스마트 카드를 이용한 서버 인증이 필요 없는 디지털 콘텐츠 보호 기법

정회원 김 영 식*, 종신회원 임 대 운**°

Digital Contents Protection Without Server Authentication Using Smart Cards

Young-Sik Kim* *Regular Member*, Dae-Woon Lim**° *Lifelong Member*

요 약

오늘날 게임이나 동영상과 같은 디지털 콘텐츠를 불법 사용과 복제로부터 보호하는 것은 매우 중요한 일로 인식되고 있다. 많은 경우 허가받은 사용자만 디지털 콘텐츠를 사용토록 하기 위해서 하나 이상의 보안 서버를 두고서 이 서버와의 통신을 통해서 사용자 인증을 수행하게 된다. 하지만 이러한 방식은 사용자와 새로운 콘텐츠가 늘어날수록 인증 요청이 많아지게 되어 서버와의 통신에 상당한 비용이 발생하게 되는 문제가 있다. 더 나아가 제한적인 통신 기능만을 탑재한 플레이어의 경우에는 디지털 콘텐츠의 보호와 사용에 큰 제약이 따르게 된다. 이러한 문제를 해소하기 위해서 이 논문에서는 중앙 서버를 통한 인증이 없이도 카트리지 형태의 디지털 콘텐츠를 플레이어에서 인증이 가능하도록 하고, 디지털 콘텐츠의 불법 복제를 막을 수 있는 방법을 제안한다. 이 방법은 재생공격, 중간자 (MITM) 공격, 그리고 데이터 치환 공격에 안전하다.

Key Words : DRM, Digital Contents, Mutual Authentication, Smart Card.

ABSTRACT

Nowadays, it is considered as an important task to protect digital contents from illegal use and reproduction. In many cases, there are secure servers to authenticate the allowed users and the user authentication process is performed by communication between the servers and users. However, if the number of users and contents are increased, the servers should treat a large amount of authentication loads and the authentication cost will be considerably increased. Moreover, this scheme is not adequate for some players in which only a limited function of communication is deployed. In order to solve this problem, this paper proposes an authentication method which can certificate both the digital contents and players, and prevent illegal reproduction without the certification server. The proposed scheme is secure in the replay attack, the man in the middle attack, and data substitution attack.

Ⅰ. 서 론

오늘날 게임이나 동영상과 같은 각종 디지털 콘텐츠 보호에 대한 관심이 크게 증가하고 있다. 디지털 콘텐츠를 정해진 사용자와 플레이어에서만 읽을 수 있도록 하기 위해서는 사용자와 플레이어를 인증하는 과정이 필요하다. 많은 경우 이러한 인증 과정은 제3의 인증 서버를 두고서 이 서버와의 통신을 통해서 이

※ 본 연구는 한국연구재단 기초연구사업의 지원을 받아 수행되었음(과제번호: 2010-0002355)
* 조선대학교, 정보통신공학과 (iamyskim@chosun.ac.kr), ** 동국대학교 정보통신공학과 (daewoonlim@gmail.com), (°: 교신저자)
논문번호 : KICS2010-10-513, 접수일자 : 2010년 10월 31일, 최종논문접수일자 : 2011년 3월 4일

루어지게 된다. 하지만 이러한 통신 환경이 배제된 상황에서는 정당한 사용자라 하더라도 자신이 구매한 디지털 콘텐츠를 자유롭게 사용하는데 제약이 따르게 어지, 반대로 이러한 제약을 완화시키면 디지털 콘텐츠에 대한 보호가 취약해 지는 문제가 발생하게 된다. 즉, 구매한 디지털 콘텐츠의 정당한 사용 범위를 정해진 장비에 한정하거나 정해진 지역에 한정한다면 사용자의 불편은 그만큼비에 커게 된다지만, 제약을 풀 경우 불법 복제와 불법 사용을 막기가 어려워진다.

또한 인증 과정에서 서버와의 지속적인 통신이 이루어지면, 서버는 여러 플레이어에서 요청한 인증 과정을 동시에 처리해야 하는데, 사용자와 디지털 콘텐츠의 개수가 증가할수록 처리해야하는 부담이 더 커지게 된다.

따라서 서버의 부담을 최소화하면서도, 특히 서버에 접속하지 않은 상태에서도 적법한 사용자가 적법하게 구매한 디지털 콘텐츠를 자유롭게 사용하도록 할 수 있는 서버에 독립적인 디지털 콘텐츠 보호 방법이 필요하다.

한편 오늘날 스마트 카드의 다목적성, 이동성, 편리성, 그리고 보안과 같은 특성 때문에 스마트 카드를 사용하는 분야가 매우 다양해 졌다. 교통카드와 신용카드와 같은 분야는 물론이고 기업이나 단체에서 내부자를 인증하고 관리하기 위한 도구로도 널리 활용하고 있다.

오늘날 널리 쓰이는 스마트 카드에는 기본적으로 RSA나 타원 곡선 암호와 같은 공개키 암호나 AES와 같은 블록 암호를 위한 연산 하드웨어 및 소프트웨어를 기본으로 탑재하고 있어서 보안에 필요한 연산 과정을 고속으로 수행할 수가 있다. 특히 많은 스마트 카드들이 부채널 공격(side channel attack)에 대한 기본적인 방어 기능(countermeasure)들을 내장하고 있어서 인증, 식별, 무결성, 부인방지, 기밀성과 같은 다양한 암호학적 기능들을 안전하게 제공해 줄 수가 있다. 또한 스마트 카드는 하드웨어적으로 부정조작 방지(tamper- resistant)를 제공해 줄 수가 있다.

디지털 콘텐츠 인증과 관련해 다음과 같은 연구 결과들이 있다. 먼저 Lamport는 검증 테이블을 사용 인증하는 방법을 제시하였으나 패스워드를 기반의 방식과 동일한 문제를 지니고 있었다[1]. Hwang과 Li는 ElGamal 암호를 이용한 원격 사용자 인증 프로토콜을 제시하였으나[2], Chan과 Cheng이 가장 공격(impersonation attack)이 가능함을 보였다[3]. Sun은 스마트 카드를 이용한 원격 사용자 인증 방식을 제안하였고[4], Chien, Jang, 그리고 Tseng이 상호 인증 방식으로 개선시켰다[5]. 그러나 Hsu는 Chien 등의 방법 역시 가장 공격이 가능함을 지적하였다[6].

Juang은 효율적인 다중 서버 패스워드 인증 방법을 스마트 카드를 활용해서 제안하였다[7,8]. 이 방법에서는 스마트 카드를 이용하기 때문에 원거리 사용자 인증 과정을 단순화시킬 수 있었지만, 등록 센터가 핵심적인 역할을 맡게 되어 결과적으로 등록 센터에 병목현상이 발생하는 문제를 지니고 있다.

이 논문에서는 스마트 카드에서 제공하는 기본적인 암호 연산들을 이용해서 서버와의 통신이 없이도 디지털 콘텐츠를 상호 인증하는 방법을 제시한다. 또한 디지털 콘텐츠를 암호화하고 이 암호화에 대한 키를 다시 암호화함으로써 디지털 콘텐츠의 불법적인 사용과 복제를 방지하는 기법을 제시할 것이다. 이 방법을 사용하면 재생공격이나 중간자 (Man in the Middle, MITM) 공격 및 데이터 치환 공격에 기본적으로 안전하며 이러한 인증시스템이 만족해야 할 다양한 보안 기준들을 만족할 수 있음을 보일 것이다.

이 논문은 다음과 같이 구성된다. 제2장에서는 이 논문에서 만족시키고자 하는 기본적인 보안 요구사항에 대해서 정의할 것이다. 그리고 제3장에서는 이러한 요구사항을 만족시키기 위한 프로토콜에 대해서 기술한다. 그리고 제4장에서는 이 프로토콜을 여러 가지 공격에 대해서 어떠한 보안을 제공할 수 있는지에 대해서 논의할 것이다. 마지막 장에서 이 논문을 정리하고 결론을 맺을 것이다.

Ⅱ. 문제의 정의

오늘날 디지털 콘텐츠를 보호하기 위해서 DRM (Digital Right Management)기법이 널리 사용된다[9-12]. 그러나 DRM은 불법 사용 방지와 구매한 장치에서만 사용하도록 제한하기 때문에 카트리지를 통해서 디지털 콘텐츠를 사용자간에 자유롭게 교환하는 것이 불가능하다. 이런 불편을 해소하기 위해서 허가된 도메인 안에서는 구매한 콘텐츠를 상호 교환하여 이용하는 것이 가능한 AD-DRM (authorized domain DRM)이 제안 되었지만[11,12] 멤버 탈퇴를 처리하는 문제가 복잡하다는 단점을 가지고 있다.

일반적으로 DRM을 사용할 때는 제3의 신뢰기관이 존재해서 인증과정을 도와주게 된다. 하지만 유선이나 무선통신을 통해서 제3자로부터 매번 인증을 받지 못하는 상황에서는 이런 기법을 사용할 수가 없다. 예를 들어 휴대용 게임기에서 카트리지를 이용해서 게임 데이터를 읽어 오는 경우에 휴대용 게임기의 가

격 경쟁력을 위해서 제한된 범위의 통신 기능만을 제공해 주는 경우가 많이 있다. 이런 경우에는 게임 데이터를 보호하기 위해서는 서버와의 통신이 없이도 인증과정을 수행하는 것이 가능해야만 한다. 서버를 통한 인증 과정을 사용하는 경우 무선 통신 서비스 영역을 벗어나면 이미 내장된 디지털 콘텐츠 외에 새로운 디지털 콘텐츠를 적용해서 사용하는 것이 불가능하게 된다. 이러한 불편을 해소하고 서버의 부담을 최소화하기 위해서는 제3의 신뢰기관과의 통신이 없이 인증이 가능한 새롭고 안전한 방법이 필요하다.

또한 기본적으로 디지털 콘텐츠를 적법하게 구매한 사용자가 적법한 시스템(플레이어)에서 사용할 수 있도록 하기 위해서는 디지털 콘텐츠와 플레이어 간의 상호 인증을 통해서 안전성을 확보해야만 한다. 보안을 위해서는 서버와의 통신 없이 상호 인증을 수행할 때 기본적으로 인증에 사용하는 비밀 정보를 공유하는 참여자의 수는 최대한 적게 유지하여야만 한다. 또한 사용자 개인 정보를 유출하지 않고서도 단말 대 단말 사이의 인증과정을 제공해 주어야 한다.

앞으로 이 논문에서는 디지털 콘텐츠를 담아 유통하는 장치를 카트리지라 부르고 이 카트리지를 재생하기 위한 장비를 플레이어라 부를 것이다.

Ⅲ. 보안 위협 및 요구사항

디지털 콘텐츠를 사용하는 과정에서 발생할 수 있는 주요 보안 위협들로는 아래와 같은 것들이 있다.

- ☐ 중간자 공격(man-in-the-middle attack): 제3의 공격자가 플레이어와 카트리지 사이의 통신 내용을 가로채서 비밀 정보를 가로채거나 정당한 객체로 위장하는 공격.
- ☐ 재생 공격(replay attack): 플레이어와 카트리지 사이의 통신 내용을 저장한 후에 다시 이를 반복함으로써 플레이어 또는 카트리지를 속여서 정당한 기기로 인정받는 공격.
- ☐ 가장 공격 (impersonation attack): 부정한 사용자의 ID_i와 PW_i를 사용해서 또 다른 정당한 ID_j와 PW_j를 만드는 공격 방법.
- ☐ 불법 복제: 디지털 콘텐츠 또는 이를 포함한 카트리지를 불법적으로 복제해서 유통하는 것. 또한 불법적으로 복제 및 제작된 플레이어를 사용해서 정상적인 디지털 콘텐츠를 사용하는 것.
- ☐ 데이터 치환 공격(data substitution attack): 인증은 정상적인 카트리지 하나를 통해서 받도록 하더라도 실제 실행 데이터를 마음대로 치환함으로써 사실상 인증 과정을 우회하는 방법.

Ⅳ. 제안하는 방식

이 논문에서는 스마트 카드의 여러 기능을 활용하는 콘텐츠 보호 기법을 제시한다. 스마트 카드를 활용하게 되면 여러 가지 암호 연산을 고속으로 안전하게 수행하는 것이 가능할 뿐만 아니라 여러 비밀 정보들을 안전하게 보호하는 것이 가능하다. 또한 스마트 카드를 활용하게 되면 이러한 보안성을 비교적 저렴한 가격에 확보하는 것이 가능하다.

스마트 카드에서는 많은 경우 RSA나 타원곡선 암호(Elliptic Curve Cryptography)와 같은 공개키 암호 연산을 위한 하드웨어 엔진을 제공해 줄 뿐만 아니라 AES나 DES/TDES의 암호화 및 복호화를 고속으로 수행할 수 있는 하드웨어 엔진을 가지고 있다. 또한 안전한 의사난수발생기(Pseudo Random Number Generator)나 진난수발생기(True Random Number Generator) 중 적어도 하나를 내장하고 있다. 이러한 것들은 해당 연산을 매우 빠르게 수행하는 것이 가능한 환경을 만들어 준다.

제안하는 방식에서 플레이어와 카트리지는 스마트 카드를 각각 하나씩 가지고 있다고 가정한다. 생성된 비밀정보들은 플레이어와 스마트 카드의 보안 메모리에 저장된다. 이 때 보안 메모리에 저장되는 비밀 정보들은 스마트 카드의 부정 조작 방지를 위한 각종 센서들을 통해서 안전하게 보호된다고 가정한다. 그러면 다음과 같이 1) 사전작업 2) 상호 인증 3) 데이터 전송의 세 단계로 디지털 콘텐츠를 보호하게 된다.

4.1 사전작업

사전작업은 신뢰가 보장되는 관리기관에 의해서 이루어진다. 관리기관은 플레이어와 카트리지들 각각의 공개키와 개인키를 만들고 마스터키 쌍 (x_1, x_2)를 사용해서 카트리지의 ID와 패스워드를 생성한다. 여기서 마스터키 쌍은 임의의 큰 소수 p에 대해서 $x_1, x_2 \in Z_p$를 만족한다. 사전작업은 다음과 같은 절차로 이루어진다.

(1) 공개된 인증 채널(public authenticated channel)을 통해서 플레이어들의 공통의 공개키 (PUB_G)를 모든 플레이어와 카트리지가 공유해야 한다.

그리고 플레이어들의 공통의 개인키(PRI_G)와 마스터키 쌍(x_1, x_2)을 플레이어에 내장된 스마트 카드에 저장시킨다.

(2) 카트리지들은 각자 개별 공개키와 개인키 쌍(PUB_{L_i}, PRI_{L_i})을 하나씩 소유하고 있고 두 개의 키 모두 비공개로 한다.

(3) 카트리지의 아이디(ID_i)와 패스워드(PW_i)는 다음과 같이 관리기관이 보유한 마스터키 쌍 (x_1, x_2)를 사용해서 생성한다.

$$ID_i = h(PUB_{L_i})$$
$$PW_i = [ID_i^{x_1} + 1]^{x_2} \bmod p$$

여기서 $h(\cdot)$는 일방향 해쉬 함수이고 PUB_{L_i}은 i번째 카트리지의 공개키이다. 생성된 패스워드는 카트리지에 포함된 스마트 카드의 보안 메모리에 저장된다.

(4) 디지털 콘텐츠(D)는 개별 콘텐츠 카트리지가 가진 고유의 비밀키(K_{L_i})를 사용해서 AES 블록 암호(BC)로 암호화($BC_{K_{L_i}}(D)$) 되고, 암호화에 사용된 비밀키(K_{L_i})는 다시 카트리지의 개인키(PRI_{L_i})로 암호화되어서 스마트 카드의 메모리에 저장된다.

아래 그림 1은 카트리지에 포함된 스마트 카드에 저장되는 비밀정보 및 디지털 콘텐츠를 저장하고 있는 롬(ROM)의 구조를 보여주고 있다.

4.2 상호 인증

(1) 카트리지는 먼저 자신의 공개키(PUB_{L_i})와, 패스워드(PW_i), 스마트 카드에 포함된 난수 발생기(RNG)에서 새롭게 생성한 세션키(N_t), 그리고 현재의 타임스탬프(T_1)를 연접한 값 ($PUB_{L_i} \| PW_i \| N_t \| T_1$)을 플레이어의 공개키 ($PUB_G$)로 암호화 한 후에 이를 플레이어로 전송한다.

(2) 플레이어에서는 공통의 개인키(PRI_G)로 카트리지에서 전송받은 암호문을 복호화한 후에 카트리지의 공개키(PUB_{L_i})와 세션키(N_t)를 얻게 된다.

(3) 플레이어에서는 우선 카트리지의 타임스탬프 (T_1)를 확인하여 미리 정해진 값(T_{th}) 보다 작은 경우, 카트리지의 공개키(PUB_{L_i})에 일방향 해쉬 함수를 적용시켜서 ID_i를 만든다. 그 후 다시 마스터키 쌍 (x_1, x_2)을 이용해서 PW_i를 만들어서 카트리지가 전송한 PW_i와 비교한다. 이 때 두 값이 같으면 플레이어는 카트리지를 인증할 수 있다. 그러나 만일 타임스탬프가 미리 정해 진 값보다 더 큰 경우 플레이어는 유효기간이 지난 요청으로 판단해 인증을 거부한다.

(4) 이제 플레이어에서는 카트리지의 공개키(PUB'_{L_i})와 현재의 타임스탬프(T_2)를 연접시킨 ($PUB'_{L_i} \| T_2$)를 세션키 N_t를 사용해서 대칭키 암호로 암호화한 후에 다시 카트리지로 보낸다.

(5) 카트리지는 저장하고 있던 세션키(N_t)를 사용해서 대칭키 암호문을 복호화한 후 플레이어가 보내온 타임스탬프(T_2)를 미리 정해진 값(T_{th}) 보다 작은 경우, 보내온 카트리지의 공개키 (PUB'_{L_i})값이 올바른지를 확인함으로써 플레이어를 인증할 수 있다. 만일 타임스탬프가 T_{th} 보다 더 큰 경우 카트리지는 인증을 거부한다.

이 방식에서 플레이어의 인증은 플레이어의 공통 개인키(PRI_G)를 알고 있다는 것을 간접적으로 확인함으로써 이루어지고, 카트리지의 인증은 카트리지가 보낸 공개키(PUB_{L_i})와 이를 통해 생성한 PW_i를 카트리지가 보내온 PW_i와 비교함으로써 이루어진다.

플레이어의 인증이 필요한 경우는 플레이어와 소프트웨어의 형식을 특화함으로써 공급을 독점하는 방식의 사업 모델에서 유용한 기능이다. 예를 들어 닌텐도와 같은 게임기에서는 전체적인 표준에 의지하지 않고서 공급 업체가 게임기를 공급하고 해당되는 소프

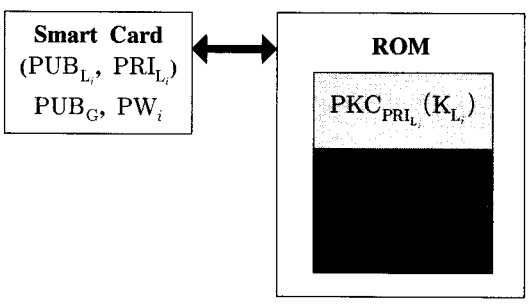


그림 1. 카트리지의 스마트 카드와 롬(ROM)의 구조

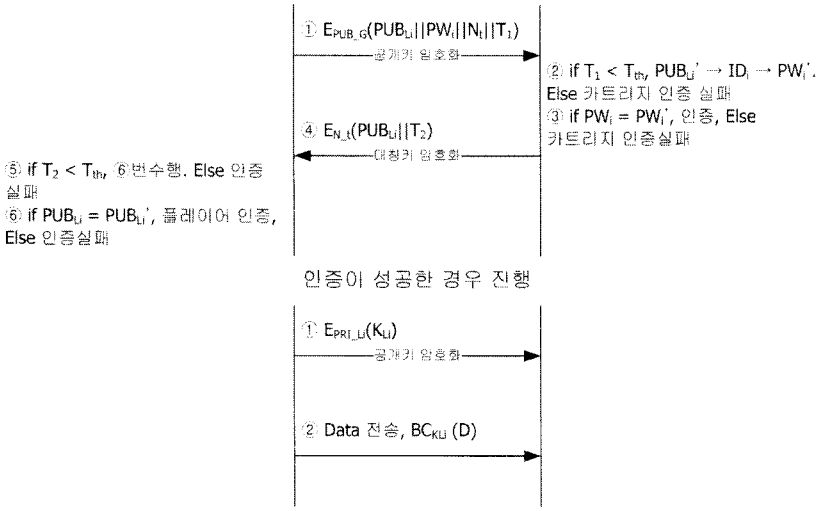


그림 2. 상호 인증 과정 및 데이터 전송 과정.

트웨어도 게임 플레이어에 특화되어 있다는 특징을 지닌다. 이 경우에는 소프트웨어 불법 복제가 가장 큰 문제가 될 뿐만 아니라, 플레이어의 불법 복제 역시 문제가 된다. 따라서 정품 플레이어에서 불법 소프트웨어를 막는 것 못지않게, 불법 플레이어에서 정품 소프트웨어를 사용하지 못하게 하는 것 역시 해당 기업에서는 중요한 이슈가 된다. 제안한 방식에서는 만일 플레이어의 개인키를 알지 못하는 불법 복제 플레이어의 경우는 위의 값들을 얻을 수가 없다.

플레이어의 공통 개인키(PRI_G)는 플레이어 내부의 스마트 카드의 보안 메모리에 저장되어 있고 이 공통 개인키(PRI_G)는 스마트 카드를 발급하는 기관에서 관리하고 모든 플레이어가 공유하게 된다.

4.3 데이터의 전송.

상호 인증이 이루어진 후에는 카트리지는 플레이어에게 암호화된 디지털 콘텐츠를 전송한다.

(1) 실제 디지털 콘텐츠를 사용하기 위해서 먼저 카트리지는 인증된 플레이어에게 자신의 개인키(PRI_{L_i})로 암호화시킨 블록 암호의 비밀키(K_{L_i})를 플레이어로 전달한다.

(2) 플레이어들의 공통의 개인키(PRI_G)를 알고 있는 정당한 플레이어는 이미 카트리지의 공개키(PUB_{L_i})를 안전한 채널로 전달받았기 때문에 블록 암호의 비밀키(K_{L_i})를 해독할 수가 있다.

(3) 그러면 카트리지는 다시 블록 암호화된 디지털 콘텐츠($BC_{K_{L_i}}(D)$)를 플레이어로 전달하게 된다.

(4) 그러면 블록 암호의 비밀키(K_{L_i})를 사용해서 D를 복구해서 플레이하게 된다.

2단계 상호 인증 과정 및, 3단계 데이터의 전송 과정을 그림 2에서 요약해서 보여주고 있다.

V. 안전성 분석

이 장에서는 제Ⅲ장에서 언급한 보안 위협들에 대해서 이 논문에서 제안한 방식이 안전한지를 분석해 볼 것이다.

□ 중간자(MITM) 공격: 플레이어의 개인키(PRI_G)는 정당한 플레이어들이 공유하는 비밀 정보로서 존재하고 카트리지의 공개키(PUB_{L_i})는 플레이어의 공개키(PUB_G)로 암호화된 상태로 공개된 채널로 전송되기 때문에 중간에서 카트리지와 플레이어의 전송 메시지들을 위장하는 MITM 공격은 불가능하다.

예를 들어 카트리지에서 플레이어로 보내는 메시지는 플레이어의 개인키(PRI_G)를 알아야 하지만 이 정보는 플레이어의 스마트 카드 안에 내장되어 있어서 안전하게 보호된다. 반대로 플레이어에서 카트리지로 보내는 메시지의 경우 카트리지의 개인키(PRI_{L_i})를 알아야 복호가 가능하지만 이 정보는 플레이어의 스마트 카드 안에 내장되어 있어서 역시 안전하게 보호된다.

□ 재생공격(replay attack): 인증과정에서 플레이어와

카트리지는 타임스탬프 T_1과 T_2를 서로 주고받아 제한 시간이 지난 요청에 대한 인증을 거부함으로써 재생공격을 방지할 수 있다.

□ 가장 공격: 카트리지의 ID_i와 패스워드 PW_i는 플레이어가 소유한 마스터키 쌍 (x_1, x_2)를 기반으로 만들어지기 때문에, 공격자가 카트리지의 공개키와 개인키 쌍 (PUB_{L_i}, PRI_{L_i})를 생성하더라도 마스터키 쌍을 모르기 때문에, 유효한 PW_i를 만드는 것이 불가능하다.

□ 비밀 키의 관리: 플레이어들은 하나의 개인키를 비밀정보로서 공유하지만 플레이어에 포함되는 개인키는 스마트 카드를 인증하고 발급하는 기관에서만 관리하고 스마트 카드 안에 저장되기 때문에 외부에서 물리적으로 이 값을 알아낼 수가 없다.

□ 불법 복제 방지: 데이터를 블록 암호화한 후에 블록 암호의 키를 카트리지의 개인키로 암호화해서 저장하였다. 카트리지의 공개키에 플레이어만 알고 있는 마스터키를 적용해 패스워드를 만들기 때문에, 공격자가 임의의 불법 소프트웨어를 정당한 카트리지로 제작할 수 없다. 또한 스마트 카드의 비밀 정보를 복제하지 않는 이상 암호화된 디지털 콘텐츠에 대한 재생 가능한 사본을 만드는 것이 불가능하다.

□ 데이터 치환 공격: 디지털 콘텐츠가 블록 암호화되어 있고 블록 암호의 비밀키를 스마트 카드의 비밀키로 다시 암호화해서 플레이어로 전달하기 때문에 스마트 카드와 롬에 포함된 데이터는 긴밀하게 연결되어 있다. 따라서 단순히 롬을 치환하는 것으로는 인증 과정을 우회할 수가 없다.

제안한 스마트 카드 인증방식에서 모든 보안 시스템의 기반은 플레이어들이 공유하는 개인키(PRI_G)를 가지고 있다. 따라서 만일 플레이어의 공유 개인키를 여러 참여자가 공유한다면 전체 시스템의 보안이 취약해 질 수가 있다. 그러나 이 키는 플레이어를 제작하는 제작자만 알고 있고, 디지털 콘텐츠를 만드는 소프트웨어 제작자들은 공유 공개키(PUB_G)를 공개된 인증 채널을 통해서 전달받기만 하면 되기 때문에 비밀 키를 관리하는 비용을 최소화 할 수가 있다.

VI. 결 론

이 논문에서는 스마트 카드를 활용해서 디지털 콘텐츠를 서버와의 통신을 통한 인증 과정 없이도 인증하는 기법을 제안하였다. 서버와의 통신 과정이 없기 때문에 통신 기능이 없거나 제한적인 플레이어에서도 정상적인 디지털 콘텐츠를 플레이할 수 있으며, 정상적인 디지털 콘텐츠를 구매한 사용자가 특별한 통신에 제약을 받지 않고서 다양한 콘텐츠를 사용할 수 있도록 만들어 준다.

이 논문에서 제안한 방법은 기본적으로, 재생 공격, 중간자 공격, 그리고 데이터 치환 공격에 안전하며, 스마트 카드에서 제공되는 AES와 공개키 암호, 그리고 표준적인 해쉬 함수를 사용함으로써 관련된 암호 연산을 고속으로 수행할 수가 있다.

이 논문에서는 플레이어가 동일한 공개키와 비밀키를 사용하도록 하였지만, 향후에는 플레이어가 동일한 공개키와 비밀키를 사용하지 않으면서도, 스마트 카드 기반의 서버 인증 과정을 거치지 않는 방식에 대한 연구가 더 필요할 것으로 보인다.

참 고 문 헌

[1] L. Lamport, "Password authentication with insecure communication," *Commun. ACM*, Vol.24, No.11, pp.770-772, 1981.

[2] M. S. Hwang and L. H. Li, "A new remote user authentication scheme using smart cards," *IEEE Trans. Consumer Electron.*, Vol.46, No.1, pp.28-30, Feb. 2000.

[3] C. K. Chan and L. M. Cheng, "Cryptoanalysis of a remote user authentication scheme using smart cards," *IEEE Trans. Consumer Electron.*, Vol.46, No.4, pp.992-993, Nov. 2000.

[4] H. M. Sun, "An efficient remote user authentication scheme using smart cards," *IEEE Trans. Consumer Electron.* Vol.46, No.4, pp.958-961, Nov. 2000.

[5] H. Y. Chien, J. K Jan, and Y. M. Tseng, "An efficient and practical solution to remote authentication: Smart card," *Computers and Security*, Vol.21, No.4, pp.372-375, Aug. 2002.

[6] C. L. Hsu, "Security of two remote user authentication schemes using smart cards," *IEEE Trans. Consumer Electron.*, Vol.49, No.4, pp.1196-1198, Nov. 2003.

[7] W.-S. Juang, "Efficient multi-server password authenticated key agreement using smart cards," *IEEE Trans. Consumer Electron.*, Vol.50,

pp.251-255, 2004.

[8] W.-S. Juang and J.-L. Wu, "Efficient User Authentication and Key Agreement With User Privacy Protection," *Int. J. Network Security*, Vol.7, No.1, pp .120-129, July 2008.

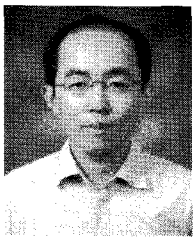
[9] F. Bao, R. H. Deng, and P. Feng, "An efficeint and practical scheme for privacy protection in the e-commerce of digital goods," ICICS 2000, LNCS 2836, pp.162-170, 2001.

[10] F. Pestoni, "IBM response to DVB-CPT call for proposals for content protection and copy management," http://www. almaden,ibm.com/software/ds/ContentAssurance/papers/xCP_DVB.pdf

[11] B. Popescu, B. Crispo, A. Tanenbaum, F. Kamperman, "Systems and architectures: A DRM security architecture for home networks," in Proc. 4th ACM Workshop DRM, 2004.

[12] A. M. Eskicioglu and E. J. Delp, "An overview of multimedia content protection in consumer electronic devices," Signal Processing: Image Commun., Vol.16, No.5, pp.681-699, Apr. 2001.

김 영 식 (Young-Sik Kim) 정회원



2001년 2월 서울대학교 전기공학부 공학사
2003년 2월 서울대학교 전기·컴퓨터공학부 석사
2007년 2월 서울대학교 전기·컴퓨터공학부 박사
2007년 3월~2010년 8월 삼성전자 책임연구원
2010년 9월~현재 조선대학교 정보통신공학과, 조교수
<관심분야> 암호학, 정보보호, 오류정정부호, 정보이론

임 대 운 (Dae-Woon Lim) 종신회원

1994년 2월 한국과학기술원 전기및전자공학과 학사
1997년 2월 한국과학기술원 전기및전자공학과 석사
2006년 8월 서울대학교 전기·컴퓨터공학부 박사
1995년 9월~2002년 8월 LS산전(주) 중앙 연구소 선임 연구원
2006년 9월~현재 동국대학교 IT학부 조교수
<관심분야> OFDM, 부호 이론, 시공간 부호