

소프트웨어 산업의 발전을 위한 확장된 소프트웨어 인증체계

서희석* · 김상호* · 이승재**

For the development of software industry, extensive software certification scheme

Seo, Hee Suk · Kim, Sang Ho · Lee, Seung Jae

〈Abstract〉

For the development of software industry, offers an expanded software authentication scheme caused by the unauthorized copying of software is to reduce the damage to software developers, retail sales and to promote the development of the software industry was studied. Serial Number of the current software registration is conducted in such a simple verification procedure if the Serial Number only illegal and can be installed on multiple computers, such as program code to allow third parties to enter the Serial Number, or the extract can be used without is a reality. The proposed extension to the software authentication system when you install the software, my phone authentication and MAC Address Authentication Service introduced to distinguish normal user, the user of the MAC Address of the server and software development company that was sent to the registered MAC Address of the computer to be run only by the use of genuine software and to make unauthorized copies of software generated by the software developer can reduce the damage of the proposed plan.

Key Words : MAC Address, Phone authenticate themselves, Install

I. 서론

오늘날과 같은 디지털시대에는 과거와 달리 서류 기타 종이에 기록하던 대부분의 데이터를 디지털화하여 컴퓨터파일로 보관하게 되고, 이러한 데이터를 다른 사람과 주고받는 경우에도 과거처럼 디스켓에 담아 전달하는 것이 아니라 이메일 또는 FTP 전송에 의하여 간단히 주고받을 수 있다. 그런데 이렇게 편리한 시대에 살고 있는

만큼 그 부작용도 심각하다. 예컨대 애써 만든 데이터나 파일 또는 프로그램의 집합체인 대용량의 소프트웨어마저도 사이버공간에서는 다운로드를 통하여 간단히 복제가 가능하기 때문에 이를 노리는 비양심적 네티즌들에 의하여 사이버공간은 순식간에 불법복제 소프트웨어 천지로 변해가고 있다. 최근 국내에도 소프트웨어 저작권자들이 많아지고 정부의 단속이 강도 높게 행해지면서 국내의 소프트웨어 불법 복제율이 과거에 비하여 상당히 감소되었다는 통계가 여러 곳에서 나오고 있기는 하지만 여전히 마음만 먹으면 사이버공간 어딘가에서 필요

* 한국기술교육대학교 컴퓨터공학부(제1저자)

** 한국기술교육대학교 건축공학부(교신저자)

한 소프트웨어를 구할 수 있는 것이 아직까지의 현실이다. 이처럼 불법 SW의 공유가 쉬운 이유로는 소프트웨어의 설치 시에 필요한 모든 데이터가 CD에 담겨 있어 데이터의 복사가 간단하고 CD없이 실행 불가능한 소프트웨어도 가상이미지장치를 통해 가용이 가능하도록 할 수 있고, 또한 Serial Number를 필요로 하는 프로그램도 프로그램코드 역분석 등을 통해서 사용이 가능하기 때문이다. 이는 국내 소프트웨어 시장의 발전에 큰 악영향을 끼치며, 이로 인해 기업에서 소프트웨어 개발자들의 수요가 감소함에 따라 일자리의 감소로 이어 지게 되어, 청년 실업률에도 악영향을 끼치고 있다. 이러한 이유로 소프트웨어 사용 희망자들은 비싼 돈을 주고 정품 소프트웨어를 구매하여 사용하기 보다는, 불법 소프트웨어를 구해서 사용하는 사용자들의 비율이 상대적으로 많이 생기게 되었다[1].

본 논문은 소프트웨어 불법복제로 인한 피해를 보다 효과적으로 방지하기 위한 대안 책으로 정품 소프트웨어 설치 시, 휴대폰 본인인증 서비스와 MAC Address를 통하여 정상적인 사용자와 PC를 판별 하여 불법 소프트웨어의 설치 및 실행을 방지하고, 소프트웨어 라이선스의 구매 기간별 가격 책정과, 모바일 결제를 통해서 소프트웨어 사용자에게 좀 더 효과적이고 간편한 소프트웨어 구매를 할 수 있도록 하여 국내 소프트웨어 산업의 발전을 지금 보다 더 증진 시킬 수 있도록 확장된 소프트웨어 인증체계를 제안 하였다.

II. 관련 연구

2.1 소프트웨어 불법복제의 개념과 유형

소프트웨어 불법복제란 “저작권자의 명백한 동의 없이 불법적으로 소프트웨어의 내용을 복사한 것”을 말하며, 소프트웨어의 단순 복사, 하드디스크 저장, 대여, 위조, 온라인 유통 등의 유형을 모두 포함한다. 현행 컴퓨

터프로그램보호법은 정당한 권한 없이 다른 사람의 프로그램저작권을 복제, 개작, 번역, 배포, 발행 및 전송의 방법으로 침해해서는 안 되며, 이를 위반하는 자는 형사 처벌하도록 규정하고 있다. 흔히 허용되는 것으로 착각하기 쉬운 불법복제의 사례를 들면, 친구로부터 정품 CD를 빌려 내 컴퓨터에 프로그램을 설치한 경우, PC구입 시 판매처에서 서비스 차원에서 라이선스 없는 윈도우를 무상으로 설치한 경우, 인터넷 또는 PC통신을 이용하여 정품 소프트웨어를 다운받아 설치한 경우, 두 대의 컴퓨터를 보유하고 있는 자가 정품 한글 CD 1장을 구입하여 두 대의 컴퓨터에 설치한 경우, A학교에서 구입한 프로그램을 B학교에서 구입한 프로그램과 교환하여 사용한 경우 등이 모두 불법복제에 해당한다. <표 1> 은 소프트웨어 불법 복제의 유형을 정리하여 나타내었다.

<표 1> 소프트웨어 불법 복제의 유형[2]

1. 사용자 단순 복사	조직 또는 회사에서 일하는 사람이 사무실이나 집에서 사용하기 위해 개인적으로 불법 복제하는 것을 말한다. 라이선스 된 소프트웨어 한 카피(copy)를 구입한 다음, 라이선스 약정서의 조건을 위반하여 여러 대의 기계에 복제하는 행위
2. 하드디스크 탑재	PC 판매상등이 불법 복제된 소프트웨어 복사본이 실린(내장된) 컴퓨터를 판매하는 행위
3. 대여	소프트웨어의 대여는 1994년 컴퓨터 프로그램보호법 개정에 의해 원칙적으로 국내에서 법으로 금지
4. 위조	정품 소프트웨어와 똑같이 복제되어 판매되는 것을 말한다. 이것은 매뉴얼의 포장에서부터 등록카드, 디스크 레이블 등에까지 거의 완벽한 위조가 이루어지는 것으로, 또 다른 형태로는 복제 본을 정품 소프트웨어와는 전혀 다른 이름으로 바꾸어 판매하는 행위
5. 인터넷을 통한 불법복제	상용 소프트웨어를 누구나 복제할 수 있도록 온라인게시판, 또는 인터넷에 올리는 행위를 말하며 혹은 그러한 서비스를 통해 상용 소프트웨어를 복제하는 행위

2.2 소프트웨어 불법복제의 실태와 심각성

BSA(Business Software Alliance, 사무용소프트웨어연합회) 보고서에 따르면 전 세계의 2002년도 소프트웨어

불법복제율은 39%이고 매년 감소 경향을 보이고는 있지만 여전히 세계 소프트웨어 산업을 어렵게 만드는 가장 큰 원인이 되고 있다. 지역적으로 서유럽, 북미, 중동·아프리카, 라틴아메리카 지역은 모두 불법복제율이 감소하고 있는 추세이나 동유럽의 불법복제율은 상당히 높은 편이며, 아시아·태평양의 불법복제율은 1996년 이래 최고 수준인데 이는 중국의 92%라는 높은 불법복제율이 그 원인이다.

한국의 2002년도 불법복제율은 50%로 1994년도의 75%에서 꾸준히 감소해오고 있으나 2001년도의 48%보다는 다소 높게 나타났다. 이는 미국(23%), 캐나다(39%), 독일(32%), 일본(35%) 등 선진국과는 상당한 격차가 있는 반면, 같은 아시아지역 내의 홍콩(56%), 중국(92%) 보다는 낮은 수치이다. 2001년도에는 한국(48%)이 싱가포르(51%), 대만(53%) 등보다 복제율이 낮았으나 2002년도에는 싱가포르(48%), 대만(43%)보다 한국(50%)이 더 높아졌다는 사실은 경계를 요하는 부분이다. <표 2>는 2009년 기준으로 작성된 OECD가입 국가의 소프트웨어 불법복제 현황을 나타내었다.

<표 2> OECD 국가 소프트웨어 불법복제율[3]

순위	나라	불법복제율
1	United States	20 %
2	Japan	21 %
3	Luxembourg	21 %
4	New Zealand	22 %
5	Australia	25 %
6	Austria	25 %
7	Belgium	25 %
8	Finland	25 %
9	Sweden	25 %
28	South Korea	41 %
29	Spain	42 %
30	Slovakia	43 %

조사한 통계를 보면 국내의 불법복제율은 41%보다 약간 더 높게 나타나고 있으며 이는 기업과 기관의 불법복

제율만을 계산하였을 때의 수치이고, 개인의 불법복제율(75%)을 반영하면 전체 불법복제율은 60%에 이르는 것으로 나타났다.

개인의 경우 4명중 3명은 불법복제 소프트웨어를 이용하고 있다는 뜻이 된다. 이처럼 많이 이용되고 있는 불법 복제 소프트웨어는 친구나 동료로부터 얻는 경우가 50%를 넘고, 컴퓨터를 구입할 때 미리 설치하는 경우가 20%, 인터넷을 이용하여 얻는 경우가 10% 정도로 나타나고 있지만, 최근에는 접근이 손쉬운 인터넷을 통한 불법복제(다운로드)가 급격히 늘고 있는 추세여서 그 심각성을 더해가고 있다. 인터넷을 통한 불법복제경로는 이른바 와레즈(Warez) 사이트에서 다운로드하는 경우(30%)와 소리바다 등 P2P 방식의 다운로드(30%)가 중심을 이루고 있고, 기타 팝폴더, 웹하드, PD박스 등 개인정보 저장 공간을 이용하거나 FTP에 의한 전송 등에 의해서도 불법복제가 많이 행해지고 있다[2, 3].

2.3 소프트웨어 불법복제에 대한 법적 책임

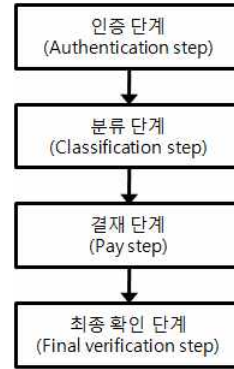
소프트웨어, 즉 컴퓨터프로그램은 저작권법의 특별법인 컴퓨터프로그램보호법에 의하여 보호되는 저작물이다. 컴퓨터프로그램보호법상 소프트웨어제작자는 프로그램을 스스로 복제, 개작, 번역, 배포, 발송 및 전송할 배타적 권리를 가지며, 타인에게 이러한 권리를 허락할 수 있는 대역 권과 이를 금지할 수 있는 권리를 가진다. 그러나 컴퓨터프로그램은 여전히 저작권법상으로도 보호되는 저작물의 하나로 규정되어 있으므로 컴퓨터프로그램보호법에 규정이 없는 사항에 대하여는 저작권법이 적용된다. 타인의 저작물인 소프트웨어를 복제하여 사용하는 것은 민법상 불법행위에 의한 저작재산권침해에 해당하므로 그 손해배상책임이 인정된다. 그리고 컴퓨터프로그램보호법이 규정하는 저작권보호규정을 위반한 경우에는 3년 이하의 징역 또는 5천만 원 이하의 벌금이라는 중한 형사 처분을 받게 된다. 다만, 재판을 위하여 필요한 경우, 교육기관에서의 수업목적을 위한 경우, 시험을

목적으로 하는 경우 등에는 복제가 허용되며, 또한 정당한 소지자가 멸실·훼손 등에 대비하기 위하여 복제를 하는 것도 가능하다. 종래 인터넷서비스제공자(ISP)라고 흔히 지칭해오던 용어에 대하여 컴퓨터프로그램보호법과 저작권법은 좀더 넓은 범위의 온라인서비스제공자(OSP)라는 용어를 사용하고 있는데, 이러한 OSP에게 불법복제 소프트웨어의 유통에 대한 공동불법행위책임을 묻는 것은 OSP의 활동영역의 제한을 가져와 결과적으로 사이버공간의 발달을 저해하게 된다는 우려도 있으나, 불법복제 소프트웨어의 유통을 방지할 수 있는 실질적 감독권한을 갖고 있는 자는 OSP뿐이므로 그에게 침해저작물의 존재를 인식하거나 인식하였어야 하는 경우에 그 공동불법행위의 책임을 묻는 것은 타당하다고 보아야 한다. 이러한 OSP의 책임은 불법복제 소프트웨어의 경우 뿐 아니라 명예 훼손성 게시물에 의한 명예훼손에 대한 책임 등의 경우에도 해당된다. 미국의 디지털밀레니엄저작권법(DMCA)이나 우리 저작권법은 OSP의 저작권침해에 대한 직접적 규정 대신 OSP의 책임한정조항, 즉 면책조항만을 둬으로써 그 규정된 책임의 내용은 여전히 명확하지 않지만, 판례에 의하여 그 불법행위책임을 점차 넓혀가고 있는 추세이다.

현행법상 재판절차를 위하여 필요한 경우이거나 입법·행정의 목적을 위한 내부 자료로서 필요한 경우 저작권법에 위법이 되고(저작권법 제23조)[4], 저작물을 영리를 목적으로 하지 아니하고 개인적으로 이용하거나 가정 및 이에 준하는 한정된 범위 안에서 이용하는 경우에도 위법행위가 된다(저작권법 제30조)[4]. 그러므로 하나의 정품 소프트웨어를 자신 소유의 두 대 이상의 PC에 설치하는 것과, 친구나 심지어 가족에게까지 빌려주는 행위도 위법 행위이다.

III. 확장된 소프트웨어 인증체계

본 논문에 제안된 확장된 소프트웨어 인증체계는 크



<그림 1> 인증절차

게 <그림 1>과 같이 4가지의 단계로 구성된다. 첫 번째 인증 단계는 사용자와 사용자가 사용하는 컴퓨터를 휴대폰 본인 인증 서비스와 네트워크 인터페이스 카드의 MAC Address를 이용하여 인증 하는 단계 이다. 두 번째 분류 단계는 첫 번째에서 인증 받은 결과를 토대로 정상 고객, 비 구매 고객, 재설치 고객으로 구분하는 단계이다. 세 번째 결제단계는 두 번째에서 분류된 비 구매 고객에게 모바일 결제를 이용하여 결제를 유도하는 단계이다. 마지막으로 네 번째 최종 확인 단계는 앞의 단계의 흐름으로 설치가 완료된 소프트웨어의 실행에 앞서 최종적으로 소프트웨어 인증 여부를 판별하는 단계이다.

3.1 확장 소프트웨어 인증체계 전체구성

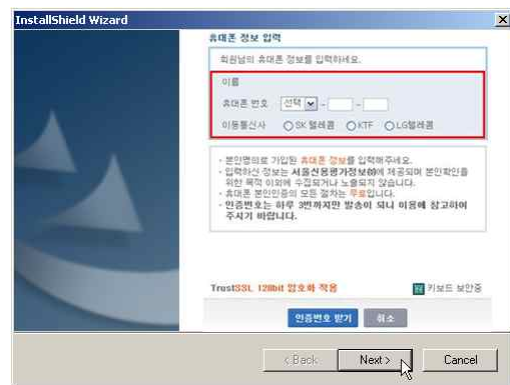
다양한 복제·프로그램코드 역분석 등의 기술이 인터넷을 통해 빠른 속도로 전해지고 이를 무분별하게 사용하는 시점에서 현재의 소프트웨어 정품 인증 체계는 소프트웨어 개발 기업에게 상당한 피해를 야기 시킨다. 본 논문에서 제안하는 확장된 설치체계는 소프트웨어 설치시 사용자의 휴대폰 본인인증을 거치고 사용할 PC의 MAC Address와 본인인증 정보를 해당 소프트웨어 회사의 DB와 비교한 뒤 각 조건 별로 진행이 되도록 한다. 정상적인 구매자가 단순 재설치를 하려는 경우는 바로 설치가 진행 되도록 하고, 비 구매 고객이 새로 프로그램



을 설치할 경우 모바일 결제 페이지로 넘어 가게 하고, 다른 컴퓨터에 재설치 하려는 경우 네트워크 인터페이스 카드도 교체 하였다면 해당 소프트웨어 회사의 DB에 바뀐 컴퓨터에 장착된 네트워크 인터페이스 카드의 MAC Address 정보를 서버로 입력 받아서 갱신한 뒤에 정상적인 설치가 가능 하도록 한다. 이때의 결제는 프로그램 라이선스를 기간제한 사용 혹은 영구사용으로 나누어 결제가 가능하도록 한다. 이렇게 설치가 완료 된 후에 프로그램을 실행할 때 최종적으로 설치 과정에서 서버의 DB에 저장된 MAC Address와 현재 프로그램을 실행한 PC의 MAC Address를 비교하여 정상적인 MAC Address를 비교한 뒤 같다면 정상적으로 실행이 되도록 하지만, 비교결과가 다르면 같은 사용자가 여러 PC에 저장해 두고 사용하는 경우이거나, 불법적인 경로로 설치를 한 경우이기 때문에, 라이선스 추가 결제를 하도록 유도 하여 <표 1>의 1번, 2번 3번, 5번 항목의 위험을 최소한으로 줄일 수 있다. 영구적인 라이선스를 구매 하여, 정상적으로 설치가 완료되면 차후 사용하는 PC의 랜카드를 변경하거나 다른 PC에 설치하여 사용 하는 경우가 아니면 설

치된 PC에서 해당 소프트웨어를 영구적 인증 상태로 사용할 수 있다. 이러한 시스템은 무단 복제, Serial Number 유출 및, 생성기 등을 이용하여 자유롭게 소프트웨어를 공유하는 것을 차단 할 수 있어 국내 소프트웨어 기업의 피해를 줄일 수 있다.

3.2 인증 단계



<그림 3> InstallShield에 포함된 본인 인증

<그림 2>은 인증 단계의 흐름 구상도를 나타낸다. 현재 사용되어 지고 있는 휴대폰 본인인증 서비스에 MAC Address인증을 결합한 방법이다. 인증방식은 <그림 3>에서 보이는 것과 같이 설치 과정중의 단계로 포함 한다. 기존 휴대폰 번호 및 주민등록번호와 이동통신사의 가입 정보를 이용하는 신뢰성 높은 인증방법에 해당 소프트웨어의 DB에 저장된 회원의 MAC Address주소를 비교 하는 과정을 추가 하였다. 고객이 주민등록번호 및 휴대폰 번호와 통신사를 선택하여, 인증을 요청하면 이동통신사는 등록되어있는 휴대폰 가입정보와 대조하여 일치하는 경우 인증번호 SMS를 등록된 휴대폰 번호로 전송을 하게 되고, 전송된 인증번호를 소프트웨어 사용자가 입력 창에 넣고 인증을 받는 과정에서 현재 프로그램을 설치 하고 있는 PC의 MAC Address를 획득 하여 해당 소프트웨어의 회사로 보낸다[5, 6]. 여기서 MAC Address를

획득 하는 과정으로 단순히 ARP(Address Resolution Protocol)를 사용 할 수 있는데 ARP는 단지 NIC 수준에서 같은 네트워크상에서 호스트 혹은 라우터의 MAC Address를 알아내기 위한 제한적인 프로토콜이며, 이것을 사용하는 것은 MAC Address를 알아내기 위해 다시 ARP 브로드캐스트를 수행하기 때문에 효율성 면에서 떨어지므로, 여기에선 클라이언트 컴퓨터에서 직접 MAC Address를 획득 하여 이를 패킷으로 전송한다. <표 3>은 클라이언트 컴퓨터에서 직접 MAC Address를 획득하는 세 가지 방법의 함수를 나타낸다.

```

DWORD dwBufLen = sizeof(AdapterInfo);
DWORD dwStatus = GetAdaptersInfo(
    AdapterInfo,
    &dwBufLen);
assert(dwStatus == ERROR_SUCCESS);
PIP_ADAPTER_INFO pAdapterInfo = AdapterInfo;
do {
    PrintMACAddress(pAdapterInfo->Address);
    pAdapterInfo = pAdapterInfo->Next;
}
while(pAdapterInfo);
    
```

3.3 분류 단계

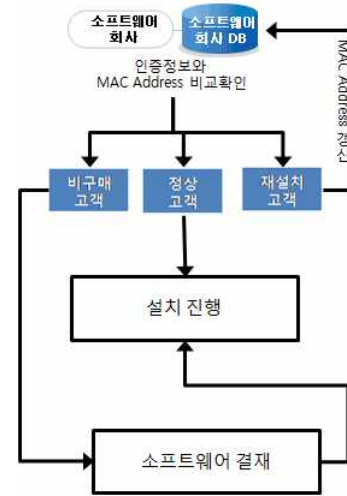
<표 3> Three ways to get your MAC address[6]

```

static void GetMACAddress(void){
    unsigned char MACData[6];
    UUID uuid;
    UuidCreateSequential( &uuid );
    for (int i=2; i<8; i++)
        MACData[i - 2] = uuid.Data4[i];
    PrintMACAddress(MACData);
}

static void GetMACAddress(void){
    unsigned char MACData[8];
    WKSTA_TRANSPORT_INFO_0 *pwkti;
    DWORD dwEntriesRead;
    DWORD dwTotalEntries;
    BYTE *pbBuffer;
    NET_API_STATUS dwStatus = NetWkstaTransportEnum(
        NULL, 0, &pbBuffer, MAX_PREFERRED_LENGTH,
        &dwEntriesRead, &dwTotalEntries, NULL);
    assert(dwStatus == NERR_Success);
    pwkti = (WKSTA_TRANSPORT_INFO_0 *)pbBuffer;
    for(DWORD i=1; i< dwEntriesRead; i++) {
        wsscanf((wchar_t *)pwkti[i].wkti0_transport_address,
            L"%2hx%2hx%2hx%2hx%2hx%2hx",
                &MACData[0],
                &MACData[1],
                &MACData[2],
                &MACData[3],
                &MACData[4],
                &MACData[5]);
        PrintMACAddress(MACData);
    }
    dwStatus = NetApiBufferFree(pbBuffer);
    assert(dwStatus == NERR_Success);
}

static void GetMACAddress(void){
    IP_ADAPTER_INFO AdapterInfo[16];
    
```



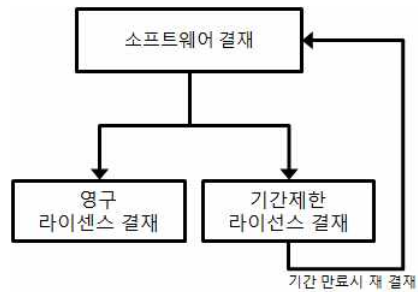
<그림 4> 분류 단계

<그림 4>는 분류 단계의 흐름 구상도를 나타낸다. 본 논문은 인터넷에 접속 할 수 있도록 네트워크 인터페이스 카드가 장착 되어 있는 PC에 설치하는 프로그램을 대상으로 설정 하였으며, 정품 소프트웨어가 설치되는 PC는 설치과정의 휴대폰 본인인증단계 이후 인증번호 입력이 처리되는 과정에서 네트워크 인터페이스 카드의 MAC Address 정보가 해당 소프트웨어 회사의 DB로 전송되어 진다. MAC Address는 통신을 위한 네트워크 인터페이스 카드의 고유한 식별 번호이다. 이 MAC Address주소는 <그림 5>의 방법으로 자신의 고유의

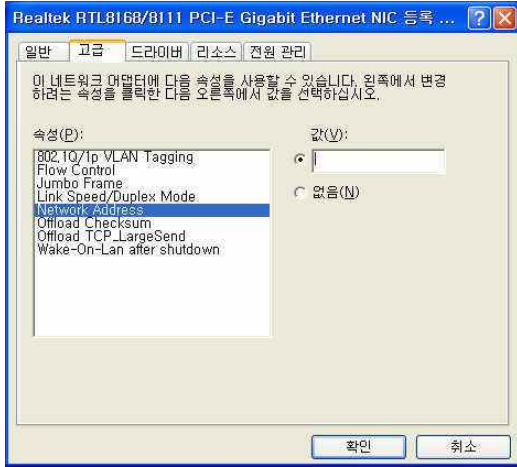
MAC Address 대신 임의의 MAC Address 또한 사용 가능하다. 물론 MAC Address는 지구상에서 유일해야 하기 때문에, 누군가가 그 맥주소를 가지고 있다면 MAC Address 충돌이 발생해서 인터넷을 사용하지 못할 수도 있지만, <그림 6>에서 보는 바와 같이 해당소프트웨어의 DB에 저장되어지는 MAC Address의 값은 유일하고, 본인 인증 정보와 함께 MAC Address를 쌍으로 저장하게 함으로써 설치 과정의 본인인증 단계와 MAC Address 비교 단계에서 이로 인한 피해를 방지 할 수 있다. 인증 단계에서 획득한 MAC Address와 본인 인증 정보를 바탕으로, 해당 소프트웨어 회사의 DB에 저장된 값과 비교를 통해 사용자를 분류하여 각 조건에 해당되는 실행을 하도록 한다. 우선 해당 소프트웨어 회사의 DB에 사용자 정보와 MAC Address 모두 등록이 되어 있지 않을 경우에는 미 구매 고객으로 분류되어 바로 모바일 결제 창으로 넘어가게 되어, 소프트웨어를 구매하여야만 정상적인

설치를 진행 할 수 있고, 사용자 정보와 MAC Address가 해당 소프트웨어 회사의 DB 정보와 일치하는 경우, 정상 고객으로 분류되어 바로 설치가 가능하다. 또한 사용자 정보는 있지만 MAC Address가 다른 경우에는 재 설치 고객으로 분류되어, 새로운 MAC Address로 해당 소프트웨어 회사의 DB가 갱신되어지게 되고, 설치가 계속 진행이 가능하게 된다[7].

3.4 결제 단계



<그림 7> 결제 단계



<그림 5> MAC Address 변경

[인증 정보 Table]

*고객명	*MAC Address	라이선스 기간	...	프로그램 이름
------	--------------	---------	-----	---------

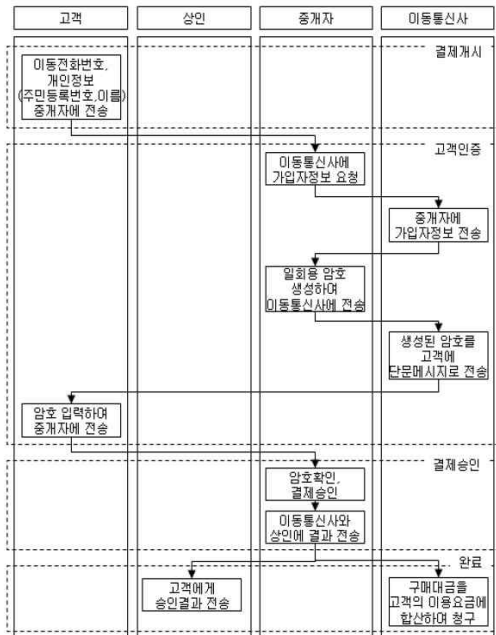
고객명, MAC Address -> 라이선스 기간, ..., 프로그램 이름

<그림 6> 서버 내 DB의 인증정보 Table의 예시

<그림 7>은 결제 단계의 흐름 구상도를 나타낸다. SMS를 이용한 이동통신 통합 과금 방법으로 결제가 이루어지며, 영구 라이선스를 구입 할 경우 차후 사용하는 PC의 랜카드를 변경 하거나 다른 PC에 설치하여 사용하는 경우가 아니면 설치된 PC에서 해당 소프트웨어를 영구적 인증 상태로 사용할 수 있고, 기간제한 라이선스를 구매하였을 경우에도, 결제한 기간 동안에는 별다른 제한 사항 없이 사용이 가능하다. 본 논문은 간편하고 언제 어디서나 가능하며, 즉시 결제가 가능한 휴대폰 소액 결제에 초점을 두었다. 소액결제라고는 하나 최대 20만원까지 결제가 가능하므로 소프트웨어 결제수단으로는 적합하다. 모바일 결제의 흐름은 <그림 8>에 자세히 나타내었다. 암호화는 모빌리언스 사의 MCash를 기준으로, 결제완료시점까지 2차레에 걸쳐 고객을 확인하므로 도용을 원천적으로 방지할 수 있으며 세계적 보안업체인 Verisign에서 보증한 128bit SSL암호화 자료는 방화벽과

침입탐지 시스템을 탑재하여 가장 안전한 결제 환경을 갖추고 있다. 소프트웨어를 구매 할 경우 사용자의 필요에 따라서 크게 영구 라이선스 사용과 기간제한 라이선스로 나누고, 기간 별로 가격 차이를 두어 사용자의 소프트웨어 가격에 대한 부담을 줄일 수 있다. 어떤 필요에 의해서 일회성으로 사용되어야 할 소프트웨어가 있다고 가정할 때, 비싼 가격을 모두 주고 정품 소프트웨어를 구매하기에는 소비자의 부담이 크기 때문에, 부담을 줄일 수 있는 방법으로 기간제한 라이선스를 제안 하였다.

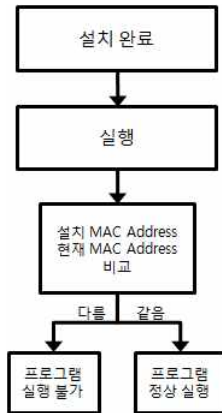
MAC Address를 암호화 하여 저장 해 두고, 설치 완료 후에 프로그램을 실행 할 때 마다 암호화하여 저장한 MAC Address를 비교하여 같으면 프로그램이 정상적으로 실행이 되고, 같지 않을 경우에 실행을 할 수 없도록 하였다. 그러므로 비정상적인 절차로 프로그램을 설치한 사용자는 실행이 불가능 하고, 네트워크 인터페이스 카드를 교체한 사람은 프로그램을 삭제 후, 재설치를 통해 MAC Address를 갱신 하여야 한다. <그림 9> 에 최종 확인 절차 흐름 구상도를 표현하였다.



<그림 8> SMS를 이용한 이동통신 통합 과금 방법[7]

3.5 최종 확인 단계

소프트웨어가 PC에서 실행이 될 경우 정상적인 결제와 설치가 이루어졌을 경우에는 아무 이상 없이 소프트웨어가 구동하여야 한다. 하지만 비정상적이거나, 네트워크 인터페이스 카드가 고장으로 인해 교체하였을 경우를 대비한 방법으로 정상적으로 설치가 진행 될 때 상태의



<그림 9> 최종 확인 단계

IV. 결론

본 논문의 소프트웨어 산업의 발전을 위한 확장된 소프트웨어 인증체계 제안은 정품 소프트웨어를 설치할 때 일반적으로 본인 확인에 사용되는 휴대폰 본인인증 서비스와 통신에 필요한 네트워크 인터페이스 카드의 고유한 MAC Address를 결합한 인증방식으로, 소프트웨어를 설치 할 때 휴대폰 본인인증 서비스를 통해, 고객을 확인 하고, 커널에서 MAC Address를 획득하여 고객을 구분 받고, 필요시 바로 결제를 하며, 최종적으로 실행 할 때마다 설치시의 MAC Address 와 현재 PC의 MAC Address 를 판별하여 정상적인 실행을 할 수 있도록 한다.

확장된 소프트웨어 인증체계는 프로그램의 불법 복제 및 부정사용을 보다 효과적으로 방지하고 사용자에게 올바른 정품 소프트웨어의 사용을 유도하게 함으로써 소프트웨어 개발업계에 불법복제, 양도, 대여 등으로 개발에 투자한 비용을 회수하지 못하는 근본적인 문제점을 해소하고 소프트웨어 개발 의욕을 크게 증진시켜 양질의 소프트웨어 개발이 지속될 수 있을 뿐만 아니라 국내 소프트웨어 시장의 성장을 촉진 시킬 수 있고, 이로 하여금 극심한 취업난이 조금이나마 해소 될 수 있을 것으로 기대 된다.

참고문헌

- [1] 김정완, "소프트웨어 불법복제와 저작권보호," 인터넷법률신문, 연구논단, 제 3220호, 2003. 11.
- [2] 권동혁, 이병관, "정품 소프트웨어 불법 복제 방지를 위한 응용소프트웨어 웹 설치 서비스 설계," 한국인터넷정보학회 학술발표대회논문집, 제9권, 제2호, 2008, pp. 137-138.
- [3] John Gantz, "Seventh Annual Global Software Piracy Study", BSA, 2010, p. 9
- [4] 국회, 저작권법, 제18차 (타)일부개정 법률 제9785호, 2009. 7.
- [5] 김우경, "SMS와 일회용 패스워드에 기반한 사용자 인증시스템 설계 및 구현," 부경대학교, 공학석사 학위논문, 2005, p. 17.
- [6] Khalid Shaikh, "Three ways to get your MAC address," Network Information. April 15, 2002, <http://www.codeguru.com/Cpp/I-N/network/networkinformation/article.php/c5451>
- [7] 한국전산원, "모바일 결제 표준 모형 연구," 정보통신연구진흥원 학술기사, NCA IV. RER-0 4015, 2004. 12, p. 112.

■ 저자소개 ■



서희석
Seo, Hee Suk

2005~현재 한국기술교육대학교
컴퓨터공학부 조교수
2005 성균관대학교 전기전자 및
컴퓨터공학과 박사
2005 (주)정보감리평가원 선임연구원
2002 성균관대학교 전기전자 및
컴퓨터공학과 석사
2000 성균관대학교 산업공학과 학사
관심분야 : 네트워크 보안, 보안 시뮬레이션,
악성코드분석
E-mail : histone@kut.ac.kr



김상호
Kim, Sang Ho

2005년 3월~현재
한국기술교육대학교 컴퓨터공학부
(학사)
관심분야 : 네트워크 보안, 보안 시뮬레이션
E-mail : idimida@kut.ac.kr



이승재
Lee, Seung Jae

2003년~현재 한국기술교육대학교 교수
1998년 동경대학교 전임강사
1998년 동경대학교 공학박사
1995년 동경대학교 공학석사
관심분야 : 건축구조해석
E-mail : histone@kut.ac.kr

논문접수일 : 2010년 5월 18일
수정일 :
게재확정일 : 2010년 6월 3일