P2P 표준화 및 기술 동향

Standardization and Technology Trend of Peer-to-Peer Communication

u-IT839의 정보보호 이슈 특집

권혁찬 (H.C. Kwon) P2P보안연구팀 선임연구원
문용혁 (Y.H. Moon) P2P보안연구팀 연구원
구자범 (J.B. Gu) P2P보안연구팀 연구원
고선기 (S.K. Kho) P2P보안연구팀 연구원
나재훈 (J.H. Nah) P2P보안연구팀 팀장
장종수 (J.S. Jang) 네트워크보안그룹 그룹장

목 차

초기에 P2P가 등장할 때만 해도 저작권, 보안 등의 문제 등으로 인해 '문제아' 정도로 인식되었던 것은 사실이다, 그러나 최근 들어서는 P2P를 응용 인프라 구축을 위한 하나의 통신계층으로 보는 시각이 등장할 정도로 인터넷에서 매우 대중화된 서비스가 되어 버렸으며, 실제로 VoIP, video streaming, game 등 매우 다양한 응용의 인프라로 P2P가 사용되고 있다. 본 고에서는 이러한 P2P에 대한 표준화 및 기술 동향, 보안 취약성 및 대응 기술 등을 살펴본다.

Ⅰ. 서론

2005년 9월 NGN2005에서는 2003년을 기점으로 하여 인터넷에서 가장 많은 트래픽을 차지하는 서비스가 P2P 서비스라는 통계를 발표하였고, 같은 해 Network World지에서도 인터넷 트래픽의 60~89% 정도의 트래픽을 P2P 응용이 차지하고 있다고 하였다. 실제로 현재 수많은 사용자가 P2P 서비스를 이용하고 있으며 다양한 P2P 응용이 급속 출현되고 있는 현실이다. 과거에는 P2P 응용하면 instant messaging, file sharing, distributed computing 정도를 떠올렸으나, 지금은 VoIP, video streaming, multicast, web caching, game, virtual office 등 무척이나 다양한 분야의 응용에 적용되고 있는 실정이다. 문제는 저작권 문제나 보안 문제와 같은 P2P 서비스의 부작용을 최소화하면서 안전하고 효율적인 방법으로 P2P 서비스를 사용하는 환경을 조성하는 것이다. 본 고에서는 이러한 P2P에 대한 기술 동향, 표준화 동향, 보안 취약성 및 대응 기술 등을 살펴본다.

Ⅱ. P2P 표준화 동향 분석

P2P 관련 표준화 활동은 IETF, IRTF, ITU-T, 및 3GPP와 같은 국제 표준화 기구들을 중심으로 이루어지고 있다. 본 장에서는 그 개략적인 활동에 대해 언급하기로 하겠다.

1. IETF

P2P-SIP WG는 65차 회의에서 BoF 미팅이 시작되어 현재 그 구성이 진행중인데, 본 작업그룹은 세션 설치 및 관리가 중앙서버보다는 단말들의 집합체에 의하여 완전히 또는 부분적으로 처리되는 설정에서의 SIP 세션 이용을 위한 메커니즘과 가이드라인을 개발하는 것에 주된 목적을 두고 있다. 이러한 아이디어는 서비스 공급자의 프록시들에 의존하는 기존 SIP 접근법의 대안이 될 수 있을 것으로 예상된다. SIP에 P2P 기술을 도입하려는 주된 이유는 P2P의 확장성과 서버 유지비용의 절감이다. 수백만 개 peer들의 등록과 위치정보를 관리해야 하는 SIP 서버들의 역할을 P2P 기술을 활용하여 커버하고자 하는 것이다[1]. 더불어 SIMPLE WG은 IMP (RFC 2779[2]) 서비스에 적합한 SIP 응용의 표준화에 초점을 맞추고 있으며 IMP, CMIP의 요구사항을 만족시키는 형태로 진행되고 있다.

SEND WG의 목적은 별도의 수동적 keying 작업 없이 보안된 IPv6 인접 노드 탐색(securing IPv6 neighbor discovery)을 지원하는 프로토콜을 정의하는 것이다. 이를 위해 SEND 프로토콜에서는 공개 서명키(public signature key)를 IPv6 주소에 적재(binding)하는 방법을 정의하고 있으며, 이를 위한 특별한 주소로 공개키(public key)와 부가적인 파라미터를 암호적 기법의 단방향 해시 함수에 적용하여 생성한 CGA[3]를 사용한다. 즉, IPv6 주소로부터 전달된 메시지는 첨부된 공개키, 부가적인 파라미터 그리고 관련된 비밀키를 이용한 서명을 통해 보호 받을 수 있게 된다. 특히 SEND 프로토콜은 CA 또는 별도의 보안 인프라 없이 IPv6 네트워크 상의 보안된 메시지 교환을 가능하게 한다는 점에서 그 의의가 있다. 본 작업그룹은 3건의 RFC 문서를 등록한 후 2004년에 종료되었다.

XMPP WG는 IM의 표준을 제정하기 위한 작업그룹으로서, 이를 위해 보안 기능이 추가된 XMPP 프로토콜의 표준화 작업을 진행하였다. 또한 채널 암호화를 위해 SASL과 TLS/SSL을 사용하도록 규격을 정의하였으며, 개체 암호화를 위해 OpenPGP [4]를 사용하도록 규격을 정의하였다. XMPP WG는 표준화 작업을 완료한 뒤 2004년 10월 종결되

● 용 어 해 설 ●

Peer-to-Peer Technology: 네트워크에 참여하는 각 peer가 적은 수의 일부 중앙 서버에 의존하는 기존의 client/server 방식의 컴퓨팅 방식과는 달리, 각 개별 peer간에 자원(공유콘텐츠, 컴퓨팅 파워) 등을 공유하는 방식의 새로운 분산컴퓨팅 패러다임을 의미하며 단순히 네트워크 토폴로지 형태를 기초로 P2P 네트워크라 명명하는 경우도 있다.

었다. 본 작업그룹에 의해 등록된 RFC는 모두 4건이다.

2. IRTF

P2P RG[5]는 IRTF의 12개 연구그룹들 중 하나로 2003년 말에 시작되었다. P2P RG의 설립 목적은 연구자들에게 근본적인 P2P 관련 이슈들을 폭넓게 연구할 수 있도록 포럼을 열고, 연구결과를 IETF에 제출함으로써 P2P 프로토콜 표준화 작업을 담당할 미래의 작업그룹들에게 도움이 될 만한 기반을 제공하는 것이며, 현재 P2P에 대한 전반적이고 근본적인 연구가 진행중이다. P2P RG 하위에는 더욱 세분화된 연구를 위한 여러 서브그룹들이 존재한다.

SAM RG[6]는 많은 멀티캐스트 그룹과 네트워크 자원의 참여를 전제로 하는 확장성이 우수하고 적응성이 뛰어난 멀티캐스트 프로토콜에 관해 집중하고 있는데, 그 주요한 연구 주제로는 ALM, OM, 기존의 IP native multicast 뿐만 아니라 이를 혼용한 hybrid 방법론(예; P2P overlay network)을 포함한다. 2006년 3월과 7월에 각각 개최된 IETF 65차, 66차 회의에서는 SAM 관련된 요구사항 정의, survey 리포트 및 NEMO, NICE, XCAST와 같은 ALM 사례가 소개되었으며, 특히 66차 회의에서 독일 Göttingen 대학에서 DMMP에 관한 초안(draft-lei-samrg-dmmp-00)을 제출한 바 있다. 현재 2007년도에 개최될 68차 회의 및 P2PM07 (Workshop on Peer-to-Peer Multicasting)을 차기 주요 일정으로 예정하고 있다.

3. ITU-T

ITU-T의 특정화된 13개의 SG 중 SG17은 보안, 개발언어, telecommunication 소프트웨어 분야의 표준을 담당하고 있으며, 그 아래에 보안 통신 서비스 분야를 담당하는 Question Q.9/17이 존재한다. 현재 이곳에서 P2P 보안 이슈가 다루어지고 있는데 2005년 10월에 일본 측에서 P2P 보안 분야의 요구사항(위협 분석 등)에 관한 프로젝트인 X.p2p-1을, 한국 측에서 P2P 보안을 위한 세부 기술에 관한 프로젝트인 X.p2p-2를 담당하기로 결정되었다. 2006년 4월 제주도에서 개최된 SG17 Q.9 회의에서는 이들 프로젝트에 관련하여 총 6건의 기고서가 제출되었는데, 한국에서 'Secure Routing on P2P Overlay Network', 'Reputation System' 'Trusty ID Authentication Architecture', 'P2P Detection and Control' 등에 관하여, 일본에서는 X.p2p-1의 구조, 중국은 P2P 보안 신뢰 모델에 관한 기고서를 각각 제출하였다.

국내외적으로 P2P로 인한 과다 트래픽 발생, 개인정보나 기밀 유출사고가 잦아지고 있고, P2P를 이용한 해킹의 위험성도 매우 높아지고 있다. 현재 X.p2p-1와 X.p2p-2에서도 이러한 보안 위협들에 대처하기 위한 방법을 찾는 데 중점을 두고 있으며, 앞서 언급한 draft들의 주제들이 향후 Q.9/17에서의 주요 P2P 보안관련 표준화 이슈가 될 것으로 예상된다. 이번 Q.9/17에서 제안된 X.p2p-1과 X.p2p-2의 마일스톤은 <표 1>과 같으며, 스위스 제네바에서 SG17 회의(2006.12.4.~15.)가 진행되었다.

〈표 1〉 X.p2p-1/X.p2p-2 Milestone

Draft	First Draft	Final Draft	Consent
X.p2p-1	2Q/2007	3Q/2007	2Q/2008
X.p2p-2	2Q/2007	3Q/2007	2Q/2008

4. 3GPP

3GPP[7]는 PCG를 중심으로 하위 4개의 TSGs로 구성되어 있는데, 이중 TSG Service and System Aspects의 하위그룹인 TSG SA WG5 Telecom Management에서는 기존의 TM 아키텍처에 P2P 인터페이스를 추가하기 위한 기법 및 종전의 IRPs를 본 구조에 적용하기 위한 방법론에 대해서 표준화된 문서를 작성하고 있다. 서브넷을 위해 EMF와 DMF를 제공하는 DM은 P2P 인터페이스를 통해 다른 peer DMs와 협력적인 도메인 관리 기능을 제공할 수 있다는 것이 본 작업그룹의 주요한 골자를 이루는 논지이다. P2P 인터페이스는 여러 개

의 IRPs로 분류될 수 있으며, 이러한 IRPs는 각 DM에 존재하는 IRPManager와 IRPAgent간 정보교환을 통해 서로 다른 DM이 관리하고 있는 네트워크 경계(border)에 대한 정보를 local DM에 인지시키고 이를 TM 기반의 네트워크 관리에 적용할 수 있도록 한다.

Ⅲ. P2P 보안 취약성 및 대응책

P2P는 자치적인 성격의 분산컴퓨팅 기술을 기반으로 하고 있으므로 분산환경에서의 특수한 보안 취약성에 대한 분석의 선행이 필수적이다. 즉 기존의 잘 알려진 보안 위협에 추가적으로 P2P 네트워크 특유의 문제점에 대한 이해가 요구되며 더불어 대응책을 고려함에 있어 기존의 보안 메커니즘의 적절한 변이를 숙고해야 할 필요성이 있다. 본 장에서는 대표적인 6가지 P2P 보안 취약성에 대해 살펴보고자 한다.

1. Whitewashing

현재 인터넷에서 큰 문제점을 야기시키고 있는 대표적인 취약점이다. P2P 네트워크는 기본적으로 peer의 자유로운 참여로 조성되는 네트워크 구조다. 이러한 특징은 각 peer의 익명성(anonymity)을 보장하는 장점이 되는 반면에 free-rider[8]인 peer들이 손쉽게 저렴한 비용으로 사용 실체에 대한 검증 없이 새로운 ID를 가지고 P2P 네트워크에 참여할 수 있는 기회를 제공하는 문제점을 안고 있다.

일례로, 단순히 온라인 상에서 주민등록번호로 인증을 하고 ID 발급을 하면, 본인의 동의 없이 도용/오용된 주민등록번호인 경우에 수많은 ID의 생성을 야기시킬 뿐만 아니라 악의적 이용자의 자유로운 인터넷 출입을 허용하게 되는 것이 현 실정이다.

Whitewashing에 대한 구체적인 대안 모델로써, 먼저 strict model을 고려할 수 있다. 중앙신뢰기관(central trusted authority) 또는 신뢰할 수 있는 로그인 서버(trusted login server)에 의해 강력한 할당 기법을 바탕으로 각 peer에게 고유한 ID를 부여한다. 그러나 본 기법은 중앙 서버의 개입을 통해 ID가 부여되고, 관리된다는 구조적 문제점을 안고 있다.

즉 현실적으로는 PKI와 같은 인증을 위한 인프라가 있지만 실체 확인을 위하여 F2F 검증을 하여야 하므로 P2P와 같은 분산환경에서는 불가능한 방법이며, P2P 서비스를 위하여 현재의 은행에서 F2F 검증을 대행하여야 하며, PKI 기반의 인증서가 없는 사람은 P2P 서비스를 받을 수 없다는 문제점이 발생된다.

두번째 모델로써, 중앙신뢰기관을 통한 메커니즘의 사용이 불가능하다면, reputation model을 고려할 수 있다. 즉, P2P 네트워크에 참여하고자 하는 whitewashers를 포함한 모든 새로운 peer에게 합리적인 방법으로 penalty를 부여하는 방법을 고려할 수 있다. 그러나 해당 방어 기법은 reputation system과 같이 cost를 기반으로 peer의 악의성 여부를 판단하는 시스템상에서만 고려될 수 있다는 한계를 가지고 있다. 또한, peer간 상대적이고 동적인 cost 증감을 고려해야 하므로 P2P 네트워크로의 빈번한 참여 시도는 P2P 시스템 전체의 성능 저하를 가져올 수 있다.

2. ID Spoofing

본 공격은 악의적 peer가 바로 자기 자신의 식별정보(Identity, ID)를 속여 다른 대상 시스템을 공격하는 기법이다. 공격자는 획득한 식별정보를 target peer에 접근하는 ID로 사용하거나 두 peer 사이의 통신과정에서 responder peer인척 함으로써 비인가된 통신을 지속할 수 있다.

이와 같은 공격이 가능한 이유는 기본적으로 분산 환경을 기반으로 한 현재의 인터넷에서 ID 발급이 자유롭게 허용되어 이에 대한 추적이 어렵기 때문이다. 즉 아무런 규칙 없이 ID 발행을 허용한다면 ID가 도용되었을 때에 허가된 영역, 권한 외에서의 사용에 대한 능동적 대처가 어렵게 된다. 그러므로

ID 발급에 대한 최소한의 인증서버가 있어서 ID에 대한 명확성과 제한성을 부여하여 ID 검증 체계를 강화해야만 한다.

이러한 공격은 ID 인증 기반의 접근 제어와 패킷 필터링 접근 제어, 취약점 서비스 사용의 제거, 암호화 프로토콜의 사용을 통해서 방어가 가능하다.

3. Reputation

상기 언급한 whitewashing 및 IP spoofing 등의 공격을 통해 획득된 신뢰성 없는 ID를 가지고 사이버 공간에서 문제점을 야기시키는 공격자가 있다 하더라도 공격자 본인이 해당 ID를 사용하지 않았다고 거짓말을 하면 ID 사용의 실체를 검증하지 못하므로 ID의 소유자가 사이버공간에서 한 행위에 대하여 최종 부인을 할 수 있게 된다. 즉, 본 공격 유형에 대해서는 행위 부인에 대한 실제 검증이 어려운 문제점이 있다.

4. Man-in-the-Middle Attack

Peer 간에 상호인증을 통해 보안적으로 신뢰성 있는 통신 채널이 생성되더라도 중간자 공격(이하 MITM) 공격방법을 통해 통신 채널에서 전송되는 데이터들의 악의적 수집이 가능하다.

본 공격은 peer 간에 전송되는 데이터 스트림(data stream)의 불법 수정이나 거짓 데이터 스트림 생성을 통한 신분위장(masquerade), 재전송(replay), 메시지 불법수정(modification of message), 그리고 서비스 부인(denial of service) 등의 공격을 감행하는 특징이 있다.

즉, 악의적인 객체 또는 공격자가 중간에서 가로챈 중요한 데이터의 내용을 거짓된 내용으로 수정함으로써 인증된 객체가 수정된 내용을 믿게 되어 통신중인 peer에게 있어 강한 위협 요인에 노출되게 만드는 P2P 네트워크상의 대표적인 적극적 공격 유형이다.

MITM에 대비하기 위해서는 다음과 같은 요구사항을 만족해야만 한다.

- 상대 객체에 대한 안전한 인증 서비스 필요함
- 인증된 객체만이 패킷을 복호화 할 수 있는 암호화 키 서비스 필요함
- 교환되는 모든 메시지들이 중간에서 수정될 수 없어야 하며 수정된 경우 이를 탐지해야 함
- 각 객체 시스템에 개인 firewall, anti-virus 프로그램과 같은 보안 대책이 수립되어야 함
- 등록된 데이터의 위치 정보에 오류가 있음을 인식했을 때 피해가 확산되지 않도록 빠른 대처 방법이 필요함

5. Privacy

P2P 분산환경에서는 개체(사용자 또는 peer) 간의 정보를 어떤 기준에 의해 사용/공유할 수 있는지에 대한 정의가 없으며 관리의 주체도 존재하지 않으므로 개인의 정보가 더 쉽게 노출될 수 밖에 없는 상황에 놓이게 된다. 물론, PKI라는 개인정보보호를 위한 훌륭한 인프라가 존재하지만, 인증서 발급을 위해 제공해야 하는 개인정보의 양이 불필요하게 많다는 비판이 있으며, 이러한 정보가 공개키를 포함하여 TTP에 수록되어 있다는 것에 대한 보안상의 우려를 낳고 있는 실정이다. 즉 개인정보보호를 하기 위하여 구축된 PKI 인프라가 역으로 개인정보를 손쉽게 얻을 수 있는 중앙 개체로써 기능할 수 있다는 것이다. 즉 정보를 불필요하게 집중화시키는 것에 대한 거부감이 존재하기 때문에 분산환경에서의 개인정보보호는 해당 당사자간에만 정보를 제공하고 처리하는 자치적 관리구조로 관리 체제를 구축할

● 용 어 해 설 ●

Public Key Infrastructure: ITU-T에서 공개키 암호 방식을 안전하게 사용하고 관리하기 위한 정보 보호 표준 방식으로 채택한 X.509 방식을 이용하여 인증 기관(CA)에서 발행하는 인증서를 기반으로 상호 인증을 수행하는 방식을 의미한다. 즉 암/복호화키로 구성된 공개키를 이용해서 송/수신 데이터를 암호화하고 디지털 인증서를 통해 인터넷 사용자를 인증하는 시스템을 일컫는다.

필요성이 있다. 이 경우 정보가 공개되어도 국지적 위협의 양상을 보이며 그 피해가 최소화 될 수 있다.

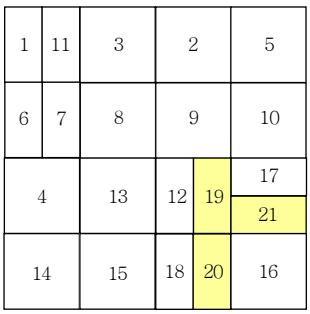
6. DHT 기반 Overlay Network 취약성

본 절에서는 DHT 기반의 오버레이 네트워크를 구축하여 P2P 서비스를 제공하는 경우에 발생할 수 있는 보안 취약성을 분석한다.

가. Node ID Related Attack

P2P 오버레이 네트워크에 참여하고자 하는 peer는 자신의 node ID 즉 joining point를 선택할 수 있어 많은 보안 위협에 노출되게 된다. 예를 들어 structured P2P network의 대표적인 사례인 CAN [9] 네트워크를 가정해 보자((그림 1) 참조). 만약 공격자가 joining point로 19, 20, 21을 선택하여 참여하게 되면 이 공격자는 16번 노드의 오버레이 네트워크 접근을 제어할 수 있게 된다. 또한 다른 노드에서 16번 노드가 관리하는 정보를 얻기 위해 접속을 시도할 경우, 이 역시 공격자에 의해 제어될 수 있게 된다. 또한 공격자는 파일에 대한 접속을 제어할 수도 있다. 이와 관련된 공격인 sybil attack은 공격자가 많은 수의 합법적인 노드 ID를 획득하여 공격에 사용하는 방식을 사용한다.

Chord[10]와 Pastry[11] 같은 경우에도 자신의 노드 ID를 선택할 수 있다면, ID circle 상에 joining point를 선택할 수 있기 때문에 CAN에서와 동일하게 P2P 오버레이 네트워크 접속과 특정 파일에 대한 접속을 임의대로 제어할 수 있는 위협이 존재하게 된다.



(그림 1) Node ID 관련 공격 사례

나. Attacks on Message Routing

이미 설명된 바와 같이 DHT 기반 P2P 오버레이 네트워크에서는 각각의 peer들이 응용계층에서 검색 메시지를 전달하는 방식의 라우팅 기법을 사용하게 된다. 라우팅 관련 보안 공격은 메시지를 라우팅하는 과정에 참여하는 peer의 다음과 같은 행동으로 야기된다.

- 메시지를 전달하지 않고 임의로 폐기
- 메시지를 잘못된 위치로 전달
- 메시지를 위/변조하여 전달
- 거짓 정보를 반환
- 라우팅 테이블 업데이트 정보 위/변조

다. DoS Attack

DHT 기반의 오버레이 네트워크에서 서비스 거부 공격은 다양한 방법으로 발생할 수 있는데 가장 대표적인 두 가지에 대해 언급하고자 한다. 먼저, 공격자가 수많은 검색 메시지를 생성하여 희생자 노드(victim node)에게 전송하는 방법이 가능하다. 또한 검색 요구가 있을 때 검색된 모든 결과 자료에 대해서 그 소유자가 희생자 노드인 것으로 검색 요청 peer에게 반환을 한다면 희생자 노드로 트래픽이 집중될 것이다. 즉, 해당 피공격 peer는 심각한 성능 저하의 문제에 직면하게 될 것이다.

라. Rapid Join and Leave Attack

DHT 기반 P2P 오버레이 네트워크의 가장 큰 취약점으로 꼽을 수 있는 위협 중 하나가 rapid join and leave 공격이다. DHT 기반 P2P 오버레이 네트워크는 새로운 노드의 참여나 노드의 탈퇴 시에 다른 노드의 라우팅 정보를 갱신하는 과정이 필요하며, 이 과정에서 일부 메시지의 송수신이 필요하다. 이러한 노드의 참여/탈퇴를 의도적으로 짧은 시간

동안 여러 차례 반복하게 되면, 이에 대한 라우팅 정보 업데이트 메시지의 송수신을 위해 네트워크와 노드의 부하가 폭주하게 되어 결국 DoS 공격의 효과가 나타날 수 있다. 그러므로 본 공격을 넓은 범주에서의 DoS 공격으로 분류하는 것도 가능하다.

마. Storage and Retrieval Attack

본 공격 유형은 공격자가 자신이 파일 정보의 정상적인 소유자임에도 불구하고 아닌 것처럼 행동하거나 혹은 파일의 존재를 알려주면서도 파일에 대한 서비스는 제공하지 않는 등의 방식을 통해 data lookup을 방해하는 특성이 있다.

상기 '가'~'마'절에서 언급한 보안 위협 외에도 P2P 오버레이 네트워크의 정상 참여자가 정의된 프로토콜을 준수하지 않고 비정상적인 동작을 통해 의도하지 않게 야기되는 다양한 공격이 가능할 것이다.

7. 주요 보안 대응책

본 고에서 언급한 전형적인 P2P 네트워크에서의 보안 취약성에 대한 다양한 대응기술을 요약하면 <표 2>와 같다.

다음은 DHT 기반의 P2P 오버레이 네트워크 환경에서 고려될 수 있는 주요 공격 유형에 대한 대응

〈표 2〉 P2P 보안 취약성에 대한 주요 대응방안

공격 유형	대응 기술
Whitewashing	Persistent Peer ID 보장 Strict Model (Central Trusted Authority) 활용 Reputation Model을 통한 Cost vs. Penalty 기법 적용
ID Spoofing	접근 제어 (Access Control) 기법 활용 패킷 필터링을 통한 접근제어 취약점 서비스 사용의 제거 암호화 프로토콜 활용
MITM	상대 객체에 대한 안전한 인증 서비스 인증된 객체만이 패킷을 복호화 함 교환되는 메시지의 수정 여부 탐지 각 객체마다 Firewall, Anti-Virus 탑재 등록된 데이터의 위치 정보 오류 탐지
Privacy	PKI Infrastructure 분산환경에 적합한 자치적 관리구조

방안을 고려해 보자. 먼저, node ID 관련 공격에 대응하기 위한 방안으로 node ID 생성을 IP 주소와 공개키를 통해 유도하는 기법 또는 node ID를 인증할 수 있는 Trust Authority (CA) 서버를 두는 관리 구조 등을 고려할 수 있다. 또한 sybil attack을 방지하기 위해 node ID 당 요금을 부과하여 공격자의 네트워크 진입 속도를 늦추는 방안 및 node ID와 real world ID를 매핑시키는 기법의 검토도 가능하다.

라우팅 메시지 또는 테이블 관련 공격의 경우, 다중 해시 함수를 사용하여 키 정보를 복제하여 분산시키고 이에 대한 라우팅 경로를 다양화하는 방안 등도 제시되고 있다. 실례로, pastry 기반의 프로젝트인 PAST[12]의 경우 파일정보 복제 및 분산 기법을 채택하고 있다.

이를 요약하면 <표 3>과 같다.

〈표 3〉 DHT 기반 P2P Overlay Network에서의 보안 위협에 대한 주요 대응방안

공격 유형	대응 기술
Node ID Related	Node ID Derived from IP Address and Public Key Trust Authority (CA) 활용
Sybil Attack	Node ID 생성에 따른 과금 징수 Node ID와 사용실체를 실검증하는 방안
Message Routing	다중 해시 함수를 사용하여 키 분산복제 (예; PKI 기반의 전자서명 활용)

현재까지 DHT 기반의 오버레이 네트워크를 인터넷 정도의 범용적 확장성을 갖는 P2P 서비스에 실제 적용하여 응용되고 있지는 않은 실정이다. 그러나 DHT 기반의 오버레이 네트워크는 검색 효율성 측면에서 매우 뛰어나기 때문에 상기 기술한 주요 보안 이슈가 해결된다면 차세대 P2P 서비스로의 활용 가치가 더욱 높아질 수 있을 것이다.

Ⅳ. P2P 보안 기술 동향

P2P 프레임워크는 운용되는 형태에 따라 다음과 같이 크게 세 가지로 분류될 수 있다.

• 중앙 집중형

중앙 인덱스 서버를 두고 있는 Napster, 소리바다 등이 대표적임

• 분산형

- Structured: Chord, CAN, Pastry, Tapestry
- Unstrutured: Gnutella[13]

• 혼합형

Super peer/simple peer가 존재하는 Kazza[14]가 대표적인 사례임

상기 분류의 기준이 P2P 아키텍처의 운영 형태에 기초한 구분이라면, P2P 프레임워크의 보안은 신뢰정보(credential)를 관리하는 주체가 누가 되는가에 따라 중앙 집중형과 분산형 두 가지로 구분할 수 있다.

중앙 집중형 신뢰정보 관리 방식은 신뢰할 수 있는 서버가 정보의 생성/분배/인증/폐기 등 보안과 관련된 일련의 과정에 개입하는 형태를 의미한다. 반면에, 분산형 신뢰정보 관리 방식은 중앙 서버의 도움 없이 네트워크상에 분산되어 있는 노드간의 협업을 통해서 신뢰정보를 관리하는 형태를 뜻한다. 전자의 관리 방식의 경우는 이미 국내외의 인터넷 환경에서 매우 효과적으로 사용되던 방식이지만, 분산환경 기반의 P2P에서 신뢰정보 관리를 위해 중앙집중형이 직접적인 적용이 가능한지, 만약 가능하다 하더라도 그것이 보안 및 성능 측면에서 의미있는 것인지, 그렇지 않다면 새로운 분산형 관리 구조의 보안모델에 대한 검토가 필요한 것인지에 대한 보다 구체적인 논의가 필요한 시점이다.

1. 중앙 집중형 신뢰정보 관리

가. PKI 기반의 인증 모델

PKI 기반의 인증 기법은 공인된 서버로부터 신뢰정보를 부여 받는 형태이고, 상대에 대한 신뢰는 바로 이 신뢰정보를 발급받았다는 점에 의존한다. 그러나 PKI 방식의 확장성은 인증기관의 인증서 관리 형태에 따라 결정된다고 할 수 있기 때문에 인증서의 발급, 갱신, 폐기 등과 같은 PKI를 구성하는 요소들은 오히려 P2P 네트워크에 적용하는 데 제약 사항으로 작용할 소지가 크다고 할 수 있다.

이에 대한 좋은 사례로, JXTA를 소개하고자 한다. JXTA 기반의 P2P 네트워크의 경우 그룹 생성자가 인증기관의 역할을 수행할 수 있도록 하여 그룹에 참여하는 노드에게 X.509 인증서를 발급해 주는 형태의 인증서 관리가 가능하도록 설계된 특징이 있다. 이 방식은 소규모의 제한된 그룹에서 매우 강력한 인증 방법이 될 수 있고, 이에 따라 임의의 두 노드 간의 연결은 TLS 세션에 의해 암호화 될 수 있으나 개방된 P2P 환경에서는 그룹에 참여하는 노드 간에는 상대에 대한 신뢰정보가 결여되어 있기 때문에 이 방식을 글로벌 그룹에 적용하는 데는 제약이 있다.

나. 신뢰정보 관리 및 사용자 인증 기법

중앙 집중형 신뢰정보 관리 형태의 사용자 인증 기법을 채택하고 있는 대표적인 사례로는 이미 IT 분야에서 큰 관심의 대상이 된 Napster와 같은 파일 공유 P2P 응용 서비스와 VoIP 분야에서 서비스 시작 2년 반 만에 1억 명의 가입자를 유치하는 등의 큰 파장을 불러온 Skype를 언급할 수 있다.

PKI에서는 공인된 등록기관(RA)을 통해 오프라인으로 사용자를 등록한 후에 이용이 가능한데 반해 Thawte에서 발행하는 개인 인증서는 간단한 온라인 등록과 함께 이메일을 통한 간접적인 오프라인 사용자 인증을 병행하고 있다. 이러한 '다중 경로'를 이용한 사용자 인증 방식은 국내의 인터넷 환경에서도 쉽게 찾아볼 수 있는데, 네이트온과 같은 IM 서비스에서는 사용자의 휴대폰으로 단문 메시지(SMS) 형태로 인증 번호를 전송하는 것이 대표적이며 분산환경에서 ID와 실체를 확인할 수 있는 좋은 방안이 될 수 있지만 실소유자의 휴대폰이 타인에게 양도 또는 도용되지 않았다는 물리적 보안이 전제가 되어야 하는 현실적 한계를 갖고 있다.

다. P2P 환경에서의 신뢰정보와 사용자 인증 고려

지금까지 여러 가지 형태의 중앙 집중형 신뢰정보 관리에 따른 사용자 인증 방식에 대해 논의하였다. 전술한 바와 같이 이러한 기법들은 서버가 직간접적인 방법으로 사용자 인증에 관여하고, 또 그 결과를 다른 사용자에게 전달하여 사용자간 상호 인증이 가능하도록 하는 구조라고 할 수 있다. 이들 기술 중 일부가 P2P 서비스에 적용되어 이용되고 있으나, P2P를 위한 보안 기술이라기 보다는 인터넷 환경에서의 서버 의존형 보안 기술이 그대로 적용된 것이라고 할 수 있다. 따라서 이것을 P2P 환경에 적용할 경우에 여러 가지 제약이 따를 수 밖에 없다.

예를 들어, 단문 메시지를 이용하는 사용자 인증 기법은 국내의 인터넷 및 휴대전화망에 의존하고 있으므로 글로벌 네트워크 환경에서 적용하는 데 어려움이 있다. 이메일을 이용하는 Thawte의 인증 기법은 사용자가 임의로 다수의 이메일 주소를 생성하는 것이 가능하다는 점을 고려한다면 궁극적인 해결책이 될 수는 없을 것이다. Skype의 경우는 가장 개방적인 P2P 환경을 기반으로 하고 있어 아무런 사용자 인증을 제공하지 않는다. 따라서 악의적인 사용자는 무수히 많은 아이디를 보유할 수 있다.

P2P는 peer 노드간의 연결성을 최우선시 하기 때문에 기 언급한 바와 같이 그 운용 형태에 따른 분류가 무엇이냐 하는 점은 보안 기술과는 큰 관계가 없다고 할 수 있다. 따라서 본 고에서 대상으로 하고 있는 P2P 환경은 첫째, 신뢰정보를 관리하는 주체가 존재하지 않거나 분산된 형태, 둘째, 신뢰정보를 관리할 수 있는 서버가 존재하더라도 그 역할이 매우 제한적이고, 사용자에 대한 직접적인 인증을 수행하기 보다는 사용자간 상호인증에 도움을 주는 형태이다.

특히 사용자를 인증할 수 있는 서버가 존재하지 않는다는 점은 신뢰정보가 존재하지 않는다는 것을 의미하고, 따라서 사용자간에 상대방을 인증할 수 있는 매개체가 존재하지 않기 때문에 사용자간의 인증이 불가능하다. 이러한 상황에서 P2P 네트워크에 참여하는 노드에게 주어진 것은 상대방을 식별할 수 있는 고유한 아이디뿐이다. 즉 각 사용자는 상대 노드의 아이디에 의존하여 신뢰성을 판단하는 것이다. 따라서 P2P의 보안 기술은 아이디에 의존한 신뢰가부를 판단함에 있어 그 정확도를 높일 수 있는 다양한 형태의 기술로 정의할 수 있다. 다시 말해서 사용자의 인증을 통해 신뢰를 높이는 것이 기존 네트워크의 보안 모델이라고 한다면 P2P의 보안 모델은 상대방에 대한 인증 없이 아이디에 대한 신뢰를 높이는 것이다.

2. 분산형 신뢰정보 관리

가. 아이디 신뢰성

온라인 상에서의 아이디는 통신의 종단점(communication end-point)이 되기도 하고(예; 전화번호), 전송되는 프레임을 구분할 수 있는 인자가 되기도 하고(예; EAP 프로토콜의 identifier 필드), 상대의 네트워크 주소가 될 수도 있으며(예; IP 주소), 네트워크 토폴로지를 결정하는 요소가 되기도 한다(structured 방식의 P2P 오버레이 네트워크가 대부분 여기에 해당한다). P2P 환경이 개방된 네트워크임을 감안한다면, 온라인 상에서 사용자를 인식하기 위해 사용되는 아이디는 공개된 값이고, 아이디를 소유하고 있다는 것만으로는 사용자를 인증하거나 신원을 증명하는 데에 이용될 수 있는 어떠한 신뢰정보도 제공할 수 없다.

따라서 P2P 환경에서 사용자는 임의로 다수의 아이디를 생성하는 것이 가능해진다. 이러한 특성은 아이디에 대한 신뢰를 떨어뜨리는 결과를 가져오게 되고 다양한 형태의 보안 위협을 초래하게 된다. P2P 분야에서는 이러한 다수의 아이디 생성 및 그와 관련된 공격 기법을 sybil 공격이라고 정의하고 있다.

나. 아이디 소유권 증명 기법

CGA 방식에서 아이디는 그것을 생성한 사용자의 공개키와 강력한 보안적 결합을 이루고 있어 아

이디 검증자는 그 아이디를 생성한 사용자가 해당 아이디를 소유(ownership)하고 있으며 배타적(exclusiveness)으로 사용하고 있다는 것을 검증하는 방법을 제공해야 한다. CGA는 본래 IPv6용 주소를 생성하기 위한 기법으로 [15]에서 제안되었으며 이후에 RFC3972로 표준화된 것이다. 이와 유사한 아이디 생성 방식으로 SUCV가 있다.

여기에서 생성된 아이디가 가질 수 있는 범위를 줄여주는 기법이 부가적으로 필요하나, 사용자는 아이디 생성을 위해서 암호학적인 '퍼즐'을 풀어야 하는 형태이다. 즉 CGA에서는 생성된 아이디의 상위 p 비트가 0이 되도록 한다는 조건을 두고 있다. 따라서 이 조건을 만족하기 위해서 사용자는 반복적인 아이디 생성 알고리듬을 수행해야 한다.

CGA의 아이디 생성 기법은 아이디를 생성한 사용자가 그 아이디에 대한 소유권을 증명할 수 있는 매우 강력하면서도 간단한 방법을 제공한다.

[16]에서는 CGA와 유사한 방법을 이용하여 P2P 네트워크의 임의의 노드 간에 보안 연계(SA)를 생성하는 방안이 제안되어 있는데 다음과 같다. 두 노드 간의 보안 연계를 위해서는 해당 IP 주소와 아이디를 사용하고 있는 사용자임을 증명할 수 있어야 하는데, 이 증명을 위해서 우선 오프라인으로 사용자의 주소와 공개키 정보를 쌍방 간에 저장하는 형태이다.

이 프로토콜에서 해시와 전자 서명을 함에 있어 아이디와 IP를 이용하는 부분이 CGA에서 목표로 하고 있는 배타적 소유권을 제공하는 것이다. 여기에서 주의할 점은 실제 사용자 간에 인증은 오프라인에서 전달된 신뢰정보인 IP 값과 Hash(Nonce|ID|Key|IP) 값에 의존하여 결정이 된다는 점이다. 오프라인 과정이 없다면 위의 프로토콜은 CGA가 그러하듯이 배타적 소유권만을 제공할 수 있으나 상대방에 대한 인증이 결여되어 있기 때문에 보안연계가 불가능하다. 보안연계가 없는 프로토콜이 글로벌 네트워크에 적용될 경우 MITM 공격에 취약할 수밖에 없으며, ID spoofing 공격의 표적이 될 가능성이 있다.

다. 아이디 기반 암호화 및 전자서명 기술

아이디 기반 암호 기술(IBC)은 공개키 기반 암호 기법을 사용하는 데 있어 발생하는 문제점인 키 인증 문제, 즉 사용자와 공개키 간의 바인딩을 형성하여 주어진 공개키가 그 사용자의 공개키가 맞는다는 것을 검증해야 하는 절차와 이를 위하여 사용자의 공개키를 수집하거나 디렉터리에 보관해야 하는 문제점을 해결하기 위하여 제안된 방법이다.

이름에서 유추할 수 있듯이 아이디 기반 암호 기술은 사용자의 공개키/개인키 쌍을 생성하는 데 있어 기존의 방식이 일정한 크기의 바이너리 값을 공개키로 이용했으나 IBC에서는 손쉽게 구별할 수 있는 사용자의 아이디 정보를 공개키로 이용하게 된다. 예를 들면 'bob@abc.com'과 같은 이메일 주소가 공개키로 사용될 수 있다. 다시 말해서 고유성만 보장할 수 있다면 어떠한 문자 값이라도 공개키로 이용이 가능하다는 것으로 이메일뿐만 아니라 전화번호나 IP 주소 등이 이용될 수 있다. 요컨대, Bob이라는 사람에게 암호화된 메시지를 전달하고자 한다면 그의 공개키인 'bob@abc.com'을 이용하여 암호화할 수 있다는 것이다.

1984년 Adi Shamir에 의해 아이디 기반 전자서명 기법이 처음 제안되었으며[17] 최근에는 아이디 기반의 암호화 기법이 개발되었다. 아이디 기반 암호 기술은 본래 해결하고자 했던 키 인증 문제뿐만 아니라 다양한 형태의 아이디를 공개키로 이용할 수 있다는 점에서 P2P 보안 기술에 적용될 경우 매우 유용할 것으로 기대된다.

예를 들어 아이디를 생성하는 데 있어 사용자를 구분 지을 수 있는 홍채, 지문 등의 바이오 정보를 추가하여 그것을 공개키로 이용할 수 있다. 사용자의 바이오 정보를 해시한 값이 'D74123BC45'인 경우 아이디는 'bob@abc.com|D74123BC45'와 같이 사용될 수 있고 이것이 곧바로 Bob의 공개키가 된다. 이러한 방식은 전자여권과 같이 사용자의 신분을 확인할 수 있는 시스템 구축에 매우 유용할 수 있고, P2P와 같은 네트워크 상에서도 충분히 활용이 가능할 것으로 예상된다.

현재까지 개발된 아이디 기반 암호 기술의 한 가지 문제점은 공개키에 해당하는 개인키를 서버(KGC)가 생성하여 사용자에게 전달해야 한다는 것이다. Alice가 Bob에게 암호화된 메시지를 전달하기 위하여 그의 공개키로 'Bob@abc.com'을 이용하는 경우에, Bob은 그 공개키에 해당하는 개인키를 KGC로부터 받아서 메시지를 복호화 할 수 있다. 그러므로 Bob에게 개인키를 전달하기 위해서 KGC와 Bob 간에는 신뢰할 수 있는 통신 채널이 있어야 한다. Adi Shamir가 최초 제안한 방법은 스마트카드를 이용하여 개인키를 오프라인 방식으로 미리 전달하는 것이다. 현재까지 이 부분에 대한 대안은 제시되지 않고 있다.

P2P 상에서 KGC와 같이 모두가 신뢰할 수 있는 서버를 두고 신뢰할 수 있는 통신 채널을 통해 온라인으로 개인키를 전달하는 것은 어려운 문제일 수 있다. 그러나 기존의 서버가 사용자를 직접적으로 인증해 주는 역할을 수행하는 반면 KGC는 사용자 간의 암호 기술을 적용하는 데 있어 필요한 파라미터만 설정해 주기 때문에 사용자 간의 상호작용에 도움을 주는 역할을 수행하는 것으로 볼 수 있다. 이런 운용상의 문제점이 존재하기는 하지만 아이디 기반 암호 기술은 P2P 상에서 사용자의 아이디와 보안 기술을 결합할 수 있는 강력한 도구가 될 수 있을 것으로 기대된다.

라. 임계 암호 기반 보안 기술

임계 암호 시스템(threshold cryptosystem)[18]은 비밀 분산(secret sharing)을 구현하기 위한 방법으로 하나의 사용자가 수행하던 작업을 다수의 사용자에게 나누어 공동 작업을 수행할 수 있도록 하는 방식이다. 따라서 원래의 개인키가 수행하던 작업을 복원하기 위해서는 일정 수 이상의 사용자가 모여서 공동 작업이 이루어져야 하므로 공격자가 이러한 시스템을 공격하는 데 어려움이 있게 된다. (t, n) 임계 방식의 경우 비밀을 n명의 사용자에게 나누고, 그 중 t ($t < n$) 명의 공동 작업에 의해서 원래 비밀 값을 복원하거나 비밀 값을 통해 수행할 수 있는 기능을 복원할 수 있도록 하는 방식이다.

1979년 Adi Shamir가 최초 제안한 방식은 Lagrange의 다항식 보간법(polynomial interpolation)을 이용한 방식이다. 1979년 George Blakeley가 제안한 방식은 다차원 평면이 만나는 한 점을 분산 정보로 하여 비밀 분산에 참여하는 사용자에 각 평면에 대한 정보를 나누어 주는 방식이다.

최근에 이러한 비밀 분산 기법을 이용하여 CA의 인증서 발행 기능을 분산하는 기법이 제안되고 있다. 즉 네트워크에 참여하는 노드에 대해서 기존의 네트워크 멤버 중 t명이 서명 정보를 제공할 수 있다는 것이다. 이러한 서명 정보는 사용자의 공개키에 대한 서명이 될 수도 있고 사용자에 대한 신뢰 정보로 이용될 수도 있다. 이러한 방식이 다수의 아이디를 생성하는 sybil 공격에 대해서 취약할 수밖에 없기는 하지만 P2P 네트워크에 참여하는 노드를 위해 인증서 발행 기능뿐만 아니라 아이디 기반 암호 기술에서의 KGC 기능을 분산하는 형태로 발전한다면 두 암호 기술이 갖고 있는 장점을 극대화하면서 상호 기능을 보완할 수 있을 것으로 기대된다.

V. 결론

얼마 전까지만 해도 특히 저작권 문제 등이 대두되면서 P2P 서비스가 '문제아' 정도로 인식되었던 것은 사실이다. 그러나 최근 들어서는 P2P를 응용 인프라 구축을 위한 하나의 통신계층으로 보자는 시각이 등장할 정도로 인터넷에서 매우 대중화된 서비스가 되어 버렸다. 실제로 무척이나 다양한 응용이 P2P를 기반으로 서비스되고 있고, P2P가 인터넷의 가장 많은 트래픽을 차지하고 있는 것이 현실이다. 본 고에서는 P2P 기술에 대한 표준 및 연구 동향과 P2P 보안 취약성 및 대응 기술에 대해 논의하였다. 본 고에서도 기술하였듯이 P2P 네트워크의 특성상 – dynamic and open network – 중앙 집중형 보안 메커니즘을 그대로 적용하는 것은 어려우며, 분산 환경에 적용 가능한 형태의 보안기술이 필요할 것이다.

약 어 정 리

3GPP	The 3rd Generation Partnership Project
ALM	Application Level Multicast
BoF	Birds-of-a-Feather
CA	Certificate Authority
CGA	Cryptographically Generated Address
CMIP	Common Presence and Instant Messaging
DHT	Distributed Hash Table
DM	Domain Manager
DMF	Domain Management Function
DMMP	Dynamic Mesh-based overly Multicast Protocol
DoS	Denial of Service
EMF	Element Management Function
IBC	Identity Based Cryptography
ID	Identity
IETF	Internet Engineering Task Force
IM	Internet Message
IMP	Internet Message and Presence
IRPs	Integration Reference Points
IRTF	Internet Research Task Force
ITU-T	International Telecommunication Union Telecommunication Standardization
KGC	Key Generation Center
MITM	Man-In-The-Middle
OM	Overlay Multicast
OpenPGP	Open Pretty Good Privacy
P2P	Peer-to-Peer
PCG	Project Co-ordination Group
PKI	Public Key Infrastructure
RA	Registration Authority
RG	Research Group
SA	Security Association
SAM	Scalable Adaptive Multicast
SASL	Simple Authentication and Security Layer
SEND	Secure Neighbor Discovery
SIMPLE	SIP for Instant Messaging and Presence Leveraging Extensions
SIP	Session Initiation Protocol
SSL	Secure Sockets Layer
SUCV	Statistic Uniqueness and Cryptographic Verifiability
TLS	Transport Layer Security
TM	Telecommunication Management
TSGs	Technical Specification Groups
TTP	Trusted Third Party
VoIP	Voice of IP
XMPP	Extensible Messaging and Presence Protocol
WG	Working Group

참 고 문 헌

[1] K. Singh and H. Schulzrinne, "Data Format and Interface to an External Peer-to-Peer Network for SIP Location Service," draft-singh-p2p-sip-00, IETF, Mar. 2006.

[2] M. Day et al., "Instant Messaging/Presence Protocol Requirements," RFC2779, IETF, Feb. 2000.

[3] T. Aura, "Cryptographically Generated Addresses (CGA)," RFC3972, IETF, 2005.

[4] http://www.pgpi.org/

[5] http://www.cs.umd.edu/projects/p2prg/

[6] http://www.samrg.org/index.html

[7] Web Stie, http://www.3gpp.org/About/3GPP.ppt and 3GPP TR 32.806 V7.0.0 (Release: June 2006)

[8] Michal Feldman et al., "Free-Riding and Whitewashing in Peer-to-Peer Systems," *the 3rd Annual Workshop on Economics and Information Security (WEIS2004)*, 2004.

[9] Sylvia Ratnasamy et al., "A Scalable Content-Addressable Network," *SIGCOMM'01*, San Diego, CA. USA, Aug. 27-31, 2001.

[10] Ion Stoica et al., "Chord: A Scalable Peer-to-Peer Lookup Service for Internet Applications," *SIGCOMM'01*, San Diego, CA. USA, Aug. 27-31, 2001.

[11] Antony Rowstron, "Pastry: Scalable, Decentralized Object Location and Routing for Large-scale Peer-to-Peer Systems," *the 18th IFIP/ACM Int'l Conf. on Distributed Systems Platforms (Middleware 2001)*, Heidelberg, Germany, Nov. 2001.

[12] A. Rowstron and P. Druschel, "Storage Management and Caching in PAST, a Large-scale, Persistent Peer-to-Peer Storage Utility," *in Proc. of the 18th ACM Symp. on Operating Systems Principles (SOSP'01)*, 2001, pp.188-201.

[13] http://www.gnutella.com/

[14] http://www.kazaa.com/

[15] G. O'Shea and M. Roe, "Child-proof Authentication for MIPv6 (CAM)," *SIGCOMM Comput. Commun. Rev.*, Vol.31, 2001, pp.4-8.

[16] S. Čapkun, J.-P. Hubaux, and L. Buttyán, "Mobility Helps Peer-to-Peer Security," *IEEE Transactions on Mobile Computing*, Vol.5, 2006, pp.43-51.

[17] A. Shamir, "Identity-based Cryptosystems and Signature Schemes," *Presented at Proc. of CRYPTO 84 on Advances in cryptology*, Santa Barbara, California, United States, 1985.

[18] A. Shamir, "How to Share a Secret," *Commun. ACM*, Vol.22, 1979, pp.612-613.