

# Peer-to-Peer 환경에서의 정보 공유를 위한 인증 메커니즘에 관한 연구

이정기\* · 배일호\* · 박찬모\* · 이준\*\*

\*조선대학교 컴퓨터공학과, \*\*조선대학교 컴퓨터공학부

## A Study on the Authentication Mechanism that Information Sharing in Peer-to-Peer Environment

Jeong-ki Lee\* · Il-ho Bae\* · Chan-mo Park\* · Joon Lee\*\*

\* Dept. of Computer Engineering, Chosun University.

\*\* School of Computer Engineering, Chosun University.

E-mail : sitdol@yahoo.co.kr

### 요 약

최근 클라이언트- 서버방식의 네트워크 서비스보다 P2P(Peer-to-Peer)서비스 환경이 더욱더 각광을 받고 있다. P2P는 자유로운 네트워크를 구성할 수 있고 중앙 서버 기능을 없애거나 약화시켜서 각 User 간에 참여할 수 있는 개방 네트워크이기 때문에 각 User 간에 인증에 관한 문제가 대두되고 있다. Network에 있는 어떤 사용자가 공개된 환경에 있다고 가정하면, 우리는 각 User간에 허가 받은 사용자에게만 접속을 제한하기 위해선 서비스에 대한 요구를 인증해 줄 수 있기를 바란다 본 논문에서는 이를 해결하기 위해 P2P환경에서 안전하게 정보공유를 할수 있는 메커니즘으로 kerberos인증 메커니즘을 인용하여 인증 메커니즘을 설계하고자 한다.

### ABSTRACT

P2P(Peer-to-Peer) can compose free network and take away center server function or problem about authentication is risen between each User because is opening network that can participate between each User weakening. We desire to authenticate request about service to user who is admitted between each user to limit connection. Wish to admit Kerberos authentication mechanism to mechanism that can do information sharing safety in P2P environment to solve this in this treatise and design authentication mechanism.

### 1. 서 론

P2P서비스가 기존 인터넷 비즈니스 모델과 차이점은 마케팅비용이 상대적으로 저렴하다는 것이다. 기존 B2C 모델의 경우 회원 확보를 위해 막대한 비용을 투자해야 했지만 P2P의 경우 사이트 개설 시 기호에 맞는 사용자들이 쉽게 접근할 수 있고 자연스럽게 고객을 확보할 수 있다는 장점이 있다. 하지만 문제점도 여겨져서 나오고 있다. 고객이 원하지 않는 정보유출이 문제인데 P2P서비스에서 보안문제는 매우 중요하다. 악의적인 또는 버그가 있는 피어 프로그램은 사용자의 하드디스크에서 정보를 수집하는 일종의 스파이 역할을 하게 될 위험이 있다는 것. 이러한 점 때문에

P2P서비스를 제공하는 업체는 보안에 중점을 두고 사용자의 신뢰성 문제에 대한 해결에 중심을 두어야 한다는 의견이 지배적이다.

P2P를 단순히 파일 공유 서비스로 생각하는 사람들이 많다. 하지만 실질적으로 P2P에서 중요한 것은 P2P가 갖고 있는 양방성의 네트워크 모델이다. 이런 네트워크 모델을 이용해 파일 공유 서비스 외에도 분산 컴퓨팅 혹은 분산 그룹웨어 와 e-커머스 같은 다양한 서비스에 이용할 수 있다. 하지만 P2P는 서버를 없애거나 약화시킴으로 인해 각 User 간에 인증에 관한 문제가 대두되고 있다. 이 때 발생할 수 있는 문제들로 방해, 가로채기, 불법수정, 위조 등이 있다. 이 경우들 중에서 어떤 것이든, 권한이 없는 사용자가 데이터 또

는 서비스를 액세스할 수 있다는 문제점이 있다

본 논문에서는 위와 같은 문제점들을 대처하는 방안 중 특히 사용자간의 인증에 대해 중점적으로 다루고자 한다. 이러한 문제를 해결할 수 있는 메커니즘으로 Kerberos를 도입해 사용자간의 인증 문제를 해결할 수 있는 메커니즘을 제안하여 P2P 환경에서 서로간의 자원을 안전하게 공유하며 사용자 욕구를 충족시키고 통신망의 사용자들과 원활한 통신을 할 수 있도록 한다.

## II. Peer-to-Peer 와 위협행위

### 2.1 Peer-to-Peer 개념

P2P(Peer-to-Peer) 컴퓨팅은 공동 파일 서버에 전적으로 의존하지 않으면서 각 PC 간의 직접적인 리소스 교환을 지원하는 Application 및 Network 솔루션으로 정의할 수 있다. 그러므로 모두 Client/Server 양쪽으로 활동할 수 있는 "Peer"가 되며 이는 다양한 신규 Application을 위한 기초가 될 뿐 아니라, 기존 인프라스트럭처에서 상당한 로드를 덜어냄으로써 값싸고 성능에 방해가 되는 업그레이드의 필요성을 줄일 수 있는 장점을 가지고 있다.

### 2.2 Peer-to-Peer의 특징

P2P는 클라이언트-서버 구조에서 서버가 아예 없어지거나, 클라이언트의 역할이 더욱 강화된다는 가장 본질적인 특징을 가진다.

P2P Application은 Network 인프라스트럭처를 위해 중앙화된 서버와 자동적으로 Link 하는 대신에, 필요한 리소스를 제공할 수 있는 가장 가까운 "Peer"를 검색한다. 그 결과 Network 상호작용의 평균거리가 크게 줄일 수 있으며 Network 전체의 트래픽 양을 줄여 준다.

P2P 컴퓨팅모델 하에서 정보는 서로 다른 많은 클라이언트 상에 있게 되므로 기존의 모델에 비해 매우 낮은 비용으로도 매우 높은 수준의 리던던시가 가능하다.

P2P Application은 배치된 Desktop의 관리성을 높이는데 사용할 수 있다. 기업 환경의 경우 PC에서 PC로 단계적으로 업데이트 하는 Software 분산과, 통합된 바이러스에 대한 보호를 제공할 수 있다.

이처럼 P2P는 서버의 최적화, 네트워크 최적화, 인프라스트럭처의 탄력성, 그리고 Desktop 관리성까지 여러 가지 특징을 가지고 있다.

### 2.2 위협행위

P2P환경에서는 몇 가지 복잡한 보안 문제가 제기

되고 있다. 사용자들은 네트워크를 통해 메시지를 송·수신하므로 정보보호기법이 필요하다.

이러한 컴퓨터 시스템 또는 네트워크에서의 보안공격의 유형은 정보 제공자로서의 컴퓨터의 기능을 살펴봄으로써 그 특성을 가장 잘 알 수 있다. 일반적으로 정보의 흐름은 파일이나 주기억장치의 한 부분과 같은 정보의 출처로부터 다른 파일이나 사용자와 같은 정보의 목적지로 이어지게 된다. 이와 같은 정상적인 정보의 흐름이 그림1(a)에 나타나 있다. 그림 1의 나머지 부분은 다음의 네 가지 공격의 범주를 보여주고 있다:

①방해(Interruption): 시스템의 일부가 파괴되거나 사용할 수 없게 되는 경우로서 가용성에 대한 공격이다. 예를 들면 하드디스크 같은 하드웨어의 일부가 파괴되거나, 통신회선이 절단되거나, 또는 파일 관리 시스템이 무력화되는 경우 등이다.

②가로채기(Interception): 비인가자들의 불법적인 접근에 의하여 발생하는 기밀성에 대한 공격으로서, 비인가자란 사람이나 프로그램 또는 컴퓨터일 수 있다. 네트워크 상에서 데이터를 가로채기 위한 도청과 파일 또는 프로그램의 불법 복제 등을 예로 들 수 있다.

③불법수정(Modification): 비인가자들의 불법접근 뿐만 아니라 불법적인 변경에 의한 무결성에 대한 공격으로서, 예를 들면 데이터 파일내의 값 변경, 프로그램의 다른 기능 수행을 위한 변조, 그리고 네트워크 상에서 전송중인 메시지 내용의 수정 등이 있다.

④위조(Fabrication): 비인가자들의 시스템에 대한 위조물 삽입에 의한 인증에 대한 공격으로서, 예를 들면 네트워크 상에 위조된 메시지를 삽입하거나 파일에 레코드를 추가하는 경우 등이 있다.

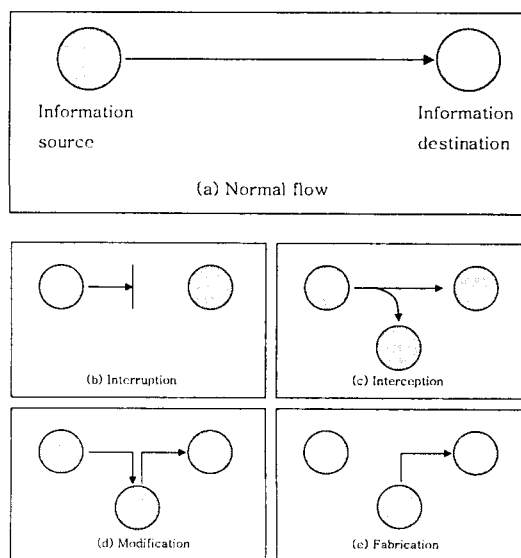


그림 1 보안에 대한 위협

### III. 인증 메커니즘

보호 장치가 없는 네트워크 환경에서는 모든 클라이언트는 서비스를 받기 위해 서비스를 제공하는 모든 서버로 접속할 수 있다. 침입자가 정당한 사용자로 위장한 후 침입하여 서버에 대한 허가받지 않은 권한을 가질 수 있는 보안상의 위험이 존재한다. 이런 위험을 막기 위해서 서버는 반드시 서비스를 요청하는 클라이언트의 신원을 확인할 수 있어야 한다. 각 서버가 각각의 클라이언트-서버의 대화에서 이러한 임무를 수행하기 위한 요구를 받을 수 있으나 실제로 이것은 각 서버에게 과도한 부하를 갖게 한다.

이를 해결하기 위한 대안은 모든 사용자의 패스워드를 알고 이것을 중앙집중식 데이터베이스에 저장하는 인증서버(AS: Authentication Server)를 사용하는 것이다. 부가적으로 Kerberos는 각 서버가 갖는 고유의 비밀 키를 공유한다. Kerberos를 통한 인증에는 3 단계가 있다. 첫 번째 단계에서 사용자는 자신이 정당한 사용자인지 인증을 받는다. 두 번째 단계에서는 사용자가 요청할 서비스를 제공하는 서버에 접근할 수 있는 인증서를 획득한다. 마지막 단계에서 목적 서버에게 인증서를 제공한다.

#### a. 인증서(Certificates)

Kerberos 인증 모델에서 사용되는 인증서에는 티켓(Ticket)과 인증자(Authenticator)의 두 가지 형태가 있다. 양쪽 모두 세션키를 사용하지만 서로 다른 키를 사용하여 암호화 된다. 티켓은 인증 서버와 목적 서버 사이에서, 티켓이 발행된 사용자의 신분 확인 통과를 엄격히 하는데 사용된다. 일단 티켓이 발행되면 티켓에 명시된 클라이언트와 서버 사이에서 클라이언트가 서버에 접속하기 위해 여러 번 사용될 수 있다. 티켓이 서버의 키로 암호화되었기 때문에 사용자가 티켓을 수정하는 것에 대한 걱정 없이 서버에게 티켓을 전송하기 위해 사용될 수 있다.

재사용할 수 있는 티켓과 달리, 인증자는 오직 한 번만 사용되고 매우 짧은 유효시간을 가지고 있다. 이 인증자는 티켓과 함께 클라이언트가 서버로 전송하는 것으로, 서버 측에서는 티켓의 내용과, 인증자를 비교하여 내용이 일치한다면 티켓을 보낸 사람이 이 티켓의 실제 소유주라는 것을 확신할 수 있다. 인증자는 서비스를 사용하기를 원하는 클라이언트가 매번 생성해야 하며 클라이언트 자신이 인증자를 만들기 때문에 문제를 일으키지 않는다. 그리고 인증자는 티켓의 부분이 되는 세션키로 암호화된다.

### IV. 인증 메커니즘 모델

서비스를 이용하기 위해 접속을 시도한 사용자가 있을 때 먼저 인증을 통해 연결이 이루어진다. 본 논문에서 제시한 P2P인증 메커니즘의 기본 구성은 TGS를 포함한 AS(인증센터)와 서비스 수신할 A client, 서비스를 사용할 B client 로 구성되어 있다. 이와 같이 구성된 인증 메커니즘 수행 절차 및 세부사항을 살펴보면 다음과 같다.

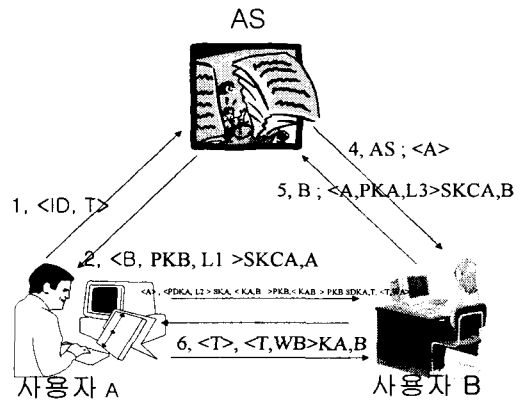


그림 3

메시지 1] client A가 client B와 안전한 연결을 설립하기 위해 AS에게 알림과 동시에 사용자 A의 이름, 사용할 서비스, 송신메시지 시간을 담고 있는 timestamp를 전송하여 공개키를 요청한다. AS는 서비스를 요청한 A가 정당한 사용자인지를 Database에서 검색하여 유효한 사용자인지 적법성을 검사한다.

[메시지 2] AS는 사용자 A를 인증한후 B의 공개키를 A가 신뢰하는 CA의 비밀키로 암호화 하여 보낸다.

[메시지 3] 사용자 A는 A와 B가 공유하는 세션키의 안전한 전송을 위해 공개 위임키를 자신의 비밀키로 암호화해서 보내며 또한 B의 공개키로 암호화된 세션키를 자신의비밀 위임키로 암호화해서 보낸다. 그리고 자신의 주소를 A,B의 세션키로 암호화하여 함께 보낸다.

[메시지 4] 사용자 B는 AS에게 A의 ID를 보내므로써 A의 공개키를 요청한다.

[메시지 5] AS는 사용자 B에게 A의 공개키를 B가 신뢰하는 CA의 비밀키로 암호화 하여 전송한다.(A와

의 부정한 연결을 시도에 이용하지 못하게 하기 위해서 사용자 B가 신뢰하는 키를 이용한다)

[메시지 6] 사용자 B는 자신의 주소를 A,B의 섹션 키로 암호화 하여 A에게 보낸다.

[메시지 7] 사용자 A는 자신의 공개키를 이용해서 섹션키 (KAB)를 찾아서 사용자 B에게 전송한다. (사용자 A가 사용자 B에게 자신을 보증하는 것이다.)

Addison Wesley, 1996

[7] W. ford. "Computer Communication Security". prentice Hall. 1995

[8] William Stalling. "Network and Internetwork Security". Prentice Hall. 1995.

## V. 결 론

P2P 환경에서 보안을 유지하는 방법들은 여러 가지가 있다. 그 목적도 다양하며 기본적인 기법들을 수정 및 추가하여 좀더 강화된 기법을 만들 수도 있다. 따라서 이러한 보안 메커니즘들은 보안을 유지하고자 하는 네트워크 상에서 수행되는 작업들과 자료의 성질 등에 따라서 적절한 방법이 선택되고 사용되어야 한다.

P2P상에서 파일공유, CPU공유, 전자상거래, 응용서비스등의 사용자 증가와 더불어 보안의 중요성이 확산됨에 따라 상호 인증 기술이 정보보호 기반기술의 중요요소로 대두되고 있다.

인증 메커니즘으로 관용 암호방식을 사용하는 Kerberos는 상호인증 알고리즘으로 손색이 없는 최적의 메커니즘을 갖는다.

본 논문에서는 다양한 자원들이 통신망에 연결되어 있는 p2p상에서 운영되는 통신망의 정보를 보호하고 정당한 사용자에게 자원을 안전하게 공유할수 있는 메커니즘으로 kerberos 인증 메커니즘을 바탕으로 p2p 환경에서 적절한 인증 메커니즘을 설계하였다.

## 참고문헌

- [1] 김문조(1998), 사회학회 공동세미나, 정보화시대의 매체정책과 문화정책, 언론학회
- [2] 박기홍 외(2000), [디지털 경제와 인터넷 혁명], 산업연구원
- [3] <http://www.openp2p.com/topics/p2p/security/>
- [4] <http://web-biz.pe.kr/web/p2p3.html>
- [5] RFC 1510, "The Kerberos Network Authentication Service(V5)," Internet Request for Comments 1510, Sep. 1993
- [6] Halsall, F. "Data Communications. Computer Networks and Open Systems," 4th Edition,