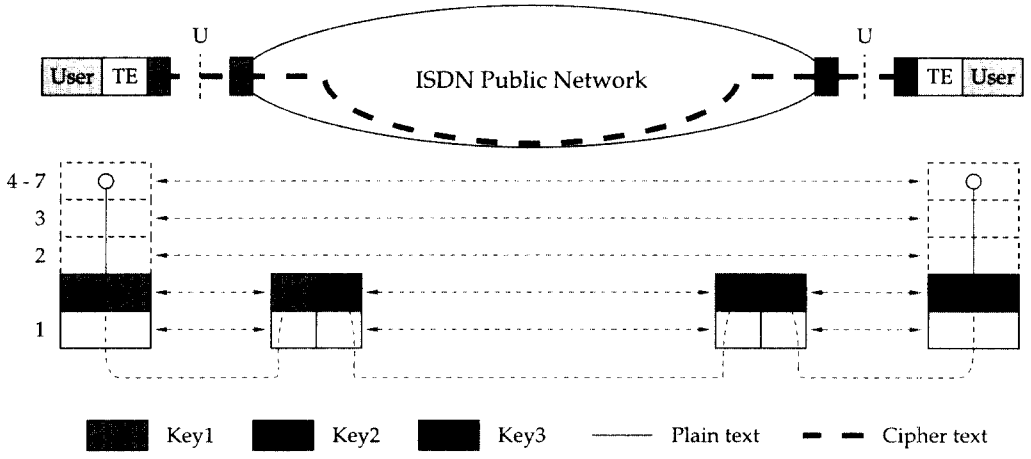
ISP1B 프로토콜은 B 채널의 제일 상위에 위치하며, 완전한 64 kbps 비트 스트림을 암호화한다. 비슷한 프로토콜들이 H0 또는 H1 비트율의 서비스를 위하여 적용될 수 있다. 이 프로토콜은 인증을 이용하여 시작하고(호출 설정동안 D 채널 사용자-대-사용자 신호방식 특수 서비스), 전송되는 모든 비트들을 위한 링크 비밀유지를 제공한다. 무결성은(데이터를 감소없이) 투명하게 제공되지는 않는다. 그러나, 대부분의 상위 계층 프로토콜들은 비밀



[그림 9] 데이터 링크 계층 패킷 암호화

유지와 연결될 때 패킷의 변경이나 재생을 거의 불가능하게 만드는 무결성 검사 기능을 제공한다. B 채널을 감시하는 침입자는 몇 개의, 그리고 어떤 크기의 패킷들이 전송되었는지 알 수 없기 때문에, 부분적인 트래픽 흐름 비밀유지가 제공된다. B 채널 패킷(예: X.25 호출 요구 패킷)에 포함된 주소는 숨겨진다. 그러나 D 채널이 보호되지 않는다면, D 채널을 감시하는 침입자에 의해서 B 채널 호출의 목적지와 사용 시간 등이 알려질 수 있다.

패킷 트래픽에만 적용되는 상위 계층 프로토콜들과는 달리 ISP1B 프로토콜은 음성, 비디오, 그리고 패킷 서비스를 포함하여 모든 B 채널의 사용을 보호한다. [그림 10]은 TE와 교환기사이에서 B채널을 보호하는 이 프로토콜의 사용을 보여주고 있다. 이 방법은 터미널



[그림 10] TE와 망 물리 계층간 암호화

에서의 키 관리는 간편하게 할 수 있으나, 레드 스위치와 망을 요구한다. 특별히 안전한 교환기와 이 교환기들 사이에 안전한 트렁크들을 사용하는 특수한 ISDN 망은 특정 응용을 위해서는 실용적이지만, 공중 ISDN 망의 관점에서는 실용적이지 않다.

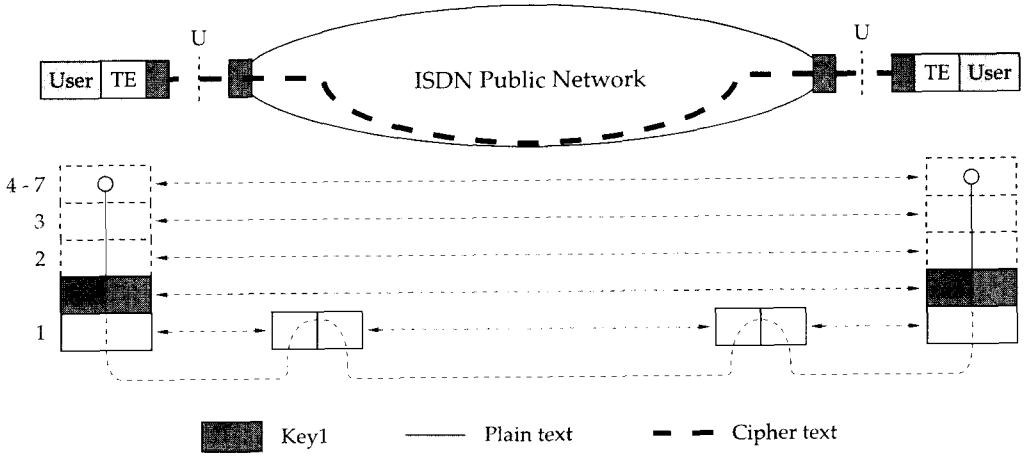
그러나, 암호화는 네트워크 교환에서 정지할 필요는 없다. [그림 11]에 나타난 바와 같이 TE-대-TE 암호화는 망에 대해 투명하며, 64 Kbps의 비제한 디지털 채널이 사용되는 한 두개의 장치된 터미널에서 사용될 수 있다. 같이 사용되는 패킷 응용 프로토콜은 호 설정동안 D 채널을 사용하여 키 관리와 인증을 위하여 안전한 링크를 초기화해야 한다.

만약 B 채널의 가장 상위 계층인 ISP1B 프로토콜이 있으면 비슷한 ISP1D 프로토콜이 있다는것을 의미한다. 그러나 Passive bus 상의 D 채널을 사용하는 경쟁(contention) 메카니즘을 혼동할 수 있기때문에 이같은 프로토콜은 실용적이지 않다. 만약 완전한 B 채널 트래픽 흐름 비밀유지가 요구된다면, 이것은 ISP2D와 ISP1B 프로토콜의 결합에 의하여 제공될 수 있다.

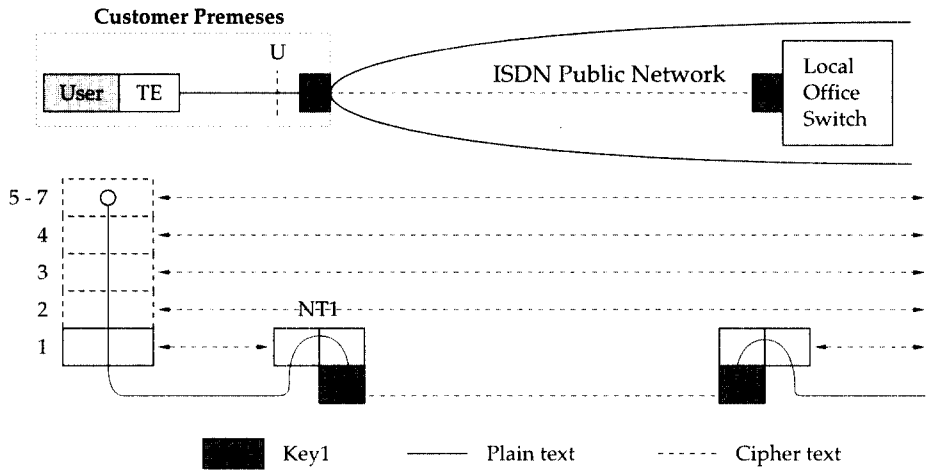
마지막으로, [그림 12]와 같이, 물리계층의 맨 아래에서 ISP0 암호화도 가능하다. 이 경우에는 B 채널과 D 채널, 그리고, 프레임, 발란스 및 제어 비트들이 모두 하나의 192 Kbps 스트림에서 암호화된다. 이 때 암호화된 신호는 NT1을 지나지 않기 때문에 이 계층에서의 암호화는 종단-대-종단으로 되지 않는다. 사실 암호화 장치는 로칼 오피스 교환기에서 라인 카드의 앞부분과 NT1 장치 앞에 삽입된다. 이것은 NT1과 교환기사이의 침입자를 막는 장점이 있다. 이것은 제한된 범위내에서는 실용적인 방법이다. 또한, 가장 취약한 부분인 사용자의 댁내와 로칼 오피스 교환기 사이의 라인에서 사용자의 정보를 완전하게 보호하여 준다.

4. ISDN 정보보호 서비스 배치

[그림 13]은 ISDN 정보보호 상호 작용을 보여주고 있다. 이 그림에서 사용자는 응용 계층 컴퓨터 프로세스, 또는 실제의 사용자가 된다. TE 또는 터미널은 ISDN 망에 연결하는 초기 연결점이다. 사용자는 어느 특정한 TE와 연결할 수 있으며 이동할 수도 있다. TE는 공중 ISDN망에 직접적으로 또는 NT2(일반적으로 PBX)를 통해 연결된다. TE와 NT2는 일괄적으로 가입자 댁내 장비(CPE: Customer



[그림 11] TE와 TE 물리 계층간 암호화



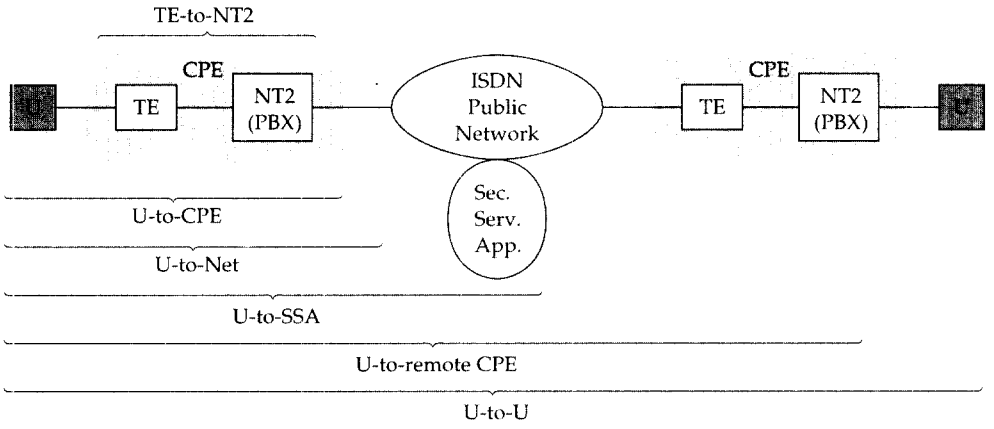
[그림 12] NT1과 로칼 오피스 교환기간 암호화

Premises Equipment)이다. SSA(Specializes Security Application)은 공중망을 통해 사용자에게 연결된다.

4.1 사용자-대-가입자 댁내 장치 (User-to-CPE)

User-to-CPE에서 중요한 정보보호는 인증과 액세스 제어이다. 만약 권한이 특정 라인과 터미널에 국한될 때 터미널에 대한 액세스는 제어되어야 한다. 이것은 터미널 액세스에 대한 물리적인 액세스 제어일 수도 있지만, 대부분의 경우에는 터미널 또는 PBX, 혹은 이 둘로 구축되어지는 인증과 액세스 제어를 요구한다.

이 계층에서의 인증과 액세스 제어의 중요한 장점은 여러가지 표준 규격이 꼭 필요하지는 않다는 것이다. 액세스 제어는 개인적인 토



[그림 13] ISDN 정보보호 상호 작용 다이아그램

큰이나 터미널을 활성화시키는 패스워드를 사용하여 터미널 내에 구축될 수 있다. 이것은 터미널의 독점 사용이 가능하게 된다.

터미널로 한정된 액세스 제어상의 약점은 침입자가 보호된 터미널을 물리적으로 제거하고 그의 터미널을 대신 사용하는 것이다. 그러므로 보다 강한 액세스 제어를 하기 위해서는, 정보보호 체계를 망 계층의 다음 계층에까지, 즉 PBX나 공중망에까지 확장하는 것이다. 터미널은 PBX 또는 공중망까지 인증을 요구한다. 터미널 또는 사용자 인증이 PBX 내에 구현되는 곳에서는 규격 표준화는 엄격히 필요하지는 않다. 그러나, 표준 규격화 없이는 안전한 터미널은 다른 PBX로 이동할 수 없다. 요즈음 ISDN PBX들은 소유를 독점할 수 있도록 구현된다.

정보보호 감사 정보는 CPE에서 수집될 수 있다. 만약 사용자가 터미널을 사용하기 전에 인증되어진다면, 매우 우수한 정보보호 환경에서는 각 통신을 하는 사용자의 기록이 정보보호 감사 정보가 될 수 있다.

4.2 사용자-대-망(User-to-Network)

여기서는 사용자와 CPE사이를 구별하지 않으며, 사용자는 CPE를 증명하도록 가정된다. 액세스 제어는 CPE에 의해 요구된다. 정보보호 목적을 위해 사용자와 CPE는 함께 한정된다. 만일 중요한 사용자-대-망 정보보호 기능이 구현된다면 인증과 액세스 제어이다. 이 경우에는 표준화가 확실히 요구된다. 사용자 인증을 수행하기 위해서 공중망의 교환기는 많은 기능의 확대가 필요하다. 공중망과 관련하여 가장 중요하게 고려하여야 할 액세스 제어는 900, 또는 장거리같은 망 서비스에 대한 사용자 액세스이다. 이같은 액세스 제어 서비스는 비지니스(business) 폰의 비인증된 사용과 가정용 전화에서 아이들의 부적절한 사용을 막을 수 있도록 가입자에게 제공될 수 있다.

4.3 사용자-대-정보보호 서비스 응용 (User-to-SSA)

실제로 다양한 사용자-대-정보보호 서비스 응용(SSA)의 상호 작용들이 나타날 것이다. 중요한 것들은 키 분배, 인증, 그리고 액세스 제어이며, 여기에서 SSA가 PACS를 제공하거나 정보보호 속성을 확인하는 믿을 수 있는 제 3자가 될 것이다. 다른 것들은 공증 서비스, 안전한 변환 서비스(즉, 안전한 아날로그 대 안전한 디지털 음성 변환), 혹은 안전한 메일 서비스를 제공한다.

대부분의 사용자-대-SSA 기능들을 실제적으로 실용화 하기 위해서는 표준 규격화가 필요하게 될 것이다. 보통 SSA가 믿을 수 있는 기능들을 제공하기 때문에, 대부분의 SSA 응용을 위해서는 인증 표준화가 필요하게 될 것이다.

4.4 사용자-대-사용자(User-to-User)

많은 ISDN 정보보호 서비스들이 아마도 인증이나 액세스 제어를 위하여 SSA의 도움으로 주로 사용자-대-사용자에 기초하여 구현될 것이다. 여기에는 다음과 같이 3가지의 주요 요인이 있다.

가. 공중 ISDN 망은 다루기 힘들고 매우 느린 속도로 발전한다. 망의 정보보호 기능의 규정화는 서비스 제공자들에게 요구된 투자액만큼 충분한 보상을 주지 못할 수도 있다. 비록 ISDN 서비스가 국가의 공중망으로부터 제공되는 초기 단계이지만, 실제로는 정보보호 기능을 포함하지 않는 ISDN 호환 교환 장비에 너무나 많은 투자가 이루어져 있다. 어떤 정보보호 기능은 단순히 교환기에서 소프트웨어의 수정으로 가능하지만, 소프트웨어가 설계되고, 코딩

되고 배치되려면 수년이 걸리게 된다. 하드웨어의 수정은 더욱 힘들 것이다. 이점에서 볼 때 사용자의 ISDN에 대한 투자는 미미하지만, 서비스 제공자의 투자는 상당하다.

나. 사용자-대-사용자 정보보호는 망에 투명하며, 기능이나 서비스가 망에 추가되는 것보다 훨씬 더 빠르게 필요한 곳에, 그리고 필요할 때에 사용자에 의해서 구현될 수 있다.

많은 정보보호에 대한 관심사는 본질적으로 종단-대-종단이며 최종 종단 앤티티만이 정보보호에 참여하는 것이 바람직하다. 몇몇 망들 그리고 서비스 제공자들이 안전한 통신에 관여될 수는 있다. 그러나 사용자-대-사용자에 기초를 둔 것들을 제외하고는 계속적인 정보보호을 보장하기는 어렵다.

인증, 액세스 제어, 그리고 비밀 보장 등은 모두 SSA나 망으로부터의 도움으로 주로 사용자-대-사용자에 기초를 두게 된다. 예를 들면, 만약 트래픽 흐름 비밀유지가 필요하면, 사용자-대-망 서비스가 요구된다.

엄격한 의미에서 사용자-대-사용자 서비스를 위하여 표준화가 꼭 요구되는 것은 아니다. 어떤 응용에서는 안전한 터미널을 단독으로 소유할 수도 있다. 그러나 이것은 별로 바람직하지 못하다. 표준화는 정보보호용 안전한 터미널을 위한 큰 시장을 개발하기 위해서, 그리고 사용자들이 어느 특정한 브랜드나 모델에 제한 받지 않고 많은 안전한 터미널 사용자들과 안심하고 통신할 수 있도록 하기 위해서 필요하게 될 것이다. 그러나, 회선 교환 서비스같은 특정한 ISDN 관련 기능들을 제외하고는 표준안이 꼭 ISDN만을 위한 표준안이 될 필요는 없다. 광범위한 OSI 지향적 정보보호 표준화는 하위 계층 데이터 전달을 위하여 ISDN을 사용하는 많은 데이터 응용들을 충족시킬 것이다.

5. 결 론

ISDN은 사용자가 필요로 하는 다양한 종류의 서비스(음성, 화상, 데이터 등)를 통합하여 효율적으로 서비스를 제공하기 위하여 디지털 전송과 디지털 교환을 기초로 발전되었다. ISDN에서는 다양한 종류의 서비스 정보를 제공하기 위해 통신망 전역에 걸쳐 디지털 전송이 이루어지므로 사용자의 중요 정보 자원에 대한 정보보호 구조 및 프로토콜 개발이 절실히 요구되는 실정이다.

ISDN에서 정보보호 서비스를 제공하기 위해서는 가장 효율적인 암호화 시스템을 정합하여 최적의 정보보호 구조와 프로토콜이 개발되어야 한다. 따라서 본 연구에서는 ISDN 정보보호 위협, 환경과 서비스에 필요한 시스템 구조 및 프로토콜에 대한 자료를 수집, 분석하여 효율적인 정보보호 서비스를 제공하기 위한 ISDN 정보보호 시스템 구조에 대해 알아보았다. 그리고, ISDN 정보보호 프로토콜과 적용 위치에 대해서도 알아보았다. 앞으로의 연구에서는 종합적인 ISDN 정보보호 서비스를 제공하는 방안에 대해서 진행하여, 이를 ISDN 시스템 구조와 프로토콜에 좀 더 효율적으로 정합하는 방안에 대하여 진행되어야 하겠다.

참 고 문 헌

[1] ITU-T Recommendation I.310 ISDN - Network Functional Principle, 1988

[2] ITU-T Recommendation Q.920 Digital Subscriber Signalling System No.1 (DSS1) -ISDN, 1988

[3] ITU-T Recommendation I.430 Basic User-Network Interface - Layer 1 Specification, 1988

[4] ITU-T Recommendation X.30 Support Of X.21, X.21 bis And Data Terminal Equipment (DTEs) By An ISDN, 1988

[5] CCITT Recommendation I.324 ISDN Network Architecture, 1984

[6] CCITT Recommendation I.464 Multiplexing ,Rate Adaptation And Support Of Existing Interfaces For Restricted 64 kbit / s Transfer Capability, 1984

[7] Warren S. Gifford, "ISDN User-Network Interfaces," IEEE Journal on SAC, Vol. SAC-4, No. 3, May 1986

[8] Umberto De Julio, Giorgio Pellegrini, "Layer 1 ISDN Recommendations," IEEE Journal on SAC, Vol. SAC-4, No. 3, May 1986

[9] Sadahiko Kano, "Layer 2 and 3 ISDN Recommendations," IEEE Journal on SAC, Vol. SAC-4, No. 3, May 1986

[10] Brian O'Higgins, "Securing information in X.25 Networks," IEEE GLOBECOM, 1990

[11] Winfred Y. Fong, "Anatomy of the ISDN's D-Channel Access Procedure," ISDN, ISDN'91, 1991

[12] Bhusri, G. "Considerations for ISDN Planning and implementation," IEEE Commun. Mag., pp.18-32, Jan. 1984

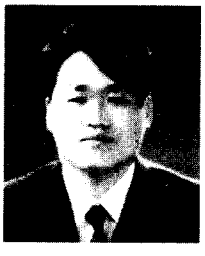
[13] Denning, D. and Denning, P. J. "Data Security," ACM Computing Surveys, Vol.11, No. 3, pp.225-249, Sept. 1979.

[14] Duc, N. Q., Chew, E. K. "ISDN Protocol Architecture," IEEE Comm. Mag., pp.15-22, Mar. 1985.

□ 著者紹介

김 봉 한

1994년 2월 청주대학교 전자계산공학과 졸업(학사)
1994년 2월 ~ 현재 한남대학교 대학원 전자계산공학과 석사과정



이 선 우

1995년 2월 한남대학교 전자계산공학과 졸업(학사)
1995년 2월~현재 한남대학교 대학원 전자계산공학과 석사과정

정 기 현

1985년 2월 경북대학교 전자공학과 졸업(공학사)
1985년 9월 ~ 현재 한국전자통신연구소 선임연구원

신 기 수

1975년 서강대학교 전자공학과 졸업 (공학사)
1989년 충북대학교 컴퓨터공학과 졸업 (공학석사)
1975년 ~ 1977년 육군 전략통신 사령부 근무
1977년 ~ 1978년 삼성전기 근무
1978년 ~ 1980년 원효전자
1980년 ~ 현재 한국전자통신연구소 책임연구원

강 철 신

1972년 ~ 1979년 한양대학교 전자공학과 졸업(공학사)
1984년 Oregon State University 전기 및 컴퓨터공학과(석사)
1987년 Oregon State University 전기 및 컴퓨터공학과(박사)
1978년 ~ 1982년 금성사 중앙연구소 연구원
1987년 ~ 1992년 미국 American University 전산정보학과 조교수
1990년 ~ 1991년 한국전자통신연구소 선임연구원(AU와 겸직)
1992년 ~ 현재 한남대학교 전자공학과 부교수

이 재 광

1984년 광운대학교 전자계산학과 졸업(이학사)
1986년 광운대학교 대학원 전자계산학과 졸업(이학석사)
1993년 광운대학교 대학원 전자계산학과 졸업(이학박사)
1986년 ~ 1993년 군산전문대학 전자계산과 교수
1993년 ~ 현재 한남대학교 전자계산공학과 조교수

※ 관심분야 : 컴퓨터 네트워크, 정보통신 정보보호