PKI를 이용한 인스턴트 메신저에서의 인증 시스템 설계

박수영* · 최광미** · 정채영*

A Design of the Certification System in a Instantant Messenger Using PKI

Su-Young Park* · Gwang-Mi Choi** · Chai-Yeoung Jung*

이 논문은 2004년도 조선대학교 학술연구비를 지원받았음

요 약

컴퓨터와 네트워크의 보급이 일반화되면서 인터넷을 통한 정보 전달이 일상생활처럼 되고 있다. 기존에는 정보를 전달하기 위한 방법이 주로 전자메일에 한정되어 있던 것에 반해, 요즘은 좀 더 즉각적으로 메시지를 전달해주는 인스턴트 메신저를 많이 사용하고 있다. 인스턴트 메신저는 이러한 장점으로 인해 국내에서도 사용자가 많이 늘고 있다. 그러나 대부분의 인스턴트 메신저 서비스는 인터넷상에서 많은 부분이 노출되지만 클라이언트는 이를 느끼지 못한 채 사용하고 있다. 이는 마치 전화도청과 같다고 할 수 있다. PKI를 사용한 암호화 기술은 인테넷에서 접근 통제, 인증, 기밀성, 무결성, 부인거절 등의 서비스들을 제공할 수 있는 공개키 기반 구조를 발달시켜왔다. 본 논문에서는 인스턴트 메신저의 안전한 통신을 위해 PKI(공개키 기반구조)를 이용한 인스턴트 메신저에서의 인증 프로토콜에 대해 설계하였다.

ABSTRACT

As computers and networks become popular, distributing information on the Internet is common in our daily life. In the past, e-mail has been the primary choice of exchanging information, but instant messengers are gaining popularity abroad and domestically because of their nature of getting immediate reponses. However a instant messenger services have the exposure of data on internet but clients use them without recognizing their exposure. It's like phone tapping. The coding technology using Public Key Cryptosystem has developed the public key infrastructure to be able to do the services of Access-control, Authentication, Confidentiality, Integrity, and Non-repudiation with internet. It is a thesis that suggests the certification protocol in a instant messenger using PKI(Public Key Infrastructure) for secure communication.

키워드

Messenger, PKI(Public Key Infrastructure), Certification

Ⅰ. 서 론

인스턴트 메신저란 네트워크를 통하여 실시간으로 메시지를 주고받을 수 있는 프로그램을 말한다. 대부분의 인스턴트 메신저 프로그램은 메시지를 전송하는 기능 외에 부가적으로 파일 전송 · 일대일 대화 · 대화 방 · 사용

* 조선대학교 컴퓨터통계학과

** 동강대학 컴퓨터인터넷 계열

접수일자 : 2005. 9. 1

자 검색 기능을 제공한다.

그러나 현재 사용되고 있는 대부분의 인스턴트 메신저는 전송되는 정보에 대한 보안 기능이 없는 상태로 운영되고 있다.

메신저의 보안을 위해서는 메신저를 사용하는 사용자가 많아 복잡한 키(Key)를 적절하게 관리할 수 있는 암호화 방식이 요구되고, 안전성과 신뢰성을 확보하기 위해 인증, 무결성, 부인봉쇄 등의 서비스가 필요되어진다.

공개키 기반구조(PKI : Public Key Infrastructure)를 구축함으로써 암호키 갱신, 복구, 위탁 등과 같은 키 관리, 인증서 생성 및 위탁 관리, 그리고 인증 정책 관리와 같은 서비스의 제공이 가능하다[1].

본 논문에서는 Ⅱ장에서 현재 서비스되고 있는 인스턴트 메신저들의 일반적인 기능과 보안 위협들을 분석하고, Ⅲ장에서는 공개키 기반구조를 서술한다. Ⅳ장에서 PKI를 이용한 인스턴트 메신저에서의 인증 처리 프로토콜을 제안하고, Ⅴ장에서는 연구의 결과 및 향후과제에 대하여 기술하였다.

Ⅱ. 관련연구

2.1 ICQ(I Seek You) 메신저

ICQ는 미라빌리스사의 제품으로 인스턴트 메신저의 원조이며, 그 사용자 수도 많다. ICQ의 특징으로는 사용자가 대화 모드를 선택하여, 현재 자신의 상태를 다양하게 표시할 수 있으며, 대화 모드에는 온라인, 오프라인, 방해금지, 비공개 등으로 모드에 따라서 메시지 수신 방법 등의 차이가 있다. 또한 ICQ는 상대방이 접속 중이 아니더라도 메시지나 파일 전송, 채팅 요구 등이 가능하다[3].

2.2 MSN(Microsoft Network) 메신저

MSN 메신저는 마이크로소프트사의 제품으로 메일 서비스 계정으로 메신저에 접속한다. MSN 메신저는 접속한 사용자에게 실시간으로 메시지 전송을 할 수 있다. 인스턴트 메시지 창은 일대일 대화 기능처럼 두 사용자가 주고받는 메시지를 한 화면에 보여주고, 두 사용자간에 일대일 대화를 하는 동안 다른 사람을 초대하여 대화방 기능처럼 사용할 수 있다. 또한 인스턴트 메시지 창에서 현재 대화중인 상대방에게 파일을 전송할 수 있다[4].

2.3 AIM(AOL Instant Messenger) 메신저

AIM 메신저는 중앙의 BOS 서버를 경유하여 한 사용자가 다른 사용자에게 HTML로 작성된 평문 메시지를 전송한다. AIM의 이미지는 BOS 서버를 경유하여 목적지 사용자에게 중계되며 직접적인 연결을 통하여 전송된다. 직접적인 연결은 음성채팅에서 이용되고 데이터는 직접 연결된 사용자들 사이에 전송된다. 또한 AIM 메신저는 먼 거리에 있는 사용자에게 게임 프로그램의 실행을 요청할 수 있지만, 이러한 요청 동안에는 어떠한 직접연결도 설정될 수 없다[5].

2.4 보안 위협

주요 인스턴트 메신저 제작회사의 공통적인 보안 위협은 다음과 같다[3][4][5].

- 감염된 파일 전송 : 의도적으로 감염된 파일을 보내거나 또는 자신도 모르는 사이 감염된 파일을 다른 사용자에게 보낼 수 있다.
- 통신 메시지 노출 : 메신저를 이용한 어떤 대화 내용도 암호화되지 않는다.
- 저작권 침해 : 메신저를 통해 완전하게 전송된 많은 파일(복사된 파일, MP3 파일, 복사된 사진 등)이 저작권법에 위배된다.
- 현혹적인 책략 : 바람직하지 않은 일부 인터넷 사용자는 개인의 신상 정보는 물론 각종 비밀번호 등의 누설을 유도한다.
- 파일 전송 시 IP 주소 노출 : 파일 전송과 이미지 전송, 음성채팅, 파일공유는 메신저 사용자의 실제 IP 주소를 노출시킬 수도 있다.

Ⅲ. PKI 구성

3.1 PKI 개요

PKI(Public Key Infrastructure)는 공개키 기반구조로, 공개키 암호시스템에서의 공개키를 공개키를 공개하는 대신 공개키와 그 공개키의 소유자를 연결하여 주는 인증서(Certificate)를 발행하는 시스템이다. 인증서는 신뢰할 수 있는 제3자(인증기관)의 서명문으로 신뢰객체가 아닌 사람은 그 문서의 내용을 변경할 수 없도록 한다[6][7].

공개키 기반구조는 크게 클라이언트로부터 실질적인 인증서 발급요청을 받아 X.509 인증서를 발행하는 인증서버(CA), 클라이언트로부터 인증서 요청과 클라이언트 신분을 확인하고 인증서버가 발행한 인증서를 클라이언트에게 전달하는 등록서버(RA), 그리고 발행한 인증서를 저장하고 차후 클라이언트 요청이 있을 경우 제공하는 디렉토리서버로 이루어진다[6][7].

그림 1과 표 1은 PKI의 구성객체를 설명해준다.

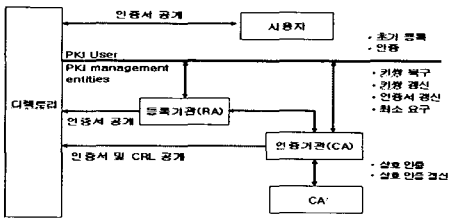


그림 1. 공개키 기반구조 구성 객체
Fig. 1. Constituent Objects of PKI

표 1. 공개키 기반구조 객체
Table 1. Constituent Objects of PKI

인증기관 (CA)	'다른 CA, 사용자, 등록기관에게 인증서 발행 및 분배 '인증서 소유자와 등록기관으로부터 취소 요구를 수용 '디렉토리에 인증서 및 인증서취소목록(CRL)을 공개 'CA 인증서들을 요구
등록기관 (RA)	'다른 CA, 사용자, 등록기관에게 인증서 발행 및 분배 'CA에 인증 요청을 전송 '디렉토리로부터 인증서와 CRL을 검색 '인증서 취소 요청을 생성
디렉토리	'인증서 및 인증서 취소목록 등 PKI 관련된 정보들이 저장 및 검색하는 장소
사용자	'일반적인 사람 뿐 아니라 PKI를 이용하는 시스템을 포함 '인증서 생성 · 취소 · 갱신 요구 '디렉토리로부터 인증서 및 CRL 획득 '인증경로 검증

3.2 인증서 X.509

인증서는 사용자의 신분과 공개키를 연결해주는 문서로 인증기관의 비밀키로 전자서명하여 생성된다 인증서의 형식은 1988년 ITU-T가 X.509 초기버전을 공표하고, 1993년에 버전 2를 공표했으며 1995년 이후로는 ISO/IEC 9594-8의 문서와 동일시되어 공동 개발되었다. 현재 X.509 버전 3까지 공표되었고, X.509 v3 형식은 그림 2과 같다[6].

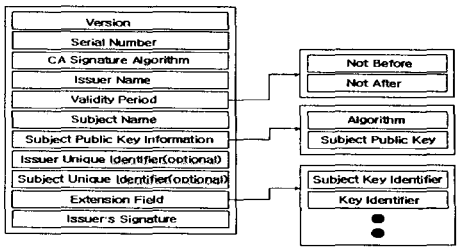


그림 2. X.509 v3
Fig. 2. X.509 v3

3.3 인증서 발급

그림 3는 인증기관을 이용한 인증서 발급절차를 보여주고 있다.

1. 인증서를 신청하는 곳에서는 우선 인증서버의 인증서를 설치해야 한다.
2. 클라이언트는 공개키와 인증서 발급요청서를 등록기관에 보낸다.
3. 접수한 인증 신청을 심사한다.
4. 신원확인에 문제가 없다면, 등록서버는 인증서버에 발행요청을 한다.
5. 인증서버는 공개키와 사용자정보를 이용하여 X.509 인증서를 만들어, 해당 인증서를 등록서버에 전달한다.
6. 등록서버는 모든 신뢰당사자가 이용할 수 있도록 인증기관의 저장소 또는 디렉토리 서버에 저장한다.
7. 등록서버는 클라이언트에게 인증서를 발급한다.
8. 발급된 인증서는 인증기관의 정책에 따라 관리된다.

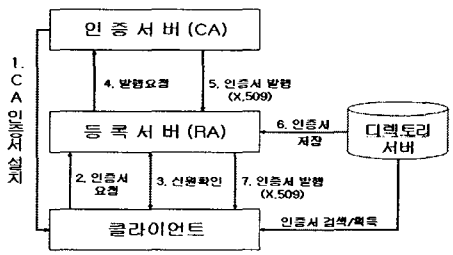


그림 3. 인증서 발급절차
Fig. 3. Issue Procedure of Certificate

Ⅳ. PKI를 이용한 인스턴트 메신저에서의 인증 프로토콜 제안

본 절에서는 제안된 사용자 인증을 위한 새로운 방법의 전반적인 흐름은 그림 4와 같다. 이에 대해서 보다 자세하게 살펴보면 다음과 같다.

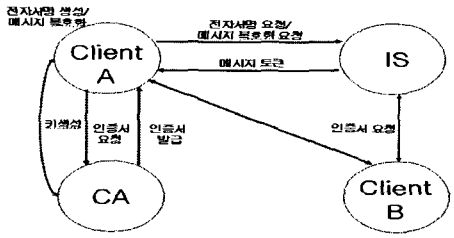


그림 4. 암호 프로토콜 전체 개략도
Fig. 4. Block Diagram of Encryption Protocol

※ 인증 프로토콜에서 사용되는 기호

CA : 인증기관
IS : 인스턴트 메신저 서버
Client A : 사용자
M : 메시지
ER : 공개키 암호알고리즘 암호화
DR : 공개키 암호알고리즘 복호화
Z : 압축 알고리즘
SER : 대칭키 암호알고리즘 암호화
SDR : 대칭키 암호알고리즘 복호화
KUa : A의 공개키
KRa : A의 개인키
KUb : B의 공개키
KRb : B의 개인키
Ks : 세션키
E : 알고리즘 암호
D : 알고리즘 복호
H : 해쉬 알고리즘
Certificate A : A의 인증서
Certificate B : B의 인증서
PSE : 개인 신상에 관한 정보 및 사용자의 공개키/개인키

4.1 인증서 요청

Client A는 PSE를 생성하여 세션키(Ks)로 암호화하고 세션키를 CA의 공개키를 암호화하여 보낸다. CA는 개인키를 이용하여 세션키를 얻은 후 세션키로 암호화된 메시지를 보게된다.

세션이 끝나면, 세션키는 없어지게 된다.

$$ERKUCA\{ Ks \} \| EKs\{ PSE \} \quad (1)$$

4.2 인증서 발행

CA는 자신의 개인키로 복호화해서 세션키를 얻고 세션키로 암호화된 메시지를 보게된다.

$$DRKRCA \{ ERKUCA\{ Ks \} \| EKs\{ PSE \} \}$$
$$= DKs\{ EKs\{ PSE \} = PSE \quad (2)$$

신원확인에 문제가 없다면, CA는 공개키와 사용자정보를 이용하여 X.509 인증서를 만들어 Client A의 공개키로 암호화하여 인증서를 발급한다. 또한 발급된 인증서는 인증기관의 정책에 따라 관리된다.

$$ERKUa \{ Certificate\ A \} \quad (3)$$

4.3 인스턴트 메신저 서버(IS)에 등록

그림 5는 Client A가 IS에 등록하는 부분이며 수행과정은 다음과 같다.

Client A는 인스턴트 메신저에 등록하기 위하여 PSE를 Hash하고 자신의 개인키(KRa)로 암호화하는 과정을 통하여 문서의 지문과 자신의 서명을 한다.

$$ERKRa\{ H(PSE) \} \quad (4)$$

그리고 차후에 발생될 전송여부와 변조여부의 시비를 확인 할 수 있도록 Hash된 문서(H(PSE))를 보관한다. 그리고 M, ERKRa{ H(PSE)}, Certificate A를 함께 압축하고 세션키(Ks)를 사용하여 관용키 암호화알고리즘으로 암호화한다.

$$EKs\{Z\{M\|ERKRa\{H(PSE)\}\|Certificate\ A\}\} \quad (5)$$

세션키(Ks)는 IS의 공개키(KUs)로 암호화한 후

ERKUs(Ks) (6)

세션키로 암호화한 문서와 같이 IS에게 전송한다.

EKs{Z{PSE||ERKRa{H(PSE)}||Certificate A}}|| ERKUs(Ks) (7)

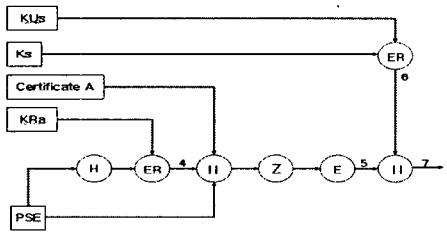


그림 5. 등록 전송전의 암호화 방법
Fig. 5. Encryption Method before Translating Registration

4.4 등록 접수

그림 6은 IS가 사용자로부터 암호화된 정보를 받아 개인키를 이용하여 해독하는 부분이며 수행과정은 다음과 같다.

IS는 Client A에게서 받은 문서 중 ERKUs(Ks)를 자신의 개인키(KRs)를 사용하여 세션키(Ks)를 구한다.

DRKRs{ ERKUs(Ks) } = Ks (8)

구한 세션키(Ks)를 사용하여 관용키 암호화된 부분을 복호화 한다.

DKs{ EKs{ Z{ PSE || ERKRa{ H(PSE) }|| Certificate A}}} (9)

사용된 압축을 풀어내고 Certificate A를 통하여 유효한 공개키인지 확인하여 유효하지 않은 인증서이면 재전송을 요구하고 유효한 인증서이면 디렉토리 서버에 저장 후 다음 작업을 수행한다.

Client A의 개인키(KRa)로 암호화 된 PSE를 Certificate A에 포함되어있는 A의 공개키를 사용하여 복호화 한다.

DRKUa{ ERKRa{ H(PSE) }} = H(PSE) (10)

압축을 풀어낸 문서에 포함된 PSE를 Hash하고 식 10에서 나온 H(PSE)과 비교하여 다르면 재전송을 요구하고 같으면 전송도중에 변조되지 않은 것으로 인정한다.

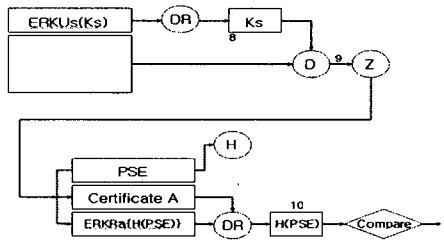


그림 6. 등록 수신후의 복호화 방법
Fig. 6. Decryption Method after Receiving Registration

4.5 사용자간의 공개키 획득

통신에 참여하는 사용자들은 서버에 인증서를 등록하고 서버의 인증서를 받은 사용자이어야 한다.

Client B는 먼저 인증기관으로부터 인증서를 받아 IS에 등록했다고 가정하자. Client A는 Client B와 통신하기 위해서 IS에 Client B의 인증서를 요청한다. 요청을 받은 IS는 저장소에서 Client B의 인증서를 검색한 후 Client B의 인증서를 Client A의 공개키로 암호화하여 전송한다.

ERKUa{ Certificate B } (11)

Client A는 IS에게서 받은 메시지를 자신의 개인키로 복호화하여 Client B의 공개키를 획득한다.

DRKRa{ ERKUa { Certificate B } = Certificate B (12)

Client A에게 대화요청을 받은 Client B 역시 IS에 Client A의 인증서를 요청하여 인증서를 획득한다. 인증서의 유효기간을 확인하여 인증서가 유효하다고 판단이 되면 비로소 획득한 공개키를 가지고 Client A와 통신이 이루어지게 된다.

획득한 공개키를 가지고 전송되는 내용을 암호화하기 위해서 짧은 키를 사용하면서도 타 공개키 암고리즘과 동

일한 안전도를 제공하는 ECC(Elliptic Curve Cryptography)를 암호화 알고리즘을 사용한다.

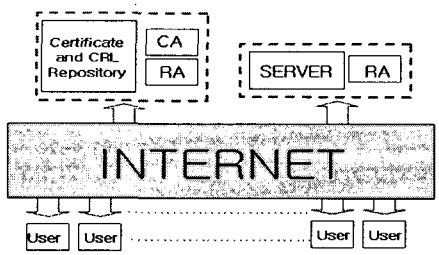


그림 7. 전체 시스템 구성도
Fig. 7. Block Diagram of Whole System

V. 결 론

본 논문에서는 안전한 암호화 통신을 위해 PKI과 새로운 프로토콜을 이용하여 사용자 인증 문제를 해결하였다. 제안된 시스템은 사용자의 아이디와 비밀번호가 유출되어도 인증서가 없으면 상대방의 공개키를 획득할 수 없어 통신할 수가 없으며, 인증서를 분실하게 되면 인증기관에서 재발급 받을 필요없이 서버에서 다운받으면 된다.

향후과제로는 PKI를 이용하여 획득한 공개키를 가지고 안전한 암호 통신을 위해 짧은 키 길이를 가지고도 타 공개키 알고리즘과 동일한 안전도를 제공하는 ECC 암호 알고리즘에 대한 연구를 계속 진행하고자 한다.

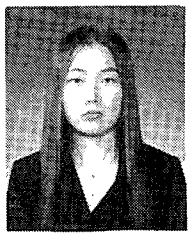
감사의 글

본 연구는 2004년도 조선대학교 학술연구부비에 의하여 이루어진 연구로서, 관계부처에 감사 드립니다.

참고문헌

[1] "전자상거래를 위한 보안 기술 체계 및 요소기술에 대한 이해", 한국전산원 차세대 서비스부, 1999.6
[2] 킬러 애플리케이션, "인스턴트 메시징", PC Week 4(19) : 66-67. 1999
[3] ICP, http://www.icq.com/.
[4] MSN Messenger, http://www.dreamsecurity.com/ products/ products_frame.html/.
[5] AOL, http://www.aim.com
[6] http://www.entrust.com/resourcecenter/whitepapers.htm, "Trusted Public-Key Infrastructures"
[7] http://www.kisa.or.kr/edu/index2.html, "공개키 기반구조"

저자소개



박 수 영(Su-Young Park)

2005년 조선대학교 컴퓨터 통계학과 박사과정수료

※ 관심분야 : 신경망, 인공지능, 정보보호 Bioinformatics

최 광 미(Gwang-MI Choi)

2003년 조선대학교 전산통계학과 이학박사
2002년~2006년 현재 동강대학 컴퓨터인터넷계열 초빙전임강사

※ 관심분야 : 신경망, 인공지능, 정보보호 디지털컨텐츠, Bioinformatics

정 채 영(Chai-Yeoung Jung)

1989년 조선대학교 컴퓨터공학과 공학박사
1986년~현재 조선대학교 컴퓨터 통계학과 교수

※ 관심분야 : 신경망, 인공지능, 정보보호, Bioinformatics