技術解說

Network Security

金 東 圭
(아주대학교 전산과 교수)

■차 례■

1 서 론

정보화 사회가 내도하고 있다. 이의 기본 도구로서 다양한 형태와 규모의 정보 통신 네트워크가 운용되기 시작하였다. 국제 간의 정보 통신 소통을 용이하게 하기 위하여 많은 표준 기구들에 의한 표준화 작업도 활발히 진행되고 있다.

이러한 시점에서 한 가지 중요한 문제가부각되기 시작하였다-네트워크 안전성(Network security), 안전성 문제는 대단히 광범위 하다. 전자 도청 (Electronic eavesdropping) 이라고 불리워 지는 문제가 가장 실감 나게 대두되고 있다. 주로 타인의 전화 통화 내용을 도청하는 것이 주류이지만 여러 형태의 컴퓨터 통신에 까지 용이하게 확장 적용될 수 있다. 미국 등지에서는 타인의 정보 통신을 도청할 수 있는 기기를 제작하여 판매하는 회사와 반대로 정보 통신 도청을 방지하거나 도청 사실을 검출할 수 있는 장비를 제작 판매하는 회사들의 광고가 등장하고 있다[1].

이 경우에 도청력과 도청 방어력의 정도와 범위를 결정 짓는 기술력이 관심사이지만 현재로서는 법률적인 측면에서는 이를 제약할 근거가 없는 실정이고 또 함부로 제약하는 것은 부수되는 파급효과 때문에 어렵다.

기본적으로 정보 통신 사용자나 설비 제공자가 스스로의 필요에 따라 안전성 서어비스를 제공하기 위한 장치를 마련하여야 한다.

포괄적인 안전성 서어비스의 제공은 경비가 많이 소요된다. 따라서 안전 체계의 일반적인 모형을 설정하고 제품화 한 후에 각 사용자의 요구 사항에 따라 안전성 기능을 재단할 수 있고 선택할 수 있도록 할 필요가 있다.

안전성 서어비스에 관하여 한 가지 원칙을제시할 수 있다. 안전성 서어비스를 제공하여 지키고자 하는 가치와 안전성 서어비스 제공에 소요되는 경비를 비교하여 가치가 더 고가일 때는 안전성 서어비스를 제공하는 것이다.

본 논문에서는 단독 시스템 내에서의 안전성에 대해서는 언급하지 않고 일반적인 네트워크

통신 환경에서 야기되는 안전성 문제에 대해서만 언급하겠다.

2 요구 사항(문제의 정의)

본론으로 들어 가기 전에 "안전성"의 정의를 내려 보자[2]. 본 논문에서는 이 정의를 바탕으로 내용 전개를 해나간다. "안전성(security)"이란 고의적이거나 혹은 비고의적이거나 간에 사고, 실패, 오용(misuse)에 대하여 저항하는 정보 통신 시스템의 특성을 말한다. 따라서, 안전성이란 어떤 종류의 오용을 예방하고 검출하고 정정함을 목적으로 하는 일단의 절차적, 논리적, 물리적 수단의 집합과 이 수단을 관리하기 위한 도구를 지칭한다.

이 정의를 따른다면 안전성이란 고의적인 오용(예를 들면 시스템에 대한 위협)뿐만 아니라 사고(예를 들면, 전문의 경로가 잘 못 잡히고 그 원인을 찾아 재정적으로 책임 있는 당사자를 식별하는 일)까지도 지칭한다.

이 견해에 의하면 안전성이란 조직 자체에 대한 위협에 대처할 뿐만 아니라 업무 시행의 정확성을 개선한다.

컴퓨터 통신에서 잠재적으로 요망되는 안전성 목표 사항을 몇가지 지적할 수 있다[3][4]. 이들은 미국의 NBS가 지원하는 OSI SIG-SEC (The OSI Implementors Workshop Special Interest Group in Security)가 확립한 바 있다. OSI환경에서 요망되는 최소한의 안전성목표 요망사항으로 다음의 다섯 가지를 들 수 있다:

- 불법 변경에 대한 데이터 보호(Sealed)
- 검출되지 않는 상실/반복에 대한 데이터 보호(Sequenced)
- 불법 노출로부터의 데이터 보호(Secret)
- 데이터 송신자의 정확한 신분 확인(Signed)
- 데이터 수신자의 정확한 신분 확인(Stamped)

OSI 구조에서 이러한 안전성 목표를 달성함으로써 하나의 OSI 시스템에서 다른 시스템으로 전송되는 데이터는 송신자가 수신자에 통고된이 없이는 변경되지 않고, 노출되지 않고, 상실되지 않고, 반복되지 않으며 아울러 통신에 참여하는 당사자의 신분은 정확히 확인될 수 있다.

이 외에도 다수의 안전 목표 사항들이 지적될 수 있다[5]:

- 민감도, 발신 주소 등에 따라서 데이터에 표식을 붙임(labeling)
- 당사자를 제외하고는 데이터의 송신자와 수신자의 신분, 교환되는 데이터의 분량 등의 정보를 노출시키지 않음.
- 네트워크 통신의 안전성 감사 기록(audit trails) 제공
- 비우호적인 환경에서도 통신의 가동성 보장
- OSI 시스템 내에서는 아주 좁은 대역이라 하더라도 비밀 채널로는 정보를 전송하지 않는 일
- 믿을만한 독립적인 제 삼자를 통하여 통신이 일어 났고 정확한 내용이 수신되었다는 사실을 증명하는 일(공증)
- 시스템과의 연결을 이루기 전에 그 시스템에 대한 액세스 허가를 공식적으로 입수하는 일

3 안전성 구조와 프로토콜

상용 제품에 안전성 서어비스 실현 작업을 시작하기 위해서는 OSI 구조에서의 안전성 관련 표준 구조가 필요하다. 이는 하나의 OSI 시스템이 다른 OSI 시스템과 통신하기 위해서 뿐만 아니라 요망되는 안전성을 가지고 통신을 수행하기 위함이다.

표준 구조는 사용자에게 제공할 수 있는 서어비스의 집합을 일반적으로 정의하여야 하며 서어비스를 실현하기 위한 메카니즘을 마련하여야 한다. 메카니즘이란 필요한 앨고리즘, 절차, 프로토콜, 데이터 구조 등을 통털어 포함한다. 어떤 서어비스가 정의되면, 그 서어비스를 운용하는 데에 필요한 관리 체계가 정의되어야 한다.

가. 서어비스

(5)에서 정의되어 있는 여러 가지 서어비스의 유형과 종류를 열거하고 요약하여 설명한다. 이 서어비스 집합은 ISO TC97/SC21/WG1과 미국의 ANSI Ad Hoc 그룹에 의하여 개발되었다.

• **신분 확인** : 통신 관련자들의 신분을 확인하고 해당 통신에 참여할 자격 유무를 점검한다.

- 대등 실체(peer entity) 신분 확인 : 통신 당사자의 신분 확인과 자격 유무 점검(연결 지향 통신)
- 발신처 신분 확인 : 데이터 발신처의 신분 확인과 자격 유무 검증(무연결 지향 통신)

• **액세스 레어** : 액세스하고자 하는 자원과 액세스 동작 유형(예 : Read, Write, Update 등)에 대한 정당성을 점검한다.

- 사용자의 정당성
- 대등 실체의 정당성

• **데이터 정확성** : 통신되는 데이터의 정확성을 점검한다. 데이터의 정확성은 에러 발생, 고의적인 삽입, 삭제, 변경 등을 통하여 파괴될 수 있다.

- 연결 지향 통신의 정확성(복구 보장)
- 연결 지향 통신의 정확성(복구 없음)
- 연결 지향 선택 필드의 정확성 : 연결 지향 통신에서 선택되는 특정 필드의 정확성을 보장
- 무연결 지향 선택 필드의 정확성
- 무연결 통신의 정확성

• **비밀 보장** : 통신되는 데이터가 불법적으로 그 내용이 노출되는 것을 방지한다.

- 연결 지향 통신 비밀
- 선택 필드 비밀
- 교통 흐름의 비밀 : 교통의 흐름을 관찰함으로써 정보의 존재와 부재, 분량, 방향, 빈도 등을 유추할 수 있다.

• **부인 봉쇄** : 이미 발생한 통신 사실을 부인할 수 없도록 하여야 한다.

- 발신 부인 : 전송된 정보에 대하여 발신 사실을 부인하지 못하게 함.
- 수신 부인 : 수신된 정보에 대하여 수신 사실을 부인하지 못하게 함.

이상과 같이 정의된 서어비스는 아래에 주어지는 것과 같은 원시 명령 집합을 사용하여 실현할 수 있다. 각 원시 명령은 매개 인수([ ] 내에 명시됨)와 더불어 호출되며, 명령이 수행된 후에는 그 결과가 돌아 온다({ } 내에 명시됨)

• AUTHENTICATE[ID; AUTHENTICATOR] {RESULT; STATUS} :

이 명령은 국지 SMIB(Secure Management Information Base)를 검색하여 AUTHENTICATOR와 ID가 일치함을 증명하고 정확한 RESULT와 STATUS로써 반응한다.

• AUTHORIZE[ID; TYPE; RESOURCE] {RESULT; STATUS} : 이 명령은 주어진 TYPE의 ID가 RESORCE를 액세스할 수 있도록 허락하고 정확한 RESULT와 STATUS를 set 시킨다.

• ENCIPHER[PT; LENGTH; KEYNAME] {CT; LENTH; STATUS} :

이 명령은 PT에서 시작되는 주어진 LENGTH의 plaintext 데이터를 CT에서 시작되는 주어 진 LENGTH의 암호문(ciphertext)으로 바꾸고 KEYNAME과 연관되는 KEY를 사용하여 STATUS를 set 시킨다.

• DECIPHER[CT; LENGTH; KEYNAME] {PT; LENGTH; STATUS} :

이 명령은 CT에서 시작하는 주어 진 길이의 암호문을 PT에서 시작되는 일정 길이의 plaintext 로 바꾸고 KEYNAME과 연관되는 KEY를 사용하여 STATUS를 set 시킨다.

• COMPUTEMAC[DATA; LENGTH; KEYNAME] {MAC; STATUS} :

이 명령은 KEYNAME과 연관되는 KEY 를 사용하여 지정된 길이의 데이터에 대한 MAC (Message Authentication code)를 산출하고 그 결과를 set 시킨다.

• VERIFYMAC[DATA; LENGTH; KEYNAME; MAC] {RESULT} :

이 명령은 KEYNAME과 연관되는 KEY 를 사용하여 지정된 길이의 DATA에 대한 TMAC (Test Message Authentication Code)를 산출한 후에 이것이 입력된 MAC와 일치하는가의

여부를 RESULT에 set 시킨다.

• SIGN[DATA;LENGTH;USERID;KEY-NAME] {SIGNATURE;STATUS} :

이 명령은 KEYNAME과 연관되는 KEY 를 사용하여 USERID로 명시되는 사용자를 위한 지정된 길이의 DATA에 대한 SIGNATURE를 산출하고 STATUS를 set시킨다.

• VERIFYSIGNATURE[DATA;LENGTH;USERID;KEYNAME;SIGNATURE] {RESSULT;STATUS] :

이 명령은 KEYNAME과 연관된 KEY를 사용하여 USERID로 명시되는 사용자를 위한 지정된 길이의 DATA에 대한 Test Signature (TSIGNATURE)를 산출하고, 이를 SIGNATURE와 비교한 후에 그 결과를 STATUS 와 RESULT에 set 시킨다.

나. 메카니즘

위에서 언급한 여러 서어비스들은 각각 적합한 메카니즘을 통하여 실현될 수 있다. 이 절에서는 현재까지 인지되고 있는 몇가지 중요한 메카니즘에 대하여 기술한다[5][6]. 이 논문에서는 OSI 구조에 특별히 유관한 것들만 고려한다.

메카니즘은 세가지 유형으로 나눌 수있다(이들은 서로 중복되는 부분도 있다) : 예방 메카니즘; 검출 메카니즘; 복구 메카니즘

• 암호화(encipherment/encryption) : 데이터나 교통 흐름 정보의 기밀성을 제공하며 다수의 다른 메카니즘을 보완할 수 있다.

- Link encryption: 데이터 링크 구간에서 전송 데이터의 기밀성을 제공한다.

- End-to-end encryption: 양단의 통신 프로세스 간에 교환되는 데이터의 기밀성을 제공한다.

대칭형 encryption(비밀 키): 암호화 키와 암호 해독 키는 서로 동일하다.

- 비대칭형 encryption(공중 키) : 암호화 키와 암호 해독 키는 서로 다르다. 암호화 키는 공중 키, 암호 해독 키는 개인 키라고 한다.

- Cryptographic checkfunction; 데이터 단위에 암호화 관련 절차를 수행함으로써 추출할 수 있는 정보.

- 키 관리 : 암호화는 키 배분 프로토콜과 키 배분 센타의 형태로 키를 관리하여야 하는 필요성을 야기 시킨다. MAC등도 효율적인 키 관리 표준이 채택되기 전까지는 별로 쓸모 없는 것이었다. 키를 교환할 때 이를 보호하기 위한 별도의 키가 필요할 수도 있다. 키 배분 센타는 신뢰할 수 있는 중간 매개 조직으로서 전체 통신 환경에 필요한 키의 수를 줄이고 키 배분에 사용되는 특별한 프로토콜을 운용하기 위하여 필요하다.

• 디지털 서명

이 메카니즘의 요체는 비밀 키(private key)를 사용하지 않고서는 데이터 전문을 생성할 수 없다는 사실을 이용하는 것이다. 세가지 조건으로 대별할 수 있다 :

- 제 삼자 조건 : 비밀 키의 소지자 아닌 어느 누구도 서명된 데이터 단위를 생성할 수 없다.

- 수신자 조건 : 수신자는 서명 데이터 단위를 생성할 수 없다.

- 송신자 조건 : 송신자는 서명 데이터 단위를 송신하였음을 부인할 수 없다.

직접 서명(direct signature)은 제 삼자 조건과 수신자 조건으로 구성된다. 서명 데이터가 수신되면 공개되어 있는 정보(공동 키 : public key)를 사용하여 서명자를 확인할 수 있다. 서명자는 해당 비밀 키의 소지자이어야 한다. 이 사실은 나중에 분쟁이 발생하는 경우 제 삼자에 의한 확인에 사용될 수 있다.

중재 서명(arbitrated signature)은 송신자 조건이 추가로 관련된다. 이 경우는 신뢰성 있는 제 삼자가 데이터의 정확성과 송신자 신분을 수신자에게 증명한다. 이를 위해서는 디지털서명과 공증(notarization) 메카니즘이 결합되어야 한다.

• 액세스 제어

사용자의 신분이 확인된 후에 그 사용자가 명시된 자원을 액세스할 자격이 있는가를 점검하고 다음에는 어떤 유형의 동작(operation)을 수행할 수 있는가에 대한 허락을 받도록 한다. 이를 위해서 다음과 같은 여러 가지 메카니즘이

사용될 수 있다.

- 액세스 제어 목록(access control list) : 어떤 주체(subject)에 대하여 액세스 대상이 되는 객체(object)와 허용되는 동작의 종류를 나타내는데 주로 행렬 구조를 사용한다.

- 패스워드(password) : 암호화되지 않은 단순한 값(숫자 혹은 문자)으로서 액세스 하려는 사용자의 신분을 확인한다. 이 값은 암호화 되지는 않으며 노출을 피하기 위하여 화면이나 지면에 인쇄되지는 않는다.

- Capability목록 : 액세스 제어 목록과는 반대로 어떤 객체에 대하여 액세스가 허용되는주체와 수행 가능한 동작의 목록을 명시한다. 보다 유연성 있고 효율적인 메카니즘으로 인식되

표 1 서어비스와 메카니즘

서어비스 유형 / 서어비스 종류		암호화	디지털서명	액세스 제어	데이터의 정확성	실체의 신분확인	교통의 패딩	경로 제어	공증	세방향 교환
신 분 확 인	대등 실체	S	S			S			S	
	발신처 신분 확인	S	S		S				S	
액세스 제어	사용자의 정당성			Y						
	대등실체의 정당성			Y						
데이터정확성	연결통신 정확성(복구)	S			Y					S
	연결통신 정확성(복구 없음)	S			Y					S
	연결선택필드의 정확성	S			Y					S
	무연결선택필드의 정확성	S	S		Y					S
	무연결 통신의 정확성	S	S		Y					S
비 밀 보 장	연결지향 통신비밀	Y						S		
	무연결지향 통신 비밀	Y						S		
	선택 필드 비밀	Y								
	교통 흐름의 비밀	Y					S	S		
부 인 봉 쇄	송 신		S		S				S	
	수 신		S		S				S	

범례 Y : Yes ; S : sometimes

고 있다.

- Credentials : 어떤 실체로부터 다른 실체로 전달되는 데이터로서 송신 실체의 액세스권한을 확립하는 데에 사용된다.

- Labels: 통신 시스템 환경에서 속성을 지니는 레이블은 다양한 역할을 수행한다. 데이터 항목, 프로세스 혹은 실체, 자원(예 : 채널) 등에는 레이블을 붙일 수 있다. 각 레이블의 속성들이 필요한 안전성을 제공하는데에 어떻게 사용될 수 있는가는 안전성 정책이 지시하여야한다. 협상을 통하여 특정 레이블 속성들의 적절한 안전성 의미를 확립하는 것이 필요할 수도 있다.

• 데이터의 정확성 : 데이터의 내용이 정확하다는 것을 보장하기 위하여 사용되는 메카니즘이다.

- Checksum

- Sequencing; timestamping

• 실체의 신분 확인(Identification/authentication)

- 패스워드

- 암호 메카니즘

• 교통의 패딩(padding) : 실제의 데이터가 아닌 정보를 안전성 제공의 목적으로 정해진 규칙에 따라 삽입할 수 있다.

• 경로 제어 : 어떤 수준의 안전성을 달성하는 데에 필요하거나 유용한 전송 경로(물리적 혹은 논리적)를 선택할 수 있도록 한다.

• 공증(notarization) : 안전성 서어비스를 제공하는 데에 있어송신자와 수신자가 아닌 제삼자의 위치에 있는 중재자의 개입을 통하도록 한다. 이는 보통 디지털 서명 메카니즘과 함께 사용되며 송신 사실의 부인과 수신 사실의 부인을 봉쇄하는 데에 필요하다.

• 세방향 교환(3-way handshake) : 정보가 전달 과정에서 상실되거나 중복되는 것을 정확히 검출하여 필요한 동기를 행할 수 있게 한다. 데이터의 정확성 서어비스를 실현하는 데에 유용한 메카니즘이다[7][8].

다. 관 리

적절한 메카니즘을 사용하여 서어비스를 실현하게 되는데 서어비스를 지속적으로 제공하기 위해서는 적절한 관리 절차가 수행되어야 한다. 이를 위해서는 필요한 제어 정보를 데이터베이스 형태로 유지/갱신하여야 하고 안전성 관련 사건을 일지 형태로 기록을 하고 유지하여야 한다. 또한 필요할 때 사건 기록을 검색하고분석을 수행하여야 한다.

관리를 위하여 필요한 조직도 구성하여야 한다. 예를 들면, 키 배분 센타 등이 있다.

지금까지 언급한 여러 가지 일반적인 서어비스와 이들 서어비스 실현에 관련되는 메카니즘의 관계를 표1에 요약하여 본다[5].

라. 안전성 서어비스의 계층 배치

특정 서어비스는 하나 혹은 하나 이상의 계층에서 제공될 수 있다. 하나 이상의 계층에서 제공될 때에는 어떤 계층은 그 서어비스를 직접 제공하지 않고 하위 계층이 제공하는 서어비스를 이용할 수도 있다. 서어비스를 직접 제공하지 않는 경우에도 안전성 서어비스 요청을 하위 계층에 전달하기 위하여 그 계층의 서어비스 정의는 수정을 필요로할 수도 있다.

두 개의 상이한 시스템에 안전성 서어비스가 연관되어 있을 때에는 두 시스템의 안전성 계층 할당이 동일하여야 한다. 그렇지 않으면 호환성에 문제가 야기된다.

안전성 서어비스를 계층에 할당하는 데에는 몇가지 원칙이 고려되어야 한다[6].

• 서어비스를 실현하는 데에 사용될 수 있는 선택 가능한 방법의 수는 최소화 되어야 한다.

• 하나 이상의 계층에 안전성 서어비스를 제공할 수 있다.

• 안전성을 제공하기 위하여 필요한 기능 추가는 기존의 OSI 기능과 불필요하게 중복되어서는 안된다.

• 계층 독립의 원칙이 위배되어서는 안된다.

• 하나의 계층이 안전성 서어비스를 제공하는 데에 있어 하위 계층 실체에 위치하는메카니즘에 의존하는 경우에, 중간 계층들에서 안전성 위반이 일어날 수 없도록 설계 되어야 한다.

표 2 OSI 계층과 안전성 서어비스 배치

서어비스유형 \ 서어비스 종류		계층 1	2	3	4	5	6	7
신분확인	대등 실체			×	×		×	
	발신처 신분확인			×	×		×	
액세스제어	사용자의 정당성							×
	대등실체의 정당성			×	×		×	×
데이터정확성	연결통신정확성(복구)			×	×		×	
	연결통신정확성(복구없음)			×	×		×	
	연결선택필드의 정확성						×	
	무연결선택필드의 정확성						×	
	무연결 통신의 정확성			×	×		×	
비밀보장	연결지향통신 비밀	×	×	×	×		×	
	무연결 지향통신 비밀		×	×	×		×	
	선택필드 비밀						×	
	교통 흐름의 비밀	×		×				×
부인봉쇄	송 신						×	
	수 신						×	

• 가능한 한, 안전성 기능이 어떤 계층에 추가될 때에 그 실현은 독립된 모듈로서 이루어질 수 있도록 배려 되어야 한다.

안전성 서어비스 요청과 제공을 정의하는 계층 실체간 명령 호출 모형은 다른 통신 서어비스의 경우와 동일하므로 별도로 고려되어야 할 사항은 없다. 표 2에 OSI 참조 모형의 각 계층과 계층에서 제공되는 안전성 서어비스의 관계가 주어진다.

4 OSI 안전성 관련 국제 연구 및 표준화 동향

여러 가지 형태의 정보 통신 시스템이 실현됨에 따라 안전성 문제가 중요한 쟁점으로 부각되고 있고 이에 대한 연구가 활발히 진행되고 있다. 안전성 문제는 정보 통신 관련 국제 표준기구들이 본격적으로 대처하기 시작하였다.

ISO TC97/SC21 (WG1 security ad hoc, WG4 directories and security management, WG6 CASE and ULA), SC20 (WG1 secret key algorithms, WG3 cryptographic techniques in communications architectures), SC18 (distributed office applications), CCITT (SG Ⅶ Q. 35 directory service and protocols

ad hoc group) 등을 열거할 수 있다[9~15].

신분 확인과 정당성 점검(authentication) 이외에도 광범위한 안전성 서어비스의 필요성이 인식되어 이들의 구조적인 뼈대를 구축하는 작업이 제안되고 진행되고 있다. 이들은 신분 확인과 정당성 점검, 액세스 제어, 부인 봉쇄, 안전성 감사(audit), 데이터 정확성, 트랜스포트 암호화, 링크 레벨 암호화, 선택 필드 매개인수 암호화 등이다.

안전성 문제는 분산 사무 자동화 환경, 개방형 분산 처리 환경 등에서도 쟁점으로 부각되고 있다.

5 요약 및 결론

여러 가지 정보 통신 환경에서 고려되어야 할 안전성 문제에 대하여 고찰하여 보았다. 안전성의 목표, 안전성 구조의 개관과 분석-서어비스 종류와 원시 명령 집합의 제안, 각종 서어비스의 실현에 적용 가능한 메카니즘, OSI의 각 계층에 대한 서어비스 배치 등-을 제시하였다.

필요한 안전성을 제공하는 일은 매우 고가의 경비를 수반하게 될 것임으로 일반적인 안전성 구조를 확립하고 이를 기반으로 개개의 응용 환경에서 요구되는 사항들을 선택적으로 제공할 수 있는 안전성 시스템이 연구 개발되어야 한다. 본 논문은 이러한 관점에서 진행되고 있는 연구 프로젝트의 중간 결과를 요약한 것으로 안전성 연구 개발 작업의 좋은 지침을 제공할 수 있을 것으로 믿는다.

참 고 문 헌

1. John Horgan, "Tworting the information thieves, IEEE SPECTRUM, July 1985.
2. ISO TC97/SC21 N1875, Distributed Office Application Security.
3. 김동규, "OSI 정보 통신 안전 체제," '정보통신의 해' 기념 전자 통신 종합 학술 대회논문집, 1987. 9.
4. D.K. Braustad, "Considerations for Security in the OSI Architecture," IEEE Network Magazine, Vol.1 No.2, April 1987.
5. PDAD 2 to ISO 7498, Information Processing System-Open System Interconnection-PDAD2 to ISO7498 on Security Architecture.
6. M.D. Abrams et.al., "Network Security: Protocol Performance Model and the Trusted Computer System Evaluation Criteria," IEEE Network Magazine, 1987.
7. 김동규, 컴퓨터 통신 네트워크, 상조사, 1986.
8. A.S. Tanenbaum, Computer Networks, Prentice-Hall, 1983.
9. Distributed Office Application Security, ISO TC97/SC21 N1875, 1987.
10. Joint Security Meeting Minutes, ISO TC97/SC21 N1990, 1987.
11. Coordination of Work on Security, ISO TC97/SC21 N2113, 1987.
12. Proposal for the organization of work on security within SC21, ISO TC97/SC21 N2025, 1987.
13. Initial Working draft and draft proposal for a new work item on access control framework for OSI, ISO TC97/SC21 N2028, 1987.
14. Initial working draft and draft proposal for a new work item on authentication framework for OSI, iSO TC97/SC21 N2027, 1987.
15. Initial working draft and draft proposal for a new work item on nonrepudiation framework for OSI, ISO TC97/SC21 N2029, 1987.
16. M.E. Hellman, "Commercial Encryption," IEEE Network Magazine, April 1987.
17. D.B. Newman, Jr., et.al., "Public Key Management for Network Security," IEEE Network Magazine, April 1987.
18. R.R. Jueneman, "Electronic Document Authentication," IEEE Network Magazine, 1987.
19. Eric E. Summer, "Technology Perspective," IEEE Network Magazine, Vol.1, No.2, April 1987.

金 東 圭

저자약력

- 1947년 2월 7일생
- 1973. 2 : 서울대학교 공대 응용수학과 (공학사)
- 1979. 2 : 서울대학교 자연과학대 계산 통계학과 대학원 졸업 (이학석사 : 전산학)
- 1984. 7 : 미국 Kansas State University 대학원 전산과 졸업 (Ph. D. : 전산학 / 컴퓨터 통신)
- 1973~1977 : KIST 전산부 연구원
- 1977~1979 : KIET 전산개발부 선임연구원
- 1981~1982 : 미국 Kansas State University Instructor
- 1979~현재 : 아주대학교 교수

용 어 해 설

● **부성 저항기** (negative resistor) : 하 양단에 가해진 전압 증감에 따라서 전류가 증감하지 않고 반대로 줄거나 증가하는 역현상이 나타날 때 이를 부정 저항이라고 하며, 이러한 특성을 갖는 소자를 부성 저항기 또는 부성 저항 소자라 한다. 부성 저항을 나타내는 특성으로는 전류 제어형과 전압 제어형이 있으며 전류 제어형으로는 PNPN 다이오드, 2중 주입형 다이오드 등이 있고 전압 제어형으로는 터널 다이오드, 건 다이오드 등이 있다.

● **부속 벨** (extension bell) : 전화기에 부착된 벨 이외에 착신 표시를 필요로 할 때 사용하는 일종의 벨을 가리킨다.