PKI를 이용한 인스턴트 메신저에서의 사용자 인증 처리

박수영*, 최광미* 정채영*
*조선대학교 컴퓨터통계학과
e-mail : csssy@nate.com

The Certificate Processing of the user in the Instant Message Using PKI

Su-Young Park*, Gwang-mi Choi*, Chai-Yeoung Jung*
*Dept. Computer & Statistics. Chosun University

요 약

컴퓨터와 네트워크의 보급이 일반화되면서 인터넷을 통한 정보전달이 일상생활처럼 되고 있다. IDC 보고서에 따르면 2003년 전 세계적으로 1억 3천명 정도가 무료 메신저를 사용하고 있으며 이중 8천만 명 정도는 매일 메신저를 이용하고 있는 것으로 나타났고 메신저의 사용은 앞으로 점점 늘어날 것으로 전망된다. PKI를 사용한 암호화 기술은 인터넷에서 접근 통제, 인증, 기밀성, 무결성, 부인거절 등의 서비스들을 제공할 수 있는 공개키 기반 구조를 발달시켜왔다. 통신의 주체가 되는 각각의 클라이언트들 간의 통신과 Server와 Client의 통신에 있어 악의적인 침입에 의한 정보누출이 문제가 되고 있다. 본 논문에서는 이러한 문제의 해결방안으로 환경에 적합한 PKI(공개키 기반 구조)를 이용한 인증 시스템을 설계하였다.

1. 서 론

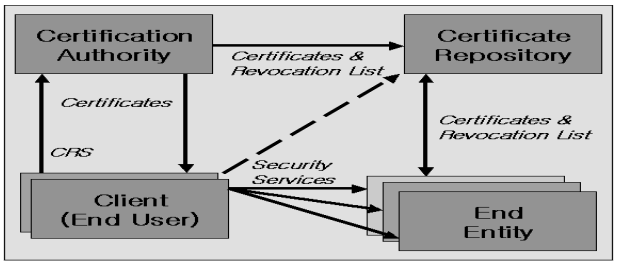
인터넷 사용인구가 증가하고 인터넷을 이용한 e-비즈니스와 서비스가 다양해짐에 따라, 인터넷을 이용한 통신 방법도 매우 다양해지고 있다. 인스턴트 메신저는 온라인 상에 있는 사용자들이 실시간으로 메시지를 주고 받을 수 있는 서비스이다. 인스턴트 메신저는 전자메일이 사용자가 메일 서버에 접속하여 메일을 읽어오는 과정을 요하는 것에 비해, 자동적으로 사용자 화면에 메시지를 전달함으로써 보다 간편하고 즉각적인 메시지의 전달을 기대할 수 있다. 그러나 현재 사용되고 있는 대부분의 인스턴트 메신저들이 정보전달에 있어 안전하지 못하다[1]. 메신저 등과 같은 인터넷 응용 기술의 안전성과 신뢰성을 확보하기 위해 인증, 무결성, 부인봉쇄 등의 서비스는 전자서명 기술을 활용함으로써 해결 가능하다. 전자서명 기술을 효과적으로 이용하기 위해서는 공개키 암호 방식이 필요하며, 공개키 암호 방식을 이용한 인증 방법을 구현하기 위해서는 기술적, 제도적 기반이 요구되는데 이를 공개키 기반구조(PKI : Public Key Infrastructure)라고 한다. PKI를 구축함으로써 암호키 갱신, 복구, 위탁 등과 같은 키 관리, 인증서 생성 및 취소 관리, 그리고 인증 정책 관리와 같은 서비스의 제공이 가능하다[2].

본 논문에서는 2장에서 PKI를 구성하는 각 객체들의 요구사항 및 객체의 특징에 대하여 설명하고, 3장에서는 현재 서비스되고 있는 인스턴트 메신저들의 보안 위협들을 분석하고 4장에서 PKI를 이용한 인스턴트 메신저에서의 인증 처리 프로토콜을 제안하며, 끝으로 5장에서 연구의 결론 및 향후과제에 대하여 기술하였다.

2. PKI 구성요소 및 요구 사항 분석

본 절에서는 PKI구성객체들의 운용을 위해 요구되는 사항들을 기술한다. PKI는 인증서의 발급, 사용 및 취소와 관련된 서비스를 제공하며, PKI환경을 구축하는 주요 객체는 인증기관(CA - Certification Authority), 인증서 저장소(Certificate Repository), 최종 사용자(End-User of Client) 그리고 서비스 제공 주체(e-commerce service 제공자)로 구분된다[4].

<그림 1>는 PKI 구성객체의 기본적인 트랜잭션을 보여준다.



(그림 1) PKI 기본 구성 객체

인증기관(CA: Certification Authority) : 사용자에게 인증서를 발급하거나 취소하고 공개키 인증서와 인증서 취소 목록(CRL: Certificate Revocation List)을 공개된 장소에 공고하는 역할을 담당한다. CA에서 요구되는 기능을 요약하면 다음과 같다[1-2, 4]

- 전자서명의 생성기능
- 인증서의 생성 및 확인
- 인증서의 발급 및 재발급
- 인증서 소유자에 대한 정보 관리
- 사용자의 이름 및 공개키의 유일성 확인
- 디렉토리 서버 관리
- 인증서 취소 목록(CRL) 관리
- 자료의 백업

CA의 기능 중 발행된 인증서 및 CRL을 실시간적으로 인증서 저장소에 공고 할 수 있는 기능이 요구된다. CA는 항상 CA인증서와 상호 인증서 쌍과 상호 인증서 쌍과 CRL을 공개 할 수 있어야 한다. 또한 CA들은 계층적 신뢰 모델에 기반을 둔 PKI를 지원하기 위해 상위 CA로부터 인증서를 요구할 수 있어야 한다[6].

인증서 저장소(Certificate Repository) : 디렉토리 서비스(Directory Service)라고도 하며, 인증서와 인증 경로를 찾기 위해서 사용된다. CA에 의해 발행된 공개키 인증서와 CRL을 저장하고 열람할 수 있도록 검색 기능을 제공해야 한다.

사용자(Client, End-User) : PKI구성 객체 중에서 Client가 요구하는 기능은 전자서명을 검증하고, 인증서 저장소에서 인증서와 CRL을 획득 할 수 있어야 한다. 최종 사용자 측에서 요구되는 기능은 다음과 같이 요약 할 수 있다.

- 저장 서명키 생성 기능
- 인증서 설치 기능
- CRL 설치 기능
- 인증서 검증 기능

인증서(Certificate) : 인증서는 공개키의 합법성을 보증하는데 이용된다. 서명을 확인하는 사람은 인증서의 서명을 확인하여 서명에 위조나 변조가 없다는 사실을 확인한다. 현재 공개키 인증 시스템에서 사용되는 표준은 ITU-T X.509 표준에 의해서 정의된다[6].

인증서 폐지목록(Certificate Revocation List) : 예정된 유효기간이 만기일이 도래하기 전에 취소된 인증서에 대한 정보를 인증서 취소 목록이라 한다[6].

3. 메신저의 보안위협

ICQ, Microsoft, AIM등 주요 인스턴트 메시징 제작 회사는 프라이버시 노출 사례와 알려진 결함에 대한 내용을 정기적으로 발표하고 있다. 주요 인스턴트 메시징 제작회사의 공통적인 보안위협은 다음과 같다[7-9]

- Infected Files : 의도적으로 감염된 파일을 보내거나 또는 자신도 모르는 사이 감염된 파일을 다른 사용자에게 보낼 수 있다.

- Unencrypted Communication : 메신저를 이용한 어떤 대화 내용도 암호화되지 않는다.

- Copyright Infringement : 메신저를 통해 완전하게 전송된 많은 파일(복사된 파일, MP3 파일, 복사된 사진 등)이 저작권법에 위배된다.

- Social Engineering : 바람직하지 않은 일부 인터넷 사용자는 매우 현혹적인 내용으로 개인의 신상 정보는 물론 각종 비밀번호 등의 누설을 유도한다.

- File Transfers Reveal IP Address : 파일 전송과 이미지 전송, 음성채팅, 파일고유는 메신저 사용자의 실제 IP 주소를 노출시킬 수도 있다.

AIM 메신저의 또 다른 파일공유 특성은 익명의 AIM 사용자가 잘못하여 고유한 디렉토리에 있는 중요한 정보를 우연히 발견 할 수 있다.

ICQ이 메시지 로깅 특성은 메시징 세션을 텍스트 파일로 기록하는 기능이 있으며, 만일 의도적인 사용자가 텍스트 파일에 대한 액세스 권한을 얻을 경우 이 정보는 노출될 수가 있다.

4. PKI를 이용한 인스턴트 메신저에서의 인증 프로토콜 제안

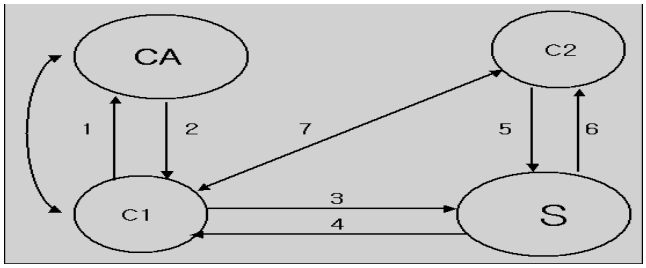
인스턴트 메신저에서 사용자 인증을 위한 새로운 방법의 전반적인 흐름은 다음과 같으며 제안한 프로토콜은 사용자가 사용하고자하는 인스턴트 메시징 벤더들의 서버에 아이디와 패스워드를 제출하는 것으로 한다.

M : 메시지

ER : 공개키 암호알고리즘 암호화

DR : 공개키 암호알고리즘 복호화

SER : 대칭키 암호알고리즘 암호화



(그림 2) 암호 프로토콜 전체 개략도

※ 인증 프로토콜에서 사용되는 기호

CA : 인증기관

S : 인스턴트 메시징 서버

C1, C1 : 사용자

SDR : 대칭키 복호알고리즘 복호화

KUa : C1의 공개키 KRa : C1의 개인키

KUb : C2의 공개키 KRb : C2의 개인키

E : 알고리즘 암호 D : 알고리즘 복호

KA : 인증키 KS : 대칭키

Certificate C1 : C1의 인증서 Certificate C2 : C2의 인증서

PSE : 사용자 이름, 사용자의 공개키/개인키, 자신이 믿는 루트 인증기관의 공개키를 저장하고 있는 국부메모리

4.1 인증서 등록

인증서 신청 및 발행 절차는 <그림 2>와 같으며 수행과정은 다음과 같다.

CA와 C1는 메시지를 보호하기 위한 초기 인증키와 참조값을 안전한 방법(out of banc)을 통하여 고유하고 있어야 한다. C1은 PSE를 생성하여 인증키로 암호화하여 인증기관에 전송한다.

$$ERKUKA\{ PSE \} \quad (1)$$

4.2 인증서 발행

CA는 인증키로 럼증 후 생성된 인증서를 C1의 공개키로 암호화하여 전송한다.

$$ERKUa\{ Certificate\ C1 \} \quad (2)$$

4.3 개인키 소유 증명

C1은 C2와 대화하기 위해 자신의 인증서를 S의 공개키로 암호화하여 전송한다.

$$ERKUs\{ Certificate\ \ C1 \} \quad (3)$$

S는 자신의 개인키를 사용하여 암호화된 부분을 복호화한다.

$$DRKRs\{ Certificate\ C1 \} = Certificate\ C1 \quad (4)$$

S는 C1의 개인키 소유 증명을 위해 인증서내에 포함된 공개키를 이용하여 암호화된 임의의 대칭키로 암호화하된 인증서를 C1에게 보낸다.

$$ERKUa\{ SERKS\ \{ Certificate\ C1 \ \} \} \quad (5)$$

C1은 개인키를 이용하여 관용키로 암호화된 부분을 복호화하여 대칭키로 암호화된 인증서를 대칭키를 이용하여 구한다.

$$DRKRa\{ ERKUa\ \{ SERKS\ \{ Certificate\ C1 \ \} \} = SERKS\ \{ Certificate\ C1 \ \} = SDRKS\{ SERKS\ \{ Certificate\ C1\} = Certificate\ C1 \quad (6)$$

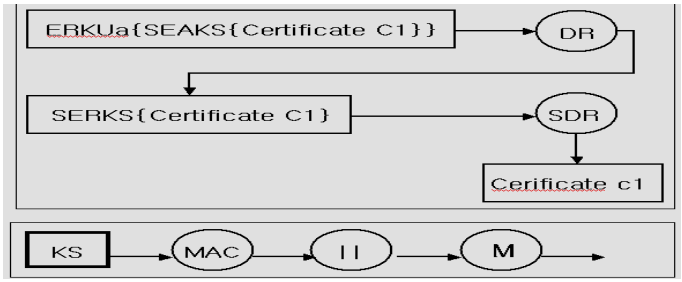
C1은 대칭키를 이용하여 생성한 MAC을 포함한 확인 메시지를 S에게 전송한다.

$$M\{ KS\ \{ MAC \ \} \} \quad (7)$$

4. 인증서 획득

확인메시지를 받은 S는 C1의 인증서를 저장소에 저장하고 C1이 대화하고자 하는 C2의 인증서와 공개키를 C1의 공개키로 암호화하여 전송한다.

$$ERKUa\{ Certificate\ C2 \ || \ KUb \ \} \quad (8)$$



(그림 3) 개인키 소유 증명 방법

C1으로부터 대화요청을 받은 C2역시 S에 C1의 인증서와 공개키를 요청한다. 요청을 받은 S는 저장소에서 C1의 인증서를 검색한 후 C1의 인증서와 공개키를 C2의 공개키로 암호화하여 전송한다.

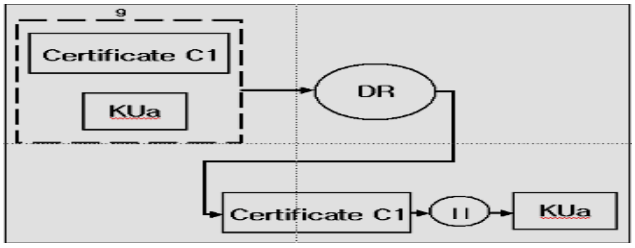
$$ERKUb\{ Certificate\ C1 \ || \ KUa \ \} \quad (9)$$

C2는 S에게서 받은 메시지를 자신의 개인키로 복호화 하여 C1의 인증서와 공개키를 구한다.

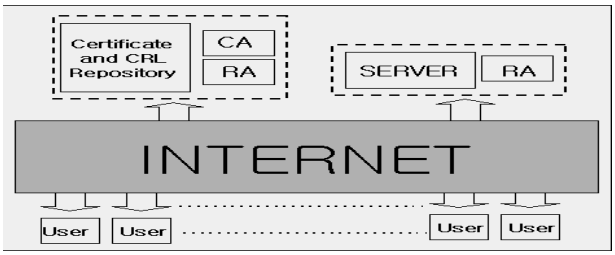
$$DRKRb\{ ERKUb\ \{ Certificate\ C1 \ || \ KUa \ \} = Certificate \ || \ KUa \quad (10)$$

C2는 Certificate C1를 통하여 획득한 공개키가 유

효한지 확인한 후 C1과의 대화를 시작한다. 전송되는 내용을 암호화하기 위해서 짧은 키를 사용하면서 타 공개키 알고리즘과 동일한 안전도를 제공하는 ECC를 암호화 알고리즘을 사용한다.



(그림 4) 메시지 수신 후 복호화 방법



(그림 5) 전체 시스템 구성도

5. 결 론

정보기술이 급속히 발전함에 따라 정보 기술을 이용한 새로운 응용서비스의 구현도 증가하고 있다. 그러나 이러한 최신 정보기술의 편리함 속에는 기존의 환경에서는 상상할 수 없었던 새로운 정보 기술 보안상의 문제점이 상존하고 있다.

본 논문에서는 서버와 클라이언트 환경에서 PKI를 이용한 사용자 인증 시스템을 제안하였다. 제안된 시스템은 사용자 아이디와 비밀번호가 유출되어도 인증서가 없으면 통신 할 수가 없으며, 인증서를 분실하게 되면 인증기관에서 재발급 받을 필요 없이 서버에서 다운받으면 된다.

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

참고문헌

[1] "Common Presence and Instant Messaging Message format", http://www.ietf.org/internet-drarts/draft-ietf-impp-opim-mesgfmt-03.txt

[2] R.L. Rivest, A. Shamir and L.M. Adleman,"A method for obtaining digital signaturesand public-key cryptosystem", Communications of the ACM 21, pp.120-126, 1978

[3] M. Myers, C. Adams, D. Solo, K. Kemp, RFC 2500, "Internet X.509 Certificate Request Message Format", IETF X.509 PKI(PKIX) Working Grout., March 1999.

[4] "Recommendation for a Unique Identifier for X.500 Distinguished Names.", 4, March, 983

[5] "CA-Browing System-A Supporting Application for Global Security Service", ISOC Symposium on Network and Distributed System Security, San Diego, pp.123-128, Feb. 94

[6] Jalal Feghhi, Jalil Feghhi, Peter Willianms, "Digital Certificate - Applied Internet Security", Addison Wesley, 1998

[7] ICQ, http://www.icq.com

[8] MAN, http://www.dreamsecurity.com/products

[9] AOL, http://ww.aim.com