http://dx.doi.org/10.7236/JIWIT.2012.12.5.67
JIWIT 2012-5-9

동영상 콘텐츠 보안 스트리밍

Video Contents Security Streaming

김민세*, 안병구**

Minseh Kim, Beongku An

요 약 현재 유료 동영상 콘텐츠는 보안 취약점을 이용하여 제 3자가 취득할 수 있는 문제점이 있다. 본 연구에서는 제3자의 위법적인 다운로드를 차단하기 위하여 상용화되어 사용 중인 동영상 암호화 방식을 분석하였다. 그리고 기존에 있던 방식인 주소 암호화 방식과 암호화 프로토콜을 사용하는 방식에 추가하여 프로그램 자체에서 암호화 및 복호화를 하여 송, 수신하는 방식을 제안하였다. 성능평가를 위해서 암호화를 통한 인코딩과 디코딩 지연시간을 최대한으로 줄이면서 보안 향상을 이룰 수 있는지를 가지고 기존의 방식과 비교 분석하였다.

Abstract Since current paid video contents have a security vulnerability, anyone can obtain the information of video contents. In this paper, we analyze current video encryption methods which are used commercially to prevent illegal downloading movies. And we propose an address encryption method which can encrypt and decrypt video contents in program itself. In the performance evaluation, we compare the proposed method with the conventional method to show the improvement of security with the reduced delay for encoding and decoding through encryption.

Key Words : 동영상 콘텐츠, 보안 취약점, 암호화

I. 서 론

최초의 휴대폰이 출시되고서부터 현재까지 휴대폰 망은 지속적으로 발전하였다. 덕분에 현재 보급되는 스마트폰으로 사용자들은 언제 어디서나 음악을 듣거나 영상을 볼 수 있게 되었다. 하지만 너무 많은 사용자들로 인하여 3G망의 한계에 도달하여 사용자들이 질 좋은 서비스를 제공받는데 문제가 생기게 되었다. 그래서 통신사에서는 외국에서 몇 년 전부터 상용화 되어진 4G를 우리나라에서도 올해 도입하였고 상용화 서비스중이다. 이론적으로 3G의 통신속도는 14.4Mbps이고 4G는 이동시 100Mbps 고정상태에서는 155Mbps-1Gbps까지 속도를 낼 수 있기 때문에 4G가 상용화되면 유무선 통합에 의한 진정한 멀티미디어 통신이 가능하게 되고 유비쿼터스 서비스를 누릴 수 있다. 사용자들은 이런 빠른 속도를 기반으로 더욱 더 다양한 멀티미디어 서비스를 이용하게 될 것이다. 그에 따라 서비스를 제공하는 기업에서는 많은 수요에 의해 공급을 강화할 것이다. 하지만 보안적인 측면이 등한시 된다면 수요에 따른 매출은 증가하게 되지 않게 되므로 기업에서는 이익과 콘텐츠 보호를 위하여 보안적인 측면에서 더 강화되어야할 필요성을 찾게 될 것이다. 본 논문에서는 현재 동영상 스트리밍 서비스에

*준회원, 홍익대학교 컴퓨터정보통신공학과
**종신회원, 홍익대학교 컴퓨터정보통신공학과
접수일자 : 2012년 7월 15일, 수정완료 : 2012년 8월 29일
게재확정일자 : 2012년 10월 12일

Received: 15 July 2012 / Revised: 29 August 2012 /
Accepted: 12 October 2012
**Corresponding Author: beongku@hongik.ac.kr
Dept. of Computer & Information Communications Engineering, Hongik University, Korea

사용되고 있는 암호화 방식의 취약점 분석 및 성능에 대하여 연구하고 보안 성능을 향상 시킬 수 있는 암호화 방식을 제안하였다[1] – [10].

본 논문은 다음처럼 구성되어 있다. Ⅱ장에서는 관련연구에 대하여 설명한다. Ⅲ장에서는 주소암호화 및 프로토콜 암호화 방법들에 대한 취약점을 분석한다. Ⅳ장에서는 제안된 주소 암호화 방법에 대해서 설명하고, Ⅴ장에서는 성능평가를 수행하고, 마지막으로 Ⅵ장에서 본 논문의 결론을 설명한다.

Ⅱ. 관련연구

1. 스트리밍 전송

스트리밍 전송은 인터넷에서 음성이나 영상, 애니메이션 등을 실시간으로 재생하는 기법을 말한다[6] – [8]. 1995년 리얼네트워크사가 개발한 리얼오디오에서 처음으로 선보였다. 인터넷에서 영상이나 음향·애니메이션 등의 파일을 하드디스크 드라이브에 다운로드받아 재생하던 것을 다운로드 없이 실시간으로 재생해 주는 기법이다. 전송되는 데이터가 마치 물이 흐르는 것처럼 처리된다고 해서 “스트리밍(streaming)” 이라는 명칭이 붙여졌다. 파일이 모두 전송되기 전이라도 클라이언트 브라우저 또는 플러그인이 데이터의 표현을 시작하게 되어 있다. 따라서 재생시간이 단축되며 하드디스크 드라이브의 용량도 영향을 거의 받지 않는다.

스트리밍이 동작하려면 데이터를 수신하고 있는 클라이언트 측은 데이터를 모으고, 그 데이터를 사운드나 그림으로 변환해 주는 응용프로그램에 끊임없이 보내줄 수 있어야 한다. 만약 클라이언트가 데이터를 수신하는 속도가 너무 빠르면 여분의 데이터를 버퍼에 저장하면서 동시에 스트리밍하게 된다. 그러나 데이터 수신속도가 빠르지 않으면 데이터의 표현이 매끄럽지 않게 된다.

인터넷이 발달할수록 점점 더 중요한 위치를 차지하고 있는 기술로, 특히 인터넷방송이 활성화되는 계기를 마련했다는 평가이다. 일반 사용자들 역시 대용량 멀티미디어 파일을 즉시 다운로드할 만큼 빠른 접속회선을 갖추고 있지 않으므로 이 기술을 적용하는 리얼플레이어나 윈도미디어플레이어와 같은 소프트웨어가 필수사항으로 자리잡고 있다. 또한 스트리밍 서비스를 해주는 회사도 급격하게 늘어나고 있다.

2. 스트리밍 암호화 방식

스트리밍 암호화에서 가장 중요한 것은 스트리밍 서비스가 암호화 후에도 암호화 전과 비교하여 느리지 않게 실시간으로 서비스가 가능한 가 이다. 위 조건의 전제 하에 현재의 스트리밍 암호화 방식은 프로토콜을 이용한 RTP, RTSP, MMS, RTMP, RTMPS, RTMPE, RTMPTE, RTMFP 등이 있다[2] – [6]. 위에서 제시한 프로토콜에서 대부분은 주소 암호화만을 제공하여 누구나 손쉽게 프로그램을 이용하면 주소를 쉽게 얻어 낼 수 있기 때문에 보안에 취약하다.

3. 프로토콜

본 절에서는 위에서 소개한 현재의 스트리밍 암호화 방법들을 자세하게 설명한다[2] – [6].

RTP: 실시간으로 음성이나 동영상을 송수신하기 위한 전송 계층 통신 규약이며, RFC 1889에 RTCP (RTP control protocol)와 함께 규정되어 있다. 자원 예약 프로토콜(RSVP)과는 달리 라우터 등의 통신망 기기에 의지하지 않고 단말 간에 실행되는 것이 특징이다. RTP는 보통 사용자 데이터그램 프로토콜(UDP)의 상위 통신 규약으로 이용된다. 송신 측은 타임 스탬프를 근거로 재생 동기를 취해 지연이 큰 패킷을 포기할 수 있다. 또 수신 측에서 전송 지연이나 대역폭 등을 점검, RTCP를 사용해서 송신 측의 상위층 애플리케이션에 통지하는 것으로 부호화 속도 등을 조정하여 서비스 품질(QoS) 제어를 실현할 수 있다. LAN/인터넷 환경에서의 비디오 회의 시스템에 대한 ITU-T 권고 H.323에 채용되었으며, 미국 마이크로소프트사의 영상 회의 프로그램 넷미팅 등이 탑재되어 있다.

RTSP: 실시간 스트리밍 프로토콜(Real Time Streaming Protocol, RTSP)은 IETF가 1998년에 개발한 통신 규약이 RFC 2326에 정의되어 있다. RTSP는 스트리밍 시스템에 사용되며, 미디어 서버를 원격으로 제어할 때 쓰인다. 명령어는 “PLAY”, “PAUSE” 같이 VCR 동작하고 비슷하며 시간 정보를 바탕으로 서버에 접근을 한다. 실제 미디어 스트리밍 데이터를 전송하지는 않는다. 대부분의 RTSP 서버는 RTP 규약을 사용해서 전송 계층으로 실제 오디오/비디오 데이터를 전송한다.

MMS: 마이크로소프트 미디어 서버(MMS)는 마이크로소프트의 사유 네트워크 스트리밍 프로토콜로, 윈도 미디어 서비스(이전 이름: NetShow 서비스)의 유니캐스

트 데이터를 전송하는 데 쓰인다. UDP나 TCP를 통해 전달할 수 있고, 기본 포트는 UDP/TCP 1755이다.

RTMP: 리얼 타임 메시징 프로토콜(Real Time Messaging Protocol, 흔히 줄여서 RTMP)은 어도비 시스템즈사의 독점 컴퓨터 통신 규약이다. RTMP는 오디오, 비디오 및 기타 데이터를 인터넷을 통해 스트리밍할 때 쓰인다. RTMP는 어도비 플래시 플레이어와 서버 사이의 통신에 이용된다. 처음 목표는 오직 플래시(Flash)에만 쓰이는 것이었다. 플래시 이외에도 어도비 라이브 사이클 데이터 서비시즈 ES와 같은 다른 응용프로그램에서 RTMP이 쓰이고 있다. 그리고 RTMP 규격은 2009년 1월 20일에 어도비에서 발표했다.

RTMPS(RTMP Secure): RTMP 데이터를 HTTPS로 감싼다. 플래시 재생기는 SSL 입출력을 지원하므로 그 기능을 사용한다.

RTMPE: 128비트로 암호화된 RTMP 프로토콜이다. SSL보다는 가볍지만 SSL 인증같은게 없음. 암호화 채널을 사용하기 때문에 기본 RTMP보다 약간 성능에 영향을 줄 수 있다.

RTMPTE(Encrypted RTMP Tunneled): RTMPT, RTMPE 섞어 놓은 형태이고 플래시 플레이어 최신버전이 필요하며 서버 성능에 영향을 준다.

RTMFP (Real Time Media Flow Protocol): UDP에서 동작하며 기본 RTMP는 TCP에서 동작. 항상 암호화 된 상태로 데이터를 전송한다.

III. 주소암호화 및 프로토콜 암호화 방법 취약점 분석

1. 주소 암호화 취약점 분석

기업 및 단체에서 동영상을 스트리밍 서비스 하기 위해선 해당 동영상을 서버에 올리게 되고 이 과정에서 사용자가 볼 수 있도록 URL주소가 만들어 진다. 하지만 이 주소를 중간 과정을 생략 하고 얻는다면 문제가 생기게 될 것이다. URL주소를 간편하게 얻을 수 있는 프로그램(Url snooper, GetFlv, Replay Media Cathcer4, jakasta 등)을 사용하면 쉽게 얻을수 있다. 이와 같은 프로그램은 웹페이지와 사용자 사이에서 송/수신 되는 HTTP코드중 동영상 관련 프로토콜 또는 확장자를 찾아내어 사용자가 볼수 있도록 표시해준다.

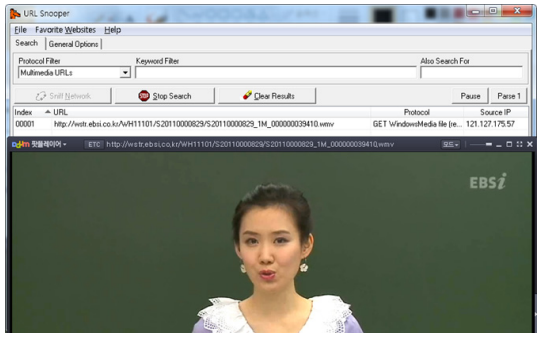


그림 1. 파싱된 EBSi URL 주소
Fig 1. EBSi URL address parshinged

위에 그림1 에서 볼 수 있듯이 주소가 그대로 노출 되어 있고 플레이어에 주소를 입력하자 바로 동영상이 재생되었다. 현재 EBSi는 국영방송으로써 누구나 무료로 재생이 가능하다. 그렇다고 우회적인 접속이 안전하다고 보장할 수 없다. 만약 EBSi에서 트래픽을 조절하기 위해 접속 인원수를 100명으로 제한했다고 가정해보자. 우회 접속으로 100명이 초과하여 접속하게 되었을 경우에는 서버에 부담을 줄 수 있고 타 서비스 까지 영향을 받을 수 있다.

EBSi와 같이 파싱을 당하지 않기 위해서 현재 사용되고 있는 주소 암호화 방식이 있다. 이 방식은 매우 다양한 방식으로 서비스 되고 있기 때문에 정해진 방식은 없다. 표 1은 주소 암호화 방법들을 분석한 내용을 설명하고 있다[3]-[10]. 각 방법들의 장단점을 분석 설명하면 다음과 같다.

표 1. 주소 암호화 분석
Table 1. Analysis of address encryption

종류	비용	암호화 강도	속도	호환성
URL Encoder/Decoder	하	하	상	상
JavaScript	중	중	중상	상
FLV	중상	상	중	중상
ActiveX	중상	상	중하	중

가. URL Encoder / Decoder

평문 : http://test.com

변환 : http%3A%2F%2Ftest.com. 아주 간단한 암호화 방식으로 포털 검색을 통해 Decoder가 나와 있으므로 보안에 약하다.

나. 자바스크립트 암호화

자바스크립트 안에서 해쉬함수(MD5, sha1), 자체 제

작한 함수로 주소를 암호화 하는 방식이다. 자바스크립트는 인터넷에 노출된 부분이기 때문에 안전하다고는 할 수 없다.

다. FLV 암호화

동영상 주소 뒤에 키값을 GET으로 플래시에 전송하여 플래시에서는 복호화 과정을 통해 사용자 및 권한을 확인하는 작업을 거치게 된다. 이때 검사를 통과하게 되면 플래시에서 파일을 스트리밍을 통해 사용자에게 전송하게 한다. 이 정보들은 키 값에 암호화 되어 있고 매번 접속할 때 마다 변경되어 진다. 키 값이 포함된 암호화된 주소는 다음처럼 나타내어진다.

http://localhost/test.flv?**KEY=JY0Uh9Cwne41vHRNtbwgtJF15FF6w5zjggFCvaoClwpziuxVW8fSrx1tuIkO8w6GQhSlpNnNETEEthTJE7gVQ==&Rnd=ABBKeQ==**

이 방식은 브라우저의 호환성과 성능이 좋아서 현재 주소 암호화방식으로 가장 많이 사용되는 방식이다. 하지만 이 방식은 플래시 취약점을 이용하여 볼 수 있는 방식이므로 완벽하다고는 할 수 없다.

라. ActiveX 암호화

ActiveX내에 디코딩 함수를 넣어 놓고 실제 HTML 내에는 암호화된 주소를 넣어놓고 실행시 복호화 되어 동영상 주소를 불러와 재생시키는 방식이다. ActiveX는 익스플로러에서만 동작하므로 한 브라우저만 사용해야 하는 단점이 있고 ActiveX를 지양하는 현재 시대에 맞지 않다.

2. 프로토콜 암호화 취약점 분석

몇 개의 사이트에서 동영상 스트리밍 서비스를 제공하는 방식을 조사하여 보았다. 일단 국내 사이트에서는 동영상을 프로토콜로 암호화 스트리밍 하는 방식은 찾을 수 없었고, 외국 스트리밍 사이트를 찾아보니 몇 개의 사이트가 프로토콜 암호화 방식을 사용중이였다. 표 2는 동영상 스트리밍 프로토콜들에 대한 취약점 분석 결과를 설명하고 있다[2] – [10].

표 2. 동영상 스트리밍 프로토콜
Table 2. Video contents streaming protocol

사이트	유/무료	프로토콜	암호화	서비스방식
EBSi	무료	HTTP	X	자체플레이어
SBSi	유료	RTSP, RTSPT, MMS	O(주소)	자체플레이어
Tving	유료	RTMP	X	FMS
Mtv	무료	RTMPE	O	FMS
BBC	무료	RTMPE	O	FMS
Megastudy	유료	RTSP, RTSPT, MMS	O(주소)	자체플레이어

프로토콜 암호화 방식은 현재 Adobe시스템에서만 제공되는데 그 중 가장 많이 사용되는 RTMPE[2]는 Replay Media Cathcer4란 프로그램으로 쉽게 다운로드가 가능하다(그림 2).

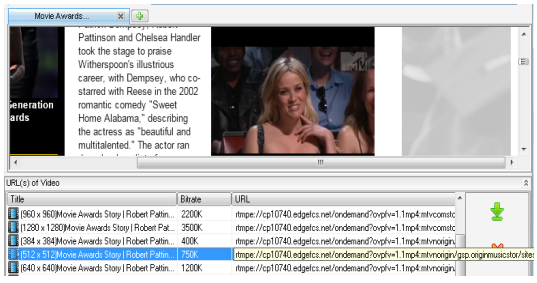


그림 2. 암호화된 동영상을 받는 화면
Fig 2. View of encrypted video contents

암호화되어 전송된 동영상을 플래시에서만 재생되도록 하였는데 이 프로그램을 사용하면 동영상으로 저장되어 재생이 가능하다(그림 3).

그림 3. 재생중인 화면
Fig 3. Replying view

이 프로토콜의 취약점을 알아보기 위해 FMS(Flash Media Server)을 설치하여 WireShark로 패킷을 분석하여 보았다. 일단 RTMPE[2] 프로토콜을 분석하기 전에

HTTP 프로토콜과 RTMP 프로토콜을 분석하였다(그림 4).

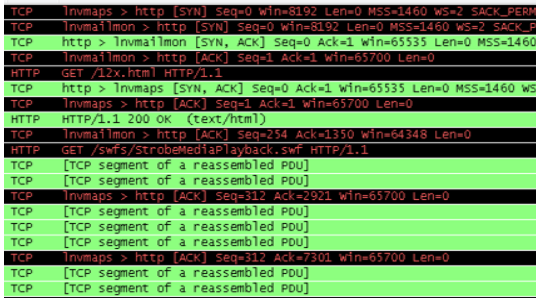


그림 4. HTTP 프로토콜 패킷
Fig 4. HTTP protocol packet

HTTP 프로토콜 패킷은 암호화가 되어 있지 않기 때문에 전송되는 정보가 모두 노출되어 있다.

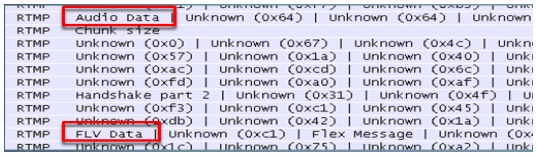


그림 5. RTMP 프로토콜 패킷
Fig 5. RTMP protocol packet

RTMP 프로토콜 패킷에서는 모든 정보가 분석되어 나오지 않고 Audio data와 FLV data 일부가 노출된 것이 확인되었다. RTMPE 프로토콜은 RTMP프로토콜을 사용하고 암호화가 되어 전송되어 진다. WireShark로 패킷을 본 결과는 다음과 같다(그림5, 그림6).

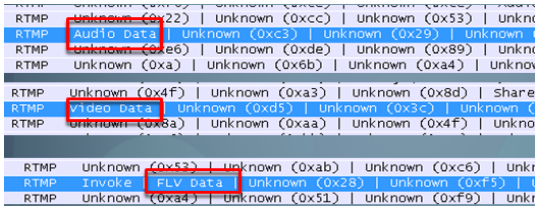


그림 6. RTMPE 프로토콜 패킷
Fig 6. RTMPE protocol packet

RTMPE로 전송하여도 Audio Data, Video Data, FLV Data가 전송되는 것을 확인 할 수 있었다. 암호화가 전체적으로 되어 있지 않기 때문에 중간자 공격(Man-in-the-middle Attack)을 통해 비디오와 오디오 데이터를 취득하게 되면 재생이 가능해 진다. 표 3은 동영상 스트리밍 프로토콜들의 암호화 분석 결과를 설명하고 있다.

표 3. 프로토콜 암호화 분석
Table 3. Analysis of protocol encryption

종류	비용	암호화 강도	속도	호환성
HTTP	하	하	상	상
RTSP, RTSPT	중하	하	상	상
MMS	중하	하	상	상
RTMP	상	중	중	중상
RTMPE	상	중상	중	중상

IV. 제안된 주소 암호화 방법

본 장에서는 제안된 주소 암호화 방법[2]-[10]을 설명한다.

위에 설명한 기존방식이 아닌 PHP를 통하여 개인의 정보를 수집 하여 암호화 키를 생성하고 사용자가 원하는 스트리밍 사이트에 접속하면 사용자에게 발급된 키로 본인확인을 거쳐서 동영상을 재생한다. 만약 유출된 주소로 다른 사람이 사용하였을 경우에는 재생이 불가능하게 하였다. 제안된 주소 암호화 방법을 플로우차트 그림으로 나타내면 그림 7과 같다.

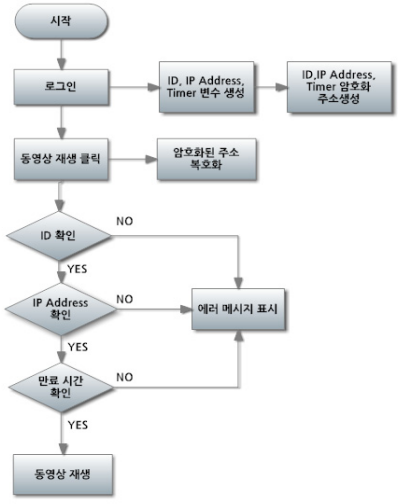


그림 7. PHP 암호화 플로우 차트
그림 7. Flow chart of PHP encryption

가. 로그인

일반적으로 웹사이트에서는 사용자가 로그인에 성공하게 되면 세션에 아이디값을 저장해 두게 된다. 이를 이용하여 사용자가 이용중인 사이트에서 동영상을 볼 때는 세션에 저장된 아이디를 사용하게 된다.

```
<p align="center">로그인</p>
<FORM name="form"
action="./pass.php" method="post">
<p align="center">ID :
<INPUT type="text" id="id" name="id"></p>
<p align="center">PW :
<INPUT type="password" id="pw"
name="pw"></p>
<p align="center">
<INPUT type="submit" value="접속"></p>
</FORM>
```

나. ID, IP Address, Timer 변수 생성

```
$id = $_POST["id"];
$_SESSION["session_id"] = $id;
$ip = getenv(REMOTE_ADDR);
$enc = $id."//".$ip."//".time();
```

로그인 폼에서 넘어온 ID값을 받아 세션에 저장하고 아이피와 현재 시간을 묶어서 ENC변수에 저장한다.

다. ID, IP Address, Timer 암호화 주소 생성

```
function encrypt($String) {
$temp1 =  strrev($String);
$temp2 = base64_encode($temp1);
return   strrev($temp2);
}
<a href = "./video.php?key=<?echo encrypt($enc);?>
">비디오 보기</a>
```

PHP 암호화 과정을 설명하는 것이기 때문에 간단한 암호화를 사용하였다. ENC변수에 저장된 값을 넣어 앞뒤를 뒤집고 BASE64로 인코딩한다. 그리고 다시 앞뒤를 뒤집어서 키 값을 생성한다.

라. 암호화된 주소 복호화

사용자가 암호화된 PHP주소를 클릭하면 값이 GET 방식으로 비디오를 출력시키는 창으로 넘어가게 된다.

```
function decrypt($String) {
        $temp1 = strrev($String);
        $temp2 = base64_decode($temp1);
        return strrev($temp2);
}
```

복호화 방식은 암호화 방식의 반대로 진행하였다.

마. ID, IP Address, 만료시간 확인

```
function play($key,$id,$ip){
        $post = explode('//',decrypt($key));
        echo time() - $post[2].'초';
        echo '<br />';
        if(strcmp($id,$post[0])){
            echo '<br />아이디가 틀림';
            return false;
        }else if(strcmp($ip,$post[1])){
            echo '<br />아이피가 틀림';
            return false;
        }else if(time() - $post[2] > 30){
            echo '<br />세션 시간 만료';
            return false;
        }
        return true;
}
```

복호화한 데이터를 다시 ID, IP Address, Timer로 나눈다음 각각의 값을 현재 접속한 계정의 ID와 비교하고 통과되면 다음으로 IP 주소를 확인한다. 마지막으로 키 값이 생성된 시간으로부터 30초가 지났는지 확인하여 그 이내이면 동영상을 재생시킨다. 30초는 절대적인 수치가 아니라 변경이 가능하여 유동적으로 서비스에 맞게 변경하면 될 것이다.

바. 동영상 재생

```
if(play($key,$id,$ip)){
        echo '<video id="player" autobuffer controls>
          <source src="./test.mp4" />
          </video>';
}
```

위 과정에서 세가지의 확인을 모두 통과하면 TRUE값이 리턴되어 실제 동영상이 출력되게 된다.

V. 성능 평가

1. 성능평가 환경 및 시나리오

본 논문에서 제안된 주소 암호화는 PHP 5.2.12버전을 설치하여 PHP 구문을 작성하고 PC 및 스마트폰에서 암호화 과정을 테스트하였다. 실제 Mysql은 로그인에서 사용되지만 암호화 과정에서는 불필요하기 때문에 생략하였다.

2. 성능평가 결과

가. 로그인 화면(Index.php)

로그인

ID :

PW :

접속

가장 처음에 나오는 로그인 화면이다. 콘텐츠 구매자가 이용하여야 하기 때문에 로그인은 필수적이다. 그리고 로그인을 통하여 세션에 저장된 사용자의 ID값이 주소암호화에 사용된다.

나. 동영상 보기 페이지(Pass.php)

비디오 보기

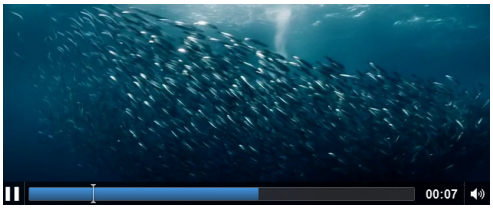
127.0.0.1/vidoe.php?key==8yLxlzNuAjLw4SMv8SMzEzNwlzMyYTM

로그인 화면에서 얻은 아이디와 아이피, 시간을 암호화하여 표기하였다.

다. 비디오 재생 화면

동영상 보기 페이지에서 넘겨받은 값을 다시 복호화하여 ID, IP Address, 시간으로 다시 분할하여 현재 사용자와 비교한다. 그리고 정상일시에는 동영상을 출력하고 비정상일시에는 상황에 맞는 에러메시지를 출력하고 동영상은 재생되지 않는다.

(1) 인증 성공시



정해진 콘텐츠가 정상적으로 재생된다.

(2) 아이디가 틀릴 경우

로그인한 아이디와 암호화된 주소에 입력된 아이디가 다를 경우에 에러메시지가 표시된다. 예를들어 콘텐츠를 구매하지 않은 사람이 주소만 얻어서 실행시켰을 경우에 위와 같은 메시지가 나타나게 된다.

Error : 아이디가 틀림

(3) 아이피가 틀릴 경우

주소만 복사하여 다른곳에서 사용할수 없도록 아이피를 검사하여 아이디와 마찬가지로 현재 접속한 아이피와 암호화된 아이피가 다를경우에 위와 같은 메시지가 나타나게 된다.

Error : 아이피가 틀림

(4) 시간이 만료된 경우(30초)

본 논문에서 제안된 암호화는 1회성이므로 주소를 얻은 제3자와 구입한 사람 모두 같은 주소로는 동영상을 볼 수 없도록 하였다. 즉, 해당 사용자는 정상적인 루트로만 접속을 하여 동영상 콘텐츠를 볼 수 있다. 이를 통하여 동영상을 재생할 수 있는 기간이 만료 되었을 시 해당 사용자를 차단할 수 있다.

31초

Error : 세션 시간 만료

VI. 결 론

본 논문에서는 동영상 콘텐츠 보안 스트리밍에 대하여 취약점을 알아보기 현재 서비스 중인 방법들 및 업체들을 분석하였다. 암호화 스트리밍 방식에는 주소 암호화 방식과 프로토콜 암호화 방식으로 크게 2가지로 나누어지게 된다. 프로토콜 암호화 방식은 약 200만원 정도의 상용 소프트웨어를 구입해야지만 사용할 수 있고 일반 스트리밍 보다 서버에 좀 더 무리를 줄 수 있기 때문에 국내에서는 Tving에서만 사용중이고 다른 곳에서는 거의 주소 암호화 방식만을 사용하고 있다. 외국계 기업에서는 MTV, BBC 방송계 회사들이 암호화 프로토콜을 주로 사용중이다. 하지만 주소 암호화나 프로토콜 암호화 모두 특정 프로그램을 통하여 주소가 모두 노출되어 허가 받지 않은 사용자가 동영상을 다운 받게 되는 경우가 생기게 된다. 그에 대한 제안방법으로 본 논문에서는 PHP와 세션을 이용하여 1회용 키를 발급함으로써 정해진 사용자 이외에는 동영상을 볼 수 없도록 구현하였다. 본 논문에 구현된 방법도 마지막에는 실제 주소가 노출되어 있지만 FLV 암호화 방식과 혼용하여 사용한다면 한층 더 스트리밍 보안은 향상될 것이라고 생각된다.

참 고 문 헌

[01] http://www.wikipedia.org

[02] http://lkcl.net/rtmp/RTMPE.txt

[03] Siu-Kei Au Yeung; Shuyuan Zhu; Bing Zeng, "Perceptual video encryption using multiple 8×8 transforms in H.264 and MPEG-4," Proc. of IEEE ICASSP 2011, pp.2436-2439, May 2011.

[04] Elkilani, W.S.; Abdul-Kader, H.M.; , "Performance of encryption techniques for real time video streaming," Proc. of ICNM 2009, pp.130-134, March 2009.

[05] Bojnordi, M.N.; Hashemi, M.R.; Fatemi, S.O.;, "Implementing an efficient encryption block for MPEG video streams," Proc. of ELMAR 2005, pp.127-130. June 2005.

[06] Euijin Choo; Jehyun Lee; Heejo Lee; Giwon Nam;, "SRMT: A Lightweight Encryption Scheme for Secure Real-time Multimedia Transmission," Proc. of MUE 2007, pp.60-65, April 2007.

[07] Jie Shen;, "Privacy-Protection in Real-Time Video Communication," Proc. of ICESS 2009. pp.217-220, May 2009.

[08] Gibson, J.D.; Servetti, A.; Dong, H.; Gersho, A.; Lookabaugh, T.; De Martin, J.C.;, "Selective encryption and scalable speech coding for voice communications over multi-hop wireless links," Proc. of IEEE MILCOM 2004, vol.2, pp.792-798, Oct. 31 2004-Nov. 3 2004.

[09] Shubo Liu; Zhengquan Xu; Jin Liu; Wei Li;, "A Novel Format-Compliant Video Encryption Scheme for H.264/AVC Stream in Wireless Network," Proc. of WiCOM 2008, pp.1-4, October 2008.

[10] Fujiyoshi, M.; Saitou, W.; Watanabe, O.; Kiya, H.;, "Hierarchical Encryption of Multimedia Contents for Access Control," Proc. of IEEE ICIP 2006, pp. 1977-1980, October 2006.

※ 이 논문은 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임(2012-0007119).

저자 소개

김 민 세(준회원)

• 2012년 : 홍익대학교 컴퓨터정보통신공학과 (학사)

<주관심분야: 동영상 콘텐츠, 정보보호, 암호화 프로토콜, 이동 무선네트워크>

안 병 구(종신회원)

• 1988년 : 경북대학교 전자공학과 (BS)

• 1996년 : (미)Polytechnic University, Dept. of Computer and Electrical Eng., USA (MS).

• 2002년 : (미)New Jersey Institute of Technology(NJIT), Dept. of Computer and Electrical Eng., USA. (Ph.D)

• 1989년 ~ 1994년 : 포항산업과학기술연구원(RIST), 선임연구원

• 2003년 ~ 현재 : 홍익대학교 컴퓨터정보통신공학과 교수

• 2012년 ~ 현재 : 대한전자공학회 컴퓨터소사이어티 회장

• 2005년 ~ 2011년 : Marquis Who's Who in Science and Engineering was listed.(세계과학기술인명사전 등재)

• 2006년 ~ 2011년 : Marquis Who's Who in the World was listed.(세계인명사전 등재)

<주관심분야: Wireless Networks, Ad-hoc & Sensor Networks, Multicast Routing, QoS Routing, Cross-Layer Technology, Cooperative Communication, Network Coding, Bioinformatics, LED Communication>