웹 환경에서 SPKI 인증서를 이용한 접근 제어*

김 점 구**

요 약

웹 서비스는 모든 사용자에 대해 동등한 접근 권한을 부여하여 서로의 자원을 공유할 수 있도록 하고 있다. 이러한 상황에서는 인터넷을 통한 다양한 공격에 따른 취약성이 예상되므로 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 Web Environment

Jeom Goo Kim*

ABSTRACT

Web service is giving an equal privilege to all user 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.

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

* 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음(IITA-2006-C1909-0603-0027).

** 동국대학 컴퓨터학과

1. 서 론

네트워크 환경의 급속한 발전으로 인터넷 사용량이 증가하고 인터넷 이용자들이 필요로 하는 자료의 양이 증가하면서 특정 정보를 얻기 위한 정보 검색 작업은 인터넷상에서 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 효율적 사용, 효율적인 자료 관리 차원에서 "클라이언트-클라이언트" 모델이라 할 수 있다[1].

P2P 서비스는 인터넷상의 정보를 찾기 위해서 기존의 호스트를 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 클라이언트들이 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 가전제품도 모두 하나의 "피어"로 볼 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 P2P에서는 피어 간에 전송하는 정보에 대하여 기밀성, 무결성을 제공해야 하고, 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 특정 피어에 연결을 요청하는 피어들에게 "SPKI(Simple Public Key Infrastructure) 인증서"를 발행하여 피어별로 접근 권한을 설정하고, 설정된 권한에 따라 정보 제공 피어의 자원을 제한적으로 사용할 수 있도록 하는 방안을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구로 P2P 서비스 개념과 모델, SPKI 인증서에 대해 살펴보고, 3장에서는, P2P 서비스에서 "SPKI 인증서"를 이용한 접근 제어를 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 서비스

이다. P2P에서는 각 피어들이 프로세싱 파워, 저장 공간, 컨텐츠 등의 하드웨어 자원들의 일부를 공유하는 것을 가능하게 한다. 즉, P2P란 인터넷 상의 정보를 찾기 위해 검색 엔진을 거쳐야 하는 기존 방식과 달리 인터넷에 연결된 모든 개인 컴퓨터로부터 직접 정보나 서비스를 제공받고 검색은 물론 내려 받을 수 있는 서비스로 기존의 웹 사이트에 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].

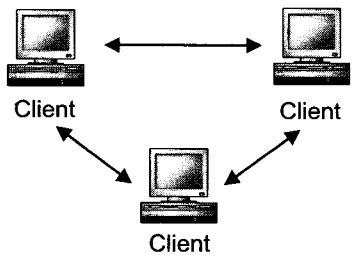
P2P 서비스 이용에 있어 장점은 다음과 같다. 기존의 인터넷 서비스는 서버에 문제가 생기더라도 모든 사용자에게 서비스가 중단되는 경우는 발생하지 않으며, 또한 네트워크에 연결되어 있는 여러 사용자들이 가진 정보에 대하여 손쉬운 공유가 가능하다. 한편, 피어 프로그램의 유지 보수 부담이 있고, 시스템 운영의 안정성과 신뢰도 문제, 그리고 개방되고 분산되어 있는 만큼 P2P 작업을 수행하는 사용자들의 책임성이 요구된다. 또한, 서버의 기능이 배제될수록 시스템의 성능은 더욱 저하될 수 있으며, P2P 서비스를 이용하는 참여자가 항상 온라인 상태로 유지되어야 하고, 악의적인 소프트웨어의 손쉬운 분배로 인한 보안 문제를 야기시키는 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 사용자들의 컴퓨터가 서버뿐만 아니라 클라이언트로 동작하는 모델이다. P2P 애플리케이션이 클라이언트로 다운로드 되면, 네트워크에 연결된 피어들은 네트워크에 접속된 다른 피어들을 동적으로 찾아 파일을 업로드/다운로드 할 수 있다. 순수 P2P 모델은 사용자들 자신이 나름대로의 규칙을 지정할 수 있도록 해주며, 그들 자신의 네트워크를 설정할 수 있게 해주는 특징을 가진다. 그러나 순수 P2P에서는 필요로 하는 정보 검색을 위해 각 피어가 서로에게 질의를 보내는 동작이 중복해서 발생하므로 병목 현상이 생길 수 있고, 시스템 전체를 검색해야 하므로 전체 대역폭을 증가시킬 뿐만 아니라 질의를 수행하는데 오랜 시간이 걸리게 된다. 또한, 특정 피어가 보낸 검색 패킷에 대한 수명을 TTL(Time to Live) 값으로 관리하기 때문에, 맡은 임무를 수행하고도 네트워크 상에 돌아다니는 패킷이 많아져 네트워크 전체가 오버헤드를 일으키게 된다. 그러므로 신뢰성, 속도, 검색 능력은 감소하면서 네트워크 트래픽은 증가하게 되고, 네트워크를 안전하게 관리할 책임을 가진 관리자가 없으므로 네트워크의 관리나 컨텐츠의 관리가 되지 않고 있다.

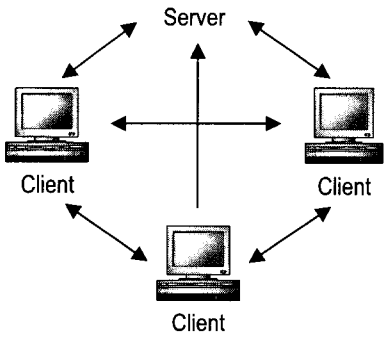


(그림 1) 순수 P2P

2.1.2 간단한 조회 기능 서버를 가진 P2P

이 모델은 실질적으로 서버를 포함하고 있는 것은 아니지만 약간의 관리를 위해 서버의 역할이 포함되어 있는 모델로, 서버는 P2P 서비스를 이요하기 위하여 접속하는 피어에게 이미 접속되어 있는 피어들의 이름을 제공하는 작업만 수행하게 된다.

서비스에 참여하는 피어들은 로그인을 통해 서버에 자신의 존재를 알리게 되고 서버는 단지 피어들에게 현재 접속된 피어들의 목록을 제공함으로써 피어들을 돕는 것이며, 다른 피어와의 연결을 설정하고 파일 다운로드 등과 같은 통신 작업은 피어들 개개인이 수행해야 한다. 이와 같은 모델은 서버가 이미 접속된 다른 피어들의 목록을 제공하여 많은 수의 피어들을 조회할 수 있으므로 스스로 연결을 위한 피어를 찾아야 하는 순수 P2P 모델에 비해 편리하다. 그러나 특정 자원을 다운로드 받기 위해, 피어는 연결되어 있는 각각의 피어들에게 개별적으로 접근하여 다운로드 요청을 보내게 되는데 요청에 대한 처리 시간이 길어지기도 한다.



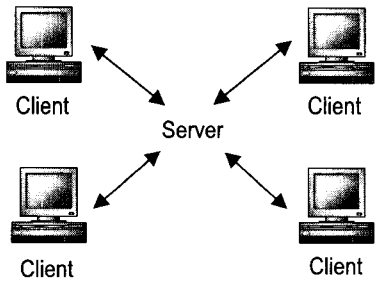
(그림 2) 간단한 조회 기능을 가진 P2P

2.1.3 조회 서버와 룩업 서버를 가진 P2P

순수 P2P 모델과 간단한 조회 서버를 가진 P2P 모델의 특징을 통합한 모델로 서버는 접속된 피어 목록을 각각의 이용 가능한 자원과 함께 제공한다. 서비스에 참여하는 각 피어들이 필요한 자원을 얻기 위해 각각의 피어를 일일이 방문할 필요가 없기 때문에 각 피어들에 대한 부담이 줄어드는 장점을 가진다. 이 모델에서 서버는 두 피어들 사이에 통신을 개시하고 두 개의 연결된 피어들은 통신을 개시하고 유지하면서 다양한 동작을 수행하게 된다.

2.1.4 조회/룩업/컨텐츠 제공 기능의 서버를 가진 P2P

서버가 기존의 클라이언트/서버 구조에서처럼 지배권을 가지고 동작하는 모델로 피어들의 요청은 모두 서버로 전달되고, 모든 자원들이 중앙에 위치한 서버의 데이터베이스에 저장되어 있기 때문에, 피어들 간의 직접적인 연결은 허용하지 않는다. 예를 들어, 특정 한 피어가 정보를 요청하면, 다른 피어와 통신을 하는 대신 서버에 접근하고 서버는 요청들을 처리해서 정보를 제공한다. 이 모델은 많은 요청이 동시에 쇄도할 경우 서버의 처리 속도가 느려지고, 서버가 데이터를 관리, 저장해야 하고, 스스로 모든 요청을 처리해야 하기 때문에 비용이 늘어나는 단점을 가진다.



(그림 3) 조회/룩업/컨텐츠 서버를 가지고 있는 P2P

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 사용 가능한 인증서로 권한 인증서(authorization certificate)라고도 한다[6]. SPKI 인증서는 서버에 의해 발행되고 클라이언트가 소유하고 있다가 서버가 제공하는 서비스를 사용하기를 원할 경우 SPKI 인증서를 제출함으로써 서버의 자원을 제한적으로 사용할 수 있게 된다. SPKI 인증서는 인증서 발급시 사용자의 ID가 아닌 사용

자의 공개키나 공개키의 해쉬값을 사용하여 Issuer와 Subject를 나타내므로 익명성을 유지할 수 있으며, 서버 데이터베이스의 수정 없이 발급 받은 인증서를 다른 Subject에게 쉽게 위임할 수 있고, 특정 서비스에 대해 독립적이며 안전한 통신이 가능하다. 또한, 인증서를 발행하고 관리하기가 쉽고, 유지 보수 가격이 저렴한 특징을 가진다[6, 7].

SPKI 인증서는 사용에 있어 다음의 요구 사항을 가진다[5]. 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, 권한을 자유롭게 지정하고 분배할 수 있고, 권한지정은 사용하는 응용 분야에 따라 자유롭게 지정 가능하다. 넷째, 인증서의 유효 기간을 명확하게 지정해야 한다. 다섯째, 사용자의 이름 대신 공개키를 사용한다. 여섯째, 이름이나 속성에 따라 공개키를 찾는 X.509보다 좋은 방법을 제공할 수 있어야 한다.

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 대해 가질 수 있는 접근 권한을 설정하는 필드이다.

SPKI 인증서의 구조는 다음과 같이 다섯 개의 필드를 포함하는 서명된 메시지이다[6, 7, 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 표현된다. True로 지정할 경우 Issuer는 Subject에게 위임 권한을 주고, Subject는 자신의 인증서를 재위임 할 수 있다. 이때, Subject는 자신이 Issuer로부터 받은 권한과 동일하거나 적은 권한을 다른 Subject에게 위임할 수 있다.
- *Authorization(access rights)* : 인증서를 발급받는 Subject에게 권한을 지정하는 필드로 Issuer가 Subject를 위해 인증서에 서명할 때는 반드시 Subject가 가질 수 있는 권한을 지정해야 한다. 권한 지정은 사용하는 응용 분야에 따라 Issuer가 자유롭게 지정할 수 있다.
- *Validity* : *Issuer*가 인증서의 유효기간을 명시한다. 유효 기간은 Issuer의 개인키 노출이나 분실이 발생할 경우를 대비하여 짧게 지정하는 것이 좋다.

실제 발행되는 인증서는 다음과 같이 Issuer의 비밀키(S(I))에 의해 서명되어 발행된다.

<P(I), P(S), TRUE, read(file1), (7/May/2003)>S(I)

- *P(I)* : Issuer의 공개키 또는 공개키의 해쉬값
- *P(S)* : Subject의 공개키 또는 공개키의 해쉬값
- *True* : delegation이 가능함을 나타낸다.
- *read(file1)* : Issuer가 가진 자원 중 file1에 대하여 "read" 권한을 지정했음을 나타낸다.
- *7/May/2003* : 인증서 유효기간을 나타낸다.
- *S(I)* : Issuer의 비밀키

3. P2P 환경에서 SPKI 인증서를 이용한 접근제어

본 논문에서는 P2P 모델 중 간단한 조회 기능 서버를 가진 P2P 모델에 기반을 두고 "SPKI 인증

서"를 이용한 접근 제어 방법을 제안한다.

3.1 제안 방안

P2P 서비스는 서버 없이 피어들 간에 데이터를 전송함으로써 의도적이거나 고의적인 공격자에 의한 위협에 상당히 노출되어 있다. 그러므로 서비스에 참여하는 피어들에 대한 인증이나 전송되는 메시지에 대한 기밀성, 무결성 등과 같은 보안 서비스와 특정 피어에 대해서 자신의 시스템에 대해 무엇을 할 수 있는 지와 무엇을 할 수 없는지 등의 권한 설정을 통해 서비스에 참여하는 피어들에 대한 접근 제어가 필요하다. 이에 본 논문에서는 먼저 서비스에 참여하는 모든 피어들에게 익명 인증서(anonymous certificate)[9]를 발행하여 자원 공유를 위하여 연결 요청 시 피어들 간 인증이 가능하도록 한다. 서비스에 참여하는 각 피어들에 대한 인증 후 정보 제공 피어는 연결 요청 피어들에게 "SPKI 인증서"를 발행하여 자신의 자원에 대한 접근 권한을 부여하여 자원을 요청하는 모든 피어들이 동등한 권한을 가지고 자원을 사용할 수 있는 것이 아니라, SPKI 인증서에 부여된 권한에 따라 제한적으로 자원을 사용하도록 한다.

3.2 제안 방안의 동작 방식

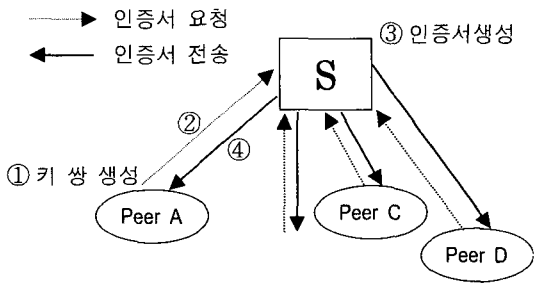
제안 방안에서 사용되는 익명 인증서는 기존의 익명 인증서 형식에 피어 간의 통신에 필요한 식별자로 피어의 가명(pseudonym) 정보가 추가된다. 이를 통해 피어간 익명성을 유지하면서 자원 검색 및 공유가 가능하다. 인증서의 유효 기간은 피어가 서버에 로그인하여 작업하는 동안으로 제한하고, 로그오프 후 다시 로그인할 경우는 새롭게 인증서를 발급 받는 것으로 한다. 그리고 SPKI 인증서 사용에 있어 "delegation"은 하지 않는 것으로 가정한다.

제안 방안에서 사용되는 표기법은 <표 1>에 주어졌고, 동작 절차는 다음과 같다.

〈표 1〉 표기법

표 기	설 명
S	익명 인증서를 발행하고 공유 파일 목록을 관리하는 서버
S_{id}	서버의 identity
Sig_s	익명 인증서 발행시 사용되는 서버의 서명값
ν_p	피어의 공개키
S_P	피어의 개인키
ID_P	피어의 identity
PS_P	피어의 가명(pseudonym)
AC_S	서버가 발행한 익명 인증서

(1) P2P 서비스에 참여하는 모든 피어들은 중앙의 서버를 통하여 익명 인증서(anonymous certificate)를 발급받는다.



(그림 4) 인증서 발급 과정

익명 인증서 발급 과정은 다음과 같다.

① 서비스에 참여하는 각 피어들은 익명 인증서를 발급받기 위하여 자신의 공개키 (ν_p)와 개인키 (S_P)쌍을 생성한다.

② 키 쌍 생성 후 각 피어는 인증서 발급을 위하여 자신이 생성한 공개키 ν_p와 자신의 identity (ID_P), 가명(pseudonym : PS_P) 정보를 서버로 전송한다.

③ 서버는 인증을 요청한 피어에 대한 확인 후 피어의 공개키 ν_p와 피어의 가명 PS_P서버의 정보를 나타내는 S_{id}를 사용하여 서명값 Sig_s

(ν_p, PS_P, S_{id})를 생성한다.

④ 서명 생성 후 서버는 인증서 발급을 요청한 피어에게 피어의 공개키 ν_p, 가명 PS_P, 서버의 정보 S_{id}와 서명값 $Sig_s(\nu_p, PS_P, S_{id})$을 포함하는 익명 인증서 $AC_S(\nu_p) = (\nu_p, PS_P, S_{id}, Sig_s(\nu_p, PS_P, S_{id}))$를 발행한다. 인증서 발행을 요청한 피어의 실제, ID는 서버만 알고 있고 서비스에 참여하는 피어들은 각 피어의 가명을 이용하여 작업을 수행한다.

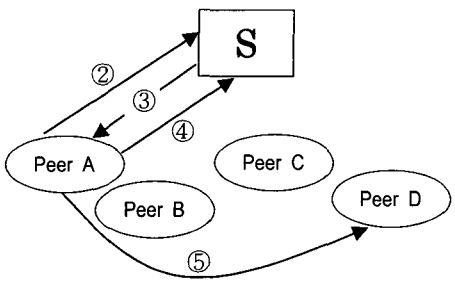
⑤ 각 피어들은 서로의 자원에 대한 공유를 요청할 때 서버로부터 발급받은 인증서 제출을 통해 인증을 거친 후 공유 자원에 대한 사용이 가능하다.

(2) 인증서를 발급 받은 피어는 서버에 로그인하여 자신이 가진 파일들 중 공유하고자 하는 파일 목록을 서버에 등록하고, 필요로 하는 자원을 찾기 위한 검색어를 서버로 전송한다.

(3) 서버는 Peer A의 질의에 일치하는 자원을 가진 피어들의 목록을 Peer A에게 전송한다.

(4) Peer A는 서버로부터 전송 받은 피어 목록 중 가장 적절하다고 판단되는 피어(여기서는 Peer D라 가정한다)를 선택하고 연결을 위하여 필요한 정보를 서버에게 요청하고, 서버는 관련 정보를 전송해 준다.

(5) 서버로부터 받은 정보를 이용하여 Peer A는 Peer D에 연결을 요청한다.



(그림 5) 공유자원 검색 및 연결요청

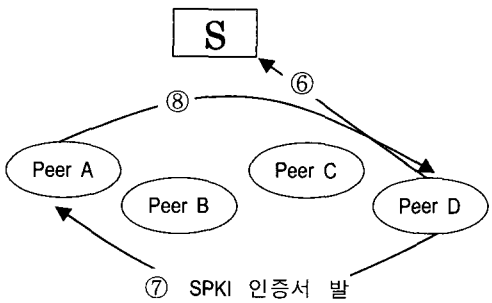
(6) Peer D는 연결을 요청한 Peer A가 제출한 인증서의 유효성을 서버를 통하여 확인한다.

(7) Peer A에 대한 인증 후 Peer D는 자신의 공유 자원에 대한 접근을 제한하기 위해 자신의 개인키로 서명한 SPKI 인증서를 Peer A에게 발행한다.

<P(D), P(A), false, read, 2003/7/19>S(D)

- *P(D)* : SPKI 인증서를 발행한 Peer D의 공개키나 공개키의 해쉬값을 나타낸다.
- *P(A)* : 인증서를 발급받은 주체자로 Peer A의 공개키나 공개키의 해쉬값을 나타낸다.
- *false* : 현재 인증서를 발급 받은 주체자가 다른 사용자에게 인증서를 발행할 수 있는지에 대한 위임 여부를 true, false로 나타낸다.
- *read* : Peer D가 가진 공유 자원에 대해 "read"만 가능함을 나타낸다.
- *19/July/2003* : 인증서의 유효기간을 나타낸다.
- *S(D)* : 인증서에 서명한 Peer D의 비밀키를 나타낸다.

(8) Peer A는 필요로 하는 자원 다운로드를 위하여 Peer D로부터 발급 받은 SPKI 인증서를 제출하고, Peer D는 인증서의 검증을 통해 유효성 여부를 검사한 후 Peer A가 부여받은 접근 권한에 따라 자신의 공유 자원을 이용할 수 있도록 한다.



(그림 6) SPKI 인증서를 이용한 접근 제어

위의 인증서는 Peer D가 가진 전체 자원에 대해 "read" 권한만 지정했지만, Peer D가 가진 공유 자원 하나 하나에 대해 접근 권한을 부여하고자 할 때는 다음과 같은 형식의 인증서를 발행할 수 있다.

< P(D), P(A), false, read(file1, file2), download(file3, file4), 19/July/2003 >S(D)

이 경우, Peer D가 가진 공유 자원 중 file1, file2에 대해서는 "읽기"만 가능하고, file3, file4에 대해서는 다운로드가 가능하다. 자원을 요청하는 피어들에게 SPKI 인증서를 발행할 때 접근 권한 지정은 사용하는 어플리케이션에 따라 다양하게 지정할 수 있다.

P2P 서비스에 참여하는 모든 피어들은 이와 같은 방법으로 서버로부터 먼저 인증받은 후 연결을 요청하는 피어들에게 SPKI 인증서를 발행하여 자신의 공유 자원에 대한 접근을 제어할 수 있다. 이를 통하여 서비스에 참여하는 모든 피어들에게 동등한 접근 권한을부여하는 기존의 방식에서 자료를 요청하는 피어마다 다른 접근 권한을 부여하여 제한적으로 자원을 사용하도록 할 수 있다. 또한, 익명 인증서의 사용으로 인해 서비스에 참여한 피어들의 익명성은 보장하면서 특정 피어로부터 다운로드 받아 실행한 자원이 공유 목록에 등록했던 자원과 다른 경우 실제 피어의 ID는 모르지만 가명을 통해 해당 피어를 추적할 수 있는 특징을 가진다.

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 대해서 살펴보았다. P2P 서비스는 인터넷에 연결되어 있는 모든 컴퓨터가 동등한 권한을 가지고 동작하는 방식으로 기존의 클라이언트-서버 방식에 대한 대체 방안으로 여러 가지 장점을 제공하는 반면 자원을 공유하는 각 피어들에 대한 인증, 피어 간에 주고 받는 메시지에 대한 기밀성, 무결성, 각 피어들의 공유 자원에 대한 접근 제어등의 보안을 필요로 한다. 따라서, 본 논문에서는 여러 가지 보안 요소 중 익명 인증서를 사용하여 각 피어들을 인증한 후 특정 피어가 연결을 요청할 때 개별적으로 SPKI 인증서를 발행하여 자원을 요청하는 각 피어들에게 접근 권한을 부여하여 부여된 접근 권한에 따라 제한적으로 정보 제공자 피어들의 공유 자원을 사용하도록 하는 방안을 제안하였다. 여러 가지 보안 서비스를 P2P 모델에 실제 적용하여 구현할 경우 본 논문에서 제안한 접근 제어 방안 외에 피어들 간에 전송되는 정보에 대하여 안전한 전송을 보장하고, 전송된 정보에 대한 무결성을 보장하기 위해 암호화나 전자서명과 같은 기존의 암호 기술을 추가적으로 적용해야 할 것이다. 또, 사용자가 선택한 자원에 대하여 공유 파일 목록에서 제공되는 파일 이름과 내용이 다를 수 있으므로 실제 내용에 대한 신뢰성을 얻기 위해 다운로드 전 주변 피어들에게 질의하여 해당 자원에 대한 평판(reputation)을 얻는 기능을 추가한다면 다운로드 받으려는 자원의 내용에 대한 신뢰성까지 보장할 수 있을 것이다. P2P 서비스를 파일 공유뿐만 아니라 개인 경매와 같은 전자상거래, 지식 공유 등과 같은 부분에 활용하기 위해서는 응용 분야에 따라 발생 가능한 보안 문제와 표준화, 디지털 컨텐츠에 대한 저작권 보호 등에 관한 추가적인 연구가 필요하다.

참 고 문 헌

[1] Dejan S. Milojicic, Vana Kalogeraki, Rajan Lukose, Kiran Nagaraja, Jim Pruyne, Bruno

Richard, Sami Rollins, and 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, 제5호, 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, and T. Ylonen, "SPKI Certificate Theory", RFC 2693, September 1999.

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

[10] Refik Molva and Yves Roudier, "A Distributed Access Control Model for Java", ESORICS, 2000.

[11] Stefan Saroiu, P. Krishna Gummadi, and Steven D. Gribble, "A Measurement Study of Peer-to-Peer File Sharing Systems", MMCN, 2002.

[12] Krishna Kant and Ravi Iyer, Vijay Tewari, "A Framework for Classifying Peer-to-Peer Tech-nologies", CCGRID, 2002.

[13] 이영록, 김민수, 김용민, 노봉남, 이형효, "역할 기반 접근제어 및 비밀통신을 지원하는 SPKI/SDSI HTTP 보안서버", 정보보호학회 논문지 제12권, 제6호, 2002. 12.

[14] 이재규, "신세대 네트워크의 키워드 'P2P'의 힘", 마이크로소프트웨어, 2000.

김 점 구

광운대학교 전자계산학과 이학사
광운대학교 전자계산학과 이학석사
한남대학교 컴퓨터공학과 공학박사
(주) 제성프로젝트 연구원
(주) 시사컴퓨토피아 인터넷사업본부장
현재 남서울대학교 컴퓨터학과 교수
관심분야 : 정보보호, 컴퓨터 네트워크, 무선통신