



TWO WAY PIRACY PROTECTION APPROACH

Kawshik. K. R., Pavithra. A. E

Department of Information Technology, Amrita School of Engineering, Ettimadai, Coimbatore – 641112,
Tamil Nadu, India.

Abstract: *The objective of this paper is to explain the process of reducing piracy of software using a technique called tow way piracy protection scheme. We hope to address the serious drawbacks in the existing methods of piracy protecting for software's that are distributed online. A rather simple approach which proves effective as almost all applications are becoming more and more dependent on the Internet for distribution and it's working.*

I. INTRODUCTION

Software piracy in simple terms is the process of duplication of software and its distribution illegally or without copyright. Even though there are strict laws in place to prevent the same it is not possible to track and monitor the various softwares that are being cracked and distributed over the internet.

A recent study by Business Software Alliance (BSA) has shown that more than 57 percent of the world uses pirated software's. Many efforts have been taken therefore in order to prevent or make it impossible to make the software's impervious to piracy. However with time almost all software's are cracked pirated and released. It is estimated that around 63.4 billion dollar worth of software is being stolen. Thus it's one of the leading concerns and area of research to develop new techniques to prevent software piracy.

Originally piracy was a result of four main factors Lack of funds or absence of that software in the region or country. With time piracy became a means of income for those who practice hacking of software irrespective of whether there is need for piracy. Factors like cost of software or its availability affect only those who use the software and not those who pirate it. With demand comes supply but in the world of piracy there is supply irrespective of demand

Our approach aims to curb piracy in two steps. First through a web application and incorporating a outer shell around the software itself, which work together to authorise a user for using the software.

II. LITERATURE SURVEY

Before advising the proposed strategy extensive research was made on the existing techniques and methods used commonly to enforce protection for software's. The list of techniques based on chronological order is as follows:

- A. **Generation of a product key (serial key):** Perhaps the most common method of piracy protection. A unique key supplied with the original copy of the software where as the part of installation authentication of the key code happens failing which the software installation does not proceed. The problem with this system being that hackers are able to bypass the lines of code which enforce the authentication process.
- B. **External Dongle:** Here there is an external dongle connected to the system with the software. The dongle contains a unique serial number which is recognised by the software and thus allowing further access to the software. The drawback with this system is in the fact that with more software come the need for more external dongles which might be practically impossible.
- C. **External Hardware Component:** Usually a microprocessor which helps in decrypting or organising information needed by different modules of the code, thus rendering the software useless without the appropriate microprocessor. Also another strategy is where the external hardware contains a few module of the software itself and completing the software's functionality would require its presence. It shares drawbacks similar to the one's mentioned above.

III. PROPOSED METHODOLOGY

As mentioned before the protection system works two fold.

THE WEB APPLICATION PHASE: Almost all applications are downloaded from the net. By creating a web application for the software vendor from which the user has to download the software to use. Now the idea is to create and store a unique digital signature for a user and his system to which the software will be associated with and verified again. The application on first download of the software retrieves the MAC address and hard disk serial number of the downloading system and stores it in a database and also using RSA algorithm encrypts both and stores the same in the local registry of the downloading system. On further download the MAC address and hard disk serial number present on the database is verified against the decrypted MAC address and hard disk

serial number retrieved from the local registry of the downloading system.

THE APPLICATION PHASE: In this phase the application the user intends to download is cover with another piece of software or code if you will that also retrieves the MAC address and hard disk serial number of the system and again encrypts it and matches it with the already existing code in the local registry.

Thus copying the downloaded software to another system or trying to download it directly to another system is not possible. Also techniques like bypass coding which can circumvent all the above techniques are made difficult to perform because of this strategy.

IV. CONCLUSION

Without the need for external devices to impose strict piracy protection this method is a step forward in piracy protection. With scope to advance the counter measures in both the phases mentioned this can be quite advancement in the field of software security.

REFERENCES

- [1] Ninth Annual BSA Global Software 2011 Piracy Study, <http://globalstudy.bsa.org/2011>.
- [2] Aladdin Company, white paper for software vendors, “*Software Protection-The Need, the Solutions, and the Rewards.*” Available on http://www.cuj.com/documents/s=8254/cuj1053119171067/hasp_softwareprotection.pdf
- [3] Tim Maude and Derwent Maude, “*Hardware protection against software piracy,*” Communications of the ACM, 27 (9) : 950 - 959, September 1984.
- [4] Antonio Mana, Ernesto Pimentel, “*An Efficient Software Protection Scheme,*” in Michel Dupuy, Pierre Paradinas (Eds.) : Trusted information : The New Decade Challenge, IFIP TC11 Sixteenth Annual Working Conference on Information Security (IFIP/Sec’01), June 11-13, 2001, Paris, France. IFIP Conference Proceedings 193, ISBN 0-7923-7389-8, Kluwer, pp. 385-402, 2001.
- [5] Ingrid Schaumueller-Bichl and Ernst Piller, “*A Method of Software Protection Based on the Use of Smart Cards and Cryptographic Techniques*”, Proceedings of Eurocrypt’84. Springer-Verlag. LNCS 0209, pp. 446-454. 1984.