# 인트라넷에서의 내부 보안 모델

신°원 , 이경현
부경대학교 전자계산학과

# Security Model in Intranet Environment

Weon° Shin , Kyung-Hyune Rhee
Department of Computer Science, Pukyong National University

요 약

기술 개방형 구조의 인터넷 표준 기술들을 바탕으로 기업 내부의 업무와 정보를 효율적으로 처리하고자 하는 새로운 네트워크 개념으로 등장한 인트라넷은 기존 기업 환경을 변화시킬 새로운 인프라로 인식되고 있다. 이러한 인트라넷은 개방된 인터넷 기술과 기업 내 정보 시스템의 결합이라는 그 특성상 기업내 정보를 보호하기 위한 정보보호 기술이 필수적으로 요구된다. 현재까지 인트라넷 외부로부터 정보를 보호하기 위해 접근제어, 데이터 암호화 등을 중심으로 연구되었지만, 인트라넷 내부에서 정보를 보호하고자 하는 연구는 전무한 실정이다. 본 논문에서는 현재 구현되고 있는 인트라넷 서비스에 대해 기업 내부에 초점을 맞추어 각종 보안위협들을 살펴본 후 그에 대응하는 보안 모델을 제안하고 각종 프로토콜 및 알고리즘을 컴퓨터 시뮬레이션을 통해 수행한다.

## 1. 서론

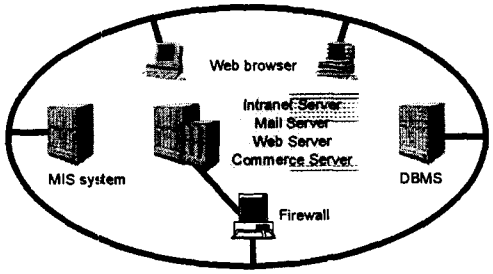
표준 기술과 개방성에 기반하는 인터넷의 장점들을 기업내부 업무 및 정보를 처리하기 위해 적용된 기술이 바로 인트라넷(Intranet)이다. 즉, 인트라넷은 인터넷 관련 표준 기술들을 바탕으로 기업 내부망 및 인터넷으로 네트워크 환경을 구축하여 기업 내부의 업무와 정보 처리를 보다 효율적으로 하고자하는 새로운 네트워크 개념이다. 이러한 인트라넷은 기술 개방형 구조로써 기존의 기업 환경을 변화시킬 새로운 인프라로 인식되고 있다[1]. 특히, 인트라넷은 개방된 인터넷 기술과 기업 내 정보 시스템의 결합이라는 그 특성상 기업 내 정보를 보호하기 위해 정보보호 기술이 필수적으로 요구된다. 이에 기업 내 정보를 보호하기 위해 침입차단 시스템(Firewall) 등이 구축되어 기업 외부망으로부터 인트라넷을 보호하고 있지만, 침입 사례 중 많은 비중을 차지하는 내부의 보안 위협에 대해서는 속수무책인 것이 현실이다[2].

본 논문에서는 인트라넷 내부에 초점을 맞추어 현재 구현되고 있는 서비스별 인트라넷 기술에 대한 기업 내부에서의 보안위협들을 살펴보고, 암호기술 및 암호프로토콜을 이용한 인트라넷 환경 내에서의 보안 모델을 제안하고자 한다. 먼저 2장에서는 인트라넷이 어떻게 구성되고 있는지 살펴보고, 3장에서는 현재 인트라넷이 구현되어 제공하는 각종 서비스를 조사한 후 내부 보안위협에 대해서 분석한다. 그리고, 4장에서는 실제 적용 가능한 암호 기술 및 프로토콜을 알아보고, 5장에서는 각종 서비스에 정보보호 기술을 적용한 보안 모델을 제시한다. 6장에서는 5장에서 제안한 모델을 바탕으로 실제 환경에서 사용될 각종 프로토콜 및 알고리즘을 컴퓨터 시뮬레이션을 통해 수행하고 결론을 유도한다.

## 2. 인트라넷의 구성

인트라넷은 기본적으로 TCP/IP(Transmission Control Protocol / Internet Protocol)를 지원하는

LAN(Local Area Network) 환경으로 기업 내에 구축되어 웹브라우저 상에서 업무를 수행하도록 해준다. 즉, 전자메일, 전자결재 등 각각의 다른 시스템에서 주고받던 다양한 형태의 정보들을 월드와이드웹 기반의 하이퍼링크 방식 인터페이스 위에서 통합함으로써 업무의 효율성뿐만 아니라 시스템 구축 용이, 운영 비용의 절감 등을 꾀할 수 있다. 이러한 인트라넷은 적용되는 기술에 따라 인터넷 요소, 데이터베이스 요소, 보안 요소, BPR(Business Process Reengineering) 요소의 4가지로 이루어진다. 필수 요소들을 구체적으로 살펴보면 다음과 같으며, <그림 1>은 이들의 관계를 그림으로 나타내었다.




<그림 1> 인트라넷의 필수 요소

(1) 인터넷 요소 : 인터넷 기술을 적용한 인터넷 및 월드와이드웹의 각종 서비스 등을 구현하는 기술로써 web browser, web server, mail, news, ftp, proxy, search agent, 저작도구 등을 말한다. 이를 다시 서버 관련 기술과 클라이언트 관련 기술로 나눌 수 있다.

① 서버 관련 기술
CGI(Common Gateway Interface)
SSI(Server Side Interface)
Server Power Setup(Security, logging)
Multimedia Inline skill, Design skill

② 클라이언트 관련 기술
HTML(Hyper Text Markup Language)
Client Interface

(2) 데이터베이스 요소 : 기존의 데이터베이스와 인터넷 기술을 서로 연결하기 위한 요소로써 인트라넷 내의 정보를 저장, 검색하기 위한 데이터베이스 구축, 인트라넷 서버와의 통신을 위한 DBMS Interface Module 등이 여기에 포함된다.

(3) 보안 요소 : 인트라넷을 외부망으로부터 보호하기 위한 기술로 적극적인 방어 개념인 침입차단 시스템(Firewall), 소극적인 방어 개념의 데이터 암호화가 포함되고, 나아가 보다 안전한 거래를 처리하기 위한 암호 프로토콜도 여기에 속한다.

① 침입차단 시스템(Firewall System)

② 정보 암호화 및 전송 기술
S-HTTP(Secure Hyper Text Transfer Protocol)
SSL(Secure Socket Layer)

③ 전자지불시스템

(4) BPR(Business Process Reengineering) 요소 : 업무분석 기법을 기반으로 인트라넷 내에서 실제 업무와 적용하는 Web-Base Group System으로 다음과 같은 것들이 포함된다.

① Java/ActiveX Programming

② Business Process Analysis

③ EDI(Electronic Data Interchange)

## 3. 인트라넷 제공 서비스 및 내부 보안 위협

인트라넷의 가장 큰 장점은 기존의 인터넷 환경을 이용해서 하드웨어나 운영체제의 제한을 받지 않고 기업 내 구성원을 서로 유기적으로 연결할 수 있다는 것이다. 이러한 장점을 이용한 전자우편, 전자게시판, 전자결재, 정보검색, 문서관리, 그룹 및 개인 정보관리 시스템 등과 같은 다양한 서비스들이 제공되고 있다. 각 서비스에는 수많은 보안 취약점이 존재하며 외부뿐 아니라 내부에서도 공격 대상이 되기도 한다. 현재 인트라넷에서 가장 많이 사용하고 있는 서비스에 대해 각 서비스별 구조 및 특징과 보안 위협에 대해 알아보면 다음과 같다.

### 가. 전자우편

전자우편은 각종 정보를 특정인과 주고받는 인터넷에서 가장 많이 사용되는 의사소통의 도구로써 여러 RFC와 X.400 시리즈의 권고안으로 지정되어 있다[7,8,9]. 초기에는 주로 텍스트만을 지원하였지만 MIME(Multipurpose Internet Mail Extension)[11,12]의 등장으로 이미지, 사운드, 동영상 등의 멀티미디어 자료들을 전송할 수 있게 되었다. 현재 인터넷 환경 하에서는 전자우편 보안을 위해 PGP(Pretty Good Privacy)[13], PEM(Privacy Enhanced Mail)[14,15,16,17], S/MIME[18] 등을 사용하고 있지만 사용자 인증 및 키관리의 문제점(PGP), 엄격한 키관리 방식 채택으로 사용자 확보 실패(PEM), 안전하지 못한 알고리즘의 사용(S/MIME) 등의 문제점들이 발생하고 있다. 특히, 여러 전자우편 보안 도구가 사용됨에 따라 각 보안 소프트웨어 간의 호환성이 결여되어 사용자 간에 혼란도 야기되고 있다..

### 나. 전자게시판

전자게시판은 공통된 업무, 각종 제안, 주된 관심사 등을 토론하고 상호간의 수많은 정보를 공유하는 공간이 되고 있다. 기업 내에서 공유해야할 정보를 데이터베이스와 연동하여 전자화된 게시판에 공개함으로써 조직 구성원간의 시간, 공간의 제약을 극복하면서 폭넓은 정보를 제공하도록 해준다. 실제 시스템으로 구현할 때 모든 게시물에 대한 무결성 보장, 사용자 인증 및 부인방지 문제가 발생한다.

### 다. 전자결재

전자결재는 업무흐름의 자동화, 문서의 체계적 관리 및 분류의 목적으로 전자서명을 통해 문서 결재가 이루어진다. 특히, 국가경쟁력 강화를 위한 일환으로 전자상거래를 관계 부처 및 민간 부문에서 추진하고 있는데, 그 안전성과 신뢰성을 보장하기 위해서 전자문서, 전자서명, 전자인증 등을 법률로써 규정하고 있다[3,4,5,6]. 전자결재 시스템은 데이터베이스를 이용하여 현재 활용중인 기안 형태를 양식화하여 각종 업무와 연동하고 있는데, 현재 통용중인 전자결재 시스템은 이미지 스캐너를 이용한 결재로 정보보호 기술이 전혀 도입되지 않아 기안자와 결재자 사이에서 일어날 수 있는 분쟁에 대한 진위 판별 기능이 없다. 이러한 전자결재가 안전하게 이루어지기 위해서는 전자서명, 전자인증을 바탕으로 사용자 인증, 서류의 무결성, 부인방지 등이 보장되어야 한다.

### 라. 정보 및 문서관리

최근 기업 내에서 업무 수행 결과 생기는 각종 전자문서, 수많은 정보 등을 저장하여 인가된 사용자만 접근할 수 있도록 하는 정보 및 문서관리 시스템이 등장하고 있다. 특히, 중요한 문서 및 정보에 접근할 수 있는 권한은 기업 내의 직책에 따라 결정되고 있는데, 각 사용자마다 보안등급을 두어 그에 해당하는 사용자만이 접근할 수 있도록 하는 것이다. 이 경우, 사용자 인증이 기본적으로 요구되고, 계층적 구조에 따른 다중레벨 정보 관리 방법이 요구된다.

## 4. 적용 가능한 암호기술 및 프로토콜

네트워크 컴퓨팅 기술의 발달로 각 사용자들은 인터넷을 이용한 상거래, 업무 수행 등이 자신의 컴퓨터에서 보다 편리하고 빠르게 처리하는 것이 가능해졌다. 하지만, 실제 생활에서의 여러 가지 업무가 전

자화되어 네트워크 상에서 구현됨에 따라 사용자 식별(Identification) 및 인증(Authentication), 전자서명(Digital Signature), 계약의 동시성 등과 같은 보안 문제들이 생겨났다. 이러한 문제점들을 해결하기 위하여 많은 암호기술이 구현되어 현재 사용되고 있다. 본 장에서는 3장에서 살펴본 실제 인트라넷 환경 내에서의 서비스에 적용 가능한 암호 기술 및 프로토콜을 살펴본다.

가. Oblivious Transfer Protocol[19]

전자계약 암호 프로토콜을 구성하기 의해 소개된 "oblivious transfer protocol"은 상대방을 신뢰하지 못하는 상태에서 서로에 대해 속이지 못하도록 하는 프로토콜로써 비밀 정보의 교환, 계약 서명, 전자우편에서 암호학적 기본 도구로써 널리 사용되고 있다.

나. Digital Signature

전자서명(digital signature)은 정보가 변경되지 않고 본래 정보 그대로임을 보장하는 메시지 인증과 사용자 $A$가 바로 그 사용자 $A$임을 증명하는 사용자 인증의 두 가지를 모두 포함한다. 즉, 어떤 메시지 $M$에 대해 무결성을 보장 할뿐만 아니라 서명자만이 그 메시지에 대한 서명을 생성해 낼 수 있고, 생성된 서명에 대해서는 누구나 그 서명자의 서명임을 확인할 수 있으며 서명자는 서명 사실에 대해 부인할 수 없다. 실제 구현되어서 전자문서, 전자계약, 전자인증 등의 다양한 분야에서 사용되고 있다.

다. Special Signature

보통의 서명과는 달리 특수한 상황, 조건 아래에서의 이루어진 서명으로써 다음과 같은 것들이 있다.

(1) Proxy Signature[20]

서명자가 직접 서명을 할 수 없는 상황에서 자신의 대리인을 두어, 자신의 비밀키에 대한 정보를 알리지 않고도 대리인을 통해 서명을 할 수 있는 기법으로써 대리결재 등에 응용할 수 있다.

(2) Multisignature[21]

어떤 메시지 $M$에 대해 여러 사람이 동시에 또는 순차적으로 서명할 수 있는 방식으로 RSA 공개키 암호시스템을 이용하여 구현한 방법들이 소개되고 있다. multisignature는 업무의 흐름에 따라 기안자가 결재자를 지정하여 서명하도록 하여 전자결재 시스템에 적용할 수 있다.

(3) Group Signature[22]

서명자의 신분을 알리지 않고도 어떤 그룹에 속하는 구성원이라는 사실을 증명할 수 있는 서명기법으로 그 특성에 비추어 정확한 여론 조사를 위해 비공개를 바탕으로 하는 무기명 게시판 등에 이용 가능하다.

라. Data Encryption/Decryption

데이터를 보호하기 위해 송신자는 암호화키를 사용하여 메시지 $M$을 암호화한 다음 통신로를 통해 전송하고, 수신자는 이를 받아서 복호화키를 사용하여 복호화하여 원래의 메시지 $M$을 얻어낸다. 암호화키와 복호화키가 같으면 관용키(대칭) 암호시스템이라 하고 데이터 암호화에 DES, IDEA, RC5 등이 주로 쓰이고 있고, 서로 다르면 공개키(비대칭) 암호시스템이라 하고 키분배, 전자서명 등에 RSA, ElGamal, Elliptic Curve 암호시스템 등이 쓰인다.

마. Hash Algorithm

메시지의 무결성을 보장하는 알고리즘으로 일방향 함수를 이용하여 메시지 $M$을 정해진 크기의 메시지 $M'$(보통 128비트 또는 160비트)으로 압축 변환한다. 구현 예로 MDx 계열, SHA-1 등이 있다.

바. Contract Signing Protocol[19]

$A$가 어떤 계약 문서 $M$에 대해 $B$의 서명을 받고자 하는 경우, $A$는 $B$가 먼저 서명하기를 원하고, $B$는 $A$가 먼저 서명하기를 원하게 됨으로써 양자가 만족할만한 동시성을 이루지 않고서는 계약이 이

루어지지 않는다. 이러한 문제를 해결하기 위하여 1985년 Even 등[19]이 oblivious transfer를 이용하여 제안한 프로토콜로써, 동시성을 요구하는 각종 전자계약 등에서 사용되는 매우 중요한 암호 프로토콜이다.

사. Certified Mail[19]

송신자가 어떤 메시지 $M$을 암호화하여 전송한 후, 메시지 $M$에 대한 키와 수신자가 서명한 영수증을 contract signing protocol을 통하여 서로 동시에 교환하는 형태의 프로토콜이다. 프로토콜이 성공적으로 수행된 후 송신자는 영수증을 받음으로써 수신자가 확실하게 전자문서를 받았다는 사실을 알 수 있으며, 수신자는 송신자로부터 전자문서에 대한 키를 받음으로써 그 내용을 확인할 수 있다.

아. Multilevel Key Management[23,24]

각 사용자 집합간에 계층적인 구조가 주어지는 경우, 키관리 대상 사용자들을 보안등급(security class)에 따라 사용자 집합으로 분리하고 서로 배반인 사용자 집합들( $U_1, U_2, \cdots, U_n$)로 나누어 각 사용자 집합에게 보안등급을 부여한다[23,24]. 즉, 만약 $U_i \leq U_j$이면, 집합 $U_i$의 사용자들은 보안 등급에서 집합 $U_j$의 사용자들보다 낮거나 같다. 이것은 실례로써 집합 $U_j$의 사용자들은 집합 $U_i$의 사용자들의 정보에 대한 접근 및 컴퓨터 등의 사용 권한이 부여되지만, 그 반대 ( $U_i$가 $U_j$에 대한 관계)의 경우는 성립하지 않는다.

## 5. 서비스별 인트라넷 보안 모델

OSI(Open Systems Interconnection) 보안 구조 7498-2[26]에 규정된 5가지 보안 서비스는 모든 보안 모델에서는 가장 기본적으로 제공되어야 한다.

- 인증(Authentication) 서비스
  어떤 개체(개인이나 시스템)의 신분을 보증하는 서비스로써 메시지 인증과 개체의 일방향 또는 쌍방향 인증을 포함한다.
- 접근 제어(Access control) 서비스
  시스템 자원의 허가 없는 사용이나 조작을 방지하는 서비스이다.
- 기밀(Confidentiality) 서비스
  허가되지 않은 개체에게 정보가 누설되는 것을 방지하는 서비스로 암호 알고리즘에 기반한다.
- 무결성(Integrity) 서비스
  허가 없이 데이터를 변경, 삭제, 대치하는 것을 방지하는 서비스이다.
- 부인 방지(Non-Repudiation) 서비스
  통신 당사자가 메시지 교환이 일어났다는 사실을 부인하는 것을 방지하기 위한 서비스이다. 항상 인증, 무결성 서비스를 포함하고 기밀 서비스를 포함할 수도 있다.

이들 보안 서비스들은 인트라넷에서도 기본적으로 제공되어야 할 서비스들이다. 인트라넷 보안의 관점에서 본다면 외부로부터 인트라넷을 보호하기 위해 중요한 서비스로는 인증 서비스, 접근 제어, 기밀 서비스가 여기에 해당되고, 인트라넷 내부에서 업무 흐름에 따른 보안 서비스에는 인증 서비스, 무결성 서비스, 부인 방지 서비스가 해당된다. 본 장에서는 3장에서 언급했던 인트라넷 제공 서비스를 내부 보안 위협에 초점을 맞추어, 4장에서 설명했던 암호 기술과 프로토콜을 이용하여 보안 모델을 제안한다.

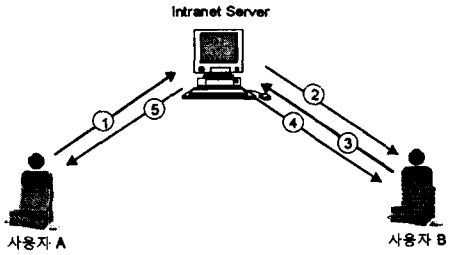
제안 모델에서 모든 사용자는 자신의 컴퓨터가 1대씩 할당되어 있다고 가정하고, 각 사용자는 스마트 카드 등과 같은 인증 절차 후 컴퓨터를 사용할 수 있으며 각종 암호 기술 및 프로토콜은 사용자의 선택에 따라 컴퓨터 내에서 자동적으로 수행된다. 그리고, 제안 모델의 모든 프로토콜에서 사용되는 용어들은 다음과 같이 정의된다.

$K$ : 관용키 암호 시스템에서 관용키
$SK_A$ : 공개키 암호 시스템에서 사용자 $A$의 비밀키
$PK_A$ : 공개키 암호 시스템에서 사용자 $A$의 공개키
$H(M)$ : 메시지 $M$에 대한 해쉬값
$E_K(M)$ : 관용키 암호 시스템에서 $K$를 이용하여 암호화
$D_K(M)$ : 관용키 암호 시스템에서 $K$를 이용하여 복호화
$SK_A(M)$ : 공개키 암호 시스템에서 메시지 $M$에 대한 사용자 $A$의 전자서명
$PK_A(M)$ : 공개키 암호 시스템에서 사용자 $A$의 공개키로 메시지 $M$을 암호화

가. 전자우편

전자우편은 인터넷 초창기부터 제공되어져 온 서비스이므로 그에 대한 다양한 연구가 이루어져 정보를 안전하게 전송하고자 하는 노력들이 많이 있어왔고, 또한 보안 도구들도 많이 개발된 상태이다. 그러나 3장에서 언급한 것과 같은 많은 문제점이 발생하고 있으므로, 최근에는 이를 해결하기 위한 인증서[10]를 기반으로 하는 전자메일, 배달 증명 및 내용 증명이 가능한 전자메일[25]도 제안되었다. 본 장에서는 인트라넷 환경에 적용하여 내부 보안 위협에 대비한 전자우편 보안 모델을 제안한다.

① $A \rightarrow Server$ : $B$, $SK_A(M)$, $SK_A(H(M))$
② $Server \rightarrow B$ : $SK_{Server}(E_K(M))$, $SK_{Server}(R)$
③ $B \rightarrow Server$ : $SK_B(R)$
④ $Server \rightarrow B$ : $SK_{Server}(K)$, $R$
⑤ $Server \rightarrow A$ : $SK_{Server}(SK_B(R))$




<그림 2> 전자우편 보안모델

프로토콜 설명 :

① 먼저 사용자 $A$는 메시지 $M$과 그 해쉬 결과에 자신이 서명한 후 $SK_A(M)$, $SK_A(H(M))$을 $B$가 수신자라는 사실과 함께 서버에 보낸다.

② 서버는 이를 받아 $A$의 공개키를 이용하여 서명이 맞는지 확인하여 복호화하여 메시지 $M$의 해쉬값이 $H(M)$과 같은지 검사하고, 임의의 세션키 $K$를 생성하고 대칭키 암호시스템을 이용하여 암호화한 $SK_{Server}(E_K(M))$와 $M$의 레이블에 해당하는 임의의 난수 $R$을 서명하여 $SK_{Server}(R)$을 사용자 $B$에게 전송한다.

③ 사용자 $B$는 응답으로 $R$에 자신의 서명을 하여 $SK_B(R)$을 서버로 전송한다.

④ 서버는 다시 암호화 때 사용했던 세션키를 서명하여 $SK_{Server}(K)$와 $R$을 사용자 $B$에게 보낸다. 사용자 $B$는 $K$를 사용하여 복호화하여 메시지 $M$을 확인할 수 있다.

⑤ 서버는 결과로써 $SK_{Server}(SK_B(R))$을 사용자 $A$에게 전송한다. 사용자 $A$는 $SK_{Server}(SK_B(R))$를, 서버는 $SK_A(M)$, $H(M)$, $SK_B(R)$를, 사용자 $B$는 $SK_{Server}(R)$를 각각 보관한다.

나. 전자게시판

월드와이드웹의 폭발적인 인기에 힘입어 구축되기 시작한 전자게시판은 비교적 최근에 나온 서비스이다. 안전한 월드와이드웹 서비스를 구현하기 위해 SSL, S-HTTP 등이 구현되고 있지만, 역시 내부 보안 위협에는 아직 속수무책이다. 현재 인트라넷 환경에 적용하여 발생할 수 있는 내부 위협에 초점을 맞추어 안전한 전자게시판 보안 모델을 제안한다.

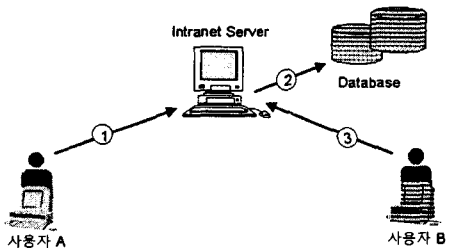
(1) 일반 게시판

일반 게시판은 메시지와 함께 서명, 해쉬값을 보관하는 방법을 사용하여 다른 모델에 비해 비교적 쉽게 구현할 수 있다.

① $A \rightarrow Server$ : $SK_A(M)$, $SK_A(H(M))$

② $Server$ : $M$, $H(M)$, $SK_A(M)$ 을 데이터베이스에 저장, 게시

③ $B \leftarrow Server$ : $M = PK_A(SK_A(M))$ 확인




<그림 3> 일반 게시판 보안모델

프로토콜 설명 :

① 사용자 $A$는 메시지 $M$과 그 해쉬 결과에 자신이 서명한 $SK_A(M)$, $SK_A(H(M))$ 을 서버로 전송한다.

② 서버는 서명을 확인하고 메시지의 해쉬값을 확인한 후 $M$, $H(M)$, $SK_A(M)$ 을 데이터베이스에 저장하고, 전자게시판에 게시한다.

③ 검증자 $B$는 $M$에 대한 서명을 통해 $M = PK_A(SK_A(M))$ 임을 확인하여 사용자 $A$의 게시물이라는 것을 확인할 수 있고, $M$에 해쉬함수를 적용함으로써 메시지의 무결성을 직접 확인할 수 있다.

부가적으로 메시지 재생 공격을 대비하기 위해서는 timestamp를 적용하면 된다.

(2) 무기명 게시판

기업 내 여론 조사 등의 의견수렴을 위한 비공개를 바탕으로 하는 무기명 게시판이 인트라넷의 새로운 서비스로 등장하고 있다. 이 서비스는 그룹 내 구성원의 익명성을 보장하여 솔직한 의견들을 반영하기 위한 방법으로 도입되고 있는데, 현재 구축되어 구현된 것은 사용자 인증, 부인 방지 등이 전혀 고려되어 있지 않다. 공개키 암호시스템을 사용하여 무기명 게시판을 다음과 같이 구성할 수 있다.

1. 준비

① $Server$ : 임의의 $m$개의 공개키 쌍 $(PK_{i1}, SK_{i1})$, … , $(PK_{im}, SK_{im})$ $(1 \le i \le n)$ 를 생성

② $Server \rightarrow$ 사용자 $i$ $(1 \le i \le n)$ : $SK_{i1}$, … , $SK_{im}$

③ $Server$ : $n \times m$개의 모든 사용자 공개키를 임의의 순서로 공개

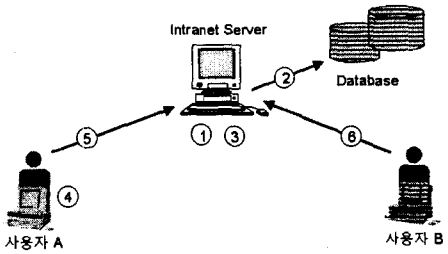
2. 서명 후 게시

④ $A$ : 비밀키 $SK_A = SK_{Aj}$, 공개키 $PK_A = PK_{Aj}$ $(1 \le j \le m)$

⑤ $A \rightarrow Server$ : $M$, $SK_A(M)$

3. 서명확인

⑥ $B \leftarrow Server$ : $M = PK_A(SK_A(M))$ 확인




<그림 4> 무기명 게시판 보안모델

프로토콜 설명 :

① 서버는 $n$명의 사용자에 대해 임의의 공개키 쌍 $(PK_{i1}, SK_{i1}), \cdots, (PK_{im}, SK_{im})$ $(1 \le i \le n)$을 생성한다.

② 서버는 사용자 $i$에 대한 $m$개의 비밀키 $SK_{i1}, \cdots, SK_{im}$를 사용자에게 전송하고, 이름을 저장해둔다. 이것을 $n$명의 사용자에 대해 반복수행하는데, 서버가 비밀키에 서명을 한 후 전송할 수도 있다. 모든 사용자들은 $m$개의 비밀키와 공개키 쌍을 가지게 된다. 그러므로 모든 비밀키와 공개키 쌍의 개수는 $n \times m$개가 된다.

③ 서버는 $n \times m$개의 모든 사용자 공개키를 임의의 순서로 리스트를 작성한 후 모두에게 공개한다.

④⑤ 사용자 $A$가 게시물을 작성한다면, $m$개의 비밀키 $SK_{i1}, \cdots, SK_{im}$ 중에서 임의로 $SK_A = SK_{Aj}$ $(1 \le j \le m)$를 선택한다. 그에 대한 공개키는 당연히 $PK_A = PK_{Aj}$ $(1 \le j \le m)$이 된다. 이를 이용하여 메시지 $M$과 그에 대한 전자서명 $SK_A(M)$을 생성하여 서버에 전송한다.

⑥ 어떤 사용자 $B$가 게시물에 대한 서명을 확인할 때는 해당하는 공개키를 적용하여 $M = PK_A(SK_A(M))$인지 확인하면 된다.

모든 키의 소유자는 서버만이 알고 있고, 검증자는 구성원의 신원을 모르는체 그룹의 소속원이라는 사실을 확인할 수 있다. 분쟁발생시 서버의 정보를 이용하여 서명자의 신원을 확인할 수 있다. 만약, 메시지 $M$에 대한 무결성을 보장하려면 공개된 해쉬 알고리즘을 적용한 해쉬값 $H(M)$을 전자서명하여 함께 게시하도록 하면 된다.

다. 전자결재

업무의 효율성을 위해 구축되고 있는 전자결재 시스템은 보안 위협에 대해 전혀 고려되어 있지 않다. 서류의 무결성 뿐 아니라 서명에 있어서도 결재자의 서명을 이미지 스캔하여 처리하고 있는 실정이다. 최근 "전산망보급확장 및 이용촉진에 관한 법률[3]"에서 전자문서, 전자서명, 전자인증 등을 규정하여 결재문서에 대해 법적인 효력도 부여하고 있으므로, 조만간 정보보호 기술을 이용한 전자결재 시스템이 등장할 것으로 사료된다. 여기서는 인트라넷 환경에 적용하여 업무흐름에 따라 발생할 수 있는 내부 위협에 초점을 맞추어 안전한 전자결재 보안 모델을 제안한다.

① $A \rightarrow Server$ : $SK_A(E_K(M))$, $SK_A(K)$

② $Server$ : $M$, $H(M)$, $R$

③ $Server \rightarrow B$ : $SK_{Server}(E_K(M))$

④ $Server \rightarrow A$ : $SK_{Server}(R)$

⑤ $A \rightarrow B$ : $E_{K_1}(S), \cdots, E_{K_{2n}}(S)$

(random $K_1, \cdots, K_n$, $K_{n+1} = K \oplus K_1, \cdots, K_{2n} = K \oplus K_n$)

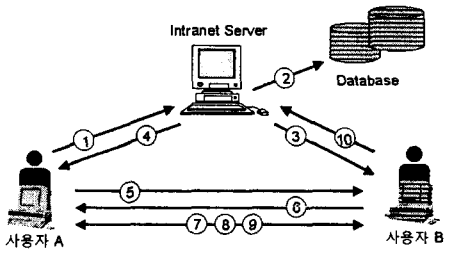
⑥ $B \rightarrow A$ : $E_{H_1}(T_r), \cdots, E_{H_n}(T_r)$, $E_{H_{n+1}}(T_l), \cdots, E_{H_{2n}}(T_l)$

⑦ $A \leftrightarrow B$ : $K_1, \cdots, K_{2n}$, $H_1, \cdots, H_{2n}$ 중 $n$개를 oblivious transfer를 이용하여 교환

⑧ $A \leftrightarrow B$ : $K_1,\cdots,K_{2n}$, $H_1,\cdots,H_{2n}$를 한 비트씩 $2n$번 반복하여 서로 교환

⑨ $A \leftrightarrow B$ : oblivious transfer protocol에서 사용한 비밀키 교환

⑩ $B \rightarrow Server$ : $SK_B(M)$




<그림 5> 전자결재 보안모델

프로토콜 설명 :

① 사용자 $A$는 서류 $M$을 관용키 암호시스템을 이용하여 암호화하여 서명한 $SK_A(E_K(M))$과 키 $SK_A(K)$를 서버에게 보내고 보관한다.

②③④ 서버는 사용자 $A$의 서명을 확인하고, 서류 $M$, 해쉬값 $H(M)$, 그에 해당하는 레이블 난수 $R$을 데이터베이스에 저장한 후, 사용자 $B$에게 자신이 서명한 $SK_{Server}(E_K(M))$을 전송하고, 사용자 $A$에게는 $SK_{Server}(R)$을 보내어 그 사실을 알려준다.

⑤ 사용자 $A$는 $n$쌍의 관용키를 생성하는데, 여기서 $K_1,\cdots,K_n$는 임의로 생성하고, 나머지는 $K_{n+1}=K \oplus K_1$, $\cdots$ , $K_{2n}=K \oplus K_n$와 같은 형태로 둔다. 다음으로 임의의 한 메시지 $S$를 $2n$개의 키를 각각 사용하여 암호화하여 사용자 $B$에게 전송한다.

⑥ 사용자 $B$는 $n$쌍의 관용키 $H_1,\cdots,H_{2n}$를 임의로 생성한 다음, 메시지 "$i$번째 영수증 왼쪽($T_r$)"은 $H_i(1\le i\le n)$를, 메시지 "$i$번째 영수증 오른쪽($T_l$)"은 $H_{n+i}(1\le i\le n)$을 각각 사용하여 암호화한 다음 사용자 $A$에게 전송한다.

⑦ 이제 사용자 $A$와 $B$는 $n$쌍의 키 $K_1,\cdots,K_{2n}$ , $H_1,\cdots,H_{2n}$에서 각 쌍에 대해 하나씩을 oblivious transfer protocol을 사용하여 서로 주고받는다. 그러면 사용자 $A$와 $B$는 각 키 쌍에 대해 하나씩의 키를 가지게 되고 메시지의 반을 복호화할 수 있게 되어 암호화된 메시지가 정당하다는 것을 확인할 수 있다.

⑧ 다시 사용자 $A$와 $B$는 모든 키를 한 비트씩 $2n$번 반복하여 서로 주고받으면 모든 키가 전송이 되고, 나머지 반을 복호화할 수 있게 된다. 여기서, 사용자 $A$는 $B$로부터 영수증을 받은 것이 되고, 사용자 $B$는 모든 키에 대해 "⊕"를 적용하여 $K=K \oplus K_i \oplus K_i$을 확인한 후 $E_K(M)$를 복호화하여 $M$을 얻을 수 있게 된다.

⑨ oblivious transfer protocol에서 사용한 비밀키를 교환하여 서로 속이지 않았는지 확인한다.

⑩ 사용자 $B$는 $M$의 내용을 본 후 전자서명한 $SK_B(M)$을 서버로 보낸다.

라. 다중레벨 정보관리

업무 수행 후 발생하는 각종 전자문서, 데이터베이스에 저장된 수많은 정보에 대한 효율적인 관리방법이 대두되고 있다. 기업의 특성상 직책에 따른 정보 접근에 대한 보안 등급을 두어 각 사용자는 자신의 등급에 맞는 문서 및 정보를 다룰 수 있도록 한다. 특히, 김주석 등[28]은 의사랜덤치환을 이용한 다중레벨 키 분배방안을 제시하였는데, 여기서 그 내용을 소개하고 계층적 구조를 따르는 기업 내에서 정보 및 문서관리에 대해 인트라넷 환경에 적용하여 보안 모델을 제안한다.

◆ 의사랜덤치환을 이용한 다중레벨 키분배

- 크기가 $N$인 임의의 치환과 $(0, N!-1)$ 정수가 일대일 대응되는 성질을 이용
- 선형합동법에 의해 발생되는 난수에 대응되는 치환들을 결합하여 랜덤치환을 발생
- 난수 발생 알고리즘 : 선형합동법 $X_{m+1} = X_m + Q \bmod N!$
- Trapdoor 일방향 치환 발생

  $X_1 = X_0 + Q \bmod N! \leftrightarrow P_1$

  $X_2 = X_1 + Q \bmod N! \leftrightarrow P_2$

  $P_1' = P_1 \circ P_2$
- 치환 $P_1'$에 대응되는 난수 $X_1'$의 발생은 쉽지만 이 $X_1'$로부터 치환 $P_1$에 대응되는 난수 $X_1$ 또는 치환 $P_2$에 대응되는 $X_2$를 찾는 것은 계산량적으로 어려움에 있어 trapdoor 일방향성을 가짐

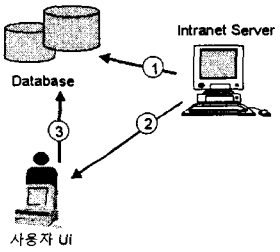
1. 준비

   ① *Server* : $K_i$ 생성, 각 보안 등급별 데이터를 $K_i$로 암호화

   ② *Server* → $U_i$ : $SK_{Server}(K_i)$ $(1 \le i \le n)$

2. 사용

   ③ 사용자 $U_i$ : 자신의 보안 등급에 해당하는 데이터를 $K_i$를 이용하여 복호화하여 접근 가능




<그림 6> 다중레벨 정보관리 모델

프로토콜 설명 :

① 인트라넷 서버는 각 데이터와 사용자 클래스를 직책에 따른 보안 등급으로 나누고, 각 사용자 클래스 $U_i$에 해당하는 키 $K_i$를 생성한 후 이를 이용하여 보안 등급별 데이터를 각각 암호화하여 저장해둔다.

② 서버는 생성된 $K_i$에 서명한 $SK_{Server}(K_i)$ $(1 \le i \le n)$를 보안 등급에 해당하는 각 사용자 클래스 $U_i$에게 전송한다. 필요하다면 certified mail을 적용할 수도 있다.

③ 사용자 클래스 $U_i$에 속하는 사용자들은 $K_i$를 이용하여 자신의 보안 등급에 해당하는 데이터를 복호화하여 접근할 수도 있고, 자신보다 낮은 보안 등급을 가지는 사용자 클래스의 데이터에도 접근할 수 있다. 하지만 그 역은 성립하지 않는다.

## 6. 제안 모델의 구현 및 결론

5장에서 제안한 각 서비스에 대한 보안 모델을 컴퓨터 시뮬레이션을 통하여 구현하였다. SUN UltraSparc(143MHz) 시스템의 Solaris 2.5 환경과 Pentium Pro(180MHz) PC의 Windows 95 환경 하에서 JDK(Java Development Kit) 1.1.4를 이용하여, 인트라넷 서버에 해당하는 서버 프로그램과 각 사용자에 해당하는 클라이언트 프로그램을 Java application 형태로 생성하여 보안 모델의 프로토콜에 따라 서로 통신할 수 있도록 하였다. 각 모델에 기본적으로 적용된 알고리즘들로는 관용키 암호시스템으로

데이터 암호화에 IDEA, 공개키 암호시스템으로는 주로 사용자 인증에 RSA를 사용하였다. 각 메시지에 대한 무결성 보장을 위한 해쉬 알고리즘으로는 MD5, SHA를 사용하였고, 의사랜덤치환 발생 알고리즘은 직접 제작하여 구현하였다. 본 시스템 구현에서는 실제 적용할 수 있는 인트라넷을 구성하기보다는 시뮬레이션을 통하여 각 서비스에 보안 모델을 적용한 사례를 보여주는데 주력하였다. 본 보안 모델을 기반으로 스마트 카드 등을 이용한 사용자 인증, 윈드와이드웹 서버 프로그램을 통한 인트라넷 서버 구축, CGI · Java · ActiveX 기술 등을 이용한 암호 기술 및 프로토콜을 구현함으로써 윈드와이드웹 인터페이스에 그대로 적용한다면 일반 사용자들은 전혀 불편함 없이 각 인트라넷 서비스를 이용할 수 있다.

지금까지 인트라넷 보안에 관한 연구가 주로 외부로부터 보호하는데 초점을 맞추어 진행되어왔는데 반해, 본 논문에서는 실제 위협 사례에 대한 통계적 자료를 바탕으로 하여 보안 위협 사례의 많은 비중을 차지하는 내부 위협에 초점을 맞추어 연구를 진행하였다. 특히, 인트라넷에서 가장 많이 사용되고 있는 전자우편, 전자게시판, 전자결재, 정보 및 문서관리 서비스에 있어서 기존 방식의 문제점 및 내부위협을 분석하고, 실제 적용 가능한 기존의 암호 기술 및 프로토콜에 대해 조사하였다. 이를 기반으로 인트라넷에 적용 가능한 보안 모델을 각 서비스별로 제안하고, 컴퓨터 시뮬레이션을 통하여 구현하였다.

본 제안 모델은 인트라넷에서 제공되는 각종 서비스에 적용될 수 있으며, 기업 및 정부기관 내에서 매우 민감한 기밀 자료를 다루는 인트라넷 환경 내에서도 직접 응용될 수 있다. 앞으로 각 기업의 인트라넷 도입 영향으로 그 시장은 더욱 성장할 것이고, 기업 내 · 외부로부터 보다 안전한 인트라넷 서비스를 제공하기 위해 많은 연구들이 진행될 것이다. 특히, 기업 내에서 업무흐름에 따라 생겨나는 수많은 전자문서와 정보들을 보호하기 위한 연구는 암호학적 관점에서 보다 깊이 있고 광범위하게 진행되어야 하며, 최근 인트라넷과 상반되는 개념인 익스트라넷(Extranet), 기업 내의 모든 업무 프로세스를 통합하는 ERP(Enterprise Resource Planning)의 등장으로 인트라넷 환경 내에서의 보안은 필수적으로 요구되는 연구 분야이다.

## 참 고 문 헌


[1] http://www.forrester.com, Forrester Research Homepage
[2] 한국정보보호센터, 정보시스템 해킹 현황 및 대응, 1996
[3] 전산망보급확장과 이용촉진에 관한 법률
[4] 무역업무자동화촉진에 관한 법률
[5] 공업 및 에너지기술기반조성에 관한 법률
[6] 화물유통촉진법
[7] J.B.Postel, Simple mail transfer protocol, RFC 821, 1982
[8] D.Crocker, Standard for the format of ARPA Internet text messages, RFC 822, 1982
[9] CCITT Recommendation X.400, "Message Handling System and Service Overview", 1988
[10] CCITT Recommendation X.509, "The Directory - Authentication Framework", 1988
[11] N.Borenstein, and N.Freed, Multipurpose Internet Mail Extensions(MIME) : Message Header Extensions for Non-ASCII Text, RFC 1521, 1993
[12] K.Moore, Multipurpose Internet Mail Extensions(MIME) : Mechanisms for Specifying and Describing the Format of Internet Message Bodies, RFC 1522, 1993
[13] http://www.ifi.uio.no/~staalesc/PGP/, International PGP Home page
[14] J.Linn, Privacy Enhancement for Internet Electronic Mail : Message Encryption and Authentication Procedures, RFC 1421, 1993
[15] S.Kent, Privacy Enhancement for Internet Electronic Mail : Certificate-Based Key Management, RFC 1422, 1993
[16] D.Balenson, Privacy Enhancement for Internet Electronic Mail : Alogorithms, Modes, and Identifiers, RFC 1423, 1993
[17] B.Kaliski, Privacy Enhancement for Internet Electronic Mail : Key Certification and Related

Services, RFC 1424, 1993
[18] http://www.rsa.com/, RSA Inc., S/MIME
[19] S.Even, O.Goldreich, and A.Lempel, "A Randomizing Protocol for Signing Contracts.", Communicatons of the ACM, vol.28, no.6, pp. 637-647, 1985
[20] M.Mambo, K.Usuda, and E.Okamoto, "Proxy Signature", SCIS 95, pp. B1.1.1-17, 1995
[21] 박상준, 박상우, 원동호, "효율적인 RSA 다중 서명 방식", 통신정보보호학회논문지, vol.7, no.2, pp.17-26, 1997
[22] D.Chaum, "Group Signatures", Advances in Cryptology - EUROCRYPT '91 Proceedings, pp. 257-265, 1991
[23] S.G.Akl, and P.D.Taylor, "Cryptographic solution to a multilevel security problem", Advanced in Cryptology : Proceedings of CRYPTO '84, pp.237-248, 1985
[24] 김주석, 신원, 이경현, "랜덤치환을 이용한 다중레벨키 관리방안", 한국정보처리학회 '97 춘계학술발표논문집, pp. 1038-1043, 1997
[25] J.Zhou, and D.Gollmann, "Certified Electronic Mail", Advanced in Cryptology : Proceedings of CRYPTO '97, pp.160-171, 1997
[26] ISO 7498-2 : Security Architecture
[27] W.Ford, "Computer Communication Security", Prentice-Hall, 1994
[28] D.Atkins, P.Buis, C.Hare, R.Kelley, C.Nachenberg, A.B.Nelson, P.Phillips, T.Richey and W.Steen, "Internet Security Professional Reference", New Riders, 1996
[29] D.Garrett, G.Bivings, M.Woodell, M.Mazan, E.Ashman, R.Simon, J.Noland, J.Ablan, M.Benson, S.Chandramouli, H.Herzog, M.Handy, M.Baird, J.Doody, J.Miller, A.M.Yerks, L.Sandage, A.Klein, F.Pappas, N.Goth, P.Itoi, S.Greenberg, J.Becker, E.Landgraf, C.Majersik, "Intranets Unleashed", Sams Net, 1996
[30] B.Schneier, "Applied Cryptography", 2nd, John Wiley & Sons, 1996