Kerberos를 이용한 P2P 보안 프로토콜 설계

*이 규 형(李 揆 炯), *송 영 상(宋 榮 祥), **우 찬 일(禹 讚 益), ***신 인 철(申 仁 澈)
*단국대학교 대학원 전자,컴퓨터공학과
**단국대학교 대학원 전자공학과
***단국대학교 전기,전자,컴퓨터공학부
전화 : (02) 709-2592 / 팩스 : (02) 709-2590
H.P 번호 : 011-257-3062

Design of P2P Secure Protocol Using Kerberos

*Kyu Hyung Lee, *Young Sang Song, **Chan Il Woo, ***In Chul Shin
*Dept. of Electronics and Computer Engineering, Dankook University, Seoul, Korea
**Dept. of Electronics Engineering, Dankook University, Seoul, Korea
***School of Electric, Electronics and Computer Engineering, Dankook University, Seoul, Korea
E-mail : podscat@dankook.ac.kr

Abstract

P2P implies direct exchange between peers. If you have something I want, I go directly to you and obtain it. There is one of the most advantages of formation of community in P2P. For a specified purpose through P2P, the peers who make temporary a group delivery a request efficient and safe. And the resources can be jointed common, cooperation and communication. When P2P is developed more, we can expect more formation of online community and development. But to be a safe of personal ID and password in internet, it should be possible to make a key-exchange.
In the paper, it suggest P2P security system suitable to personal security that Kerberos be transformed. The user who make community in P2P, have Kerberos Server, and using Physical Address of Ethernet card in personal computer, authenticate users.

I. 서론

최근 들어 정보 통신망이 확대 보급되고 컴퓨터 기술이 급속하게 발전됨에 따라 인터넷 등의 대중 네트워크를 통하여 언제 어디서나 원하는 자료를 주고받을 수 있는 환경으로 변하고 있다. 이에 따라 사용자간에 컴퓨터를 서로 연결하여 자료를 공유할 수 있는 Peer-to-Peer(P2P) 기술에 대한 연구가 활발하게 진행되고 있다.[1-3]

P2P 기술은 인터넷 상의 정보를 검색 엔진을 거쳐 찾아야 하는 기존의 방식과는 달리 인터넷에 연결된 모든 컴퓨터로부터 직접정보를 제공받을 수 있는 서비스로 웹사이트에 한정 되어있던 정보를 개인이나 기업에서 제공하는 데이터베이스로까지 확대할 수 있다.[4]

그러나, P2P 시스템은 다음과 같은 문제점을 나타내고 있다. 첫째, 넵스터(Napster), 소리바다와 같은 P2P 방식은 파일공유를 위하여 중재용 서버(브로커)를 두고 있어 서버운영자에 대하여 저작권 문제가 발생한다. 둘째, P2P 기술은 소스가 공개되어 대중적으로 사용할 수 있지만 해커에 의해 서버가 악의적인 목적으로 이용당할 수 있다. 셋째, 사용자들은 인터넷과 같은 대중 네트워크를 이용하기 때문에 공유되는 정보가 네트워크 상에 노출될 수 있다.[5-7]

따라서, 이러한 문제를 해결하기 위하여 정보 제공자와 사용자간에 서로 신뢰할 수 있는 인증 시스템을 필요로 한다. 그리고 공유되는 정보가 제3자에 의해 노출되는 문제를 해결할 수 있어야 한다. 본 논문에서는 사용자간에 파일 공유를 위하여 중재용 서버 없이 파일을 공유할 수 있는 방법을 Kerberos를 이용하여 제안한다.

II. Peer-to-Peer(P2P)

2-1. P2P의 개요

P2P는 크게 3가지 형태로 나눌 수 있다. 첫째는 브로커 중재형 파일 공유시스템으로 정보제공자는 브로커에게 공유할 파일을 등록하고, 브로커는 정보를 얻고자하는 사용자에게 파일이 어디에 있는지 알려주어 해당파일이 있는 컴퓨터로부터 사용자가 원하는 파일을 복사해 오게 된다. 이러한 방식을 사용하는 서비스는 넵스터와 소리바다 등이 있다. 두번째 방법은 그림 1과 같은 P2P 파일공유형 시스템으로 네트워크에 연결된 사용자들에게 자신이 갖고 있는 파일을 중간에서 중재해주는 브로커 없이 다른 사용자에게 직접 전달할 수 있다.

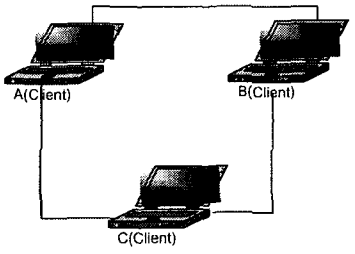

그림 1. P2P 파일공유형

세 번째 방법은 특정 컴퓨터에 처리 속도 향상을 위하여 네트워크에 연결된 각각의 컴퓨터에 일을 분담시켜 처리한 후 통합하는 것으로 이러한 형태의 P2P 모델을 Cycle Sharing이라고 한다.

2-2. P2P 보안

P2P 방법은 기본적으로 인터넷에 접속한 불특정 다수와 정보를 공유한다. 하지만 경우에 따라 보안이 필요한 공유를 하기 위하여 보안이 필요하다. 따라서 Peer-to-Peer Working Group의 Security Requirements Use-Cases White paper에서 "Security Requirements Document Version 0.9.2"를 권고하고 있으며 이 중 Peer-to-Peer Collaborative Apps는 "Security Requirements Document" 중 하나이며 그 권고사항은 1. Eavesdropping 2. Manipulation 3. Impersonation 4. Denial of service 등이 있다. 이를 해결하기 위한 보안 요구는 1. Identity 2. Authentication 3. Authorization 4. Secure Messaging 등이 있다.[8]

III. Kerberos

Kerberos는 MIT의 Athena 프로젝트의 일환으로 개발된 인증 서비스로 네트워크를 통해 연결된 특정 서버에 접속하려고 하는 공개된 환경에서 서버로부터 허가받은 사용자에게만 접속을 허가하고 서비스에 대한 요구를 수행하는 방법을 제공한다. 따라서 Kerberos는 네트워크 상에서 권한이 없는 사용자가 데이터 또는 서비스를 액세스할 수 없다.

3-1. Kerberos 프로토콜

Kerberos는 Kerberos Server와 티켓서버승인서버(Ticket Granting Server)와 인증서버(Authentication Server), 티켓(Ticket), 인증자(Authenticator)로 구성되어 있으며 Kerberos Server와 TGS가 Ticket을 생성하여 TGS와 서비스 Server와의 통신에 사용되며 Ticket의 구성정보는 Server와 Client 이름, 타임스탬프(TimeStamp), 유효시간(Lifetime), 세션키(Session Key)를 포함한다. 인증자는 Client에 의해 생성되고 생성된 인증자는 한번만 사용할 수 있으며 인증정보는 *Client의 이름과 웍크스테이션의 IP 주소, 현재의 시간*을 포함하고 있다.

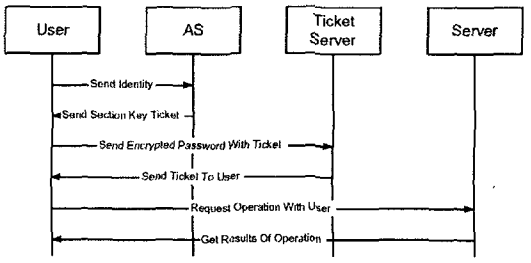

그림 2. Kerberos 프로토콜

그림 2는 Kerberos 프로토콜을 보여주고 있으며 Kerberos는 서버에 대한 사용자를 그리고 사용자에 대한 서버를 인증해 주는 기능을 갖는 중앙집중식 인증서버를 제공한다. Kerberos는 DES와 같은 비밀키 암호화 기법을 기반으로 수행되기 때문에 그 보안 정도가 매우 높으며 Ticket이라 불리는 암호화된 데이터를 이용하여 사용자를 인증하기 때문에 보안상으로 볼 때 좀 더 안전하게 통신할 수 있게 한다.

Client는 Ticket을 보관하여 서비스에 접속할 때마다 이 Ticket을 이용하여 TGS(티켓발행 서버)에게 접속하고 AS(인증서버)는 자신의 DB에 저장되어 있는 Client의 패스워드로 Client의 암호키(K_C)를 생성하여 Ticket(인증용으로 암호화된 데이터)을 발급한다. 패스

워드의 입력 시기는 Ticket이 도착한 후에 자신의 패스워드를 입력하여 키를 생성하고 Ticket을 복호화한다. 또한 Ticket의 가로채기를 봉쇄하기 위해 Ticket이 발행된 시간과 유효시간을 포함하고 있다. AS는 Client와 TGS간 그리고 Client와 Server간에 세션키 ($K_{C,TGS}$, $K_{C,V}$)를 제공하여 제한된 유효시간 안에 신원을 확인시켜 준다. 또한 가로채기의 위험을 방지하기 위하여 Client의 인증자($Authenticator_C$)를 사용하고 있다.[9-12]

Kerberos 프로토콜은 다음과 같다.

① C -> AS : $ID_C || ID_{tgs} || TS_1$

② AS -> C : $E_{K_c}[K_{C,tgs} || ID_{tgs} || TS_2 || Lifetime_2 || Ticket_{tgs}]$

$Ticket_{tgs} = E_{K_{tgs}}[K_{C,tgs} || ID_C || AD_C || ID_{tgs} || TS_2 || Lifetime_2]$

③ C -> TGS : $ID_V || Ticket_{tgs} || Authenticator_C$

④ TGS -> C : $E_{K_{C,tgs}}[K_{C,V} || ID_V || TS_4 || Lifetime_2]$

$Ticket_{tgs} = E_{K_{tgs}}[K_{C,tgs} || ID_C || AD_C || ID_{tgs} || TS_2 || Lifetime_2]$

$Ticket_V = E_{K_V}[K_{C,V} || ID_C || AD_C || ID_V || TS_4 || Lifetime_4]$

$Authenticator_C = E_{K_{C,tgs}}[ID_C || AD_C || TS_3]$

⑤ C -> V : $Ticket_V || Authenticator_C$

⑥ V -> C : $K_{C,V}[TS_5 + 1]$

$Ticket_V = E_{K_V}[K_{C,V} || ID_C || AD_C || ID_V || TS_4 || Lifetime_4]$

$Authenticator_C = E_{K_{C,tgs}}[ID_C || AD_C || TS_5]$

Ⅳ. Kerberos를 이용한 제안 P2P 방법

네트워크를 통한 개인 사용들은 유동 IP와 IP 공유라는 방식을 사용하고 있어 IP 정보는 고정 IP를 쓰는 사람 이외에는 믿을 수 있는 정보라 할 수 없다. 따라서 Kerberos에서 사용하는 Ticket 정보 중 하나인 AD(Client의 IP Address) 정보로는 사용자 인증을 할 수가 없다. 따라서 본 논문에서는 IP와 이더넷 카드에 있는 고유한 시리얼 번호인 MAC Address를 이용하여 사용자를 인증하고 P2P 주체가 되는 컴퓨터를 Kerberos 서버로 사용하여 인증하고 정보를 암호화하여 안전하게 공유할 수 있는 방법을 제안하며, 제안 방법에서는 정보를 제공하는 모든 사용자가 서버가 될 수 있다.

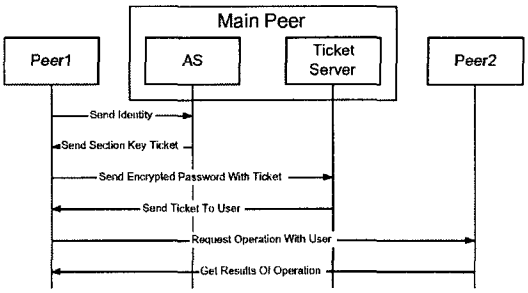

그림 3. 제안된 P2P 환경의 Kerberos 프로토콜

본 논문에서 제안한 P2P 방법은 그림 3과 같이 자료요청 사용자(Peer1), AS, Ticket Server, 정보제공 사용자(Peer2)로 구성되고 사용자들 중 중심이 되는 사용자가 AS와 Ticket Server가 된다.

그림 3에서와 같이 Main Peer는 Peer2와 이미 인증되어 있다고 가정하고 Ticket의 움직임을 중점으로 새로운 Peer인 Peer1가 Peer2와 공유하기 위해 다음과 같은 프로토콜을 설명한다. 또한 Peer1은 Main Peer에게 MAC Address를 전송하고 Main Peer는 Peer1에게 공유할 수 있는 키를 전송한다.

$E_{K_{Peer1}}[K_{Peer1,MainPeer} || ID_{MainPeer(TGS)} || TS_2 || Lifetime_2 || Ticket_{MainPeer(TGS)}]$

$Ticket_{MainPeer(TGS)} = E_{K_{MainPeer(TGS)}}[K_{Peer1,MainPeer(TGS)} || ID_{Peer1} || AD_{Peer1}' || ID_{MainPeer(TGS)} || TS_2 || Lifetime_2]$

Peer1은 상호간에 공유된 키를 사용하여 Section Key Ticket을 복호화하여 $Ticket_{MainPeer(TGS)}$를 추출하고 $Ticket_{MainPeer(TGS)}$를 공유키로 암호화한 후 Main Peer에게 전송한다. Main Peer는 Peer1에게 Peer2와 자료공유를 할 수 있는 Ticket을 발행한다.

$Ticket_{Peer2} = E_{K_{Peer2}}[K_{Peer1,Peer2} || ID_{Peer1} || AD_{Peer1}' || ID_{Peer2} || TS_4 || Lifetime_4]$

AD_{Peer1}' : MAC Address

Peer1은 받은 티켓을 Peer2에게 보내고 Peer2는 받은 티켓을 사용하여 Peer1에게 공유할 수 있는 ID와 공유 패스워드를 인증한다.

표 1. 기존 P2P 방법과 제안 P2P 방법 비교

	브록커 중재형 P2P	제안된 P2P
데이터 보안	없음	있음
인증방법	ID, Password	MAC Address, ID, Password
신뢰성	없음	보장
키관리	인증서버	사용자들

V. 결론 및 추후 연구

본 논문에서는 파일 공유 시스템(브로커 없는 P2P) P2P 환경에서의 보안성을 높이기 위해 비밀키 인증방식인 Kerberos를 이용하여 키를 분배한 후 사용자를 인증하는 방법을 제안하였다. 본 논문에서 제안한 파일 공유형 P2P는 자료를 원하는 사용자, 자료를 제공하기 위한 사용자로 구성되어 있다. 또한 P2P 환경에 적용하기 위하여 두사람 이상이 인증된 그룹에 중심이 되는 사용자를 AS와 Ticket Server로 사용하고 파일 공유를 원하는 임의의 사용자들을 인증할 수 있도록 설계하였다. 그리고 사용자 인증을 위하여 Ethernet Card의 고유번호인 MAC Address를 사용하였다. 제한 방법은 Peer-to-Peer Working Group에서 권고한 보안 정도 중 Peer-to-Peer Collaborative Apps 위협되는 사항에 충족된다.

향후에는 해킹 기술의 발달로 더욱 안정적인 인증 서비스를 위해 개인이 사용하는 패스워드의 관리를 위하여 강화되어야 한다. 이를 위해 SmartCard나 PDA 등을 이용하여 관리할 수 있는 개발이 필요하다.

참고문헌

[1] Dana Moore, John Hebeler, " PEER-TO-PEER", McGrawHill, 2002

[2] Dreamtech Software Team, "Peer-to-Peer Application Development", Hungry Minds, 2002

[3] Sing Li, "JXTA Peer-to-Peer Computing with Java", WROX, 2001

[4] www.networkmagazine.com/article /NMG20020206S0005

[5] www.nwfusion.com/newsletters/sec/2000 /0828sec1.html?nf

[6] www.guntellanews.com/information /firewalls.shtml

[7] www.plus.or.kr/book/SecurityPLUS-1st /node199.html

[8] Andrew A. Chien, Editor Nov 27, 2001 Version 0.9.2 PEER-TO-PEER WORKING GROUP, "SECURITY REQUIREMENTS DOCUMNET"

[9] Athena Technical Plan, Section E.2.1 27 Oct 1988 "Kerberos Authentication and Authorization System"

[10] 윤재우, 이승형, 정보보호학회지, 제11권 제6호 2001. 12 pp.53-62 "IP 기반 VPN 프로토콜의 연구동향 : 확장성과 보안성"

[11] 장청룡 외 4, 정보보호학회지, 제11권 제6호 2001. 12, pp.12-23, "블록암호 표준화 동향"

[12] 신광철, 정진욱, 정보보호학회지, 제12권 제2호, 2002. 4, pp.123-133, "네트웍 환경에서 안전한 Kerberos 인증 매커니즘에 관한 연구"