P2P 환경에서 SPKI 인증서를 이용한 접근 제어

신 정 화† · 이 영 경† · 이 경 현††

요 약

P2P 서비스는 서버를 거치지 않고 관련 프로그램만으로 연결된 사용자들끼리 서로의 정보를 공유할 수 있는 기술로 인터넷에 연결된 모든 개인 컴퓨터들이 서버 또는 클라이언트로 동작하면서 직접적인 연결을 통해 정보나 서비스를 제공받거나 공유하는 것이 가능하다. 현재, P2P 서비스는 모든 사용자에 대해 동등한 접근 권한을 부여하여 서로의 자원을 공유할 수 있도록 하고 있다. 이러한 상황에서는 인터넷을 통한 다양한 공격에 따른 취약성이 예상되므로 보다 양질의 보안 서비스가 필요하다. 따라서, 본 논문에서는 자원 공유를 위해 연결을 요청하는 사용자들에게 "SPKI(Simple Public Key Infrastructure) 인증서"를 발행하여 접근 권한을 지정하고, 정보 요청자는 자신에게 주어진 접근 권한에 따라 제한적으로 정보 제공자의 자원을 사용할 수 있는 방안을 제안한다.

An Access Control using SPKI Certificate in Peer-to-Peer Environment

Jung-Hwa Shin† · Young-Kyung Lee† · Kyung-Hyune Rhee††

ABSTRACT

The P2P service is a technology that can share their information with each other who is able to be connected with a relating program without passing by a server. Since all personal computers that linked to the Internet under the P2P service can operate as a server or a client, they can provide and share both their information and services through the direct connection. Currently, the P2P service is giving an equal privilege to all users for sharing their resources. Under this situation, a lot of vulnerability against the various attacks through the Internet is possible, more sophisticated security services are necessary. In this paper, we propose an access control scheme using SPKI (Simple Public Key Infrastructure). The scheme designates an access control by providing the certificate to users who request a connection for resource sharing and limits the resource usage of information provider according to the access right that is given to their own rights.

키워드 : P2P(Peer-to-Peer), 접근제어(Access Control), SPKI(Simple Public Key Infrastructure)

1. 서 론

네트워크 환경의 급속한 발전으로 인터넷 사용량이 증가하고 인터넷 이용자들이 필요로 하는 자료의 양이 증가하면서 특정 정보를 얻기 위한 정보 검색 작업은 인터넷 상에서 가장 빈번하게 사용되고 있는 서비스중의 하나가 되었다. 지금까지 네트워크 환경에서 자료 저장과 관리를 위해 가장 널리 사용되어 온 "클라이언트-서버" 모델은 클라이언트가 서버에게 특정 기능을 요청하면 서버가 그에 맞는 동작을 수행하여 클라이언트에게 제공하는 방식으로 서버가 담당하게 되는 작업의 양이 상대적으로 많아져 서버의 부하가 심해지는 단점을 가지고 있다. "클라이언트-서버" 모델이 가진 단점을 해결하기 위한 방안으로 새롭게 등장한 P2P(Peer-to-Peer) 서비스는 네트워크에 연결된 모든 컴퓨터가 동등한 권한과 책임을 가지고 동작하는 형태로 신속한 정보 교환과 비용 절감, 통신 대역폭의 효율적인 사용과 효율적인 자원 관리 차원에서 "클라이언트-클라이언트" 모델이라 할 수 있다[1].

P2P 서비스는 인터넷상의 정보를 찾기 위해 기존의 서버를 거쳐야 하는 방식과 달리 인터넷에 연결된 모든 개인 컴퓨터로부터 직접 어떤 정보나 서비스를 제공받고 공유하는 방식으로 사용자들의 컴퓨터는 서버와 클라이언트 기능을 모두 가지고 동작하기 때문에 집중된 서버의 처리를 각각의 클라이언트들이 나누어 수행하게 되므로 클라이언트의 수가 증가할수록 많아지는 서버의 처리 용량과 통신 대역폭에 대한 제한점을 해결해 주는 네트워크 상호작용을 대칭적으로 만드는 컴퓨팅 방식이다. 초기의 P2P 서비스는 파일 공유를 위한 서비스로 인기를 끌었지만 이외에도 분산 컴퓨팅, 전자상거래, 협업 시스템 등과 같은 기존의 중앙 집중식 시스템을 상대로 발전하고 있다[2, 3].

P2P 서비스에 있어 통신이 가능한 모든 정보 단말기를 "피어(peer)"라고 하며, 기존의 네트워크 모델에서 단순히 클라이언트로 동작하던 개인용 PC, 모바일 단말기(휴대폰, PDA), 혹은 통신이 가능한 가전 제품도 모두 하나의 "피어"로 볼

† 준 회 원 : 부경대학교 대학원 전자계산학과
†† 종신회원 : 부경대학교 전자컴퓨터정보통신공학부 교수
논문접수 : 2003년 7월 22일, 심사완료 : 2003년 10월 2일

수 있다[4].

한편, P2P 서비스에서는 모든 피어들이 서비스를 제공하거나 받을 수 있으므로 의도적이거나 고의적인 공격자에 의한 공격에 상당히 노출되어 있고, 트로이 목마와 같은 악의적인 소프트웨어를 적은 비용으로 손쉽게 확산할 수 있다. 그러므로, P2P 서비스에서는 피어 간에 전송하는 정보에 대하여 기밀성과 무결성이 요구되고, 자원을 공유하는 피어들에 대한 인증 및 특정 피어의 자원에 대한 접근 제어 등 여러 가지 보안 서비스를 필요로 한다. 이에, 본 논문에서는 익명 인증서(anonymous certificate)를 발행하여 서비스에 참여하는 피어들을 인증한 후 공유 자원을 가진 피어에 연결을 요청하는 피어들에게 요청 피어가 얻은 평판 값을 기반으로 "SPKI(Simple Public Key Infrastructure) 인증서"를 발행하여 피어마다 접근 권한을 설정하고, 설정된 권한에 따라 정보 제공 피어의 자원을 사용하는 방안을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구로 P2P 서비스 개념과 모델, SPKI 인증서에 대해 살펴보고, 3장에서는 P2P 서비스에서 각 피어들로부터 받은 "평판"을 기반으로 "SPKI 인증서"를 발행하여 각 피어의 공유 자원에 대한 접근을 제어할 수 있는 방안을 제안한다. 마지막으로, 4장에서는 결론 및 향후 연구 방향을 서술한다.

2. 관련 연구

2.1 P2P 서비스

P2P 서비스는 각 컴퓨터가 동등한 책임과 권한을 가지고 통신을 수행하는 방식으로 기존의 특정 컴퓨터가 다른 컴퓨터들에게 서비스를 제공하는 "클라이언트-서버" 구조와는 달리 "클라이언트-클라이언트" 구조로 서버를 통한 정보의 공유가 아닌 "피어"간의 정보 교환 및 공유가 가능한 서비스이다. P2P에서는 각 피어들이 프로세싱 파워, 저장 공간, 컨텐츠 등의 하드웨어 자원들의 일부를 공유하는 것을 가능하게 한다. 즉, P2P란 인터넷상의 정보를 찾기 위해 검색 엔진을 거쳐야 하는 기존 방식과 달리 인터넷에 연결된 모든 개인 컴퓨터로부터 직접 정보나 서비스를 제공받고 검색은 물론 다운로드 받을 수 있는 서비스로 기존의 웹사이트에 한정되어 있던 정보 추출 경로를 개인이나 회사가 운영하는 데이터베이스까지 확대하여 정보 공유가 가능하다. P2P 서비스는 각종 멀티미디어 파일 전송, 인터넷 컨텐츠 검색과 활용, 협업을 위한 업무용 도구, 인터넷 쇼핑 및 경매 서비스 등과 같은 멀티미디어 환경에서 널리 사용될 수 있다[4].

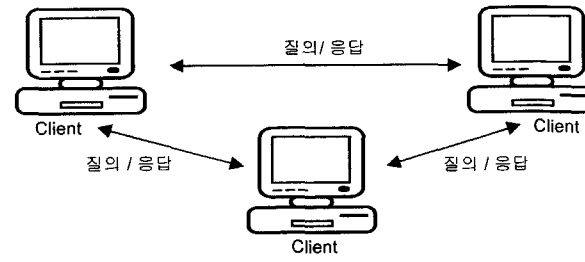
P2P 서비스 이용에 있어 장점은 다음과 같다. 기존의 인터넷 서비스는 서버에 문제가 생길 경우 모든 사용자의 서비스가 중단되는 반면, P2P 서비스는 특정 서버에 문제가 생기더라도 모든 사용자에게 서비스가 중단되는 경우는 발생하지 않으며, 또한 네트워크에 연결되어 있는 여러 사용자들이 가진 정보에 대하여 손쉬운 공유가 가능하다. 한편, 피어 프로그램의 유지 보수 부담이 있고, 시스템 운영의 안정성과 신뢰도 문제, 그리고 개방되고 분산되어 있는 만큼 P2P 작업을 수행하는 사용자들의 책임성이 요구된다. 또한, 서버의 기능이 배제될수록 시스템의 성능은 더욱 저하될 수 있으며, P2P 서비스를 이용하는 참여자가 항상 온라인 상태로 유지되어야 하고, 악의적인 소프트웨어의 손쉬운 분배로 인하여 보안 문제를 야기 시키는 단점이 있다.

P2P 서비스를 제공하는 모델은 다음과 같이 분류된다[5].

- 순수 P2P
- 간단한 조회 기능 서버를 가진 P2P
- 조회 서버와 룩업 서버를 가진 P2P
- 조회/룩업/컨텐츠 제공 기능의 서버를 가진 P2P

2.1.1 순수 P2P

순수 P2P 모델은 중앙 서버가 존재하지 않는 모델로 사용자의 컴퓨터가 서버 또는 클라이언트로 동작하는 모델이다. P2P 애플리케이션이 클라이언트로 다운로드 되면, 네트워크에 연결된 피어들은 네트워크에 접속된 다른 피어들을 동적으로 찾아 파일을 업로드/다운로드 할 수 있다. 그러나, 필요한 정보 검색을 위해 각 피어가 서로에게 질의를 보내는 동작이 중복해서 발생하므로 병목 현상이 생길 수 있고, 질의에 대해 시스템 전체를 검색해야 하므로 전체 대역폭을 증가시킬 뿐만 아니라 질의를 수행하는 시간이 오래 걸린다. 또한, 특정 피어가 보낸 검색 패킷에 대한 수명을 TTL (Time to Live) 값으로 관리하므로, 맡은 임무를 수행한 후에도 네트워크 상에 돌아다니는 패킷이 많아져 네트워크 전체에 오버헤드를 일으킬 수 있다. 그러므로, 신뢰성, 속도, 검색 능력은 감소하면서 네트워크 트래픽은 증가하게 되고, 네트워크를 안전하게 관리할 책임을 가진 관리자가 없으므로 네트워크의 관리나 컨텐츠의 관리가 되지 않는 있다. (그림 1)은 순수 P2P 모델의 동작 방식을 나타내고 있다.

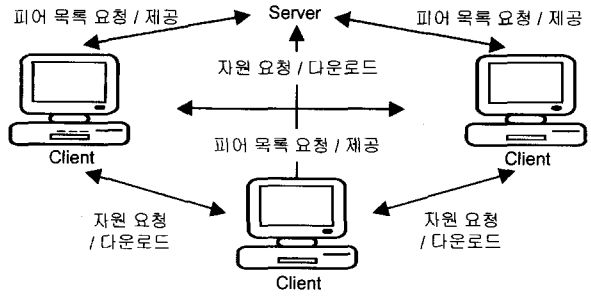


(그림 1) 순수 P2P 모델

2.1.2 간단한 조회 기능 서버를 가진 P2P

실제로 서버를 포함하고 있는 것은 아니지만 최소한의 관리를 위하여 서버의 역할이 포함되어 있는 모델로, 서버는 P2P 서비스 이용을 위해 접속하는 피어들에게 이미 접속되어 있는 피어들의 이름만 제공하고, 필요로 하는 파일에 대한 다운로드 등과 같은 작업은 각각의 피어들이 직접적으로 수행한다. 이 모델은 서버가 이미 접속되어 있는 피어들의 목록을 제공하므로 많은 수의 피어들을 손쉽게 검색할 수 있는 이점을 가지는 반면, 특정 자원에 대한 다운로

드를 위해 피어들은 현재 연결되어 있는 각 피어들에게 개별적으로 연결하여 다운로드 요청을 보내게 되므로 요청에 대한 처리 시간이 길어지기도 한다. (그림 2)는 간단한 조회 기능을 가진 P2P 모델을 나타내고 있다.

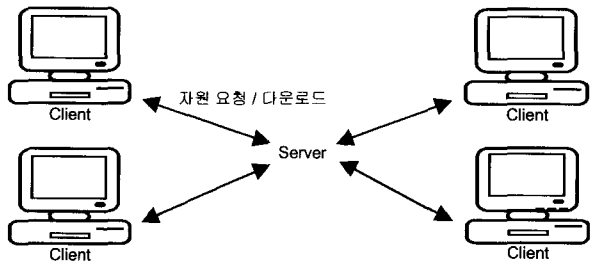


(그림 2) 간단한 조회 기능 서버를 가진 P2P

2.1.3 조회 서버와 룩업 서버를 가진 P2P

순수 P2P 모델과 간단한 조회 서버를 가진 P2P 모델의 특징을 통합한 모델로 서버는 현재 접속되어 있는 피어 목록과 접속된 각 피어들이 제공하는 공유 자원 목록을 함께 제공한다. 각 피어들은 서버를 통해 필요로 하는 자원을 소유한 피어를 확인한 후 해당 피어로 연결을 요청하여 직접 다운로드를 받을 수 있다.

2.1.4 조회/룩업/컨텐츠 제공 기능의 서버를 가진 P2P



(그림 3) 조회/룩업/컨텐츠 서버를 가지고 있는 P2P

기존의 클라이언트/서버 모델에서처럼 서버가 모든 것을 관리하는 모델로 피어들의 요청은 모두 서버로 전달되고, 서버의 데이터베이스에 피어들이 가진 모든 자원이 저장되어 있기 때문에, 피어들 간의 직접적인 연결은 허용하지 않고 모든 작업은 서버를 통해 이루어진다. 그러므로, 동시에 많은 요청이 있을 경우 서버의 처리 속도가 느려지고, 서버가 데이터를 관리, 저장하고 모든 요청에 대한 처리를 수행하기 때문에 비용이 늘어나는 단점이 있다. (그림 3)은 조회/룩업/컨텐츠 서버를 가지고 있는 P2P 모델의 동작 방식을 나타내고 있다.

2.2 SPKI(Simple Public Key Infrastructure)

SPKI 인증서는 공개키 인증서를 위하여 제안된 표준으로 사용자의 권한(authority)을 사용자의 ID가 아닌 공개키와 바인딩(binding)하여 접근 제어를 제공하기 위한 목적으로 사용가능한 인증서로 "권한 인증서(authorization certificate)"라고도 한다[6]. SPKI 인증서는 서버에 의해 발행되고 클라이언트가 소유하고 있다가 서버가 제공하는 자원에 대한 사용을 원할 경우 서버로부터 발급 받은 SPKI 인증서를 제출함으로써 서버가 지정한 접근 권한에 따라 제한적으로 서버의 자원을 사용할 수 있게 된다. 또한, SPKI 인증서는 인증서 발급시 사용자의 ID가 아닌 사용자의 공개키나 공개키의 해쉬값을 사용하여 Issuer와 Subject를 나타내므로 사용자에 대한 익명성을 유지할 수 있고, 서버 데이터베이스의 수정 없이 발급 받은 인증서를 다른 Subject에게 쉽게 위임 가능하다. 이는 특정 서비스에 대해 독립적이며 인증서 발행과 관리가 쉬우므로 유지 보수 가격이 저렴한 특징을 가진다[6, 7].

SPKI 인증서는 사용에 있어 다음의 요구 사항을 가진다[6]. 첫째, 인증서의 생성이 자유로워야 하고, 다른 사용자에게 접근 권한을 위임할 수 있으며, 중앙기관이나 등록된 엔티티만 인증서를 생성할 수 있는 것이 아니라, 누구든지 다른 사람의 허가 없이 자유롭게 인증서를 발행할 수 있다. 둘째, 모든 사용자는 인증서 발행자로부터 받은 권한을 위임할 수 있다. 셋째, 권한은 사용하는 응용 분야에 따라 자유롭게 지정하고 분배할 수 있다. 넷째, 인증서의 유효 기간을 명확하게 지정해야 한다. 다섯째, 사용자의 이름 대신 공개키를 사용한다.

이러한 특징과 요구 사항을 가지는 SPKI 인증서는 기존의 공개키 인증서와 달리 인증서 구성 형식에 <delegation> 필드와 <authorization> 필드가 존재한다. <delegation> 필드는 발행된 인증서에 명시된 접근 권한에 대한 위임 여부를 설정하는 필드이고, <authorization> 필드는 인증서를 발행한 서버의 자원에 대하여 가질 수 있는 접근 권한을 설정하는 필드이다.

SPKI 인증서는 다음의 다섯 개의 필드를 포함하는 Issuer의 개인키로 서명된 메시지이다[6-8].

< *Issuer*, *Subject*, *Delegation*, *Authorization*, *Validity* >

- *Issuer* : 인증서를 생성하거나 인증서에 서명한 인증서 발행자를 표시하는 필드로 Issuer의 공개키나 공개키의 해쉬값으로 나타낸다.
- *Subject* : 인증서에 주어진 권한을 받는 사용자를 표시하는 필드로 Subject의 공개키나 공개키의 해쉬값으로 나타낸다.
- *Delegation* : Issuer가 Subject에게 부여한 권한을 위임할 수 있는지를 표시하는 필드로 "True"나 "False"로 표현한다. True로 지정할 경우 Issuer는 Subject에게 위임 권한을 주고, Subject는 자신의 인증서를 재위임 할 수 있다. 이때, Subject는 자신이 Issuer로부터 받은 권한과 동일하거나 적은 권한으로만 위임 가능하다.
- *Authorization(access rights)* : 인증서를 발급 받는 Subject에게 권한을 지정하는 필드로 Issuer가 Subject를 위해 인증서에 서명할 때는 반드시 Subject가 가질 수 있는 권한을 지정해야 한다. 권한은 사용하는 응용 분야에 따

라 Issuer가 자유롭게 지정할 수 있다.

- *Validity* : 인증서의 유효기간을 명시한다. 유효 기간은 Issuer의 개인키 노출이나 분실이 발생할 경우를 대비하여 짧게 지정하는 것이 좋다.

발행된 인증서의 예는 다음과 같다.

$$<P(I),\ P(S),\ TRUE,\ read\,(7/May/2003)>_{S(I)}$$

- $P(I)$: Issuer의 공개키 또는 공개키의 해쉬값
- $P(S)$: Subject의 공개키 또는 공개키의 해쉬값
- *True* : delegation이 가능함을 나타낸다.
- *read* : Issuer가 가진 자원에 대해 "read"가 가능함을 나타낸다.
- *7/May/2003* : 인증서 유효기간을 나타낸다.
- $S(I)$: Issuer의 개인키

3. P2P 환경에서 SPKI 인증서를 이용한 접근제어

본 논문에서는 P2P 모델 중 조회 서버와 룩업 서버를 가진 P2P 모델에 기반을 두고 각 피어가 제공하는 공유 자원에 대한 신뢰도를 공유 자원을 사용한 피어들로부터 얻은 다음, 이를 사용하여 접근 제어를 위한 "SPKI" 인증서를 발행하여 피어들의 자원 사용을 제한하고자 한다.

3.1 제안 방안

P2P 서비스에서는 피어간 직접적인 자원 교환이 가능하므로 의도적이거나 고의적인 공격자에 의하여 신뢰할 수 없는 자원에 대한 분배가 손쉽게 이루어질 수 있다. 그러므로, 서비스에 참여하는 피어들에 대한 인증이나 피어 간에 교환하는 자원에 대하여 기밀성, 무결성과 같은 보안 서비스를 필요로 하고, 자원을 요청하는 피어들이 공유 자원에 대해 무엇을 할 수 있는지와 할 수 없는지 등의 접근 권한을 설정하여 서비스에 참여하는 피어들에 대한 접근을 제한할 수 있는 방법을 필요로 한다.

이에, 본 논문에서는 서비스에 참여하는 모든 피어 들에 익명 인증서(anonymous certificate)[9]를 발행하여 필요한 자원을 얻기 위해 특정 피어에 연결을 요청할 때 연결을 요청한 피어에 대한 인증이 가능하도록 한다. 또, 서버가 지정한 SIA(SPKI Issuing Agent)에 의해 자원을 요청한 피어는 자신이 제공한 공유 자원을 사용한 피어들로부터 받은 평판 값(신뢰 정보)에 따라 SPKI 인증서를 발급 받아 자원 요청시 이 인증서를 제출하여 자신에게 부여된 접근 권한에 따라 공유 자원을 사용하도록 한다. 평판 값은 SIA가 관리하므로 자원을 요청한 피어는 자신이 어떤 평판 값을 받았는지 알 수 없으며, 익명 인증서의 사용으로 자신에게 평판을 한 피어가 누구인지도 알 수 없다.

SIA가 피어들에게 SPKI 인증서 발행시 접근 권한을 지정하는 기준은 특정 피어에 연결하여 자원을 다운로드 하여 실행한 후 자신이 목적으로 한 자원이 맞는지 여부에 따라 SIA에게 해당 자원을 제공한 피어에 대한 평판 값(자원 제공 피어의 ID, success 또는 fail)을 전송하고, SIA는 이와 같은 평판 값을 기반으로 각 피어 들에게 접근 권한을 명시한 SPKI 인증서를 발행한다.

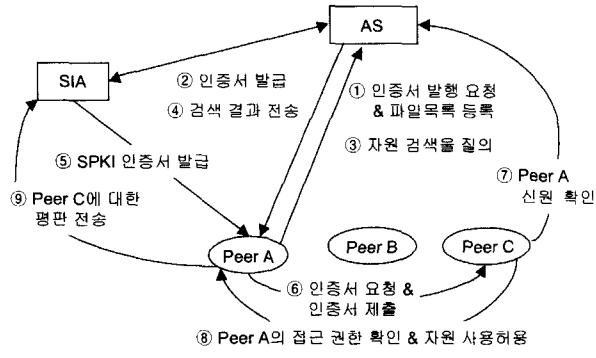
제안 방안에서 사용되는 익명 인증서와 SPKI 인증서의 유효 기간은 피어가 서버에 로그인하여 작업하는 동안으로 제한하고, 로그오프 후 다시 로그인할 경우는 새로 발급 받는 것으로 한다.

3.2 제안 방안의 동작 방식

제안 방안에서 사용되는 표기법은 <표 1>에 주어졌고, 동작 방식은 크게 4단계로 다음과 같다.

〈표 1〉 표기법

표 기	설 명
AS	익명 인증서를 발행하고 공유 파일 목록을 관리하는 서버
SIA	각 피어들로부터 받은 평판 값을 기반으로 SPKI 인증서를 발행하는 에이전트
Sid	서버의 identity
Sig_S	익명 인증서 발행시 사용되는 서버의 서명값
v_p	피어의 공개키
s_p	피어의 개인키
ID_p	피어의 identity
AC_S	서버가 발행한 익명 인증서
success	좋은 평판을 받은 횟수
fail	나쁜 평판을 받은 횟수



(그림 4) 제안 방안의 전체 동작 방식

3.2.1 초기화 단계

① *Peer* → *AS* : 로그인, 인증서 발급 요청, 자원 목록 등록

P2P 서비스에 참여하는 모든 피어들은 중앙 서버에 로그인하여 익명 인증서(anonymous certificate)를 발급 받고, 자신이 가진 자원 중 공유하고자하는 자원 목록을 서버에 등록한다.

익명 인증서의 발급 과정은 다음과 같다.

- *Peer A* : (v_{IDA}, S_{IDA}) 생성

서비스에 참여하는 각 피어들은 익명 인증서를 발급 받기 위하여 자신의 공개키(v_{ID_A})와 개인키(s_{ID_A})쌍을 생성한다.

• *Peer A* → *AS* : *request*(v_{IDA}, ID_A)

키 쌍 생성 후 각 피어는 자신이 생성한 공개키(v_{ID_A})와 자신의 identity(ID_A)를 서버로 전송하여 인증서 발급을 요청한다.

• *AS* : $Sig_S(v_{ID_A}, S_{id})$

서버는 인증서 발급을 요청한 피어에 대한 신원 확인 후 피어의 공개키 v_{ID_A}와 서버의 신원, 유효 기간 등을 나타내는 정보 S_{id}를 사용하여 서명값 $Sig_S(v_{ID_A}, S_{id})$를 생성한다.

• *AS* → *Peer A* : AC_S 전송

서명 생성 후 서버는 인증서 발급을 요청한 피어에게 피어의 공개키 v_{ID_A}, 서버의 정보 S_{id}, 서명값 $Sig_S(v_{ID_A}, S_{id})$를 포함하는 익명 인증서 $AC_S(v_{ID_A}) = (v_{ID_A}, S_{id}, Sig_S(v_{ID_A}, S_{id}))$를 전송한다.

• 서비스에 참여하는 피어들은 필요로 하는 자원을 가진 피어에 연결 요청시 서버로부터 발급 받은 인증서를 제출하여 인증을 거친 후 해당 자원에 대한 접근이 가능하다.

3.2.2 검색 단계

① *Peer A* → *AS* : *Request*

*Peer A*는 필요로 하는 자원 검색을 위해 서버에 질의한다.

② *AS* → *Peer A* : 피어 목록 전송

SIA → *Peer A* : SPKI 인증서 발행

서버는 *Peer A*가 요청한 질의에 일치하는 자원을 가진 피어 목록을 전송하고, SIA에게 요청하여 SIA가 가지고 있는 *Peer A*의 평판 값 중 "success" 값을 기반으로 접근 권한을 지정한 SPKI 인증서를 발행한다. SIA는 다음 형식으로 평판 값에 대한 정보를 유지한다.

$$<ID_P, success, fail>$$

• ID_P : 자원을 이용한 피어들로부터 평판을 받은 자원 제공 피어의 ID

• *success* : ID_P가 제공한 자원에 대하여 자원 이용 피어로부터 좋은 평판을 받은 횟수

• *fail* : ID_P가 제공한 자원에 대하여 자원 이용 피어로부터 나쁜 평판을 받은 횟수

SIA가 *Peer A*에게 발행한 SPKI 인증서의 예는 다음과 같고, *Peer A*는 특정 피어가 제공하는 공유 자원에 대해 "읽기" 권한만 가지는 것을 알 수 있다.

$$<v_{SIA}, v_{IDA}, false, read, 2003/7/19>\, s_{SIA}$$

• v_{SIA} : SPKI 인증서를 발행한 SIA의 공개키나 공개키의 해쉬값을 나타낸다.

• v_{IDA} : 인증서를 발급받은 주체자 *Peer A*의 공개키나 공개키의 해쉬값을 나타낸다.

• *false* : 현재 SPKI 인증서를 발급 받은 주체자가 다른 사용자에게 인증서를 발행할 수 있는 권한을 가질 수 없음을 나타낸다.

• *read* : 특정 피어가 제공하는 공유 자원에 대하여 "Read" 권한만 가짐을 나타낸다.

• 19/*July*/2003 : 인증서의 유효기간을 나타낸다.

• s_{SIA} : 발행자인 s_{SIA}의 개인키를 나타내는 것으로 인증서 발행시 서명을 위하여 사용한다.

만약, *Peer A*가 자신이 제공한 공유 자원에 대하여 다른 피어 들로부터 좋은 평판을 받은 "success"의 횟수가 높은 경우 SIA는 *Peer A*에게 좀 더 많은 권한을 부여한 SPKI 인증서를 발행할 수 있다.

$$<v_{SIA}, v_{IDA}, false, (read, write, download), 19/July/2003>\, s_{SIA}$$

이 경우, *Peer A*는 특정 피어가 제공하는 자료에 대해 "read, write, download" 권한을 가질 수 있다. SPKI 인증서를 발행하는데 있어 접근 권한 지정은 인증서를 어떤 응용에 사용하는가에 따라 다양하게 지정할 수 있다.

③ *Peer A* → *AS* : 선택한 피어 관련 정보 요청

AS → *Peer A* : 전송

Peer A → *Peer C* : 연결 요청

*Peer A*는 서버로부터 받은 피어 목록 중 하나의 피어(여기서는, *Peer C*로 가정한다)를 선택하고, 연결을 위하여 필요한 정보를 서버에게 요청한다. 서버로부터 받은 정보를 이용하여 *Peer C*에 연결을 요청한다.

3.2.3 인증 및 다운로드 단계

① *Peer A* → *Peer C* : 익명 인증서 제출

Peer C → *AS* : Peer A 신원 확인

Peer → *Peer C* : SPKI 인증서 제출

*Peer A*는 *Peer C*에 연결 요청시 서버로부터 발급 받은 익명 인증서를 제출하고, *Peer C*는 서버를 통해 *Peer A*의 신원을 확인하고, *Peer A*가 자원 요청시 SPKI 인증서 제출을 요청한다.

② *Peer C*는 *Peer A*가 제출한 SPKI 인증서를 통해 자신이 제공하는 공유 자원에 대하여 *Peer A*가 어떤 접근 권한을 가지는지 확인하고, 인증서에 명시된 권한에 따라 자신의 자원을 이용하도록 한다.

3.2.4 실행 및 평가 단계

① *Peer A* → *SIA* : *Peer C*(*success* 또는 *fail*)

*Peer A*는 자신에게 지정된 권한에 따라 요청한 자원을 읽거나 다운로드 하여 실행한 후 *Peer C*가 제공한 자원에 대한 평판 값(success 또는 fail)을 SIA에게 전송한다.

② SIA는 각 피어 들로부터 전송되어 오는 자원 제공 피어에 대한 평편 값을 기반으로 각 피어들에 대한 평판 값을 업데이트 한다.

제안 방안에서 서비스에 참여하는 모든 피어들은 이와 같은 단계를 거치면서 서버로부터 인증서를 발급 받고, SIA가 저장하고 있는 자신의 평판 값을 기반으로 SPKI 인증서를

발급 받아 공유 자원을 가진 피어에 연결 요청시 인증을 받은 후 SPKI 인증서 제출을 통해 자신이 가진 접근 권한에 따라 자원 제공 피어의 공유 자원을 이용할 수 있다.

본 논문에서는 익명 인증서의 사용을 통해 공유 자원을 요청한 피어에 대하여 익명성을 제공할 수 있으며, 모든 피어들에게 동등한 접근 권한을 부여하는 기존 방식에서 다른 피어와 공유를 위하여 자원을 제공하는 피어들에게 공유 자원을 사용한 피어들로부터 받은 평판 값을 기반으로 SPKI 인증서를 발행하여 피어들이 자신에게 주어진 접근 권한에 따라 공유 자원을 사용할 수 있도록 하였다. 공유 자원을 이용한 피어들로부터의 평판 값을 통해 악의적이거나 고의적으로 잘못된 자원을 제공하는 피어들에게 최소한의 접근 권한을 가지는 SPKI 인증서를 발행함으로써 정보 제공자의 자원에 대한 악의적인 행동을 막을 수 있다.

4. 결론 및 향후 연구

본 논문에서는 인터넷 환경의 발전으로 인터넷에 연결된 여러 컴퓨터들이 기존의 "클라이언트-서버" 방식이 아닌 "클라이언트-클라이언트" 형태로 정보를 공유할 수 있는 P2P 서비스에 대해 살펴보았다. P2P는 인터넷에 연결되어 있는 모든 컴퓨터가 동등한 권한을 가지고 동작하는 방식으로, 기존의 클라이언트-서버 방식에 대한 대체 방안으로 여러 가지 장점을 제공하는 반면 바이러스나 웜과 같은 프로그램의 손쉬운 분배로 인하여 자원을 공유하고 교환하는 각 피어들에 대한 인증, 피어 간에 주고 받는 자원에 대한 기밀성 및 무결성 그리고, 각 피어들의 공유 자원에 대한 접근 제어 등의 보안 서비스를 필요로 한다.

이에, 본 논문에서는 여러 가지 보안 서비스 중 익명 인증서를 사용하여 각 피어들을 인증하고 각 피어들이 다른 피어들로부터 얻은 평판 값을 기반으로 SPKI 인증서를 발행하여 피어들 각각에 접근 권한을 지정하여 자원 요청시 자신에 부여된 접근 권한에 따라 제한적으로 공유 자원을 사용하는 방안을 제안하였다.

P2P 서비스 이용을 위한 모델 구현에 있어 본 논문에서 제안한 접근 제어 외에 피어 간 전송되는 공유 자원에 대한 기밀성과 무결성 보장을 위하여 암호화나 전자서명과 같은 기존의 암호 기술을 적용한다면 좀 더 안전한 P2P 서비스를 이용이 가능할 것이다.

P2P 서비스는 파일 공유나 메시지 교환뿐만 아니라 개인 경매와 같은 전자상거래, 지식 공유 등과 같은 다양한 분야에 활용 가능하므로 응용 분야에 따라 발생 가능한 보안 문제와 P2P 서비스에 대한 표준화, 그리고 파일 공유에 있어 디지털 컨텐츠에 대한 저작권 보호 등에 관한 추가적인 연구가 필요할 것으로 판단된다.

참 고 문 헌

[1] Dejan S.Milojicic, Vana Kalogeraki, Rajan Lukose, Kiran Nagaraja, Jim Pruyne, Bruno Richard, Sami Rollins, Zhichen Xu, "Peer-to-Peer Computing," Hewlett-Packard Company, 2002.

[2] Andy Oram, "PEER-to-PEER," O'Relly, 2001.

[3] 김봉한, 임명현, 임재명, 이재광, "P2P(Peer to peer) 환경에서의 정보보호 위협과 정보보호 서비스," 정보보호학회지, 제12권 5호, 2002.

[4] 전현성, 조용중, 박천구, "세상을 바꾸는 힘의 중심 P2P," 프로그램 세계, 2002.

[5] Dreamtech Software Team, "Peer-to-Peer Application Development : Cracking the Code," John Wiley & Sons, 2001.

[6] Yulian Wang, "SPKI," Network Security, 1998.

[7] Takamichi SAITO, Kentaro UMESAWA, Hiroshi G. OKUNO, "Privacy Enhanced Access Control by SPKI," IEEE, 2000.

[8] C. Ellision, B. Frantz, B.Lampson, R. Rivest, B.Thomas, T. Ylonen, "SPKI Certificate Theory," RFC 2693, September 1999.

[9] Kazuomi Oishi, "Unconditionally Anonymous Public-key Certificates and their Applicstions," Master thesis, August, 1999.

신 정 화

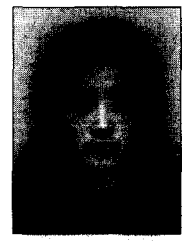
e-mail : shinjh@lisia21.net

1997년 한국방송통신대학교 전자계산학과(학사)

2000년 부경대학교 대학원 전산정보학과(이학석사)

2001년~현재 부경대학교 대학원 전자계산학과 박사 과정

관심분야 : 암호이론, 네트워크 보안, 이동에이전트, XML 보안, Peer-to-Peer



이 영 경

e-mail : twinkle@lisia21.net

2002년 부경대학교 전자계산학과(학사)

2002년~현재 부경대학교 대학원 전자계산학과 석사과정

관심분야 : 암호이론, XML 보안, Access control, Authorization, SPKI

이 경 현

e-mail : khrhee@pknu.ac.kr

1982년 경북대학교 수학교육과(학사)

1985년 한국과학기술원 응용수학과(이학석사)

1992년 한국과학기술원 수학과(이학박사)

1985년~1993년 한국전자통신연구소 선임연구원

1995년~1996년 Univ. of Adelaide 응용수학과, Australia 방문교수

1999년 Univ. of Tokyo, 객원 연구원

2001년~2002년 Univ. of California at Irvine, USA, Visiting Scholar

2002년~2003년 Intergovernmental Organization, Colombo Plan Staff College, Manila, Philippines Chair of Division of Information & Communication Technology

1993년~현재 부경대학교 전자컴퓨터정보통신공학부 부교수

1997년~현재 한국멀티미디어학회 학술이사

2001년~현재 한국정보보호학회 논문지 편집위원

관심분야 : 정보보호론, 멀티미디어 정보보호, 네트워크 성능 평가, 그룹키 관리, 재시도 대기체계론