한국통신학회 1987년도 춘계학술발표회 논문집(1987. 5. 23)

87428

네트워크 안전성

김 동규
아주대학교 전자계산학과

Network Security

Kim, Dong Kyoo
Ajou University, Department of Computer Science

Abstract

The general problem definition of network security is presented in this paper, and the network security architecture under OSI environment is summarized with descriptions on generic services, mechanisms and management.

1. 서 론

정보통신의 개발과 이용이 광범위하게 확산되면서 관련되는 안전성 문제가 중요한 과제로 부각되고 있다.

정보통신에서 안전성은 그 자체로서 넓은 영역과 복합적인 속성을 갖는 하나의 분야를 이룬다.

안전성은 일반적으로 전자도청(Electronic Evaves-dropping)에 관련되는 문제를 지칭하지만 보다 넓은 범위로서는 통신과정에서의 여러가지 에러 문제도 포함한다.

본고에서는 일반적인 OSI 환경에서의 네트워크 안전성 문제를 개괄적으로 논의하고자 한다.

2. 안전구조(Security Architecture)

안전성 관련 사항은 광범위하고 복잡하다. 안전성 문제를 보다 체계적으로 용이하게 이해하기 위해서는 이를 하나의 구조로서 파악할 필요가 있다.

이 구조는 다음과 같은 사항을 포함하여야 한다.

- 문제의 정의(용어 및 기호 포함)
- 서비스
- 메카니즘
- 서비스,메카니즘,계층의 관계
- 서비스와 메카니즘의 계층 배치
- 관리
- 실현

3. 안전성 문제

정보통신의 안전성에 관련되는 제반 문제들을 고찰하여 보자.

- 물리적인 도청

음성,데이타,형상 등 여러 형태의 정보는 통신 진행과정에서 물리적으로 도청될 수 있다(Tapping,Bug 등). 이는 물리적 매체상에서 정보가 노출되는 것을 말한다.

- 능동적인 안전성 위해

시스템의 상태에 대한 불법적인 변경을 행하는 것으로 여기에는 다음과 같은 종류가 있다.

-전문 수정
-전문의 Replay
-전문의 삽입
-신분 코드(id)의 조작
-억세스 권한의 조작
-서비스의 거부:여기에는 여러 가지 사항들이 포함된다. 하나의 통신 실체가 적절한 기능과 동작을 수행하지 않음으로써 다른 실체들의 적절한 기능 수행을 저해하는 것이다. 이런 형태의 위해는 특정한 목표를 지닐 수 있다. 예를 들면, 어떤 실체가 어느 특정 목적지로 향하는 모든 전문을 고의로 파기할 수 있다(예를 들면,안전성 Audit 서비스). 더 나아가 전문 파기는 보다 일반적으로 행하여 져 어떤 실체가 모든 전문을 파기할 수도 있다.

위에서 언급된 것 외에도 이러한 종류의 위해는 불필요한 전문을 만들어 내는 것도 포함된다. 하나의 실체가 어느 특정 목적지로 향하는(혹은 어떤 특정 경로를 거치는) 연속적인 전문 대열을 생성하는지, 혹은 무작위적으로 전송할 수도 있다.

하나의 실체가 네트워크의 정상적인 작동을 교란할 의도로 전문을 생성할 수 있다. 특히 전문의 중계기능을 담당하는 실체들이 다른 중계 실체들로부터 들어오는 상태정보에 입각하여 경로제어 결정을 내리는 네트워크가 심각한 위해를 받을 수 있다.

- 안전체제 해독

어떤 안전 체제와 관련된 입력 및 출력을 분석하여 비밀번수나 민감한 데이타를 인출해 내는 것을 말한다.

- 수신 날조

전문을 수정하거나 위조한 후 상대측으로부터 수신되었다고 주장하는 것을 말한다.

- 수동적인 위해

시스템의 상태 변경없이 정보가 노출되는 것을 말함.

- 물리적 안전성

고의적이거나 우연의 위해에 대해서 자원의 물리적 보호를 제공하기 위해 사용되는 방법.

- 교통 분석

교통 흐름의 관측으로부터 정보의 존재,부재,분량 방향,빈도 등을 유추하는 것.

- 교통 Padding

날조된 통신 사안(Instance),데이타 단위,데이타의 생성.

4. 안전성 서비스

제공될 수 있는 각종 안전성 서비스를 체계적으로 고찰하여 보자.

- 대등 실체(Entity),확인(Authentication)

이 서비스는 연결의 확립 혹은 데이타 전파 단계에서 제공되는 것으로 연결된 실체의 신분(id)을 확인하기 위한 것이다. 즉 관련되는 실체가 자기 신분을 날조하거나 혹은 지난 번 연결을 되풀이 하여 보이고 있지 않음을 확신하기 위한 절차이다.

- 억세스 제어

통신 시스템 내에서 억세스 할 수 있는 자원을 허락없이 불법적으로 사용하는 것을 방지하기 위한 서비스이다.

대상이 되는 자원은 집단 혹은 개체 별로 취급될 수 있고 제어의 대상도 자원 그 자체 뿐만아니라 그 자원에 대하여 행하여 지는 억세스 행위(예:Read,W-

rite,Update 등)가 될 수 있다.

● 데이타 기밀성

데이타가 불법적으로 노출되는 것을 보호하기 위한 서비스이다. 다음과 같이 세분될 수 있다.

-연결지향적 통신환경에서 사용자 데이타 기밀유지

-무연결 통신환경에서의 사용자 데이타 기밀유지

-선택되는 필드의 기밀성

-교통흐름 안전성:교통의 흐름을 관측함으로써 인출하여 낼 수 있는 정보를 보호

● 데이타 정확성 및 일치성

동적인 위해로부터 데이타의 정확성과 일치성을 유지.

-연결 서비스 지향의 모든 사용자 데이터의 정확성 보장 서비스로서 정보 데이타의 변조,삽입,삭제, Replay 등을 검출하고 복구를 시도한다.

-위와 동일하나 복구를 시도하지 않는다.

-연결통신 서비스,선택 필드의 정확성

-무연결,정확성

-무연결,선택 필드 정확성

● 데이타 근원 확인

통신되는 데이타의 근원이 정확함을 확인하여 준다(보통 계층 - N이 N+1에 제공하는 서비스 형태로 됨).

● 불법적인 부인 봉쇄

-전송 부인 봉쇄:정보 전송측이 나중에 고의적으로 데이타 전송 사실을 부인할 수 없도록 수신측에게 데이타의 발생원에 대한 증명이 제공된다.

-수신 부인 봉쇄:반대의 경우로서 수신측이 고의적으로 데이타 수신 사실을 부인할 수 없도록 전송측에게 데이타의 배달 증명이 제공된다.

5. 메카니즘

지금까지 언급된 서비스를 계층 N이 계층 N+1에게 제공하는 데에 사용될 수 있는 메카니즘을 논하여 보자. 어떤 종류의 서비스이든지 그 천실을 위해서는 적절한 메카니즘이 필요하게 된다.

● 특정 서비스를 위한 메카니즘

-암호화:데이타 혹은 교통 흐름 정보의 기밀성을 제공하기 위한 메카니즘이다. 암호화 알고리즘에는 두 가지 일반적인 유형이 있다:

1) 대칭형 암호화(예:비밀 키)에서도 암호화 시키는 키를 알면 암호를 푸는 키도 알게 되어 있고 그 역도 성립한다.

2) 비대칭형 암호화(예:공용 키)에서는 암호화 키를 알더라도 암호를 푸는 키는 알려지지 않는다. 이 역도 성립한다. 이러한 시스템의 두 가지 키를 공용키,사용 키라고 부른다.

암호화 메카니즘의 존재는 키 관리 메카니즘의 사용을 의미한다.

-디지탈 서명 메카니즘:이 메카니즘은 다음의 두 절차를 정의한다:

1) 데이타 단위에 서명

2) 서명된 데이타 단위의 검증

첫번째 절차는 서명자의 사용 정보(즉, 서명자에게만 고유한 기밀 사항임)를 사용한다. 두번째 절차는 공용적으로 알려져 있는 정보와 절차를 사용한다. 그러나 그로부터 서명자의 사용 정보는 유추될 수 없다. 이 과정을 한번 명시하여 보자.

서명 과정에서는 데이타 단위의 암호화나 혹은 데이타 단위의 암호검사 기능의 생성이 포함된다(서명자의 사용 정보를 사용 키로 사용).

다음 검증단계에서는 공용절차나 정보를 사용하여 서명이 서명자의 사용 정보를 사용하여 생성되었는지의 유무를 결정한다.

서명 메카니즘의 본질적인 특성은 서명이 서명자의 사용 정보에 의해서만 생성될 수 있다는 점이다. 따라서 서명이 검증된 후에는 오직 그 사용 정보의 소유자만이 서명을 행하였으리라는 점을 제3자(예:판정자 혹은 중재자)에게 언제든지 증명할 수 있다.

-억세스 제어 메카니즘:이런 메카니즘은 하나의 실체의 확인된 신분 혹은 그 실체에 관한 신빙성 있는 정보(예:알려진 실체 집합의 회원증 혹은 그 실체의 권능(Capability로 불리워 짐)이나 자격)를 사용하여 어떤 실체의 억세스 권한을 결정하고 집행한다. 실체가 억세스 자격이 부여되지 않는 자원을 사용하려고 시도할 때에는 억세스 제어기능에 의하여 그 시도는 거부되며 이 사건은 보고되어 경고를 발하든지 혹은 사건기록의 일부로 남게 된다.

억세스 제어 메카니즘은 다음 사항들의 사용에 그 기반을 둘 수 있다:

1) 억세스 제어정보 베이스:여기는 어떤 내등실체가 자원들에 대하여 갖는 억세스 권한이 유지된다. 이 베이스는 제어센터나 혹은 억세스되는 실체에 의하여 유지된다. 이 정보는 제어목록,행렬,계층적인 혹은 분산 구조를 취할 수 있다. 억세스 제어는 관련 대등실체의 신분확인이 이미 이루어 졌음을 전제로 한다.

2) 패스워드(Passwords):이를 소유하고 필요시에 제시함은 억세스하는 실체의 신분에 대한 증빙이 된다.

3) 권능(Capability):이를 소유한 후에 제시하면 이 권능에 정의된 실체나 자원에 대한 억세스 권한의 증빙이 된다.

4) 안전성 레이블(Lable):이 레이블이 실체와 연관될 때에는 안전성 정책에 따라서 억세스가 허용되거나 거부될 수 있다.

-데이타 정확성 보장 메카니즘:단일 단위나 필드 혹은 이들의 대열에 대한 정확성 보장을 고려할 수 있다. 전송측과 수신측에서 행하여 지는 프로세스가 따로 있다. 전송측에서 데이타에다 어떤 값을 첨가하고(이 값은 블럭검사 코드, 다른 형태의 잉여정보, 혹은 암호검사 기능)수신측에서는 이에 대응되는 값을 따로 생성하여 수신되는 값과 비교한다. 일단의 데이타 단위의 정확성 보호(순서 도치, 상실,Replay,데이타 삽입 혹은 수정)는 별도로 어떤 형태의 순서 번호와 타임 스탬프를 사용할 수 있다.

-신분 확인을 위한 전문 교환 메카니즘

-교통 패딩(Padding) 메카니즘

-경로 제어 메카니즘

-공증 메카니즘

6. 계층 관계

지금까지 논의한 서비스와 메카니즘은 통신구조의 계층과 연관된다. 즉, 어떤 서비스는 어느 특정 계층에만 연관될 수 있다. 물론 하나 이상의 계층에 관련될 수도 있다. 계층과 각 서비스의 상관성이 잘 고찰되어야 한다.

이 것이 본고의 초반에 정보통신의 안전체제는 그 자체로 규모가 크고 복잡한 속성을 지닌다고 말한 이유이다.

7. 관 리

안전체제의 실행은 여러가지 사항에 대한 관리를 수반한다. 몇가지 예를 들어 보자:

● 신분 확인관리

● 억세스 제어관리

● 키 관리

● 관리기록 유지와 관련 사건처리

8. 결 론

네트워크 운용의 광범위한 확산에 따라서 네트워크 안전성 문제의 중요성이 급격히 대두되고 있다.

일반적인 OSI 네트워크 환경에서의 정보통신 안전성 문제는 관련되는 서비스의 정의, 그 실현 메카니즘 그리고 management의 문제로 요약될 수 있다. 이를 바탕으로 사용자 요구 사항을 만족시키기 위한 실현이 뒤따라야 한다.

참고 문헌

[1] John Horgan,"Thwarting the information thieves", IEEE Spectrum,July 1985.

[2] ISO TC97/SC 21 N931,Information Processing System-Open Systems Interconnection-PDAD 2 to ISO 7498 on Security Architecture,1986.