P2P 환경에서 해킹 및 바이러스 대응 방안

청주대학교 김봉한*
극동대학교 조한진
한남대학교 이재광

1. 서 론

P2P(peer to peer)는 그림 1과 같이 인터넷에서 서버 컴퓨터를 거치지 않고 정보를 찾는 사람과 정보를 가지고 있는 사람의 컴퓨터를 직접 연결시켜 데이터를 공유할 수 있게 해주는 기술과 그 기술을 응용해서 제공되는 서비스를 말한다. 인터넷에서 정보를 검색 엔진을 거쳐 찾아야 하는 기존 방식과는 달리 인터넷에 연결된 모든 개인 컴퓨터로부터 직접 정보를 검색하고 제공받을 수 있다

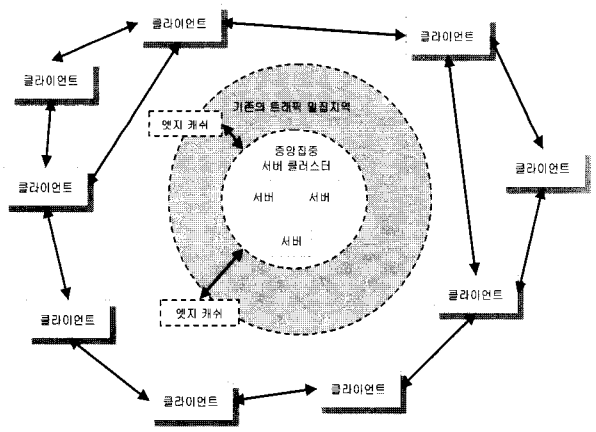


그림 1 P2P 네트워크

그러나 P2P 서비스는 서버 없이 컴퓨터와 컴퓨터간에 데이터를 전송함으로서 의도적이거나 고의적인 공격자에 의해 정보보호 위협에 상당히 노출되어 있는 실정이다. 현재 정보보호 업계에 따르면 국내에 본격 서비스되고 있는 P2P 방식으로 교환되는 파일에는 백오리피스·링제로 등 백도어 프로그램을 몰래 심어놓을 수 있어, 이를 알지 못하는 사용자는 자신의 컴퓨터를 쉽게 해킹 당할 수 있다. 더구나 공격자가 온라인 주식투자나 홈뱅킹에서 사용되는 패스워드를 알아낼 경우 경제적인 손실도 입게 돼 문제가 심각해지고 있다. 또한 P2P 서비스는 문서 파일을 MP3 파일 등으로 바꾸는 등 확장자를 전환할 수 있기 때문에 회사 기밀 정보를 외부로 손쉽게 빼낼 수도 있으며, 이 경우 추적이 거의 불가능하다[2].

현재 국내에서는 뚜렷한 해킹 피해 사례가 보고되고 있지 않지만 국외에서는 시큐리티 포커스 등 유명 정보보호관련 사이트에 P2P 해킹 수법들이 게재되고 있는 상황이다. 따라서 국내에서도 P2P 서비스 산업의 안전적인 성장을 위해서 P2P 네트워크의 무결성과 기밀성을 보장하고, P2P 네트워크에서 다양한 위협 요소의 예방과 대응 기술에 대한 연구가 요구되고 있다. 본 논문에서는 ***P2P 환경에서 다양한 멀티미디어 데이터를 안전하게 전송하기 위하여 요구되는 P2P용 정보보호 서비스를 분석하고 이러한 서비스를 제공할 수 있도록 피어에서의 해킹 및 바이러스 대응 방안과 전송되는 데이터의 무결성과 기밀성을 보장할 수 있는 암호화 키 분배 프로토콜에 대하여 연구하였다.***

2. P2P에서의 정보보호 공격과 정보보호 서비스

P2P 환경에서 발생할 수 있는 불법적인 공격 형태는 다음과 같다.

2.1 정보보호 공격 형태

P2P 시스템에서 정보보호 공격은 크게 두 종류로 나누어진다[3]. 능동적인 공격은 공격자가 능동적인 참가자이다. 능동적인 공격자는 보통 공격적인 모드에서 동작한다. 능동적 공격의 형태는 다음과 같다.

2.1.1 가장(Masquerades)

공격자가 당사자가 아니면서 당사자인 것처럼 가장해서 공격한다. 종종, 공격자는 몇몇 유효성과 특권을 가진 엔티티로 가장한다.

2.1.2 중개자(Man-in-the-middle)

이같은 공격 형태에서, 공격자는 두 네트워크 노드 사이에서 통신을 가로챈다. 공격자는 정보 흐름을 수정하거나 변조시킨다.

* 정회원

2.1.3 재생 또는 재전송 공격(Playback or Replay Attack)

이 같은 공격은 보통 두 개의 노드 사이에서 정보의 교환을 획득하거나 또 다른 실제 대화상의 정확한 어떤 단계를 반복시킨다.

수동적 공격은 공격자가 활발하지 못한 상태에서 주로 사용한다. 대부분 수동적 공격의 형태는 도청이다.

2.1.4 도청(Eavesdropping)

일반적으로 공격자에 의해 데이터의 획득이 조용히 이루어진다.

2.1.5 트래픽 분석(Traffic analysis)

공격자는 데이터 획득 뿐만 아니라 데이터를 분석함으로서 좀 더 많은 것을 얻도록 시도한다.

보통, 수동적 공격은 능동적 공격의 전 단계에서 이루어진다. 예를 들어, 공격자는 먼저 네트워크에서 수동적이다. 그리고 피어 A와 피어 B 사이에서 모든 트래픽을 살펴본다. 피어 A가 떠난 후에, 공격자는 피어 A가 처음에 전송한 정확한 데이터를 재 전송함으로서 피어 B와 통신을 할 수 있다. 이것은 재전송 공격에 대한 전 단계와 같은 도청의 한 경우이다.

2.2 정보보호 서비스

기관은 어느 시점에서 누구에 대해 어떤 정보를 공개하고 공유할 것인지, 또 PC 자원의 이용을 허가할 것인가에 대한 정보보호 정책을 명확히 하지 않으면 안된다. 그래서 부서 내, 부서 간이나 기관 간, 사용자나 타 기관 간 등에서 어느 P2P 소프트웨어를 이용하는가에 대해, P2P의 기술 동향이나 타 기관의 도입 상황을 파악하고, 검사할 필요가 있다.

표 1 P2P의 정보보호 서비스와 대책

기밀성	기술적 대책	· 파일 접근 제어 · 파일의 암호화 · 접근 로그 관리 · 개인 방화벽 · 스팸메일 방지 · 전자 인증 시스템
	물리적 대책	· P2P를 이용하는 PC의 설치 위치를 제한
	기관 · 제도적 대책	· 파일의 기밀성에 따른 분류 · 사용자(기관내 · 외)의 제한 · 기관 내부 사용자의 신분 확인 · 사용자의 정보보호 의무와 손해 배상 청구 계약의 체결
무결성	기술적 대책	· 프로토콜에 대한 트래픽 제어 · 광대역 네트워크의 정비 · 소프트웨어의 재 전송 기능의 적용 · 데이터의 순차적 갱신 · 바이러스 대책
	기관 · 제도적 대책	· 사용제한에 대한 규정 · 복수처리에 의한 계산 결과의 확인
가용성	기술적 대책	· 높은 가용성을 가진 부품의 사용 · 하드웨어의 이중화 · 데이터 백업 · 분산 병렬 처리 · IPv6의 적용
	기관 · 제도적 대책	· 허가되지 않은 소프트웨어의 사용금지

새로운 기술인 P2P라고 해도 그 기술은 기존의 TCP/IP로부터 시작되었으며 이것에 여러 가지 인터넷 기술을 선택해서 구성하고, 거기에 새로운 기능을 추가하는 것으로 이루어진다. 따라서, 현재의 인터넷의 정보보호 대책을 P2P의 특성에 맞춰서 검토하는 것이 중요하다.

P2P의 취약성에 대한 구체적인 정보보호 서비스는 표 1과 같다. 정보보호 서비스는 정보보호 관련 기술에 의한 기술적 대책, 건물과 같은 구조물에 대한 물리적 대책, 실제로 작업하는 사람이나 제도에 관한 기관·제도적 대책 등이 있다[1,5].

3. 피어(Peer)에서 해킹 및 바이러스 대응 방안

P2P는 사용자의 정보, 하드웨어 자원, 그리고 관계되는 많은 데이터를 공유할 수 있는 장점을 가지고 있다. 그러나 P2P 연결은 불법적인 공격자로부터 사용자의 P2P가 스캔되고 변경될 수가 있다. 그러므로 크고 광범위한 인터넷에서 나타나는 모든 중요한 문제들로부터 사용자 스스로가 자신의 데이터를 보호해야 한다.

현재 사용자의 컴퓨터들은 인터넷에 연결되어 있고, 사용자의 피어들을 안전하게 만들 필요가 있다. 컴퓨터 환경이 되는 LAN은 대체로 보호가 필요하지 않은 신뢰받고 있는 환경이다. 사용자의 정보보호 장치는 네트워크를 통해 수신되는 데이터에 대한 트래픽을 조사해야 한다. 정보보호 장치는 다음과 같은 일반적인 규칙을 가지고 있다.

가. 전입 요청 검사

전출 요청은 사용자의 시스템에서 시작한다. 전출 요청은 대부분이 사용자가 명령한 것이다. 전입 요청은 네트워크의 외부로부터 시작한다. 전입 요청은 사용자의 피어가 시작하지 않는다. P2P는 이 인바운드 요구를 통해 외부의 피어들에게 자원을 허가한다. 정보보호 시스템은 오직 인바운드 요구를 사용자가 인정할 때 트래픽을 허가한다. 정보보호 어플리케이션들은 일반적으로 전출 웹 요청과 같은 일반적으로 합법적인 교환에 대해 트래픽을 허락하도록 구성되어 있다.

나. 특정한 포트 번호 또는 특정 프로토콜 검사

모든 네트워크 어플리케이션들은 사용자의 시스템에서 실행한 많은 어플리케이션을 구별하기 위하여 포트들을 사용한다. 네트워크 어플리케이션은 운영체제 네트워크 소프트웨어와 이 포트 번호를 등록한다. 네트워크 소프트웨어는 네트워크 교환에 포함된 포트 번호를 검사하고, 주어진 포트로 수신되는 어플리케이션으로 그 번호를 전달한다.

만약 어플리케이션이 트래픽을 수신하지 않는다면, 소프트웨어는 패킷을 폐기한다. 정보보호 구현은 명확하게 승인 받지 않은 인터넷과 교환되는 포트 번호를 막는 것이다. 따라서 정보보호는 민감한 포트들에 대해 외부로부터의 원격 접근을 검사하고 불법적인 접근은 허가하지 않도록 구성되어야 한다.

3.1 사용자가 가지고 있는 네트워크 리스너 검사

사용자가 얼마나 많은 리스너를 가지고 있는지 검사하기 위하여, 그림 2와 같은 netstat 명령을 사용한다. 먼저 사용자의 피어에 대한 최근 연결을 검사한다. 이 명령은 단지 활성 연결만을 제공한다.

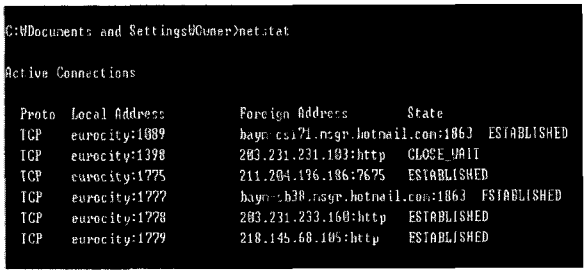


그림 2 피어에 연결된 활성 리스너

위에서 보여준 내용으로, 일반적인 컴퓨터는 여러 형태의 네트워크 활동을 한다. 이 네트워크 어플리케이션 리스너 중 상당수는 인터넷에 노출되지 않아야 한다. 그들은 프린터와 파일을 포함한 민감한 자원을 공유한다. 이것들은 지역 네트워크에 대한 특별한 현상을 발견한다. 각각의 사용자를 트래픽을 막는 규칙보다는, 데이터를 수신하는 포트에 대한 정보보호 장치를 제어해야 하는 편이 더 낫다. 기본적으로, 정보보호 장치는 모든 포트들에 대해 전입 요청을 막는다. 이것은 포트에 할당되는 P2P 솔루션을 위해 매우 잘 동작한다. 이 특정 포트들은 안전한 전송을 위해 정보보호 장치에 의해 식별된다. 또한 데이터를 전송하지 않는 모든 다른 포트들을 제거해야 한다.

시스템 정보보호의 기본적인 작업은 지정된 사용자를 제외하고 모든 포트들에서 전입 요청을 막는 것이다. 또한 정보보호는 포트들의 조사를 통해 오직 확실한 프로토콜과 IP 주소만을 허가한다.

3.2 개인방화벽 어플리케이션을 이용한 피어 정보보호

사용자 피어에서 정보보호를 처리하는 두 가지 방법이 있다. 하나는 소프트웨어 솔루션이고 다른 하나는 하드웨어 솔루션이다. 이 둘은 각각 장점과 단점을 가지고 있다. 소프트웨어 솔루션은 추가적인 배선을 요구하지 않지만 사용자 컴퓨터 수행의 일부분을 사용한다. 그것

은 또한 인터넷에 사용자의 컴퓨터를 상당 부분 노출한다. 하드웨어 솔루션은 특정 박스에 보호를 격리하나 추가적인 배선을 요구한다. 이 두 솔루션들은 모두 시스템을 보호한다. 이것들은 인터넷 연결과 사용자 서브넷 사이에 정보보호 장치를 위치시킨다. 사용자는 데이터 교환들을 위하여 규칙들을 확립한다. 사용자는 원격 IP 주소, 로컬 IP 주소, 포트 번호 또는 프로토콜 형태에 기반을 두고 인터넷 통신을 허가하거나 거부하기 위하여 규칙들을 입력할 수 있다. 일반적으로, 규칙의 기본 설정은 이미 설치되어 있다. 그리고 사용자는 특정한 필요사항에 따라 그것들을 조정한다.

소프트웨어 솔루션은 프록시 또는 인터넷 통신과 사용자의 시스템 사이에 위치하는 방화벽 소프트웨어 어플리케이션으로 구성된다. 프록시가 이미 인터넷 통신을 가로채기 할 경우, 정보보호 특성들을 추가하기가 상대적으로 간단하다. Easy Proxy 어플리케이션은 이러한 능력을 가지고 있지 않지만 Deerfield의 Wingate와 같은 정교한 어플리케이션은 이러한 차단 능력을 가지고 있다. 소프트웨어 방화벽은 독립 어플리케이션이다. 이것의 목적은 사용자의 인터넷 연결을 보호하는 것이다. 만약 사용자가 오직 1대의 컴퓨터를 가지고 있다면, 프록시는 필요하지 않다.

개인 방화벽 어플리케이션은 안철수 연구소의 개인 방화벽 도구인 MyFirewall 어플리케이션을 사용하였다. 이 어플리케이션은 문제점이 인터넷 통신에서 일어날 때 사용자에게 경고를 한다. 사용자는 앞으로의 모든 교환들을 허가하거나 거부하기 위한 규칙을 확립할 수 있다. 또한 개인 방화벽 어플리케이션은 그림 3처럼 네트워크의 포트를 관리할 수 있는 기능을 제공한다. 이러한 포트를 관리함으로서 외부로부터의 불법적인 접근을 제어하고 방지할 수 있다.

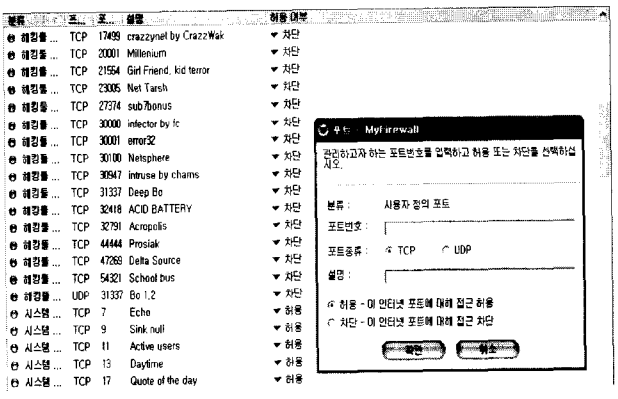


그림 3 포트 관리를 통한 외부 접근 제어

그림 4처럼 개인 방화벽은 공유 폴더에 대한 외부로부터의 접근에 대한 거부/허가를 제어할 수 있다.

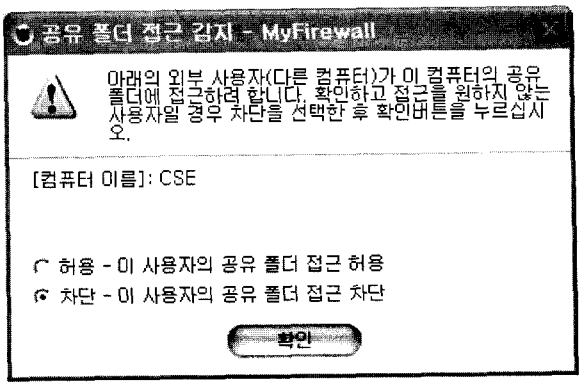


그림 4 공유 폴더에 대한 접근 제어

방화벽은 1개의 시스템을 보호한다. 소프트웨어 프록시는 여러 시스템을 보호하고 인터넷 연결을 공유한다. 이것을 결정하는 요소는 사용자가 단일 컴퓨터를 가지고 있는지 다중 컴퓨터들을 가지고 있는지에 달려있다.

3.3 바이러스로부터 데이터 보호

사용자의 피어는 컴퓨터 바이러스에 대한 보호없이 안전하다고 말할 수 없다. 이 악의적인 공격자들은 간단한 방화벽 규칙으로 부과된 제한을 우회하여 거짓된 수단을 통하여 사용자의 컴퓨터에 접근할 수 있는 권한을 얻는다. 비록 바이러스가 다양한 수단을 통해 침입을 하더라도, 바이러스는 반드시 외부로부터 사용자의 컴퓨터로 전송되어야 한다. 바이러스는 인터넷을 통하여 전송되지만, 사용자의 플로피 디스크 또는 지역 네트워크 연결을 통하여 전송될 수 도 있다. 그러므로, 방화벽은 바이러스 방지에 대한 충분한 보호가 되지 않는다. 사용자는 침입자에 대해 사용자의 컴퓨터 내부로 들어오는 모든 출입문을 감시하는 소프트웨어를 필요로 한다.

바이러스는 자신이 인스톨 되고 식별된 곳에서 변이를 한다. 바이러스는 어플리케이션과 운영체제를 변경함으로서 성장한다. 운영체제는 바이러스가 번식할 수 있는 잠재적인 구멍을 가지고 있다.

해결책은 바이러스 소프트웨어 어플리케이션과 그것에 대응하는 업데이트를 구하는 것이다. 업데이트는 기존의 바이러스의 변형과 새로운 형태의 바이러스를 방지하는데 필수적이다. 사용자는 3가지 방법으로 바이러스를 방지한다.

3.3.1 주문형 바이러스 검사

주문형은 사용자가 정확하게 언제 그것이 필요하다고 요구할 때, 바이러스 검사를 수행한다.

3.3.2 스케줄 바이러스 검사

스케줄 검사는 규칙적인 주기와 시간에 따라 실행한

다. 이것은 다른 어플리케이션들이 컴퓨터의 자원을 필요로 하지 않는 시점에서 바이러스 검사를 할 수 있도록 한다. 바이러스를 검사하는 것은 소프트웨어가 반드시 모든 파일을 검사해야 하기 때문에 사용자 컴퓨터의 자원을 소비한다. 일과시간 후에 소프트웨어를 실행하는 것이 좋은 방법이다.

3.3.3 이벤트 처리 바이러스 검사.

이벤트 처리는 잠재적으로 알려진 바이러스에 대한 변화가 생길 때마다 검사를 수행하는 것이다. 이것은 대부분의 안전한 스킴이다. 그러나 모든 전송을 검사하는 것을 요구한다. 이 검사의 레벨은 성능에 영향을 줄 수 있다 그러나 이것은 매우 높은 정보보호 레벨을 제공한다.

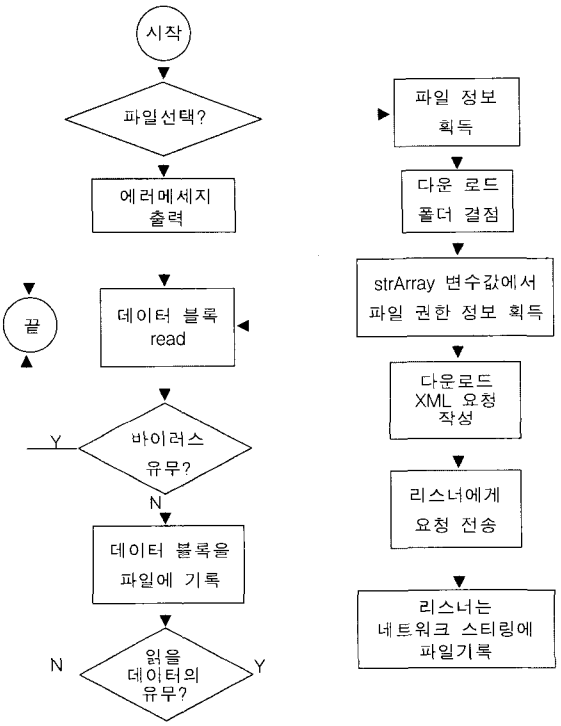


그림 5 다운로드 절차에서 바이러스 검사 적용

그림 5는 파일의 다운로드 절차에서 바이러스를 검사할 수 있는 백신 프로그램을 P2P 어플리케이션에 적용할 수 있는 위치를 보여주고 있다. 사용자는 부적당한 전입 또는 전출 요청에 대하여 시스템을 보호하도록 방화벽을 구축하고 바이러스에 대하여 사용자 시스템을 예방하기 위해 바이러스 백신 소프트웨어를 설치해야 한다.

4. 피어 사이(inter Peer)에서의 해킹 대응 방안

4.1 P2P용 키 분배 프로토콜의 요구 조건

본 장에서는 서버를 가진 P2P 어플리케이션에서 기밀성과 무결성을 제공하기 위한 키 분배 프로토콜을 설계하였다. P2P에서 두 당사자 간에 믿을 수 있는 연결을 확립할 수 있도록 하는 암호화 키 분배 프로토콜은 다음과 같은 요구 조건을 필요로 한다.

4.1.1 호환성

독자적인 프로그래머들은 다른 사람의 코드에 대한 이해 없이 성공적으로 암호학적 요소들을 교환할 수 있는 프로토콜을 이용하여 어플리케이션을 개발할 수 있어야 한다.

4.1.2 확장성

프로토콜은 새로운 공개 키와 대량의 암호화 방식들이 필수적으로 통합될 수 있도록 프레임워크를 제공하는 것이 요구되어야 한다. 이것은 또한 새로운 프로토콜을 생성하도록 하는 요구를 방지하고 새로운 정보보호 라이브러리에 대한 요구를 회피한다.

4.1.3 상대적인 효율성

암호학적 운영은 높은 CPU 강도, 특별한 공개 키 운영이 되기 쉽다. 이 같은 이유로, 프로토콜은 많은 수의 연결을 감소시키도록 그리고 네트워크 효율성을 개선하도록 스킴들을 통합한다.

4.2 P2P용 암호화 키 분배 프로토콜 설계

우선 모든 피어들은 P2P 서비스를 사용하기 위해 최초로 서버에 접속할 때 사용자 인증 절차를 통해 인증서를 발급 받는다. 표 2는 프로토콜에서 사용되는 기호들에 대한 설명이다.

표 2 키 분배 프로토콜에서 사용되는 키 표기법

키	설명
CEK(Content Encrypted Key)	내용의 기밀성을 위한 암호화 키
CHK(Content Hash Key)	무결성을 위한 해쉬 키
KR	CEK을 전달하기 위한 공개키
KU	CEK를 얻기 위한 개인키
T	해당 피어의 토큰
CERT	해당 피어의 인증서

모든 피어들은 그림 6처럼 로그인 절차를 수행한다.

그림 6 피어들의 로그인 절차

① 모든 피어들은 공개 키 쌍(KU, KR)을 생성한다.
② 모든 피어들은 서버에 로그인 한다.
③ 서버는 정당한 사용자임을 검사하고 성공한 메시지로 응답한다.
④ 피어 B는 그림 7과 같이 서버에게 특정한 파일 이름을 위한 검색하는 메시지를 전송한다.
⑤ 서버는 일치하는 파일 이름에 대해 사용 가능한 피어들의 목록을 응답한다.
⑥ 피어 B는 서버에게 피어 A에 위치하는 파일에 대해 다운로드 요구를 전송한다.
⑦ 서버는 피어 A에 대한 IP 주소와 수신 포트, 공개키(AKU)를 포함하는 자세한 정보를 응답한다.

Search-Respond(IP, Port, AKU)

⑧ 피어 B는 토큰을 생성한다. 토큰은 랜덤 넘버와 타임 스탬프로 구성된다. 피어 연결을 위해 다음과 같은 파일 요구 메시지를 전송한다.

FILE-Request(AKU{BCERT, BKU, BT})

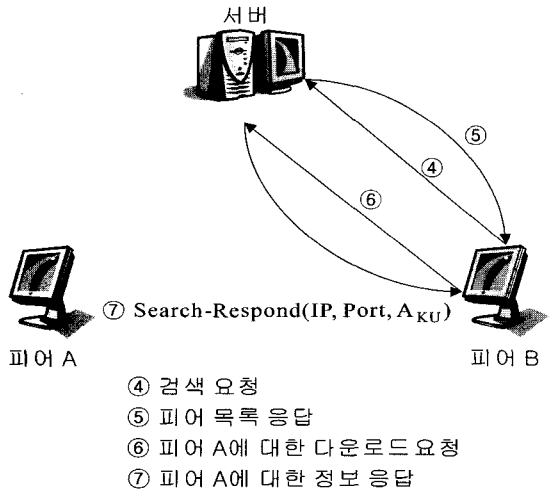


그림 7 특정 파일에 대한 피어 검색 절차

⑨ 피어 A는 그림 8처럼 자신의 개인 키(A_{KR})로 복호화 한 후 B의 인증서(B_{CERT})를 통해 B가 서버에서 인증한 정당한 사용자임을 확인한다. 그리고 피어 A는 전송할 파일을 암호화 할 CEK를 생성한다.

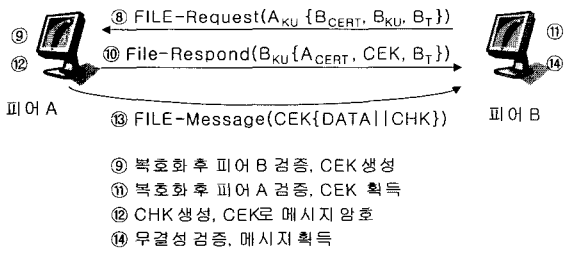


그림 8 CEK 분배 및 메시지 암호화 절차

⑩ 피어 A는 다음과 같은 응답 메시지를 전송한다.

File-Respond(BKU{ACERT, CEK, BT})

⑪ 피어 B는 자신의 개인키로(B_{KR})로 복호화 한 후 피어의 인증서(A_{CERT})를 통해 정당한 사용자임을 검증하고 BT를 통해 자신의 메시지의 수신 여부를 검증한다. 검증이 완료된 후 피어 B는 파일 전송을 위한 CEK를 획득하고 연결을 확립한다.
⑫ 피어 A는 전송할 파일의 무결성을 위한 CHK를 생성하고 전송할 메시지를 CEK로 암호화한다.
⑬ 피어 A는 다음과 같은 메시지의 전송을 시작한다.

FILE-Message(CEK{DATA||CHK})

⑭ 피어 B는 CEK를 통해 메시지를 복호화 한 후 CHK를 통해 무결성을 검증한다. 그리고 검증이 확립된 후 DATA를 획득한다.

5. 결 론

P2P는 인터넷에서 중간에 서버 컴퓨터를 거치지 않고 정보를 찾는 사람과 정보를 가지고 있는 사람의 컴퓨터를 직접 연결시켜 데이터를 공유할 수 있게 해주는 기술과 그 기술을 응용해서 제공되는 서비스를 말한다. 그러나 P2P 서비스는 서버 없이 컴퓨터와 컴퓨터 간에 데이터를 전송함으로서 의도적이거나 고의적인 공격자에 의해 정보보호 위협에 상당히 노출되어 있는 실정이다.

그러므로 본 논문에서는 P2P에서 발생될 수 있는 정보보호 공격과 정보보호 위협을 분석하였고 이러한 위협을 통해 안전한 P2P 서비스를 제공하기 위한 정보보호 서비스를 분석하였다. 그리고 정보보호 서비스를 제공하기 위한 방법으로 피어에서 사용자가 적용할 수 있는 방안과 피어 사이에서 적용할 수 있는 프로토콜을 제안하였다. 피어에서 적용할 수 있는 방안은 개인 방화벽 어플리케이션을 이용한 대응 방안, P2P 어플리케이션에 백신 소프트웨어를 적용하는 방안이고 피어 사이에서 가능한 방안은, 기밀성과 무결성을 위한 키 분배 프로토콜을 설계하여 P2P 통신 환경에 적용하는 방안이다.

제안된 방안이 완전한 P2P 정보보호를 위한 방안은 아니다. 향후 연구에서는 제안된 설계를 통해 P2P 어플리케이션에 백신 프로그램의 실제 적용과 키 분배 프로토콜을 통한 P2P 암호화 프로토콜 구현이 필요하고 이러한 모든 대응 방안을 통합한 P2P 어플리케이션 구현이 필요하다.

참고문헌

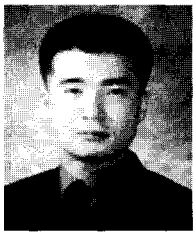
[1] Idota, Hiroki, "The Issues for Information

Security of Peer-to -Peer," Osaka Economic Papers, Vol.51, No.3, December 2001,
[2] Hurwicz, Michael, "Peer pressure: Securing P2P networking," Network Magazine, vol.17, no.2, February, 2002,
[3] Simon Kilvington, "The dangers of P2P networks," Computer Weekly, Sept 20. 2001.
[4] Dana Moore, John Hebeler, "Peer to Peer: Building Secure, Scalable, and Manageable Network," McGrawHill, 2002
[5] 김봉한, 이재광, "P2P 어플리케이션 보안을 위한 JXTA 분석", 한국정보보호학회지, 한국정보보호학회, Vol. 13, No. 3, 2003. 6.
[7] Daniel B, Darren G, Navaneeth, "JXTA:Java P2P Programming," SAMS, 2002
[6] Dreamtech Software Team, "Peer to peer Application Develop- ment: Cracking the Code" John Wiley & Sons, 2001

김 봉 한

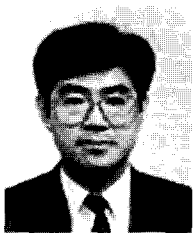
1994. 2 청주대학교 전자계산학과 졸업
1996. 2 한남대학교 전자계산공학과 석사
2000. 2 한남대학교 컴퓨터공학과 박사
2001. 3~현재 청주대학교 컴퓨터정보공학과 조교수
관심분야 : 컴퓨터 네트워크, 멀티캐스트, 정보 보호
E-mail : bhkim@chongju.ac.kr

조 한 진



1997. 2 한남대학교 전자계산공학과 졸업
1999. 2 한남대학교 컴퓨터공학(석사)
2002. 8 한남대학교 컴퓨터공학과(박사)
2002. 3~현재 극동대학교 정보통신학부 전임강사
관심분야 : 네트워크 보안, 보안프로토콜
E-mail : hjcho@kdu.ac.kr

이 재 광



1984. 2 광운대학교 전자계산학과 졸업
1986. 2 광운대학교 전자계산학과(석사)
1993. 2 광운대학교 전자계산학과(박사)
1993. 9~현재 한남대학교 컴퓨터공학과 정교수
관심분야 : 컴퓨터 네트워크, 정보통신 정보보호
E-mail : jklee@netwk.hannam.ac.kr