주 제

P2P 보안 기술

한국전자통신연구원 나재훈, 고선기, 구자범, 권혁찬, 문용혁

차례

I. 서 론

P2P (Peer to Peer) 용어는 아직 우리에게는 생소한 용어이다. 그러나 Napster, Gnutellar, eDonkey, Kazaa, Skype, 소리바다, 푸르나와 같은 것은 너무나 친숙한 용어가 되어버렸다. 이렇듯 인터넷에 커다란 변화가 있다는 것을 대다수의 사람들은 알지 못하는 사이에 P2P는 우리의 실생활에 이미 깊숙이 자리하고 있는 것이다.

이러한 변화를 명확히 규정하기엔 어려움이 있지만 두드러지는 특징은 패러다임의 전환이 일어나고 있다는 것이다. 즉 분산환경에서 불필요한 제삼자의 개입이 없이, 간편하고 이해가 쉬운 논리적 관계를 실현한 개인-대-개인으로 통신 인프라의 구축이라는 것이다. 이렇듯 P2P는 인터넷환경에서 기존의 클라이언트/서버 서비스를 능가하고, 사용자 입장에서 편리하고 효율적인 인터넷의 새로운 창을 제공하고 있는 것이다. P2P는 커뮤니티를 자연스럽게 구성하며 커뮤니티의 요구에 따라 서비스를 제공할 수 있는 폐쇄적 공간을 제공할 수 있다. 즉 열린 인터넷 공간에서 이해관계가 성립되는 불특정 다수간에 망 운영자의 간섭 없이 커뮤니티를 구축 할 수 있다는 커다란 장점을 갖고 있으며 또한 분산처리환경에 적합한 능력을 보유하고 있다는 것이다.

이러한 커뮤니티 환경에서 두각을 나타내고 있는 P2P 서비스는 인스턴트 메시지, FS (File Sharing), VoIP (Skype), 인터넷방송 (UCC, PPLive, PP Stream)등이 있으며 또한 Seti@home과 같이 저렴한 투자비용으로 분산처리 능력이 극대화된 협업 서비스 (대용량 계산, 대용량 메모리, Virtual Office)와 같이 향후 그 추이가 주목 되는 서비스들이 있다. 본 논문에서는 P2P 인프라와 서비스의 기술동향을

소개하고 이러한 환경에서 새롭게 대두되고 있는 보안 취약성을 분석하여 이에 대응할 수 있는 보안기술의 동향을 소개한다. 또한 P2P 기술의 국제적 현 위치를 알리는 표준동향을 포함하였다.

II. P2P 인프라 및 서비스

A. P2P 기술동향

P2P 기술은 크게 P2P 네트워크 인프라 구축을 위한 프레임워크기술과 응용 개발 기술로 구분할 수 있다.

• P2P 프레임워크 구축 기술

P2P 네트워크 인프라는 그 구성 방식에 따라 Structured 방식과 Unstructured 방식으로 구분할 수 있다. 또 자원 검색 방식에 따라 Centralized 구조(혹은 Hybrid 구조)와 Distributed 구조로 구분이 되기도 한다. P2P 네트워크에서는 기존의 클라이언트/서버 모델과는 달리 자원이 다수의 피어에 분산되어 있기 때문에, 여러 자원들을 관리하고 검색하는 기술이 필수적이다. 이러한 P2P Topology 구성, 자원 및 서비스 디스커버리 기법은 P2P 네트워킹에서 요구되는 주요 기술로서 현재 관련 연구가 활발히 진행되고 있는 추세이다.

초창기에는 Gnutella와 같은 Unstructured P2P를 기반으로 하는 디스커버리 기법에 대한 연구가 많이 진행 되었다. Flooding에 의존하는 Gnutella와 같은 방식은 너무 많은 메시지를 생성하여 네트워크 효율성 측면에서 문제를 발생시키기 때문에 이를 보완하기 위한 기법이 다수 제안되었다. 이 분야에서 특히 연구가 활발한 기관은 Stanford 대학이다. Stanford 대학에서는 이와 관련하여 Directed BFS technique, Iterative Deepening technique, Routing Indices, Role Differentiation, GUESS protocol 등의 기법들을 제안하였다. [1]

Structured P2P 오버레이 네트워크 구축기술은 Unstructured 방식에 비해 비교적 최근에 제안된 P2P 프레임워크 구축 기술이다. Structured P2P는 주로 DHT(Distributed Hash Table)을 기반으로 구축되는 추세이다. DHT 기반 오버레이 네트워크는 검색의 효율성을 높이고자 P2P 오버레이 네트워크에 구조적인 특성을 부여한 것이다. 대표적인 프로토콜로 Chord, Pastry, Tapestry, CAN 등이 있다. DHT 기반 오버레이 네트워크는 초창기에는 Distributed Storage, File sharing, Web caching 등에 응용 되었으며, 최근 들어서는 P2P 기반의 multicast 서비스를 제공하기 위한 Tree 생성 및 관리 기법으로도 많이 응용 되고 있다.

DHT를 사용하지 않는 Structured P2P 네트워크 구축 기술로 P-Grid[2] 방식이 있다. 이 방식은 Gridella 응용에서 사용된 구조이며, 이진 트리 기반의 P2P 네트워킹 구조를 갖는다. 이 방식은 self-organization, decentralized load balancing, efficient search 등의 장점을 갖고 있지만, 분산된 형태의 이진 트리 구축에 대한 오버헤드가 매우 크다는 문제점을 안고 있으며 보안 측면에서는 악의적인 노드의 존재에 대해 매우 취약하다는 문제가 있다.

그 밖에 P2P 프레임워크 구축을 위한 middleware를 개발하는 대표적인 프로젝트로 Sun Microsystems에서 진행하는 JXTA 프로젝트[3]가 있다. JXTA는 공개 소프트웨어 프로젝트로 진행 중이며, 80개 이상의 프로젝트에서 JXTA를 이용하고 있으며, Nokia 등의 유수 기업과 유수한 대학들이 JXTA 커뮤니티에 다양하게 참여하고 있다.

• P2P 응용 개발 기술

P2P 네트워크는 현재 VoIP, Streaming service,

web caching, file sharing 등 매우 다양하게 응용 되고 있다. P2P 프레임워크를 기반으로 이러한 각각의 응용을 위한 기술 개발에 박차를 가하고 있는 상황이다.

B. P2P 서비스 국내외 동향

P2P 서비스는 초창기에는 IM(Instant Messaging), File Sharing 응용으로 시작되었으나, 현재에는 매우 다양한 형태의 P2P 응용이 출현하고 있다. <표 1>은 현재 서비스 되고 있는 다양한 P2P 서비스의 종류를 보여준다.

〈표 1〉 P2P 서비스 종류

서 비 스	사 례
P2P file systems	Ivy, Kosha
P2P archival systems	Oceanstore, Past, CFS
P2P file sharing system	BitTorrent
Multicast systems	SCRIBE
P2P web caching	Squirrel, Coral
P2P DNS	CoDNS, CoDoNS
Internet routing	RON
Next generation Internet Architecture	I3
Generic Binding Service	OpenDHR, SFR
Multimedia Streaming	PPlive, PPstream
VoIP	Skype
Game	KartRider

국내의 경우 P2P 서비스는 주로 IM, File sharing에 집중되어 있는 편이다. 현재 국내에는 네이트온, 버디버디, 쿨메신져 등의 인스턴트 메시징 서비스를 제공하는 업체와 소리바다, 프루나, 고부기 등의 파일 공유 서비스를 제공하는 업체들이 있다. IM 서비스의 경우 초기에 제공하던 단순한 채팅 서비스를 넘어 그룹웨어와의 연동, SSO, Multi-download, Relay Up&Down 등의 다양한 기능이 추가되는 추세이다. 국내 업체인 그래택은 P2P형 파일공유 서비스인 구루구루를 단순 파일공유 서비스에서 메신저와 고화질영화 VOD 서비스 등이 결합된 P2P 기반 토털 엔터테인먼트 서비스로 전환 시키려고 준비 중에 있으며, 와이즈피어[4]는 콘텐츠 유통 시스템인 고부기(GoBoogie)에 nDRM을 적용하는 등 지속적인 기능 강화를 진행 중에 있다.

또한 국외의 경우 매우 다양한 형태의 P2P 서비스를 제공하고 있다. MSN 메신저와 같은 IM, e-Donkey와 같은 File sharing 응용 외에 VoIP, Multimedia Streaming, web caching, P2P Game 등 다양한 응용 서비스가 제공되고 있다.

P2P 기반의 VoIP 서비스 업체인 Skype는 세계 최대의 인터넷 전화 업체로 성장하였으며, 자사의 인터넷 전화 이용자가 출시 2년 6개월 만에 1억명을 돌파했다고 밝히기도 하였다. 이는 전세계 인터넷 이용자 8억 6천만 명의 12%에 달하는 수치이다. 2005년 9월 eBay는 Skype를 26억 달러에 인수하였다.

또한 최근 들어 P2P를 Multimedia streaming 서비스에 응용하는 사례가 급증하고 있다. 올 초에는 헐리우드 메이저 영화사들이 P2P 네트워크를 이용한 영화/TV 프로그램 유료시청 서비스를 제공하겠다고 밝히기도 하였다. <표 2>는 현재 서비스되고 있는 P2P 기반 멀티미디어 스트리밍 서비스의 목록 중 일부이다[5].

〈표 2〉 P2P 기반 Multimedia Streaming System

Streaming System	License	Language	OS	Supported Multimedia
Peercast	GPL (Open Source)	C++	Windows, Linux, Mac OSX	Win. Media, NullSoft vid. Theora video
Freecast	GPL (Open Source)	Java	Any platform that supports Java Runtime Environment	Theora video
ACTLab TV	GPL (Open Source)	Java	Windows, Mac.	All video codecs supported by the VideoLan open source player

Streaming System	License	Language	OS	Supported Multimedia
ESM (End System Multicast)	Free software	C/C++	Windows, Linux	
Vatata	Free software	C/C++	Windows, Linux	WMV/WMA/ ASF
P2P-Radio	GPL (Open Source)	Java	Any platform that supports Java Runtime Environment	NullSoft vid.
Stream 2 Stream	GPL (Open Source)	Java	Any platform that supports Java Runtime Environment	MP3, NSV, Ogg Vorbis
Streamer P2P	Close	C++	Windows	NullSoft vid. Theora video
Abacast	Close	C++	Windows	WMV/WMA/ mp3
RawFlow	Close	C++	Windows	WMV/WMA/ mp3/real media
PPlive	Close	C++	Windows	Win. Media, Real Media
Pcast	Close	C++	Windows	Win. Media
PPstream	Close	C++	Windows	Win. Media, Real Media
TVants	Close	C++	Windows	Wind. Media

미국의 정보기술비즈니스 전문지인 Red Herring은 2006년 기술 분야의 10대 동향으로 온라인 게임의 운용 스타일이 P2P 형태로 변경하는 것과 비디오 콘텐츠 활성화 부분에서 P2P를 이용한 프라이빗 스크리닝(Private Screening; 선택된 사용자에게 보여지는 영화나 텔리비젼 영상) 분야를 선정하였다.

이제 게임, 멀티미디어 스트리밍, 파일 공유, 전자거래, 인터넷 쇼핑, 협업 등 인터넷에서 가능한 서비스들이 점차 P2P 인프라 상에서 제공되고 있는 추세로 점차 진화하고 있으며, 향후 유비쿼터스 망 구축 시 P2P 프레임워크 기술은 핵심 네트워킹 기술로 등장할 것으로 예상된다.

III. P2P 보안 취약성

P2P 보안 취약성을 분석하기 위해서는 먼저 분산환경이라는 것을 염두에 두어야 한다. 즉 분산처리의 자치적 성격을 갖는 컴퓨팅 환경에서 취약성을 분석하여야 한다. 이것은 기존의 보안 메커니즘에 분산 환경으로 인한 추가의 취약성과 기존의 보안 메커니즘의 변이에 해당되는 것으로 분류된다. 먼저 ID 관련 취약성을 검토하고 다음으로 통신로상에서의 취약성을 검토하기로 한다.

1. Whitewashing

현재 인터넷에서도 큰 문제점을 야기시키고 있는 취약성이다. P2P 환경에서도 ID에 대한 실체의 검증이 없는 경우에는 더욱 큰 어려움을 야기 시킬 수 있는 취약성이다. 즉 단순히 온라인상에서 주민등록번호로 인증을 하고 ID 발급을 하면, 본인의 동의 없이 도용/오용된 주민등록번호인 경우에 수많은 ID의 생성을 야기시킬 뿐만 아니라 악의적 이용자의 자유로운 인터넷 출입을 허용하는 것이다.

PKI (Public Key Infrastructure) 와 같은 인증을 위한 인프라가 있지만 실체확인을 위하여 F2F (Face-to-Face) 검증을 하여야 하므로 P2P와 같은 분산환경에서는 불가능한 방법이다. P2P 서비스를 위하여 현재의 은행에서 F2F 검증을 대행하여야 하며, PKI 기반의 인증서가 없는 사람은 P2P 서비스를 받을 수 없다는 문제점이 발생된다.

2. ID Spoofing

전세계적으로 분산되어 있는 인터넷에서 ID 발급이 자유롭게 허용되어 있기 때문에 ID에 대한 추적이 어렵다. 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 Verifiability를 강화하여야 한다

3. Repudiation

ID에 대한 신뢰성이 없으므로 ID를 가지고 사이버 공간에서의 어떠한 행위에도 책임이 없는 문제점을 야기 시킨다. ID를 정당하게 발급받아 사용하고서 본인이 사용하지 않았다고 거짓말을 해도 실체를 검증하지 못하므로 해당 ID가 사이버공간에서 한 행위에 대하여 최종 부인을 할 수 있는 여지를 남기고 있다.

4. MITM(Man in the Middle) 공격

분산 인터넷 환경에서 정당하게 ID를 발급 받아 사용하는 경우에도 보이지 않는 사이버 공간에서 상대방이 내가 알고 있는 ID를 사용하고 있는 상대가 아닌 경우가 있다. 이런 경우는 키분배가 신뢰적 공간에서 이루어지지 않기 때문에 더욱 문제를 일으킨다. PKI가 대안으로 떠오를 수 있지만 분산환경에서 거대한 수의 이용자들의 ID 발급(F2F 문제점 발생) 문제점, 국제간의 PKI 연동 문제점 그리고 쌍방간의 키 생성에서 교환에 이르기까지 제 삼자의 도움을 받아 처리되어야 하므로 분산환경에 부적합한 문제점을 보이고 있다.

5. Privacy

P2P는 분산환경이 되면서 개인의 정보가 더 위협을 받는 환경이 되었다. 누가 누구의 정보를 사용/공유 할 수 있는 지에 대한 정의도 없으며 누가 관리를 하느냐 하는 것 조차 규정된 것이 없다. 이러한 환경에서 개인의 정보가 불필요하게 네트워크나 서비스 공급자에게 제공되거나 관리되어서는 안된다. PKI는 개인정보보호를 위한 훌륭한 보안 인프라 임에는 의심할 여지가 없다. 그러나 인증서를 발급 받기까지 제공해야 하는 개인 정보의 양이 불필요하게 많다는 비판이 있으며, 이러한 정보가 공개키를 포함하여 TTP(Trusted Third Party)에 수록되어 있다는 것에 대한 보안상의 우려를 낳고 있다. 즉 개인정보보호를 하기 위하여 구축된 PKI 가 오히려 개인정보보호를 쉽게 얻을 수 있는 서버를 구축하게 된 것이다. 물론 외부에서의 공격을 효과적으로 방어하면 되겠지만, 우려의 많은 부분은 서버를 관리하는 주체로부터의 오용이 큰 비중을 차지한다. 즉 정보를 불필요하게 집중화 시키는 것에 대한 거부감을 일으키는 것이다. 분산환경에서의 개인정보보호는 해당되는 당사자간에만 정보를 제공하고 처리하는 자치적 관리구조를 구축하여야 한다. 그래야 정보가 공개되어도 국지적 양상을 보이며 그 피해가 최소화 될 수 있다.

또한 통신로상의 정보의 유출과 변조의 취약성은 P2P 환경에서도 공히 상존하는 문제점이다.

IV. P2P 기술 표준동향

P2P 관련 표준화 활동은 IETF (Internet Engineering Task Force)와 ITU-T의 Telecommunication Standardization Sector와 같은 국제 표준화 기구들을 중심으로 이루어지고 있다. 본 장에서 그 활동에 관한 대략적인 개요를 설명하기로 한다.

1) IETF

P2P-SIP WG는 65차 회의에서 BOF(Birds-of-a-Feather) 미팅이 진행되어 현재 그 구성이 진

행 중인데, 본 작업그룹의 목적은 세션 설치/관리가 중앙서버보다는 단말들의 집합체에 의하여 완전히 또는 부분적으로 처리되는 설정에서의 SIP(Session Initiation Protocol) 세션 이용을 위한 메커니즘과 가이드라인을 개발하는 것이며, 이것은 서비스 공급자의 프록시들에 의존하는 재래식 SIP 접근의 대안이 될 수 있다. SIP에 P2P 기술을 도입하려는 주된 이유는 P2P의 확장성과 서버 유지비용의 절감이다. 수백만 개 Peer들의 등록과 위치정보를 관리해야 하는 SIP 서버들의 역할을 P2P가 대신하도록 하려는 것이다 [6].

또한, SIMPLE(SIP for Instant Messaging and Presence Leveraging Extensions) 작업그룹은 IMP(Instant Messaging and Presence) 서비스에 적합한 SIP 응용의 표준화에 초점을 맞추고 있으며 IMP(RFC2779), CMIP(Common Presence and Instant Messaging)의 요구사항을 만족시키는 형태로 진행되고 있다. 이와 관련하여 본 작업그룹에서 2006년 8월 현재 등록된 RFC는 모두 8건이다.

XMPP WG (Extensible Messaging and Presence Protocol)는 IM의 표준을 제정하기 위한 작업그룹으로서, 이를 위해 security 기능이 추가된 XMPP 프로토콜의 표준화 작업을 진행하였다. 또한 채널 암호화를 위해 SASL(Simple Authentication and Security Layer)과 TLS(Transport Layer Security)/SSL(Secure Sockets Layer)을 사용하도록 규격을 정의하였으며, 개체 암호화를 위해 OpenPGP를 사용하도록 규격을 정의하였다. XMPP WG는 표준화 작업을 완료한 뒤 2004년 10월 종결되었다. 본 작업그룹에 의해 등록된 RFC는 모두 4건이다.

SEND WG(Secure Neighbor Discovery Working Group) 작업그룹의 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 서명 키 (Public Signature Key)를 IPv6 주소에 적재 (Binding)하는 방법을 정의하고 있으며, 이를 위한 특별한 주소로 공개키와 부가적인 파라미터를 암호적 기법의 단방향 Hash 함수에 적용하여 생성한 CGA(Cryptographically Generated Address) [7]를 사용한다. 즉, IPv6 주소로부터 전달된 메시지는 첨부된 공개키, 부가적인 파라미터 그리고 관련된 비밀키를 이용한 서명을 통해 보호 받을 수 있게 된다. 특히 SEND 프로토콜의 이러한 기법은 CA(Certification Authority) 또는 별도의 보안 인프라 없이 IPv6 네트워크 상의 보안된 메시지 교환을 가능케 한다는 점에서 그 의의가 있다. 현재 본 작업그룹은 3건의 RFC 문서를 등록한 후 2004년에 종료되었다.

2) IRTF

P2PRG(Peer-to-Peer Research Group) [8]는, IRTF(Internet Research Task Force)의 12개의 연구그룹(RG)들 중 하나로, 2003년 말에 시작되었으며, 작업그룹에 비해 상대적으로 오랜 기간 동안 안정적으로 연구를 수행한다. P2PRG의 설립 목적은, 연구자들에게 근본적인 P2P관련 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 진행 중이다. P2P RG 아래에는 더욱 세분화된 연구를 위한 여러 Subgroup들이 존재한다.

SAM RG(Scalable Adaptive Multicast Research Group) [9]은 많은 멀티캐스트 그룹과 네트워크 자원의 참여를 전제로 하는 확장성이 우수하

고 적응성이 뛰어난 멀티캐스트 프로토콜에 관해 집중하고 있는데, 그 주요한 연구 주제로는 ALM (Application Layer Multicast), OM(Overlay Multicast), 기존의 IP 네이티브 멀티캐스트뿐만 아니라 이를 혼용한 하이브리드 방법론(i.e. P2P Overlay Network)을 포함한다. 올해 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 DMMP(Dynamic Mesh-based overlay Multicast Protocol)에 관한 초안(draft-lei-samrg-dmmp-00)을 제출된 바 있다. 현재 68차 회의 및 P2PM07 (Workshop on Peer-to-Peer Multicasting)을 차기 주요 일정으로 예정하고 있다.

3) ITU-T

ITU-T의 특정화된 13개의 SG(Study Group) 중 SG 17 은 보안, 개발언어, Telecommunication 소프트웨어 분야의 표준을 담당하고 있으며, 그 아래에 보안 통신 서비스 분야를 담당하는 Question이 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 담당하고 있다. 올해 4월 제주도에서 개최된 SG17-Q.9 회의에서는 이들 프로젝트에 관련하여 총 6건의 기고서가 제출되었는데, 한국에서 'P2P 오버레이 네트워크에서의 Secure Routing', '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.

4) 3GPP

3GPP[10]는 PCG (Project Co-ordination Group)을 중심으로 하위 4개의 TSGs (Technical Specification Groups)으로 구성되어 있는데, 이중 TSG Service and System Aspects의 하위그룹인 TSG SA WG5 Telecom Management에서는 기존의 TM (Telecommunication Management) 아키텍처에 P2P 인터페이스를 추가하기 위한 기법 및 종전의 IRPs (Integration Reference Points)를 본 구조에 적용하기 위한 방법론에 대해서 표준화된 문서를 작성하고 있다. Sub-net을 위해 EMF (Element Management Function)와 DMF (Domain Management Function)을 제공하는 DM (Domain Manager)는 P2P 인터페이스를 통해 다른 Peer DMs과 협력적인 도메인 관리 기능을 제공할 수 있다는 것이 본 작업그룹의 주요한 골자를 이루는 논지이다. P2P 인터페이스는 여러 개의 IRPs로 나누어 질 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.

V. P2P 보안 기술

P2P 프레임워크를 운용되는 형태에 따라 중앙 집중형 (Napster, 소리바다), 분산형 (structured (Chord, CAN, Pastry, Tapestry) 또는 unstructured (Gnutella)), 그리고 혼합형 (Kazza)의 세 가지로 구분할 수 있다면, P2P 프레임워크의 보안은 다시 신뢰정보 (credential)를 관리하는 주체가 누가 되는가에 따라 중앙 집중형과 분산형으로 구분할 수 있다.

중앙 집중형의 신뢰정보 관리 방식은 신뢰할 수 있는 서버가 정보의 생성/분배/인증/폐기 등 보안의 제반 과정에 개입하는 형태를 말한다. 분산형 은 이러한 서버의 도움이 없이 네트워크상에 분산되어 있는 노드간에 또는 그들 간의 협업에 의해서 신뢰정보를 관리하는 경우를 의미한다. 중앙 집중형은 이미 국내외의 인터넷 환경에서 매우 효과적으로 사용되던 방식임을 알 수 있다. 그러나 P2P 환경에서 신뢰정보 관리를 위해 중앙 집중형이 그대로 적용 가능한지 여부 또는 분산형과의 비교에 대한 검토는 제대로 이루어지지 않고 있다.

A. 사용자 인증 및 아이디 인증

1) PKI 방식의 인증 모델

PKI 기반의 인증 기법은 공인된 서버로부터 신뢰정보를 부여 받는 형태이고, 상대에 대한 신뢰는 바로 이 신뢰정보를 발급받았다는 점에 의존한다. 인증기관(CA; Certificate Authority)은 인증서의 발급, 갱신, 폐기 등에만 관여하고, 사용자간의 인증과정에는 관여하지 않으므로, 오프라인으로 동작하는 인증서버로 볼 수 있다. 따라서 이 기법은 온라인에서 서버의 도움 없이 상대방을 인증할 수 있는 매우 강력한 메커니즘을 제공한다. 그러나 PKI 방식의 확장성은 인증기관의 인증서 관리 형태에 따라 결정된다고 할 수 있기 때문에, 인증서의 발급, 갱신, 폐기 등 PKI를 구성하는 요소들은 P2P 네트워크에 적용하는데 제약 사항이 될 수 있다.

기업 내에서 운영되는 사설(private) 인증기관 기업의 구성원에게만 인증서를 발급하는 정책을 시행할 수 있는데, 이에 따라서 인증기관으로부터 인증서를 발급 받았다는 것은 곧 믿을 수 있는 인증된 사용자임을 의미한다. 또한 직원에게 스마트카드 형태의 인증서를 발급 하여 보다 강력한 인증 도구로 이용할 수 있다. 그러나 이러한 사설 인증기관의 운용은 기업망과 같이 보안 정책의 수립 및 시행이 체계적이고, 사용자가 기업의 구성원으로 한정되기 때문에 가능하다고 할 수 있다. 즉 신뢰정보에 대한 관리가 철저한 경우만 가능하다.

JXTA (juxtapose의 줄임 말로 SUN Microsystems가 주도하여 개발한 P2P 프레임워크의 명칭)를 기반으로 하는 P2P 네트워크는 그룹 생성자가 인증기관의 역할을 수행할 수 있도록 하여, 그룹에 참여하는 노드에게 X.509 인증서를 발급해 주는 형태의 인증서 관리가 가능하다. 이 방식은 소규모의 제한된 그룹에서 매우 강력한 인증 방법이 될 수 있고, 이에 따라 임의의 두 노드간의 연결은 TLS 세션에 의해 암호화 될 수 있다. 그러나 개방된 P2P 환경에서는 그룹에 참여하는 노드간에는 상대에 대한 신뢰정보가 결여되어 있기 때문에 이 방식을 글로벌 그룹에 적용하는 데는 제약이 있다.

2) 신뢰정보 관리 방식에 따른 다양한 인증 모델

최근 IT 분야에서 관심의 대상이 되고 있는 소리바다와 같은 파일 공유 형태의 P2P 응용 서비스와 이미 그 규모만으로도 인터넷 전화 (VoIP) 분야에서 큰 파장을 불러온 Skype의 사용자 인증기법은 중앙 집중형 신뢰정보 관리 형태를 띠고 있다.

소리바다가 갖고 있는 보안 모델은 아이디와 패스워드에 의해 서비스를 이용하는 사용자를 인증하는 인터넷 모델을 그대로 채용하고 있다. 사용자는 서비스 이용 인가가 있다는 것에 의해서 다른 사용자를 무조건적으로 신뢰한다. 소리바다의 파일 공유는 유료로 운용되는 형태이기 때문에 사용자가 네트워크를 사용하기 위해서는 서버의 과금 정책을 따라야 한다. 이 때문에 과금이 가능한 사용자인지 여부가 신뢰정보를 생성하는데 그대로 이용된다고 할 수 있다.

Skype의 인터넷 전화 서비스는 현재 무료로 이용

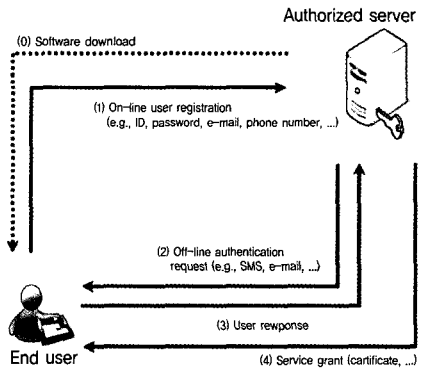
되고 있기 때문에 소리바다와 같은 과금이 결부되지 않는다. 따라서 사용자는 임의로 다수의 아이디를 손쉽게 등록할 수 있다. 전화 서비스가 상대 사용자 목소리에 의해서 사용자간 직접 인증이 가능한 매우 특별한 형태의 응용이라는 점에 의존하고 있음을 쉽게 알 수 있다. 이것은 Skype의 인증 모델과 P2P에서 요구하는 인증 모델에 현격한 차이가 있음을 보이는 것이라고 할 수 있다.

중앙 집중형 신뢰정보 관리 기법에서 아이디는 각 사용자를 구분 짓는 인자로 이용될 뿐 큰 의미를 갖지는 않는다. 서비스를 이용할 수 있는 인가와 아이디를 연계할 수 있는 매개체가 곧 사용자의 신뢰정보가 되는 것이다. Skype의 인터넷 전화 서비스에서 이러한 연계 정보로 이용되는 것은 사용자가 서비스에 조인할 때 서버가 발급해 주는 공개키 인증서이다. 이 인증서는 X.509 형식을 따르지 않는 간단한 인증서 이지만 서버가 해당 아이디의 사용자를 인증했음을 증명할 수 있고, 사용자간의 공개키 검증을 통해 상호 신뢰할 수 있는 대화 통로를 손쉽게 구성할 수 있도록 해준다.

이러한 중앙 집중형 신뢰정보 관리 방식을 P2P에 적용할 수 있도록 하기 위하여 인증기관 (Thawte)에서는 새로운 인증서 발급 서비스를 제공하고 있다. 즉 사용자가 손쉽게 PGP (Pretty Good Privacy) 형태의 이메일 보안을 위한 WoT (Web-of-Trust)를 이용할 수 있도록 개인 인증서를 발급하는 것이다. PKI (Public Key Infrastructure) 에서는 사용자 등록을 위해 공인된 등록기관(RA; Registration Authority)을 통해 오프라인으로 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 텍스트 기반 메시징 서비스에서 사용자의 휴대폰 번호를 이용해 단문 메시지 (SMS) 형태로 인증 번호를 전송하는 것이 대표적이다.

3) 신뢰정보 관리 및 사용자 인증 기법

소리바다, Thawte의 WoT인증서 발급 서비스, Skype에서 볼 수 있는 중앙 집중형 신뢰정보 관리 기술의 일반적인 형태를 그림 1에 나타내었다. 이러한 방식은 대부분 인터넷 모델에 기인하고 있기 때문에 사용자는 (과정 0)을 통하여 해당 프로그램을 다운로드 한 후 등록 과정을 진행한다고 가정하였다. (과정 1)의 절차는 사용자가 온라인으로 아이디와 패스워드를 등록하는 과정이다. Web 기반의 등록 과정인 경우 일반적으로 HTTPS에 의해 암호화된다.



(그림 1) 중앙 집중형 신뢰정보 관리 방식의 사용자 인증 과정

이 과정에서 부가적으로 사용자가 제공해야 하는 정보는 (과정 2)와 (과정 3)에서의 간접적인 오프라인 인증 기법에 따라 달라질 수 있다. 네이트온의 경우 휴대폰을 이용한 단문 메시지에 의해서 인증을 수행한다. Thawte의 WoT 인증서 발급은 이메일을 매개로 하고 있다. Skype의 경우 (과정 2)와 (과정 3)이 존재하지 않는다. (과정 4)는 등록 과정의 마지막

단계로 사용자에 대한 인증 결과를 통보해준다. 예를 들어, Skype은 사용자간에 상호인증이 가능하도록 하기 위하여 각 사용자가 임의로 생성한 공개 키에 대한 인증서를 발급한다. 이러한 등록 및 인증의 결과는 사용자가 해당 아이디를 이용하여 서비스를 받을 수 있도록 인가 받는다는 것이다.

4) P2P 환경에서의 신뢰정보와 사용자 인증

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 있기는 하지만 P2P를 위한 보안 기술이라기보다는 인터넷 환경에서의 서버 의존적인 보안기술이 그대로 적용된 것이라고 할 수 있다. 따라서 이것을 P2P 환경에 적용할 경우에 여러 가지 제약이 따를 수밖에 없다.

예를 들어, 단문 메시지를 이용하는 네이트온의 사용자 인증 기법은 국내의 인터넷 및 휴대전화망에 의존하고 있으므로 글로벌 네트워크 환경에서 적용하는데 어려움이 있다. 이메일을 이용하는 Thawte의 인증 기법은 사용자가 임의로 다수의 이메일 주소를 생성하는 것이 가능하다는 점을 고려한다면 궁극의 해결책이 될 수는 없다. Skype은 가장 개방적인 환경이어서 아무런 사용자 인증을 제공하지 않는다. 따라서 악의적인 사용자는 무수히 많은 아이디를 보유할 수 있다.

P2P 환경에서 요구되는 보안 기술, 특히 사용자 인증과 관련하여 발생 가능한 이슈를 논의하기 위하여 우선 본 논문에서 대상으로 하고 있는 P2P 환경에 대해 간략히 정의할 필요가 있다. P2P는 peer 노드 간의 연결성을 최우선시 하기 때문에 그 운용 형태가 중앙 집중형, 분산형, 또는 혼합형이냐 하는 점은 보안 기술과는 큰 관계가 없다고 할 수 있다. 따라서 본 논문에서 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 매개가 존재하지 않기 때문에 사용자간의 인증이 무의미한 것이 될 수도 있다. 이러한 상황에서 P2P 네트워크에 참여하는 노드에게 주어진 것은 상대방을 식별할 수 있는 고유한 아이디뿐이다. 즉 각 사용자는 상대 노드의 아이디에 의존하여 신뢰 가부를 판단하는 것이다. 따라서 P2P의 보안 기술은 아이디에 의존한 신뢰 가부를 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. 이것은 또한 P2P 환경에서 상대방이 어떠한 아이디와 패스워드를 알고 있다는 것만으로는 상대방을 신뢰할 수 있는 충분조건이 될 수 없음을 의미한다.

B. 아이디 관련 보안 기술

1) 아이디 신뢰성

온라인상에서의 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 수 도 있으며 (예: IP 주소), 네트워크 토폴로지를 결정하는 요소가 되기도 한다. (Structured 방식의 P2P 오버레이 네트워크가 대부분 여기에 해당한다.) P2P 환경이 개방된 네트워크임을 감안한다면, 온라인상에서 사용자를 인식하기 위해 사용되는 아이디는 공개된 값이고, 아이디를 소유하고 있다는 것만으로 사용자를 인증하거나 신원을 증명하는 데에 이용될 수 있는 어떠한 신뢰 정보도 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.

2) 아이디 소유권 증명 기법

CGA (Cryptographically Generated Address) [11] 방식에서 아이디는 "그것을 생성한 사용자의 공개키와 강력한 보안적 결합을 이루고 있어 아이디 검증자는 그 아이디를 생성한 사용자가 해당 아이디를 소유 (ownership)하고 있으며 배타적 (exclusiveness)으로 사용 하고 있다"는 것을 검증하는 방법을 제공한다. CGA의 아이디 생성 절차를 그림 2에 나타내었다. (CGA는 본래 IPv6용 주소를 생성하기 위한 기법으로 [15]에서 제안되었으며 이후에 RFC3972로 표준화 된 것이다. 이와 유사한 아이디 생성 방식으로 SUCV가 있다.)

(1) Generate public/private pair
(2) Choose random value (modifier)
(3) Select security value : 0~7
(4) Compute hash (hash2): (address prefix and collision count field are set to zero)
SHA1(Random | 0 | 0 | public key)
(5) If 16*sec left most bits are not zero, increase random by 1 and repeat (4)
(6) Compute hash (hash1):
SHA1(Random | Address prefix | collision count (set to zero) | public key)
(7) Extract 64bit identifier from the hash
(8) Check ID duplication.
If duplicate detection fails, increase collision counter and repeat from (6)

(그림 2) CGA의 아이디 생성 절차

여기에서 생성된 아이디가 가질 수 있는 범위를 줄여주는 기법이 부가적으로 이용되는데, 사용자는 아이디 생성을 위해서 암호학적인 "퍼즐"을 풀어야 하는 형태이다. 즉 CGA 에서는 생성된 아이디의 상위 p 비트가 0이 되도록 한다는 조건을 두고 있다. 따라서 이 조건을 만족하기 위해서 (퍼즐을 풀기 위해서) 사용자는 반복적인 아이디 생성 알고리즘을 수행하여야 한다.

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

[12]에서는 CGA와 유사한 방법을 이용하여 P2P 네트워크의 임의의 노드 간에 보안 연계 (SA; security association)를 생성하는 방안이 제안되어 있는데 다음과 같다. 두 노드간의 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. 프로토콜은 (그림 3)과 같다.

msg1 (secure side channel) $u \rightarrow v : IP_u \mid \xi_u$
msg2 (secure side channel) $v \rightarrow u : IP_v \mid \xi_v$
msg3 (network) $u \rightarrow v : N_u \mid ID_u \mid K_u \mid IP_u$
msg4 (network) $v \rightarrow u : N_v \mid ID_v \mid K_v \mid IP_v$
u : check $h(N_v \mid ID_v \mid K_v \mid IP_v) \models \xi_v$; check ID_v ; match (K_v, IP_v)
v : check $h(N_u \mid ID_u \mid K_u \mid IP_u) \models \xi_u$; check ID_u ; match (K_u, IP_u)
msg5 (network) $u \rightarrow v : S_u(N_v \mid ID_u \mid ID_v)$
msg6 (network) $v \rightarrow u : S_v(N_u \mid ID_v \mid ID_u)$
****
$\xi_u : h(N_u \mid ID_u \mid K_u \mid IP_u)$
K_u : *public key of u*
N_u : *nonce generated by u*
S_u : *signature of u*

(그림 3) P2P 네트워크에서 임의의 노드간 보안연계 생성 기법 [12]

여기에서 msg1과 msg2는 시스템 셋업을 위해서 오프라인으로 전달되는 메시지이고 msg3~msg6은 SA 형성을 위해서 네트워크를 통해 전달된다. msg5

와 msg6에 의해서 전자서명이 교환되고, 성공적으로 검증이 이루어지면 u와 v는 서로 간에 인증이 완료되어 보안연계를 형성할 수 있다. 이 프로토콜에서 CGA와 유사한 부분은 msg3~msg6의 과정이다. 즉 해쉬와 전자 서명을 함에 있어 아이디와 IP를 이용하는 부분이 CGA에서 목표로 하고 있는 배타적 소유권을 제공하는 것이다. 여기에서 주의할 점은 실제 사용자간에 인증은 오프라인에서 전달된 신뢰정보인 $IP_u | \xi_u$에 의존하여 결정이 된다는 점이다. msg3~msg6의 과정에서 이 신뢰정보와 일치하지 않는다면 보안 연계를 형성할 수 없다. 다시 말해, msg1과 msg2의 오프라인 과정이 없다면 위의 프로토콜은 CGA가 그러하듯이 배타적 소유권만을 제공할 수 있으며 상대방에 대한 인증이 결여되어 있기 때문에 보안연계가 불가능하다. 보안연계가 없는 프로토콜이 글로벌 네트워크에 적용될 경우 MITM (man-in-the-middle) 공격에 취약할 수밖에 없으며, 아이디 스푸핑 공격이 가능하다.

이와 같이 아이디의 배타적 소유권을 증명하는 것만으로는 P2P 사용자간에 충분한 신뢰를 보장할 수는 없지만 분산된 환경에서 아이디를 사용하는데 있어 최소한의 요구기능이 될 수 있으므로, 이에 대한 적극적인 활용이 고려되어야 할 것이다.

3) 아이디 기반 암호화 및 전자서명 기술

아이디 기반 암호기술(IBC; Identifier Based Cryptography)은 공개키 기반 암호 기법을 사용하는데 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 암호기술은 사용자의 공개키/개인키 쌍을 생성하는데 있어 기존의 방식이 일정한 크기의 바이너리 값을 공개키로 이용했던 반면 손쉽게 구별할 수 있는 사용자의 아이디 정보를 공개키로 이용한다는 것이다. 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. Bob이라는 사람에게 암호화된 메시지를 전달하고자 한다면 그의 공개키인 "bob@abc.com"을 이용하여 암호화할 수 있다는 것이다.

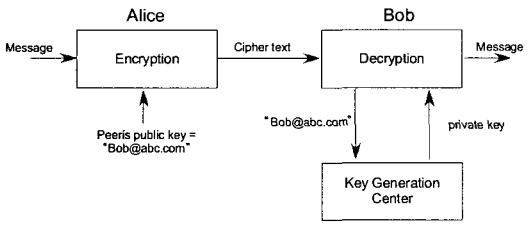
1984년 Adi Shamir에 의해 아이디 기반 전자서명 기법이 처음 제안되었으며[13] 최근에는 아이디 기반의 암호화 기법이 개발되었다. 아이디 기반 암호기술은 본래 해결하고자 했던 키 인증 문제뿐만 아니라 다양한 형태의 아이디를 공개키로 이용할 수 있다는 점에서 P2P 보안 기술에 적용될 경우 매우 유용할 것으로 기대된다.

예를 들어 아이디를 생성하는데 있어 사용자를 구분 지을 수 있는 홍채, 지문 등의 바이오 정보를 추가하여 그것을 공개키로 이용할 수 있다. 사용자의 바이오 정보를 해쉬한 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.

다른 예로 아이디에 시간 정보를 함께 표시할 수도 있는데 "bob@abc.com|2006.08.01|2006.08.02"와 같이 아이디를 생성하여 공개키로 이용한다면 해당 아이디의 사용 기간을 제한할 수 있고 재생공격 (replay attack)에도 효과적으로 대응할 수 있다. 사용자의 위치정보를 아이디에 수록함으로써 지

리적인 제약을 줄 수도 있다. IP 주소를 이용하는 경우 "bob@abc.com|123.456.789.10" 을 공개키로 이용할 수 있다. 전화번호를 아이디에 이용할 경우 앞에서 논의된 단문 메시지 방식의 사용자 인증과 결합하여 매우 강력한 키 인증을 제공할 수 있을 것으로 기대된다.

현재까지 개발된 아이디 기반 암호기술의 한 가지 문제점은 공개키에 해당하는 개인키를 서버 (Key Generation Center)가 생성하여 사용자에게 전달해야 한다는 것이다. 아이디 기반 암호기술의 일반적인 구조를 그림 4에 나타내었다. 이 그림은 Alice가 Bob에게 암호화된 메시지를 전달하기 위하여 그의 공개키로 "Bob@abc.com"을 이용하는 경우이다. Bob은 그 공개키에 해당하는 개인키를 KGC로부터 받아서 메시지를 복호화 할 수 있다. Bob에게 개인키를 전달하기 위해서 KGC와 Bob간에는 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.



(그림 4) 아이디 기반 암호기술

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 암호기술을 적용하는데 있어 필요한 파라미터만 설정해 주기 때문에 사용자 간의 상호작용에 도움을 주는 역할을 수행하는 것으로 볼 수 있다. 이런 운용상의 문제점이 존재하기는 하지만 아이디 기반 암호기술은 P2P 상에서 사용자의 아이디와 보안 기술을 결합할 수 있는 강력한 도구가 될 수 있을 것으로 기대된다.

4) 임계암호 기반 보안 기술

임계 암호시스템 (threshold cryptosystem) [14]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 공격하는데 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 복원 할 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 극대화 하면서 상호 기능을 보완할 수 있을 것으로 기대된다.

VI. 결 론

현재 P2P 기술이나 서비스는 개념에서 많은 혼돈을 야기시키고 있다. 많은 사람들이 P2P 서비스를 파일공유만 알고 있고 그 기초가 되는 기술에 대하여는 무지한 상황이다. 그 예로 Skype는 사람들이 많이 알지만 P2P기술을 기반으로 서비스가 제공된다는 것을 아는 사람은 드물다. 이러한 관점에서 본 논문은 분산처리를 향한 패러다임의 변환에서 P2P가 그 중앙에 서 있음을 언급하고 P2P 기술을 소개하였다. 분산환경에서 보안 취약성에 대하여 분석하였고, 분산환경에서 기존의 보안 메커니즘을 그대로 적용이 어렵다는 것을 검토하였고 이에 분산환경에 적합한 새로운 인증 및 키 교환 메커니즘의 필요성을 언급하면서 예시적 메커니즘을 소개하였다. 그리고 최근에 국제적으로 이루어지고 있는 P2P와 연관된 표준활동에 대한 현황을 간략히 기술하였다.

P2P 인프라는 클라이언트/서버의 역할을 동시에 감당할 수 있는 구조의 서번트(Servent)로 진화하는 과정에 있다. 가까운 미래에 홈네트워크를 중심으로 인프라구축이 예상되며 향후 U-city의 공동생산, 공동체, 그리고 협업을 위한 핵심적인 메커니즘을 제공할 것으로 귀추가 주목되는 기술이다.

[참 고 문 헌]

[1] M.Bawa, B.F.Cooper, A.Crespo, N.Daswani, "Peer-to-Peer Research at Stanford"

[2] P-Grid, http://www.p-grid.org/

[3] JXTA projects, http://www.jxta.org/

[4] 와이즈피어, http://www.wisepeer.com/

[5] Vatary, P2p live streaming: where from and where to http://www.p2p-zone.com/underground/showthread.php?t=22572

[6] 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, March, 2006.

[7] T. Aura, Cryptographically Generated Addresses (CGA), IETF, RFC 3972, March, 2005.

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

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

[10] http://www.3gpp.org/About/3GPP.ppt

[11] T. Aura, "Cryptographically Generated Addresses (CGA)," RFC 3972, IETF, 2005.

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

[13] A. Shamir, "Identity-based cryptosystems and signature schemes," presented at Proceedings of CRYPTO 84 on Advances in cryptology, Santa Barbara, California, United States, 1985.

[14] A. Shamir, "How to share a secret," Commun. ACM, vol. 22, pp. 612-613, 1979.

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

나재훈

1985년 중앙대학교 컴퓨터공학과 졸업
1987년 중앙대학교 컴퓨터공학과 석사
2005년 한국외국어대학교 전자정보공학과 박사
1987년 ~ 현재 한국전자통신연구원 P2P보안 연구팀 팀장
관심분야 : IPv6/MIPv6 보안, P2P 보안

고선기

1995년 홍익대학교 전자공학과 졸업
2004년 Golden Gate Univ. S/W공학 석사
2005년 ~ 현재 한국전자통신연구원P2P보안 연구팀 연구원
관심분야 : P2P 보안, 네트워크 보안

구자범

2000년 중앙대학교 전자공학과 졸업
2002년 중앙대학교 전자전기공학부 석사
2006년 중앙대학교 전자전기공학부 박사
2006년 ~ 현재 한국전자통신연구원 P2P보안 연구팀 연구원
관심분야 : P2P 보안, 유비쿼터스 보안, 홈네트워크 보안, 무선네트워크 보안

권혁찬

1994년 서원대학교 전자계산학과 졸업
1996년 충남대학교 전산학과 석사
2001년 충남대학교 컴퓨터과학과 박사
2001년 ~ 현재 한국전자통신연구원P2P보안 연구팀 선임연구원
관심분야 : P2P 보안, 네트워크 보안, IPv6 보안

문용혁

2003년 단국대학교 컴퓨터공학과 학사
2006년 한국정보통신대학교(ICU) 네트워크공학 석사
2006년 ~ 현재 한국전자통신연구원 P2P보안 연구팀 연구원
관심분야 : P2P 컴퓨팅, P2P 보안, 네트워크 보안