DOI: 10.3745/KIPSTC.2009.16C.6.681

국내 포털사이트 음원서비스 취약점분석 및 대응방안 제안

이 상 식[†] · 최 동 현[††] · 원 동 호[†††] · 김 승 주[††††]

요 약

현재 국내 음악산업은 음반시장에서 디지털음악시장으로 중심이 이동하고 있으며, 대부분의 대형 포털사이트에서 디지털 음원서비스를 제공하고 있는 추세이다. 본 논문에서는 국내 포털사이트(도시락, 싸이월드, 네이버)에서 제공하고 있는 음원서비스프로세스를 살펴보고 취약점을 분석한다. 또한 분석된 취약점을 바탕으로 실제 공격을 수행하여 음원서비스의 문제점을 보여준다. 마지막으로 본 논문에서는 이러한 취약점을 해결할 수 있는 기술적인 대응방안을 제안함으로써 기업과 저작권자의 이익을 보호하고자 한다.

키워드 : 보안, 온라인 음원 서비스

Security Analysis on Commercial Online Music Streaming Service and Countermeasures

Sangsik Lee[†] · Donghyun Choi[††] · Dongho Won[†††] · Seungjoo Kim[††††]

ABSTRACT

Nowadays, the music industry is moving from analog to digital. Most of the big portal sites provide commercial online music streaming services according to the tendency. In this paper, we analyze the security of the Korean commercial online music streaming services which are provide by the Korea's major portal sites(Dosirak, Cyworld, and Naver). Moreover, we show attacks on commercial online music streaming services that lead to an infringement of copyright and propose technical countermeasures for online commercial music streaming services, the contributions of the present work are that the measures protect the copyright of the music.

Keywords : Security, Commercial Online Music Streaming

1. 서 론

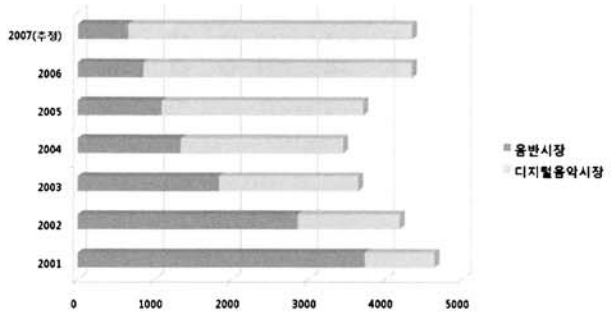
현재 국내 음악산업은 음반시장에서 디지털음악시장으로 중심이 이동하는 추세를 보이고 있으며, 저작권법 강화에 힘입어 유료 온라인 음악에 대한 수요가 늘어가는 가운데 온라인 음원업체들은 다양한 서비스를 도입, 시장을 키워나가고 있다. 대표적으로 싸이월드, 네이버와 같은 포털 사이트들은 미니홈피, 블로그, 카페의 배경음악(BGM) 서비스를 제공하며 유료 온라인음악 시장을 개척하고 있다.

이런 음악산업의 변화는 여러 가지 문제점을 나타냈다. 그중 저작권에 대한 문제가 대표적인 예이다. 근래에 들어 지적 재산권에 대한 법률재판이 많이 이루어지고 있는 실정이며, 소리바다의 서비스중지 가처분 결정과 대형 포털사이트의 저작권침해 혐의 형사 처분 등이 이를 실증해 주고 있다. 이런 사실들로 볼 때 국내 디지털음악시장은 아직 과도기에 있는 단계라고 할 수 있다.

본 논문에서는 현재 제공되고 있는 디지털 음원서비스의 프로세스를 분석하고, 분석을 통해 업계에서 안고 있는 저작권 보호상의 문제점을 기술적인 측면에서 짚어보고 대응방안을 모색함으로써 해결해보고자 한다.

분석은 국내에서 유료 음원서비스를 하고 있는 3가지 대형 포털사이트(싸이월드[2], 네이버[3], 도시락[4])의 음원서비스 프로세스를 분석하고, 취약한 음원서비스 프로세스를 통해 발생할 수 있는 취약점과 그 취약점으로 행해질 수 있는 실제 공격시나리오, 실제로 취약점을 이용해 만들 수 있는 뮤직플레이어를 보여 그 파급효과에 대해서 설명한다. 본 논문을 통해 각 포털사이트의 음원서비스 취약점과 해결방안, 음원서비스 보안모델을 제시하여 성장해가고 있는 디지털음악시장에 저작권보호의 보안적인 측면에 기여하고자

※ 본 연구는 지식경제부 및 정보통신연구진흥원의 대학IT연구센터 지원사업의 연구결과로 수행되었음(IITA-2009-(C1090-0902-0016))
※ 본 연구는 방위사업청과 국방과학연구소의 지원으로 수행되었습니다.(계약번호 UD070054AD)
† 준 회 원 : 성균관대학교 컴퓨터공학과 학부생
†† 준 회 원 : 성균관대학교 휴대폰학과 박사과정
††† 종신회원 : 성균관대학교 정보통신공학부 교수
†††† 종신회원 : 성균관대학교 정보통신공학부 교수(교신저자)
논문접수 : 2009년 3월 13일
수 정 일 : 1차 2009년 8월 18일
심사완료 : 2009년 8월 18일



(단위 : 억원)

	2001	2002	2003	2004	2005	2006	2007(추정)
음반시장	3733	2861	1833	1338	1087	848	650
디지털음악시장	911	1328	1811	2112	2621	3500	3700

(그림 1) 음반시장과 디지털음악시장의 비율[1],
(출처:디지털음악산업발전협의회)

한다.

본 논문의 2장에서는 국내 포털사이트의 일반적인 음원서비스 프로세스에 대해서 살펴보겠다. 3장에서는 각 포털사이트별로 나타날 수 있는 취약점형태 세 가지를 분석하고 이를 통해 발생할 수 있는 실제 공격시나리오와 공격과정을 보여준다. 4장에서는 분석된 취약점을 방어할 수 있는 음원서비스 대응방안을 제안하고, 마지막으로 5장에서 결론을 맺는다.

2. 음원서비스 프로세스 분석

본 장에서는 국내에서 음원서비스를 제공하고 있는 도시락, 네이버, 싸이월드의 일반적인 음원 서비스 프로세스를 분석한다. 그리고 이 분석을 통하여 3장에서는 국내음원 서비스의 취약점을 지적하도록 한다.

각 포털사이트는 자체 제작한 웹기반의 뮤직플레이어를 제공하고 있다. 기본적으로 각 포털사이트에서 제공하는 음원 서비스를 위한 뮤직 플레이어는 모두 설치되었다는 가정하에 설명한다.

국내 포털사이트의 일반적인 음원 서비스 프로세스는

① 사용자가 해당 홈페이지에서 음악을 선택한다.

② 클라이언트에서 서버로 선택한 음악정보와 클라이언트의 인증정보를 전송한다. 음악정보로는 서버에서 인식할 수 있는 음악의 번호(music_num)이다. 클라이언트의 인증정보로는 사용자 식별 아이디(uid), 로그인 하였는지 하지 않았는지 등의 정보를 쿠키나 Request 파라미터를 통해 서버로 전송한다.

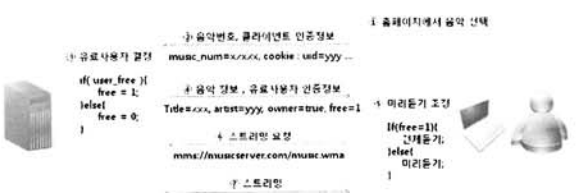
③ 서버는 인증정보를 받아 유료 사용자를 결정한다. 인증정보에 있는 사용자 식별아이디(uid)나, 로그인 유무를 통해 사용자 데이터베이스를 검색해 유료사용자인지 아닌지 선택한다.

④ 서버에서 클라이언트로 음악정보, 유료사용자 인증정보를 전송한다. 서버에서 클라이언트로 전송하는 음악정보로는 노래제목(title), 가수명(artist), 음원의 저장위치 등이 있다. 인증정보로는 현재 사용자가 이 곡을 구매하였는지 판단하는 (owner, free)와 같은 변수가 있다.

⑤ 뮤직플레이어에서 음악정보와 인증정보를 확인, 전체듣기, 미리듣기를 선택한다. 만약 인증정보를 확인하여 현재 사용자가 곡을 구매하였으면 곡 전체를 플레이하고, 곡을 구매하지 않았으면 미리듣기를 선택하여 플레이 시간을 약 1분정도로 제한한다.

⑥ 음악정보를 이용하여 서버에 스트리밍을 요청한다. 클라이언트 측에서 전체듣기, 미리듣기에 따라 음악정보에서 넘어 온 음악번호(music_num) 혹은 음악저장경로에 스트리밍을 요청한다.

⑦ 서버에서 음악을 스트리밍하면 클라이언트측 뮤직플레이어에서 재생한다.



(그림 2) 일반적인 음원 서비스 프로세스

이렇게 서버와 클라이언트는 서로 정보를 주고받으며 음원서비스를 제공하고 있다. 위에서 분석한 일반적인 음원 프로세스는 각 포털사이트의 프로세스를 일반화시켜 독자의 이해를 돕기 위한 것이므로, 실제변수가 아닌 가상의 변수명을 사용하였다. 본 장에서 분석한 프로세스는 각 포털사이트의 통신내용을 일반화시킨 것이며, 음원서비스 프로세스는 전송되는 정보의 순서가 사이트마다 조금씩 상이할 뿐 실행결과에는 영향을 미치지 않는다. 이러한 분석을 바탕으로 앞으로 설명할 3장에서는 위와 같은 음원 프로세스에서 일어날 수 있는 문제점을 취약점별로 나누어, 각 취약점을 가지고 있는 포털사이트를 실례로 들어 설명한다.

3. 취약점을 이용한 뮤직플레이어 공격

본 장에서는 각 취약점별로 현재 포털사이트에서 제공되고 있는 음원서비스의 실제 공격을 해보겠다. 이런 실제 공격을 통해 해당 취약점을 통해서 발생할 수 있는 공격 시나리오를 보이고, 각 시나리오별 영향을 분석한다. 사이트별 통신과정을 분석하기 위해서 Filddler[5] 라는 http debugging proxy 프로그램을 사용한다. 분석된 통신내용을 바탕으로 쿠키값 변조를 위해 Cooxie[6] 라는 쿠키 변조 프로그램을 사용하고, 메시지 변조를 위해 Burp suit[7] 라는 web proxy 프로그램을 사용하였다. 설명 순서는 쿠키값 변조를 통한 공격(도시락), 메시지 변조를 통한 공격(싸이월드, 네이버), 로컬 자바스크립트 변조를 통한 공격(싸이월드, 네이버)

순으로 설명한다.

3.1 쿠키값 변조를 통한 공격(도시락)

쿠키란 하이퍼텍스트의 기록서(HTTP)의 일종으로서 인터넷 사용자가 어떠한 웹사이트를 방문할 경우 그 사이트가 사용하고 있는 서버에서 인터넷 사용자의 컴퓨터에 설치하는 작은 기록 정보 파일을 일컫는다. 이 기록 파일에 담긴 정보는 인터넷 사용자가 같은 웹사이트를 방문할 때마다 서버로 전송되며, 웹 애플리케이션은 전송된 쿠키 정보를 바탕으로 웹 사이트에 방문한 사용자를 기억할 수 있고 사용자 별로 개인화된 컨텐츠를 제공할 수 있다[8]. 도시락은 쿠키를 통해 사용자 인증정보를 저장한다. 공격자는 이 쿠키값을 변조하여 유료사용자로 위장할 수 있다. 쿠키값 변조는 정상적인 음원 서비스와 쿠키값 변조를 통한 음원서비스 공격의 비교를 통하여 설명하겠다.

3.1.1 정상적인 음원 서비스 브로드 캐스팅

먼저 로그인을 하지 않았을 때 정상적인 도시락의 음원서비스를 설명한다.

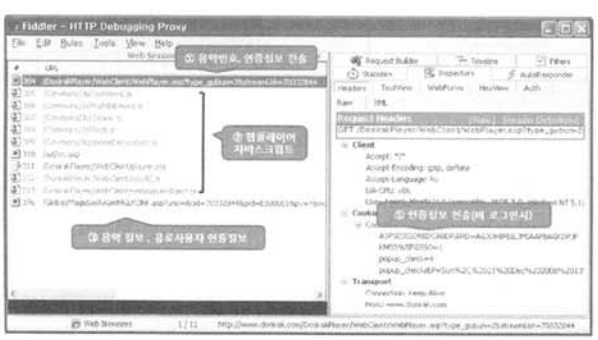
도시락의 정상적인 음원서비스 과정을 Fiddler를 통해 분석해보면

① 음악번호와, 인증정보를 서버로 전송한다. (그림 3)에서 보면 음악정보로는 Request 인자로 streamList 값을 통해 전송되는 것을 알 수 있고, 인증정보는 쿠키값을 통해 전달되는 것을 알 수 있다. 하지만 현재 (그림 3)에서는 로그인을 하지 않은 상태이기 때문에 사용자 정보가 포함되어 있지 않다. 다음 장에서 쿠키값 변조를 통한 공격을 보여주면서 쿠키 정보의 내용을 설명하도록 하겠다.

② 서버로부터 뮤직플레이어를 다운로드한다. 클라이언트 측에 자바스크립트로된 뮤직플레이어를 다운로드 하는 과정이다.

③ 서버로 음악정보를 요청한다. 세 번째 과정은 음악정보와 유료사용자 인증정보를 서버로 요청하는 과정이다.

세 번째 과정에서 음악정보와 사용자정보를 Request 파라미터로 서버에 전송하면 Response 결과로 아래와 같은 결과가 전송된다.



(그림 3) 비로그인시 도시락 정상 음원 프로세스

```
〈ASX version="3.0"〉
〈ENTRY〉
 〈TITLE〉Dosirak   Music Service〈/TITLE〉
 〈REF HREF="mms://kt68kmssst.dosirak.com/MP/1/
70332844/70332844_192K.wma" /〉
〈/ENTRY〉
〈/ASX〉
```

(그림 4) 비로그인시 Global/MagicLock/GetMGLKCInt.asp 결과값

(그림 4)의 정보는 플레이어가 스트리밍서비스를 받을 음악의 주소이다. 하지만 인증정보가 없는 비로그인시의 결과값이므로 위 주소로 접속을 하면 미리듣기 시간(1분)밖에 플레이 되지 않는다. 이와 같은 과정이 도시락의 비로그인시 정상적인 음원서비스의 과정이다.

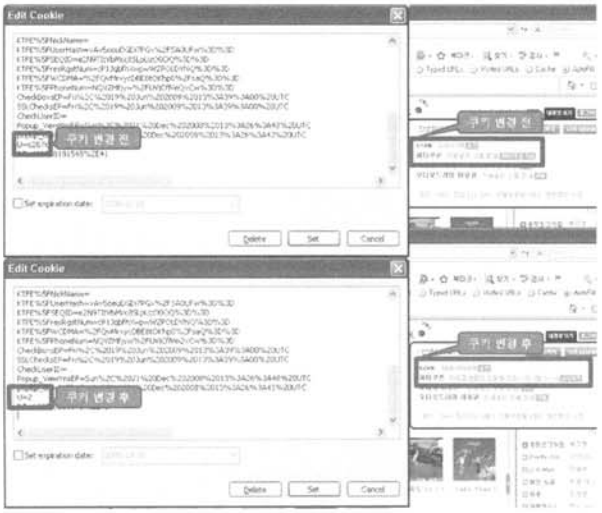
3.1.2 쿠키값 변조를 통한 음원 서비스 공격

3.1.1 절에서 비로그인시 도시락의 정상적인 음원서비스와 비교하여 본 절에서는 인증정보가 담긴 쿠키값 변조를 통한 음원서비스를 공격한다. 로그인시 도시락의 통신내용을 Fiddler로 분석해보면 (그림 5)와 같다.

(그림 5)에서 로그인을 한 상태에서 서버에 음악을 요청하는 Request의 쿠키를 분석해보면 사용자에 대한 개인정보의 일부 값 들이 암호화되어 저장되는 것을 확인할 수 있다. 많은 사용자 개인정보와 인증정보가 있지만 공격자는 'U' 변수에 주목한다. 'U' 변수는 사용자의 구분번호이다. 공격자는 'U' 변수를 변경 시켜 다른 사용자로 서버에 인식시킬 수 있다.

(그림 6)은 'U'변수를 변경하여 돈을 지불하지 않은 사용자가 유료사용자로 서버에 인식되는 화면을 보여준다. 이렇게 공격자는 쿠키값을 변조하여 타인의 유료서비스를 이용할 수 있다. 도시락의 쿠키는 일부분 암호화 되어있다. 하지만 (그림 6)과 같이 사용자 정보가 암호화되어 저장된다고 하여도 일부 암호화되지 않은 부분으로 인해 암호화의 효과

(그림 5) 로그인시 도시락의 쿠키 인증정보



(그림 6) 쿠키변조로 인한 사용자 변경

를 볼 수 없는 경우가 발생한다. 또한 한 개의 인자 값으로 사용자를 인증한다는 것은 아주 위험하다. 이렇게 변경된 사용자가 유료 사용자라면 공격자는 (그림 7)과 같은 결과 값을 얻을 수 있다.

(그림 7)의 결과를 살펴보면 음원주소에 인증된 사용자의 정보(?mky=00730105-113-0220079-048-070-0500119-08000560104&uno=2&cid=70332844&pid=PF00012)가 추가된 것을 확인 할 수 있다. 이는 서버측에서 변조된 쿠키의 'U' 인자 하나만으로 사용자를 인증한 결과이다. (그림 7)의 주소로 스트리밍을 요청하면 우리는 1분이 아닌 전체 음악을 들을 수 있게 되는 것이다. 이는 음원의 저작권뿐만 아니라 개인사용자의 정보유출, 개인의 금적적인 피해까지 이어지는 아주 위험한 상황이다.

```
〈ASX version="3.0"〉
〈ENTRY〉
        〈TITLE〉Dosirak  Music Service〈/TITLE〉
        〈REF
HREF="mms://kt68kmssst.dosirak.com/M/1/7033284
4/70332844_192K.wma?mky=00730105-113-0220079-04
8-070-0500119-08000560104&uno=2&cid=70332844&p
id=PF00012"  /〉
〈/ENTRY〉
〈/ASX〉
```

(그림 7) 로그인시 쿠키가 변조된 Global/MagicLock/GetMGLKCInt .asp 결과값

3.2 메시지 변조를 통한 공격(싸이월드, 네이버, 다음)

본 장에서 설명할 취약점은 메시지 변조 취약점이다. 메시지 변조 취약점을 이용한 공격은 서버에 Request를 요청하여 반환되는 Response 메시지의 결과 값을 변조하여 뮤직플레이어에서 유료사용자로 인식시켜 전체 음악을 들을 수 있게 하는 공격방법이다. 이 취약점은 네이버, 싸이월드 두 곳에 적용되며 각각의 사례를 통해 공격방법을 설명한다.

각 포털 사이트의 음원서비스 방식은 처음 설명한 2장에서 설명한 일반적인 음원서비스의 프로세스를 따르지만 음악정보를 받아오고, 뮤직플레이어 자바스크립트를 서버로부터 받아오는 시점이 각 사이트 별로 조금씩 상이하나, 결과에는 영향을 주지 않는다. 각 사이트의 주요 요청만 그림으로 보여주었으며 가독성을 높이기 위해 그림파일 요청을 삭제한 나머지 인증, 음악정보요청 부분만 그림에 표현하였다. 아래의 공격과정은 모두 로그인 하지 않은 상태에서 공격이 이루어진다. 분석 프로그램으로는 Fiddler를 사용하였으며, Response 메시지 변조 프로그램으로는 Burp suit 프로그램을 사용하였다. 아래는 각 사이트 별로 공격방법을 설명한다.

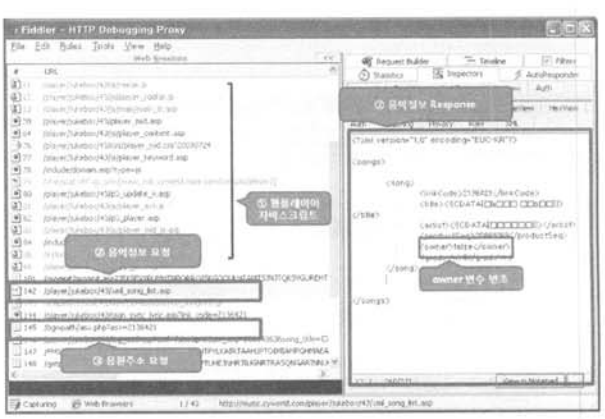
3.2.1 메시지 변조를 통한 싸이월드 뮤직플레이어 공격

싸이월드는 음악정보요청 및 인증정보 전송과정을 암호화하지 않은 채로 XML 형식으로 전송한다. 이러한 상황에서 공격자는 서버로부터 송신되는 인증정보가 담긴 메시지를 변조함으로써 공격에 성공할 수 있다.

(그림 8)을 보면 싸이월드에서는 '/player/jukebox/43/xml_song_list.asp'라는 페이지를 통해 음악정보를 받게 된다. 이 음악정보에는 유료사용자 인증정보가 함께 포함되어 XML 형식으로 전송된다.

<표 1>은 싸이월드의 음악정보 요청하는 과정의 패킷의 일부를 발췌한 것이다. 음악정보로 'product_seq'라는 정보를 Request 인자로 전송하는 것을 알 수 있다. 그 결과 값으로 서버는 클라이언트에게 XML 형식의 음악정보, 유료사용자 인증정보를 내려주게 된다. 'linkCode'는 음악번호를 나타내고 'productSeq'는 음악에 대한 상품번호를 나타낸다. 여기서 중요한 것은 'owner'변수인데 이 값이 유료사용자 인증정보를 나타낸다. 공격자는 이 변수를 'true'로 변조함으로써 공격에 성공할 수 있다.

(그림 9)는 'owner'변수의 조작한 결과로써 음악의 total 재생시간이 미리듣기 45초에서 전체듣기 3분 53초로 바뀐 것을 알 수 있고 현재 재생시간이 45초를 넘어 2분 22초를



(그림 8) 싸이월드 음악정보의 owner변수를 이용한 공격

〈표 1〉 싸이월드 음악정보 요청 / Response 메시지 / 메시지 변조공격

<table>
<tr><td rowspan="2">음악정보 요청</td><td>URL</td><td>POST /player/jukebox/43/xml_song_list.asp HTTP/1.1</td></tr>
<tr><td>음악정보</td><td>product_seq=20864063&ndr_url=cymusic</td></tr>
<tr><td>음악정보, 유료사용자 인증정보 Response 메시지</td><td colspan="2">〈?xml version="1.0" encoding="EUC-KR"?〉
〈songs〉
〈song〉
〈linkCode〉2136421〈/linkCode〉
〈title〉〈![CDATA[■0v■■■ ■■ó■■]]〉〈/title〉
〈artist〉〈![CDATA[■■■■■■]]〉〈/artist〉
〈productSeq〉20864063〈/productSeq〉
〈owner〉false〈/owner〉
〈gradeYn〉0〈/gradeYn〉
〈/song〉
〈/songs〉</td></tr>
<tr><td rowspan="2">메시지 변조 공격</td><td>공격 전 메시지</td><td>공격 후 메시지</td></tr>
<tr><td>〈owner〉false〈/owner〉</td><td>〈owner〉true〈/owner〉</td></tr>
</table>

공격 전

공격 후

(그림 9) 싸이월드 메시지 변조 공격 전 / 후 결과 화면

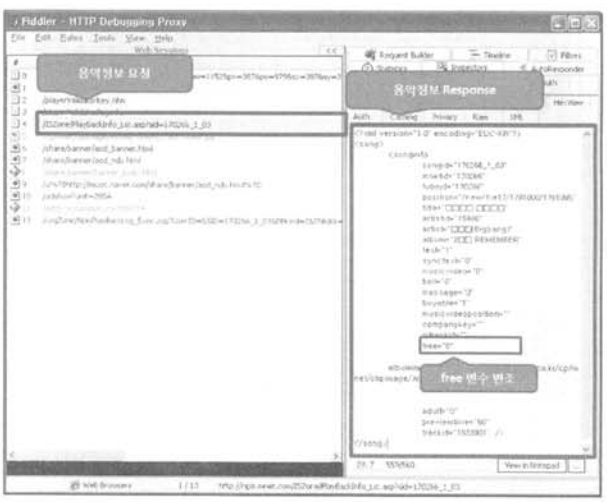
지나가는 화면을 나타내고 있다.

3.2.2 메시지 변조를 통한 네이버 뮤직플레이어 공격

네이버도 싸이월드와 동일한 방식을 취하고 있다. 서버에 음악을 요청하고 클라이언트에 음악정보와 함께 유료사용자 인증정보를 XML 형식으로 포함하여 전송한다. 공격자는 이 메시지를 변조함으로써 공격에 성공할 수 있다.

(그림 10)을 보면 네이버에서는 '/ISZone/PlayBackInfo_Lst.asp' 라는 페이지를 통해 음악정보와 인증정보를 전송한다. 메시지는 XML 형식으로 전송된다.

<표 2>는 네이버의 음악정보 요청하는 과정의 패킷의 일부를 발췌한 것이다. 음악정보로 'sid'라는 정보를 Request 인자로 전송하는 것을 알 수 있다. 그 결과 값으로 서버는 클라이언트에게 XML 형식의 음악정보, 유료사용자 인증정보를 내려주게 된다. 'sid'는 음악번호를 나타내고 'position'은 음악이 저장되어있는 경로를 나타낸다. 'adult'는 성인음악인지 나타내는 것이며 'previewtime'은 미리듣기 시간을 나타낸다. 여기서 중요한 것은 'free'변수인데 이 값이 유료사용자 인증정보를 나타낸다. 공격자는 이 변수를 '1'로 변조



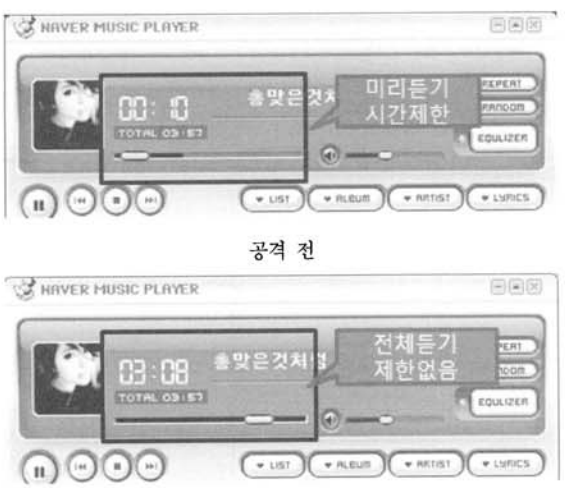
(그림 10) 네이버 음악정보의 'free' 변수를 이용한 공격

〈표 2〉 네이버 음악정보 요청 / Response 메시지 / 메시지 변조공격

음악정보 요청	URL	GET/ISZone/PlayBackInfo_Lst.asp HTTP/1.1
	음악정보	sid=170266_1_03
음악정보, 유료사용자 인증정보 Response 메시지		〈?xml version="1.0" encoding="EUC-KR"?〉 〈song〉 〈songinfo songid="170266_1_03" mnetid="170266" tubeid="170266" position="/new/file17/1791000/1791095" title="[redacted]" artistid="15466" artist="[redacted](Bigbang)" album="2[redacted] REMEMBER" text="1" synctext="0" musicvideo="0" bell="0" message="0" buyable="1" musicvideoposition="" companykey="" mtrackid="" free="0" albumimgurl="http://images.hangame.co.kr/cp/mnet/clipimage/Album/70/000/170/170266.jpg" result="0" adult="0" previewtime="60" trackid="1933901" /〉 〈/song〉
메시지 변조 공격	공격 전 메시지	공격 후 메시지
	free="0"	free="1"

함으로써 공격에 성공할 수 있다.

(그림 11)은 'free'변수의 조작한 결과로써 음악의 total 재생시간이 미리듣기 60초에서 전체듣기 3분 57초로 바뀐 것을 알 수 있고 현재 재생시간이 60초를 넘어 3분 08초를 지나가는 화면을 나타내고 있다. (그림 11)을 살펴보면 미리듣기 시간은 플레이어 하단에 검정색 막대 바 형태로 제한시간을 나타내고 있다.



공격 전

공격 후

(그림 11) 네이버 메시지 변조 공격 전 / 후 결과 화면

3.2.3 메시지 변조 자동화 프로그램을 이용한 공격

이와 같은 메시지 변조 공격은 Burp suit라는 web proxy 프로그램을 이용한다. web proxy 프로그램이란 proxy 툴의 하나로 해킹도구로 사용하고 있지만 원래의 목적은 개발자가 웹 취약점을 분석하고 보완 할 수 있도록 해주는 프로그램이다. 이 프로그램을 이용하면 실시간으로 오고가는 패킷을 검사하여 공격자가 지정한 조건에 따라 변조를 할 수 있다. 공격자는 각 사이트에 해당하는 유료사용자 인증 변수를 등록하고 원하는 값으로 통신과정에서 자동으로 변조할 수 있다.

(그림 12)는 Response body의 변경조건 설정을 통해 싸이월드, 네이버 사이트의 음원 전체를 들을 수 있도록 설정하는 그림이다. 이와 관련된 위험은 유료 사용자가 아닌 악의의 공격자가 Response 메시지 값을 변조함으로써 음원에 대한 저작권을 침해당할 수 있다. 이에 관한 영향은 인가되지 않은 사용자가 음원서비스를 무료로 이용할 수 있으며, 불법 도용할 경우에는 저작권자, 음원서비스업자 모두에게 큰 손실을 가져다 줄 수 있다. 또한 'adult'와 같은 성인물임을 증명하는 변수를 변조하면 성인인증과 관련된 제약조건을 무력화 시킬 수 있으며, 이는 공격자에게 악용될 수 있는 여지를 남겨둔다.

(그림 12) Burp suit 프로그램(web proxy)을 이용한 각 사이트별 메시지 자동변조

3.3 로컬 자바스크립트 변조 공격(네이버, 싸이월드)

로컬 자바스크립트 변조 공격은 뮤직플레이어에 사용되는 자바스크립트 소스를 고쳐 음악전체를 들을 수 있는 방법이다. 국내 포털사이트의 뮤직플레이어를 분석해보면 자바스크립트로된 소스를 가지고 있는 것을 알 수 있다. 자바스크립트 소스는 클라이언트측에 저장되며 누구나 손쉽게 수정을 할 수 있다. 이곳에 음원전체를 들을 수 있는 취약점이

존재한다.

네이버의 뮤직샘 서비스는 배경음악을 사서 카페나 블로그에 배경음악으로 들을 수 있게 해주는 서비스이다. 이 서비스에서도 미리듣기 서비스를 제공하는데, (그림 13)의 소스코드는 네이버 뮤직샘의 미리듣기 서비스 소스코드의 일부이다.

이 서비스는 간단한 자바스크립트소스로 되어있다. 'nTimeLimit'변수는 미리듣기 시간을 설정하는 변수이다. 공격자는 소스중 'gogsweb.nTimeLimit=60;' 을 'gogsweb.nTimeLimit =gogsweb.nFileTime;' 으로 변경함으로써 미리듣기 시간제한을 풀 수 있다. 공격자는 이를 고쳐 손쉽게 클라이언트측에서 음원전체를 들을 수 있다. 물론 위 소스를 수정하여 프로그램을 만들면 다른 뮤직플레이어와 똑같은 음원서비스를 들을 수 있게 된다.

싸이월드 역시 이와 같은 취약점이 존재한다.

(그림 14)의 소스코드는 서버에서 전송한 음악정보 및 인

```
function Play() {
        // 설치될 때까지 대기
        if(gogsweb.IsInstall) {
                if(isPause) {
                        Pause();
                        return;
                }
                gogsweb.Init('id', 'pw', 'param');
                gogsweb.SetPath('http://nbgm.mnet.com/cgi-bin/egg1.cgi?id=$SONGPATH$',
'http://npis.mnet.com/ISZone/NewBgmPlayBackInfo_Lst.asp?sid=$SONGID$');
                gogsweb.AddMnetID('171126_1_03');

                gogsweb.nTimeLimit = 60; //플레이 시간제한 변수

                gogsweb.Play();
                gogsweb.nVolume = "80";
                // 1초마다 호출하여 progress bar를 움직인다.
                playInfoId = setInterval("PlayInfo()", 1000);
        }
    }
```

(그림 13) 네이버의 뮤직샘 'nTimeLimit' 변수 조작을 통한 공격

```
USong.prototype = {
 id : null,
 song : null,
 initialize : function(id, song) {
        this.id = id;
        this.song = song;
 },

 isMusicAlbum : function () {
        return false;
 },

 ready : function () {
        return true;
 },

 next : function () {
        return false;
 },

 getDisplay : function () {
        return this.song.title + " - " + this.song.artist;
 },

 isOwner : function() {
        return this.song.owner;//유료사용자인지 확인하는 변수
 },

 getCurrentSongTitle : function () {
        return this.getDisplay() + (this.song.owner ? '(보유곡)' : '');
 },

 getNextSongTitle : function () {
        return this.getDisplay();
 },

 toHTML : function () {
        return SongHtml.toHTML(this.song, this.id, 'PlayingList.play');
 }
};
```

(그림 14) 싸이월드 뮤직플레이어 자바스크립트의 'song_owner'변수 변조를 통한 공격

증정보가 담긴 XML 을 class 에 저장하는 부분이다. 이 부분에서 'return this.song.owner;' 을 'return true;' 로 수정하게 되면 뮤직플레이어에서 유료사용자로 인식하고 음원전체를 들을 수 있게 된다. 물론 이 부분뿐만 아니라 다른 부분도 수정이 가능하며 소스코드를 자유자재로 변경하여 공격자의 마음대로 플레이어를 변형하여 사용할 수 있다.

로컬 자바스크립트 변조 공격 취약점은 부적절한 인증과정과 개발자가 클라이언트를 전적으로 신뢰하는데서 발생한다[9]. 유료사용자 인증과정은 서버와 클라이언트 모두에서 일어나야 하며, 이는 반드시 공격자가 인식할 수 없는 형태로 이루어져야 한다. 부적절한 인증과정과 클라이언트 신뢰의 예로는 싸이월드의 네이트온 뮤직앨범서비스에서도 찾을 수 있다. 뮤직앨범 서비스는 네이트온 친구끼리 자신이 구매한 음악을 공유하여 들을 수 있는 서비스이다. 뮤직앨범 서비스의 절대경로 'http://music.cyworld.com/player/jukebox/player.asp?msgr_cmn=xxxxxx&music_album=yyyyyyyyyy&referer=nateon'에서 공격자는 'music_album='의 숫자를 변경함으로써 친구가 추가되지 않은 타인의 음악앨범을 무단으로 청취할 수 있다. 만약 서비스의 취지가 친구끼리 음악을 들을 수 있게 한다는 취지라면 이 또한 부적절한 인증으로 인해 저작권이 침해가 되는 예라고 할 수 있겠다.

이와 같이 클라이언트측 자바스크립트에서 미리듣기를 제한하고, 서버와 클라이언트 양쪽에서 인증과정 거치지 않는 경우의 뮤직 플레이어에서는 동일한 형식의 공격을 받을 수 있으며 공격자는 무단으로 음원서비스를 받을 수 있게 된다. 이는 싸이월드, 네이버만의 문제가 아니라 동일한 방식을 채택하는 뮤직플레이어의 공통적인 취약점이다. 위의 사례에서는 음악을 듣는 것만 사례를 들었지만, 음악다운로드, 성인인증과 같은 부분도 공격의 대상이 될 수 있을 것이다.

3.4 각 사이트별 취약점과 영향

본 절에서는 3절에서 분석된 각 사이트별 취약점과 영향을 설명한다.

3절에서 분석결과 각 사이트별 취약점 및 영향은 <표 3>에서 보는 바와 같다. 도시락에서는 쿠키값을 암호화하였으나, 일부 암호화되지 않은 변수를 이용하여 유료서비스를 도용할 수 있는 취약점이 발생하였다. 하지만 도시락은 스트리밍을 요청할 때 부가적인 사용자 인증정보를 서버에서 확인하고, 미리듣기제한을 서버에서 제한함으로써 메시지 변조, 자바스크립트 변조의 공격을 차단할 수 있었다. 싸이월드와 네이버는 통신과정에서 인증정보가 암호화되지 않고, 자바스크립트에서 미리듣기를 제한함으로써 공격자로 하여금 변조를 통해 유료서비스를 도용하고 인증을 우회할 수 있는 취약점을 가지고 있는 반면에 쿠키를 암호화함과 동시에 한 개의 인자가 아닌 여러 가지 인자를 인증에 사용함으로써 쿠키값 변조의 공격을 차단할 수 있었다.

이렇게 각 사이트별로 보안조치는 되어있었으나 음원서비스에 시스템전체가 아닌 일부분에 적용됨으로써, 그로 인해

<표 3> 각 사이트별 취약점 및 영향

취약점 / 사이트	쿠키값 변조	메시지 변조	자바스크립트 변조
도시락	O	X	X
싸이월드	X	O	O
네이버	X	O	O
취약점별 영향	사용자 변경, 유료서비스 도용	유료서비스 도용, 기타 인증 우회	유료서비스 도용, 기타 인증 우회

발생할 수 있는 취약점을 이용한 공격 시나리오를 보여주고 그에 따른 영향까지 알아보았다. 이런 분석의 결과는 시스템 전체의 보안강도는 시스템상에서 가장 낮은 보안강도에 따라 결정된다고 할 수 있다. 본 장에서 알아본 분석을 바탕으로 4장에서는 각 취약점별 대응방안을 제안한다.

4. 음원서비스 취약점 대응방안 제안

본 장에서는 3장에서 분석된 세 가지 취약점 쿠키값 변조, 메시지 변조, 로컬 자바스크립트 변조로부터 음원을 보호할 음원서비스 대응방안을 제안한다.

우선 각 공격의 방어법을 알아보면 쿠키값 변조의 방어법으로는 암호화 및 메시지 다이제스트를 이용하여 기밀성, 무결성을 유지할 수 있다. 공격자는 암호화를 풀기 전에는 쿠키의 내용을 확인할 수 없으며, 또한 공격자가 원하는 값으로 수정을 가하지 못한다. 또한 암호화된 메시지 안에 메시지 다이제스트를 저장해 인증과정에서 이를 확인한다면 기밀성과 무결성을 달성할 수 있다. 음원정보값의 Response 변조 또한 암호화로 기밀성과 무결성을 달성할 수 있다. 하지만 로컬 자바스크립트 변조는 암호화로 달성할 수 없다. 그 이유는 웹 브라우저에 의해 해석이 가능해야 하기 때문이다. 따라서 자바스크립트에서 인증을 하거나, 미리듣기를 제한하는 것은 아주 위험한 법이다. 그래서 이를 해결하기 위한 대응방안으로는 인증메커니즘이나 미리듣기 제한 메커니즘은 Active X 형태 혹은 컴파일된 프로그램내에 존재하는 것이다. 컴파일된 프로그램이나 Active X의 형태는 공격자가 소스코드를 볼 수 없기 때문이다. 또한 프로그램내에 역공학을 방어하기위한 'obfuscation'과 같은 기술을 적용하면 공격자의 공격성공률은 낮아질 것이며 프로그램을 공격하기위한 노력은 증가할 것이다[10]. 이런 대응방안을 통해

<표 4> 각 취약점별 대응방안

취약점	대응방안
쿠키값 변조	1. 쿠키 암호화를 이용한 기밀성 유지, 2. 메시지 다이제스트를 이용한 무결성 유지
메시지 변조	1. 메시지 암호화를 이용한 기밀성 유지, 2. 메시지 다이제스트를 이용한 무결성 유지
로컬 자바스크립트 변조	1. 서버, 클라이언트 양방향 인증절차 2. 인증절차 프로그램화

음원서비스 프로세스의 공격 대응방안을 (그림 15)와 같이 제시한다.

① 사용자가 홈페이지에서 듣고 싶은 음악을 선택한다.

② 클라이언트측에서는 음악번호와 클라이언트의 인증정보를 전송한다. 클라이언트의 인증정보는 로그인하였는가 하지 않았는가, 하였다면 클라이언트를 식별할 수 있는 식별자가 포함되어야 할 것이다. 만약 쿠키에 사용자 정보가 저장된다면 쿠키의 메시지 다이제스트와 함께 모든 정보는 암호화되어야 할 것이다. 암호화는 속도가 빠른 대칭키를 사용하여 효율성을 높일 수 있으며 키는 클라이언트와 공유되지 않아야 한다.

③ 유료사용자를 결정한다. 유료사용자를 결정할 때는 클라이언트의 인증정보를 확인하고, 메시지 다이제스트를 확인하여 전송과정에서 변조되었는지 확인하여야 할 것이다. 로그인을 하지 않은 사용자는 유료사용자의 판단 범위에서 제외되어야 한다.

④ 음악정보, 유료사용자 인증정보를 메시지 다이제스트와 함께 암호화하여 클라이언트 측으로 전송한다. 유료사용자 인증정보와 같은 경우는 인증과정에 사용되는 모든 정보가 암호화 되어야하며, 여러 개의 인자를 사용하여 인증과정을 거쳐야 한다. 3장의 사례를 예로 들어 얘기하면 일부정보만 암호화되어 있어, 암호화되지 않은 파라미터에 의한 공격이 이루어질 수 있었으며, 한 가지 인자로 인증을 거칠 경우 공격당할 수 있는 위험이 높아진다.

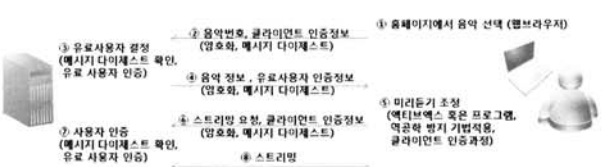
⑤ 음악정보를 복호화 후 미리듣기를 조정한다. 서버측에서 송신한 유료사용자 인증정보를 프로그램 내에서 복호화하며, 모든 미리듣기 제한은 프로그램 내에서 이루어져야 한다. 프로그램은 액티브 엑스 혹은 자체 제작한 컴파일된 목적프로그램이 될 수 있다. 프로그램내에서 인증과정을 거치는 이유는 자바스크립트의 취약성 때문이다. 자바스크립트와 같은 의도되지 않은 변조 공격을 막기 위해 'obfuscation'과 같은 역공학 방지기법이 적용되어야 한다. 웹 애플리케이션의 가장 중요한 문제는 모든 클라이언트를 신뢰할 수 없다는 것이다. 공격자는 정상적인 사용자로 가장하여 공격하기 때문이다. 로컬 자바스크립트 취약점에서 볼 수 있듯이 공격자는 내려 받은 자바스크립트를 로컬 컴퓨터에 저장시키고, 미리듣기 제한을 풀어 프로그램화 하여 서버로부터 스트리밍 서비스를 받을 수 있는 사례를 보면 모든 클라이언트를 신뢰할 수 없다는 결론을 내릴 수 있을 것이다. 이와 같은 이유로 자바스크립트는 최소한의 음악 컨트롤에만 사용되어야 하며 모든 제한, 인증 메커니즘은 프로그램내에 내장되어야 하며 프로그램은 반드시 무결성을 유지해야한다.

⑥ 스트리밍 요청시 암호화된 클라이언트 인증정보 서버로 전송한다. 3장에서 보여줬던 쿠키값 변조를 제외한 취약점들은 모두 로그인을 하지 않은 상태에서 이루어진 공격이다. 이를 확인하기 위해서는 스트리밍 요청시 클라이언트 인증정보를 함께 전송 한다.

⑦ 사용자 인증과정을 거친다. 스트리밍 직전 사용자 인증과정을 다시 한 번 거침으로써 ②~⑤ 과정에서 일어날 수 있는 공격을 예방할 수 있다.

⑧ 스트림을 전송한다.

위와 같은 과정을 통해 음원서비스를 한다면, 쿠키와 개인정보의 기밀성, 무결성을 확보하여 쿠키변조 공격을 막을 수 있다. 또한 음악정보와 유료사용자 인증정보의 기밀성, 무결성을 확보하여 메시지 변조공격을 막을 수 있다. 마지막으로 모든 인증과정 및 제한메커니즘을 역공학 방지기법이 적용된 프로그램내에 탑재함으로써 로컬 자바스크립트변조의 취약점을 원천적으로 제거할 수 있게 된다.



(그림 15) 음원서비스 프로세스의 공격 대응방안 제안

5. 결 론

지금까지 국내 포털사이트 3곳의 일반적인 음원서비스 프로세스와 트래픽 분석을 통해 음원서비스 프로세스의 취약점에 대해 자세히 알아보았다. 이러한 분석 결과로부터 행해질 수 있는 세 가지 취약점과 실제 공격과정을 설명하고 마지막으로 상기 취약점으로부터 보호받을 수 있는 음원서비스 취약점 대응방안까지 알아보았다.

현재 국내 포털서비스의 음원 프로세스의 취약점은 보안마인드를 가지지 않은 개발자의 편의 측면, 지나친 성능 중심의 개발을 통해 생긴 취약점이라고 볼 수 있다. 이를 뒷받침해주는 근거는 자바스크립트상의 소스코드에 달린 주석과 음악정보에 넘어오는 변수명, 한 가지 인자를 통한 사용자 인증, 암호화되지 않은 메시지의 전송 등을 들 수 있겠다. 소스 코드에 달린 주석은 공격자에게 아주 유용한 정보가 된다. 또한 인증에 한 가지 인자 사용과 가독성 높은 변수명은 공격을 더욱 쉽게 만드는 계기가 된다. 개발시의 효율성을 위한 주석은 사용자에게 배포될시 반드시 삭제되어야 하며, 보안에 관련된 변수명은 공격자가 쉽게 알아볼 수 없는 변수명을 선택하는 것이 보안상 유리하다. 또한 메시지의 기밀성과 무결성을 유지하기위해 인증정보가 담긴 메시지는 반드시 암호화 되어야 하며 메시지 다이제스트를 통해 검증되어야 한다. 자바스크립트 변조 공격의 취약점을 원천 제거 하기위해서는 자바스크립트대신 Active X나 프로그램내에 인증 및 제한기능을 두어야 하며 프로그램은 역공학을 유념해 두어야 할 것이다.

이런 취약점과 공격시나리오들이 존재하는 가운데 앞으로 다가올 유비쿼터스 시대에서는 많은 통신기기와 음원서비스가 통합될 것이라고 예상된다. 이런 변화에 점점 더 중요시

되는 지적재산권을 보호하기 위해서 공격자의 법적 처벌의 교정통제뿐만 아니라 기술적인 예방통제가 더욱 절실해질 것이다. 이번 논문을 통해 개발자에게는 조금 더 체계적인 음원서비스 프로세스와 신중한 프로그래밍을 통해 본 논문에서 지적한 취약점을 방어하여 기업의 이익과 저작권 소유자의 이익을 보호할 수 있는 계기가 되었으면 한다.

참 고 문 헌

[1] 정진호, "가수들이 운다... 올 음반시장 600억'최악'," 아이뉴스, 2007.9.28.

[2] 싸이월드뮤직, "http://music.cyworld.com/"

[3] 네이버뮤직, "http://music.naver.com/"

[4] 도시락, "http://www.dosirak.com/"

[5] Fiddler, "http://www.fiddlertool.com/fiddler/"

[6] Cooxie, "http://www.diodia.com/cooxietoolbar.htm"

[7] Burp suit, "http://portswigger.net/"

[8] 위키피디아, "http://ko.wikipedia.org/wiki/HTTP_%EC%BF%A0%ED%82%A4"

[9] 마이크 앤드류스, 제임스 A. 휘태커, "웹애플리케이션 해킹 대작전," 에이콘, 2007, pp.35.

[10] 장혜영, 조성제, "비주얼 C++소스 코드를 위한 obfuscator 구현", 정보과학회논문지, 소프트웨어 및 응용 제 35권 제2호, pp. 59-67, 2008. 2.

이 상 식

e-mail : crackerlss@gmail.com

2009년~현 재 성균관대학교 컴퓨터공학과 (학사)

관심분야 : 웹 보안, 정보시스템 감사, 네트워크 보안, 저작권 보호

최 동 현

e-mail : dhchoi@security.re.kr

2005년 성균관대학교 정보통신공학부(학사)

2007년 성균관대학교 전자전기컴퓨터공학과 (공학석사)

2007년~현 재 성균관대학교휴대폰학과 박사과정

관심분야 : 암호이론, 모바일 보안, 보안성 평가, DRM, SCADA

원 동 호

e-mail : dhwon@security.re.kr

1976년~1988년 성균관대학교 전자공학과 (학사, 석사, 박사)

1978년~1980년 한국전자통신연구원 전임연구원

1985년~1986년 일본 동경공업대 객원연구원

1988년~2003년 성균관대학교 교학처장, 전기전자 및 컴퓨터공학부장, 정보통신대학원장, 정보통신기술연구소장, 연구처장

1996년~1998년 국무총리실 정보화추진위원회 자문위원

2002년~2003년 한국정보보호학회장

2002년~현 재 대검찰청 컴퓨터범죄수사 자문위원, 감사원 IT 감사 자문위원

2007년~현 재 성균관대학교 정보통신공학부 교수, 한국정보보호학회 명예회장, 정보통신부지정 정보보호인증기술연구센터 센터장

관심분야 : 암호이론, 정보이론, 정보보호

김 승 주

e-mail : skim@security.re.kr

1994년~1999년 성균관대학교 정보공학과 (학사, 석사, 박사)

1998년~2004년 한국정보보호진흥원(KISA) 팀장

2004년~현 재 성균관대학교 정보통신공학부 교수

2001년~현 재 한국정보보호학회, 한국인터넷정보학회, 한국정보과학회, 한국정보처리학회 논문지 및 학회지 편집위원

2002년~현 재 한국정보통신기술협회(TTA) IT 국제표준화 전문가

2005년~현 재 교육인적자원부 유해정보차단 자문위원, 디지털콘텐츠유통협의체 보호기술워킹그룹 그룹장

2007년~현 재 대검찰청 디지털수사 자문위원, KISA VoIP 보안기술 자문위원, 기술보증기금 외부 자문위원, 전자정부서비스보안위원회 사이버침해사고대응 실무위원회 위원

관심분야 : 암호이론, 정보보호표준, 정보보호제품 및 스마트카드 보안성 평가, PET