Design of Software User Identity Module (SUIM) for Preventing Software Piracy

Adu Michael K, Alese Boniface K, Adetunmbi Adebayo O.

***Abstract*-This invention proposes a design for preventing software piracy by installing program from the developer's database over a computer network (internet). The user buys Software User Identity Module (SUIM) of any software developer to access the database and purchase software products equivalent to an amount on the SUIM card. Reinstallation may be permitted on the same or third party computer as long as the limit of installation is allowed. The program is downloaded and installed automatically to further strengthen the piracy prevention process. The principle of collecting hardware information of the user's computer and Time Usage of Software in Respect of Unforeseen Contingencies (TUSRUC) are applied.**

***Index Terms*- Software piracy, Software User identity Module (SUIM), Time Usage of Software in Respect of Unforeseen Contingencies (TUSRUC)**

I. INTRODUCTION

Software piracy is the act of making unauthorized copies of computer software. It is unauthorized duplication of software[1]. Software piracy on a network can be in the form of unauthorized transfer of copyright product on network as well as installing software on a Local Area Network (LAN) for use by individual who are not licensed users. Software systems are intricate part of the global infrastructure. They are the foundation for the world economy, ensure public safety, and provide a source for entertainment to millions.

Today, the driving force behind the industry's growth is the vast selection and availability of commodity software from many competing sources. Globally, the demand for software is growing as well as the potential revenue for software developers. With an increase in demand for software, the market for software piracy also increases. Software, like other forms of intellectual property, is protected by intellectual property laws. Due to software's unique digital format, software is an easy medium to pirate and easily disseminated using low cost digital media and the internet. Combating piracy is a difficult endeavour around the world. Lack of intellectual property laws, differing social stands on property rights, and lack of education, have hindered the pirated software reduction. Understanding the significance and impact of software piracy is equally important as it is to develop anti-piracy technologies. Recent connectivity software, such as peer-to-peer clients and the growing availability of high speed network connections. These provide the means for easy access to, and proliferation of illegal software. Currently, the monetary benefits, the low cost, access to counterfeit material, and enforcement difficulties make software piracy a growing epidemic, if left unchecked.

Software purchase means to purchase a software license. A software license highlights specific regulations and terms of use determined by the copyright and software maker. In general, most software licenses allow for use on a single machine and for a single backup copy. Copying, distributing, and exchanging software with friends, coworkers, or on the internet violate the license, and is a violation of copyright law. Stealing intellectual property is a crime and so is software piracy. It is a crime regardless of the type, severity, or motivation.

II. PREVIOUS ATTEMPTS AT PREVENTING SOFTWARE PIRACY

Several attempts had been made to curb piracy, these include:

Software Watermarking

This is defined as a technique for hiding identified information inside code and making it invisible and

Manuscript received August 29, 2013; revised on October 11, 2013.

Adu Michael Kolade. Author is with the Department Computer Science, Federal Polytechnic, Ado-Ekiti, Nigeria. Phone: +2348066714060
Email: memokadu@yahoo.co.uk

Alese Boniface Kayode. Author is with the Department Computer Science, Federal University of Technology, Akure, Ondo State, Nigeria. Phone: +2348034540465Email: bkalese@futa.edu.ng

Adetunmbi Adebayo Olusola. Author is with the Department Computer Science, Federal University of Technology, Akure, Ondo State, Nigeria.
Phone: +2348039617525Email: aoadetunmi@futa.edu.ng

ISBN: 978-988-19252-7-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

difficult to remove [2]. Watermarking by itself does not prevent piracy, but it helps to detect software piracy after the distribution of the software by reclaiming the ownership using the added mark[3]. Software watermarking can be classified as static or dynamic watermarks.

Code Obfuscation

This is a technique for modifying the code. It makes it difficult to understand and debug, thus it becomes intractable.

Software Tamper-Proofing

Tamper-proofing is a technique used to detect an alteration in the program and then causes the software to fail, if altered.

All the techniques above have proved to be ineffective in preventing software piracy. They only alert after the damage has been done.

Crypto-Microprocessors (CMP)
Programs can be protected from piracy by distributing them to users in cipher. An enciphered program is meaningless to anyone who tries to analyze it and ordinary microprocessors. Implementations of enciphered programs require a unique microprocessor; the "crypto-microprocessor" (CMP). This contains decipher circuitry and encryption keys needed to make sense of the cipher. An enciphered program can be executed only by a CMP that contains encryption keys, a match must be established with the keys used by the software developer to encipher the program. Nonetheless, the need for a special hardware to run the program is a major setback in this technique. In addition, it is possible for pirates to study the external operation of an executing program for clues as to what it contains internally. Reconstructing the program from these clues can lead to piracy. Pirates also try to trick the processor into disclosing its instructions by altering bits in the enciphered program. A pirate attempting to patch an enciphered program creates random-bit garbage in the instruction queue. Pirate created garbage include a self-disabling operation code which permanently disables the CMP.

III. NOTABLE INVENTIONS IN SOFTWARE PIRACY PREVENTION

The Method of Preventing Software Piracy during Installation from a Read Only Storage Medium is an invention by [4]. This is a method and system for limiting the number of installations of computer software from a compact disk to computer. More specifically it deters software piracy by detecting hardware during software installation, comparing the hardware to other hardware on which the software has been previously installed and either allowing or disallowing the installation based on predetermined factors. The compact disk (CD) comes with a floppy disk that keeps the detail of every computer on which installation is made. However, despite all the efforts intended to prevent software piracy by this method, major flaws are still noted. In today's technological advancement, present computer inventions has no floppy disk drives created with them, rather the CD drives are used and is viewed to be more acceptable by all users of the computers due to the fact that running software programs on floppy disk is slow. Also, there is a creation of the term "dependency" between the two storage media, in the sense that without one medium the installation of the software program to the computer cannot be accomplished. With the presence of an HDDI feature on every software, a floppy disk referred to as license floppy is required when the user initialized the installation of the software, and if such licensed floppy is not inserted the installation is disallowed.
Another notable invention is the Prevention of Software piracy by Activation Code System. The software can be used by different users with different computer system since it does not take into consideration the computer hardware features/configurations on which the software is been activated. It only considers if the code matches what is stored in the Remote Server of the developer [3]. The Remote Server of the developer authorizes installation to the user if data entered matches the stored information of the software on the database of the developer. With this view, one could possibly duplicate his activation code for purchased software into multiple copies and sell them in the market and put on the surface of each of the software user data. This implies that, piracy is not prevented since the Remote server recognizes every data provided in- as-much-as it tallies with the one in the database. Thus, it authenticates a user if the code provided matches the one on the database.

ISBN: 978-988-19252-7-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

IV. PROPOSEDINVENTION

The proposed invention is similar to the technology of the Subscriber Identity Module (SIM) of Global System for Mobile Communication (GSM). It is one of the most enduring and effective methods of allocating services to users based on their credit worth. Not only that, it is built around a technology that is relatively protected against pirates.

The Software User Identity Module (SUIM) is an integrated circuit that securely stores the software subscriber Identity and the related keys used to identify and authenticate software users on the developer network. It stores data for software subscribers such as user identity, software authorization data, personal security keys and usage details.

The SUIM is designed to remotely authenticate software users or subscribers to the Software Developer Network(SDN) and control purchase of genuine software provided by the SDN, monitors the users mode of usage up till the extent to which such software limit is exceeded, maintains their respective identities and platforms so that users have their usage right and prevents unauthorized or illegal access to the software. The SUIM card enables all users to have access to the services of any SDN such as software purchase, immediate communication and feedback from users to the developers, this basically prevents piracy of such software product by taking cognizance of the system or device that the SUIM is connected.

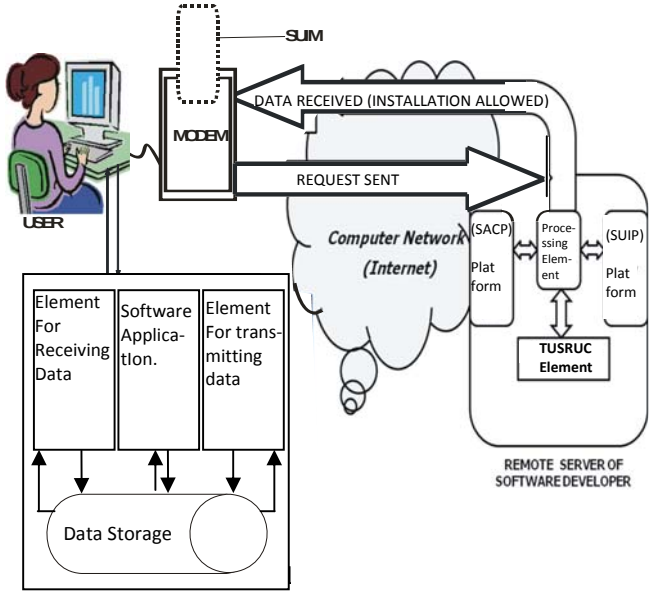

Fig 1: SUIM Architecture

FUNCTIONALITY OF THE SUIM CARD

- *Identification.* The SUIM is an ideal card to provide unique identification of every software user or subscriber. The identity of the subscriber is mapped to a user identity number programmed on the SUIM.
- *Authentication.* This is a process where the application of TURRUC algorithm is invoked. A unique response is provided for each subscriber as they purchase any legal software from the SDN. Maintaining this response, a legal software user or subscriber is logged on to the network, he or she could purchase from the list of available software products of the developer, depending on the credit worth load on the SUIM card.
- *Storage.* Storage of users' information and logs during software usage. Such as time of purchase, installation, TUSRUC period counter, expiration date, usage count, system information details.

The SUIM card contains certain amount of memory to process commands (Random Access Memory) and to store user files.

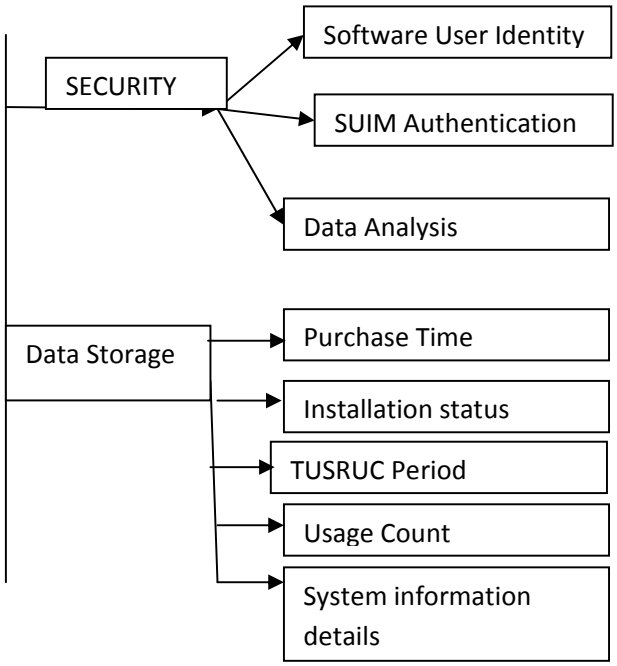

Fig 2: *SUIM Architectural Function*

ISBN: 978-988-19252-7-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

FILE SYSTEM OF THE SOFTWARE DEVELOPER.

The software catalogue is the repository of the software available by developer as well as the details regarding them. These details include but not limited to:
-Software ID
-Software Name
-Software Version Number(serial number)
-Description
-Software Type
-Software Cost

The software ID is the unique identity of the software which is always different from other software.

- *Software Name*: This is the name of the software
- *Software Version:* When the same software is produced, its version number changes depending on its development trends
- *Description*: This describes the usefulness of such software in a summarized format.
- *Software Type*: This is the type of software i.e. Application software, utility software, database software, graphics software et cetera
- *Software Cost:* This is the amount that must be paid by the user to get it installed on his/her system.

SOFTWARE USER INDENTITY PLATFORM (SUIPM) FILE

Some of the elements that make up the SUIP file are listed below:
-software ID
-software name
-Software serial no
-Date purchased
-Installation Status(TUSRUC, UNUSED, VOID)
-Software Legitimate owner
-System information

The TUSRUC feature is available for a user who is purchasing the product for the first time. The *TUSRUC Feature*states that for every first time of activation, a user might experience unforeseen contingencies which might be appalling to the user of such software (e.g Virus attack that requires reformatting the hard drive), and as such a test period of contingency (n) is placed and until n is reached, a proximity of contingency is true and can allow that same user to do further installation *only on same system,* which will be assumed as a first time installation within the period of (n). If (n) has reached the end of TUSRUC period, counting resumed forthwith, TUSRUC FEATURE is disabled and usage count = [1|1].

V. DETAILED DESCRIPTION

User buys the SUIM card from retailer/vendor and inserts it to a device (MODEM) and makes payment online via Credit card, Verve Card or alternatively by the use of scratch card of the software developer.
A SUIM user interface is open for transaction details. The user can click on the install button to download and automatically install software products equivalent in worth to the amount available on the SUIM card.

Table 1: Software User Identity Platform (SUIP)

Software Name	***Software S/N***	**S/w Usage limit**	***System information***		**Usage Count**	***Installation* Status**
Software A	00123456789	3	001a,23,FAT	Sony	1	VOID
			004b,50,NTFS	Sony	1	
			007a,100,FAT	Apple	1	
Software B	00123456782	3	003y,100,FAT	Acer	2	Not-Reached
Software C	00123456784	3	001a,23,FAT	Apple		TUSRUC ACTIVE

Immediately after installation, downloaded files are deleted. At the remote server of the software developer network, the software user identity platform file is updated by marking the software as *TUSRUC active* if it is a first time installation.
Usage Count begins after the expiration of the TUSRUC period and further installation is not possible when the usage limit is exceeded.
The TUSRUC period is the days of grace which caters for unforeseen contingencies (for example, sudden virus attack, hard disk crash, et cetera) for which the user is permitted to reinstall software without being counted against him. However, installing the same software during TUSRUC period on a third party system is not allowed, this is adequately monitored by the fact that the

ISBN: 978-988-19252-7-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

developer keeps track of every computer system on which a product is installed.

VI. CONCLUSION

The challenges of software piracy are enormous and complex especially in developing nations. There are multiple and diverse means by which software can be pirated. However, this invention proposes a method that will adequately prevent an authorized copying and distribution of software products since the software is downloaded into a temporary file that is deleted immediately after installation on the system of the legitimate owner.

The concept of Time Usage of Software in Respect of Unforeseen Contingences (TUSRUC) and collection of hardware information of respective system on which installation is made further strengthens the process.

REFERENCES

[1] M.K. Adu, B.K. Alese, O.S. Adewale and A.O. Adetunmbi, “Protecting Legitimate Software Users Interest in Designing a Piracy Prevention Technique on Computer Network”, IISTE Journal, Network and Complex Systems, Vol 3, No. 5,Aug. 2013

[2] Jasvir Nagra, Clark Thomborson, A. Collberge, functional Taxonomy for Software Watermarking, IEEE, 2000.

[3] M. Akito, Hajimulida and Ken-ichi, “ A Practical Method for watermarking Java Programs”, 24th International Computer Software and Applications Conference, 2000.

[4] E.L. Jeffrey, A. Richardson, P.ASteckler, ”Method of Preventing Software Piracy During Installation From a Read Only Storage Medium”, USA, 2001.

[5] B. Reuben, - Activation Code Systemand Method for Preventing Software Piracy. BAHAR, USA, 2008.

ISBN: 978-988-19252-7-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)