학원 교육 콘텐츠 S/W 저작권 보호를 위한 알고리즘 구현

강민재· 편도길 · 정상호 · 정회경

배재대학교 컴퓨터 공학과

Implementation of Security Algorithm to Preserve Copyright of Education Contents

Min-Jae Kang · Do-Kil Pyoun · Sang-Ho Cheong · Hoe-Kyung Jung

Dept. of Computer Engineering, Paichai University

E-mail : {kmj5228, dokil25, tophojs, hkjung}@mail.pcu.ac.kr

요 약

최근 교육 콘텐츠 개발이 활발한 가운데, 콘텐츠를 소비하는 소프트웨어(Software)의 저작권을 보호할 수 있는 방법이 다양하게 연구되고 있다. 따라서 본 연구는 이더넷(Ethernet)의 맥 주소(MAC Address)와 하드디스크 볼륨 시리얼 넘버(Hard Disk Volume Serial Number)를 통해서 소프트웨어의 저작권을 보호하기 위한 방안을 고찰, 구현 하였다.

본 연구를 통해 간단하지만 강력한 저작권 보호를 위한 알고리즘을 구현하여, 학원 교육 콘텐츠 소프트웨어의 저작권 보호를 강화하고, 불법적 소프트웨어 사용으로 인한 피해를 감소하는데 기여할 것이다.

ABSTRACT

As development of education contents has become more active, it is not much that way to preserve copyright of S/W consuming contents. So this paper studied way to preserve copyright of S/W from MAC address of ethernet and hard disk volume serial number. This study realizes the simple but powerful security algorithm to preserve copyright. So this tightens to preserve copyright of S/W of education contents and will contributes to decrease damages because of using illegal S/W.

키워드

Ethernet MAC Address, Hard Disk Volume Serial Number, MD5

Ⅰ. 서 론

온·오프라인을 통한 불법적 소프트웨어 공유를 통해, 라이센스를 취득하지 않고 사용하는 사용자들이, 과거에서 현재까지 지속적으로 증가 하였다. 하지만, 이러한 불법적 소프트웨어 공유를 통해 라이센스를 취득하지 않고 사용하는 것을 예방하기 위한 보안 알고리즘이 미흡하였다. 이로 인해, 소프트웨어 개발자들의 노력이 헛수고가 되는 경우가 많았고, 결과적으로 가격이 비싸지는 악순환을 야기했다. 기존의 시리얼 키(Serial Key) 또는 ID(Identification)를 통한 라이센스 획득 방법은 시리얼 키와 ID를 여러 사용자가 공유하여 사용함으로써, 소프트웨어의 저작권을 보호하기란 쉽지 않았다. 그래서 전술한 방안을 보완하여 나온 것이 동글(Dongle)[1]이다. 동글은 컴퓨터의 입출력 접속 구에 연결되는 장치로 특정 프로그램의 복사와 실행을 할 때 인가된 사용자만이 사용할 수 있도록 보안 키나 ID를 저장한 장치이다. 이 보안 알고리즘은 사용자가 컴퓨터의 입출력 접속 구에 연결되는 장치를 수령받기 전에는 소프트웨어를 사용할 수 없다는 단점이 있다.

이러한 상황에서 본 연구는 학원이라는 특수성을 이용하여 컴퓨터의 유일한 식별자인 이더넷의 맥 주소와 하드디스크 볼륨 시리얼 넘버를 통해서 소프트웨어의 라이센스 획득을 판별한다.

본 논문의 구성은 다음과 같다. 2장에서는 본 논문의 관련 연구를 기술하고, 3장에서는 학원이라

는 특수성을 어떻게 이용하여 저작권 보호 알고리즘을 구현하였는지 기술한다. 4장에서는 저작권 보호를 위한 보안 알고리즘과 이를 통해 구현된 결과를 기술한다. 결론 및 향후 연구 과제는 5장에서 기술한다.

Ⅱ. 관련 연구

2.1 학원 교육 콘텐츠 소프트웨어[2]

예전에는 학원 등과 같은 교육환경에서 문제 출제를 할 때 직접 찾아서 자필 또는 타이핑 하여 문제 출제를 하였다. 하지만, 최근 여러 학원 교육 콘텐츠 소프트웨어(그림1)가 출시되어, 직접 문제를 출제 하는 일이 감소하였다.

그림 1. 학원 교육 콘텐츠 소프트웨어

학원 교육 콘텐츠 소프트웨어의 기능을 보자면 대표적으로 자동 문제 출제 시스템(그림2)이다. 이 기능을 이용하여 문제 출제자는 보다 쉽고 편하게 문제를 출제·수정 할 수 있다.

그림 2. 자동 문제 출제 시스템

2.2 동글[3]

동글은 컴퓨터에 연결하는 작은 크기의 하드웨어로[4] USB 플래시 드라이브와 같이 휴대할 수 있다. 전자적으로 인증용 동글은 대개가 다른 동글 기능을 간섭하지 않는 일시적인 데이터 전송 기능이 있다. 동글이 없으면 소프트웨어는 제한된 모드에서만 실행되거나 아예 실행조차 하지 못한다. 하지만 동글은 하드웨어를 수령 받기 전에는 사용 하지 못한다는 단점이 존재하고, 매번 하드웨어를 컴퓨터에 직접 장치 시켜야 된다는 번거로움이 존재한다.

Ⅲ. 학원의 특수성

학원의 특수성이라 함은 여러 명의 사용자가 하나의 로컬 통신망에 집중되어 있는 경우라 할 수 있다. 이러한 경우 사용자들은 하나의 ID를 이용하여 여러 명이 접속하여 사용하거나, 하나의 시리얼 키 값으로 여러 클라이언트(Client)가 사용할 수 있다. 그래서 본 연구에서는 클라이언트 이더넷의 맥 주소와 하드디스크 볼륨 시리얼 넘버를 이용하여 사용자의 라이센스 획득 여부를 판별한다.

3.1 이더넷의 맥 주소

모든 컴퓨터의 유일한 식별자인 맥 주소는 변경이 가능한 소프트웨어가 존재 하여 맥 주소를 사용자 임의로 변경이 가능하므로 저작권 보호를 위한 식별자로 부적합하다. 하지만 학원의 경우는 그림 3과 같은 통신망으로 이루어져, 여러 명의 사용자가 하나의 로컬 통신망에 연결이 되어 있다. 이와 같은 상황에서는 같은 로컬 통신망 내에 동일한 맥 주소가 존재 하게 되면 통신이 불가능하게 된다.

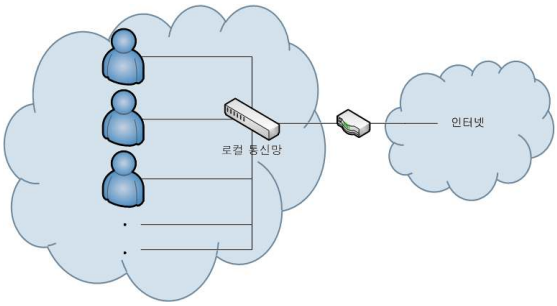

그림 3. 학원의 통신망

Ⅳ. 저작권 보호를 위한 알고리즘

본 연구에서 저작권 보호를 위한 알고리즘 구현은 그림4와 같은 절차를 통해서 진행된다. 클라이언트 측에서는 보안 키 값 생성기(Generator)를 통해서 맥 주소와 하드디스크 볼륨 시리얼 넘버를 추출하여 특별한 접두사를 부여한 후에, MD5 암호화 [5]알고리즘을 적용하여 암호화된 키 값을 서버(Server)측의 라이센스 판별기로 전송한다. 서버 측에서는 클라이언트 측에서 받은 보안 키 값을 데이터베이스(Database)에 있는 키 값과 비교를 해서 라이센스 획득을 판별한다.

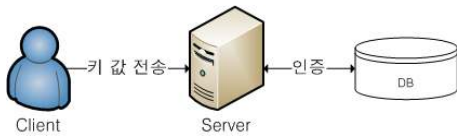

그림 4. 알고리즘 절차

4.1 키 값 전송

그림 5와 같은 클라이언트 측의 보안 키 값 전송 프로그램을 구현하여, 저작권 보호를 위한 알고리즘을 논리적으로 검증 하였다.

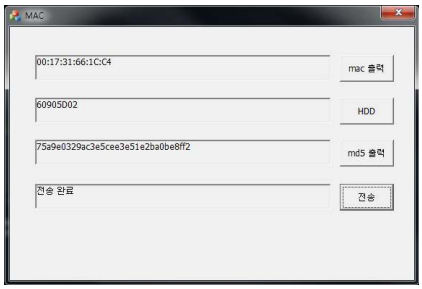

그림 5. 보안 키 값 생성기

이 프로그램은 설명의 편의상 맥 주소와 하드디스크 볼륨 시리얼 넘버가 보이지만, 실제 릴리즈(Release) 되는 프로그램은 이 두 식별자로 키 값을 만들어 전송 한다는 사실이 보여선 안 된다. 그림 5에서 보이듯 보안 키 값 생성기는 사용자 컴퓨터의 맥 주소와 하드디스크 볼륨 시리얼 넘버를 추출하고, 접두사로 사용자의 아이디를 붙인 후에 MD5 암호화 알고리즘을 적용시켜 서버 측의 라이센스 판별기로 전송한다. 전송하는 키 값은 MD5(USER_ID+MAC_ADDRESS+HARD_DISK_VOLUME_SERIAL_NUMBER)이다. MD5는 Hash함수로 구현 되어 있고, 특수한 값들로 조합되어 있기 때문에 유추가 불가능하다.

컴퓨터의 맥 주소를 추출 하는 방법은 다양한데 그 중 본 연구에서 쓰인 방법은, ARP (Address Resolution Protocol)[6]를 이용한 방법이다. ARP는 네트워크상에서 IP주소를 물리적 네트워크 주소로 대응시키기 위해 사용되는 프로토콜이다. 여기서 물리적 네트워크 주소는 이더넷 또는 토큰링의 48비트 네트워크 카드 주소를 뜻한다.

4.2 라이센스 획득 판별기

클라이언트에서 보낸 키 값을 서버가 받아서 판별 하는 판별기는 그림 6와 같다.

그림 6. 라이센스 판별기

라이센스 판별기는 클라이언트 측에서 보내온 키 값을 라이센스 등록할 때 저장해 놓았던 DB 테이블(표1)을 참조 하여 라이센스 획득을 판별한다.

표 1. DB 테이블

ID	KEY	Reg_date	Rsv1	Rsv2
kmj5228	75a9e0...	11-03-16		
banth	e86f25...	11-03-16		
kks	d6a5a4...	11-03-16		
sora	31785d...	11-03-16		
...	...	...		

그림5, 그림6과 같은 두 테스트 프로그램을 만들어 논리적인 검증을 하고, 결과적으로 강력한 학원 교육 콘텐츠 소프트웨어 저작권 보호 알고리즘을 구현 하였다.

Ⅴ. 결 론 및 향후 연구 과제

소프트웨어의 저작권을 보호하기 위해 ID인증, 시리얼 키 인증, 동글과 같은 방법들이 있다. 본 논문에서는 맥 주소와 하드디스크 볼륨 시리얼 넘버를 이용하여 저작권 보호를 위한 알고리즘을 제안하고 있다. 이 방법은 간단하지만 강력하다. 그 이유로는 맥 주소의 경우에는 동일한 로컬 네트워크상에서 같은 맥 주소가 존재 할 시 통신이 불가능하다. 그래서 학원과 같은 특수한 환경에서는 맥 주소 변경 소프트웨어를 통해서 변경, 사용할 수가 없다.

향후 연구 과제로는 한 대의 클라이언트에서 여러 사용자가 사용하는 경우 저작권 보호가 쉽지 않다. 그래서 과목 구분과 초/중/고와 같은 교과과정을 보안 키 값에 적용 시키면 한 대의 클라이언트에서 여러 사용자가 사용하는 경우를 기본적으로 예방 할 수 있다.

참고문헌

[1] naver, http://terms.naver.com/item.nhn?dirId=204&docId=4170
[2] Finetect Co., http://www.widewise.co.kr/index.a sp
[3] TeckTerms, http://www.techterms.com/definition/dongle
[4] MicroComputer Printout Vol 2:19
[5] wikipedia, http://ko.wikipedia.org/wiki/MD 5
[6] RFC826, http://www.ietf.org/rfc/rfc826.txt