USIM을 활용한 Smart Phone 상의 Streaming DRM system

박범수*, 김태용**, 이훈재**
*동서대학교 유비쿼터스IT과
**동서대학교 컴퓨터정보학부
e-mail : beumsupark@hotmail.com

The Streaming DRM system Using USIM on a Smart Phone

Beum Su Park*, Tae Yong Kim**, Hoon Jae Lee**
*Dept. of Ubiquitous and IT Graduate of General School, Dongseo University
**Div. of Computer and Information Engineering, Dongseo University

요 약

최근 IT 기술의 발달로 많은 디지털 컨텐츠 서비스 사업이 사용자에게 제공되고 있으며, 유로 컨텐츠의 경우 사용자 개인 정보를 통한 사용자 인증을 요구되고 있다. 이에 저작권 보호, 관리, 유통을 위한 DRM 기술의 확보가 콘텐츠 사업의 성장에 필수 항목으로 요구되고 있으며 기반 기술 및 국제 표준화를 위한 노력중에 있다. 본 논문은 최근 보급률이 급증하고 있는 SmartPhone 상에서 음원 컨텐츠 서비스 이용에 적용 가능한 DRM 시스템을 제안하였다. 제안된 DRM 시스템은 사용자의 USIM 카드를 이용하여 암복호화에 사용되며, 불법적인 복제 방지를 위한 방안도 제시하고 있다.

1. 서론

근래에 인터넷의 지속적인 발달로 인해 많은 컨텐츠 서비스 사업이 디지털화되어 인터넷 서비스로 제공되며, 이를 이용하는 사용자 또한 늘어나고 있다. 그리고 최근 이슈화 되고 있는 Smart Phone의 보급률 급격하게 증가하고 있으며, Smart Phone상의 다양한 컨텐츠 서비스가 생성되어 제공되고 있다.

또한, 인터넷과 정보기술의 발달로 제공되는 서비스의 양과 질이 향상되었으며, 대다수의 서비스가 개인정보를 통한 개인 인증을 요구하여 이를 통한 유료 서비스를 확장 이용하게 한다. 이에 디지털 콘텐츠의 저작권 보호, 관리, 유통을 위한 기술 체계인 DRM(Digital Rights Management) 기술의 확보가 콘텐츠 사업의 성장에 필수 항목으로 요구되고 있으며 선진국을 비롯한 국제 표준화 기구에서도 이에 대한 중요성을 인지하여 기반 기술의 개발 및 표준화 중에 있다[1].

본 논문은 Smart Phone 상에서 제공 되는 음원 컨텐츠 서비스의 저작권 보호를 위한 DRM 시스템을 제안 하였다. 또한 사용자 USIM을 이용한 DRM 시스템을 구성, 타 Smart Phone 기기에서 인증된 사용자의 USIM을 사용하여 음원 컨텐츠를 이용할 수 있도록 설계 하였다. 또한, PingPong-128 스트림 암호화와 XOR 연산을 사용하여 컨텐츠의 암복호화 속도의 향상을 용의하게 설계하여 제시 하였다.

2. 관련 연구

2.1 사용자 인증 기술

사용자 인증기술은 인터넷 통신망 환경에서 사용자 자신의 신분 및 접근권한을 통신하는 대상에게 증명하여 접근권한을 부여 받는 기술 수단이다. 사용자 인증기술은 1981년 제안된 원격사용자 인증 기법을 시작으로 수많은 인증기법들이 제안되어 왔다[2]. 이러한 인증기법들은 PKI(Public Key Infrastructure), 생체인식기술, OTP등의 형태로 구분될 수 있다.

2.1.1 공개키 기반구조(PKI)

공개키 기반구조는 기본적으로 공개키 암호시스템을 이용한 정보시스템에서 공개키에 대한 무결성과 신뢰성을 보장하기 위한 기술이다. 공개키 암호알고리즘은 개인키(Private Key)와 공개키(Public Key)라는 키쌍을 구성해서 각 키가 암호화와 복호화에 사용되는 것을 의미한다. PKI를 이용하면 기밀성(Privacy), 접근제어(Access Control), 무결성(Integrity), 인증(Authentication), 그리고 부인봉쇄(Non-repudiation) 서비스를 제공받을 수 있다[3].

2.1.2 생체인식 기술

생체인식 기술은 사람의 생물학적 및 행동학적특징을 이용하여 개인을 인증하는 방식으로 국내외에서 활발히 연구되고 있다. 가장 대표적인 생체인식 기술은 지문, 홍체, 얼굴, 서명 음성인식 등이 있으며, 그 특징은 개인마다

다르다는 생체특징의 고유성과 시간의 흐름에도 크게 변하지 않는 불변성이 기반이 된다[4].

2.1.3 OTP(One Time Password)

OTP는 이중인증방식에 사용되는 기술로 패스워드를 입시마다 새로운 패스워드를 생성하여 사용하는 것이다. OTP는 s/key 방식, 챌린지 리스펀스 방식, 시간 동기화 방식, 이벤트 동기화 방식 등으로 분류되고, 여러 가지 형태를 가지고 있다. 현재 보편화된 OTP 기기는 시간 동기화 방식을 사용하고 있으며, 30초 이내 입력하는 제약을 가지고 있다. 하지만 최초 나온 시간 동기화 방식의 OTP는 30초 이전에 공격대상의 정보를 탈취 시 해킹이 위험이 발견되어 이에 대한 방책을 연구한 논문이 발표되고 있다.

2.2 전송 보안 기술

인터넷의 많은 정보들은 정보보호 관점에서 볼 때 개방성, 공유성의 특징을 가지고 있으므로 근본적으로 몇 가지 문제점을 안고 있다. 그 중 데이터의 내용변경, 불법유출, 순서 변경 등의 위협을 내포하고 있으며, 이를 위한 정보의 안전 전송을 위해 IPSec, SSL/TLS 기술표준들을 개발되었다. IPSec는 인터넷망 계층인 IP(Internet Protocol)계층과 전송 계층 간적용할 수 있는 보안 서비스이며, 어플리케이션 독립적으로 네트워크 보안이 가능하고 호스트간의 통신에도 적용이 가능한 보안 프로토콜이다. SSL/TLS은 전송계층과 응용계층사이에 위치함으로서 다양한 응용계층의 프로그램들과 쉽게 보안설정을 하고, 클라이언트 어플리케이션이 어느 컴퓨터에서도 가능하다[5][6]. 또한 Smart Phone에서 사용되는 대부분의 모바일 웹브라우저(Apple Safari, Google Chrome, Windows Mobile, Polaris, Opera Mobile, Mozilla Fennec등)는 SSL을 채택하고 있고, 이것은 모바일 서버에 SSL 인증서를 설치하여 무선통신상에서 오고가는 개인정보를 암호화하여, 스니핑 시 개인정보 유출을 최소화 할 수 있다.

2.3 USIM 카드

인증 모듈(USIM) 카드는 WCDMA/HSDPA 네트워크상에서 가입자인증을 위한 가입자의 개인정보를 스마트 카드에 저장하는 국제표준 인증방식이다. USIM은 국내에 3G인 WCDMA가 도입되면서 다양한 단말기에서 사용화되었으며, 이동전화 가입자 번호와 이용자 ID, 주소록 등의 데이터 저장이 기본기능으로 사용된다. 또한 WCDMA 서비스에서는 USIM 카드 없이 통화 인증이 불가하며 다양한 서비스(인터넷 뱅킹, 신용카드, 교통카드, 증권 정보조회 등)를 지원할 수 있는 USAT(USIM Application Toolkit) 이라는 기능이 추가되었다.

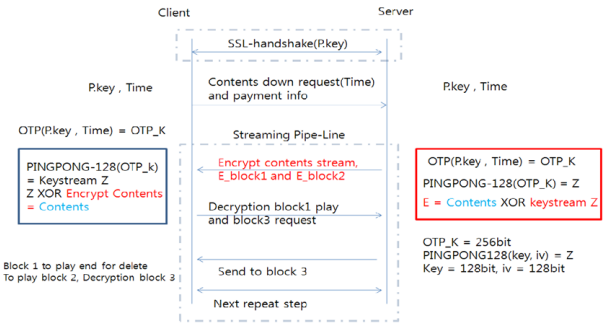
USIM 카드는 스마트 카드의 강력한 보안기능을 바탕으로 분실시에도 개인의 정보가 복제되지 않는 강화된 보안성을 보이는 장점이 있다. 또한, 탈부착이 가능한 형태로 기기변경 시에도 기존에 사용하는 기기에서 USIM 카드를 신규기기에 장착하여 개인정보의 이동을 자유로운 편리성을 제공하여 가용성이 보다 강화되었다[7].

3. 제안된 OTP를 이용한 DRM

2010년 ICCIT에 제안된 “OTP를 이용한 DRM”은 SSL-handshake를 통한 개인키를 공유하고, 컨텐츠에 대한 권한을 가진 사용자가 스트리밍을 서비스를 통한 암호화된 컨텐츠를 전송받아 실행되는 것이다[8].

먼저 공유된 개인키와 사용자가 원하는 컨텐츠 선택시 암호화되어 교환된 Time값이 OTP의 key값으로 사용되어 256bit 사이즈의 OTP를 생성하고, 생성된 OTP를 PINGPONG-128[9]의 초기 벡터와 key 값으로 사용되어 임의의 키스트림을 생성하게 된다. 생성된 키스트림은 컨텐츠와 XOR 연산을 하여 암호화 되고, 특정 사이즈 블록으로 나누어 사용된다.

전송되는 블록은 블록1과 블록2가 먼저 전송이 되어 블록1이 해독 후 실행된다. 실행되는 동안 블록2가 해독이 되면서 블록3이 전송이 되고, 블록1이 종료 되면 삭제 후 블록2가 실행된다. 동일한 과정을 반복하여 컨텐츠를 실행함으로써 복호화된 부분을 최소화하여 컨텐츠 무단 복제 및 사용을 방지한다. 또한 OTP를 이용하여 컨텐츠 암호화에 사용함으로서 재사용 공격에 강함을 알 수 있다. 하지만 제안된 DRM 시스템은 단일 기기에서 사용되어야 하는 제약을 가지고 있다.



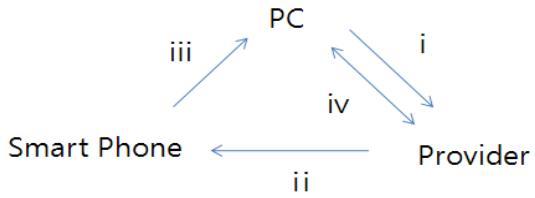
(그림 1) 제안된 DRM 구조

4. 제안하는 DRM 시스템

최근 모바일 기기 사용자들의 관심을 받고 있는 Smart Phone은 운영체제 시스템이 탑재되어 있는 소형 PC로써 다양한 프로그램들이 배포 되고 있다. 디지털 컨텐츠 사업도 이에 발마추어 많은 서비스들이 제공 중에 있으며 서비스 제공은 늘어나는 추세이다. 본 논문은 이중 음원 컨텐츠에 관한 DRM 시스템이다. 단, 본 논문은 USIM카드의 복제 및 복제사용에 관한 보안성은 안전하고 암호화 알고리즘 자체에 대한 공격은 고려하지 않으며, 컨텐츠 Player에 대한 내용은 상세 기술 하지 않는다.

4.1 사용자 등록 과정

Smart Phone에서 디지털 컨텐츠 이용 시 필요한 앱을 다운 받아 사용하려면 서비스를 제공하는 Provider에게 먼저 사용자 등록을 하여 생성하여야 한다. 따라서 제안하는 시스템의 웹서버에 최초 사용자 등록 절차는 그림 2와 같이 시작된다. Provider 웹서버 가입 시 사용인증을 요구하는 단계에서 사용자의 핸드폰 단말기에 임의의 숫자를 문자로 전송하여 사용자 인증을 하는 방법을 사용한다. 이때 사용된 번호는 Smart Phone에서 최초 Application을 실행 시 사용하여 개인키 값을 공유하는데 사용 된다.

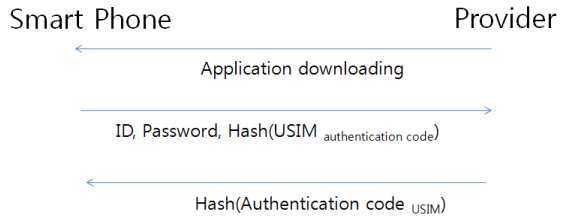


(그림 2) 최초 Provider에 사용자 등록 과정

i. 사용자는 Provider의 웹사이트에 사용자 등록을 하면서 ID, Password를 설정하며, 기타 정보를 입력한다.
ii. 등록 절차의 마지막 단계에서 Mobile을 통한 사용자 인증을 받으며, 임의의 숫자가 문자로 전송된다.
iii. Smart Phone에 전송된 임의의 숫자를 PC를 통한 Provider에 입력을 한다.
iv. Provider는 입력된 숫자를 통한 사용자인증을 하며, 인증된 사용자가 이용 가능한 서비스의 결제단계를 거친다. 단, 본 논문에서는 결제 단계에 대한 상세한 기술은 제외 한다.

4.2 OTP 개인키값 동기화

OTP 개인키값 동기화 단계는 이전 단계에서 사용된 사용자 인증 숫자를 이용하여, OTP 생성을 위한 사용자의 Smart Phone USIM을 Provider와 공유하는 것이다.



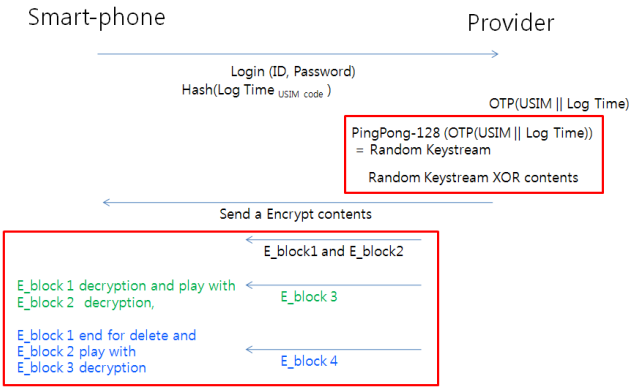
(그림 3) 사용자 USIM 교환 과정

USIM을 공유하는 방법은 그림 3과 같이 Smart Phone에서 음원 컨텐츠 서비스를 이용하기 위한 Application을 전송 받고, 전송 받은 프로그램 실행 시 ID와 Password를 입력한다. 이때 사용되는 ID와 Password는 이전 Provider의 웹사이트 등록 시에 생성된 것을 사용하여 이후 사용될 개인 ID와 Password로 사용한다. 그리고 Smart Phone에서 최소 실행 시 사용자 인증에 사용되었던 임의의 숫자를 입력하게 되며, USIM 값을 암호화 하는데 사용된다.

암호화된 USIM 값은 Provider와 사용자간 공유하여 OTP의 Key값으로 사용되며, 이것은 암호화된 음원 컨텐츠의 복호화에 사용된다. 또한 최초 등록 이후에는 동기화 단계 없이 사용 가능 하며, 다른 Smart Phone에서 등록된 사용자의 USIM을 사용하면 음원 컨텐츠 서비스를 이용할 수 있다.

4.3 제안하는 DRM의 컨텐츠 암복호화

본 논문에서 제안하는 DRM의 컨텐츠 암복호화는 OTP를 내부구조 값으로 생성된 무작위 수열과 음원 컨텐츠의 XOR 연산을 통하여 이루진다. 또한 암복호화 연산에 사용되는 PINGPONG-128 스트림암호의 내부구조 값인 OTP는 사용자 등록 단계에서 전송되는 임의의 숫자와 Provider에 접속되는 LogTime으로 생성된다. 이러한 DRM의 암복호화 과정은 그림 4와 같이 진행된다.



(그림 4) 컨텐츠의 암복호화 과정

LogTime의 동기화는 최초 Application을 통한 Login시 생성되는 Time값을 USIM값으로 암호화하여 Provider에게 전송이 되며, 초기 LogTime은 USIM값과 함께 첫 컨텐츠의 복호화에 사용될 OTP의 생성에 사용된다. 또한, LogTime을 기준으로 2차, 3차 등의 컨텐츠 이용 시에는 LogTime에 음원 컨텐츠의 총 시간(컨텐츠의 시간길이)을 더하여 나온 Time값으로 시간동기화를 시킨다.

무작위 수열은 PINGPONG-128을 통하여 만들어지며, 초기 벡터와 Key값은 OTP 생성기에 만들어진 256bit를 사용한다. 생성된 무작위 수열은 음원 컨텐츠와 XOR 연산을 통하여 암호화 되어서 사용자에게 전송 되며, 컨텐츠의 암호화 및 복호화 역시 XOR 단일 연산을 통한 빠른 속도의 연산을 수행 가능케 한다.

컨텐츠의 암호화는 PINGPONG-128를 통하여 생성된 무작위 수열과 XOR 된 값이므로 복호화 역시 같은 방식

으로 진행된다. 또한 암호화된 컨텐츠는 스트림방식으로 사용자에게 전송이 되며, 전송되는 블록의 사이즈는 컨텐츠 각각 가변적으로 진행한다.

컨텐츠의 복호화는 순서대로 블록_1과 블록_2가 함께 전송이 되어 블록_1이 복호화 되어 플레이가 되고, 이때 블록_2의 복호화와 블록 3의 전송이 시작 된다. 블록_1의 종료에 뒤이어 블록_2가 플레이되고 블록_3의 복호화와 블록_4가 전송된다. 이때 종료된 블록_1은 자동 삭제되며, 블록_4의 데이터가 블록_1의 메모리에 저장된다. 이후 과정은 동일한 패턴으로 반복되어 컨텐츠의 사용이 종료 될 때 까지 진행된다.

5. 보안성 분석

5.1 Replay Attack

재전송 공격은 프로토콜 상에서 유효 메시지를 골라 복사한 후 나중에 재전송함으로써 정당한 사용자로 가장하는 공격으로 DRM 시스템에서는 암호화된 컨텐츠의 전문과 이에 맞는 키쌍을 탈취하여 불법적인 사용에 해당한다. 본 논문에서 제안한 DRM 시스템은 PINGPONG-128을 통하여 선출된 무작위 수열을 사용하여 컨텐츠 복호화하며, PINGPONG-128에 사용되는 키쌍(초기 벡터, Key)은 OTP를 사용하여 각각의 컨텐츠마다 바뀌어지 지게 되어 있다. 또한 같은 컨텐츠의 반복 시에도 Time값이 변화 되어 적용되어 OTP값이 달라지므로 컨텐츠의 불법적인 재사용공격을 막을 수 있다.

5.2 컨텐츠의 불법 복제

컨텐츠 서비스의 핵심은 불법적인 복제 및 사용에 중점을 두고 있으며, 컨텐츠의 불법적인 복제 이후 사용되므로 불법적인 복제를 막는 것이 최우선적이라 할 수 있다.

제안된 논문은 컨텐츠의 불법적인 복제를 막기 위한 방법이 적용되어 있는데, 그 중 첫 번째는 사용자의 USIM 카드를 암호화에 사용한 것으로, USIM 카드는 지금까지 복제 및 사용이 매우 어려워 보안성이 높은 걸로 보고되고 있다. 그리고 두 번째는 컨텐츠의 복호화 과정에서 사용된 컨텐츠의 노출 시기이다. 복호화된 컨텐츠의 크기를 최소화 할 수 있는 구조로 설계되어 있고, 최소화된 컨텐츠의 사용 종료 시 그 정보를 삭제하여 노출 시기를 최소화함으로써 컨텐츠의 불법적인 복제를 매우 어렵게 한다.

6. 결론

최근 IT 기술의 지속적인 발달로 인해 많은 컨텐츠 서비스 사업이 디지털화되어 인터넷 서비스로 제공되고 있으며, 이를 이용하는 사용자의 수도 급증하고 있다. 그리고 최근 이슈화 되고 있는 Smart Phone의 보급률 급격하게 증가하고 있으며, Smart Phone상의 다양한 컨텐츠 서비스가 생성되어 제공되고 있다. 또한, 제공되는 서비스의 양과 질이 향상되어 대다수가 개인정보를 통한 개인 인증을 요구하여 유료 서비스를 이용하게 한다. 이에 본 논문에서는 디지털 콘텐츠의 저작권 보호, 관리, 유통을 위한 기술 체계인 DRM(Digital Rights Management) 기술을 음원 컨텐츠 서비스에 적용하여 제안하였다. 불법적인 복제 공격에 대한 어려움과 Replay Attack에 대한 보안성이 강화될 수 있음을 보여주었으며, DRM 적용된 컨텐츠가 다른 기기에서의 이용이 가능케 하여 사용자의 편의성을 확보 했다. 추후 상세 기술 하지 못한 부분을 추가 연구하고 동기화과정에 대한 다른 방법 및 강화 방법을 연구 할 것이다.

감사의 글

이 논문은 2010년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임 (과제번호: 20100010488)

참고문헌

[1] 최지우, 채종수, 최은화, 서창호, “분산 DRM 시스템 및 알고리즘 설계”, 한국정보기술학회 하계학술대회 논문집, pp.406-409, 2010.5

[2] 심희원, 박준형, 노봉남, “스마트카드를 이용한 향상된 동적 ID기반 원격 사용자 인증 기술”. 한국 인터넷 정보학회, 제10권 제4호, pp.223-230, 2009.2.16

[3] 전정훈, "키 관리시스템의 부하절감을 위한 향상된 키 분배 메커니즘과 보안프로토콜," 한국 컴퓨터정보학위 논문집, 제11권 제6호, pp.35~47, 2007

[4] 박강령, 김재희, “생체 정보 보호 기술”, 한국통신학회, 한국통신학회지(정보와통신), 제24권 제4호, pp. 36~48, 2007.4

[5] 뇌효영, 최정현, “PKI 인증기반 문서보호 시스템 설계”, 한국인터넷정보학회, 한국인터넷정보학회 2010 학술발표대회, pp369-374, 2010.6

[6] 이수정, 이현숙, 정휘석, “SNMP를 이용한 인터넷 장비(Internet Device)의 관리 기법”, 한국정보과학회 학술발표논문집, 제29권 제1호(A), pp.574-576, 2002.4

[7] 김주용, 장재열, 이병관, “USIM카드를 이용한 마스터키 설계”, 한국인터넷정보학회, 한국인터넷정보학회 2009 춘계학술발표대회, pp. 89~93(5pages), 2009.5

[8] Beum-Su Park, Shirly Lee, Hoon-Jae Lee, “On a Digital Right Management System using One Time Password“, ICCIT 2010, vol.2, pp.1032-1035, 2010.11

[9] Hoon-jae Lee, Kevin Chen, “"PingPong-128, A New Stream Cipher for Ubiquitous Application"”, International Conference Convergence Information Technology 2007