[정보보호] P2P (Peer-to-Peer) 보안 표준화 동향

국제표준화 기구인 ITU-T 내의 SG(Study Group) 17 중 Question 9(안전한 통신 서비스)에서 논의중인 P2P(Peer-to-Peer) 보안 표준작업 관련 진행사항 및 향후 방향에 대해 소개하고자 한다. ITU-T Q.9/SG17에서는 현재 P2P 보안에 대한 요구사항 분석 및 P2P 네트워크의 구조 및 컴포넌트간의 인터페이스 정의에 대하여 논의가 진행 중에 있다.
NGN2005(2005년 9월)에서는 2003년을 기점으로 인터넷에서 가장 많은 트래픽을 P2P 서비스가 차지하고 있다는 통계를 발표하였고, 같은 해 Network World 지에서도 인터넷 트래픽의 60%~89% 정도의 트래픽을 P2P 서비스가 차지하고 있다고 게재된 바 있다. 과거 P2P 서비스로는 Instant messaging, File sharing, Distributed computing 정도를 떠올렸으나, 지금은 VoIP, Video Streaming, Multicast, Web Caching, Game, Virtual office 등 다양한 분야에 응용되고 있으며, 저작권문제나 정보보호 문제와 같은 P2P 서비스의 부작용을 최소화할 수 있는 표준화 분야 등에 관심이 집중되고 있다. 본 고에서는 이러한 P2P에 대한 표준화 동향을 살펴본다.

표준화 관련 이슈 및 현황

P2P 관련 표준화 활동은 IETF, ITU-T, 3GPP 등과 같은 국제 표준화 기구들을 중심으로 이루어지고 있다. 본 절에서는 IETF와 3GPP의 표준 활동에 대하여 개략적으로 소개한다.

1. IETF

P2P-SIP WG(Peer-to-Peer Session Initiation Protocol Working Group)는 제 65차 회의에서 BoF(Birds-of-a-Feather) 미팅이 시작되었다. 본 작업그룹은 세션 설치 및 관리가 중앙서버보다는 단말들의 집합체에 의하여 완전히 또는 부분적으로 처리되는 설정에서 SIP세션 이용을 위한 메커니즘과 가이드라인을 개발하는 것에 주된 목적을 두고 있다. 이러한 아이디어는 서비스 공급자의 Proxy들에 의존하는 기존 SIP 접근법의 대안이 될 수 있을 것으로 예상된다. SIP에 P2P 기술을 도입하려는 주된 이유는 P2P의 확장성과 서버 유지비용의 절감에 있으며, 수 백만 개 Peer들의 등록과 위치정보를 관리해야 하는 SIP 서버들의 역할에 P2P 기술을 활용하고자 하는 것이다.

2. 3GPP

3GPP(The 3rd Generation Partnership Project)는 PCG(Project Co-ordination Group)를 중심으로 하위 4개의 TSGs(Technical Specification Groups)로 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 표준화를 추진하고 있다.

표준화 쟁점사항

ITU-T의 SG 17 은 정보보호, 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 통신을 위한 보안 요구사항(위협 분석 등)에 관한 표준안 X.p2p-1과, 한국 측에서 P2P 네트워크를 위한 보안 구조 및 프로토콜에 관한 표준안 X.p2p-2를 담당하기로 결정되었다.
현재 P2P 보안 요구사항(X.p2p-1) 표준안은 많은 부분이 완성되었으며, Skype와 같은 대표적인 상용 서비스가 P2P 모델 분류에 수용 될 수 있도록 검토되고 있으며, 취약성 분석 관점에서 MITM (Man-In-The-Middle), Sybil, Whitewashing 공격이 항목에서 누락되었음이 검토되어 P2P 보안 취약성을 재검토 하기로 하였다. P2P 보안 구조(X.p2p-2) 문서는 모든 P2P 서비스를 포함할 수 있는 모델들을 분류하고, 이 모델들에 공통적인 P2P 네트워크 구조와, 이에 따르는 각 네트워크 컴포넌트들의 인터페이스 제안을 추진 중에 있다. P2P 보안 프로토콜의 세부 정의는 향후 아이템으로 남겨질 것이며 이에 대하여 각국의 열띤 논의가 벌어질 것으로 예상된다. 가장 유력한 분야는 P2P 환경에서의 신뢰적 ID 생성(인증) 메커니즘이 되며, 이미 한국과 중국에서 이 분야에 관심을 보이고 있어서 현재까지 2편의 기고서 제안이 있었다.

향후 전망

얼마 전까지만 해도 저작권 문제 등으로 P2P 서비스가 '문제아' 정도로 인식되었으나, 최근 들어서는 P2P를 응용 인프라 구축을 위한 하나의 통신계층으로 보는 인식이 형성되고 있다. 즉, P2P 서비스는 이미 사이버 공간에서 깊이 자리를 잡아가고 있다. 이러한 모델이 점차 순기능으로 전환이 될 것이라고 믿고 있으며, 또한 그러한 노력이 많이 진행되고 있다. 이러한 시점에서 향후 세계적으로 차세대 콘텐츠의 역점 기술로 각광을 받게 될 N:N 기술(미들웨어, 프레임워크, 서비스)에 대한 표준 선점을 하여, 국가와 기업의 경쟁력을 제고하는 기회를 삼는 것이 필요하다고 사료된다.

나재훈 (한국전자통신연구원 P2P보안연구팀장, jhnah@etri.re.kr)