네트웍 시큐리티

金 東 圭
아주대학교 전산학과 교수·理博

필 자

- ▲서울대 공대 졸업(학사)
- ▲서울대 자연과학대학 전산학교 졸업(석사)
- ▲미국 켄사스주립대 대학원 전산학과 졸업(박사)
- ▲한국과학원 전산개발부 선임연구원
- ▲켄사스주립대 전산학과 전임강사
- ▲한국데이타통신(주) 고문(현)
- ▲금융결제관리원 고문(현)
- ▲한국통신학회 이사, 데이터통신 분과 회장(현)
- ▲개방형 정보통신 연구회 이사(현)
- ▲아주대학교 전산학과 교수·학과장(현)

주요쟁점으로 부각

정보화 사회로 이행하여 나가는 데에 있어 기본 도구의 하나로서 다양한 정보 통신 시스템이 구축, 운용되고 있다. 지금까지는 어떤 통신 환경에서 정보가 효율적으로 흐를 수 있도록 하는 데에 기술적인 주 역점이 투여되어 왔다. 이 노력은 이제 결실을 보아 안정된 기술이 축적되기에 이르렀다.

기술적인 측면에서 주어진 통신 환경과 사용자의 요구 사항에 따라서 다양한 네트웍으로 구현이 가능하게 되었다. 근거리 통신망(LAN), 지역망(MAN), 공중 패킷 교환망(PSDN), 광역망(WAN), 부가가치통신망(VAN) 등이 그것이다.

물론 앞으로 지향하는 통신망의 기술은 데이터의 유형(데이터, 음생, 영상, 그래픽 등)에 무관하게 디지틀 패킷으로 변환하여 전송하고, 목적지에 도착한 후에 다시 원형으로 복구하는 종합정보통신망(ISDN)을 추구하고 있지만 이는 앞으로 장기간에 걸쳐 연구 개발 노력이 지속되어야만 실현을 내다 볼 수 있다.

현 시점에서 정보통신의 중요한 쟁점으로 부각된 문제는 통신의 안정성(Security)이다. 사용자의 입장에서는 자신이 발송하는 정보가 목적지에 정확히 전달되는 것도 중요하지만 자신의 정보가 무단으로 유출되는 일이 없어야 하는 것이 중요하게 되었다. 이 문제의 확실한 보장이 없으면 사용자는 다양하고 편리한 정보통신 서비스를 이용할 수 없게 된다. 이 글에서는 이러한 정보 통신 안정성의 문제에 대하여 논하여 보고자 한다.

안전성 문제

안전성 문제의 전형적인 경우는 도청이다. 이는 수동적인 안전성 공격으로서 정보를 암호화 함으로써 극복할 수 있다.

보다 적극적인 안전성 공격은 통신 과정에서 정보를 붙잡아 변질시키는 일이다.

안전성 문제는 보다 구체적으로 안전성 서비스를 조명하여 봄으로써 더 정확히 이해할 수 있다.

안전 체제의 요구 사항

일반적으로 고려될 수 있는 네트웍 안전 체제의 목표를 나열하여 봄으로써 각 사용자의 요구 사항이 어떻게 제기될 수 있는가를 조명할 수 있다.

- 정보의 내용 변경
  통신되는 정보의 내용을 고의로 변경시킬 수 있다.
- 정보의 순서 변경
  정보가 상실되거나 변복 통신될 수 있다.
- 정보의 불법적인 유출
  정보가 통신 과정에서 목적지가 아닌 제삼자에게 불법적으로 노

출될 수 있다.

- 발신자의 신분 확인
  정보를 발신한 사람의 신분을 확인할 수 있어야 하고 거짓 조작하지 않아야 한다.
- 수신자의 신분 확인
  수신자의 신분이 확인될 수 있어야 하고 거짓 조작이 가능해서는 안된다.

개방 통신 환경에서의 안전체제

정보 통신 환경에서의 안전성 파괴라는 것은 양단에 있는 최종적인 발신자와 수신자 사이에 놓여 있는 개방형 통신 환경에서 정보의 안전성이 고의적인 공격 혹은 우발적인 사고로 인하여 파괴되는 것을 말한다.

물론 발신자와 수신자가 위치하는 컴퓨터나 터미널에서 정보의 안전성이 파괴될 수도 있다. 정보 통신의 안전성의 전제는 발신자와 수신자 위치의 단독 컴퓨터 환경에서 정보의 안전성이 보장되는 것임은 두말할 필요가 없다.

그러나 보다 어렵고 관심의 대상이 되는 것은 공간 통신 과정에서의 안전성 파괴이다.

개방형 정보통신 안전체제

네트웍은 가장 일반적인 정보 통신 환경이다. 개방형 네트웍의 안전 체제 구조는 여러 가지 구성 요소를 포함한다. 개방 시스팀의 상호 연결 환경하에서 일반적으로 고려할 수 있는 안전 체제의 구성 요소는 서비스, 메카니즘, 관리, 그리고 계층 체제이다. 이러한 기본적인 구성 요소들이 상호 밀접히 연관되어야 어떤 사용자의 요구사항을 만족 시키는 하나의 네트웍 안전 체제로 구축될 수 있다.

개방형 정보통신 안전체제 구성요소

안전 체제가 사용자에게 제공할 수 있는 서비스의 집합이 일반적으로 정의되어야 하며 서비스를 실현하기 위한 메카니즘들이 마련되어야 한다. 메카니즘이란 필요한 앨고리즘, 절차, 프로토콜, 데이터 구조 등을 통틀어 포함한다. 어떤 서비스가 정의되고 실현되면 그 서비스를 운용하는 데에 필요한 관리 체계를 정의하여야 한다.

연중기획 月別 주제

1 정보통신네트웍의 개요
朴容震 (한양대 교수)

2 네트웍 시큐리티
金東圭 (아주대 교수)

3 VAN(Value Added Network)
宋官浩 (한국전산원 선임연구원)

4 텔레마틱스(Telematics)
鄭鎭旭 (성균관대 교수)

5 LAN(Local Area Network)
鄭善鍾 (전자통신연구소 연구위원)

6 Lap-Top
鄭善鍾 (전자통신연구소 연구위원)

7 OSI(Open System Interconnection) 개요
安順臣 (고려대 교수)

8 OSI 하위층
趙國鉉 (광운대 교수)

9 OSI 상위층
李榮熙 (전자통신연구소 선임연구원)

10 ISDN(Integrated Service Digital Network)
崔陽熙 (전자통신연구소 실장)

11 WAN(Wide Area Network)
黃善泳 (건국대 교수)

12 정보통신네트웍의 미래와 과제
柳京熙 (한국데이타통신 연구위원)

서비스

여러 가지 서비스의 유형과 종류를 열거하고 요약하여 설명한다. 이 서비스 집합은 ISO TC97/SC 21/WG과 미국의 ANSI Ad hoc 그룹에 의하여 개발되었다.

- 신분 확인
  통신 관련자들의 신분을 확인하고 해당 통신에 참여할 자격 유무를 점검한다.
- 액세스 제어
  액세스 하고자 하는 자원과 액세스 동작 유형에 대한 정당성을 점검한다.
- 데이터 정확성
  통신되는 데이터의 정확성을 점검한다. 데이터의 정확성은 에러 발생, 고의적인 삽입, 삭제, 변경 등을 통하여 파괴될 수 있다.
- 비밀 보장
  통신되는 데이터가 불법적으로 그 내용이 노출되는 것을 방지한다.
- 부인 봉쇄
  이미 발생한 통신 사실을 부인할 수 없도록 하여야 한다. 여기에는 발신 부인과 수신 부인이 있다.

이상과 같이 정의된 서비스는 원시 명령 집합을 사용하여 실현할 수 있다. 원시 명령의 한가지 예를 들어 보자. 이 예제에서 [ ]내에는 매개 변수가 표시되며 명령이 호출되고 수행된 후에는 그 결과가 돌아 온다(결과는 { }내에 명시됨).

ENCIPHER[PT; LENGTH; KEYNAME]{CT; LENGTH; STATUS}

이 명령은 PT에서 시작되는 주어진 LENGTH의 평문(Plaintext)을 CT에서 시작되는 주어진 LENGTH의 암호문(Ciphertext)으로 바꾸고 KEYNAME과 관련되는 키를 사용하여 STATUS를 세트시킨다.

> "발송하는 정보가 목적지에 정확히 전달되는 것도 중요하지만 정보가 무단으로 유출되는 일이 없어야 하는 것이 중요하게 되었다."

메커니즘

위에서 언급한 여러 가지 서비스들은 각각 적합한 메커니즘을 통하여 실현 될 수 있다. 일반적으로 메커니즘은 예방 메커니즘, 검출 메커니즘, 복구 메커니즘 등 세가지 유형으로 나눌 수 있다.

- 암호화(Encryption)
  데이터나 교통 흐름 정보의 기밀성을 제공하며 안전성 관련 다른 메커니즘을 보완할 수 있다.
  여기에는 여러가지 세부 형태가 있다.
  - 링크 엔크립션
  - 양단간(End-to-End) 엔크립션
  - 대칭형 엔크립션 :
    비밀키를 사용하며 암호화 키와 암호 해독 키는 서로 동일하다.
  - 비대칭형 엔크립션 :
    공중키가 사용되며 암호화 키와 암호 해독 키는 서로 다르다. 공중키와 개인 키는 모두 암호화와 암호 해독에 사용될 수 있다. 암호화와 암호 해독에 어느 키를 쓰느냐에 따라 안전성 제공의 방향이 달라진다.
  - 키 관리 :
    암호화는 키 배분 프로토콜과 키 배분 센터의 형태로 키 관리의 필요성을 야기 시킨다. 키를 교환할 때는 이를 보호하기 위한 별도의 키가 필요할 수도 있다. 키 배분 센터는 신뢰할 수 있는 공간 매개 조직으로서 전체 통신 환경에 필요한 키의 수를 줄이고 키 배분에 사용되는 특별한 프로토콜을 운용하기 위하여 필요하다. 전문 보호 코드(MAC : Message Authentication Code)에도 키가 사용된다.
- 디지틀 서명
  정보 통신의 보편화를 바탕으로 하는 정보화 사회는 정보의 처리와 교환 시에 문서나 서류에 서명하는 것과 동일한 효과를 갖는 일종의 전자 서명이 필수적인 것

이 된다. 이것이 디지틀서명이다.

이 메커니즘의 요체는 비밀 키를사용하지 않고서는 데이터 전문을 생성할 수 없다는 사실을 이용하는 것으로 세가지 조건이 있다.

- 제삼자 조건 :
  비밀키의 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 서명은 제삼자 조건과 수신자 조건으로 구성된다. 서명 데이터가 수신되면 공개되어 있는 공증키를 사용하여 서명자를 확인할 수 있다. 서명자는 해당 비밀키의 소지자이어야 한다. 이 사실은 나중에 분쟁이 발생하는경우에 제삼자에 의한 확인에 사용될 수 있다. 중재 서명은 송신자 조건이 추가로 관련된다. 이 경우는 신뢰성 있는 제삼자가 데이터의 정확성과 송신자 신분을 수신자에게 증명한다. 이를 위하여는 디지틀 공증 메커니즘이 결합되어야 한다.

- 액세스 제어
  사용자의 신분이 확인된 후에 그 사용자가 명시된 자원을 액세스할 자격이 있는가를 점검하고 다음에는 어떤 유형의 동작을 수행할 수 있는가에 대한 허락을 받도록 한다. 이를 위해서는 다음과 같은 여러가지 세부 메커니즘이 사용될 수 있다.
- 액세스 제어 목록 :
  어떤 주체에 대하여 액세스 대상이 되는 객체와 허용되는 동작의 종류를 나타내는데 주로 행렬구조를 사용한다.
  - 패스워드(Password)
  - 권능(Canahility) 목록 :
    액세스 제어 목록과는 반대로 어액세스 제어 목록과는 반대로 어떤 객체에 대하여 액세스가 허용되는 주체와 수행 가능한 동작의 목록을 명시한다. 보다 유연성 있고 효율적인 메커니즘으로 인식되고 있다.
  - 크리덴셜(Credentials) :
    어떤 실체로부터 다른 실체로 전달되는 데이터로서 송신 실체의 액세스 전환을 확립하는 데에 사용된다.
  - 라벨(Labels)
- 데이터의 정확성
  - 체크섬
  - 타임스탬프 등을 이용하는 순서 제어
- 실체의 신분 확인
  - 패스워드
  - 암호 메커니즘
- 교통의 패딩(Padding)
  실제 데이터가 아닌 정보를 안전성 제공의 목적으로 고의적으로 삽입할 수가 있다.
- 경로 제어
  어떤 수준의 안전성을 달성하는데에 필요하거나 유용한 전송 경로(물리적 이거나 논리적)를 선택할 수 있도록 한다.
- 공증
  안전성 서비스를 제공하는 데에 있어 송신자가 수신자가 아닌 제삼자의 위치에 있는 중재자의 개입을 통하도록 한다. 이는 보통 디지틀 서명 메커니즘과 함께 사용되며 송신 사실의 부인과 수신 사실의 부인을 봉쇄하는 데에 필요하다.
- 세방향 교환
  정보가 전달 과정에서 상실되거나 중복되는 것을 정확히 검출하여 필요한 동기를 행할 수 있게 한다.

데이터의 정확한 서비스를 실현하는 데에 유용하다.

관리

적절한 메커니즘을 사용하여 서비스를 실현하게 되는데 서비스를 지속적으로 제공하기 위해서는 적절한 관리 절차가 수행되어야 한다. 이를 위해서는 필요한 제어 정보를 데이터베이스 형태로 유지 갱신하여야 하고 안전성 관련 사건을 일지 형태로 기록, 유지하여야 한다. 또한 필요할 때에 사건 기록을 검색하고 분석을 수행하여야 한다. 키 배분 센터 등의 관리를 위하여 필요한 조직도 구성하여야 한다.

OSI계층 구조와 안전 체제

개방형 통신(OSI : Open System Interconnection) 구조에서 특정 서비스는 하나 혹은 하나 이상의 계층에서 제공될 수 있다. 하나 이상의 계층에서 제공될 때에는 어떤 계층은 그 서비스를 직접 제공하지 않고 하위계층이 제공하는 서비스를 이용할 수도 있다. 서비스를 직접 제공하지 않는 경우에도 안전성 서비스 요청을 하위계층에 전달하기 위하여 그 계층의 서비스 정의는 수정을 필요로 할 수 도 있다.

두개의 상이한 시스팀에 안전성 서비스가 연관되어 있는 때에는 두 시스팀의 안전성 계층 할당이 동일하여야 한다. 그렇지 않으면 호환성에 문제가 야기된다. 안전성 서비스를 계층에 할당하는 데에는 몇가지 원칙이 고려되어야 한다. ■