새로운 복제방지 기법에 대한 연구

신준범 [0]　　이광형
한국과학기술원 전자전산학과
{jbshin, khlee}@monami.kaist.ac.kr

A Study on the New Copy Protection Mechanism

Jun-Bum Shin [0]　　H. Lee-Kwang
Department of Computer Science, KAIST

요약

정보기술의 발전으로 인하여 각종 소프트웨어 및 여러 종류의 디지털 미디어가 우리 일상생활의 일부를 차지해 가고 있다. 그러나 디지털 형태의 제품은 하드웨어적인 특성에 기반하는 복제 방지 방법을 제공하지 않으므로 새로운 종류의 복제 방지 기법이 요구된다. 본 논문에서는 복제 방지의 범위를 분류하고, 분류된 내용에 기반하여 새로운 종류의 복제방지 기법을 제안한다. 제안하는 방법은 디지털 제품 사용에 있어 사용자 단위와 시스템 단위의 사용 제약을 선택적으로 지원할 수 있다.

1. 서론

정보기술의 발전으로 인하여 각종 소프트웨어 및 여러 종류의 디지털 미디어가 우리 일상생활의 일부를 차지해 가고 있다. 그러나 디지털 형태의 제품은 물리적인 형태를 가지고 있지 않으므로 하드웨어적인 특성에 기반하는 기존의 복제 방지 방법의 적용이 어렵다는 문제점을 가지고 있었다. 따라서 현재 많은 종류의 불법 복제된 디지털 제품이 유통되고 있으며 이러한 문제로 인하여 향후 정보기술의 발전의 저해요소가 될 수 있다는 문제로까지 확산될 수 있다. 따라서 이러한 문제에 대한 해결방안이 요구된다.

현재까지 여러 종류의 디지털 제품 보호를 위한 여러 종류의 법적 장치들이 마련되어 왔다. 그러나 디지털 제품의 유통은 인터넷과 같이 다수의 사용자들이 익명으로 참여할 수 있으므로 이러한 접근 방법만으로는 문제를 근본적으로 해결하는 것은 어렵다. 따라서 보다 기술적인 접근 방법이 요구된다. 기술적 측면에서 볼 때, 디지털 제품 보호는 크게 다음의 두가지 측면으로 나누어 생각할 수 있다. 하나는 복제방지(Copy Protection) 기법으로 정당한 사용자만이 제품을 사용할 수 있도록 하는 것을 의미한다. 하드웨어적인 보호 수단 및 암호를 이용하는 기법들이 주로 사용된다. 다른 하나는 저작권 보호(Copyright Protection) 기법으로 디지털 제품에 대한 원 소유자가 누구인지를 확인시킬 수 있는 방법이다. 이 분야에서 많이 사용되는 기법으로는 디지털 워터마크가 있다. 이 방법은 디지털 데이터에 워터마크를 추가한 방법으로 타인이 그 데이터를 복제하여 사용한다고 하더라도 원 제작자를 확인할 수 있다.

본 논문에서는 여러 종류의 디지털 제품 보호 기법 중에서 1차적으로 적용 가능한 기술인 복제방지 기술을 다룬다. 본 논문의 순서는 다음과 같다. 2장에서는 관련연구를 소개한다. 3장에서는 암호와 관련된 기본 개념을 소개하고, 4장에서는 제안하는 복제방지 기법을 소개한다. 그리고 5장에서 결론을 맺는다.

2. 관련 연구

이 장에서는 현재까지 제안되어온 복제방지 기술들에 대해서 소개한다. 본 논문에서는 기본 복제방지 기법과 복제방지 기법이 적용되는 시간에 따라서 분류한다[1].

2.1. 기존 복제방지 기술

이 절에서 기술하는 내용은 [2] 논문에서 인용하는 것이며 [2] 논문의 내용을 추가한 것이다. 자세한 논문은 원 논문을 참고바란다.

- 설치 시 접근 암호를 이용하는 방법
- 하드웨어적인 키락을 사용하는 방법
- 특정 플로피 디스켓을 제시해야 하는 방법
- 비밀키가 저장된 별도의 스마트카드를 이용하는 방법
- 시스템 ID 정보를 이용하여 특정 시스템용 제품을 제작하여 공급하는 방법
- 설치 시 네트웍으로 온라인 등록하는 방법
- 공개키 인증서를 이용하여 개인키의 소유자만이 사용할 수 있도록 하는 방법

2.2. 복제방지기술 적용 시점

복제방지 기술을 적용하기 위해서는 사용자가 디지털 제품을 사용할 권한이 있는지를 검사해야 한다. 이러한 특면에서 볼 때, 다음의 2가지로 구분할 수 있다.

- 최초사용시(설치시)에만 검사

- 사용할때마다 검사

최초 사용시에만 검사하는 것은 우리가 프로그램 설치 과정에서 경험하는 것처럼 사용자가 어느정도의 불편을 감수할 수 있다고 가정할 수 있다. 그러나 사용할때마다 검사하도록 구성되어 있다면 사용자의 불편 정도는 매우 중요한 설계 관점이다. 2.1절에서 언급한 방식들은 처음것을 제외하고는 모두 사용할 때마다 검사하는 방법이다. 실제적인 측면에서 볼 때, 모든 방식에 대해서 사용자와 관계없이 자동적으로 검사를 수행하도록 설계할 수는 있다. 그러나 보안성 측면을 고려할 때, 이러한 방법의 접근은 바람직하지 않다. 대부분의 보안제품이 그러하듯 편이성의 증진은 보안성의 감소를 의미하기 때문이다. 일예로 [2] 에서 제안된 방식의 경우, 사용자는 사용할 때마다 자신의 개인키를 이용하여 검증을 수행해야 하는데 이러한 방식의 경우, 실제적으로 사용자가 자신의 개인키를 외우는 것은 불가능하므로 별도의 스마트카드를 이용하게 된다. 그러나 이 경우, 사용자 설정 부분에서 특정 시점 이후에 이 검사방식을 생략할 수 있는 옵션을 제공한다면 원하는 보안성을 얻을 수 없다. 또 다른 문제점은 모든 매체가 스마트카드 리더를 포함하고 있지는 않다는 점이다. 일예로 현재 PC의 경우에는 스마트카드 리더를 부착하여 사용하는 것이 가능하다고 하더라도, MP3 플레이어의 경우를 보면 크기상의 제약 때문에 이러한 방식의 접근이 어렵게 된다. 또한 사용자별로 한번에 두개 이상의 시스템을 동시에 사용할 수 없다는 제약 조건을 갖는다.

2.3. 라이센스 범위

앞에서 언급한 바와 같이 복제방지 기술을 적용하는 과정에서 중요한 고려요소는 라이센스의 범위를 파악하는 것이다. 현재 사용되는 방법을 보면 다음의 두가지로 구분할 수 있다.

- 하드웨어 기반(머신 기반) : 허가된 머신에서만 사용 가능
- 사용자 기반 : 허가된 사용자만이 사용 가능

위의 두가지 요소는 기술적으로 현재까지는 어느 방향으로 설계할지가 명시되어 있지는 않다. 일예로 하드웨어 구입시에 번들로 나오는 소프트웨어의 경우 하드웨어 기반 및 사용자 기반 라이센스가 현재 동시에 사용되고 있기 때문이다. 따라서 실제 시스템 설계 과정에서는 이러한 두가지 방법을 동시에 지원할 수 있는 통합적인 복제방지 기술의 개발이 필요하다.

3. 암호 기술

암호 기술은 소프트웨어 적인 특성을 가지고 있으므로 현재 많은 종류의 응용 분야에서 데이터 보호 기술로 각광을 받고 있다. 이 장에서는 암호 알고리즘과 보안 프로토콜에 대한 기본적인 내용과 용어를 정의한다. 자세한 내용은 [3]를 참고바란다.

3.1. 암호 알고리즘

- 난수 : 랜덤하게 생성된 수를 말한다. 암호에서 사용하는 난수는 대부분의 경우 160 bits 이상의 길이를 가지고 있으므로 생성될때마다 유일하다고 가정한다. 우리는 사용자 A에 의해서 생성된 난수를 N_A로 표시한다.
- 비밀키 암호 함수 : 암호화 키와 복호화 키가 같은 암호 함수이다. 키가 K라 할 경우, 비밀키 암호 함수를 이용하여 메시지 M을 암호화 한 것을 우리는 SKE(K, M)으로 표시한다.
- 공개키 암호 함수 : 암호화 키와 복호화 키가 다른 함수이다. 사용되는 키는 공개키와 개인키 두가지가 있으며 공개키 암호 함수는 비밀키 암호 함수와는 다르게 공개키를 상대방에게 공개할 수 있다는 장점을 갖는다. 우리는 A의 공개키로 메시지 M을 암호화 한 것을 PKE(A, M)으로 표기한다.
- 암호학적 해쉬함수 : 해쉬 함수는 함수값의 길이가 고정된 함수이다. 암호학적 해쉬함수는 결과값이 난수적 특성을 가지고 있는 해쉬함수로서 단방향 성질과 충돌 회피성을 지원한다. 우리는 앞으로 암호학적 해쉬함수를 해쉬함수로 표기하며, 해쉬함수로 메시지 M을 해쉬한 값을 H(M)으로 표기한다.

3.2. 보안 프로토콜

여러 종류의 프로토콜 중에서 암호 함수를 사용하는 프로토콜을 보안 프로토콜이라 한다. 보안 프로토콜을 객체 사이에 메시지를 주고 받는 과정으로서 이루어 진다. 이 때, A가 B에게 메시지 M을 보내는 것을 우리는 다음과 같이 표기한다.

$$A \rightarrow B : M$$

보안 프로토콜이 주로 이용되는 분야는 사용자 인증 또는 암호키 교환 프로토콜이다. 자세한 내용은 생략한다.

4. 제안하는 복제 방지기법

본 논문에서 제안하는 복제방지 기법은 라이센스 차원에서 하드웨어 기반 방식과 사용자 기반 방식을 모두 지원할 수 있도록 설계되었다. 본 논문에서는 지면상의 제약으로 인하여 하드웨어 기반 방식을 지원하는 방법 위주로 설명하고, 이 장의 뒷부분에서 사용자 기반 방식을 지원할 수 있도록 시스템을 확장하는 방법을 언급한다.

4.1. 디지털 제품 형태

디지털 제품은 여러 형태를 갖을 수 있다. 또한 이들을 보호하는 방법 역시 여러가지가 있을 수 있다. 강한 개념으로는 제품 자체를 암호화 하는 방법이 있고, 약한 방법으로는 제품 사용에 대한 인증만을 수행하는 방법이 있다. 그리고 본 논문에서는 제품을 사용하는 과정에서 특정 인증번호가 있어야만 사용할 수 있다고 가정한다. 이같은 가정은 위에서 언급한 강한 방법과 약한 방법에 모두 적용 가능하다. 구체적인 구현방법은 여러가지가 있을 수 있으나 지면상의 제약으로 생략한다.

4.2. 시스템 모형

제안하는 복제방지 메커니즘(Copy Protection Mechanism, 이하 CPM)은 인증코드에 기반하여 디지털 제품에 대한 사용권한을 얻는 방법을 이용한다. 제안하는 CPM은 크게 CPM-P와 CPM-H로 구분할 수 있다. CPM-P는 인증코드를 얻어오는 보안 프로토콜이며, CPM-H는 디지털 제품의 실제 동작을 담당하는 하드웨어 부분이다.

제안하는 CPM에 참여하는 객체는 크게 다음과 같이 구분할 수 있다.

- TTP : 믿을 수 있는 제 3자(trusted third party)로 믿을 수 있도록 제품 구매를 할 수 있도록 도와주는 자 역할을 수행한다.
- User : 제품을 사용하는 사용자이다. 모든 사용자는 TTP와 키를 공유하고 있다고 가정한다. 우리는 사용자 A의 키를 K_A라 한다.
- Vendor : 디지털 제품을 판매하는 자이다. Vendor는 디지털 제품 생산업자로부터 제품을 가져다가 사용자에게 판매하는 역할을 담당한다. Vendor는 K_{vendor} 를 TTP와 공유하고 있다.
- CPM-H : 사용자가 가지고 있는 하드웨어이다. CPM-H는 고유한 키(K_{CPMH})를 가지고 있으며, 추가적인 보안요소를 만족할 수 있도록 설계되었다고 가정한다. 자세한 내용은 뒤에 언급한다.

4.3. CPM-P

사용자 A가 Vendor로부터 제품번호가 ID_{code}인 디지털 제품에 대해서 인증번호를 얻어오는 과정은 다음과 같다.

1. A $\rightarrow$ Vendor : ID_{code}, N_A, $PKE(TTP, ID_A, K_{CPMH}, PaymentInfo, Time)$
2. Vendor $\rightarrow$ TTP : ID_{code}, N_A, $PKE(TTP, ID_A, K_{CPMH}, PaymentInfo), N_{Vendor}$
3. TTP $\rightarrow$ Vendor : $SKE(K_{vendor})(H(K_{CPMH}, N_A, N_{vendor}), N_A, N_{vendor}, K_{new}, SKE(K_A)(K_{new}, N_A, ID_{code}, N_{vendor}))$
4. Vendor $\rightarrow$ A : $SKE(K_A)(K_{new}, N_A, ID_{code}, N_{vendor}))$, $SKE(K_{new})(K_{IDcode} \oplus H(K_{CPMH}, N_A, N_{vendor}), N_A, N_{vendor}, ID_{code})$

프로토콜이 끝난 후, 사용자는 Vendor로부터 다음의 인증번호를 얻게 된다.

$$ID_{code}, N_A, N_{vendor}, K_{IDcode} \oplus H(K_{CPMH}, N_A, N_{vendor})$$

즉, 인증번호는 code의 ID와 CPM-P 실행과정에서 A와 Vendor가 생성한 난수, 그리고 코드의 키가 CPM-H의 키와 A와 Vendor가 생성한 난수를 이용하여 해쉬된 값을 이용하여 비트단위 XOR 을 취한 값으로 구성되어 있다. 사용자는 코드의 수행을 위해 코드 및 이 인증번호를 CPM-H에 입력한다.

4.4. CPM-H

CPM-H는 CPU, memory, 그리고, CPM-H, 3가지 부분으로 구성되어 있다. CPM-H가 동작하는 방법은 다음과 같다. 우선 CPM-H가 code와 인증번호를 입력값으로 받았다고 가정한다.

1. code의 ID를 얻는다(ID'_{code})
2. ID'_{code}가 인증번호에 있는 입력값과 같은지를 검사한다.
3. 인증번호에 있는 값들과, K_{CPMH}를 이용하여 $H(K_{CPMH}, N_A, N_{vendor})$를 계산한다.
4. 인증번호로부터 K_{IDcode} 값을 얻는다.

이 과정이 끝난후, CPM-H는 K_{IDcode}를 이용하여 code를 이용할 수 있다.

4.5. 확장 방법

지금까지 제안한 방법은 하드웨어 단위로 디지털 제품의 사용을 제안하는 방법이다. 위의 방법은 구매단계에서 여러개의 하드웨어에 대한 사용 권한을 얻을 수 있다는 장점을 갖는다.

제안한 방법은 사용자 단위 복제방지에도 적용이 가능하다. 전체적인 구성 방법은 원 프로토콜과 동일하다. 다른 내용만 적으면 다음과 같다.

- CPM-P 수행 과정에서 사용자 단위 라이센스를 발급할 것인지 하드웨어 단위 라이센스를 발급할 것인지를 선택하는 hasdshake 과정을 추가한다.
- CPM-P의 내용 변화는 K_{CPMH}를 사용자의 공개키 인증서로 변환한다.
- 인증번호에서 $K_{IDcode} \oplus H(K_{CPMH}, N_A, N_{vendor})$를 사용자의 공개키를 이용하여 K_{IDcode}를 암호화 하는 것으로 변환한다.($PKE(A, K_{IDcode})$)
- CPM-H에서 K_{IDcode}를 얻는 방법은 사용자의 개인키를 이용하여 복호화 하는 것으로 바꾼다.

5. 결론 및 향후과제

본 논문에서는 디지털 제품 복제방지를 위하여 여러종류의 라이센스를 제공할 수 있는 방법을 제안하였다.

향후 과제로는 제안된 방법의 안전성 분석 및 효율성 향상을 위하여 프로토콜을 최적화 하는 방법에 대한 연구가 요구된다.

Ack: 본 연구는 첨단정보기술 연구센터를 통하여 과학재단의 지원을 받았음.

REFERENCES

1. *P. Wayner,* Digital Copyright Protection). *Academic Press, 1997.*
2. 이병천, 임신영, 김광조, "공개키 기반 구조를 이용한 소프트웨어의 저작권보호," 한국통신정보보호학회 *1998*년학술대회, *'98.12.18-19,* 인터콘티넨탈 호텔, 서울, *1998.*
3. *A. J. Menezex, P. C. Oorschot, and S. A. Vanstone,* Handbook of Applied Cryptography. *CRC Press, 1997.*