Network and Complex Systems
ISSN 2224-610X (Paper) ISSN 2225-0603 (Online)
Vol.3, No.5, 2013

Protecting Legitimate Software Users' Interest in Designing a Piracy Prevention Technique on Computer Network

Adu Michael K[1*]. Alese, Boniface K.[2] Adewale, Olumide S.[2] Adetunmbi, Adebayo O.[2]
1. Computer Science Department, Federal Polytechnic, Ado-Ekiti, Ekiti State, Nigeria
2. Computer Science Department, Federal University of Technology, Akure, Nigeria
*Email: memokadu@yahoo.co.uk

Abstract
This paper is an attempt to substantiate the fact that socio economic issue has to be put into consideration in any effort at preventing software piracy. A legitimate software owner must be given certain period of grace to cater for unforeseen contingencies during which re-installation is allowed without being counted against him. A mathematical equation - TUSRUC EQUATION (Time Usage of Software in Respect of Unforeseen Contingencies) is developed as an algorithmic function, which shows the way the system handles cases of unforeseen contingencies during the "first time" period of using a software product. These unforeseen contingencies can include the following and not limited to; reformatting of a system, sudden virus attack, system hardware damage.
Keywords: Software Piracy, Unforeseen contingencies, TUSRUC

1.1 Introduction

Software piracy is the unauthorized duplication of computer software, installing and using software on the machine of an individual who is not a licensed user or over-installing software for use beyond the licensed number (Michael, 1986). Software Piracy on computer Network can be defined as unauthorized transfer of copyright products on a network (Lope, 1998). It also includes installing software on a Network for use by individuals who are not licensed users. To purchase software means to purchase a software license. A software license specifies specific regulations and terms of use 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. Not only is using or distributing pirated software a crime, but it increasingly violates many corporate policies and many professional organization's policies. Today corporations specify strict intellectual property policies for their employees. These policies are meant to protect the corporation from breaking copyright and property laws. The policies prevent users from installing personal software on corporate machines by securing copies of company software and licenses, and limiting access to employee workstations. Many of the corporate policies are adoptions from professional organizations laws and ethics. Proper credit should be given when using intellectual property. The professional community organizations are leaders in respecting and honoring intellectual property. When software is used illegally, a company is deprived of its earnings. Piracy undermines the software market, making it less lucrative for software developers to continue to offer innovative and high quality software. It also hurts the consumer. Frequently, pirated software does not include documentation or provide access to customer support, and or future software upgrades. Most importantly, pirated software is illegal and a crime in most countries. There are many agencies and organizations that have been created for the sole purpose of reducing and preventing acts of software piracy. Recently, legislature is empowering software developers to protect their assets. An increase in penalties for pirating software and a larger push for wider enforcement are attempts to curb the rising piracy rates worldwide. Also, new anti-piracy technologies are being incorporated to prevent and deter the counterfeiting of software. Software Piracy by users is generally believed to be of a great discomfort to the developer through lower profits and buying customers through higher prices (Bertrand et al, 2004). Solving software piracy requires a combination of education, technology, legislature, and enforcement. Anti-piracy methods must be effective in deterring piracy and not hinder the legal use of the software by the user. A successive and viable solution for piracy prevention is a solution that incorporates both hardware and software protection in conjunction with education about intellectual property rights. It is also important to provide choices for quality software at fair prices. The large growth in software application makes developing software a big business with potentially large profits. Software enables users and business to do more with their systems, and the need for software is growing. But many times, software is not free, and depending on the type of software, it can cost large amounts of money. Wherever there is potential for large profits and there exists a high demand, illegal methods for satisfying the demand at a lower cost also exist. But money is not the only motivation. Power satisfaction and lack of education are also factors for fueling the

software piracy industry. Only in the past few years, with the wide availability of large disc copying machines, the Internet, and large profit gains due to the increasing demand for pirated software, has larger, more professional groups began mass copying and distributing software. Large scale professional software counterfeiting throughout the world is largely dominated by organized crime groups.

1.2 **Background of the work**

Considering the fact that software is a valued entity which is developed to enable users to carry out their basic tasks, preventing software piracy effectively requires all-round approach. An antipiracy method should go beyond preventing multiple installations and duplications but must provide effective means for a period of grace before usage count, providing at least a measure of considerations in protecting the interest of the users who are legitimate owner of the software (Julien, et al 1999). Most users are often concerned with the first installation which are considered as the most important period of measure of software benefit and as such any unforeseen contingency like virus attack, hardware failure et cetera, that may arise within certain period of first installation should be assumed as a period of grace for which another installation is permitted on the same computer without being counted against the user. However, usage count is assumed after the expiration of the period. There are three basic ways of preventing copying, they are: *copy protection, copy identification* and *copy dissuasion* (Zamparelli, 1998). One major way to dissuade end-users is to give some benefits to encourage him within certain period of first installation. Pointing out the ethical issues of software piracy to members of the piracy supply chain is another way to counter piracy. Pfleeger suggests that the 'right to fair compensation' is a basic principle of 'universal ethics'(Pfleeger, 1997). Inadequate protection of the user interest is one of the major factors that encourage software piracy especially in a third world country like Nigeria. The socio-economic factor in piracy prevention should be put into consideration in any meaningful measure of preventing software piracy. Applications that have a high production cost per unit attract crackers – if they can crack the application, they can sell copies and make personal financial gain. Selling only a few units, crackers can make a substantial financial return. Applications that are touted as highly secure are immediate targets for hackers. Security is seen as a challenge by the hacker and he gets great personal satisfaction or recognition from cracking a "secure" application (Andre, A. et al 2002).

1.3 **Notable Inventions in Software Piracy Prevention**

The Method of Preventing Software Piracy during Installation from a Read Only Storage Medium is an invention by Jefrey, et al (2008). This is a method and system for limiting the number of installations of computer software from a compact disk to a 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 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 the application of this method, major flaws are still noted. In today's technological advancement, present computer systems 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 to the computer system is not accomplished. A floppy disk referred to as license floppy will be required if 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. Based on this work, 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 (Reuben, 2008). The Remote Server of the developer gives authority of 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 a purchased software into multiple copies and decide to sell them in the market and put on the surface of each of the software his user data, by doing this, piracy is not prevented since the Remote server recognizes every user data provided in- as-much-as it tallies with the one in the database, even though it later detects and marks such user as using a pirated copy, but after the damage has been done.

One major reason for increasing trend in piracy is non-availability of any means to dissuade end-users by provision of some benefits on the original product bought within certain period of first installation. Doing this is one of the ways of appealing to members of the piracy supply chain to counter piracy.

1.4 **Analysis and Result**

The opinion of software users comprising of students, academic and non-academic staff members of the Federal

Polytechnic, Ado-Ekiti, Ekiti State, Nigeria were sought and subsequently analysed. Tables 1 to 3 show the degree of influence of not adequately protecting the users' interest by not providing a period of grace to cater for unforeseen contingencies when he procures original/legitimate software products.

Table 1: *Percentage of students' population in response to the negative influence of not adequately protecting the users' interest by not providing a period of grace for unforeseen contingencies (2012/2013 ND II and HND II final year students of the department of Computer Science)*

CLASS	Enrollment	Agree	%	Partially Agree	%	Disagree	%	No comment	%
ND II	84	80	95.2%	2	2.3%	2	2.3%	0	0%
HND II	65	56	86.2%	4	6.2%	3	4.6%	2	3.1%

Table 2: *Percentage of Non-academic staff members in response to the negative influence of not adequately protecting the users' interest by not providing a period of grace for unforeseen contingencies.*

CATEGORY	Enrollment	Agree	%	Partially Agree	%	Disagree	%	No comment	%
JUNIOR STAFF	55	45	82%	8	15%	2	3.6%	0	0%
SENIOR STAFF	25	18	72%	4	16%	3	12%	0	0%

Table 3: *Percentage of Academic staff members in response to the negative influence of not adequately protecting the users' interest by not providing a period of grace for unforeseen contingencies.*

	Enrollment	**Agree**	**%**	**Partially Agree**	**%**	**Disagree**	**%**	**No comment**	**%**
ACADEMIC STAFF	91	82	90%	7	8%	2	2%	0	0%

The data in table 1 shows that 95.2 % of the total students in National Diploma II and 86.2% Higher National Diploma II agreed to the negative influence arising from not protecting the interest of the software users by providing a period of grace for unforeseen contingencies. This implies that this negative measure can encourage piracy on the part of legitimate users who belief he has not benefitted much from the purchase of the software product. Also table 2 shows that 82% of the Junior staff members of the polytechnic as 72% for senior members (both non-academic) felt the same.

In table 3, 150 copies of the instrument of data collection were administered among the academic staff, of which 91 copies could be accessed for this research work. However, analysis of the respondents indicates that 90% agree to the fact that if a period of grace is not provided for legitimate software users to cater for unforeseen contingencies during the first time of installation, it may encourage piracy. 2% disagreed and 0% passed no comment.

1.5 **Application of *Time Usage of Software in Respect of Unforeseen Contingencies* (TUSRUC) feature**

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.

n *= software usage limit before marking activation code as used*
$\boldsymbol{T_i}$ *= Time of Installation*
$\boldsymbol{T_u}$ *= Used period of software*
$\boldsymbol{T_c}$ *= Current Time*
$\boldsymbol{T_u = T_c - T_i}$
If $\boldsymbol{T_u = n}$ *then mark Software as used; usage count = 1*
If $\boldsymbol{T_u < n}$ *then*
Update other fields on the Software User Identity Platform (SUIP) of the Remote Server (database) of the developer, except the USAGE COUNT.
If User wants to install on another HDII, Serial number, etc. then ***Display message "THIS SOFTWARE ACTIVATION CODE HAS BEEN ACTIVATED ON A SYSTEM AND IS UNDER A TUSRUC PERIOD.***

CAN NOT INSTALL ON ANOTHER SYSTEM NOW" *Else if User tries to INSTALL ON HIS SYSTEM AGAIN DURING THE TIME OF TESTING THEN* ***Allow the installation and assume proximity of contingency was true then usage count = 1 on SUIP and status of authenticity = "used" on Software Activation code Platform (SACP).***

1.6 Detailed Description

When the user begins the installation process, the activation code is entered and mobile agent is activated. The activation code might be coat-protected and would be scratched during prompt. When such code is entered, the mobile agent first locates a platform known as the Software Activation Code Platform (SACP) this platform contains the various software developed by the Software Developer and the unique activation codes for each. A quick match is done to check if the activation code provided by the user for that particular software matches the one in the SACP platform. If it matches, it then travels back to the user's PC and takes the Software Users Identity Information (*All details that uniquely identify a computer system*) which includes and not limited to Hard disk identification information, volume, file system type, PC name. It then moves to the software developers' network and locates the platform known as the Software User Identity Platform (SUIP), stores the information in the record of the platform, at this stage the software remains in the user's pc and the TUSRUC feature is activated for that user if it is the first time of installing the software. As the TUSRUC is enabled, the user might try to install the software on another system, at trying this, the mobile agent takes the information identity of that PC and compares with the one already in the SUIP platform corresponding to the activation code entered, if it is not the same, it assumes the user is trying to pirate the software and do a multi system installation, it then prompts a message such as "THE SOFTWARE WITH THE ACTIVATION CODE PROVIDED IS UNDER A TUSRUC PERIOD AND CANNOT BE INSTALLED ON THIRD-PARTY SYSTEM". But if the user tries to install the software again on his system, the mobile agent moves to the SUIP platform and sees that the identity information is the same for the user, then it will assume proximity of contingency was true for that system, but this assumption is conclusive if the TUSRUC EQUATION is true. If the user is out of the TUSRUC period, the SUIP platform records the software as used. Hence a count has started already for that system and the software will only be checked for limit of usage for any further installation(s).

Tables 4 and 5 are Software Activation Code Platform (SACP) and Software Users' Identity Platform (SUIP) respectively of implementing this research work on server/client network over the internet. The server station provides option for adding serial numbers or activation codes for all software products, view serial status, view users identifications, Edit Admin Functions, change password and to logout.

Table 4: Software Activation Code Platform (SACP)

SOFTWARE NAMES	SERIAL NUMBER	NUMBER OF TIME USED
Software A	3333333333	3
Software A	1111111111	0
Software B	2222222222	0
Software B	4444444444	0

Table 5: Software Users' Identity Platform (SUIP)

SERIAL	**PC NAME**	**HDD FILE SYSTEM**	**C-DRIVE S IZE**	**PROCESSOR NAME**	**PROCESSOR ID**	**VALIDITY**	**DATE & TIME**
3333333333	CURMASTER	NTFS	115238498304	Intel® Atom™ CPU N450@1.66GHZ	BFE9FBFF000106CA	VIOD	2013-06-14 12:33:39
1111111111	AKINWALE-PC	NTFS	138962530304	Intel® Celeron® CPU 900@2.20GHZ	AFEBFBFF00010 67A	TUSRUC	2013-06-14 12:26:39

1.7 Description of the Piracy Prevention System

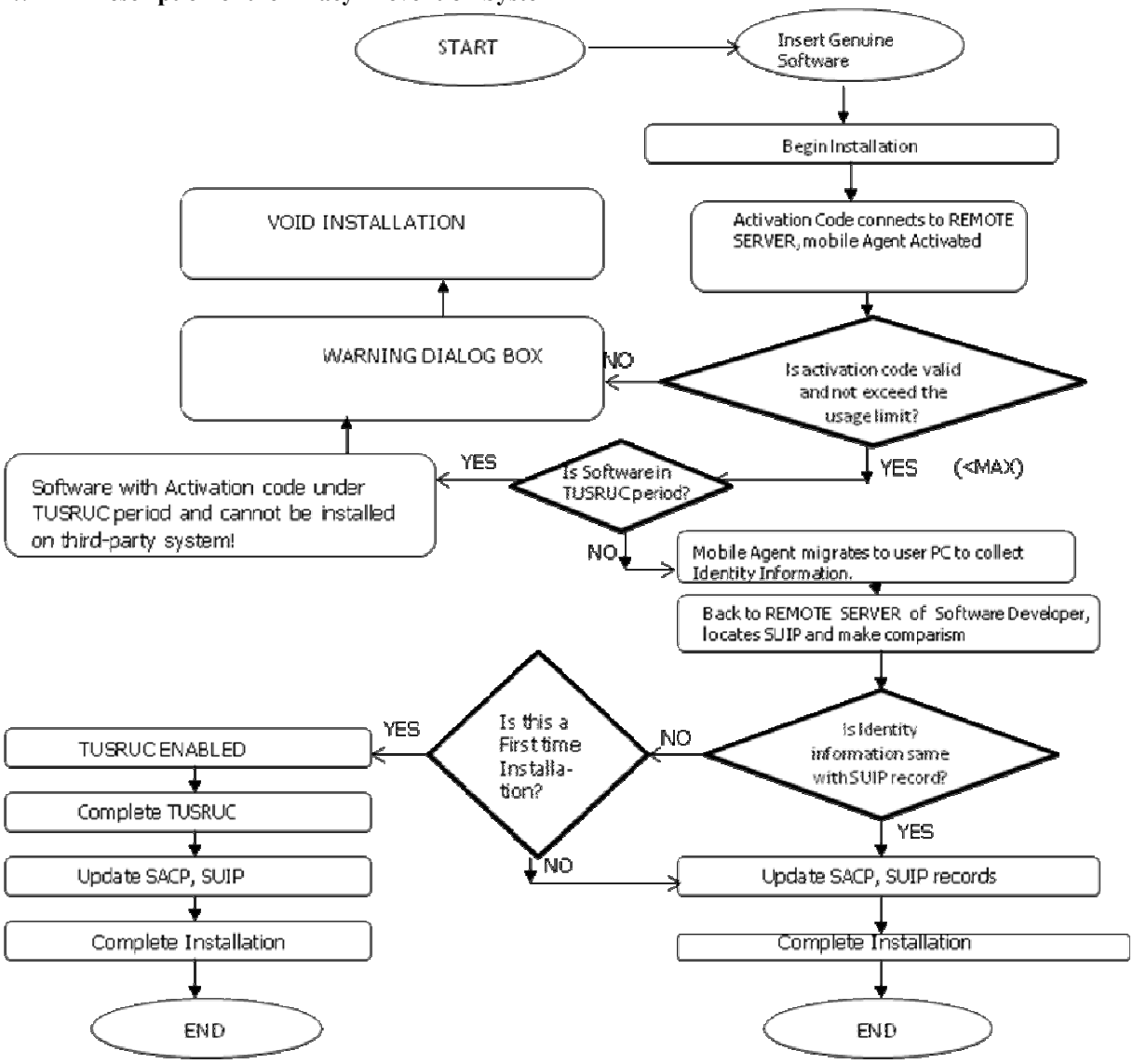

Figure 1: The flow chart description of Piracy Prevention with TUSRUC application.

1.8 Conclusion

In this paper, a novel invention is presented to prevent software piracy. This invention takes into consideration the socio-economic issue in software piracy by adequately securing the software products, hence the developer can make commensurable returns on investment since every user has to buy the original copy. Also, the interest of the user is protected at least during the period of grace "TUSRUC" period at first installation. He is consequently discouraged on piracy. The more demand from prospective users will therefore enable the price to be affordable.

In general, the procedure of our experiment is simple and implemented on the internet, which enables a wide range of information that is received by or made available to the server to be sorted, arranged and organized into retrievable data file.

Acknowledgement

This research was carried out in the Federal University of Technology, Akure, Nigeria as part of a Ph.D programme. Our sincere appreciations go to Mr. Iweama Chukwuma Patrick of Electronics and Computer Engineering Department, Nnamdi Azikiwe University, Awka, Nigeria for his technical support. We gratefully acknowledge the contributions of the referees.

References

Andre, A. et al. (2002). Basic Considerations for Preventing Software Piracy. E-security for E-Business, Rainbow Technologies, Inc.

Bertrand, A. (2004). Software Piracy Prevention through diversity. Proceeding of the 2004 ACM workshop on Digital Rights Management.

Jeffrey, E.L.et al. (2001). Method of Preventing Software Piracy During Installation From a Read Only Storage Medium, USA.

Julien, P.S. et al. (1999). Robust Object Watermarking Application code. Information Hiding, Springer-Verlag.

Lope, P. (1998). Fundamental Principles of Computer Programming Environment. IEEE Transaction on Software Engineering, Pp 472 -482.

Micheal, A. (1986). Attributes Grammars with Application to syntax- Directed Editors. Williamburg, Virginia.

Pleeger, C. (1997). Is there a security problem in Computing? Security in Computing, Chapter 1, 1-19.

Reuben, B. (2008). Activation Code System and Method for Preventing Software Piracy. West Hills, USA.

Zamparelli, R. (1998). Digital Distribution Models and copyright enforcement. Available:http//www.ftp.cogsci.ed.ac.uk/pub/roberto/diglib.ps.

This academic article was published by The International Institute for Science, Technology and Education (IISTE). The IISTE is a pioneer in the Open Access Publishing service based in the U.S. and Europe. The aim of the institute is Accelerating Global Knowledge Sharing.

More information about the publisher can be found in the IISTE's homepage: http://www.iiste.org

CALL FOR PAPERS

The IISTE is currently hosting more than 30 peer-reviewed academic journals and collaborating with academic institutions around the world. There's no deadline for submission. **Prospective authors of IISTE journals can find the submission instruction on the following page:** http://www.iiste.org/Journals/

The IISTE editorial team promises to the review and publish all the qualified submissions in a **fast** manner. All the journals articles are available online to the readers all over the world without financial, legal, or technical barriers other than those inseparable from gaining access to the internet itself. Printed version of the journals is also available upon request of readers and authors.

IISTE Knowledge Sharing Partners

EBSCO, Index Copernicus, Ulrich's Periodicals Directory, JournalTOCS, PKP Open Archives Harvester, Bielefeld Academic Search Engine, Elektronische Zeitschriftenbibliothek EZB, Open J-Gate, OCLC WorldCat, Universe Digtial Library , NewJour, Google Scholar