情報保護學會論文誌
第18卷 第4號, 2008. 8

MITM 공격에 안전한 P2P 신뢰전송 메커니즘의 설계*

김 상 춘[1†], 권 혁 찬[2‡], 나 재 훈[2‡]
[1]강원대학교 전자정보통신공학부, [2]한국전자통신연구원 정보보호연구본부

Designing Reliable P2P Transmission Mechanism Against MITM Attack*

Sangchoon Kim[1†], Hyeokchan Kwon[2‡], Jaehoon Nah[2‡]
[1]Gangwon National University, [2]Electronics and Telecommunications Research Institute

요 약

많은 인터넷응용에서 인증 및 메시지 무결성을 제공하기 위해 PKI(Public Key Infrastructure) 기반 서비스를 제공하고 있다. 그리고 몇몇 연구에서는 PKI 기반의 P2P 서비스를 제안하기도 하였다. 그러나 P2P 응용의 경우 P2P의 open, dynamic, heterogeneous, autonomous 한 특성상 PKI의 적용이 어려우며, 특히 국가간 상호운용성을 지원하지 못하는 것도 P2P에의 적용을 현실적으로 어렵게 만든다. 본 논문에서는 PKI를 사용하지 않으면서도 MITM 공격에 안전한 P2P 신뢰전송 메커니즘을 제안한다. 본 메커니즘에서 각 피어는 자신의 공개키/비밀키 쌍을 자체적으로 생성하고 분배한다. 이 경우 MITM(Man in the Middle Attack) 공격에 취약하다는 문제가 있으나, 제안한 메커니즘은 MITM 공격에 대한 안정성을 제공한다. 본 메커니즘은 P2P 기반의 파일공유, IPTV, 분산자원 공유 등 다양한 분야에 응용이 가능하다.

ABSTRACT

Many Internet application provide the PKI(public key infrastructure)-based service to provide authentication and message integrity. Several researchers proposed PKI-based p2p network framework. However, in the real world, the use of PKI is not suitable for peer to peer network, because the peer-to-peer network is an open and dynamic network. Moreover, currently there is no nation - to-nation interoperable certificate. In this paper, we designed reliable p2p file sharing application without public key infrastructure. To do this we propose reliable public key distribution mechanism to distribute public key safely without PKI infrastructure for two-tier super-peer architecture. In our system, each peer generates and distributes its public/private key pairs, and the public key is securely distributed without PKI. The proposed mechanism is safe against MITM attack. This mechanism can be applied various P2P applications such as file sharing, IPTV, distributed resource sharing and so on

Keywords : P2P security, MITM, Public key distribution, PKI, self-certificate

접수일 : 2007년 12월 4일; 수정일 : 2008년 4월 28일;
채택일 : 2008년 5월 16일
* 본 연구는 지식경제부 및 정보통신연구진흥원의 IT 신성장 동력핵심기술개발사업의 일환으로 수행하였음. [유무선 환경의 개방형 IPTV2.0 정보보호 기술 개발(2008.3~2011.2)]
† 주저자, kimsc@kangwon.ac.kr
‡ 교신저자, hckwon@etri.re.kr, jhnah@etri.re.kr

I. 서 론

많은 인터넷 응용에서 인증 및 메시지 무결성을 제공하기 위해 PKI(Public Key Infrastructure) 기반의 서비스를 제공하고 있다. 이 경우 송신되는 메시지는 전송자의 서명을 포함하고, 수신자는 CA(Certificate Authority)의

도움을 받아 전송자의 서명을 검증하게 된다.

현재 PKI기반의 서비스를 제공하는 많은 응용들이 있지만, P2P에 실 적용된 사례는 없다. 실제로 [1-3]의 연구들에서는 PKI 기반의 P2P 네트워크 프레임워크를 제안하기도 하였으나, 현실세계에서의 P2P 응용에의 적용은 불가능 하다. 이는 P2P의 open, dynamic, heterogeneous, autonomous 한 특성 때문이기도 하며, 특히 국가간 PKI 상호 운용성을 제공하지 못하는 것도 전 세계적인 사용자가 존재하는 P2P에 적용을 현실적으로 어렵게 만드는 요소이기도 하다. 또한 PKI 인프라의 구축, 인증서 발급 및 관리를 위한 비용도 만만치가 않다.

P2P 오픈소스 프로젝트인 JXTA 프레임워크[4]의 경우에도 PKI를 사용하지 않고 공개키를 이용하는 방식을 채용하였다. 이 구조에서 각각의 피어는 공개키가 포함된 자신의 인증서를 스스로 생성한 후 Peer advertise 메시지 전송과정에서 배포한다. 비교적 간단한 방법이지만 이 방식은 공개키를 인증하는 제3의 신뢰기관이 존재하지 않기 때문에 MITM 공격 발생시 적절히 대응할 수가 없다. 예를 들어 중간의 공격자가 피어 A가 보낸 Peer advertise 메시지를 위변조하여 피어 A의 공개키를 자신의 공개키로 대치한다고 해도 이를 감지할 수 없기 때문이다. [그림 1] 은 MITM 공격의 사례를 보여준다. JXTA 프레임워크 명세서에서도 이를 인정하고 있으며 보안성을 크게 요구하지 않는 non-financial 응용에 적합한 방식이라고 설명한다.

본 논문에서는 PKI를 사용하지 않으면서도 안전한 P2P 응용을 구축할 수 있는 기반 기술로 PKI를 사용하지 않고 안전하게 자가 생성한 공개키를 분배하기 위한 메커니즘을 제안한다. 본 프레임워크에서 각 피어는 자신의 공개키/비밀키 쌍을 스스로 생성하고 분배하는 기본 구조를 가지며 MITM 공격에 대해서도 안정성을 가진다.

본 논문의 2장에서는 안전한 P2P 응용을 위한 신뢰전송 메커니즘을 제안하고, 이를 이용하여 구축한 P2P 응용 프로토타입에 대해 소개하고, 3장에서 결론을 맺는다.

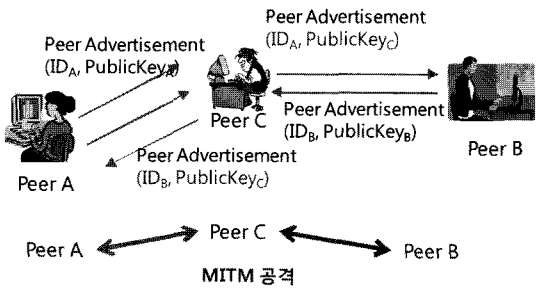
Ⅱ. P2P 신뢰전송 메커니즘의 설계

본 장에서는 설계한 P2P 신뢰전송 메커니즘에 대해 기술한다.

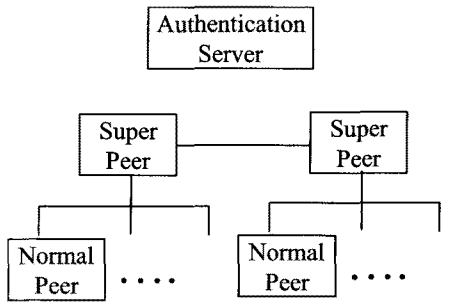
2.1 대상 응용의 기본 동작

본 논문에서 대상으로 하는 P2P 응용은 파일공유 응용이며 [그림 2]와 같은 슈퍼 피어 기반의 2계층 구조를 갖는다. 이 구조에서 각각의 피어는 유일하게 구분되는 ID를 가진다. 그리고 각각의 피어는 P2P 네트워크에 참여하기 위해 자신의 ID와 패스워드를 서버로부터 인증받아야 한다. 이 단계에서 각각의 피어는 서버로부터 슈퍼 피어의 정보들 - IP, ID, 공개키 - 을 수신하며, 이 정보를 기초로 슈퍼 피어를 선정하여 Join 메시지를 전송한다. Join이 성공하면 피어는 슈퍼피어에게 자신이 보유한 파일들의 메타정보를 전달한다. 본 논문에서는 자가 생성한 공개키/비밀키(self-certificate public/private key pairs) 쌍을 사용하며, [그림 2]의 인증서버는 PKI에서 CA(Certificate Authority)서버의 기능을 가진 서버가 아닌 단지 ID와 패스워드를 인증하는 서버이다.

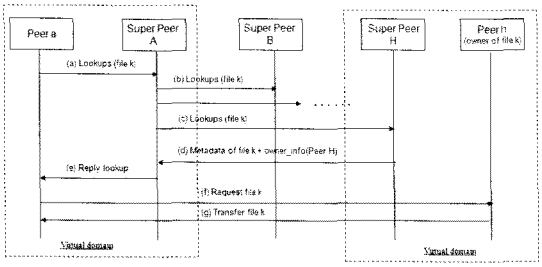
대상으로 하는 파일공유 응용의 기본적인 동작은 [그림 3]과 같다. [그림 3]의 슈퍼피어는 자신의 가상 도메인 상에 존재하는 각 피어가 소유한 파일에 대한 메타정보를 보유한다. 자원 검색을 요청하는 피어는 자신의 슈퍼피어에게 검색 요청을 하고, 슈퍼피어는 다른 슈퍼



〔그림 1〕 JXTA 프레임워크에서의 MITM 공격사례



〔그림 2〕 2계층 슈퍼피어 구조



〔그림 3〕 파일공유 응용의 기본 동작

피어들에게 파일검색 요청을 전달하여 검색을 수행하는 방식을 따른다.

2.2 보안 메커니즘

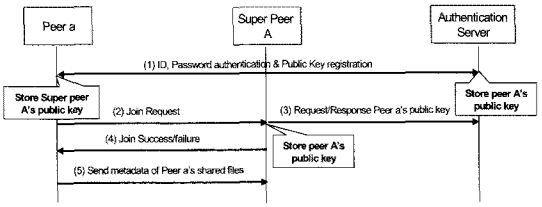
[표 1]은 본 논문에서 사용하는 기호들이다. 본 논문에서 슈퍼 피어는 응용에 의해 미리 선택되어 있는 것으로 가정한다. 또한 각 슈퍼 피어는 서버의 공개키와 현재 P2P 네트워크에 참여하고 있는 다른 슈퍼 피어의 공개키를 가지고 있다고 가정한다.

〔표 1〕 논문에 사용된 기호

기호	의미
ID_k	피어 K의 ID
IP_k	피어 K의 IP 주소
K_k^u	피어 K의 공개키
K_k^r	피어 K의 개인키
K_S^u	ID 인증서버의 공개키
K_S^r	ID 인증서버의 개인키
PW_k	피어 K의 비밀번호
$E_K(m)$	암호화 함수 (메시지 m을 암호화 키 k로 암호화)
$D_K(c)$	복호화 함수 (암호문 c를 복호화 키 k로 복호화)
$S_K(m)$	디지털 서명 (서명키 k, 메시지 m)

□ P2P 네트워크로의 Join 단계

본 프레임워크에서 각 피어는 공개키를 생성하여 인증 서버에 등록을 한다. 본 절에 나오는 수식 중 P_a, P_b는 각각 ID가 a,b인 피어를 의미하며, SP_A, SP_B는 ID가 A,B인 슈퍼피어를 의미한다. 편의상 슈퍼 피어는 대문자로 일반 피어는 소문자 기호를 사용하였다. S는 ID



〔그림 4〕 P2P 네트워크로의 Join 단계

인증 서버를 의미한다. [그림 4]는 P2P 네트워크로의 Join을 위한 전체적인 과정을 보여준다.

단계 1 : ID, password authentication & public key registration

이 단계에서는 피어 a가 ID와 패스워드를 통하여 서버에 인증을 수행하고, 자신의 공개키를 서버에 등록하는 과정이 포함된다.

① ID, Password 인증

② (피어 a → 서버) a의 공개키 등록

$$E_{K_S^u}(\text{"Public key registration"} \mid ID_a \mid IP_a \mid PW_a \mid K_a^u) \mid S_{PW_a}(m)$$

③ (서버) 피어의 ID 검증

- 서버의 개인키로 복호화
- 메시지에 저장된 패스워드와 피어가 등록한 패스워드와 비교를 통한 검증
- 피어의 패스워드를 통한 서명 검증

④ (서버 → 피어 a) 공개키 등록의 성공/실패 여부 반환

$$E_{K_a^u}(\text{"Pubkey registration success"} \mid ID_a \mid \text{"}SP\_Info\text{"} \mid \{IP_A \mid ID_A \mid K_A^u\} \mid \{IP_B \mid ID_B \mid K_B^u\} \mid ...) \mid S_{K_S^r}(m)$$

- 슈퍼피어의 목록과 IP, ID, 공개키 정보도 함께 전송
- 피어 a의 공개키로 암호화하여 전송

⑤ (피어 a) 인증서버의 ID 검증

- 자신의 개인키로 복호화
- 서버의 공개키로 서명 검증

단계 1까지는 피어를 패스워드 기반으로 인증하게 되며, 단계 1에서 피어의 공개키를 서버에 등록한 이후로 피어의 공개키가 사용가능한 상태가 된다.

단계 2 : Join Request

① (피어 a → 슈퍼피어 A) Join 요청

$E_{K_A^u}("Join\ request"|IDa|IPa|K_a^u)S_{K_a^r}(m)$

- Join 요청시 자신의 공개키도 함께 전송
- 슈퍼피어의 공개키로 암호화하고 자신의 개인키로 서명하여 전송

단계 3 : Request/Response peer a's public key

① (슈퍼피어 A → 서버) 피어 a의 공개키 요청

$E_{K_S^u}("Request\ public\ key"|IDa|IPa)S_{K_A^r}(m)$

② (서버) 슈퍼피어 A의 ID 검증
- 서버의 개인키로 복호화
- 슈퍼피어 A의 공개키로 서명 검증

③ (서버 → 슈퍼피어 A) 피어a의 공개키 반환

$E_{K_A^r}("Reply\ public\ key"|\{IDa|IPa|K_a^u\})S_{K_S^r}(m)$

④ (슈퍼피어 A) 서버의 아이디 검증
- 자신의 개인키로 복호화
- 서버의 공개키로 서명 검증

⑤ (슈퍼피어 A) 단계2에서 수신한 메시지에 포함된 피어 a의 서명 검증

단계 4 : Join success/failure

① Join 성공/실패 여부 회신

$E_{K_a^u}("Join\ success")S_{K_A^r}(m)$

② (피어 a) 슈퍼피어 A의 ID 검증
- 자신의 개인키로 복호화
- 슈퍼피어 A의 공개키로 서명 검증

단계 5 : Send matadata of peer a's shared files

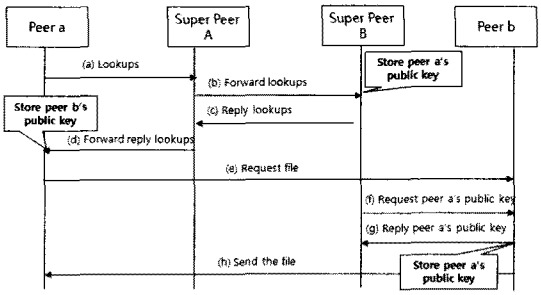
□ 안전한 파일공유 응용의 동작

[그림 5]는 본 논문에서 제안한 보안 메커니즘을 적용한 파일공유 응용의 동작과정을 보여준다.

[그림 5]의 각 단계에서 전송되는 메시지의 형식은 [표 2]와 같다.

파일 검색 과정을 요약하면 다음과 같다.

(a) 검색을 원하는 피어 a는 검색메시지(lookups)를 자신의 슈퍼피어 A에게 전송한다. (b) 이 메시지를 수신한 슈퍼피어는 이를 다른 슈퍼피어들에게 브로드캐스팅한다. 이 메시지에는 검색을 요청한 피어 a의 공개키가 포함되어 있으므로, 이 메시지를 수신한 슈퍼피어들은 피어 a의 공개키를 자신의 로컬 DB에 저장한다. (c)



〔그림 5〕 P2P 신뢰전송 동작 과정

〔표 2〕 〔그림 5〕의 전송 메시지 형식

	메시지 형식
a	$E_{K_A^u}("lookup\_req"\|\{"beyonce"\})\|S_{K_a^r}(m)$
b	$E_{K_B^u}("lookupfile"\|\{"beyonce"\}\|"requester"\|\{IDa\|IPa\|K_a^u\})\|S_{K_A^r}(m)$
c	$E_{K_A^u}("replylookup"\|\{"beyonce"\}\|fileid\|"owner"\|\{IDb\|IPb\|K_b^u\})\|S_{K_B^r}(m)$
d	$E_{K_a^u}("replylookup"\|\{"beyonce"\}\|"owner"\|fileid\|\{IDb\|IPb\|K_b^u\})\|S_{K_A^r}(m)$
e	$E_{K_b^u}("requestfile"\|fileid)\|S_{K_a^r}(m)$
f	$E_{K_B^u}("request\_pkey"\|IDa)\|S_{K_b^r}(m)$
g	$E_{K_b^u}("reply\_pkey"\|\{IDa\|K_a^u\})\|S_{K_B^r}(m)$

슈퍼피어 b는 자신의 가상도메인 내의 피어 a가 검색하는 파일을 소유하고 있음을 확인하고 이 정보를 검색을 요청한 슈퍼피어 A에게 반환한다. 이 메시지에는 파일을 소유한 피어 b의 공개키가 포함된다. (d) 슈퍼피어 A는 이 검색 응답 메시지를 피어 a에게 전달한다. 피어 a는 수신한 메시지에서 피어 b의 공개키 정보를 로컬 DB에 저장하고 파일요청을 하게 된다. (e) 피어 a는 파일을 피어 b에게 요청한다. (f,g) 피어 b는 피어 a의 공개키 정보를 갖고있지 않으므로, 슈퍼피어 B에게 a의 공개키를 요청하여 수신한다. (h) 피어 b는 요청받은 파일을 피어 a에게 전달한다.

초기에 피어가 서버에 공개키를 등록하는 메시지는 서버의 public key로 암호화되기 때문에 공격자가 복호화 하는 것이 불가능하다. 또한 피어는 자신의 패스워드로 서명을 해서 전송하며, 공격자는 이 피어의 패스워드를 모르기 때문에 서명의 위변조도 불가능하다. 서버에서 join 요청 피어로 반환하는 메시지 역시 마찬가지 이다. 일단, 서버에 공개키를 등록한 이후에는 각각의 안전한 채널을 통해 암호화된 형태로 공개키가 전달되기 때문에 공개키를 위변조하는 형태의 MITM 공격이 불가능 해진다.

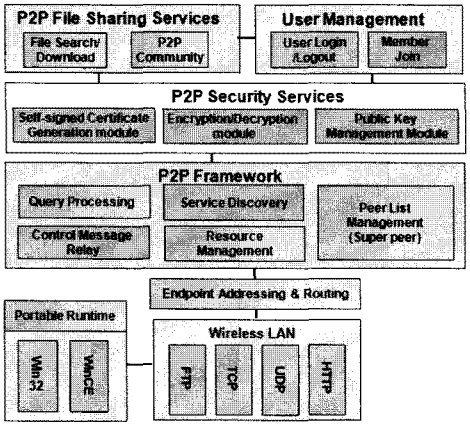
본 메커니즘은 각 피어의 공개키를 저장하고 제공하는 등의 관리 기능이 각 슈퍼피어에 분산되어 있는 구

조로 서버의 부하를 줄여준다. 또한 [그림 5]에서 볼 수 있듯이 각 피어가 파일을 검색하고 결과를 반환하기 위한 메시지 전달과정에서 각각의 신뢰적인 채널을 통해 자연스럽고 안전하게 공개키가 분배되는 구조를 갖는다.

슈퍼피어의 오류가 발생한 경우는 인증서버로 새로운 슈퍼피어 지정을 요청하고 다시 join 메시지 전송을 통해 새로운 슈퍼피어에게 가입을 한다.

□ 프로토타입 구현

본 논문에서는 제안한 보안 프레임워크를 적용한 안전한 P2P 파일 공유 응용에 대한 프로토타입을 구현하였다. 구현한 프로토타입의 소프트웨어 구조는 [그림 6]과 같다. [그림 6]에서 P2P 프레임워크는 기본적인 P2P 네트워킹을 지원하기 위한 JXTA 프레임워크를 탑재한 것이며, 그 위에 P2P 보안 서비스 모듈과 응용 모듈을 구현하였다. 본 논문에서 제안된 P2P 신뢰전송 메커니즘은 [그림 6]의 P2P Security Services의 3개 모듈에 구현하여 탑재되었다.

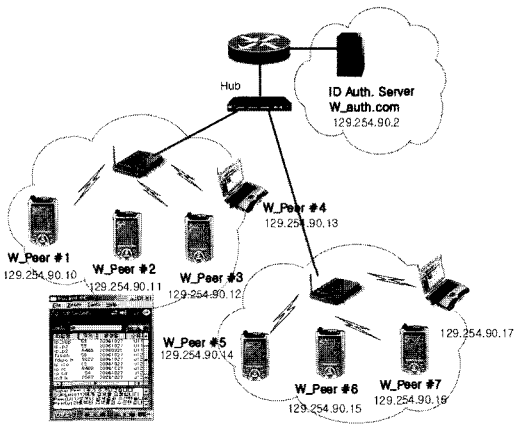


〔그림 6〕 소프트웨어 구조

JXTA framework 위에 추가로 구현한 프로토타입 모듈은 다음과 같다.

- P2P Security Services
- Self-signed Certificate Generation Module: 공개키를 자가 생성하는 모듈
- Encryption/Decryption Module: 엄/복호화 모듈
- Public Key Management Module: 공개키 관리 모듈로 다른 슈퍼 피어 및 일반 피어의 공개키를 저장 관리하는 모듈
- User Management : 로그인, Join 등 P2P 응용을 지원하기 위한 모듈을 포함한다.
- P2P File Sharing Services : P2P 파일공유 응용 모듈들을 포함한다.

본 연구에서 제안한 안전한 파일공유 응용은 WinCE 기반의 PDA 플랫폼에 구축하여 탑재하였다. [그림 7]은 테스트베드와 구현물의 메인 윈도우의 모습을 보여준다. 실제 동작시 [그림 7]의 피어 중 임의의 피어가 서버에 의해 슈퍼피어로 선택되어 동작한다.



〔그림 7〕 테스트베드

[표 3]은 본 프레임워크에서 사용한 데이터베이스의 구조를 보여준다. [표 3]의 데이터베이스는 인증서버, 슈퍼피어, 일반피어 모두가 보유하는 데이터베이스이다. [표 3]의 필드 중 Group ID 필드는 인증서버의 DB

〔표 3〕 데이터베이스의 구조

필드	설명
Group ID	그룹 ID ※ 인증 서버의 DB에만 존재
PeerID	피어의 ID
flag	N: Normal Peer, S: Super Peer, D: 자신의 가상 도메인 내의 Normal Peer ※ N, S flag는 인증서버와 슈퍼피어의 DB에 서만 사용되며, D flag는 슈퍼피어의 DB에서만 사용
PubKey	공개키
IP	IP 주소
metadata	메타데이터의 목록 ※ 슈퍼피어와 일반 피어에만 존재

에만 존재하는 필드로 가상 도메인의 그룹 ID를 저장한다. Flag 필드는 피어가 슈퍼피어인지 일반 피어인지를 구분하는 역할을 하며, D 플래그는 슈퍼 피어의 DB에만 사용되는 것으로, 자신의 가상도메인 내의 피어인지의 여부를 표시하는 플래그이다.

Ⅲ. 결 론

본 논문에서는 PKI를 적용하지 않고 안전한 P2P 신뢰전송 메커니즘을 제안하였다. 본 메커니즘은 PKI를 사용하지 않는 환경에서 MITM 공격에 안전한 형태로 공개키를 분배한다. 각각의 피어는 자신의 공개키를 자가 생성하며, 생성된 공개키는 초기의 Join과정과 이후의 파일검색과정에서 자연스럽게 배포된다.

본 메커니즘은 각 피어의 공개키를 저장하고 제공하는 등의 관리 기능이 각 슈퍼피어에 분산되어 있어 서버의 부하를 줄여준다. 본 메커니즘의 동작은 매우 간단하며 쉽게 구현이 가능하다. 또한 PKI 기반 구조에 비해 구현상의 비용이 따로 필요하지 않다. 실제로 P2P 네트워트의 특성상 PKI의 적용이 불가능하다. 실제로 국가간의 인증서 연동이 현재 불가능하며, 사용자가 자유로이 dynamic하게 가입/탈퇴하는 구조에서는 PKI기반 구조가 적합하지 않기 때문이다.

현재, 슈퍼피어에 오류가 발생한 경우, 효율적으로 P2P 망을 재구성하기 위한 추가 연구를 진행 중에 있다. 향후 본 보안 구조를 검증하는 과정, 다양한 P2P 응용에의 적용을 위한 추가의 연구 그리고 성능상의 분석 등이 필요하다. 특히 세션키를 활용하는 등 성능상의 개선방안, rekeying 방법, 악의의 슈퍼피어에 대한 대응방안, 등의 추가적인 연구가 필요하다.

참고문헌

[1] K. Berket, A. Essiari and A. Muratas , "PKI-Based Security for Peer-to-Peer Information Sharing", Proceedings of the Fourth IEEE International Conference on Peer-to-Peer Computing, Zurich, Switzerland, Aug. 25-27, 2004.

[2] Thomas Wölfl, "Public-Key-Infrastructure Based on a Peer-to-Peer Network", Proceedings of the 38th Hawaii International Conference on System Sciences, 2005.

[3] "LionShare P2P Profile of SAML", Tech. Report, Pennsylvania State University, 2005

[4] T.Dengler and al, The Project JXTA2.0 Super-Peer Virtual Network, Sun Microsystems, Tech. rep. May, 2003.

[5] J.Gu, J.Nah, C.Chae, J.Lee and J.Jang, "Random Visitor : a Defense against Identity Attacks in P2P Overlay Networks", LNCS 4298(WISA2006), 2006.

[6] Reidemeister, T., Ward, P.A.S., Bohm, K., Buchmann, E., "Malicious Behaviour in Content-Addressable Peer-to-Peer Networks", 3rd Annual Conference on Communication Networks and Service Research, pp.319-326, May 2005.

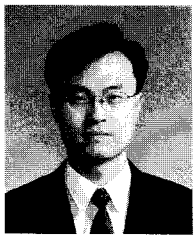
[7] Mudhakar Srivatsa and Ling Liu, "Vulnerabilities and Security Threats in Structured Overlay", Proceedings of the 20th Annual Computer Security Applications Conference (ACSAC'04), 2004.

[8] S.A.Baset and H.Schulzrinne, "An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol", Computer Science Department, Columbia University, Tech. Rep. CUCS-039-44, 2004.

[9] J.Risson and T.Moors, "Survey of research towards robust peer-to-peer networks: Search method", IRTF Internet Draft, draft-irtf-p2prg-survey-search-00.txt, Mar. 2006.

〈著者紹介〉

김 상 춘 (Sang Choon Kim) 종신회원
1986년 8월 : 한밭대학교 전자계산학과 공학사
1989년 2월 : 청주대학교 전자계산학과 석사
1999년 8월 : 충북대학교 전자계산학과 박사
1983년 4월~2001년 3월 : 한국전자통신연구원 정보보호연구본부(선임기술원)
2001년 7월~현재 : 전자통신연구원 정보보호연구본부 초빙연구원
2001년 4월~현재 : 강원대학교 정보통신공학과 부교수
<관심분야> 네트워크 보안, 소프트웨어공학



권 혁 찬 (Hyeok Chan Kwon)
1994년 2월 : 서원대학교 전자계산학과 공학사
1996년 2월 : 충남대학교 전산학과 석사
2001년 2월 : 충남대학교 컴퓨터과학과 박사
2001년 1월~현재 : 한국전자통신연구원 정보보호연구본부 선임연구원
<관심분야> IPTV 보안, P2P 보안, 네트워크 보안, MIPv6 보안

나 재 훈 (Jae Hoon Nah) 정회원
1985년 : 중앙대학교 컴퓨터공학과 공학사
1987년 : 중앙대학교 컴퓨터공학과 석사
2005년 : 한국외국어대학교 전자정보공학과 박사
1987년~현재 : 한국전자통신연구원 정보보호연구본부 팀장
<관심분야> IPTV 보안, IPv6/MIPv6 보안, P2P 보안