韓國 컴퓨터情報學會 論文誌
第10卷 第3號, 2005. 7.

2005-10-3-1-13

CDN에서 패스워드를 이용한 키 교환 프로토콜

신 승 수*, 한 군 희**

Key Exchange Protocol using Password on CDN

Seung-Soo Shin *, Kun-Hee Han **

요 약

디지털 콘텐츠는 품질의 손상 없이 복제되어 인터넷을 통해 배포 가능하며, 이는 디지털 콘텐츠 제공자에게 커다란 경제적 손실을 주게 된다. 이에 따라 디지털 콘텐츠를 안전하고 효율적인 전송을 위해 키 교환 프로토콜에 대한 연구가 필요하다. 디지털 콘텐츠를 사용자의 편의성과 실행 속도, 보안성 문제 등이 있는데, 본 논문에서는 디지털 콘텐츠를 효율적으로 전송하기 위하여 패스워드 기반의 키 교환 프로토콜을 제안하고자 한다. 제안한 프로토콜의 안정성은 이산대수문제와 Diffie-Hellman 문제의 어려움에 기반을 두고 있으며 패스워드 추측 공격 등 다양한 공격에 안전한 보안성을 제공한다.

Abstract

Digital contents can be distributed via internet without quality defect and this will bring a great loss to the contents provider. Therefore, it is necessary to investigate on the key exchanging protocol to protect the digital contents effectively. In this study we propose the key exchanging protocol based on password to send the digital contents efficiently. The stability suggested here is based on the difficulty of the discrete algebra and Diffie-Hellman problem and also it provides a secure safety against various attacks such as a guess attack on the password.

▸ Keyword : CDN, DCP, 이산대수문제, Diffie-Hellman

• 제1저자 : 신승수
• 접수일 : 2005.06.04, 심사완료일 : 2005.07.05
* 동명정보대학교 정보보호학과 교수
** 천안대학교 정보통신학부 교수

Ⅰ. 서 론

초기 인터넷 연구의 대부분은 네트워크 인프라 즉, 데이터 링크, 네트워크, 트랜스포트 계층에 집중되었다. 그러나 웹, 스트리밍 등의 새로운 대표적 응용분야가 발생하고, 이에 대한 수요가 기하급수적으로 증가함에 따라 인터넷 인프라는 한계에 다다랐다. 인터넷 인프라의 확충은 기본적으로 고비용을 요구하기 때문에 연구자들은 애플리케이션 계층에서 해결을 시도하였다. 이로 인해 나온 기술이 콘텐츠 네트워킹 기술이다. 기존 연구들이 네트워크 대역폭 증가, 전송의 효율화에 중점을 두었다면, 콘텐츠 네트워킹 기술은 네트워크에 지능을 부여한다. 사용자와 보다 인접한 위치에 콘텐츠를 준비하고, 사용자에게 가장 인접한 위치에 콘텐츠로 안내함으로써 보다 고품질의 콘텐츠 서비스가 가능하도록 한다.

콘텐츠 네트워킹의 가장 대표적인 기술은 CDN(Contents Delivery Network)이다. CDN은 콘텐츠를 사용자와 보다 인접한 위치로 이동시켜 네트워크 상에서 콘텐츠 전송 비율을 줄인다. 뿐만 아니라, CDN은 지능적 전송과 체계적 관리를 부여함으로써 관리자가 한 지점에서 전체 콘텐츠 전송을 완벽하게 제어할 수 있도록 한다[1].

CDN이란 인터넷 사용자들로부터 멀리 떨어져 있는 CP(Contents Provider)의 웹 서버에 집중되어 있는 콘텐츠 중 그림, 배너, 비디오, 또는 오디오와 같은 용량이 크거나 사용자들의 요구가 잦은 콘텐츠를 여러 ISP(Internet Services Provider)의 POP(Point of Presence)들에 설치한 CDN 서버에 미리 저장해 놓고, 콘텐츠 요구 발생 시 가장 최적의 CDN 서버로부터 사용자에게 콘텐츠를 전달해 주는 신 개념의 대용량 데이터 전송방식이다[2]. 즉, 대용량의 콘텐츠를 인터넷 사용자 근처에 미리 옮겨놓고, 그곳에서 그 콘텐츠를 인터넷 사용자들에게 신속하게 배달하는 서비스로, 인터넷 사용자는 HTML 텍스트와 같은 용량이 작은 콘텐츠는 CP의 웹 서버에서, 동영상 같이 용량이 큰 콘텐츠는 CDN 서버에서 받아보게 되는 것이다.

지금까지는 서로 다른 ISP간 Traffic이 교환되는 Internet Exchange Point, ISP 및 NSP(Network Service Provider)간의 정략적 제휴 지점인 Peering Point에서 발생하는 데이터의 손실과 병목현상으로 인기가 있는 콘텐츠나 영화, 뮤직비디오, 노래, 게임 등 대용량의 콘텐츠를 이용할 경우, 접속이 끊기거나 접속 성능 저하되는 등의 문제들이 발생해 왔다. 그러나 CDN 서비스를 이용하게 되면 대용량의 콘텐츠가 복잡한 인터넷의 중간 경로를 거치지 않고 여러 ISP의 다수의 POP에 설치한 CDN 서버로부터 사용자들에게 바로 전달되므로 위와 같은 데이터의 손실이 발생하지 않음은 물론 웹 서버의 부하도 줄게 되어 인터넷 사용자들은 대용량의 오디오 및 콘텐츠를 보다 안정적이고 빠른 속도로 인터넷을 통해 이용할 수 있다. 다음 (그림 1)은 CDN 방식의 서비스를 나타낸 것이다.

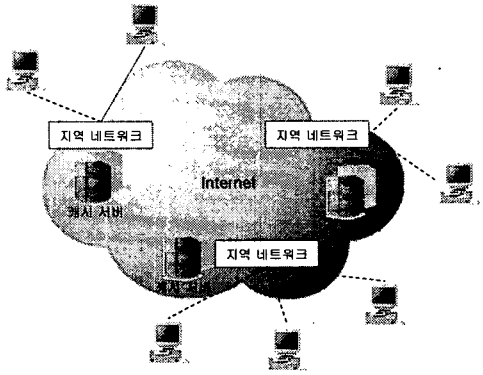

그림 1. CDN 방식의 서비스
Fig 1. Service of CDN method

아무리 좋은 CDN을 갖추고 있어도, 인터넷 자체는 보안을 고려하지 않은 전송매체이기 때문에 보안 문제가 발생한다. 또한 ISP(Internet Services Provider)의 서버 시스템은 불법 침입 및 데이터 파괴의 위협에 노출되어 있으며, 해킹이나 크래킹의 위협이 더욱 심해지고 있다. 따라서 서버 시스템 보호를 위한 보안 대책이 요구된다. 디지털 콘텐츠의 안전한 분배를 위해서는 전송되는 디지털 콘텐츠의 보안 기술이 필요하다. 일반적으로 멀티미디어 고품질 콘텐츠는 품질의 손상 없이 불법 복제가 가능하다. 또한 인터넷에서 불법 복제된 콘텐츠의 배포는 디지털 콘텐츠 제공자들에게 커다란 경제적 손실을 주고 있다. 따라서 디지털 콘텐츠의 안전하고 효율적인 분배를 위한 연구가 필요하다. 일반적으로 디지털 콘텐츠의 안전한 분배를 위해 암호화 과정을 통해 전송되며, 이로 인해 디지털 콘텐츠의 부담이 증가 된다[3,4]. 결국, 암호화와 복호화 부담의 증가와 디지털 콘텐츠 자체의 부담 증가는 전송지연과 실행지연을 통해 사용자의 응답지연이 발생하게 된다. 이러한 관점에서 패스워드

를 이용한 공개키 기반의 프로토콜 설계의 가장 중요한 이슈는 사용자의 편의성, 실행속도, 보안성에 관련된 문제라 할 수 있는데, 본 논문에서는 보안성에 중점을 두고자 한다.

안정성과 실행속도 및 사용자의 편의성을 개선한 공개키 기반의 안전하고 효율적인 디지털 콘텐츠 분배 시스템을 사용하였다[5].

본 논문에서는 CDN에서 패스워드를 이용한 공개키 기반 프로토콜을 제안하고자 한다. 이 프로토콜은 이산대수문제 DH 문제의 어려움, 그리고 해쉬 함수의 암호학적 강도에 기반을 두고 있다.

본 논문의 구성은 다음과 같다. 2장에서는 기존 연구에 대하여 알아보고 3장에서는 CDN에서 패스워드를 이용한 키 교환 프로토콜을 제안한다. 4장에서는 CDN에서 패스워드를 이용한 키 교환 프로토콜의 안정성을 분석한다. 마지막으로 결론을 맺는다.

II. 기존 연구

클라이언트와 서버 사이의 신뢰성과 안정성을 확보하기 위해서는 웹 보안 프로토콜과 평문 데이터를 암호화 복호화하는 알고리즘이 필요하다[4]. 웹 보안 프로토콜에는 응용계층에서 메시지 전체를 암호화하여 전송하는 방식과 메시지에서 몸체 일부분만을 암호화하여 전송하는 방식이 있다. 또한 SSL(Secure Socket Layer)과 같이 응용계층과 전달계층 사이에 암호화 계층을 별도로 삽입하여 암호화하는 방법이 현재 많이 사용되고 있다. 웹 클라이언트와 서버사이의 신뢰성과 안정성을 확보하기 위해서는 클라이언트와 서버 각각을 인증서버(Certificate Server)를 통하여 인증받는 절차가 필요하다. 이때 사용되는 데이터의 집합이 인증서이다. 인증서의 형식으로 가장 널리 사용되는 표준은 ITU-T의 X.509이다[6].

공개키 암호방식은 암호화 할 때 사용되는 공개키(Public Key)와 복호화 할 때 사용되는 비밀키(Private Key)가 달라서 공개키는 공개하고 비밀키만 안전하게 유지하는 방식이다. 공개키 기반의 웹 보안 시스템에서는 클라이언트와 웹서버의 인증이 종료된 후에 암호화 채널을 형성하여 실질적인 데이터를 주고받을 때는 공개키와 비밀키를 이용한다. 실제로 많은 웹상용 보안시스템의 경우 RSA 공개키 알고리즘을 이용하고 있다. RSA 방식은 계산에 소유되는 시간이 대칭키 방식에 비해 오래 걸리지만 공개키 방식은 대칭키 방식에 비해 암호화 과정에서 사용하는 키의 안전한 분배가 용이하여 상용시스템에서 많이 사용되고 있다.

일반적으로 HTTP 요구의 효율적인 처리를 위해 웹 캐싱을 사용하였다[7,8]. 웹 캐싱은 인터넷에서 사용자와 지리적으로 가까운 곳에서 사용자가 요청한 웹 객체를 저장하여 빠른 응답과 네트워크 사용의 효율성을 증가시킨다[9]. 웹에서 디지털 콘텐츠의 효율적인 분배를 위해 CDN과 같은 연구가 점차 각광을 받고 있으며, 이러한 CDN의 설계에서 캐싱 기술의 활용은 시스템의 성능을 좌우하는 중요한 요인이라 할 수 있다.

2.1 기존 시스템

디지털 콘텐츠 분배 시스템은 DCP(Digital Contents Provider)에서 DC(Digital Contents)를 제공받는 DCUG (Digital Contents User Group)에 속한 인가된 사용자에게 안전하고 효율적으로 DC를 분배하는 목적으로 하고 있다. (그림 2)는 시스템의 구성을 나타낸 것이다[4].

SPSM(Secure Proxy Server Manager)은 DCUG의 프록시 서버를 관리하는 관리자이다. 프록시 서버는 필터링, 액세스 권한, 보안 기능 등이 있다.

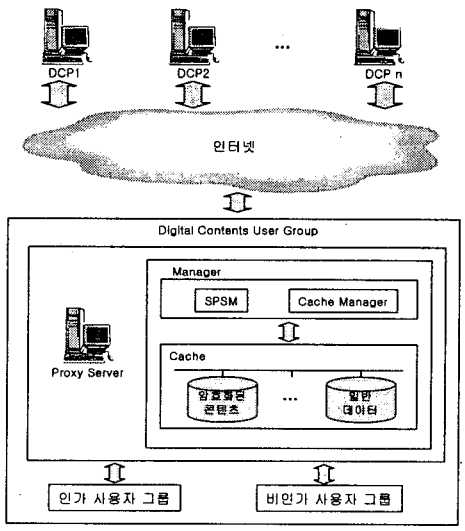

그림 2. 시스템의 구성
Fig 2. Configuration of systems

2.2 암호화

디지털 콘텐츠를 보호하기 위하여 다음과 같은 암호화 기법을 사용하였다. 안정성과 키 분배의 효율성을 위해 RSA 공개키 기법을 사용하였다. 1계층에서 공개키에 의해 암호화된 DC는 2계층의 디지털 콘텐츠 사용자 그룹에서 개인키에 의해 복호화 되고, 2계층의 디지털 콘텐츠 사용자 그룹은 3계층의 사용자 실행의 속도를 고려하여, 복호화된 DC 평문을 다시 공개키로 부분적으로 암호화하여 캐시에 저장한다. 2계층과 3계층 사이의 전송은 인트라넷을 통해 시스템적인 보안성을 가진 전송이다. 2계층은 승인된 사용자에게만 부분 암호화된 콘텐츠를 제공한다.

2계층은 디지털 콘텐츠 사용자 그룹에 해당하며, 1계층과 2계층의 콘텐츠 전송은 보안성이 없는 인터넷을 통해 이루어진다. 따라서 디지털 콘텐츠 제공자와 디지털 콘텐츠 사용자 그룹 사이의 콘텐츠 전송에는 보안성이 검증된 안전한 암호화 기법이 필수적이다. 다음 (그림 3)은 암호화 및 복호화 계층구조를 나타낸 것이다.

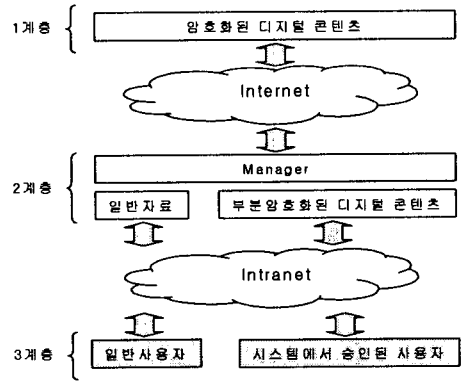

그림 3. 암호화 및 복호화 계층 구조
Fig 3. Level structure of encryption and decryption

2.3 인증 절차

디지털 콘텐츠 사용자 그룹의 허가된 사용자가 캐시 목록에서 원하는 콘텐츠를 찾을 수 없을 경우 디지털 콘텐츠 사용자 그룹은 해당 디지털 콘텐츠 제공자 서버에서 콘텐츠를 전송받아야 한다. 이 경우 디지털 콘텐츠 사용자 그룹과 디지털 콘텐츠 제공자 서버는 상호간의 암호화 데이터를 주고받기 전에 CA(Certificate Authority) 서버에 접속하여 인증서를 발급 받아야 한다. 인증서의 발급절차는 다음과 같다. CA 서버에 접속하여 인증서 발급을 요청한다. CA 서버는 인증서 요청을 디지털 콘텐츠 사용자 그룹과 디지털 콘텐츠 제공자 서버에 전송한다. 디지털 콘텐츠 제공자 서버와 디지털 콘텐츠 사용자 그룹은 자신의 키 쌍을 생성하고, 인증서 요청을 작성한다. 디지털 콘텐츠 사용자 그룹과 디지털 콘텐츠 제공자 서버는 자신의 공개키와 인증 요청서를 확인하여 공개키를 포함한 인증서를 발급한다. CA 서버는 디지털 콘텐츠 사용자 그룹과 디지털 콘텐츠 제공자 서버의 인증서 요청서 정보와 인증서를 DB에 저장하고, CA는 서버는 디지털 콘텐츠 사용자 그룹과 디지털 콘텐츠 제공자 서버의 인증서를 디지털 콘텐츠 사용자 그룹과 디지털 콘텐츠 제공자 서버에 전송한다. 디지털 콘텐츠 사용자 그룹과 디지털 콘텐츠 제공자 서버는 CA 서버로부터 수신된 인증서를 자신의 비밀키와 함께 저장한다.

정보통신 산업의 발달은 네트워크 속도를 향상시키고 있으며, 디지털 콘텐츠를 서비스하는 전자상거래가 늘어나고 있다. 인터넷 자체는 보안을 고려하지 않은 전송매체이기 때문에 보안 문제가 발생한다. 또한 기업의 서버시스템은 불법 침입 및 데이터 파괴의 위협에 노출되어 있으며, 해킹이나 크래킹의 위협이 더욱 심해지고 있다. 따라서 서버시스템의 보호를 위한 보안 대책이 요구된다. 디지털 콘텐츠의 안전한 전송을 위해서는 전송되는 디지털 콘텐츠의 보안 기법이 필요하다. 일반적으로 멀티미디어 고품질 콘텐츠는 품질의 손상 없이 불법 복제가 가능하다. 또한, 인터넷에서 불법 복제된 콘텐츠의 배포는 디지털 콘텐츠 제공자에게 커다란 경제적 손실을 주고 있다. 따라서 공개키 기반의 안전하고 효율적인 패스워드 기반의 키 교환 프로토콜이 요구된다[12].

III. 제안 프로토콜

디지털 콘텐츠를 서비스하는 전자상거래가 늘어나고 있다. 인터넷 자체는 보안을 고려하지 않은 전송매체이기 때문에 보안 문제가 발생한다. 또한 기업의 서버시스템은 불법 침입 및 데이터 파괴의 위협에 노출되어 있으며, 해킹이나 크래킹의 위협이 더욱 심해지고 있다. 따라서 인터넷과 같은 공개된 통신망을 통하여 안전하게 통신을 하기 위해서는 전송하려는 정보를 암호화하여야 하며 통신 상대자간에 암호화를 위해 공통으로 사용할 키를 공유해야한다. 이때 통신 상대자간에는 정보를 교환하고 있는 상대가 실제 상대인지를 확인하는 인증과정이 반드시 필요하다.

1976년에 제안된 Diffie-Hellman 키 교환 프로토콜은 안전하지 않은 통신상에서 세션키를 공유하기 위한 가장 잘 알려진 방법이다[3]. 이 프로토콜은 유한 필드 상에서 이산 대수문제와 Diffie-Hellman 문제의 어려움을 이용하여 참여자들 간에 세션키를 공유한다. 하지만 참여자들을 인증하는 방법을 제공하지 않기 때문에 중간 침입자 공격에 취약하였다. 참여자 인증을 위한 기술들은 다음과 같이 분류할 수 있다.

- 패스워드와 같은 사용자가 알고 있는 지식을 통한 인증 (What you know)
- 지문이나 홍채와 같은 사용자의 물리적인 특징을 통한 인증 (Who are you)
- 스마트카드와 같은 사용자가 소유한 물건을 통한 인증 (What you have)

이러한 방법 중에서 첫 번째는 간단하고, 편리하고, 적응이 쉽고, 이동성, 그리고 하드웨어 사용의 불필요 등의 장점을 가지고 있기 때문에 가장 널리 이용되는 방법이지만 가장 안전하지 못하다. 왜냐하면, 프로그램의 변수 범위에 따라 추측이 가능하기 때문이고, 패스워드의 대부분은 쉽게 추측이 가능한 것을 사용하는 것도 이유가 된다.

생물학적 인증은 이것보다 더 낫지만, 아직까지 과학이 이를 뒷받침 해주지 못하고 있다. 음성 같은 경우에는 만일 감기가 걸린다면 목소리가 일치하지 않으므로 거부당하게 되고, 지문 인증과 같은 경우에는 손에 상처가 나게 되면, 역시 거부당하게 된다.

앞으로 프로토콜의 안정성을 분석하는데 용어에 대한 편리성을 위하여 다음과 같이 쓰기로 한다. 디지털 콘텐츠 사용자 그룹을 클라이언트(Client)로 나타내고, 디지털 콘텐츠 제공자를 서버(Server)로 나타내고자 한다.

3.1 제안 프로토콜의 용어

안정성과 실행속도 및 사용자의 편의성을 공개키 기반의 안전하고 효율적인 디지털 콘텐츠 분배 시스템을 설계를 위하여 2장에서는 안정성과 키 분배의 효율성을 위해 RSA 공개키 기법을 사용하였다. 본 논문에서는 디지털 콘텐츠의 보호를 위하여 디지털 콘텐츠 사용자 그룹은 패스워드를 디지털 콘텐츠 제공자는 그 패스워드의 검증자를 사용하여 서로를 인증하고 세션키를 공유할 수 있는 CDN에서 패스워드를 이용한 공개키 기반 프로토콜을 제안하고자 한다.

표 1. 기호의 정의
Table 1. Definition of notation

용 어	의 미
id	클라이언트의 ID
g	곱셈 군 Z_n^*의 생성자
n	큰 소수
π	클라이언트에 의해 선택된 패스워드
π'	공격자에 의해 추측된 패스워드
v	서버에 저장되는 패스워드 검증자
a, b	클라이언트와 서버에 의해 각각 선택된 Z_n^*의 임의의 원소
$h()$	안전한 일 방향 해쉬함수
K	세션키
$\oplus$	비트 XOR 연산
$x \doteq y$	x와 y값이 같은지를 비교
k	보안 파라미터

3.2 암호화

디지털 콘텐츠를 보호하기 위하여 다음과 같은 암호화 기법을 사용하였다. 안정성과 키 분배의 효율성을 위해 Diffie-Hellman 공개키 기법을 사용하였다. 1계층에서 공개키에 의해 암호화된 디지털 콘텐츠는 2계층의 디지털 콘텐츠 사용자 그룹에서 개인키에 의해 복호화되고, 2계층의 디지털 콘텐츠 사용자 그룹은 3계층의 사용자 실행의 속도를 고려하여, 복호화된 디지털 콘텐츠를 다시 공개키로 부분적으로 암호화하여 캐시에 저장한다. 2계층과 3계층 사이의 전송은 인트라넷을 통해 시스템적인 보안성을 가진 전송이다. 2계층은 승인된 사용자에게만 부분 암호화된 콘텐츠를 제공한다.

2계층은 디지털 콘텐츠 사용자 그룹에 해당하며, 1계층과 2계층의 콘텐츠 전송은 보안성이 없는 인터넷을 통해 이루어진다. 따라서 디지털 콘텐츠 제공자와 디지털 콘텐츠 사용자 그룹 사이의 콘텐츠 전송에는 패스워드를 이용한 키 교환 프로토콜을 사용한다.

3.3 프로토콜

프로토콜의 두 참여자 디지털 콘텐츠 사용자 그룹과 디지털 콘텐츠 제공자은 합법적인 참여자들이다. 디지털 콘텐츠 사용자 그룹과 디지털 콘텐츠 제공자은 안전하게 Z_n^* 상의 생성자인 g와 큰 소수인 n을 미리 공유하고 있다고 가정한다. $h()$는 $\{0,1\}^* \rightarrow \{0,1\}k$인 안전한 일방향 해쉬 함

수[10]이다. 이 해쉬 함수는 랜덤 오라클[11]로써 동작한다고 가정한다. 보안 파라미터 k는 해쉬 함수의 출력 값의 비트 크기이며 전사(Brute-force) 공격을 막을 수 있을 만큼 충분히 큰 크기를 가져야 한다. $\{0,1\}^*$는 임의의 길이를 갖는 유한한 이진 문자열이고 $\{0,1\}k$는 k의 길이를 갖는 이진 문자열을 나타낸다. 프로토콜의 참여자인 디지털 콘텐츠 사용자 그룹과 디지털 콘텐츠 제공자는 합법적인 사용자들이다. 디지털 콘텐츠 사용자 그룹은 패스워드 π를 소유하고 있고 디지털 콘텐츠 제공자는 디지털 콘텐츠 사용자 그룹의 id와 패스워드의 검증자인 $v = g^{h(Client, Server, \pi)}$를 패스워드 파일에 저장하고 있다고 하자.

디지털 콘텐츠 사용자 그룹과 디지털 콘텐츠 제공자가 세션키를 생성하기를 원할 때, CDN에서 패스워드를 이용한 키 교환 프로토콜은 다음 (그림 4)와 같이 수행된다.

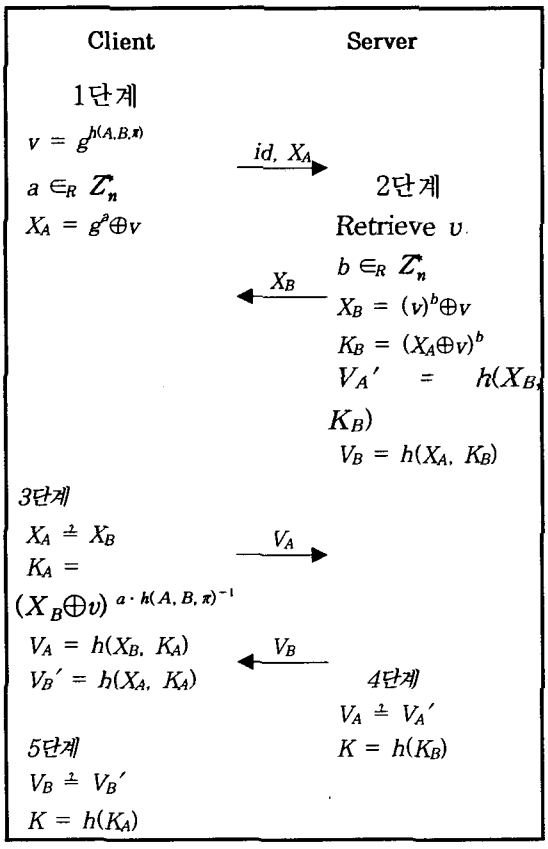

그림 4. 프로토콜 절차
Fig 4. Process of protocol

(그림 4)에서 A는 클라이언트이고 B는 서버를 의미한다.

제안한 프로토콜은 크게 두 과정, 즉 세션키 정보 생성 과정과 세션키 정보 검증 과정으로 나뉠 수 있다. 세션키 정보 생성과정은 Client와 Server가 각각 자신의 정보와 상대방의 정보를 조합하여 Diffie-Hellman 값인 g^{ab}를 계산하는 과정이고 세션키 정보 검증 과정은 계산된 이 값이 정확한지를 검사함으로써 서로를 인증하는 과정이다. 제안된 프로토콜이 성공적으로 완료하면 Client와 Server는 같은 세션키인 $K = h(K_{Client}) = h(K_{Server}) = h(g^{ab})$를 공유하게 된다.

Ⅳ. 제안 프로토콜의 안정성 분석

디지털 콘텐츠는 품질의 손상 없이 복제되어 인터넷을 통해 배포 가능하며, 이는 디지털 콘텐츠 제공자에게 커다란 경제적 손실을 주게 된다. 이에 따라 디지털 콘텐츠를 안전하고 효율적인 전송을 위해 키 교환 프로토콜이 필요하다.

디지털 콘텐츠를 사용자의 편의성과 실행 속도, 보안성 문제 등이 있는데, 본 절에서는 3장에서 제안한 디지털 콘텐츠를 효율적으로 전송하기 위하여 패스워드 기반의 키 교환 프로토콜에 대한 안정성 분석을 한다.

패스워드 기반의 키 교환 프로토콜에 대한 안전성은 이산대수문제와 Diffie-Hellman 문제의 어려움, 그리고 해쉬 함수의 암호학적 강도에 기반을 두고 있다. 이 프로토콜은 중간 침입자 공격, 패스워드 추측 공격 측면에서 안정성을 분석하고자 한다.

4.1 중간 침입자 공격

키 교환 프로토콜은 공격자의 도청, 수정, 반송, 재전송, 위장 공격들에 대하여 세션키와 패스워드에 관한 정보를 노출시켜서는 안 되며 잘못된 세션키의 공유를 탐지할 수 있어야 한다.

다음은 중간 침입자 공격 기법에 대하여 분석하자 한다. 중간 침입자 공격 기법에는 다음과 같다.

① 수동적인 공격을 고려해보자.
공격자는 전송 메시지들을 청하여

$$X_{Client} = g^{a} \oplus g^{h(Client, Server, \pi)},$$
$$X_{Server} = g^{b \cdot h(Client, Server, \pi)} \oplus g^{h(Client, Server, \pi)},$$
$$V_{Client} = h(g^{b \cdot h(Client, Server, \pi)} \oplus g^{h(Client, Server, \pi)}, g^{ab}),$$
$$V_{Server} = h(g^{a} \oplus g^{h(Client, Server, \pi)}, g^{ab})$$

를 얻을 수 있다. 그러나 공격자가 이 값들을 획득한다 하더라도 π와 K를 계산할 수 있는 방법은 없다.

② 적극적인 공격자의 수정 공격을 고려하자.
공격자가 X_{Client}와 X_{Server}를 중간에서 수정하여 상대에게 전송한다면, 이 위조된 값들은 Client와 Server에 의해 K_{Client}와 K_{Server}를 생성하는데 각각 사용되게 된다. 그러나 Client는 임의의 정수 a를 사용하여 K_{Client}를 계산하고 Server는 임의의 정수 b를 사용하여 K_{Server}를 계산하기 때문에 K_{Client}와 K_{Server}의 값이 같게 될 확률은 무시할만하다. 결국, 이 공격은 검증 값들을 다르게 만들므로 검증 단계에서 탐지될 수밖에 없다.

③ 적극적인 공격자의 재전송 공격을 고려하자.
재전송 공격은 이전 세션의 전송 메시지들을 저장해 두었다가 이후 세션들에 이용하는 공격이다. 그러나 매 세션 마다 각 참여자들은 새로운 임의의 난수 a와 b를 생성하여 사용한다. 공격자가 이 난수들을 알 수 있는 확률은 무시할 만하다.

④ 적극적인 공격자의 반송 공격을 고려하자.
즉 공격자는 통신선로 중간에서 Client가 Server에게 보낸 X_{Client}와 V_{Client}를 Client에게 되돌려 보내어 잘못된 세션키 생성을 유도하려 할 수 있다. 그러나 3단계에서 Client는 Server로부터 X_{Server}를 받은 후에

$$X_{Client} \stackrel{?}{=} X_{Server}$$

인지를 검사하기 때문에 이러한 공격은 성공할 수 없다.

⑤ 공격자는 합법적인 참여자로 위장하여 정상적인 방법으로 다른 합법적인 참여자와 세션키를 공유하려고 할 수 있다. 그러나 이러한 위장공격은 공격자가 패스워드를 알지 못하기 때문에 검증 단계에서 탐지될 수밖에 없다.

다섯 가지에 대하여 분석한 결과 제안한 프로토콜들은 이와 같은 중간 침입자 공격들에 안전하다.

4.2 패스워드 추측 공격

패스워드 추측 공격은 온라인 패스워드 추측 공격과 오프라인 패스워드 추측 공격으로 나뉠 수 있다. 온라인 패스워드 추측 공격은 패스워드 인증 실패 횟수를 누적함으로써 쉽게 탐지되고 시도 횟수를 제한함으로서 쉽게 조치될 수 있다. 그러나 공격자는 안전하지 않은 통신상에서 메시지를 도청하거나 정당한 사용자로 가장하여 다른 정상 사용자와의 메시지 교환을 통해 발생하는 정보들을 저장해 두고 오프라인으로 패스워드에 관한 정보를 알아내려고 할 수 있다. 이러한 공격을 오프라인 패스워드 추측 공격이라 한다.

① 도청한 메시지만을 이용하는 수동적인 패스워드 추측 공격을 고려하자.
공격자는 메시지 X_{Client}, X_{Server}, V_{Client}, V_{Server}를 가로채 저장하고, 패스워드로 사용될 수 있는 π'를 추측한다. 그리고 π'을 도청한 값들에 적용하여 비교함으로 검증한다. 이를 모든 패스워드 범위에 대하여 반복 수행함으로써 추측한 π'가 참여자들이 사용하고 있는 정확한 π인지를 확인해야 한다. 그러나 제안된 프로토콜들에서는 전송 메시지인 X_{Client}, X_{Server}, V_{Client}, V_{Server} 에 π'를 적용하여도 π'가 정확한지를 검증할 방법이 없다.

② 공격자가 정당한 참여자로 위장한 적극적인 패스워드 추측 공격을 고려해 보자.
공격자가 Client로 위장한다면 자신이 만든

$$a, g^{a}, g^{a} \oplus g^{h(Client, Server, \pi')}$$

와 Server로부터 받은

$$g^{b \cdot h(Client, Server, \pi)} \oplus g^{h(Client, Server, \pi)}$$

를 얻을 수 있다. 그러나 이들을 이용해서는 π'가 정확한지를 검증할 방법이 없다. 그리고 공격자가 Server로 위장한다면 자신이 생성한

$$b,\ g^{b},\ g^{h(Client,Server,\pi')},\ g^{b\cdot h(Client,Server,\pi')},$$
$$g^{b\cdot h(Client,Server,\pi')} \oplus g^{h(Client,Server,\pi')}$$

와 Client로부터 받은

$$g^{a} \oplus g^{h(Client,Server,\pi)},$$
$$h(g^{b\cdot h(Client,Server,\pi')} \oplus g^{h(Client,Server,\pi')},$$
$$(g^{b\cdot h(Client,Server,\pi')} \oplus g^{h(Client,Server,\pi')})^{a\cdot h(Client,Server,\pi)^{-1}})$$

값들을 얻을 수 있다. 그러나 이 값들을 이용해서도 π'가 정확한지를 검증할 방법이 없다. 그러므로 제안한 프로토콜들은 패스워드 추측 공격에 안전하다.

V. 결 론

디지털 콘텐츠는 많은 저작자들의 창의성과 노력으로 만들어진다. 하지만, 디지털 데이터는 그 특성상 원본과 복사본의 구분이 불가능하기 때문에 디지털 콘텐츠 파일의 무단 복사 및 도용은 많은 저작자들의 저작 의욕을 저하시킬 뿐만 아니라 디지털 콘텐츠 사업에 심각한 위협을 초래하게 한다. 따라서 디지털 콘텐츠에 대한 불법 복제를 방지하기 위해서 저작권 정보를 생성하고 이를 디지털 콘텐츠 파일에 워터마킹하는 정보보호 기법의 적용은 필수적이다.

이러한 디지털 콘텐츠의 저작권들을 보호하고 안전하게 디지털 콘텐츠를 전송하기 위하여 본 논문에서는 패스워드를 이용한 키 교환 프로토콜을 제안하였고, 그에 대한 안정성을 입증하기 위하여 중간 침입자 공격, 패스워드 추측 공격 측면에서 안전하다는 것을 입증하였다. 디지털 콘텐츠를 만드는 저작자들에게 유용하게 사용될 수 있다고 본다.

참고문헌

[1] 최승락, 양철웅, 이중식, "CDN의 핵심 구성 기술들과 경향", 정보과학회지, 제 20권 제 9호, 2002.9

[2] 지경용, 조은진, 고중걸, "콘텐츠 유통기술의 혁명", 진한도서,

[3] W. Diffie and M. E. Hellman, "New Directions in Cryptography," IEEE Transaction on information theory, Vol. 1T-22, No. 6, Nov., 1976.

[4] Spectral Lines, "Talking about Digital Copyright," IEEE Spectrum, Vol. 38, Issue 6, p. 9 June, 2001.

[5] 고일석, 나윤지, 조동욱, "공개키 기반의 계층 구조를 갖는 디지털콘텐츠 분배 시스템의 설계," 정보처리학회논문A, 제 11-A권 제 2호, pp. 175-180, 2004. 4.

[6] ITU-T Rec. X.509, Information technology-Open Systems Interconnection-The Dictionary : Public-key and attribute certificate framework, March, 2000.

[7] G. Barish, K. Obraczka, World Wide Web Caching : Trends and Techniques, IEEE Communications, Internet Technology Series, May, 2000.

[8] H. Bahn, S. Noh, S. L. Min and K. Koh, "Efficient Replacement of Nonuniform Objects in Web Caches," IEEE Computer, Vol. 35, No. 6, pp. 65-73, June, 2002.

[9] Thorwkrth N. J., Horvatic P., Weis R., Jian zhap, "Security methods for MP3 music delivery," Signals, Systems and Computer, 2000. Conference Record of the Thirty-Fourth Asilomar Conference on, Vol. 2, pp. 1831-1835, 2000.

[10] D. R. Stinson, Cryptography Theory and Practice, CRC, 1995.

[11] M. Bellare and P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols." In ACM security 93, pp.62-73, 1993.

[12] 고병수, 장재혁, 최용락, "디지털 콘텐츠 유통 및 보호를 위한 인증 시스템 설계 및 구현", OA학회, 제8권 3호, 2003.
[13] 이성진, "인터넷 쇼핑몰의 구매모델에 관한 연구", 한국컴퓨터정보학회 논문지, 제10권 제2호, pp.199-204, 2005.

저 자 소 개

신 승 수

2001년 2월 충북대학교 수학과 (이학박사)
2004년 8월 충북대학교 컴퓨터공학과 (공학박사)
2005년 3월~현재 동명정보대학교 정보보호학과 교수
〈관심분야〉 암호학, PKI, 네트워크 보안, 콘텐츠보호

한 군 희

2000년 8월 충북대학교 컴퓨터공학과 (공학박사)
2001년 3월~현재 천안대학교 정보통신학부 교수
〈관심분야〉 콘텐츠보호, 웹시스템 개발