INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN 2278 – 0211 (Online)

Inhibition to Software Piracy Using Challenging Response Protocol

Surendra Mahajan
Professor, Department of Computer Science and Information Technology
Pune Vidyarthi Grihas College of Engineering, Pune University, India
Hemant Choudhari
Student, B.E. Information Technology
Pune Vidyarthi Grihas College of Engineering, Pune University, India
Sonali Kolte
Student, B.E. Information Technology
Pune Vidyarthi Grihas College of Engineering, Pune University, India
Pratik Chothe
Student, B.E. Information Technology
Pune Vidyarthi Grihas College of Engineering, Pune University, India

Abstract:
In todays IT World main approach of software developer is to prevent the software piracy. Lots of implementations are done to prevent software piracy. So, many ideas are suggested to stop it. In this paper we are presenting an approach, which based on SMS Gateway System. The server initiates the authentication process and identifies the genuine copy software on client machine. In brief we are implementing a general key distribution system, which provides the maximum inhibition to software piracy. In which server starts the process by sending the authentication challenge to client then client will response to the challenge and server will verify the response. After getting expected reply from client, server will send status message to client according to that client machine will decides what should be done next. After getting proper output from client side server send either success or failure status. At the end software installation process starts or software uninstallation process starts.

1. Introduction

Developing specific software usually takes a lot of efforts and investment. Illegal creation of software and circulation of any software are come under the issue of software piracy. The consequences tend towards ruining the software piracy.

The roots of software piracy are coming from 1960s when computer programs were freely distributed with mainframe hardware manufactures.

The main objective is to support antipiracy. The software piracy is one type of threat, which proves disadvantages in protecting the intellectual property rights. Whenever someone bought software, the software publisher delivers software and its associated license to the customer. A complete usage policy and license agreement is clearly mentioned in software license documents. In other words, the customer is actually purchasing license to use that software. Breaking those terms and policies specified in license, some people redistribute this software by creating copies of it and remove any licenses associated with that respective software, resulting in software piracy [3, 4]. This pirated software is similar to the original software except for its license. Using pirated software without a license is against law. The piracy can thus define itself as being any situation of malpractice of intellectual property rights (copyright).

2. Existring System

Piracy rate can be calculated as:

Unlicensed s/w units are calculated by subtracting the total numbers of S/W legally acquired during the year from total no of pc s/w was deployed during the year.

Piracy rate = Unlicensed S/W unit by Total s/w unit Installed.

There are several types of software piracy classified by their importance degree in five big categories:

2.1. Industrial Imitation

This type of piracy is often made under the shape of a software reproduction, which is engraved on CD - ROM, and supplies with documentation and a license, identical to legal software. They are afterward sold on Internet on sites as eBay4.

2.2. Software Piracy via Internet

The development of the Internet, by reducing the cost of distribution of the numeric goods, allowed the emergence of platforms of exchanges between individuals. According to a study made by the IDC (2008), the number of individual in the world having access to Internet amounts at present to 1.2 billion persons and this number increased in one year about 135 millions among which 100 millions in emerging countries (or emerging market). Certain platforms became fast the place of exchanges, on which users share works protected by the intellectual property right (essentially video, music and software) by violating the lawmaking on the copyright.

2.3. Software Piracy by the users

The Piracy by the users is particularly made by small and medium firms and by private individuals, who reproduces software copies without authorization in purposes of personal or commercial usage. According to a study IDC published by BSA in May 2007, 45 % of the software installed on microcomputers in France in 2006 lacked license. This piracy can take on the following forms:

- Abuse of license: install a program under license on several computers.
- Change copies of software under license.
- Acquire software for a usage different from that planned by the license.
- Copy software with the aim of an installation or of a distribution.
- Benefit from update offers without having a previous legal copy.

2.4. Piracy by the sellers of hardware

It is the case of certain retailers of hardware who install a not authorized copy of commercial software on a computer system. The most known is "Hard Disk Loading" which is an illegal copy of a software on the hard disk of computers and which the hardware seller can charge in the global cost price of the material. The user pays then pirated software which he does not possess an original copy and documentation.

2.5. Misuse of the customer-server

This type of piracy occurs when a company has a local area network (LAN), used simultaneously by several employees.
If the company decides to install programs on the server, she has to make sure that the license authorizes it and that the number of users is not superior to that authorized by the license, without which it is in situation of misappropriate. [6] Software companies are facing huge losses due to software piracy, which instigates them to develop technical measures to prevent piracy. The main idea behind the efforts to stop piracy is to implement an identifier or token which can be either software based license key, serial number, license file or hardware based components like Dongle, smartcard, CD etc. There are situations where even the link between software and identifier can be weak or strong. Companies mainly concentrate on activating and authenticating user, using these identifiers and giving full access to software. Although many measures are taken to prevent illegitimate user to access software.

2.6. Loss

The value of pirated software worldwide rose 14 percent to $58.8 billion last year, almost double the total in 2003, among rising theft of programs in emerging markets, according to a trade group that tracks piracy. Countries with emerging economies, including China, Russia, India and Brazil, now account for more than half of the money lost to piracy, according to the Business Software Alliance, a Washington group that is releasing its annual piracy report today. The U.S. topped all other countries with $9.52 billion lost to piracy, with China second at $7.78 billion.

3. Issues in Software Piracy Inhibition

3.1. MAC Address

MAC address means media access control address is an address of any network interface for communication. MAC address generally stored in Ethernet adapter in its hardware. These days all the Ethernet ports are on motherboard and the MAC address also stored on the motherboard of a computer. MAC address is always unique throughout world and can work as IMEI address of mobile set. We can trace any computer using this address. With IP address we can search the location and with MAC address we can know the exact computer. MAC address of any machine depends on its NIC card. If a machine is having two or more NIC cards then it will not have unique MAC address. Suppose a machine having a LAN card and a wireless card then for each NIC it has a unique MAC address and it will be effective accordingly [6]. So if any user installs the software second time on that machine using different NIC card then it will show an error message, and that is not adequate for client machine. Mac is a computers unique address. It is a 12-digit hexadecimal numbers. The first half contains ID number of the adapter manufacturer and the second half contains serial number assigned to the adapter by the manufacturer. It is a hardware address that uniquely identifies each node of a network. When you're connected to the Internet from your computer IP address and computer's physical (MAC) address are recorded. All network adapter manufacturers have their own code, called the Organizationally Unique Identifier (OUI).

MAC addresses are usually written in one of the following two formats:
MM: MM: MM:SS: SS: SS
MM-MM-MM-SS-SS-SS
The example,
00:A0:C9: 14:C8: 29
The prefix 00A0C9
Indicates the manufacturer is Intel Corporation.
00-14-22-01-23-45, the first three octets are 00-14-22.This is the OUI for Dell. Other common OUIs include 00-04-DC for Nortel, 00-40-96 for Cisco and 00-30-BD for Belkin. If you enable MAC address filtering; only the devices with MAC addresses configured in the wireless router or access point will be allowed to connect. It is possible to spoof the MAC address, so an attacker could potentially capture details about a MAC address from your network and pretend to be that device to connect to your network

3.2. Time Offset
The time in UTC clock system varies from location to location and so does the date. In targeted approach, XOR of date and MAC address is send to the server and in response server sends XOR of unique id and server date to the client. Date on client and server side may vary due to different time offset on different geometric locations. When- ever server tries to retrieve the MAC address (by XORing the received digest and current local server date) it may misinterpret and will get wrong MAC address for that machine. [1] In another case when server sends the digest of unique code and current date then user machine may also misinterpret the unique code and whenever client enter the unique code in installing process, the process will terminate with an error message that the unique code is not correct and a genuine user will not get the services he required.

3.3. Man in the Middle Attack (MiTM)
An attack where a user gets between the sender and receiver of information and sniffs any information being sent. In this the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. All cryptographic systems that are secure against MITM attacks require an additional exchange or transmission of information over some kind of secure channel. Many key agreement methods have been developed, with different security requirements for the *secure* channel.
In this approach, no one focus on data security in transmission mode. A third person can easily capture all the data packets and can easily get the unique code without actually buying the product Initially, whenever the client send the XOR of the current date and MAC of its machine, the middle person simply captures the packet and can retrieve the MAC of that machine by XORing the current date with the captured data and save it for future at- tack. Now whenever the server sends the packet with the product (XOR of unique id and current date), the middle man can also capture the packet and can retrieve the unique code by simply XORing the current date with the captured data. The middleman has the unique id (only necessary item to run the software) without actually paying for it.

4. Proposed System
In this paper, we are suggesting a smart approach in order to overcome from the problem of software piracy
We are providing Inhibition to Software Piracy through SMS Gateway and make it more Stable and effective against piracy.
The refined approach is, the will initiate authentication process from server side instead of client and at regular time intervals.
“Inhibition to Software Piracy through SMS Gateway” is used to communicate with the authentication server by user system.

- Server Initiates the authentication process and identify the genuine software copy
- Server starts the process by sending authentication challenges to client.
- Server will verify the client response

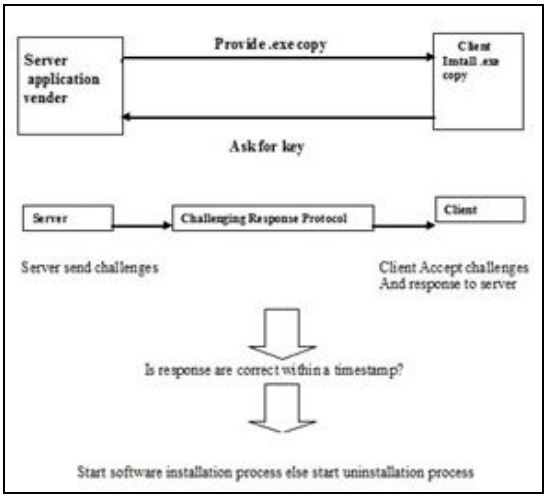

Figure 1: Proposed System Depiction

Software activation key must be protected from MiTM attack by using some encryption/decryption algorithm. Since Asymmetric key cryptographic algorithm is most popular and suited for an open multi user. We are going to use RSA algorithm Asymmetric algorithm. In RSA two different keys are used for protection purpose. The encryption key is public and differs from the decryption key, which is kept secret.

TTL to handle Time offset we use Time to Live (TTL) we are assign some time for that particular software. Actual software installation should be in between that time offset if TTL time expires then s/w installation would fail.

In proposed technique, at the time of purchasing software, authentication server maintains FN, LN, Address and a mobile number MN association. Server starts the process by sending periodic challenge to each of its client on registered mobile number by sending server time stamp Ts encrypted by private key of server SKr which provides

Integrity for authenticated user. Server saves all user information in database for further authentication. Then server waits for response from client. Client receives challenge compare received H {Ts} with D (SKu, E (SKr, H (Ts))) or decrypted hash of server timestamp with public key of server i.e. SKu. Client again fills user information at this time user has to enter key send by server. Server tallies information at database. At this timeserver get MAC address of user machine. After that Server send actual activation key of software by SMS gateway. If client will not receive challenge at fix period or received hash is not equal to calculated hash i.e. challenge is tempered, software Uninstallation process starts.

5. Algorithm

Server Side

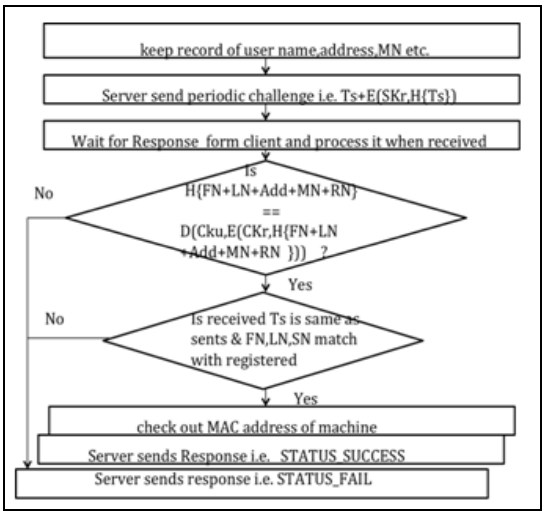

Figure 2: Client Side Algorithm

Client Side

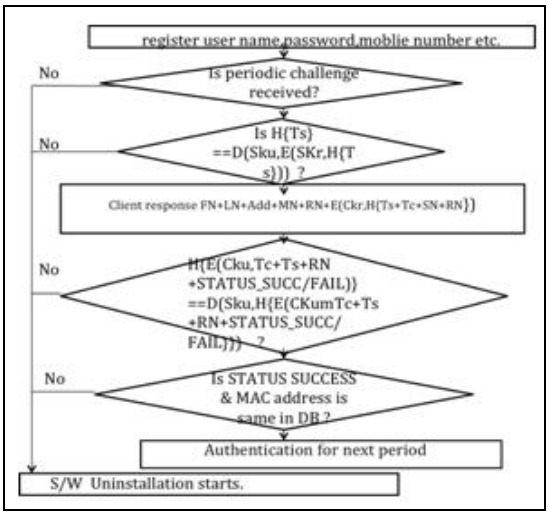

Figure 3: Server Side Algorithm

6. Expected Result

In this paper we are trying to achieve maximum software piracy inhibition. It may be in the range of above 90%. We are creating one system with one server and many client and they are connected in network. The client can login to the system by completing server side challenge. If the accepted challenge is correct then same time the keys are generated and pass to the client. In that process same keys not be generated for new client. The key generation part is dynamic, so there is assurance that one key may not be generated next

time. One legitimate client can access to the software perfectly. Also illegal use of software is avoided. Another client cannot get the access to the old client details for software piracy. Because we are providing the direct access to the client and server while software installation process. Some additional criteria

- **Low Cost** A cost-benefit analysis should result positive for the use of the protection mechanism: The cost of using the protection should be lower than the cost of losses caused by not using it.
- **Good Performance** It is important for a solution to be able to perform at an acceptable time, which does not degrade the use of the software itself. A trade-off between effectiveness and performance may be usually required, giving each the necessary position.
- **Transparency** The requirement is that the protection mechanism should be unobtrusive, so that integration with the writers of external software is made with ease and without affecting (much) the design of the external software.
- **Generality/Flexibility** A decent protection mechanism should be compatible with a wide range of applications, systems and equipment, rather than requiring relying on a certain technology or equipment, which the system should be dependent on. [5].

7. Conclusion

The work presented on this proposition contains a short, structured description of the problems in the field of Logical Property Protection, respectively Software Copy-Protection. The focus of the project has been developing a better; more secure way of protection software with the use SMS Gateway.

We are trying to provide more than 90% software piracy prevention through server and client communication. Make a key distribution system Automatic for checking the authenticity of the Software at every fixed time interval gives it advantage to identify fake unauthorized users. Through which time offset problem can be overcome.

We provide new extra security feature to solve the problem of man in middle attack. For which we are Using Hash function calculation and encryption algorithm (RSA). If server identifies unauthorized user then blocking such installed software save software companies from huge loss.

8. Table of Figures

Serial No	Figure Name
1	Proposed System Depiction
2	Client Side Algorithm
3	Server Side Algorithm

9. References

1. Ajay Nehra, Rajkiran Meena, Deepak Sohu, and Om Prakash Rishi 978-1-4673-0455-9/12/$31.00 ©2012 IEEE {main paper referred}
2. Watermark, Hardware Parameters and License Key: An Integrated Approach of Software Protection
3. Piracy Detection and Prevention using SIFT based on Earth Mover's Distance (EMD)
4. Y. Zhang, L. Jin, X. Ye, and D. Chen," Software Piracy Prevention: Splitting on Client", in Proc. International Conference on Security Technology, pp. 62-65, IEEE, 2008.
5. Assessment of Dongle-based Software Copy Protection Combined with Additional Protection Methods A. Liutkevicius, A. Vrubliauskas, E. Kazanavicius Real Time Computing Systems Centre, Kaunas University of Technology, Student str. 50, LT-51368, Kaunas, Lithuania, e-mails: agnius@ifko.ktu.lt, aras@ifko.ktu.lt, ekaza@ifko.ktu.lt
6. [Software piracy and producers developers' strategies, Attaya Heger , CEPN , University of Paris 13 , Juin 2009-06-2