

Protection of Software by Magnified License Maker

Sahana B R¹, Vartika Sharma²

¹M.Tech student, Computer Science & Engineering, GSSSIETW, Mysuru, India, Affiliated to Visvesvaraya Technological University, Belagavi, Karnataka

²Assistant professor, Dept of CSE, GSSSIETW, Mysuru India, Affiliated to Visvesvaraya Technological University, Belagavi, Karnataka

¹sahana3lok@gmail.com

²vartikasharma@gss.edu.in

ABSTRACT

Software companies are facing so much loss in present day because of software piracy which means, the hacker crack software and installs as many times the user want, which is illegal and leads to loss for the companies. It is a most difficult job for the developers of software to reduce the piracy and to prevent it. Many methods were introduced to protect the software from these kind of malicious behavior. But for some reasons, some methods were unable to execute and achieve the goal. This paper will discuss some of the techniques that are used for prevention and protection of the software from piracy or from cracking[9].

Keywords: Software piracy, License maker, software protection, Smart card, copy protection & licensing.

INTRODUCTION

Software developers are facing a huge loss in their business because of software being pirated by the software pirates. They have lost huge amount due to the illegal copying and piracy. Many software developers have introduced different methods and algorithms to get rid from this piracy. This paper surveys on various technologies that is used for the prevention of the software from tampering or from piracy. By using these methods, it will be very useful for software developers to protect the software from piracy.

RELATED WORK

License Key Management using Smart Cards

A According to the analysis by the Alliance of Business Software, many software publishers have lost many US dollars recent years because of illegal copying of the products. Many protection mechanisms were been proposed and applied to prevent this piracy or illegal copying of the products. But the hackers or software pirates will find a new way for this. Copy-protection static and Digital right management techniques[2] were been used by software publishers for the prevention of software against illegal distribution and unauthorized copying. Because of some

issues in rigid structure of licensing, which will change according the environment of the market, it is becoming less useful.

The authors of this paper presents a method of using the smart cards to prevent the software from malicious use and the illegal distribution. Along with the software, a smart card is provided to customers in which the software license key is stored. This helps in establishing a distinctive relationship between smart card and the software. When the software is installed to any machine, there is a requirement of the license key which is available in the smart card that will be read using a card reader. We have to establish distinctive relationship between smart card and the software. So the author used a key exchange algorithm of Diffie Hellman to provide security of higher degree and to stop the software piracy.

But using this smart card technique it is not flexible and scalable for large company environments based on license management because each time it requires a license key which is available in the smart card. So it is useful for the home environment. This is an ethical solution for an efficient tamper resistant software.

Software watermarking

Illegal copying, malicious modification, unlawful redistribution and misuse are the threats which has to be faced by the software at the digital domain. Many mechanisms and algorithms were introduced to avoid piracy. Such mechanisms like licensing, copyright protection[7], intellectual property, security dongles and information auditing to protect the software form these kind of malicious behavior. Many software are now using without having any ownership rights that is pirated. To overcome this piracy the author proposes a method called watermarking. In this the secret information will be embedded by the

owner in the code which acts as an identification mark which authenticates and ensures the ownership rights. Software watermarking[3][6] is a very powerful technique which is used for the prevention of software piracy.

There are two techniques in watermarking algorithm, one is dynamic watermarking and other is static watermarking. These techniques embeds the information while execution state and embeds the watermark in codes respectively. But both static and dynamic watermarking needs more maturity to enhance their work using the hash function or some relevant methodologies.

Software Copy Protection and Licensing

In IT market, the topic which is very important is software licensing and copy protection[1][4]. Software distribution control will be extended by software licensing, and copy protection is used to prevent illegal distribution of software and piracy. The license structure will be described by the XrML standard which is based on XML that is used in the copy protection system[8]. While maintaining the entity authentication and the license integrity, this license describes the conditions and rights that is applied for software.

To achieve higher possible security, the hardware authentication media and protected software will be combined with this license. And the PKCS standards are mainly used interfaces and applications. PKCS#11 shows how data will be stored on smart token with PKCS object structure. This is the data structure that contains many attributes which is used for storing information on token memory and different data types.

PROPOSED TECHNIQUE

To purchase any software, first the user will enter to the website by registering himself to the website by entering username, password and other details specified. After entering to the website, the user will be able to see the available products to purchase and download and details about the software. Whichever the product he selects, he will be required to provide the username, password again. Once he clicks on download, the application will fetches the MAC address of the system. Other device's information also be fetched and the application generates a serial key. Then all the data will be stored into the registry or the database.

The key generation and fetching the MAC address is done by using the RSA algorithm which is very efficient and easy to use. Then the encryption of the key will be done using the same algorithm. If the user with same system tries to download the same software by providing the user credentials, the application will check the registry for the data provided by the user. If the same contents are there in registry, then the application will check for the number of counts specified for that software and the system. According to the counts specified, the application will proceed will proceed to further process. Before this process, the application will check for the user login whether he is a first time user or not. If the login is first time then the application will allow the user to download the software as shown in the Fig 1. And if the same software which is downloaded is copied to other system will not work.

CONCLUSIONS

As software piracy have become the major issue for software developers, they have been lost many US dollars due to this piracy. So protecting the software from the software pirates is a very hectic task for the software

developers. Many methodologies and algorithms were introduced like XrML and PKCS#11, software watermarking and smart card technique to overcome from software piracy. These techniques make sure the piracy can be eliminated and controlled. This paper discusses about different algorithms and methods that will be helpful in protecting the software from software piracy. But the proposed method will be very efficient and effective than other methods which will be cost effective and user friendly too.

REFERENCES

1. Usama, M. & Sobh, M., 2011. Software Copy Protection and Licensing based. IEEE, pp. 856-861.
2. Nützel, J. . & Beyer, A., 2006. Towards Trust in Digital Rights Management Systems. ACM workshop on Digital rights.
3. Eberhardt, G. & Nagy, Z., 2006. Copy protection through software watermarking and obfuscation.
4. Mark Perry & Leili Noorian, Autonomic Software License Management System: licensing patterns implementation. 2009 Fifth International Conference -Autonomic and Autonomous Systems. IEEE 978-0-7695-3584-5/09
5. G. Joan Daemen.Vincent Rijmen. The Design of Rijindael: AES-the Advanced Encryption Standard[M] .Springer Verlag, 2003,pp:S772 .
6. C. Collberg and C. Thomborson, Watermarking, "Tamper-Proofing, and Obfuscation-Tools and Software Protection," IEEE Trans. Soft. Engi. 28 (8), 2002, pp. 735-747.
7. H. Zamani, M. G. Sanaei, B. E. Abarghouei, and G. Hakimi, "Online Modules: Novel Model in Serial-Based Method of Software Copy Protection," International Journal Computer Science and Telecommunication, pp. 1-9, 2013.
8. T.C. Ralph, K.J. Resch, A. Gilchrist, "Efficient Toffoli gates using qudits", *Phys. Rev. A*, vol. 75, pp. 022313, 2007.

9. deepdyve.com. 'preventing application software piracy an imperial investigation of technicalcopy protection'.[online]. Available:http://www.deepdyve.com

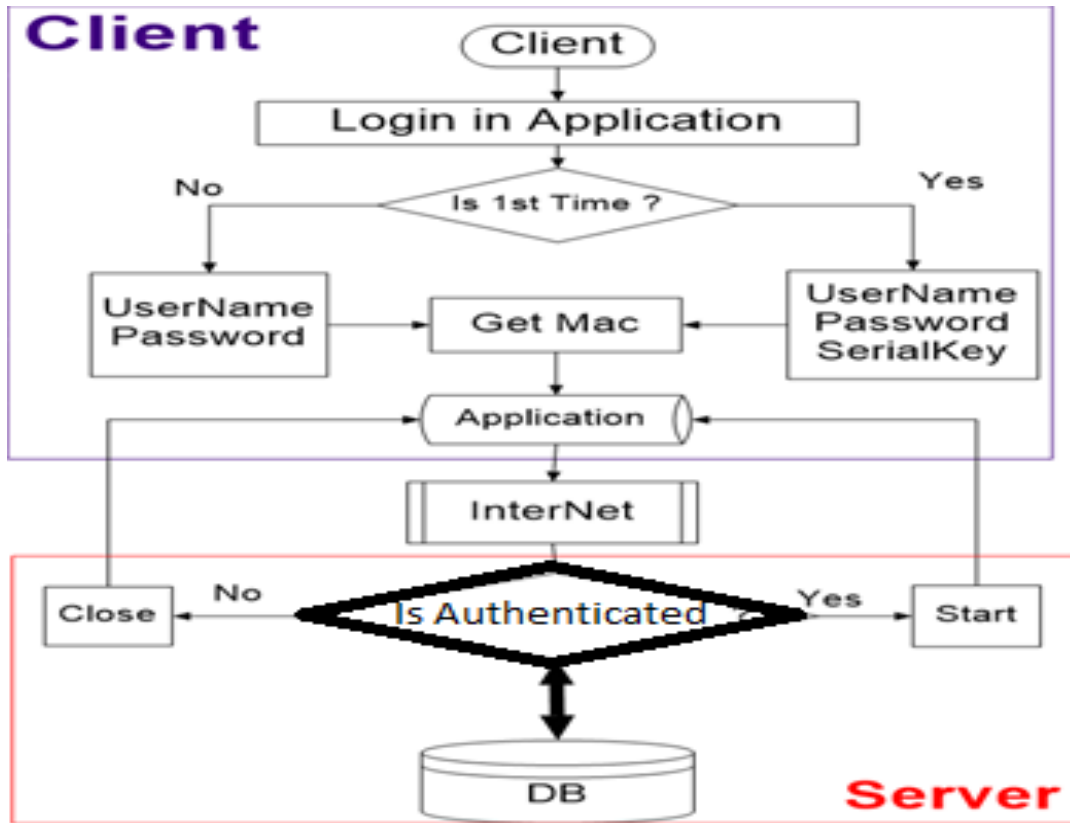


Fig 1: Server and Client Communication Model