情 報 保 護 學 會 誌
第17卷 第3號, 2007. 6

P2P 사용자 인증과 OTP 분석

문용혁*, 권혁찬*, 나재훈*, 장종수**

요 약

유비쿼터스 서비스 인프라로 부각되고 있는 P2P(Peer-to-Peer) 네트워크는 사용자 제작 콘텐트, 동영상, 파일 등으로 대표되는 지식 콘텐트뿐만 아니라, 컴퓨터 및 네트워크 자원(Resource)을 다양한 환경에서 N 대 N의 형태로 상호 공유 및 분배할 수 있는 구조적 가능성을 제공하고 있다. 그러나 "Open, Dynamic, Anonymous" 등의 특성을 기반으로 하는 P2P 네트워크는 신뢰적 ID(Identity) 생성 및 관리 그리고 이의 적절한 인증에 대한 지원 없이는 현실적으로 잠재적인 보안 위협에 노출되는 제약이 따르게 된다. 한편, 최근 금융보안업계가 주축이 되어 일회용패스워드로 지칭되는 OTP(One Time Password) 인증 메커니즘(Authentication Mechanism)을 제 1 등급 보안방법으로 명시화하고 있고, 온라인 업계에서도 이를 활용하는 기술적 시도 및 개발 사례가 늘어나고 있어, OTP 기술의 보안성 검토 및 활용 범위를 확대하는 방안에 대한 논의의 필요성이 대두되고 있다. 본고에서는 이러한 기술적 흐름 및 산업계 동향에 발맞춰 P2P 네트워크에서 사용자 인증을 위해 OTP 메커니즘을 활용하기 위한 방안에 대해 검토하고 이의 적용 가능성을 분석한다.

Ⅰ. 서 론

종래의 분산 컴퓨팅 네트워크 환경에서, 사용자 인증(User Authentication) 절차는 서비스 요청 및 이용의 주체를 확인하는 매우 주요한 기술적 수단으로 사용된 바 있다. 이는 시스템 및 서비스 인프라를 관리하는 기관 또는 관리자가 이른바 인가되지 않은 사용자의 시스템, 정보, IT 자원, 또는 서비스로의 접근을 감지하고 차단할 필요성이 있기 때문이다. 또한 적절한 인증 절차의 선행이 없이는 적절한 권한부여(Authorization)가 불가능하게 된다. 다시 말해 사용자 인증은 사용자의 시스템으로의 접근제어(Access Control)를 위한 초석을 다지는 보안 기술이라 할 수 있다. 이를 위해서는 구현 가능성과 신뢰성이 높은 인증 메커니즘의 제공이 필연적으로 요구된다.

일반적으로 컴퓨터 보안 분야에서 의미하는 인증의 개념은 사용자, 응용, 및 네트워크 인증과 같이 구분될 수 있으나 본고에서는 사용자 인증만을 그 고려의 대상으로 한정한다. 더불어, 사용자 인증은 보안 강도에 따라 크게 Weak/Strong 인증으로 양분될 수 있다. 클라이언트로부터 서버로 패스워드가 전달되는 정적 패스워드 기반의 약한 인증(Weak Password Authentication) 기법은 스니퍼(Sniffer) 또는 네트워크 분석기(Network Analyzer)를 이용한 악의적 도청/도난으로부터 자유로울 수 없다. 이는 본 방법론이 두 개체 사이에 안전한 연결 및 상호 신뢰라는 가정을 기본 전제로 하고 있기 때문이다. 또한 재생공격(Replay Attack)[1]을 통해 이뤄지는 불법적인 로그인에 대해서도 무방비로 노출될 위험성을 내재하고 있다. 부연하자면, 적합한 사용자에 대한 유효성을 타진하는 절차는 곧 ID 검증(Identity Proofing) 과정을 거쳐서 이뤄져야만 하는 것이다. 잘 설계되고 구현된 사용자 인증 메커니즘은 이러한 과정의 수행 결과를 통해 그 보안 강도 및 신뢰성 정도를 평가받을 수 있다고 해도 과언이 아닐 것이다. 이와 같은 점을 고려하여 제안된 것이 바로 강한 인증(Strong Password Authentication) 기법인데, 최근 많은 논의가 진행되고 있는 OTP 역시 이러한 범주에 속하는 인증 기법 중 하나라고 볼 수 있다. ID 검증의 중요성은 다음과 같은 3가지 사항으로 요약될 수 있다. 먼저, 신뢰성 있는 ID 관리 인프라의 구축을 가능하게 해준다. 둘째,

본 연구는 정보통신부 및 정보통신연구진흥원의 IT 신성장동력핵심기술개발사업의 일환으로 수행하였음.
[2005-S-090-03, 유무선 IPv6 기반 P2P 네트워크 정보보호 기술개발]
* 한국전자통신연구원 정보보호연구단 P2P보안연구팀 (yhmoon@etri.re.kr, hckwon@etri.re.kr, jhnah@etri.re.kr)
** 한국전자통신연구원 정보보호연구단 보안응용그룹 (jsjang@etri.re.kr)

적합한 검증 기능의 제공은 다른 보안 기능과의 연계를 위한 초석이 된다. 셋째, 기관으로 하여금 현재 접근을 요청 하였거나, 내부에서 활동 중인 사용자가 합법적인 이용자(Legitimate User)인지 여부에 대한 확신을 갖도록 해준다.

최근 다양한 분야에서 신규 인터넷 서비스 인프라로서 부각되며 그 잠재력을 인정받고 있는 P2P 네트워크 역시 동일한 고민을 안고 있는 것이 사실이다. 동적인 사용자[1]를 적절한 인증 방법론에 연계(Binding) 시키는 것은 상황을 예측하기 어려운 네트워크 특성과 익명성에 뿌리를 두고 있는 P2P 환경에서 더더욱 어려운 문제임에 틀림없다. 또한 아키텍처(Architecture) 구성 방법에 따라 "Pure, Centralized, Hybrid", 또는 DHT (Distributed Hash Table) 사용 여부에 따라 "Structured/Unstructured"로 구분[2] 될 수 있는 구조적인 다양성, 분산 컴퓨팅, 파일 공유, 협업 등의 다양한 서비스 모델을 위한 인프라로서의 가용성 및 전 지구적 규모의 확장 가능성(High Scalability)으로 요약될 수 있는 P2P 네트워크의 특성은 이러한 문제를 더욱 악화시키기에 충분하다. 특히 이와 같은 환경에서는 상호 인증을 기본 보안 기능으로 요구하기 때문에 사용자 인증에 대한 명확한 구조적 절차(보안 프로세스)의 제공이 필수적이다. 한편, 근래에 들어 동적으로 암호(Password)를 생성하여 사용자를 식별할 수 있는 OTP 인증 기법의 사용 및 그 적용 대상이 늘어나면서, 정적 패스워드 (Static Password)를 기반으로 한 기존 Identity/Password 인증의 문제점을 보완할 수 있는 의미 있는 기술로서 관련 산업계에 그 위치를 새롭게 자리매김하고 있는 실정이다.

이에, 본고에서 주목하고자 하는 점은 N 대 N 형태의 P2P 네트워크에서 Peer 상호간 OTP 기반의 인증기법을 통해 신뢰성 있는 인증 모델(Trust Authentication Model) 구축의 실효성을 검토하는 것이다. 또한 OTP 인증 메커니즘을 P2P 네트워크에서 어떻게 활용할 수 있는가에 대해 알아보고 그 기술적 적합성에 대해 분석한다. 이를 위해 먼저, P2P 네트워크가 안고 있는 보안 취약점을 익명성 관점에서 언급하고, 특히 ID 관련 공격 유형 및 방어 기법을 살펴봄으로써 P2P 환경에서의 강한 인증의 필요성에 대해 검토한다. 또한 OTP 인증 메커니즘에 대해 분석하고 이의 적용 가능성을 잘 알려진 여타 기법과 비교한다. 더불어 자금 거래를 기반으로 하는 상업 P2P 시스템 시나리오에서 OTP 활용 시 요구되는 기술 사항의 이해를 통해 그 적용 가능성을 타진한다.

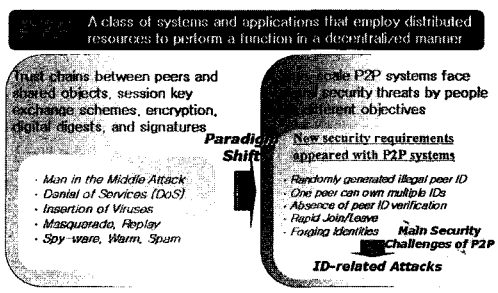
Ⅱ. P2P 관련 보안 쟁점

P2P 네트워크는 종래의 일반적인 분산 컴퓨팅 환경에서 논의된 바 있는 보안 취약성(Security Vulnerabilities)[2]에 대부분 노출되어 있다. 그러나 P2P 컴퓨팅 환경이 특수한 기법[3]을 통해 분산 자원들을 대상으로 기능을 수행하는 시스템 또는 응용프로그램으로 규정지어질 수 있는 만큼, 기존의 그것과는 다른 형태의 위험 요소를 내재하고 있다고 볼 수 있다. 즉, 새롭게 등장하는 보안 요구사항들이 주요한 P2P 정보보호 이슈로 떠오르고 있는 실정이며 이를 약술하면 다음과 같다.

- Worm, Bot, Virus 전파의 주된 통로로 활용됨
- P2P를 통한 개인정보 및 기밀 유출 피해 급증
- P2P 공유 Port를 통한 해킹 공격 급증
- ID 도용 피해 다수 발생
- Collaborative attack, Sybil attack 등 다양한 형태의 공격 출현

그러므로 본 장에서는 P2P 환경의 특수성 및 주요한 보안 취약성에 대하여 살펴보도록 하겠다.

2.1. P2P 네트워크의 익명성



〔그림 1〕 P2P 환경에서의 새로운 보안 취약성의 등장[3]

1) Dynamic IP Address, Frequent Join/Leave, Multiple IDs Generation 등의 특성을 갖는 사용자를 의미함.

2) Man in the Middle Attack, DoS, DDoS, Virus, Replay Attack, Spy-ware, Spam 등의 공격을 의미함.

3) 자원 공유 및 배포, 커뮤니티 생성/관리, 분산 태스크의 스케줄링, 실행 및 모니터링, 오버레이 라우팅 기법, 이기종 자원에 대한 관리 등이 P2P 네트워크 기반의 응용 서비스에 요구되는 주요한 기법들로 정의될 수 있다.

P2P 커뮤니티는 자발적으로 생성 및 소멸될 수 있는데 이는 Peer의 자유로운 참여로 조성되는 네트워크라는 구조적인 특징에 기반 한다. 이러한 자율적인 구조를 가능케 하는 근본적인 이유는 P2P가 기본적으로 익명성(Anonymity)을 지원하고 있기 때문이다. 이것은 네트워크의 확장성을 높이고, 특정 자원이나 서비스를 필요로 하는 모든 Peer에게 손쉽고 공평한 접근성을 보장하는 장점을 제공한다. 그러나 익명성을 보장한 네트워크 참여 및 탈퇴(Join/Leave)는 일반 사용자들로 하여금 P2P는 "무료, 무제한 사용", 반면에 사업자에게는 "불법적 이용, 관리의 부재"라는 상반된 인식을 강하게 불어 넣는 부정적 결과를 초래하였다. 즉, 자원 및 서비스에 대한 비제한적 접근을 보장함으로써 가용성을 높여주었으나, 사용자 입장에서 연결된 다른 Peer들을 신뢰할만한 수단을 적절히 제공해 주지 못함으로써 그 요청 결과의 정확성에 대해서는 보장해 주지 못하는 구조적 제약을 낳게 되었다. 또한 서비스 제공자 역시 과도한 P2P 트래픽의 양산[4]으로 인한 네트워크 운용 자원의 심각한 고갈을 경험하고 있으나, 이에 대한 발생 비용을 부담할 적절한 소비자 모델을 찾지 못하고 있는 실정이다. 익명성은 개별 개체에 대한 개인정보보호(Privacy) 차원에서 그 효력을 발휘할 수 있으나, 법적인 테두리 내에서 추적 또는 제어가 불가능한 (Uncontrolled Anonymity) 네트워크 모델은 관리 방법의 복잡도를 높여 결국 추가적인 비용을 유발하게 된다. 결과적으로 이는 사업자로 하여금, P2P 서비스 인프라의 활용 잠재력은 인정하나 그 구체적인 효용성에 대해서는 의문을 제기하게 만드는 한 가지 주요한 요인으로 작용하고 있다.

P2P 네트워크에서 실체에 대한 검증 없이 새로운 ID를 생성하여, 자유로운 참여 및 탈퇴를 허용하는 구조는 Whitewashing[4]와 같은 대표적인 보안 취약성 문제를 야기 시키고 있다. 일례로, 온라인에 불법적으로 유포되어 있는 주민등록번호를 이용하여 수많은 ID를 발급받아 사용할 경우 마치 여러 금고의 열쇠를 한 사람에게 부여하는 것과 유사한 위험을 초래할 소지를 갖게 만든다. 물론, 복수개의 ID 생성이 직접적으로 보안 침해사고와 연계되는 것은 아니라고 할 수 있으나, 보안 감사 및 추적을 어렵게 만들기에는 충분할 것이다. 또한 ID Spoofing 및 MITM과 같은 구체화된 공격의 출발점이 된다는 점에서 시사하는 바가 크다고 할 수 있다.

그러므로 익명성에 기반한 P2P 네트워크 모델은 제어된 익명성(Controlled Anonymity)의 제공 또는 식별 및 추적이 가능한 ID 기반 관리 구조의 지원이 적절히 제공될 때, 보안 위협의 가능성을 낮출 수 있다고 할 수 있다. 부연하자면, 현재의 P2P 네트워크는 종래의 인터넷에서와 같이 ID 생성 및 이의 검증 기술을 통해 사용자를 식별하는 형태로 서비스되고 있다. 그러나 ID 관리의 취약성은 또 다른 보안 문제를 야기 시키고 있다 [그림 1].

2.2. ID 관련 보안 취약성

P2P 네트워크 환경에서 신뢰적 ID 생성 및 이의 관리에 대한 요구가 등장함에 따라 개체에 대한 적절한 인증이 뒷받침 되지 않을 경우 [표 1]과 같이 잘 알려진 P2P ID 관련 보안 취약사항에 노출될 위험성이 존재할 수 있다.

먼저, Whitewashing은 비교적 손쉽게 낮은 비용으로 신규 ID를 생성하여, P2P 네트워크에 참여할 수 있게 됨에 따라 발생하게 되는 공격 유형이다. 이처럼 개체의 ID가 적절히 검증되기 어려운 환경에서 ID Spoofing 공격은 ID 관리 체계에 더욱 큰 혼란을 가중시키는 요인으로 작용한다. 즉, 악의적 Peer는 합법적인 다른 Peer(Legitimate Peer)로부터 탈취한 ID를 통해 자신의 식별 정보를 속여 네트워크에서 활동하며 비 인가된 통신을 지속할 수 있게 된다. 그 예로 본 공격은 DoS 시도를 위한 좋은 기회를 제공한다.

[표 1] P2P ID 관련 공격유형 대비 방어기법

공격유형	방 어 기 법
White-washing	1) Persistent Peer ID 보장 2) Strict Model(Central Trusted Authority)활용 3) Reputation Model을 통한 Cost vs. Penalty 기법적용
ID Spoofing	1) 접근제어(Access Control) 기법 활용 2) Packet Filtering을 통한 접근제어 3) 취약점 서비스 사용의 제거 4) 암호화 프로토콜 활용
Sybil Attack	1) Peer ID 생성에 따른 과금 징수 2) Peer ID와 사용실체를 실검증하는 방안

4) Network World 2005의 조사에 따르면, Internet Traffic 전체 볼륨 중 60~89%에 육박하는 트래픽이 P2P인 것으로 추정된 바 있다.

Sybil 공격[5] 역시 다량의 ID를 생성하여 Reputation 시스템[5]을 기반으로 하는 P2P 네트워크를 파괴할 목적을 가지고 있다. 이와 같은 ID 관련 공격은 바로 Entity와 ID간의 1:N 매핑 구조가 가능하다는 것에 기인한다.

특히 자금 교환 등의 중요 거래가 수반되는 시스템 및 환경에서는 보다 엄중한 인증 과정이 필요하다. 그러므로 수행 절차 및 결과에 대한 신뢰성이 보다 높은 강한 인증에 대한 필요성이 제기된다.

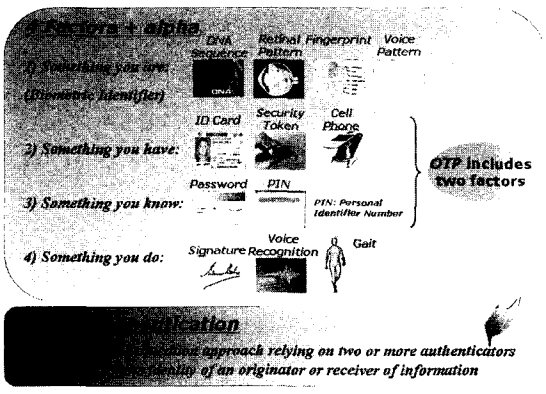
Ⅲ. P2P 인증 메커니즘에 대한 고찰

본 장에서는 먼저 다인자(Multifactor) 인증 기법의 구성 요소 및 각 실례를 살펴보고 강한 인증에 대한 필요성을 언급한다. 또한, 기존에 잘 알려진 인증 메커니즘들에 대한 간략한 개요를 설명하고 P2P 네트워크에서의 활용 가능성에 대한 비교 검토를 통해 각 기술별 보안성을 분석하며, 특히 OTP를 중심으로 그 잠재력을 타진한다.

3.1. 강한 인증 매체로서의 OTP 분석

인증 메커니즘은 인증의 대상(사용자, 응용, 네트워크)이 무엇이냐에 따라, 또한 사용자 인증의 경우 그 강도에 따라 상기 I~II장에서 기술한 바와 같이 구분될 수 있으며, "인증 수단"의 관점에서 보다 세부적으로 분류될 수 있다. 특히 이를 "Multifactor Authentication"이라 하는데, [그림 2]와 같이 크게 4가지 유형의 기법으로 분류될 수 있다. 즉, 각 유형별 구분의 기준은 인증을 위해 이용되는 수단이다.

[그림 2] Multifactor Authentication and Strong Authentication[6][7]



먼저, "Something you are (Biometric Identifier)"는 생물학적으로 각 개체별 독립성 및 유일무이함(Uniqueness)이 증명될 수 있는 신체 기관또는 특성에 근간을 둔 인증 기법이다. 예를 들어 DNA 염기서열, 망막패턴, 지문인식, 음성패턴 등이 그 대표적인 사례로 언급될 수 있다. 둘째로, "Something you have"는 ID 카드, Smart 카드, 보안 토큰, 휴대전화와 같이 본인만이 휴대할 수 있는 개인 소유물을 통해 개체를 식별해주는 인증기법을 의미한다. 셋째로, "Something you know"는 본인만이 알고 있는 독립성이 보장된 정보를 이용하여 인증 절차를 수행하는 경우인데, 일반적으로 패스워드, 개인 식별 번호(PIN: Personal Identifier Number) 등을 고려할 수 있다. 넷째로, "Something you do"는 인증의 대상만이 가지고 있는 고유한 행동 특성 및 양식을 인증 메커니즘에 반영하고자 한 유형으로써 서명, 음성인식, 걸음걸이(Gait)등이 대표적으로 연구 및 개발되고 있는 실정이다.

특히 근래에 들어, 온라인 은행 거래(Online Banking Transaction)를 기반으로 한 전자 상거래 분야에서 보다 견고한 보안 인증의 필요성이 요구되고 있어, 상기 언급된 4가지 Factor 중 두 가지 이상을 조합하여 하나의 통합된 인증 메커니즘으로 활용하는 기법의 사용이 현실화된 바 있다. 이를 "강한 인증[6]" 이라 하는데, OTP는 두 번째, 세 번째 Factor를 활용하고 있어 이에 속하는 인증 메커니즘으로 분류될 수 있다.

경우에 따라서는 "Somebody you know[7]"와 같이 본인이 아는 온라인의 다른 누군가 즉 대리인(Delegators)을 통해 상호 인증을 수행하는 구조를 고려할 수 있으나, 상용 온라인 거래 시스템에서의 그 실용화는 아직까지 요원한 것으로 판단된다.

3.2. OTP 인증 기법에 대한 검토

RFC2289에 기술된 바 있는 OTP 메커니즘을 이용한 일회용 패스워드의 생성은 [그림 3]과 같이 도식화 될 수 있으나, 현재 OTP 상업 솔루션 업체는 개별적인 알

5) P2P 네트워크를 구성하는 각 Peer가 자원 공유 및 배포 등의 서비스에 참여한 타 Peer의 신뢰도를 평가함으로써, 서비스를 요구하는 다른 Peer들이 기 구축된 평판(Reputation) 정보를 기초로 상대 Peer의 행동(Behavior)의 유해성 여부를 판단할 수 있는 시스템을 의미한다. 일례로, 인센티브(Incentive)에 기초한 Reputation 시스템을 고려할 수 있다.

고리즘을 기반으로 제품을 개발 및 판매하고 있다[6].

기본적으로 OTP는 손쉽게 생성할 수 있는 동적 패스워드를 바탕으로 한 강한 인증을 지원한다는 측면에서 우수한 보안성을 제공하는 것으로 평가받을 수 있다. 또한 암호학적으로 현재의 패스워드로부터 다음에 사용될 패스워드의 유추가 불가능하다. 그러므로 악의적 Peer가 중간자 공격(MITM: Man in the Middle Attack)을 통해 특정 사용자의 패스워드를 획득한다 할지라도, 이를 이용한 재생공격의 가능성을 봉쇄할 수 있게 한다. 다시 말해 이는 *Onewayness*를 지원하는 일방향 해쉬함수(Oneway Hash Function)를 이용하여 일회용 패스워드를 생성하는 OTP의 특성에서 비롯되는 보안적 강점이라 할 수 있다. 이러한 장점에도 불구하고, OTP(특히, Challenge-Response Type)는 MITM 공격을 완전히 무력화 시킬 수는 없으며, 현재 금융권 및 일부 전자상거래에서 사용되고 있는 OTP 인증 기법은 하드웨어 생성기에 의존하고 있는 만큼, 이것의 분실 또는 도난과 같은 오프라인 공격(Offline Attack)에 취약한 면모를 드러내고 있다. 또한 무엇보다도, 하드웨어 OTP 생성기의 경우 제품 출고 당시, OTP 중앙 서버와의 동기화된 정보를 탑재해야만 하는 오프라인 상의 절차를 동반하게 되며, 사용이 빈번할 경우 디바이스의 전원 수명 문제도 고려해야만 한다.

상기 언급한 OTP 인증 수행 모델의 몇몇 특징은 P2P 네트워크에서의 인증 구조와의 직접적인 연계 가능성을 저해하는 요인으로 작용한다[표 2].

즉, 현재의 인터넷 이용자는 P2P 서비스를 사용하기 위해 별도의 인증 기기를 구매 또는 부여받아야 하는 불편함을 감수할 만큼 여유롭지 못하다. 또한, P2P 네트워크의 특성상 빈번한 네트워크 참여/탈퇴를 반복하는 구조에서는 별도의 인증 디바이스를 통한 패스워드의 생성은 오히려 사용자 측면에서 불편함을 초래할 뿐이다. 이를 Software type OTP generator로 구현하더라도, 각 Peer(Client S/W)는 OTP 중앙 인증서버와의 패스워드 생성을 위한 기본 정보를 동기화하고 있어야 하는데, 동기화 정보의 교환 및 이의 관리는 인증 절차상 별도의 오버헤드(Overhead)로 작용하여 관리 및 보안상의 결점을 제공하게 된다.

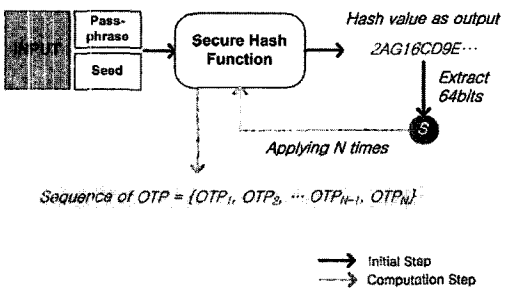
또한, 사용자가 생성한 일회용 패스워드를 검증하고 각 개체를 식별하는 역할을 중앙 인증 서버에서 수행하게 되므로 확장성 및 분산도가 매우 큰 P2P 네트워크에서는 "Single Point of Failure"와 같은 단일 관리 서버 또는 시스템의 오류 및 결함으로부터 자유로울 수 없는 문제점을 내포하게 된다.

그러나 II장에서 언급한 바와 같이 P2P 네트워크에서 개체의 식별 및 추적을 통한 관리의 시작은 ID Management를 필연적으로 요구하고 있기 때문에, 쉽고 간편하며(Cost-effective), 강한 인증(Strong Authentication)을 제공할 수 있는 기법의 고안 및 이의 적용이 여전히 필요한 것이 사실이다.

약술하자면, OTP는 강한 인증 기법을 제공하는 반면, P2P 네트워크를 위한 인증 메커니즘으로 동작하기에는 어려운 몇 가지 면모를 갖고 있는 것으로 판단할 수 있다. 그러나 OTP는 작고 가벼운 알고리즘을 통해 효율적으로 동작할 수 있는 구조적인 특징을 제공하고 있으며, Software type OTP 생성기 이용에 따른 정보 동기화의 오버헤드로 인한 보안 취약성 발생은 SSL (Secure Socket Level) 등의 신뢰 채널 구축을 통해 보완될 수 있으므로, 그 적용 가능성에 대한 보다 구체적인 검토가 필요한 것으로 사료된다.

[표 2] P2P 환경에서의 OTP 인증 시 고려 사항

Drawback	Description
하드웨어 디바이스	Hardware type OTP generator, battery life
동기화 절차	Pre-sharing synchronized information
중앙 인증 서버	Central OTP server and scalability issue



[그림 3] OTP 생성 과정[8][9]

6) OTP 인증은 그 동기화 방법론에 따라 크게 Challenge-Response, Time-Synch, Event-Synch, Time/Event-Synch와 같은 4가지 유형으로 구분될 수 있다 (∵ Synch: Synchronization).

3.3. P2P 환경에서의 인증 메커니즘 보안성 평가기준

인증 메커니즘별 기술성을 검토하기에 앞서 P2P 환경에서 인증 메커니즘에 요구하는 기술 사항의 정의 및 보안성 평가의 기준을 설정하는 과정이 선행되어야 할 필요성이 있다. 다음에 제시된 내용을 살펴보자[10].

- SR1. Weak Authentication
- SR2. Strong Authentication
- SR3. Accountability
- SR4. Cost Effectiveness
- SR5. Authentication based on Attribute
- SR6. Scalability
- SR7. Community Authentication

∵ SR: Security Requirement

P2P 네트워크에서의 인증과 관련된 보안성 검토 항목은 먼저 인증의 강도에 따라 두 가지 요구사항(SR1, SR2)으로 도출 될 수 있다. 또한 시스템 내에서 각 개체(Peer)는 유일하게 식별되어야 하며 이를 통해 내부 규칙을 위반한 사용자를 추적하고 그에 상응하는 책임을 물을 수 있도록 하는 책임 추적성(SR3)이 세 번째 검토 사항으로 언급될 수 있다. 다음으로, 해당 인증 메커니즘의 구현 및 수행 복잡도 그리고 이의 운용에 따른 비용을 지적할 수 있다(SR4). 더불어 각 개체의 속성을 반영하여 인증을 지원하는가 하는 방법론적인 측면에서의 검토 항목이 추가될 수 있으며 (SR5), 네트워크를 기반으로 한 시스템의 특성상 인증 대상 개체가 증가하더라도 신뢰성 있는 인증을 수행할 수 있으며, 각 개체에 대한 관리가 가능할 필요성이 있다. 즉 이는 인증 기법의 확장성에 대한 검토 항목이 되겠다(SR6). 끝으로, 특히 P2P 네트워크에서처럼 커뮤니티 또는 그룹 기반의 지역 통신(Localized Communication)을 통해 확장 구조를 지향하는 모델의 경우 커뮤니티의 참여/탈퇴와 관련된 그룹 보안에 대한 이슈가 고려될 필요성 있다 (SR7).

다만, 본고에서 제시한 P2P 네트워크에서의 인증과 관련된 보안성 검토 사항은 P2P 응용 및 서비스의 유형 및 특성에 따라 유동성을 가질 수 있다.

3.4. 인증 메커니즘별 P2P 적용성 검토

본 소단원에서는 상기 언급한 인증 메커니즘의 보안성 평가 기준을 근거로 잘 알려진 인증 기법에 대한 비교 분석을 통해 OTP의 활용 가능성에 대한 검토를 심화시키고자 한다.

- CS1. Static Password Authentication
- CS2. PGP(Pretty Good Privacy)
- CS3. PKI(Public Key Infrastructure)
- CS4. HSM(Hardware Security Module)
- CS5. OTP(One Time Password)
- CS6. Self-Assigned

∵ CS: Candidate Solution

우선, 가장 일반적이고 간편한 접근 방법으로 ID/Password의 조합을 사용자 자격 증명(User Credentials)의 수단으로 이용하는 경우를 고려 할 수 있다. 즉, 정적 패스워드 기반의 본 인증 방법은 자격 증명의 암호화 전송 및 DB 매칭 등을 통해 사용자를 식별하게 된다. 그러므로 비교적 손쉽게 구현이 가능하며 엄중한 보안 수위를 요구하지 않는 시스템에 적합하다.

둘째, Email의 암호화된 전송을 지원하기 위한 암/복호화 기법으로 제시된 바 있는 PGP[11]의 경우 PKI[12]의 X.509 증명서(Certificates)와 다른 구조의 PGP 증명서를 통해 상호 인증을 수행한다. 즉 PKI가 CA (Central Authority)에 의존하는데 반해, PGP는 하나의 증명서에 다른 복수 사용자의 "Key/Identification (Self-Signature)"을 포함함으로써 사용자간 Key의 유효성을 판단하는 체계로 동작한다. 요컨대 PGP 기법에서 모든 사용자는 타인을 식별해주는 유효성 검증자(Validator)로서의 역할을 수행함으로써 "Web-of-Trust"를 구축하게 되며, 본 환경에서 PGP 사용자는 "Vote Counting"과 같은 Reputation 기법을 통해 상호간의 신뢰도를 판단하게 된다. 그러나 PGP 역시 CA와 같은 중앙신뢰기관(Central Trusted Authority)를 통해 PKI와 유사한 자격 증명 구조를 차용할 수도 있다.

셋째, PKI는 국내의 경우 이미 공인된 인증 방법으로 정착되어 있으며, 특히 은행권을 비롯한 대부분의 거래 시스템의 경우 PKI에 절대적으로 의존하고 있는 실정이다. 그러나 PKI는 핵심적 역할을 수행하는 CA의 경우 국가간 연계가 되지 않을 뿐만 아니라 인증서 발급을 위해서는 각 개인으로 하여금 오프라인 등록 절차의 선행을 요구하고 있으며, 강력한 인증을 지원하는데 반해, 불필요한 개인 정보의 중앙 집중화로 인한 문제점을

드러내고 있다. 또한 운영 및 유지 비용 역시 타 인증 기법에 비해 높다는 점을 감안할 필요성이 있다. 이와 같은 PKI의 특성은 P2P 네트워크로의 적용 가능성을 떨어뜨리는 주요 요인으로 작용한다.

또한 OTP와 더불어 금융감독원으로부터 1등급 보안 매체로 지정된 바 있는 HSM의 경우 하드웨어 보안 토큰에 의존하는 만큼, 개인키의 유출을 방지할 수 있고, 복호화 및 서명 작업이 보안토큰 내부에서 이루어진다는 장점을 제공할 수 있다[13][14]. 그러나 HSM의 인증 방식은 공개키 기반의 인프라에 의존하고 있으며 더불어 하드웨어 매체에 의존적이므로 P2P와의 구체화된 연계는 다소 요원한 것으로 판단된다.

다음으로 Self-Assigned 기법[15]은 공개키를 Peer 자체적으로 생성하여 분산 네트워크 환경에서 중앙인증기관의 도움 없이 상호 인증 및 식별을 수행하고자 하는 아이디어에 바탕을 둔 방법론이다. 이의 현실화를 위해서는 P2P의 커뮤니티 또는 그룹에 기반을 둔 신뢰 관계 모델(Trust Relationships), 인증을 수행하는 대행자(Delegator)의 지정, 그리고 이의 동작(Protocol)에 대한 정의가 요구된다. 현재까지 연구가 진행 중인 분야이며, 적용 가능성 역시 낮은 것으로 평가할 수 있다.

대략적으로 살펴본 바와 같이 공개키 기반의 인증 체계를 직접적으로 P2P와 연계하기 위해서는 표면적인 보안 요구사항 이외에도 많은 고려사항이 뒤 따르게 된다. 그러나 P2P 인증 메커니즘의 고안은 P2P 서비스 모델을 산업화로 직접 연계시킬 수 있는 주요한 수단을 제공한다는 점에서 의미하는 바가 크다고 할 수 있다. 그러므로 이제 P2P 환경에 보다 적합한 형태의 보안 정책을 수립하고 수행할 수 있도록 유연하면서도 엄중한 인증을 제공할 수 있는 보안 메커니즘 구조의 제시가 필요한 시점이다.

인증 메커니즘 별로 지원하는 보안성 평가 기준을 요약하면 다음 [표 3]와 같다.

[표 3] 인증 메커니즘 별 기술성 분석

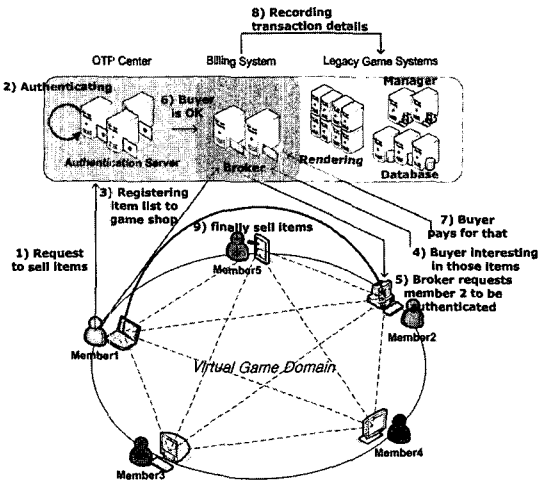
대안 솔루션	P2P 보안 평가 기준
CS1	SR1, SR4
CS2	SR2, SR6
CS3	SR2, SR3, SR5
CS4	SR2, SR3
CS5	SR2, SR3, SR4, SR7
CS6	SR2, SR4, SR5, SR6

Ⅳ. OTP를 활용한 P2P 인증 시나리오

본 장에서는 자금 교환을 기본으로 하는 상업용 거래 시스템에서의 P2P 인증 시나리오를 고려한다. 즉, Peer 상호간의 연계가 직접적으로 자금 거래로 이어지는 모델을 전제로 한다. 또한, 소프트웨어 형태로 구현된 OTP 기법을 활용한 인증 메커니즘을 가정한다. P2P e-Commerce[16] 시장에서 Peer 상호간 관계에 있어 가장 문제시 되는 것은 바로 자신이 모르는 타인과의 거래에 대한 분명한 보장이 없다는 것이다. 즉, 상용 거래 시스템에서 개체간 식별 및 인지는 실제 거래에 앞서 반드시 선행되어야 할 절차인 것이다. 다음은 P2P 게임 아이템 거래 시스템에 OTP를 활용한 시나리오를 언급하고자 한다[그림 4].

각 이용자들은 P2P 형태로 게임에 참여하고, 온라인에서 현물로서의 가치를 지닌 아이템의 거래 시 아이템 판매자는 OTP Center를 통해 사용자로서 식별되며, 거래 중계(Broker) 시스템에 아이템이 등록되면, 해당 아이템을 필요로 하는 인증된 타 사용자와 상호 실거래가 이루어지게 된다. 종래의 아이템 거래 시스템이 게임 네트워크 참여 시 고정된 패스워드를 통해 한 번의 인증을 수행하는 반면에, 본 시스템은 실거래시 마다 일회성 패스워드를 통해 매번 사용자를 식별함으로써 보다 강화된 보안성을 제공할 수 있게 된다.

이와 같은 시나리오를 일반적인 P2P 네트워크 환경으로 좀 더 확장해 보면, 파일, 스트리밍, UCC(User Created Contents) 등으로 대표되는 소위 u-지식 콘텐



[그림 4] P2P Game Item Transaction System

트의 공유 및 배포가 가능한 N 대 N의 거래 환경을 고려할 수 있다.

네트워크의 규모 및 그 분산도가 매우 큰 환경에서 [그림 4]와 같이 단일인증서버에 의존한 구조는 중앙의 OTP 센터에 많은 처리량을 요구하게 되며, 보안 취약 포인트로 노출될 가능성을 열어두게 되는 문제점을 낳는다. OTP 센터가 없는 구조에서의 Peer 상호 인증이 가능하기 위해서는 먼저 동기화된 정보의 공유가 우선되어야 하는데 이의 관리는 인증에 따른 오버헤드로 작용할 가능성이 크며, 기존 OTP가 제공하는 OOB (Out-Of-Band) 방식의 장점을 잃게 될 소지가 있다. 그러므로 OTP 인증 메커니즘을 활용하여 P2P 상업 서비스의 보안을 제공하기 위해서는 P2P 사용자에게 적합한 보다 유연한 OTP 매체의 개발내지는 오프라인 상의 절차를 동반하지 않고 동기화된 정보를 안전하게 상호 공유할 수 있는 보안 모델의 고안이 우선적으로 요구된다고 사료된다.

V. 결 론

지금까지 P2P에서의 익명성 및 ID 관련 보안 요구사항을 바탕으로 OTP 및 일반적인 인증 메커니즘의 P2P 네트워크로의 적용 시 고려할 사항에 대해서 살펴보았다. 기존의 자격 증명 체계는 P2P와 같이 사용자의 빈번한 참여/탈퇴 및 다양한 커뮤니티의 생성/소멸로 인한 동적 구조 변화를 지향하는 네트워크에 민감히 대응하기 어려운 측면이 있다. 물론, 중앙 서버를 근간으로 한 강력한 인증 체계를 구축한다 할지라도 거대 P2P 네트워크에 참여하는 개별 개체를 식별하는 것은 여전히 쉽지 않은 문제로 볼 수 있다. 즉, 중앙 서버를 배제한 분산 네트워크 인프라에서 유연한 인증 체계를 구축한다는 것은 그만큼 난제로 분류된다.

구체적으로 인증 서버의 분산화 및 협업구조 모델에 대한 연구가 요구되며, 또한 자금 교환을 기본으로 하는 거래 시스템의 경우 사용자 식별을 위한 오프라인 절차의 배제 또는 이를 온라인에서 대치할 수 있는 방안에 대한 모색이 필요하다. 더불어 상기 기술한 내용을 고려하여 OTP와 같이 이른바 "Two-Factor Authentication" 이상의 보안성을 제공하면서 P2P의 "Open, Dynamic, Unpredictable, Scalable" 등의 네트워크 특성을 반영할 수 있는 인증 메커니즘의 고안이 요구되며, 이에 대한 보다 체계적인 연구가 진행될 필요성이 있는 것으로 사료된다. 이와 같은 인증의 설계 및 구축을 위해 보다 구체적인 사례 연구를 통해 심도 있는 논의가 지속된다면 P2P 응용 서비스의 시장성을 높여줄 뿐만 아니라 보안 신뢰성 제고에 긍정적인 영향을 끼칠 것으로 예상된다.

참고문헌

[1] Paul Syverson, "A Taxonomy of Replay Attacks", In Proceeding IEEE Computer Security Foundations Workshop VII, pages 131-136. IEEE Computer Society Press, June 1994.

[2] Oram, A.: Peer-to-Peer : "Harnessing the Benefits of a Disruptive Technology", 1st edn. O'Reilly, Beijing; Sebastopol, CA(2001).

[3] 권혁찬, 문용혁, 구자범, 고선기, 나재훈, 장종수, "P2P 표준화 및 기술 동향", 전자통신동향분석, u-IT839의 정보보호 이슈 특집 논문, 한국전자통신연구원, 22권 1호(통권 103호) 2007.02.

[4] Michal Feldman, et al., "Free-Riding and Whitewashing", Selected Areas in Communications, IEEE Journal on Pages 1010-1019, Vol.24, Issue 5, May 2006.

[5] John R. Douceur, "The Sybil Attack", The 1st International Workshop on Peer-to-Peer Systems (IPTPS '02), 2-8 March 2002, MIT Faculty Club, Cambridge, MA, USA.

[6] Committee on National Security Systems(CNSS) Instruction No. 4009, National Information Assurance (IA) Glossary, published by the United States Federal government, Revised June, 2006.

[7] John Brainard, et al., "Fourth-Factor Authentication: Somebody You Know", ACM Conference on Computer and Communications Security (CCS'06), October 30-November 3, 2006, Alexandria, Virginia, USA.

[8] N, Haller, et al., "One-Time Password System", RFC 2289, IETF OPT Working Group, Feb, 1998.

[9] Neil M. Haller, "The S/KeyTM One-Time Password System", Bellcore, Morristown, New Jersey.

[10] Y.Zhang and D.Zhang, "Authentication and Access Control in P2P Network", LNCS 3032, 2004.

[11] Philip Zimmermann, "The Official PGP User's Guide", MIT Press,. 1994.

[12] Carl Ellison and Bruce Schneier, "Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure", Computer Security Journal, Vol. XVI. Number 1, 2000.

[13] "전자거래 안정성 강화 종합대책", 금융감독원(FSS), 2005. 9.

[14] "금융정보화 주요동향 제84호", 보험개발원(KIDI), 2007. 1.

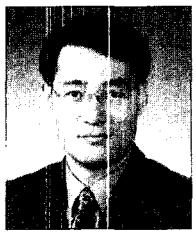
[15] Daniel Brookshier et al., "Chap. 8" JXTA and Security in JXTA: Java P2P Programming", Published by Sams, June, 2002.

[16] Prem Devanbu, et al., "The Next Revolution: Free, Full, Open Person-2-Person (P2P) E-commerce", July 3, 2000.

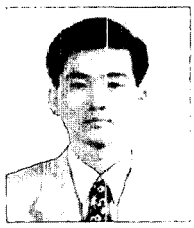
〈著者紹介〉

문용혁 (Yong-Hyuk Moon)
2003년 8월 : 단국대학교 컴퓨터공학과 공학사
2007년 2월 : 한국정보통신대학교(ICU) 컴퓨터 공학 석사
2007년 4월~현재 : 한국전자통신연구원 정보보호연구단 P2P 보안연구팀 연구원
관심분야 : P2P 보안, P2P Traffic Management, Grid 컴퓨팅, 네트워크 보안

권혁찬 (Hyeok Chan Kwon)
1994년 2월 : 서원대학교 전자계산학과 공학사
1996년 2월 : 충남대학교 전산학과 석사
2001년 2월 : 충남대학교 컴퓨터과학과 박사
2001년 1월~현재 : 한국전자통신연구원 P2P보안연구팀 선임연구원
관심분야 : P2P 보안, Mobile IPv6 보안, 네트워크 보안



나 재 훈 (Jae Hoon Nah)
정회원
1985년 : 중앙대학교 컴퓨터공학과 공학사
1987년 : 중앙대학교 컴퓨터공학과 석사
2005년 : 한국외국어대학교 전자정보공학과 박사
1987년 ~ 현재 : 한국전자통신연구원 P2P보안연구팀 팀장
관심분야 : P2P 보안, IPv6/MIPv6 보안



장 종 수 (Jong Soo Jang)
정회원
1984년 : 경북대학교 전자공학과 공학사
1986년 : 경북대학교 전자공학과 공학석사
2000년 : 충북대학교 컴퓨터공학과 공학박사
1989년~현재 : 한국전자통신연구원 정보보호연구단 네트워크보안그룹 그룹장
관심분야 : 네트워크보안, 웹서비스보안, Secure OS, IDS/IPS, Traffic Management