通信情報保護學會誌
第1卷, 第3號, 1991. 12

전산망의 안전대책 개요(II)[1]

이필중[2] · 정진욱[3] · 박명순[4] · 이재용[5]

3.3 안전 서비스별 대책

안전에 관한 서비스는 여러가지 있겠으나 여기에서는 특히 정보 그 자체의 안전 서비스에 관해서만 상세히 고려해 본다.

3.3.1 인증(Authentication)

많은 개발 시스템 응용분야들은 각 정보의 비밀정도에 따라 보안 요구사항이 달라진다. 이러한 요구사항에는 인증(authentication), 접근 제어(access control), 무결성(integrity) 등과 같이 공격자에게 알려지면 서비스의 효과를 감소시키거나 또는 아주 없앨 수 있는 보안 서비스를 제공하는데 쓰이는 정보에 대한 보호(Protection)가 포함된다.

3.3.1.1 정의

전산망의 사용에서는 여러가지 많은 실체들이 확인될 필요가 있을 수 있다. 이에 해당되는 물리적인 실체(예, 하나의 컴퓨터 시스템), 논리적인 실체(예, 통신계층의 각 실체) 그리고 인간 자체이다. 인증이란 이러한 실체를 가장(Masquerade)하여 전산망에 침입하는 경우를 대비하여 보호화 정보의 재사용으로 인한 실체에 대한 위협에 대응하는 작업을 의미한다.

이러한 인증은 아래의 4가지 원리에 기초한다.

- 무언가 알고 있는 것(예 : 비밀 패스워드)
- 무언가 소유하고 있는 것(예 : IC 카드)
- 무언가 모방할 수 없는 특징(예 : 망막무늬)
- 확인되고 믿을 수 있는 제3자의 인증을 받아들임.

3.3.1.2 인증 서비스의 구성

인증서비스의 구성단계는 설치, 분배, 수집, 전달, 확인, 삭제 등의 6단계로 나눌 수 있다. 설치단계에서는 요구자 인증정보와 확인자 인증정보가 등록, 유효화, 확인 등의 세부 단계를 거친다. 분배단계는 임의실체가 확인에 필요한 인증 정보를 사전에 분배해 갖는 과정이며, 수집 단계는 인증 요구자에 의해 특별한 형태의 인증서를 만드는 과정

---

(1) 본 연구는 전산원의 전산망관리 표준화연구회 보안관리 소위원회에서 1990년에 행해졌던 연구의 결과임.
(2) 정회원, 포항공과대학 전자전기공학과
(3) 정회원, 성균관대학교 정보공학과
(4) 정회원, 고려대학교 전산과학과
(5) 정회원, 포항공과대학 전자계산학과

이다. 전달 단계는 요구자가 인증을 위해 인증서를 전달하는 과정이며 확인 단계는 인증서를 조사하는 단계이다. 등록제거 단계는 한 주체를 인증할 수 있는 집단에서 제거하는 단계이다.

3.3.1.3 인증의 사용

인증은 두가지 목적으로 사용된다. 하나는 데이타 발신 인증으로, 데이타의 발신지를 증명하는데 사용된다. 다른 하나는 관련 당사자간 인증으로 원격지에 있는 상대를 인증하는 것이다. 인증은 일방 또는 쌍방간 인증으로 분류되기도 하는데 데이타 발신증명은 일반 인증이고, 당사자간 인증은 쌍방 인증이다. 인증의 신뢰는 쌍방 또는 다수 관련자 사이의 신뢰에 따라 분류되는데 양자간 신뢰는 쌍방이 서로 믿는 경우이며, 상호 합의한 패스워드나 키에 근거한다. 이 방법은 당사자의 수 증가치의 제곱(square)에 비례하여 인증 정보가 증가하게 된다. 다자간 신뢰는 믿을 수 있는 제 3 자가 관련된다. 제 3 자는 인증절차에 온-라인이나 오프라인으로 인증에 참여하게 된다.

인증이 사용될 때 아래와 같은 사항들이 고려되어야 한다.

• 인간 사용자의 인증 : 이 경우는 인간과 기계와의 대화가 수반되며 위장 침입의 가능성이 높다. 따라서 인간에게 적절하고, 경제적이며, 안전한 방법이 요구된다.

• 대리승계 : 인증 실체의 대리자가 시스템내에 발생하는 경우, 대리자의 인증 승계도 고려되어야 한다. 여기에 대한 예는 한 시스템에서 로그-온하면 망 대리자에 의해 다른 시스템에도 자동적으로 로그-온된다. 대리자는 인증 실체와 인증 당국자의 이름이 복합된 신분을 갖는다.

• 계속적인 인증 : 인증이 어느 순간에만 유효한 것임을 고려하여 계속적인 인증서비스를 제공하는 것이 고려되어야 한다. 이를 위해 간헐적으로 인증행위를 수행하는 방법과 계속적으로 인증 서비스와 무결성 서비스를 연결시키는 방법이 있다.

3.3.1.4 인증 정보

일반적인 인증 정보란 요청자와 확인자 사이에 인증과정에서 전달된 데이타를 말하는데 이 중 인증서의 특이한 형태로 인증 토큰이라는 것이 있다. 이는 인증 당국자에 의해 보증된 데이타형 보증서이며 인증토큰에 포함되는 요소는 다음과 같다.

1) 암호화 체크섬(checksum)을 만들어낸 방법의 식별
2) 인증 당국자의 신분과 인증 토큰 발행기관의 신분
3) 인증 당사자의 신분
4) 데이타의 지문
5) challenge 또는 독특한 숫자
6) 토큰 생성시간
7) 토큰 유효기간
8) 토큰이 관련된 당사자의 속성이나 신분
9) 토큰이 적용될 수 있는 정책
10) 토큰을 얻기 위해 사용된 인증방법
11) 인증 참고번호

3.3.1.5 인증 서비스

인증에 관한 서비스는 아래와 같은 것이 있다.

1) 인증 정보의 설치
2) 인증
3) 인증 정보의 변경
4) 인증 종료
5) 인증 회복
6) 인증서 조사

3.3.1.6 인증체계와 방법의 분류

인증체계와 방법의 분류는 다음과 같다.

1) class 0 : 비 보호
2) class 1 : 노출로부터 보호
3) class 2 : 재사용(replay)이나 가장(masquerade)으로부터 보호

class 0는 인증정보의 노출을 포함해서 여러 위협에 취약하다. 이 분류급에서는 요청자의 신분과

인증정보만이 단순히 따라간다(아래 그림 참조).

인증요청＋신분＋요청자의 인증정보

class 1에서는 인증정보의 노출은 방지된다. 그러나 재사용에 약하다. 인증정보 부분 등의 선택된 부분에 암호화(F) 또는 일방향 함수(One-Way Function)를 적용하는 방법이 있다(아래 그림 참조).

인증요청＋신분＋F(요청자 인증정보)

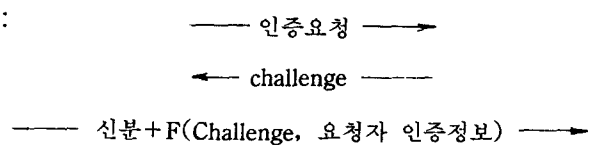
인증요청＋신분＋OWF(요청자 인증정보

class 2의 방법은 재사용등의 위협에서 보호되며, 암호화 체인을 사용하거나 유일한 숫자를 사용하게 되는데 Challenge 방법이 사용된다.

암호화 체인 : 인증요청＋신분＋F(요청자 인증 정보)

유일한 숫자이용 : 인증요청＋신분＋F(유일한 숫자＋요청자 인증정보)

challenge 방법 :



이외에 전담된 Challenge 기법, 계산된 응답법 등이 있으며 3단계 hand-shaking을 한다.

3.3.2 접근제어(Access Control)

3.3.2.1 정의

접근제어라 함은 전산망에서 자원의 사용가능 여부를 결정하는 과정을 말하며 컴퓨터 혹은 통신 시스템의 요소들에 관련되는 비인가된 동작들의 위협(인증되지 않은 사용, 폭로, 변형, 파괴, 서비스 부인 등)에 대하여 자원을 보호하는데 그 기본 목적을 두고 있다.

3.3.2.2 접근 제어의 기능

접근 제어를 수행하는데 있어서 기본적으로 필요한 실체(entity)와 기능으로는 개시자(initiator), 접근제어 시행기능, 접근제어 결정기능, 그리고 목표물(target)이 있다. 여기서 개시자는 다른 실체에 접근을 시도하는 실체인 사용자와 컴퓨터에 관련된 실체들을 의미하고, 접근제어 시행기능이란 개시자와 각 프로세서의 목표 노드사이에 접근경로의 부분을 담당하는 기능을 말하며, 접근제어 결정기능이란 개시자가 목표물에 접근하여 제어 결정을 담당하는 기능을 말한다. 이 제어 결정에는 접근제어 정책, 규칙 접근제어 정보, 요구된 행동 등이 이용된다. 목표물은 개시자에 의해 접근되는 실체를 의미한다.

3.3.2.3 접근제어 활동(Activity)

실제 시스템에서의 접근제어를 위해서는 아래와 같은 활동이 이루어져야 한다.

• 접근제어 정책 표현 확립 : 접근제어는 실세계(real-world)정책에 따라 수행되는데, 이러한 정책들은 접근제어 기능에서 수행될 수 있는 규칙들의 집합으로 표현되어야 한다.

• 접근제어 정보의 확립 : 여러 접근제어 정보가 실시스템에서 어떻게 표현되어야 하는지가 결정되어야 한다.

• 접근제어 데이타 값의 각 보안 영역 요소내에 할당 : 보안 영역 담당자는 보안정책이 해당 보안 영역에 있는 각각의 요소에게 어떻게 적용해야 하

는지를 결정해야 하는데, 이러한 보안정책은 각각의 요소에 관련된 실세계 접근제어 속성들의 집합으로 표현된다. 결국 이러한 속성들이 해당 보안 요소들에 대한 접근제어 데이타의 내용을 결정하게 된다.

• 접근제어 정보를 접근제어 기능이 이용 가능토록 함 : 접근제어 기능이 해당기능을 수행하기 위해서 여러가지 필요한 접근제어 정보가 있어야 한다. 여기에서 실체의 실제적인 위치, 접근제어 기능 또는 실제 접근제어 정보에 관련하여 어떠한 가정도 있어서는 안된다.

3.3.2.4 접근제어 정보의 속성

접근제어 정보는 아래와 같은 세가지의 속성을 갖는다.

• 특권속성(Privilege Attribute) : 개시자로서의 역할로 사용되기 위해 실체에 속한 속성

• 데이타 보안 속성(Data Security Attribute) : 데이타에 속한 속성

• 제어속성(Control Attribute) : 목표물로서의 역할로 사용되기 위해 실체에 속하는 속성

3.3.2.5 접근제어 기능의 위치

접근제어 시행기능과 접근제어 결정기능은 시스템의 내부 또는 외부에 존재할 수 있다.

3.3.2.6 접근제어 서비스의 설계원칙

접근제어 서비스는 아래와 같은 설계원칙을 따른다.

• 특권의 최소화(Least privilege) : 모든 주체에 대한 접근에의 권한은 그 임무에 대해 최소화한다.

• 메카니즘의 간소화(Economy of mechanisms) : 보호 메카니즘은 간소화되어야 한다.

• 수용성(Acceptability) : 보호 메카니즘은 사용되기에 간편해야 한다.

• 완벽한 중재(Complete mediation) : 모든 객체에 대한 접근이 구현되어야 한다.

• 개방된 설계(Open design) : 메카니즘이 공개되어야 한다.

3.3.2.7 접근제어 소프트웨어의 검토(Review)를 위한 검사항목(Check List)

① 정보 보안 접근제어 소프트웨어(Information Security Access Control Software)가 하드웨어와 운영체제를 위해 제공되는가?

② 정기적으로 만나서 보안 소프트웨어 패키지에 대한 확장을 요구할 수 있는 소프트웨어 판매 사용자 그룹이 있는가?

③ 소프트웨어 판매자는 소프트웨어 패키지의 사용에 관한 연수과정을 제공하는지 그리고 그 패키지를 사용하는 보안 관리자에게 보안에 대한 일반적인 정보에 대한 연수과정을 제공하는가?

④ 보안 소프트웨어가 모든 종류의 화일 구조와 프로그램을 통제하기 위해 사용될 수 있는가?

⑤ 보안 소프트웨어가 접근이 허락되지 않는 경우에 이러한 접근을 묵인할 수 있는 기본적인 레벨의 제어를 제공하는가?

⑥ 보안 소프트웨어가 조직의 모든 요구사항에 일관될 수 있도록 접근 규칙을 만드는데 있어서 유연성(flexibility)을 제공하는가?

⑦ 보안 소프트웨어를 더욱 안전하게 하기 위하여 보안 매니저에게 적어도 8문자의 패스워드를 구성할 옵션을 허락하는가?

⑧ 패스워드의 보안 소프트웨어의 다른 키 요소가 다른 사람에게 참조될 수 없도록 비밀화(encryption)되는가?

⑨ 보안 소프트웨어는 패스워드가 인정될 때까지 어떤 동작도 하지 않으므로서 로그-온 보호(log-on Protection)를 제공하는가?

⑩ 보안 소프트웨어는 사용자가 연속해서 부적절한 패스워드를 시도할 때 터미널에서 자동적으로 로그아웃(log-out)할 수 있는 기능을 가지고 있는가?

⑪ 보안 소프트웨어는 모든 보안에 관련된 트랜잭션(transaction)이 보호된 로그화일에 기록될 수 있는 보호 로깅 기능(protected logging facility)을 가지고 있는가?

⑫ 보안 소프트웨어는 보안 위반 시도에 대해 자동 레포트를 제공하는가?

⑬ 보안 소프트웨어는 보안 관리 기능에 필요한 여러가지 정보에 관련된 보안 레포트를 할 수 있는 유연성을 제공하는가?

⑭ 보안 소프트웨어에 의해 만들어진 상태 레포트나 위반 레포트가 보안 관리 구역에 있는 터미널이나 프린터에 접근 가능할 수 있도록 제한되어 있어야 한다.

⑮ 보안 소프트웨어 판매자는 보안 관리자에게 전화 혹은 온라인으로 도움을 줄 수 있는가?

3.3.3 비밀 보장(Confidentiality)

3.3.3.1 소개

데이타의 비밀성을 유지하는 것을 비밀 보장(Confidentiality)이라 한다.

3.3.3.2 범주와 응용 분야

보안 체계(framework)는 데이타 요소와 특정 보안 서비스를 하기 위해 사용되는 일련의 동작(operation)을 다룬다. 이러한 보안 서비스는 시스템간에 교환되는 데이타와 시스템이 관리하는 데이타 뿐만 아니라 시스템들에 있어서의 통신 실체(communication entities)에도 적용된다.

이 절에서는 검색, 전송, 관리되는 데이타의 비밀화에 대하여 다룬다. 이것은 다음을 포함한다.

- 기본개념을 정의한다.
- 비밀화 메카니즘의 가능한 등급을 표시한다.
- 비밀화 메카니즘의 등급들에 따르는 서비스와 필요한 추상형 데이타 타입(abstract data type)을 정의한다.
- 비밀화 메카니즘의 등급들을 지원해 주는데 필요한 관리를 표시한다.
- 비밀화 메카니즘과 이의 지원 서비스들과 다른 보안 서비스 및 메카니즘 사이의 상호작용하는 것을 다룬다.

이 밖에도 비밀화를 위해 수행될 필요가 있는 프로토콜 교환에 대해서도 관심을 두어야 한다.

3.3.3.3 비밀화(Confidentiality)에 관한 일반적인 논의

비밀화(Confidentiality)는 권한이 없는 사용자, 실체, 프로세스에게는 이용가능하지 않게 숨겨지는 데이타의 특성이다. 비밀화 메카니즘은 권한이 없는 사용자에게 이용가능한 데이타를 이용 가능하지 않은 데이타(이를 confidential data라 함)로 만든다. 비밀화 서비스는 다음의 2가지 주요한 단계에서 이루어진다.

제 1 단계 은닉(Hide) : 데이타로부터 비밀화 데이타의 생성.

제 2 단계 노출(Reveal) : 비밀화 데이타로부터 원래 데이타의 재생성.

은닉되지 않은 부분과 비밀화된 데이타 부분 및 이미 노출된 부분 등으로 이루어질 수 있는 논리적 데이타 장치에서는 은닉 및 노출이 병렬적으로 이루어질 수 있다. 데이타 관리에서는 은닉/저장과 검색/노출이 조합되어 보다 높은 수준의 저장과 검색 서비스를 이룰 때에 비밀화가 이루어진다. 다른 형태의 비밀화는 은닉/노출이 다른 동작 등과 조합하여 달성될 수 있다.

비밀화 메카니즘은 다음의 두가지로 분류할 수 있는데 이들 각각은 다른 목표를 가지고 있다.

- 비밀이 요구되는 데이타가 우연히 권한이 없는 사용자, 실체 또는 프로세스에게도 이용가능하게 될 위협
- 비밀이 요구되는 데이타가 비밀화 메카니즘을 파괴하려는 고의적인 시도에 의해서 권한이 없는 사용자에게도 이용가능하게 될 위협

후자의 위협을 방지하는 메카니즘은 또한 전자의 위협까지도 방지한다. 여러가지 보안 이유 때문에 비밀화를 할 필요성이 있는 경우에는 후자 단계의 위협은 가정되어져야 한다.

3.3.3.4 고려사항

비밀화 서비스에서 고려할 점들로서는 구조적인 고려사항, 정책적인 고려사항 및 비밀화 위반에 대한 방지 등이 있다. 구조적인 고려사항에는 통신 비밀화 및 데이타 비밀화가 포함되며 비밀화 위반에

대한 방지로는 물리적 제어와 접근 제어가 포함될 수 있다.

3.3.3.5 비밀화 메카니즘

비밀화 메카니즘으로는 접근 제어방식에 의한 비밀화를 들 수 있는데, 비밀화 위반을 할 수 있는 잠재력이 있는 모든 자들이 접근 제어에 의해 관리될 수 있다면 접근제어 방식이 비밀화를 구현하는데 사용될 수 있다.

이 방식은 권한을 부여받지 못한 개시자(initiator)가 비밀정보를 알아낼 수 있는 목표물(targets)들에 접근을 시도하는 것을 막기 위해 접근제어를 이용한다. 어떤 개시자들은 목표물들처럼 행동할 수 있기 때문에 그러한 목표물들에 접근할 때 개시자로서 다른 목표물들로부터 알아낼 수 있는 정보를 알려주어서는 안된다. 이러한 것은 개시자와 목표물들에 허용되는 접근의 한계를 잘 제한하거나 정보가 목표물로부터 개시자로 전달될 때 정보 하나하나에 접근제어 정보(Access Control Information)를 유지하고 이에 근거하여 접근제어를 함으로써 이루어질 수 있다.

접근제어 방식에 의한 비밀화가 위협을 받을 수 있을 경우, 이중의 보호장치로 통신 및 데이타의 비밀화를 위하여 전송되거나 보관되는 정보가 암호화되어 보호되는 것도 필요하다. 이때 비밀화 서비스를 제공하는 기관은 암호화에 필수적으로 필요한 키 관리 문제도 해결해 주어야 한다.

3.3.4 무결성(Integrity)

3.3.4.1 정의

무결성은 권한을 부여받지 않은 방식으로는 변경되거나 파괴되지 않는 데이타의 특성을 의미한다.

3.3.4.2 범주와 응용 분야

여기서는 정보의 검색, 전송, 관리에 있어서 데이타의 무결성(Integrity)에 대해 다룬다. 즉,

- 기본 개념을 정의한다.
- 무결성 메카니즘의 가능한 등급들을 표시한다.
- 무결성 메카니즘의 등급들에 대한 서비스와 필요한 추상형 데이타 타입을 정의한다.
- 무결성 메카니즘의 등급을 지원하기 위해 요구되는 관리를 표시한다.
- 무결성 메카니즘과 지원 서비스들과 다른 보안 서비스와 메카니즘 사이의 상호작용을 다룬다.

여기서 다루어지는 무결성은 어떤 데이타 값이 가질 수 있는 다른 형태의 불변값에 의해서가 아니라 데이타 값의 불변화에 의해 정의된다. 특히 데이타가 표현하는 어떤 정보의 불변화를 말하지는 않는다. 프리젠테이션(Presentation) 계층보다 상위 계층의 무결성이 다루어지거나 커넥션(connection) 무결성 서비스에 의해 제공되는 어떤 순서의 무결성이 다루어질 때는 범주가 확장될 필요가 있다.

3.3.4.3 무결성의 일반적인 논의

무결성 메카니즘은 변경이나 삭제되기 쉬운 데이타를 무결성 보호 데이타로 변경한다. 무결성 보호 데이타는 검출이 안되면서 데이타의 변경이나 삭제가 되지 않는다. 무결성 서비스의 제공은 두 단계로 이루어진다.

- 차폐(Shield) : 데이타에서 무결성 보호 데이타의 생성
- 차폐해제(Unshield) : 무결성 보호 데이타로부터 데이타의 검사와 가능한 재생성

같은 논리적 데이타 장치가 차폐되지 않은 부분과 무결성 보호 데이타로 된 부분, 차폐 해제된 부분으로 이루어지는 경우에는 차폐와 차폐 해제가 순차적이 아니고 병렬적으로 이루어질 수 있다.

무결성의 다른 형태는 차폐와 차폐 해제가 다른 동작(예를 들면 데이타 관리의 목적으로 사용된 동작)과 조합함으로써 이루어질 수 있다.

- 복구 기능없는 차폐 해제 : 만약 차폐 해제가 무결성 보호 데이타의 변경이나 삭제를 나타내는 데이타에 적용된다면 차폐 해제 작업은 원래의 데이타를 되찾을 수 없어서, 에러를 내보낸다.

• 복구 기능을 가진 차폐 해제 : 만약 차폐 해제가 무결성 보호 데이타의 변경이나 삭제를 나타내는 데이타에 적용된다면 차폐 해제 작업은 원래의 데이타를 되돌려 줄 수 있다.

이와 같은 두가지 종류의 차폐 해제 작업은 무결성 서비스의 두가지 주요 분류법을 만들어 내는데, 이 두가지는 복구 기능이 없는 무결성과 복구 기능이 있는 무결성이다.

무결성 메카니즘에는 두가지 분류법이 있는데, 각각은 다른 목표를 가지고 있다.

• 무결성 보호 데이타에 대한 임의 수정이 가능한 환경에서 데이타 값의 불변화

• 무결성 보호 데이타에 대한 수정은 무결성 메카니즘을 파괴하도록 되어 있는 환경에서 데이타 값의 불변화

후자의 목표를 만족시키는 메카니즘은 물론 전자를 만족시킨다. 여러가지 보안 이유 때문에 무결성을 제공하려는 요구조건이 있는 곳에는 후자의 목표가 추구되어져야 한다. 여기서 논의되는 메카니즘은 후자의 목표를 다룬다. 이 목표를 충족시키기 위해서는 모든 잠정적 공격자는 제한작업(confined operation)을 수행할 수 없도록 확신하는 것이 필요하다.

3.3.4.4 고려사항

무결성 서비스에서 고려해야 할 점으로 구조적인 고려사항과 정책적인 고려사항이 있다. 구조적인 문제로서는 통신 무결성 문제와 객체 무결성 문제가 있는데 통신 무결성은 통신 계층에 의해 보호가 행해질 때, 전송되는 동안의 데이타의 무결성으로 이해되어지며 무결성 위반에 대한 예방이나 검출 및 복구에 대한 논의가 이루어져야 한다. 객체 무결성은 보호가 기본적인 보안 서비스에 의해 제공되는 것이 아니고 객체에 덧붙여졌을 때 저장중인, 또는 전송중인 동안의 데이타 무결성으로 해석되어진다.

무결성 위반에 대한 예방으로는 물리적 통제와 접근 제어가 있는데 이를 통하여 무결성 메카니즘의 필요성을 줄일 수 있다. 무결성 위반에 대한 검출과 복구 메카니즘은 서로 독립적이다. 무결성 서비스의 일반적 사용으로는 한 가지 이상의 보안 서비스가 무결성 서비스 메카니즘을 사용하여 다음과 같은 결합(binding)기능을 제공한다.

결합은 데이타의 두가지 이상의 요소가 함께 결합되어져 있기 때문에 요소들의 검출없이는 나누어지거나 수정되어질 수 없는 것을 말한다. 결합은 무결성 서비스를 데이타 요소의 연결에 적용함으로써 제공되어진다. 무결성 메카니즘의 구현방법으로는 메세지 확인 부호(MAC, Message Authentication Code)를 사용하여 적은 양의 고의적이 아닌 오류를 찾아 내어 고치는 방법이 있다. 그러나 오류 정정 부호를 사용할 때에는 그 오류가 고의에 의해 비롯된 것이라면 잘못 수정하고도 옳은 결과를 복호화해 내었다고 착각함으로써 보안 위협을 받을 수 있으므로 주의를 요한다.

3.3.5 부인봉쇄(Non-Repudiation)

3.3.5.1 정의

부인봉쇄는 데이터의 송신자가 송신 사실을 거짓으로 부인하는 것으로부터 수신자를 보호하기 위하여 발신 증거를 제공하거나 수신자가 수신 사실을 거짓으로 부인하는 것으로부터 송신자를 보호하기 위하여 배달 증거를 제공하는 보안서비스 중의 하나이다.

3.3.5.2 부인봉쇄의 종류

부인봉쇄 서비스에는 발신 부인봉쇄와 수신 부인봉쇄의 두가지가 있다. 발신 부인봉쇄 서비스는 메세지의 발신자가 추후 메세지의 발신 사실을 부인하는 것을 봉쇄하는 것이며, 수신 부인봉쇄 서비스는 메세지의 수신자가 추후 메세지의 수신 사실을 부인하는 것을 봉쇄하는 서비스이다.

두가지 서비스는 발신 및 수신 사실의 부인으로부터 발생하는 논쟁을 해결하는데 필요한 증거로서 활용이 가능하다.

3.3.5.3 제 삼자의 존재

부인봉쇄는 부인봉쇄로부터 야기된 논쟁을 조정하는 것을 주임무로 하는 상호간에 동의를 얻어 믿을 수 있는 제 3 자(agreed trusted third party)의 존재를 전제로 한다.

부인봉쇄 서비스 중의 하나로서 믿을 수 있는 제 3 자는 증거를 기록할 수 있고 실시간으로 증명서를 발급할 수 있는 공증인이다. 다른 부인봉쇄 서비스에서의 믿을 수 있는 제 3 자는 증명이 발급된 시간에 충분히 가까운 시간내에 증거를 기록해야 하는 공증인이다.

두가지 경우 모두 믿을 수 있는 제 3 자는 논쟁을 해결하는 일을 담당한다. 그러나 논쟁을 해결할 수 없는 경우도 있다. 이 경우는 믿을 수 있는 제 3 자와의 통신 수단이 일시적으로 끊긴 경우에 나타난다.

3.3.5.4 메카니즘

서비스는 디지탈서명, 암호화, 데이타 무결성, 공증 메카니즘의 응용에 의해 제공된다. 서비스는 문제가 된 응용의 보안 요구에 적절한 메카니즘의 조합을 이용한다. 기본적인 공증 서비스는 기술적인 그리고 기능적인 선에서 기술된다. 이는 비밀리 그리고 확인된 방법으로 공증하는 서비스를 수행하는 공증인에게 서명, 암호화, 무결성 메카니즘을 이용하는 기능적인 사양을 포함한다.

보안과 관련된 변수에 의존하지 않는 데이타 교환과 관련된 어떤 특성을 확인하기 위해서는 또다른 메카니즘에 의존한다.

3.3.5.5 부인봉쇄의 수행절차

〈배달증명에 의한 부인봉쇄〉

배달증명에 의한 부인봉쇄는 수신자가 데이타의 수신 사실이나 그 내용을 거짓으로 부정하는 것을 방지하기 위한 것이다. 이 서비스가 효과적이 되려면 부인봉쇄 메카니즘은 데이타가 수신자에게 전송되기 이전에 시작되어야 한다. 그렇지 않으면 수신자는 데이타를 조사해 보고 서비스를 계속 진행시킬 것인지를 결정하여 후에 데이타의 수신을 부정할 수도 있게 해주는 것이다.

배달증명에 의한 부인봉쇄 서비스는 믿을 수 있는 제 3 자의 이용에 의해 이루어질 수 있다. 제 3 자가 단순히 데이타를 전송하고 데이타 전송을 공증하는 것만으로는 수신자가 데이타를 수신하였다는 증거를 제공하기에 충분치 못하다. 수신자는 통신 회선이 고장나서 데이타가 수신되지 않았다고 주장할 수도 있다. 통신 회선이 정말로 고장이었는지 시스템이 통신 회선이 고장난 것처럼 꾸몄는지를 구별할 수 있는 방법은 쉽지 않다. 믿을 수 있는 제 3 자와의 통신이 일시적으로 사용 불가능하였을 때 이 문제를 해결하는 방법은 없다.

두가지 경우를 구별하기 위하여 데이타 그 자체를 보내기 전에 메세지를 보내는 것이 도움이 될 수 있다. 그러나 두 메세지 사이에 정말로 통신 회선이 고장날 가능성은 여전히 존재한다. 첫번째 메세지는 최소한 데이타의 압축 요약(hashed summary)과 시간 인장(time stamp)으로 이루어지는 "수신 의향" 메세지이다. 수신 의향이 있는 수신자는 제 3 자가 데이타를 보내기 전에 그 메세지에 서명해야 한다.

이것으로 더 이상의 문제를 제기해서는 안된다. 왜냐하면 통신의 장애시 믿을 수 있는 제 3 자는 장애사실을 기록하고 통신의 재확립을 위해 노력하기 때문이다.

〈발신처 증명에 의한 부인봉쇄〉

1) 제 3 자와 실시간 상호 작용 없이 발신처 증명의 형성

발신증명을 통한 부인봉쇄는 두 단계로 이루어진다.

〈1단계〉 메세지의 발신자는 그의 개인 키로 직접 서명을 생성할 수 있다. 이때 서명의 요소는 다음과 같다.

- 서명될 메세지의 디지탈 지문(메세지에 대해 단방향 해싱함수(hashing function)를 적용하여 얻음).

- 발신자 이름
- 서명한 날짜, 시간

그리고 메세지와 함께 전송되어야 할 요소는 다음과 같다.

- 서명시 사용한 암호와 알고리즘을 포함한 방법의 식별자
- 서명시 사용한 개인키의 식별자
- 서명된 메세지의 디지탈 지문
- 발신자의 서명

위의 항목들이 모두 포함된 메세지를 서명된 메세지라고 부른다.

〈2단계〉 메세지의 발신자나 수신자는 현재 시간을 정확히 유지하고 있고 믿을 수 있는 제3자와 접촉한다. 이 경우 믿을 수 있는 제3자를 "시간표시 서비스"(Time Stamping Service)라고 부른다.

시간표시 서비스는 그 자신의 개인 키를 사용하여 서명된 메세지에 자신의 서명을 한다. 서명된 메세지에 포함된 날짜와 시간은 현재의 날짜와 시간에 충분히 가까워야 한다. 시간표시 서비스는 발신자의 신원(identity)에 대해서 알 필요가 없고 그가 하는 것을 기록할 필요도 없다. 시간표시 서비스에 서명하는 것을 대응 서명(Counter Signature)이라고 부른다.

서명된 메세지에는 아래와 같은 사항이 포함된다.

- 서명된 메세지의 디지탈 지문
- 발신자의 이름
- 서명된 날짜와 시간
- 발신자의 서명

대응 서명의 일부가 될 요소들은 다음과 같다.

- 서명된 메세지의 디지탈 지문
- 발신자의 이름
- 서명된 날짜와 시간
- 발신자의 서명
- 시간표시 서비스의 이름
- 반대서명이 이루어진 날짜와 시간

시간표시 서비스에 의해 되돌려져야 할 요소는 다음과 같다.

- 대응 서명을 할 때 이용된 암호 알고리즘을 포함한 방법의 식별자
- 대응 서명을 할 때 사용된 개인키의 식별자
- 시간표시 서비스의 이름
- 대응 서명이 이루어진 날짜와 시간
- 시간표시 서비스의 대응 서명

이 요소들은 서명된 메세지와 연관될 필요가 있고 안전한 장소에 보관되어야 한다.

2) 제3자들과 실시간 상호작용에 의한 발신처 증명의 생성

발신자가 직접 서명할 수 없는 경우에는 제3자와의 실시간 상호작용이 필요하다.

* 개인키/공중키 기술의 이용

이 경우 발신자는 믿을 수 있는 제3자에게 서명의 권한을 위임한다. 이러한 제3자를 "서명 서비스"라고 부른다. 이 서비스는 다시 서명 서비스가 발신자의 권한 위임에 의해 자기 자신의 개인키를 이용하는 경우와 발신자의 개인키를 이용하는 경우로 나눌 수 있다. 서명 서비스의 개인키가 이용되는 경우에는 서명과 서명된 메세지에 두개의 이름을 포함시킬 필요가 있다.

- 발신자의 이름
- 서명자의 이름

서명자에게 제시되어야 할 요소는 다음과 같다.

- 서명될 메세지의 디지탈 지문
- 발신자의 이름

서명 서비스에 의해 되돌려져야 할 요소는 다음과 같다.

- 서명에 사용된 암호화 알고리즘을 포함한 방법의 식별자
- 서명에 사용된 개인키의 식별자
- 서명자의 이름
- 발신자의 이름

• 서명된 날짜와 시간
• 서명자의 서명

이 요소들은 서명된 메세지를 만들기 위해 메세지에 추가될 필요가 있다. 시간 표시 서비스로부터의 대응 서명은 서명을 확인하기 위해 여전히 필요하다. 그러나 서명 서비스와 시간 표시 서비스는 하나의 서비스로 묶여질 수 있고, 그렇게 되면 단순화된다. 대응 서명은 더이상 필요없고 서명/시간 표시 서비스에 의한 단일 서명으로 충분하다.

3.3.5.6 기타

부인봉쇄 서비스는 아직도 연구가 진행중인 분야로서 이 서비스를 실현하기 위해서는 여러가지 암호기술이 뒷받침되어야 한다. 그러나 전산망의 이용이 일상화될 경우 부인봉쇄에 의한 논쟁의 소지가 커지게 될 것이므로 반드시 구현되어야 할 서비스 중의 하나이다.

3.3.6 컴퓨터 보안 감사

3.3.6.1 정의

시스템의 기록과 행동을 사후 독립적으로 조사 관찰함으로써 보안 침해 사실을 발견하고자 하는 보안 활동중의 일종이다.

3.3.6.2 효과

감사 활동을 통하여 보안 침해의 기록을 분석함으로써 침입자를 추적해내거나 공격방법 등을 알아낸다. 침입자에게 사후에 침입사실이 발견될 수 있는 가능성을 예고함으로써 사전에 예방효과를 얻을 수 있다.

3.3.6.3 응용범위

보안 감사는 컴퓨터 보안 전 분야에 걸쳐서 요구되며 다음과 같이 분야를 분류할 수 있다.

1) 물리적 보안 감사
2) 인적 보안 감사
3) 데이타 보안 감사
4) 응용 소프트웨어 보안 감사
5) 시스템 소프트웨어 보안 감사
6) 통신 보안 감사
7) 컴퓨터 운영 보안 감사

3.3.6.4 분야별 보안 감사

가. 물리적 보안 감사

전산망과 관련된 일체의 물리적 시설물이나 컴퓨터 등의 장비 및 장비를 적절히 운영하기 위한 환경 그리고 보안이 유지되어야 할 장소 등에 대한 출입통제 등의 일체의 보안 활동이 적절히 이루어지고 있는지를 감사한다.

감사 대상에는 다음과 같은 사항들이 포함될 수 있다.

• 물리적 보안을 위한 표준서, 지침서 등이 마련되어 있고 적절히 활용되고 있는가
• 물리적 보안을 위한 적절한 장비가 사용되고 있으며, 관리는 제대로 이루어지고 있는가
• 환경의 조절은 정해진 기준치내에서 잘 이루어지고 있는가
• 출입증, 열쇠 등이 분실, 도난, 복제되고 있지 않는가

나. 인적 보안 감사

인적 보안 감사는 전산망에 관련된 모든 사람에 대하여 행해져야 한다. 즉 전산부서 직원뿐만 아니라 다른 조직의 모든 직원 그리고 통신망을 통하여 시스템을 이용하는 모든 사람에 대하여도 행해져야 한다.

감사대상에는 다음과 같은 사항들이 포함될 수 있다.

• 관련된 인원에 대한 보안 정책이 수립되고 운영되는가
• 직원, 부서, 조직 도표와 전화번호 등이 적절히 관리되고 있는가
• 보안 부서의 조직 도표와 직원 전화번호 등이 적절히 관리되고 있는가
• 보안 부서의 서신, 보고서, 메모, 문서 등이 적절히 관리되고 있는가

다. 데이타 보안 감사

컴퓨터 시스템내에 저장된 데이타에 대해 인가

되지 않은 사용이나 무결성 유지 등에 대한 감사가 행해져야 한다.

- 패스워드 관리가 이루어지고 있는가
- 데이타의 중요도, 비밀의 보호정도에 대한 분류 및 관리가 이루어지고 있는가
- 비밀유지가 필요한 데이타에 대한 암호화 등이 이루어지고 있는가
- 백업과 회복 절차가 적절히 수행되고 있는가

라. 응용 소프트웨어 보안 감사

응용 소프트웨어가 인가되지 않은 채로 사용되지는 않는가, 무결성이 유지되고 있는가 등에 대해 감사가 이루어져야 한다. 이는 데이타 보안의 경우와 유사하다.

감사 대상에는 다음과 같은 사항들이 포함될 수 있다.

- 응용 소프트웨어가 의도대로 동작되고 있는가
- 개발, 유지, 운영하는 동안 소프트웨어의 무결성이 유지되는가
- 데이타 보안에 준하는 사항이 잘 지켜지고 있는가

마. 시스템 소프트웨어 보안 감사

데이타베이스 운영시스템, 데이타 사전, 유틸리티 소프트웨어, 운영 체제 등의 시스템 소프트웨어에 대해 무결성이 유지되고 있으며 장애시에 대책수립 등이 적절히 수행되고 있는지 감사가 필요하다.

감사 대상에는 다음과 같은 사항들이 포함될 수 있다.

- 시스템 소프트웨어가 의도적으로 혹은 우연히 변경되지 않는가
- 인가되지 않은 사람들에 의해 시스템 소프트웨어가 엑세스되고 있지는 않는가
- 시스템 프로그래머가 응용 소프트웨어 등을 불법으로 엑세스하지는 않는가
- 데이타 보안에 준하는 사항이 잘 지켜지고 있는가

바. 통신 보안 감사

컴퓨터 통신에 관련된 하드웨어, 소프트웨어, 통신 회선 등 네트워크 시설물 전체가 적절히 보안조치되고 있는지의 여부를 감사한다.

- 네트워크 운영자의 콘솔이나 통신회선 등이 인가되지 않은 제3자에 의해 엑세스되지 않는가
- 터미널 등의 보안이 적절한가
- 통신용 하드웨어와 소프트웨어, 통신회선 등의 장애에 대한 대책은 수립되어 있으며 적절히 운영되고 있는가
- 시스템 소프트웨어에 준하는 사항이 잘 지켜지고 있는가
- 물리적 보안에 준하는 사항이 잘 지켜지고 있는가

사. 컴퓨터 운영 보안 감사

컴퓨터 동작, 작업일정 및 계산서 작성 행위, 운용자, 작업제어 언어, 외부 서비스, 테이프, 디스크 등의 관계, 프로그램 라이브러리 관리 등이 보안체계에 맞게 운영되고 있는가를 검사한다.

- 시스템 데이타 세트와 데이타 기록, 운영기록 등이 적절히 관리 운영되고 있는가
- 데이타와 프로그램의 백업이 적시에 이루어지고 있는가
- 비상사태에 대한 대응책은 수립되어 있는가
- 출력은 비밀정도에 따라 적절히 구분 관리되고 있는가
- 부당하게 사본이 만들어지고 있지 않은가
- 시스템의 고장기록이 적절히 유지되고 있는가
- 물리적 보안에 준하는 사항이 잘 지켜지고 있는가

4. 결 론

본고에서는 전산망 안전을 위협하는 요소들과 그 대비책을 특히 기술적인 대책을 중점으로 해서 살펴보았다. 이러한 관점에서 볼 때에 아직아무런

전산망 안전에 대한 구체적인 방안을 마련하고 있지 않은 우리나라는 기술적인 면에서는 우선 각 요소 기술마다 시행 지침이나 표준을 제정하는 일이 시급하다 하겠으며, 제도적으로 어떠한 전산망 안전을 전담하는 센터를 만들어 키의 분배, 인증, 감사 등의 서비스를 제공하고 보안 관련 제품에 대한 평가와 승인을 할 수 있도록 하는 것이 요망된다. 전산망 보호에 관한 법률이나 시행령 등을 제정, 공포, 시행하고, 매스콤과 전문교육기관 등을 통해 일반인과 전문가들을 교육 훈련시킴으로써 전산망의 안전을 보장하는 것이 정보화 시대를 앞당겨 국민에게 보다 나은 생활을 가져다 줄 수 있다고 본다.

한국전산원은 금년 안으로 물리적 보안, 패스워드 사용, PC 바이러스 감염대비에 관한 세가지의 지침서 초안을 내어 놓을 예정이다. 내년에는 이들 초안을 보충 정리하여 실제 사용 가능한 지침서를 만들며, 또 개인용 컴퓨터의 안전관리, 전산센터의 접근제어 등 몇가지 중요하면서도 시급한 문제들에 대해 지침서 초안을 만들 예정이다. 아울러 암호화 알고리즘과 암호화 프로토콜, 안전 운영체제 등의 핵심기술에 대한 기초 연구를 시작하여 5년 이내에 표준이 되어야 할지를 결정할 것이다. 또한, 국내외 학회와 표준활동에 참여하여 기술동향을 분석함과 동시에 본 연구의 결과에 대한 평가도 받는다. 그 익년도부터는 지침서들의 확정 및 추가 개발과 기초 연구의 계속, 학회 및 표준화 활동에의 지속적인 참여, 표준 초안 및 확정안 개발 등을 함으로써 95년말까지는 일차적으로 시급한 중요 기술 요소에 관한 한 지침과 표준이 완성될 수 있도록 한다. 96년 이후에도 지속적으로 사회의 변화에 적응할 수 있도록 지침과 표준을 수정 보완하는 작업이 계속되어야 할 것이다.

참 고 문 헌

1. 타임-라이프 북스 편집부, 컴퓨터의 세계, 컴퓨터의 보안, 한국일보 타임-라이프 편집부, '90. 3.

2. 김세헌, 정보통신망의 정보보안체계 설계에 대한 종합적 연구, 한국경영과학회 '89전기통신학술연구과제 최종보고서, '90. 1.

3. 김동용, 컴퓨터 망의 보안에 관한 연구, 한국통신학회, '89 전기통신 학술연구과제 최종보고서, '89. 12.

4. International Standard Organization, "Information Processing-OSI Reference Model-Part 2, Security architecture", International Standard ISO 7498-2, Geneva, 1988.

5. CCITT, "OSI-The Directory-Authentication franework", Recommendation X. 509, Melbourne, 1988.

6. R.R. Moeller, Computer Audit, Control and Security, Wiley, 1989.

7. J.M. Carrol, Computer Security, 2nd ed., Butterworths, 1987.

8. J.W. Wack & L. J. Camahan, Computer Viruses and Related Threats, A Management Guide, NIST Special Publication 500-166, Aug. 1989.

9. M.E. Haykin & R. B. Warnar, Smarcard Technology, New Methods for Computer Access Control, NIST Special Publication 500-157, Sept. 1983.

10. IEEE, Standard for Interoperable LAN Security, P802-10, May, 1990.

11. X/Open, X/Open Security Guide, Prentice Hall, 1989.

12. K.E. Kirkpatrick, "Standards for Network Security", Proc. of IIth NCSC, Oct. 1988.

13. Y. LeRoux, "Technical Criteria for Security Evaluation of Information Technology Product", IFIPS TC-11 Conference, May, 1990.

14. NIST, SDNS Network, Transport, and Message Security Protocols, NIST IR 90-4250, Feb. 1990.

15. 박태규, 이형수, 신종태, "컴퓨터/네트워크 시스템 보안 표준화 동향 분석", 제2회 정보보호와

암호에 관한 워크샵 논문집, pp. 95-113, 유성, 1990. 9.

16. 한국전자통신연구소, 정보보호체계 구성 방식연구, 1990. 3.

17. Department of Defence, Trusted Computer System Evaluation Criterial, US Government Printing Office, CSC-STD-001-83, Aug. 1983.

18. NBS, Guidelines for Automatic Data Processing Physical Security and Risk Management, FIPS Pub 31, June 1974.

19. D.E. Denning, Cryptography and Data Security, Addison-Wesley, 1982.

20. D.D. Steinauer, Security fo Personal Computer Systems, A Management Guide, BNS Special Pub 500-120, Jan 1985.

21. NCSC, Personal Computer Security Considerations, NCSC-WA-002-85, 1985.

22. European Computer Manufacturers Association, Security in Open Systems, A Security Framework, ECMA TR/46, July, 1988.

23. American National Standard for Personal Identification Number(PIN) Management and Security, ANSI X. 9.8., Jan. 1982.

24. ISO, User Requirements on Security, ISO ITSI/SC18N2003, E.J. Humphreys, CEN/CENELEC Toward a Taxanomy for Standardization of Security, British Telecom, England, Apr. 1990.

25. 전산원, 전산원 보안관리 연구(개요), NCA-RE-9025, Dec. 1990.

26. 전산원, 패스워드 사용지침(안), NCA-RE-9028, Dec. 1990.

27. 전산원, 컴퓨터 보안관리지침 연구 : 물리적 보안 분야, NCA-RE-9022, Dec. 1990.

□ 著者紹介

李 弼 中(正會員)

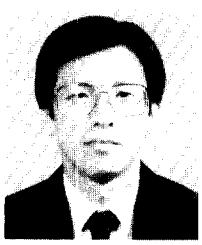
1951年 12月 30日生
1974年 2月 서울大學校 電子工學科 學士
1977年 2月 서울大學校 電子工學科 碩士
1982年 6月 U.C.L.A. System Science, Engineer
1985年 6月 U.C.L.A. Electrical Engineering, Ph.D.
1980年 6月～1985年 8月 : Jet Propulsion Laboratory, Senior Engineer
1985年 8月～1990年 2月 : Bell Communications Research, M.T.S.
1990年 2月～現在 : 浦項工科大學 電子電氣工學科, 副教授

정 진 욱(正會員)

成均館大學校 電氣工學科 卒業(學士)
成均館大學校 大學院 電子工學科(碩士)
서울大學校 大學院 計算統計學科(博士)
韓國科學技術研究所 研究員/韓國科學技術院 시스템공학센터 데이타통신研究室長
Racal Milgo Co. 研究員(미국 Florida 所在)
現在 成均館大學校 情報工學科 副教授

박 명 순(정회원)

1965年 서울大學校 電子工學科 卒業
1982年 Utah大學校 電氣工學科에서 碩士學位 取得
1985年 Iowa大學校 電氣 및 컴퓨터工學科에서 博士學位 取得
1985年～1987年 Marquette大學校 電氣 및 電算學科에서 助教授로 勤務
1987年～1988年 浦項工大 電子電氣 및 電子計算學科에서 助教授로 勤務
1988年～現在 高麗大學校 電算科學科에서 助教授, 副教授로 在職中
관심분야 : 컴퓨터 구조, 운영체제 등



이 재 용(정회원)

1977年 2月 廷世大 電子科 卒業(學士)
1984年 5月 Iowa State University, 電算機工學科(碩士)
1987年 5月 Iowa State University, 電算機工學科
1987～1982年 國防科學研究所 研究員
1983～1986年 Iowa State University, 研究助教
1987年 1月～1987年 6月 Iowa State University, 助教授
1987年 7月～現在 浦項工科大學 電子計算學科 助教授