Secure-VOD 시스템의 설계 및 구현에 관한 연구

정회원 한 성 민*, 유 황 빈*

A Study on Implementation and Design of Secure VOD System

Sung-Min, Han*, Hwang-Bin, Ryou* ***Regular Members***

요 약

본 논문에서는 기존의 VOD 시스템에서 예상되는 보안상의 취약 요소와 이를 해결할 수 있는 방안을 기술하고, 보안상의 안전한 VOD(Secure-VOD) 시스템을 제안한다. 본 논문에서 제안한 Secure-VOD 시스템에서는 사용자 인증, 비디오 서버 정보에 대한 메시지 인증, 비디오 서버 정보의 메시지 암호화 등의 암호기술을 적용하였다. 본 Secure-VOD 시스템은 일회용 패스워드 기법을 이용하여 기존의 고정 패스워드 체계를 보강하여 안전성을 향상시켰으며, HMAC-HAS160 알고리즘을 이용한 메시지 코드 생성 및 검증으로 비디오 서버 정보에 대한 무결성을 제공하며, 비디오 서버 정보에 대한 비밀성을 보장하기 위해서, RC5 암호 알고리즘을 사용하였다.

ABSTRACT

In this paper, we address vulnerabilities of legacy VOD system and implement secure-VOD system to protect security holes of it. Our secure-VOD system provide user authentication using one-time password, message authentication and encryption/decryption for video server information.

To improve security of existing fixed password system, our secure-VOD system use one-time password. Also, our secure-VOD system provides integrity for video server information by generating and verifying message authentication code using HMAC-HAS160 algorithm. Finally, our secure-VOD system uses RC5 encryption algorithm to guarantee confidentiality for video server information.

Ⅰ. 서 론

통신 기능의 발달은 문자 위주의 통신 방식에서 소리, 화상, 영상 등의 매체들도 통신 매개체로 이용할 수 있도록 하였다. 초기에 개발된 VOD 시스템은 사용자의 요청에 의해서 비디오 스트림의 전송이 시작되고, 사용자는 전송되는 비디오 스트림을 받아서 시청하는 단순한 형태의 시스템이었다. 최근에는 인터넷의 보편적인 대중화로 말미암아, 웹 환경에서 VOD 서비스를 제공하게 되었다. 사용자는 웹 브라우저를 통해서 시청 가능한 비디오를 선택하고, 비디오가 선택되면 VOD 서버는 사용자에게 비디오 스트림을 전송하게 된다. 비디오 스트림의 전송이 시작되면 사용자는 비디오 클라이언트 프로그램으로 비디오를 시청한다. 그러나 인터넷은 본질적으로 신뢰할 수 없는 네트웍이기때문에, 정보의 흐름을 통제하기가 대단히 어렵다. 따라서, 인터넷 환경에서의 웹 기반 VOD 시스템은 보안상의 취약점을 가질 수밖에 없다. 즉, 웹 기반의 VOD 시스템을 이용하는 사용자가 정당한 사용자인지를 확인이 어려우며, 사용자에게 전송되는 비디오 서버의 정보가 사용자에게 정확히 전달되는지 확인이 곤란하다. 또한 비디오 서버 정보에 대한 메시지 위·변조가 발생할 수 있으며, 비디오 서버 정보에 대한 불법 누출, 도청이 발생할 가능성이 높다. 또한 서비스 제공에 대한 과금 처리시, 사용자와 서비스 제공자간에 분쟁이 발생할 수 있다. 본 논문에서는 이

* 광운대학교 컴퓨터과학과
논문번호 : 99386-0920, 접수일자 : 1999년 9월 20일

러한 보안상의 취약요소를 제거할 수 있는 Secure VOD 시스템을 설계, 구현하였다. 본 논문의 구성은 제 2 장에서는 VOD 시스템에서 발생할 수 있는 보안상의 취약 요소와 이를 해결할 수 있는 보안 대책에 대해서 기술하고, 제 3 장에서는 보안 기능을 가진 Secure-VOD 시스템의 설계와 구현에 관해서 기술하며, 제 4 장에서는 결론과 향후 과제에 관하여 기술한다.

Ⅱ. VOD 서비스의 보안상 취약 요소 및 대책

2.1 VOD 서비스의 보안 필요성

인터넷 환경에서의 웹 기반 VOD 서비스는 비디오의 시청과 직결되는 비디오 서버 연결 정보의 구성이 텍스트로 된 경우이다. 비디오 서버 연결정보는 대부분 웹브라우저의 캐쉬 디렉토리에 일정기간 남게되므로 사용자의 특별한 옵션 지정 없이는 해결할 수 없다. 불법적인 목적의 사용자는 이 비디오 서버 정보를 웹브라우저 캐쉬 디렉토리에서 입수해서 구성된 내용을 수정하고 이를 실행함으로써 원래 시청하려는 비디오가 아닌 다른 비디오를 시청하게 할 수 있다. 물론 이런 문제점은 상업적인 목적의 서비스가 아닌 공개된 형태의 VOD 서비스에서는 큰 문제가 되지 않을 수 있다. 그러나 폐쇄 그룹(CUG)을 대상으로 하는 VOD 서비스나 상업적인 목적의 VOD 서비스에서는 보안 기능이 요구된다.

이러한 문제점을 해결할 수 있는 방법으로는 폐쇄 그룹을 대상으로 하는 VOD 서비스에서는 폐쇄 그룹에 대한 가입을 별도의 가입 시스템을 이용하게 함으로써 사용자의 확인이 가능하게 할 수 있다. 단지 사용자가 불법적으로 비디오 서버 정보를 읽지 못하도록 암호 알고리즘을 이용하여 비디오 서버 정보를 암호화하면 비교적 간단하게 보안상의 문제를 해결할 수 있지만 상업적인 목적의 VOD 시스템에서는 사용자의 가입, 로그인 과정을 비롯한 과금 서비스를 필요로 하게 된다. 정확한 과금을 위해서는 사용자에 대한 인증과 비디오 정보에 대한 메시지 인증이 필수적이다.

2.2 VOD 서비스의 보안상 취약 요소

VOD 서비스에서의 보안상 취약요소는 허가 받지 않은 사용자가 VOD 서버에 로그인 행위, 사용자에게 전송되는 비디오 서버 정보의 불법적인 위·변조, 불법누출 등이 있다.

(가) 비디오 게이트웨이의 사용자 불법 접근: 허가 받지 않은 사용자가 VOD 서버에 불법적인 접근을 시도하는 경우로 사용자 클라이언트에 대한 신분 확인이 불가능하기 때문에 발생할 수 있다. VOD 서버의 불법적인 접근에 성공을 하면 허가 받은 사용자의 신분으로 위장하여 비디오를 시청할 수 있다.

(나) 비디오 서버 정보의 불법 위·변조: VOD 서버에서 사용자에게 전송되어지는 비디오 서버 정보에 대한 불법적인 위·변조로 인해서 사용자가 원하는 비디오를 시청하지 못할 수 있다.

(다) 비디오 서버 정보의 불법누출, 도청: VOD 서버에서 비디오 클라이언트에 전송되는 비디오 서버 정보를 제 3자가 도청해서 입수한 비디오 서버 정보로 비디오 서버에 직접 접근하여 비디오를 시청할 수 있다.

2.3 VOD 서비스의 보안 대책

본 논문에서는 이러한 기존의 VOD 시스템의 보안상 취약 요소를 해결하기 위해서 일회용 패스워드를 이용한 사용자 인증, 사용자에게 전송되는 비디오 서버 정보에 대한 메시지 인증, 비디오 서버 정보의 암호화를 이용하는 Secure-VOD 시스템을 제안한다.

(가) 사용자 인증 과정

VOD 서버에 대한 불법적인 접근을 막기 위한 대책으로 일회용 패스워드를 이용하여 사용자 인증을 수행한다. 일회용 패스워드를 사용함으로써, 고정식 패스워드를 사용할 경우 발생할 수 있는 반복 시도공격 등에 대해서 대처할 수 있다. 로그인 시 Challenge/Response 방식의 일회용 패스워드를 생성하여 비디오 게이트웨이에 접속하고, 일회용 패스워드 생성에 사용되는 키는 사용자의 로그인 패스워드를 사용한다. 일회용 패스워드를 이용한 사용자 로그인 과정은 그림 1과 같다[3,4].

(나) 비디오 서버 정보에 대한 메시지의 인증

비디오 게이트웨이에서 사용자 클라이언트에게 전송되는 비디오 서버 정보에 대한 불법적인 위·변조를 막기 위해 HAS160 해쉬 알고리즘을 이용해서 HMAC 코드를 생성한다[1,5]. HMAC 코드 생성에 필요한 키는 사용자 등록과정에서 미리 안전하게 공유하여, 사용한다. 비디오 서버 정보에 대한 메시지의 인증 절차는 그림 2와 같다.

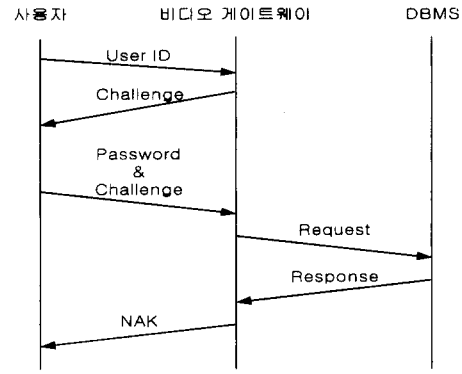

그림 1. 일회용 패스워드를 이용한 사용자 로그인 과정

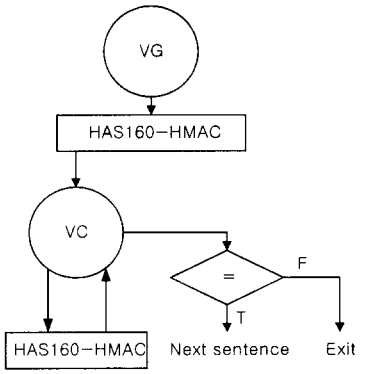

그림 2. 비디오 서버 정보 메시지 인증 코드 생성

(다) 비디오 서버 정보에 대한 암호화/복호화

비디오 게이트웨이에서 사용자에게 전송되는 비디오 서버 정보에 대한 불법적인 누출을 막기 위해서 전송되어지는 비디오 서버 정보를 암호화/복호화한다. 본 논문에서는 RC5 암호 알고리즘을 사용하고, 사용되는 키는 사용자 등록 과정에서 공유된 키를 사용한다[6]. 비디오 서버 정보에 대한 암호화/복호화 과정은 그림 3과 같다.

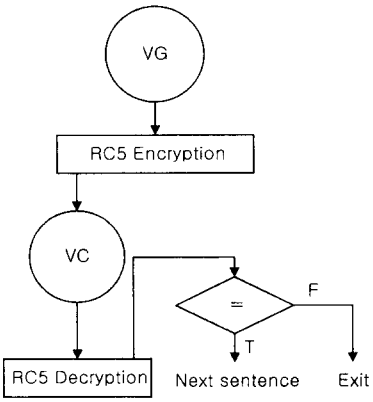

그림 3. 비디오 서버 정보 암호화/복호화

Ⅲ. Secure-VOD 시스템 설계 및 구현

3.1 구성요소 및 역할

본 논문에서 제안한 Secure-VOD 시스템의 구조는 다음 그림과 같이 크게 VOD 서버 부분과 사용자 클라이언트 부분으로 구성되고, VOD 서버는 비디오 선택 기능 제공, 사용자 인증, 메시지 인증, 암호화를 담당하는 비디오 게이트웨이와 비디오 스트림 전송을 담당하는 비디오 서버 그리고 사용자 정보와 비디오 서버 정보를 관리하는 DBMS로 구성된다. 사용자 클라이언트 부분은 사용자 로그인, 메시지 인증 코드의 검증, 복호화 등을 수행하는 웹브라우저 플러그인 부분과 비디오 재생을 담당하는 비디오 클라이언트 부분으로 구성된다.

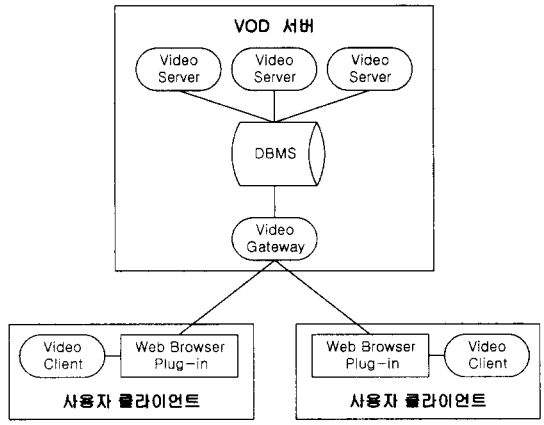

그림 4. Secure-VOD 시스템 구조

(가) 비디오 게이트웨이: 사용자 등록, 사용자 인증, 비디오 서버 정보에 대한 메시지 인증 코드 생성 및 암호화를 수행한다.

(나) DBMS: 사용자 클라이언트에 대한 키와 사용자의 신원 정보, 등록된 비디오 안내, 비디오 시청 내역 등을 관리한다.

(다) 비디오 서버: 비디오 스트림의 저장 및 관리 기능과 사용자에게 비디오 스트림을 전송하는 기능을 한다.

(라) 플러그인 모듈: 비디오 게이트웨이와의 통신하는 모듈로 일회용 패스워드를 생성한다[8].

(마) VOD 클라이언트: 비디오 서버에서 비디오 스트림을 수신하여 사용자가 비디오를 시청할 수 있도록 하고 비디오 서버 정보에 대한 메시지 인증 코드 검증 및 복호화를 수행한다.

3.2 인증 과정 및 암호화/복호화 과정

본 논문에서 제안한 Secure-VOD 시스템의 사용자 인증, 비디오 서버 정보에 대한 메시지 인증, 암호화 과정은 다음 그림 5와 같다. 사용자에게 전송하는 비디오 서버 정보에는 비디오 서버의 IP 주소와 포트번호, 비디오 인덱스 번호와 비디오 제목을 포함하고 있으며, 동적 순서는 다음과 같다.

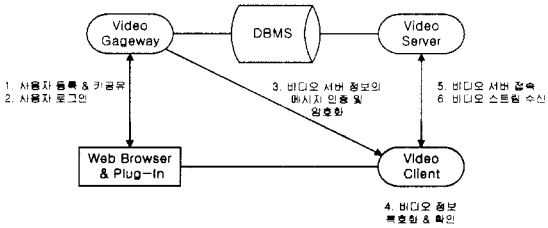

그림 5. Secure-VOD 시스템의 인증 절차

① 비디오 클라이언트 프로그램을 전송 받아서 설치한 사용자는 웹 브라우저를 이용해서 비디오 게이트웨이(VG)에 접속하여 가입 신청을 한다. 가입 신청에는 사용자의 신상 정보를 입력하고 비디오 클라이언트와 비디오 게이트웨이간의 키(k) 공유를 하게 된다.

② 비디오 게이트에서는 사용자가 신청한 신상 정보를 참조해서 가입 여부를 결정하게 되고, 가입이 허가된 사용자는 자신의 ID와 로그인 패스워드를 이용해서 비디오 게이트웨이에 로그인할 수 있다. 사용자 로그인 과정에서 비디오 게이트웨이는 사용자의 ID를 입력받아서 해당 사용자에게 Challenge 문자열을 전송하고, 사용자는 전송된 Challenge 문자열과 로그인 패스워드를 이용하여 일회용 패스워드를 생성하고 비디오 게이트웨이에 Response하게 된다. 비디오 게이트웨이는 사용자로부터 전송된 일회용 패스워드를 검증해서 정상적인 사용자인지 확인하게 된다.

③ 사용자가 시청을 원하는 비디오를 선택하면 비디오 게이트웨이는 사용자가 선택한 비디오 서버 정보(m)를 해쉬 알고리즘을 이용하여 HMAC을 생성하게 된다. 해쉬 알고리즘에 사용할 원시 메시지는 비디오 서버 정보와 키(k)이다. HMAC이 생성되면 비디오 게이트웨이는 RC5 암호 알고리즘을 이용해서 비디오 서버 정보와 HMAC을 함께 암호화한다. 그림 9에서와 같이 비디오 서버 정보에 대한 암호화가 완료되면, 비디오 클라이언트에게 암호화된 형태의 메시지를 비디오 클라이언트에게 전송한다.

RC-5 Header	Server IP No.	Port No.	Movie index	HMAC

그림 6. 암호화된 비디오 서버 정보

④ 비디오 서버 정보 파일의 확장자에 의해서 MIME 타입에 대한 검색이 이루어지고, 자동으로 비디오 클라이언트 프로그램이 실행되면서 비디오 클라이언트는 시스템 레지스트리에 저장된 키를 참조한다. 웹 브라우저와 비디오 클라이언트는 시스템 레지스트리에 저장된 키를 함께 사용한다. 비디오 게이트웨이에서 비디오 클라이언트로 전송된 비디오 서버 정보(E(m||H(m)))를 RC5 암호 알고리즘을 이용해서 복호화(D(m))하고 공유된 키(k)와 복호화한 메시지(m)를 원시 메시지로 이용해서 HMAC (H(m))을 생성한다. 비디오 클라이언트에서 생성한 HMAC과 복호화한 HMAC이 동일하면 정상적인 연결이고, HMAC이 동일하지 않은 메시지는 비디오 게이트웨이에서 보내진 메시지가 아니다.

⑤ 비디오 클라이언트는 비디오 서버 정보의 비디오 서버 IP 주소와 포트번호, 비디오 인덱스 번호를 참조해서 해당 비디오 서버에 연결하여 비디오 인덱스 번호를 전달한다.

⑥ 비디오 서버는 비디오 클라이언트의 연결 신호를 허락하고 DBMS에 비디오 클라이언트의 IP 주소와 비디오 인덱스 번호를 입력하고 해당 사용자가 비디오를 시청하고 있음을 표시하고, 비디오 클라이언트에게 비디오 스트림을 전송한다. 사용자가 비디오 시청 중간에 시청을 정지하거나 통신망 사정으로 비디오 서버와의 접속이 끊어질 경우 DBMS에 사용자의 비디오 시청이 종료되었음을 표시한다.

3.3 시스템 구현

3.3.1 시스템 구축 환경

본 논문에서 구현한 VOD 시스템은 그림 7과 같은 구성으로 이루어져있다. FastEthernet 환경의 허브로 구성된 네트워크 망에 VOD 서버와 비디오 게이트웨이 역할을 하는 한 대의 서버로 구성이 되고 여기에 사용자는 접속을 하는 형태이다.

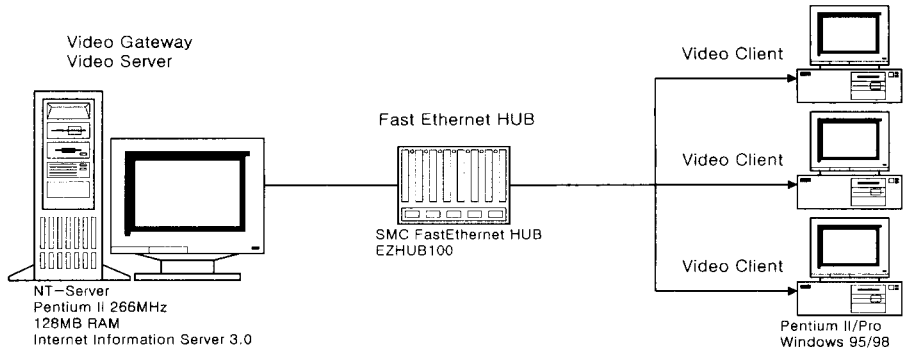

그림 7. 시스템 구축 환경

3.3.2 개발 시스템 환경

개발 시스템의 환경을 살펴보면 프로세서는 서버와 클라이언트로 구분된다. 서버의 환경은 펜티엄 II 급의 프로세서를 사용하며, 클라이언트 프로세서 환경은 펜티엄 II 급과 펜티엄 Pro 급의 프로세서를 사용한다. 다음으로 운영체제 환경은 역시 서버와 클라이언트로 분류되며 서버는 윈도우즈 NT 서버 4.0 이상의 버전을 사용하며, 웹 데몬은 IIS(Internet Information Server) 4.0 이상의 환경을 사용한다. 클라이언트는 윈도우 95, 98, NT 워크스테이션 및 서버 환경에서 동작이 이루어진다. 그밖에 네트워킹 환경은 Fast Ethernet(100Mbps) 환경을 지원하며, 개발에 사용된 툴은 VOD 부분은 비주얼 C++ 6.0 버전과 소프트웨어 MPEG 디코더(DirectShow SDK)을 활용하였으며, 비디오 선택과 관련된 웹 프로그래밍은 ASP를 사용하였다.

3.3.3 로그인 과정

로그인 과정에서는 기본적인 고정식 패스워드 확인 과정에 일회용 패스워드에 대한 확인 과정이 추가된다. 로그인 환경을 제공하는 비디오 게이트웨이는 ASP 문장을 활용하여 일회용 패스워드를 생성하게 된다. 먼저 로그인 과정은 그림 8, 그림 9와 같다. 일반적인 로그인 과정처럼 사용자 ID와 비밀번호를 사용자에게 동시에 질의하지 않고, 사용자 ID만 질의를 하게된다. 사용자로부터 입력된 사용자 ID를 검색하고 사용자의 고정식 패스워드와 세션 함수를 이용한 일회용 패스워드 문자열을 발생하게 된다. 발생된 문자열은 로그인한 사용자에게 전송됨과 동시에 비디오 게이트웨이와 연동된 DB에 저장이 된다. DB에 저장된 고정식 패스워드와 일회용 패스워드는 사용자로부터 전송된 응답 결과와 비교를 하게된다.

그림 8. 비디오 게이트웨이 로그인 과정 1단계

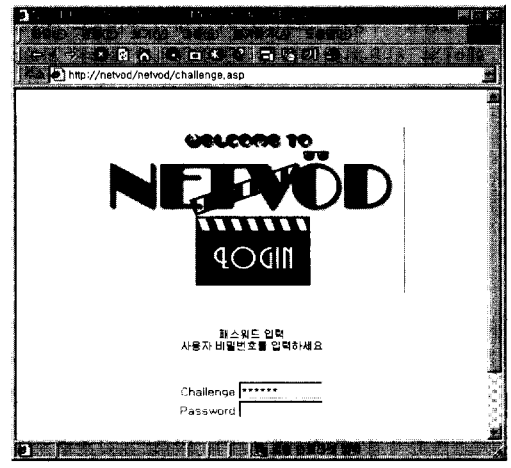

그림 9. 비디오 게이트웨이 로그인 과정 2단계

비디오 게이트웨이 로그인 1단계 과정에서 사용자의 ID가 입력되면 로그인 2단계 과정에서 입력된 ID를 기준으로 일회용 패스워드를 생성하게 된다.

생성되는 ASP 문장은 그림 10과 같다. 사용자에게 제공된 로그인 2단계 화면에서 사용자의 고정식 패스워드를 입력하고 전송을 선택하면 사용자로부터 전송된 고정식 패스워드와 일회용 패스워드를 확인하는 그림 11과 같은 과정을 거치게 된다.

3.3.4 키 공유 과정

키 공유 과정은 비디오 게이트웨이에서 등록이 허가된 사용자가 VOD 클라이언트 프로그램을 전송받아서 시스템에 설치한 다음에 키 공유 과정을 거칠 수 있다. 사용자 컴퓨터의 브라우저에 설치된 플러그인 프로그램을 이용해서 서버와 클라이언트에서 키를 공유하게 된다. 공유된 키는 서버와 클라이언트에 개별적으로 저장된다. 서버는 연동된 DB에 저장을 하게되며 클라이언트는 시스템 레지스트리에 저장이 된다. 공유된 키는 인증 목적으로 사용되는 해쉬 알고리즘과 암호 알고리즘에서 활용되게 된다.

3.3.5 해쉬 알고리즘 처리 과정

사용자 등록과 키 공유를 마친 사용자가 비디오 게이트웨이에 접속해서 시청하고 싶은 비디오를 선택하면 사용자에게 전송할 비디오 서버 정보 메시

```
Sql="Select USER_ID, USER_RND from VODUSER where USER_ID = '"
Sql=Sql & request.form("uid") & "'"
set result=Session("DbCon").execute(Sql)
if result.eof = false then
        if request("uid") = result("USER_ID") then
                Session("chg") = right(time,2) & left(result("USER_RND"),4)
                result.close
                Sql="Insert Into VODUSER(USER_ID,USER_OTP) values('"
                Sql=Sql & session("uid") & "','"
                Sql=Sql & session("chg") & "')"
        end if
end if
```

그림 10. 일회용 패스워드 생성과정

```
Sql="Select USER_ID, USER_OTP, USER_PWD, USER_LEVEL from VODUSER
where USER_ID = '"
Sql=Sql & session("uid") & "'"
set result=Session("DbCon").execute(Sql)
if result.eof = false then
        if request("opwd") = result("USER_PWD") and chr(request("chlleng")) =
chr(result("USER_OTP")) then
                if result("USER_LEVEL")=0 or result("USER_LEVEL")=1 then
                        session("Current_ID")=result("USER_ID")
                        session("USER_LEVEL")=result("USER_LEVEL")
                        session("LogTime")=Now
                        result.close
                else
                        result.close
                        response.redirect "logon.asp?MODE=B"
                end if
        else
                result.close
                response.redirect "logon.asp?MODE=A"
        end if
else
        result.close
        response.redirect "logon.asp?MODE=B"
end if
```

그림 11. 일회용 패스워드 확인과정

```
원본 메시지 :
                5b 53 65 63 75 72 65 56 4f 44 5d 49 50 3d 31 32
                38 2e 31 33 34 2e 34 33 2e 33 38 50 6f 72 74 3d
                30 30 30 30 4d 6f 76 69 65 3d c5 d7 bd ba c6 ae
                49 6e 64 65 78 3d 30 3b
HAS160-결과 :
                57 8c 02 0e 6a d8 a3 47 6d 74 8f a3 8b 7c ef eb
                05 68 ba e8
```

그림 12. HAS160-HMAC 생성

지가 구성되게 된다. 이렇게 구성된 메시지를 HAS-160 실행 모듈로 입력을 시켜서 160비트의 고정된 문자열의 HMAC을 출력한다. 출력된 HMAC은 서버의 임시 변수에 저장되어 있다가 사용자에게 전달될 비디오 서버 정보에 첨가된다.

3.3.6 비디오 서버 정보의 암호화/복호화 과정

비디오 게이트웨이에서 사용자에게 전송할 비디오 서버 정보와 보관중인 HMAC을 합쳐서 RC5 암호 알고리즘을 이용하여 암호화 처리를 하게된다. 암호화가 완료되면 생성된 메시지를 사용자에게 전송한다. VOD 클라이언트는 비디오 게이트웨이에서 전송된 암호화된 형태의 메시지를 복호화하여 원문을 복원한 후에 HAS-160 해쉬 알고리즘을 이용하여 HMAC을 생성하고 전송받은 HMAC과 비교를 한다.

3.4 안전성 분석

본 논문에서 제안한 인증 시스템은 그림 8의 ①에서 ④에 이르는 단계에서 이루어진다. 사용자 인증을 위해서 일회용 패스워드를 사용하고 비디오 서버 정보 메시지 인증을 위해서 HMAC을 사용하고, 비디오 서버 정보의 암호화를 위해서 RC5 암호 알고리즘을 사용한다. 일회용 패스워드는 고정된 패스워드를 사용함으로써 발생하는 문제점을 예방하는 기능을 제공한다. 해쉬 알고리즘을 이용한 HMAC은 사용자가 선택한 비디오 서버 정보와 공유된 키를 이용하여 생성하고 사용자에게 전송된 비디오 서버 정보에 대한 메시지 인증을 제공한다. RC5 암호 알고리즘은 암호화와 복호화에 동일한 키를 이용하는 관용 암호 방식의 알고리즘으로 현재까지 보안상으로 안전하고, 다른 비밀키 암호 방식인 DES 보다 처리 속도가 빨라서 VOD 클라이언트의 부담을 줄여준다.

본 논문에서 제안한 인증 과정은 암호화와 복호화에 사용되는 키의 전달 과정이 없도록 키 공유 알고리즘을 사용하기 때문에 키의 유출로 인한 보안 침해가 일어날 수 없으며, 만일 HMAC을 위조하여 비디오 서버에 직접 연결해도 비디오 클라이언트에서 생성되는 HMAC과 동일할 수 없기 때문에 정상적인 비디오 시청이 불가능하다. 본 논문에서 제안한 Secure-VOD 시스템은 각종 암호 알고리즘을 이용하여 사용자 인증, 메시지 인증, 메시지 암호화/복호화를 하기 때문에, 암호 알고리즘에 보안상 취약하지 않으면, 보안상의 안전하다고 볼 수 있다.

Ⅳ. 결 론

본 논문에서는 기존의 VOD 시스템에 사용자 인증, 메시지 인증 기능, 메시지 암호화 및 복호화 기능을 포함하고 있는 새로운 VOD 시스템을 제안하였다. 암호화 과정의 안전성 확보를 위해서 문제가 발생할 가능성이 있는 키의 전송 과정을 생략하고, 서버와 클라이언트가 통신상에서 키를 공유할 수 있도록 Diffie-Hellman 키 설정 알고리즘을 이용하였다. 사용자 인증을 위해서 일회용 패스워드를 사용하였으며, 비디오 서버 정보에 대한 메시지 인증은 HAS160-HMAC을 사용하였다. 향후 연구 과제로는 사용자 메시지에 대한 인증기능과 비디오 소스 스트림 자체의 암호화/복호화에 따른 성능 개선 문제가 있다.

참 고 문 헌

[1] M. Bellare, R. Canetti and H. Krawczyk, "Keying hash functions for message authentication", presented at the 1996 RSA Data Security Conference, San Francisco, Jan. 1996

[2] Whitfield Diffie and Martin E. Hellman., "New directions in cryptography", IEEE Transactions on Information Theory, 22(6):644-655, Novem-

ber 1976
[3] Haller, N, et. al., "The S/KEY One-Time Password System", IETF RFC 1760. Feb 1995
[4] Haller, N, et. al., "A One-Time Password System", IETF RFC 2289, Feb. 1998
[5] H. Krawczyk, M. Bellare, R. Canetti, "HMAC : Keyed-Hashing for Message Authentication", IETF RFC 2104, Feb. 1997
[6] R. Baldwin, R. Rivest, "The RC5, RC5-CBC, RC5-CBC-Pad, and RC5-CTS Algorithms", IETF RFC 2040, October. 1996
[7] William Stallings, "NETWORK AND INTER-NETWORK SECURITY, 1995, Prentice-Hall
[8] Zan Oliphant, "Programming NETSCAPE PLUG-INS", 1996, sams net

한 성 민(Sung-Min, Han)

1996 .2 : 독학사(이학사)
1999 .8 : 광운대학교 전산대학원 (이학석사)
1999.8～현재 : 한국생산성본부 강사

<주관심 분야> 멀티미디어통신 및 응용, 네트워크 (인터넷/인트라넷) 보안

유 황 빈(Hwang-Bin, Ryou)

1975년 인하대학교 전자공학과 (학사)
1977년 연세대학교 대학원 전자공학과 (공학석사)
1989년 경희대학교 대학원 전자공학과 (공학박사)

1981년～현재 : 광운대학교 컴퓨터과학과 교수
1994년～1995년 : 미 UCSD 객원교수
1995년～1997년 : 광운대학교 전자계산소장
1997년～1999년 : 광운대학교 중앙도서관장
1999년～현재 : 광운대학교 기초과학연구소장
2000년～현재 : 광운대학교 전산정보처장
<주관심 분야> 멀티미디어통신 및 응용, 네트워크 (인터넷/인트라넷) 보안