국내 P2P 서비스 환경 하에서의 보안 취약점 및 위협 요소 분석

신원* · 이경현**

Risk Analysis on Vulnerabilities and Threats for Domestic P2P Service Environments

Weon Shin* · Kyung-Hyune Rhee**

요 약

최근 P2P는 인터넷에서 매우 대중화된 서비스로 다양한 분야에 응용되고 있으나, P2P 네트워크 특성에 따른 취약점으로 인해 여러 가지 보안 위협이 등장하고 있다. P2P 네트워크는 인터넷을 기반으로 하는 오버레이 네트워크 형태이기 때문에 기존의 인터넷 환경에서 발생하는 보안 문제뿐만 아니라 P2P 네트워크 자체만의 보안 문제도 가지고 있다. 본 논문에서는 국내 상용 P2P 서비스의 취약점 및 위협 분석을 다양한 실험을 통하여 수행한 후 위험분석을 수행하고 대응방안을 제시하였다.

ABSTRACT

Recently P2P is the most popular network service on Internet and is applied various areas such as streaming, file sharing and software distribution, but there are many security threats depending on vulnerabilities by P2P network environments. Conceptually P2P network is a overlay network based on Internet, and it has security concerns of itself as well as those of Internet environments. In this paper, we analyze the vulnerabilities and threats for domestic P2P services through various experiments and describe their risk analysis. We expect that this work contributes to new domestic P2P services in consideration of service qualities and security vulnerabilities.

키워드

P2P, 오버레이 네트워크, 취약점, 위협, 위험관리

Key word

P2P, Overlay network, Vulnerability, Threat, Risk analysis

* 정회원 : 동명대학교 정보보호학과 (주저자, shinweon@tu.ac.kr)
** 정회원 : 부경대학교 IT융합응용공학과 (교신저자)

접수일자 : 2012. 03. 02
심사완료일자 : 2012. 03. 21

Open Access http://dx.doi.org/10.6109/jkiice.2012.16.7.1447

Ⅰ. 서 론

최근 P2P는 인터넷에서 매우 대중화된 서비스로 비디오 스트리밍, 파일 공유, 소프트웨어 배포 등 다양한 분야에 응용되고 있으나, P2P 네트워크 자체가 가진 취약점으로 인해 여러 가지 보안 문제가 등장하고 있다. 그 중 P2P 네트워크를 이용한 악성코드 확산과 P2P 봇넷(Botnet) 기반의 분산서비스거부(DDoS, Distributed Denial of Service) 공격 등이 최근 심각한 위협으로 대두되고 있다. 따라서, 신뢰성 있고 안전한 P2P 서비스가 운영되기 위해서는 P2P 네트워크의 구조적 특성을 파악하고 P2P 서비스 제공시 관련한 취약점 분석으로 P2P 네트워크 위협을 사전에 차단하고 탐지할 수 있는 대응이 필요하다.

특히, 국내 P2P는 상업용 서비스에 초점을 맞추고 있으며 콘텐츠 중계 및 방문자 광고 노출을 통하여 수익을 창출하는 구조이고, 해외 유명 P2P와는 달리 콘텐츠 배포와는 별도로 사용자 인증과 요금 결제를 위한 중앙 서버가 존재하는 구조로 되어 있다. 이러한 특징으로 인하여 국내 P2P 서비스는 다양한 취약점을 내포하고 있으며, 국내 P2P 서비스 업체는 대부분 영세한 업체이므로 취약점 및 침해 발생 시 즉각적인 대응이 어려운 상태이다. 최근에는 취약한 P2P 서버 운영으로 악성 코드 및 개인정보 유출의 온상이 되고 있으며, 콘텐츠의 악성코드 모니터링과 적극적인 대응이 어렵기 때문에 지속적인 해킹으로 인하여 악성코드 유포에 이용되기도 한다.

본 연구에서는 국내 P2P 네트워크 구조의 취약점을 분석하고 P2P를 기반으로 발생할 수 있는 각종 위협에 대한 위험 분석을 연구 목표로 한다. 본 연구 결과는 국내의 안전한 P2P 서비스 운영의 기반기술로써 활용할 수 있으며 향후 등장하는 새로운 P2P 서비스에 대한 안전성 제고에 기여할 수 있을 것으로 예상한다. 본 논문의 구성은 먼저 2장에서 P2P 네트워크 구조와 국내 P2P 서비스 현황을 살펴보고, 3장에서 국내 P2P 서비스의 위협과 취약점을 분석한다. 4장에서는 국내 P2P에 대한 위험 분석을 수행하고, 마지막 5장에서 결론을 맺는다.

Ⅱ. P2P 개요와 국내 서비스 현황

2.1. P2P 오버레이 네트워크 개요

P2P 기술은 기존의 클라이언트/서버 방식과 달리 PC들이 연결되어 자원을 공유하고 모든 참여자가 서버인 동시에 클라이언트의 역할을 수행하는 특징을 갖는다. 즉, 참여자인 피어(Peer)들이 P2P 서비스에 등록하면, 물리적 네트워크 구성과는 별개로 등록된 피어들 간의 가상 네트워크인 P2P 오버레이 네트워크(Overlay Network)가 만들어진다[1][2]. P2P 오버레이 네트워크상에서 피어들은 서버의 도움 없이 다른 피어들과 직접 정보를 공유하고 교환할 수 있다. 이러한 P2P 개념은 단순

표 1. P2P의 분류
Table. 1 P2P classification

분류	세부	내용
중앙집중형 P2P		• 중앙 서버가 모든 피어들을 관리하며 메시지 전달을 매개하는 구조 • 중앙 서버가 지속적으로 서비스를 제공하므로 각 피어가 효율적으로 정보를 검색하고 저장할 수 있는 장점을 가지나 피어의 수가 늘어나게 되면 서버의 부하 또한 커지게 되어 확장성 문제가 발생 • 특히, 중앙 서버에 문제가 생기면 네트워크 전체가 동작하지 않음
분산형 P2P	Unstructured P2P	• 중앙 서버가 존재하지 않고, 모든 피어들이 자발적으로 참여하여 P2P를 유지하며 메시지를 전달하고 서비스를 제공 예) Gnutella[5], KaZaA[6], BitTorrent[7] • 분산된 네트워크의 자원을 효율적으로 탐색하는 것이 어려우므로, 다른 구조의 P2P 네트워크에 비해 네트워크 트래픽이 많이 발생
	Structured P2P	• 분산 인덱싱을 제공하여 콘텐츠와 피어들을 공통의 단일 주소 공간으로 매핑하는 분산 구조 예) Kademlia[8], eDonkey[9] • 구조적인 자체 네트워크를 구성하지만, 라우팅 알고리즘이 복잡하고, 피어들의 참여와 탈퇴를 처리하기 위한 네트워크 유지보수에 많은 비용 발생

히 컴퓨터와 컴퓨터가 연결됨을 의미할 뿐만 아니라, 이를 통해 더 빠르고 안전한 네트워크 자원의 공유와 데이터 처리를 수행할 수 있게 되었다.

P2P 네트워크는 오버레이 네트워크 구성 방법에 따라 표 1과 같이 중앙 집중형 P2P 네트워크, 분산형 P2P 네트워크로 분류할 수 있다. 그 중 분산형 P2P 네트워크는 동작 방식과 구조에 따라 Unstructured P2P와 Structured P2P로 다시 나뉜다[3][4].

2.2. 국내 P2P 동작과 특징

국내 P2P 서비스는 회원 가입을 통하여 음악 파일, 동영상, 프로그램 등을 공유하고 있으며 대부분 하이브리드 방식으로 동작하는데, 로그인 시에는 중앙집중형 P2P로 동작하고 콘텐츠 배포 시에는 비구조적 P2P로 동작한다. 그림 1은 이러한 국내 P2P 동작 방식을 보여준다. 동작 방식의 한 예로써, ① 피어 a.b.137.128은 서버(c.d.196.32)에 접속하여 로긴 후, 다운로드 받을 콘텐츠를 검색한다. ② 피어 a.b.137.128은 서버(c.d.196.32)로부터 콘텐츠를 가진 피어의 정보를 얻은 후 해당 피어(g.h.228.76, i.j.186.182)로부터 콘텐츠를 다운로드 받는다.

국내 P2P 서비스의 특징은 다음과 같이 요약할 수 있다. 첫째, 국내 P2P는 상업용 서비스에 초점을 맞추어 서비스 되고 있다. 해외 P2P 서비스는 대부분 콘텐츠 배포를 위해 분산형 P2P 형태를 취하므로 별도의 서버 개념이 없으나, 국내 P2P는 콘텐츠 배포와는 별도로 사용자 인증과 요금 결재를 위한 중앙 서버가 존재하는 구조이며 이를 통하여 콘텐츠 중계 및 방문자 광고 노출 등을 통하여 수익을 창출하는 방식을 취하고 있다. 둘째, 국내 P2P 서비스는 대부분 하이브리드 방식으로 동작한다. 즉, 사용자 인증 및 사용량에 따른 요금 결재 시에는 중앙집중형 P2P 방식으로 동작하여 중앙 서버에 접속하도록 하고, 콘텐츠 배포시에는 분산형 P2P 방식 중 비구조적 P2P로 동작하여 각 피어들끼리 콘텐츠를 업로드/다운로드를 수행하는 구조이다. 셋째, 국내 P2P 업체는 콘텐츠 중계 및 디렉터리 역할을 수행한다. 여기서, 중앙 서버는 사용자가 요청한 콘텐츠를 소유한 대상 피어에 대한 정보만을 제공함으로써 검색된 콘텐츠 업로드/다운로드는 해당 피어들 간의 개별적인 통신으로만 수행하도록 한다. 이는 콘텐츠에 대한 저작권 문제를 해결하기 위한 방편이라 할 수 있다. 마지막으로 국내 P2P 서비스 업체는 대부분 영세한 업체이다. 따라서, 서비스에 대한 보안 취약점 및 침해 발생 시 즉각적인 대응이 어려운 상황이다.

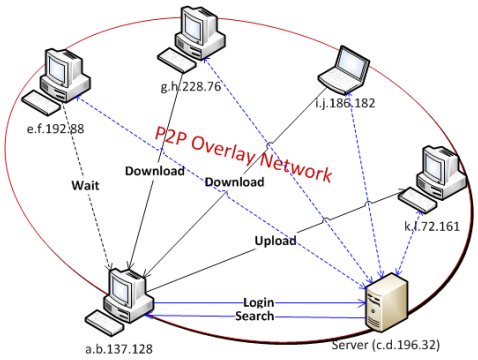

그림 1. 국내 P2P 동작 방식
Fig. 1 The behavior of domestic P2P

Ⅲ. 국내 P2P 보안 취약점

3.1. P2P 보안 취약점 분석 환경

국내 P2P 서비스의 보안 취약점을 분석하기 위한 기본 환경 구성과 분석 방법은 다음과 같다. 그림 2는 취약점 분석 환경을 간략히 보여주고 있다.

○ 운영체제가 설치된 VMWare Image 준비

가상화 소프트웨어 중 가장 많이 사용하는 VMware에 기본 운영체제를 설치하여 유무선 인터넷 연결 설정 후 국내 P2P 프로그램 개별 설치를 통한 각종 분석을 실시한다.

○ 기본 가상 이미지 설정

P2P 프로그램 이외에 다른 요인을 최소화하기 위한 방편으로 운영체제 환경설정 후 분석 도구만 설치된 가상 이미지를 기본 이미지를 설정하여 동일한 환경을 구성하고, 기본 가상 이미지를 복사하여 각각 운영체제 부팅 후 P2P 프로그램 설치 및 분석 동작을 수행한다.

○ 취약점 분석 방법

P2P 서비스의 취약점 분석 방법은 다음과 같다.

- 운영체제 기본 명령 활용 : 작업관리자(Task Manager), 네트워크 명령어 netstat, ipconfig 등 사용
- 레지스트리 및 설치 파일 분석 : Systrace 도구를 이용하여 변경/생성된 새로운 레지스트리, 각종 설치 파

일 분석

- 프로세스 및 네트워크 연결 분석 : Pstools 도구를 이용하여 실행 프로세스 상태 분석 및 네트워크 설립 분석
- 패킷 분석 : Wireshark 및 MS Network Monitor 도구를 이용하여 로그인 동작, 콘텐츠 검색, 콘텐츠 다운로드/업로드 분석과 패킷 모니터링 수행

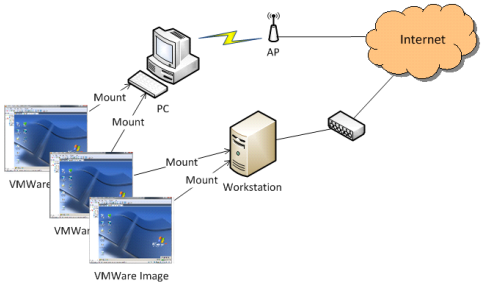

그림 2. 취약점 분석 환경
Fig. 2 Experiments of vulnerability analysis

3.2 보안 취약점 분석 방법

P2P 보안 취약점 분석은 표 2와 같이 정적 분석 방법과 동적 분석 방법으로 나누어 수행하였다. 정적 분석은 P2P 관련 프로그램을 설치하고 난 후 프로그램 실행 만으로 이루어지며 레지스트리 분석, 파일 분석, 프로세스 분석, 로그인 분석을 포함한다. 이와 달리 동적 분석은 P2P 관련 프로그램을 설치하고 난 후 로그인을 통하여 콘텐츠를 다운로드/업로드를 하면서 프로세스 분석, 네트워크 연결 분석, 콘텐츠 검색, 콘텐츠 다운로드 & 업로드 분석을 포함한다.

표 2. 정적 분석 방법과 동적 분석 방법
Table. 2 Static and dynamic analysis

분류	정적 분석	동적 분석
방법	레지스트리 분석 파일 분석 프로세스 분석 로그인 분석	프로세스 분석 네트워크 연결 분석 콘텐츠 검색 콘텐츠 다운로드/업로드
시점	P2P 프로그램 설치 및 실행 시점	P2P 프로그램 로그인 후 시점 콘텐츠 검색 시점 콘텐츠 다운로드/업로드 시점

3.3. 국내 P2P 보안 취약점과 위협

P2P 취약점 분석 대상을 선정하기 위하여 국내 유명 포털 사이트에서 디렉터리 검색을 수행하고 P2P 인기도 순 Top 10을 후보로 하였다. 국내 P2P 보안 취약점은 표 3과 같이 분류할 수 있다.

표 3. 국내 P2P 보안 취약점 분류
Table. 3 Vulnerabilities of domestic P2P

분류	세부 내용
컴퓨팅 환경 임의 변경	공유 목적의 폴더 임의 설정 신뢰 사이트 등록 방화벽 설정 임의 변경 그리드 딜리버리 서비스 설치 제휴 프로그램 자동 시작 등록
사용자 컴퓨터 과부하 유발	사용자 동의 없이 시작 프로그램 및 즐겨찾기 등록 지속적인 연결 설립 그리드 딜리버리 동작에 따른 과부하
중요정보 유출 및 조작	개인정보 및 로그인 정보 유출 성인 인증 정보 조작
웹사이트 보안 문제점	취약한 플랫폼 XSS(Cross-Site Scripting)에 취약
서비스 이용 약관 문제	무분별한 개인정보 수집 개인정보의 제3자 제공

국내 유명 P2P 서비스에 대해서 앞에서 설명한 보안 취약점 분석 방법인 각종 정적 분석 및 동적 분석을 수행하여 얻은 보안 취약점과 해당 위협은 표 4와 같다.

VI. 국내 P2P 위험분석

4.1. P2P 위험분석 절차

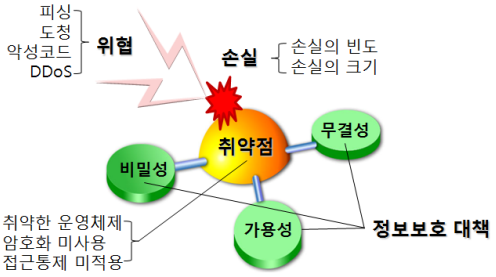

그림 3. 위험분석 구성요소
Fig. 3 Components of risk analysis

국내 P2P 위험분석 구성요소와 각 요소들의 관계를 그림 3에서 개략적으로 보여준다. 특히 손실은 위험도 산정을 위하여 필수적인 요소인데, 일반적으로 손실의 크기(또는 자산의 중요도)와 빈도(또는 발생가능성)에 따라 산정한다.

본 연구에서 수행하는 국내 P2P 위험분석 절차는 다음과 같다.

① 위험분석 범위 선정 : P2P 서비스, 정보 및 가용자 특성에 따라 가능한 국내 정보보호관리체계 범위에 근거한 위험분석 범위를 선정

표 4. 국내 P2P 서비스의 보안 취약점
Table 4. Security vulnerabilities of domestic P2P services

분류	위협(T)
A1. 공유 목적의 폴더 임의 설정	T1.1. 각종 콘텐츠 및 사용자 개인 파일이 본인 모르게 P2P를 통하여 배포되어 다른 피어에게 유출 가능성이 존재 T1.2. 유출된 콘텐츠 및 사용자 개인 파일에 의한 피싱, 위장 등 2차적인 피해 발생 가능
A2. 신뢰할 수 있는 사이트 등록	T2.1. P2P 사이트가 신뢰할 수 있는 사이트로 등록됨으로써, 사용자 PC의 IE(Internet Explorer)를 통해 신뢰할 수 없는 임의의 콘텐츠 설치 및 동작 유도 가능 T2.2. 인증되지 않은 ActiveX 컨트롤, 기타 프로그램 및 코드는 보안경고 없이 설치가 가능하므로 사용자는 어떠한 프로그램이 설치되는지 확인할 수 없음
A3. 방화벽 설정 임의 변경	T3.1. P2P 콘텐츠 배포를 위한 포트가 열려있어 다양한 정보 제공으로 취약점 노출 가능 T3.2. 방화벽 정책에 네트워크 접속이 허용가능하도록 설정된 파일 및 프로세스로 위장한 악성코드 설치 가능 T3.3. 방화벽은 인터넷 IP 주소와 해당 포트만을 필터링하므로 콘텐츠 자체에 대한 필터링은 불가능하므로 내부 정보 유출이나 악성코드 설치와 같은 위협 존재
A4. 그리드 딜리버리 서비스 설치	T4.1. 무제한적인 그리드 딜리버리 동작에 의해 과부하 발생으로 다른 프로그램 동작을 방해하거나 네트워크 자원의 소모 발생 T4.2. 사용자의 의지와 상관없이 프로세스 및 네트워크 자원을 서비스 업체에서 임의로 제어
A5. 제휴 프로그램 자동 시작 등록	T5.1. 사용자 검색어 등의 개인정보를 활용하여 맞춤형 광고를 수행하거나 관련 온라인 쇼핑몰 연결을 유도 T5.2. 악성코드로 볼 수 없는 코드를 악성코드로 보고하여 사용자의 불안을 야기함으로써 악성코드 치료를 명목으로 지속적인 결재를 요구하여 금전적인 피해 발생 가능
A6. 상업적인 프로그램의 시작 메뉴 및 즐겨찾기 등록	T6.1. P2P와 상관없는 각종 상업적인 프로그램을 설치하고 사용자 관심을 유도하고 관련 사이트 연결로 동작 방해 T6.2. P2P 프로그램과 연계한 사용자 개인정보의 유출 가능
A7. 쿠키에 의한 개인정보 노출	T7.1. 사용자 PC에 특정 프로그램을 설치하여 개인정보 유출 가능 T7.2. 네트워크 중간에서 도청을 통해 개인정보 탈취 가능 T7.3. 탈취한 개인정보를 수집하여 피싱 등에 활용하여 금전적 피해 야기 가능
A8. 로그인 정보 노출	T8.1. 사용자 PC에 특정 프로그램을 설치하여 개인정보 유출 가능 T8.2. 네트워크 중간에서 도청을 통해 로그인 정보 탈취 가능 T8.3. 탈취한 로그인 정보를 이용하여 정상 사용자로 위장 후 각종 콘텐츠 구입 및 다운로드를 수행하여 금전적 피해 야기 가능 T8.4. 탈취한 개인정보를 수집하여 피싱 등에 활용하거나 새로운 사용자 ID 발급 등으로 금전적 피해 야기 가능
A9. 웹사이트 보안 문제점	T9.1. 취약한 서버 운영으로 이미 알려진 취약점을 이용한 악성코드 및 해킹 위협에 노출 T9.2. Directory Traversal 또는 Directory Listing 등으로 웹사이트 구조 파악 가능 T9.3. SQL Injection으로 데이터베이스를 접근하여 개인정보의 유출/조회/검색 등 가능 T9.4. File Upload 또는 Source Code Injection으로 내부 명령어 실행 후 시스템 제어 및 각종 정보 유출 가능 T9.5. XSS 등에 취약한 웹사이트 운영으로 개인정보 유출 가능성
A10. 서비스 이용 약관 상의 문제	T10.1. 서비스 제공을 위해 필요한 최소한의 정보 수집, 수집된 정보의 제3자 제공 절차, P2P 서비스 탈퇴시 개인정보 파기 요건 등의 불만족 T10.2. 콘텐츠에 대한 각종 저작권 관련 문제 발생시 서비스 제공자의 책임 회피 T10.3. 약관에 명시되지 않은 임의의 스파이웨어 설치를 허용하여 개인정보 유출 발생 가능 T10.4. 서비스 제공자의 상업적인 의도에 따라 사용자 PC를 조정할 수 있는 권한 부여

② 위험분석 방법 정의 : 효율적인 위험분석 수행을 위하여 계량화 여부에 따른 정성적 방법을 선택하고, 접근방법에 따라 기준선 접근법을 기반으로 전문가 판단법을 함께 사용
③ 항목 분석 : 연관된 정보 및 정보시스템을 포함하는 항목을 식별하고, 해당 항목의 기밀성, 무결성, 가용성이 상실되었을 때의 결과가 조직에 미칠 수 있는 영향을 고려하여 가치를 평가
④ 위협 분석 : 위협의 식별 및 발생 가능성 정도를 전문가 의견 또는 내부 토론을 통하여 측정
⑤ 취약점 분석 : 식별된 위협에 대하여 자산항목이 어느 정도 취약한가를 전문가 의견 또는 내부 토론을 통하여 판명
⑥ 우려사항 분석 : 데이터 또는 정보와 같이 위협과 취약점의 구분이 어려운 경우는 우려사항이라는 용어의 정의로서 이용 가능
⑦ 위험도 산정 : 식별된 자산, 위협 및 취약점을 기준으로 위험도를 산출하고 기존의 보호대책을 파악한 후 식별된 항목별 위협, 취약점 및 위험도를 정리하여 위험을 평가
⑧ 보호대책의 선정 : 위험도 평가결과를 토대로 해당 위험도를 수용 가능한 위험수준(DoA)까지 낮추기 위한 보호대책을 선정

4.2. 수용가능 위험 수준에 따른 정보보호 대책

수용가능한 위험 수준의 분석을 위해 DoA(Degree of Acceptance)를 중요도 7.5와 빈도 7.5로 잡으면, 그림 4와 같다.

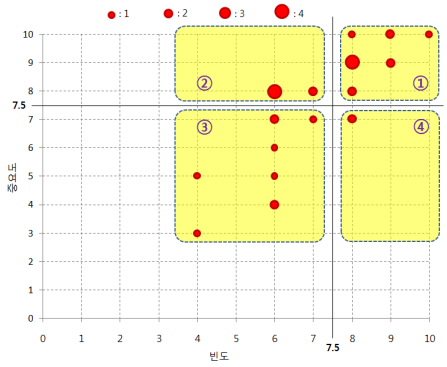

그림 4. 위험수준 평가를 위한 DoA 적용
Fig. 4 A DoA for acceptable risk

위 보장수준에 따른 각 취약점 및 위협에 대한 정보보호 대책은 표 5와 같다.

위험 수준에 따른 정보보호 대책은 다음과 같이 시행된다.

○ 위험수용
- 현재의 위험을 받아들이고 잠재적 손실 비용을 감수하는 것
- 어떠한 대책을 도입하더라도 위험을 완전히 제거할 수 없으므로, 일정수준 이하의 위험은 감수하고 P2P 사용

○ 위험관리
- 잠재위험으로 주변 환경의 변화에 따라 위험요인으로 변화가 가능하므로 지속적인 모니터링 실시

○ 위험감소
- 직접적인 피해가 발생할 수 있는 중대한 위험을 잠재하고 있으므로 정보보호대책을 선택하여 구현

○ 위험회피
- 위험이 존재하는 P2P를 사용하거나 서비스하지 않고 포기

V. 결 론

P2P 시스템은 네트워크 환경에서 중앙 서버 없이 분산 자원의 공유를 목적으로 동등한 자격을 가진 피어로 이루어진 자율 구성 네트워크이다. 이러한 기본 개념을 통하여 P2P는 수동적 협조에서 능동적 협동, 집중화에서 분산화로의 패러다임 변화를 주도하여, 대중화된 서비스로 비디오 스트리밍, 파일 공유, 소프트웨어 배포 등 다양한 분야에 응용되고 있다.

특히, 국내 P2P 서비스의 대부분은 콘텐츠 중계 및 방문자 광고 노출을 통하여 수익을 창출하는 상업용 서비스에 초점을 맞추고 있으므로, 해외 P2P와는 사용자 인증과 요금 결제를 위한 중앙 서버가 존재하는 구조이다. 이러한 국내 P2P 서비스만의 독특한 특징으로 인하여 해외 P2P 서비스와 다른 다양한 취약점을 내포하고 있다. 그러나, 국내 P2P 서비스 업체는 대부분 영세한 업체이어서 취약점 및 침해 발생 시 즉각적인 대응이 어려운 상태이다. 뿐만 아니라 최근에는 취약한 P2P 서버 운영으로 악성 코드 및 개인정보 유출의 온상이 되고 있으나, 콘텐츠의 악성코드 모니터링과 적극적인 대응이 어렵

표 5. P2P 취약점과 위협에 따른 정보보호대책
Table 5. Safeguards against P2P vulnerabilities and threats

취약점(V)	위협(T)	정보보호대책
V1 P2P 프로그램이 공유 목적으로 공유 폴더를 임의로 설정	T1.1. 각종 콘텐츠 및 사용자 개인 파일이 본인 모르게 다른 피어에게 유출	위험수용
	T1.2. 유출된 파일에 의한 피싱, 위장 등 2차적인 피해 발생	위험관리
V2 레지스트리 변경을 통하여 P2P 사이트의 도메인 주소를 IE의 신뢰할 수 있는 사이트로 등록	T2.1. 신뢰할 수 있는 사이트로 등록되어 사용자 PC의 IE를 통해 임의의 콘텐츠 설치 및 동작 유도	위험감소
	T2.2. 인증되지 않은 ActiveX 컨트롤, 기타 프로그램 및 코드는 보안경고 없이 설치 가능	위험감소
V3 방화벽 관련 레지스트리 값 임의 수정	T3.1. P2P 콘텐츠 배포를 위한 포트를 통해 다양한 정보 제공	위험감소
	T3.2. 방화벽 정책을 수정하여 악성코드 설치	위험관리
	T3.3. 방화벽을 통한 내부 정보 유출이나 악성코드 설치 발생	위험관리
V4 그리드 딜리버리 서비스 자동 시작 등록	T4.1 다른 프로그램 동작을 방해하거나 네트워크 자원의 소모	위험수용
	T4.2 프로세스 및 네트워크 자원을 서비스 업체에서 임의로 제어	위험수용
V5 사용자 확인 없이 제휴 프로그램 자동 시작 등록	T5.1 개인정보를 활용하여 맞춤형 광고를 수행하거나 관련 온라인 쇼핑몰 연결을 유도	위험수용
	T5.2 사용자 불안을 야기하여 악성코드 치료를 명목으로 금전적인 피해 발생	위험감소
V6 사용자 동의 없이 임의로 상업적인 프로그램의 시작메뉴, 단축아이콘, 즐겨찾기에 등록	T6.1 상업용 프로그램을 설치하고 사용자 관심을 유도, 관련 사이트 연결로 동작 방해	위험수용
	T6.2 P2P 프로그램과 연계한 사용자 개인정보의 유출 가능	위험수용
V7 사용자 PC의 쿠키에 검색정보, 성별, 이름, 나이 등 개인정보 저장	T7.1. 개인정보 유출 가능	위험수용
	T7.2 도청을 통한 개인정보 탈취 가능	위험수용
	T7.3 탈취한 개인정보를 활용하여 금전적 피해 야기	위험관리
V8 로그인시 ID, 비밀번호, 주민번호 등 개인정보 노출	T8.1. 개인정보 유출 가능	위험감소
	T8.2 도청을 통한 로그인 정보 탈취 가능	위험감소
	T8.3 정상 사용자로 위장 후 각종 콘텐츠 구입 및 다운로드 수행	위험감소
	T8.4 탈취한 개인정보를 활용하여 금전적 피해 야기	위험감소
V9 오래된 버전의 취약한 P2P 서버 운영	T9.1 취약한 서버 운영으로 악성코드 및 해킹에 노출	위험관리
	T9.2 웹사이트 구조 파악 가능	위험관리
	T9.3 데이터베이스를 접근하여 개인정보의 유출	위험감소
	T9.4 내부 명령어 실행 후 시스템 제어 및 각종 정보 유출	위험감소
	T9.5 XSS 등에 취약한 웹사이트 운영으로 개인정보 유출 가능성	위험감소
V10 사용자 PC에 서비스 약관에도 없는 프로그램 설치 및 설정 변경, 임의적인 개인정보 수집 및 활용, 수집된 정보의 제3자 제공	T10.1 서비스 제공을 위해 필요한 개인정보 취급 방침 불만족	위험감소
	T10.2 각종 저작권 관련 문제 발생시 서비스 제공자의 책임 회피	위험감소
	T10.3 스파이웨어 설치도 허용함으로써 개인정보 유출 발생 가능	위험감소
	T10.4 상업적인 의도에 따라 사용자 PC를 조정	위험감소

기 때문에 지속적인 해킹으로 인하여 악성코드 유포에 이용되고 있는 실정이다.

본 연구에서는 이러한 P2P 통신구조 및 보안체계 연구를 위하여 P2P 오버레이 네트워크 보안 요구사항 분석에 대하여 조사하였고, 국내 P2P 서비스 현황에 따른 취약점 및 위협 분석도 수행하였다. 또한, 국내 P2P 환경 하에서 위협에 대한 대응 방안을 도출한 후 위험분석에 대하여 논의하였다. 본 연구결과는 새로운 P2P 서비스 모델 정립에 정보보호 기반 기술로 활용 가능하고, P2P 통신구조 상의 다양한 요인을 고려한 각종 시뮬레이션

으로 인터넷 환경에서 실제 P2P 취약점 발생 시 피해 정도의 정확한 예측, 과거 P2P를 기반으로 한 악성코드, 공격 패턴의 보다 나은 이해를 통하여 미래에 등장할 P2P 기반 침해의 행동, 특성 및 파급 효과 예측이 가능할 것으로 판단되며 또한, P2P 기술 및 취약성 분석을 통하여 P2P 기반 서비스 및 제품 보호를 위한 대응 방안 마련에 활용할 수 있을 것이다.

참고문헌

[1] Sameh El-Ansary and Seif Haridi, “An Overview of Structured P2P Overlay Networks”, IEEE Communications Surveys and Tutorials, 2005.

[2] Eng Keong Lua, Jon Crowcroft, Marcelo Pias, Ravi Sharma and Steven Lim, “A Survey and Comparison of Peer-to-Peer Overlay Network Schemes”, IEEE Communications Surveys and Tutorials, 2004

[3] Vivek Vishnumurthy and Paul Francis, “A Comparison of Structured and Unstructured P2P Approaches to Heterogeneous Random Peer Selection”, 2007 USENIX Annual Technical Conference, pp.309-322, 2007.

[4] 박호진, 박광로, “P2P 기술 동향 및 홈네트워크 응용”, 전자통신동향분석 제 21권 제 5호, pp.1-10, 2006.

[5] Gnutella, http://en.wikipedia.org/wiki/Gnutella/

[6] KaZaA, http://en.wikipedia.org/wiki/Kazaa

[7] BitTorrent, http://www.bittorrent.com/

[8] Kademlia, http://en.wikipedia.org/wiki/Kademlia/

[9] eDonkey network, http://en.wikipedia.org/wiki/EDonkey_network/

[10] D. S. Milojicic, V. Kalogeraki, R. Lukose, K. Nagaraja, J. Pruyne, B. Richard, S. Rollins, and Z. Xu, “Peer-to-Peer Computing”, HP TechReport HPL-2002-57, 2002.

[11] 권혁찬, 문용혁, 구자범, 고선기, 나재훈, 장종수, “P2P 표준화 및 기술 동향”, 전자통신동향분석 제 22권 제1호 2007.

[12] 개인정보보호 종합지원 포털, http://www.privacy.go.kr/

[13] KISA 정보보호 및 개인정보보호관리체계 인증, http://isms.kisa.or.kr/

[14] 이경현, 신원, “P2P 통신구조 및 보안체계 연구”, 한국정보보호학회, 2011.

저자소개

신원 (Shin, Weon)

2005.3～현재 동명대학교 정보보호학과 전임강사, 조교수, 부교수
2002.3～2005.1 (주)안철수연구소 선임연구원

※관심분야 : 소프트웨어 보안, 악성코드 확산, 디지털 포렌식

이경현 (Kyung-Hyune Rhee)

1982.2～1993.3 한국전자통신연구원 선임연구원
1995.7～1996.7 호주 애들레이드 대학 객원연구원(Post Doc.)
2001.7～2002.7 미국 UC Irvine 방문교수
2002.7～2003.7 필리핀 CPSC 교학부장
2011.7～2012.7 일본 큐슈대학교 방문교수
1993.3～현재 부경대학교 IT융합응용공학과 교수

※관심분야 : 암호이론, 암호프로토콜, VANET 시큐리티, 멀티미디어 보안