

# Software Security by Providing License Key with Cryptography

Er. Tarannum Sharma<sup>1</sup> and Girish<sup>2</sup>

**Abstract-** With the rapid growth of information technology, there has been an increasing trend to digitalize tools and information and move away from the traditional forms of doing business. This rapid advancement has been seen for the most part as positive. Unfortunately it has led to a number of unforeseen problems. Copyright laws that had originally been suited for physical texts and tools could no longer be applied to digital works. The entire notion of property as something necessarily physical has transformed into something more abstract, giving rise to the concept of intellectual property. Intellectual property is defined as anything created using one's intellect. This includes computer software, books, art, schematics, music, and other creative works. With the concept of intellectual property came new legislation to protect these works. Unfortunately, this legislation, though it prohibits software piracy, has been insufficient to prevent widespread piracy in most of the world.

**Keywords** –Software security, Cryptography, Piracy, License.<sup>1</sup>

## I. INTRODUCTION

Software piracy [1], software licensing and license control are all important issues to software developers. People who use illegal software not only hurt themselves, they also contribute to a problem that cumulatively can hurt job creation locally and regionally in the software industry and related businesses. Software piracy also has a significant impact on the high-tech industry, resulting in lost jobs, decreased innovation and higher costs to consumers.

At the time of this research there was no system commercially available to independent software developers that would control number of installations of licensed software products. A company could obtain a single license and use it among the network. Users would break terms of their license agreement by using software on multiple computers without purchasing additional licenses.

There are certain ways to prevent or restrict those illegal activities. One way is tying software installation to hardware. Hardware tying, however, has a huge drawback to software publishers: a user has to pass a Hardware ID to the software manufacturer at the time of ordering, which might his willingness to purchase that product at all, playing its role in the decision of getting this or competitor's product. Additionally, a user will have to manually obtain a Hardware ID and pass it to the ordering system, which is usually implemented as a SSL-encrypted Web order form.

Product Activation is an anti-piracy method to verify a software license and limit the spread of software piracy. Product Activation ensures that the users install each software license on as many computers as it is permitted by a software license agreement. Every time a product is installed on a new PC or if there is a change in hardware of the PC' on which it was installed, the user has to activate his copy of the software product by obtaining an Activation Code from the activation server. If a product is not activated within 14 days, it will cease working, and only the activation functionality will be available.

<sup>1</sup> Department of Computer Science Engineering GVIET, Ramnagar, Banur, Punjab, India

<sup>2</sup> Department of Computer Science Engineering GVIET, Ramnagar, Banur, Punjab, India

More companies are developing software activation systems. Searching for “software activation” on Google.com did not provide any meaningful links in May 2002; in September 2002 the same search returned around 20 companies requiring their users to activate a copy of a product they’ve just purchased.

Most computer security is not easy for people to use. Even before the Internet became a household word, security failures were more likely to be caused by user errors than by weak cryptography or bad protocol design. This was true even when networked computers were used primarily by people who had some degree of technical skill or professional training; it is overwhelmingly truer now that a personal computer with an Internet connection has become a standard consumer good. Hundreds of millions of people now use the Internet to communicate, find information, and conduct financial transactions on a regular basis. Ideally, they should be empowered to make and enforce their own security and privacy decisions, but the usability barrier has so far made this implausible.

## II. LITERATURE REVIEW

Laurie E. MacDonald et al.[2] argued that although software piracy has serious implications for the software industry and the economy, the topic receives very little detailed coverage in MIS textbooks. Software piracy has a significant impact on the software industry and on the economy as a whole. Lost sales due to software piracy amount to over \$11 billion annually and lost taxes approach \$1 billion annually. Current technology makes it a simple task for even a novice computer user to copy software and therefore, unauthorized software is not uncommon. The researchers conducted an evaluation of MIS texts and found that software piracy receives very little coverage in the texts. The research suggests that MIS faculty need to provide material to supplement the textbook coverage in order to provide adequate coverage of this serious issue.

Susan Athey et al. [3] evaluated the nature, relative incidence and drivers of software piracy. In contrast to prior studies, they analyze data that allows us to measure piracy for a specific product – Windows 7 – which was associated with a significant level of private sector investment. Using anonymized telemetry data, we are able to characterize the ways in which piracy occurs, the relative incidence of piracy across different economic and institutional environments, and the impact of enforcement efforts on choices to install pirated versus paid software. They find that: (a) the vast majority of “retail piracy” can be attributed to a small number of widely distributed “hacks” that are available through the Internet, (b) the incidence of piracy varies significantly with the microeconomic and institutional environment, and (c) software piracy primarily focuses on the most “advanced” version of Windows (Windows Ultimate). After controlling for a small number of measures of institutional quality and broadband infrastructure, one important candidate driver of piracy – GDP per capita – has no significant impact on the observed piracy rate, while the innovation orientation of an economy is associated with a lower rate of piracy. Finally, they are able to evaluate how piracy changes in response to country-specific anti-piracy enforcement efforts against specific peer-to-peer websites; overall, they find no systematic evidence that such enforcement efforts have had an impact on the incidence of software piracy.

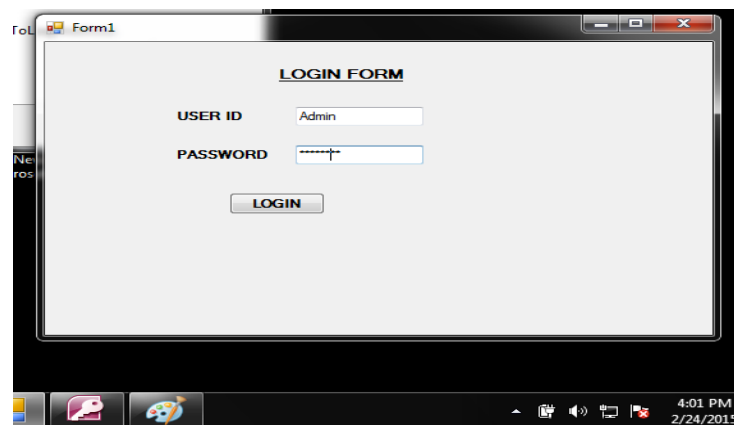
UmangGarg et al.[4] discussed that networking is the vast growing technology in their culture today. One of the technologies is Internet Protocol. It is the main network protocol in the Internet model (TCP/IP). The success of TCP/IP as the network protocol of the Internet is largely because of its ability to connect together networks of different sizes and systems of different types. These networks are arbitrarily defined into three main classes (along with a few others) that have predefined sizes, each of which can be divided into smaller subnet works by system administrators. A subnet mask is used to divide an IP address into two parts. One part identifies the host (computer), the other part identifies the network to which it belongs. In this paper they analysis that when MAC address is unique for all machines although they are using IP address for networking purpose. They studied and analyzed various attributes related to IP address scheme and MAC address. A detailed review study is discussed in this paper.

Gupta Nishant et al.[5] discussed that Software protection is an area of active research in which the software industry is encountering a number of threats. Software piracy is one such threat, which proves detrimental in protecting the intellectual property rights. There have been a variety of techniques developed to address the issue like software watermarking, code obfuscation, and tamper-proofing. In the current research they address the issue of software piracy through a prevention technique known as software watermarking which aims at providing copyright protection and authorized access of commercial software. In this paper fragile software watermark is used to embed personal information into the software. Then this personal information is merged with the hardware parameters of the client machine extracted during the process of installation and License key provided by the vendor. This combined string (Watermark + Hardware parameters + key) is send to the server for registration. This process is implemented and tested on different machines and the accuracy of the proposed model is found to be 99%. The proposed model will be beneficial in combating software piracy and securing the software from redistribution.

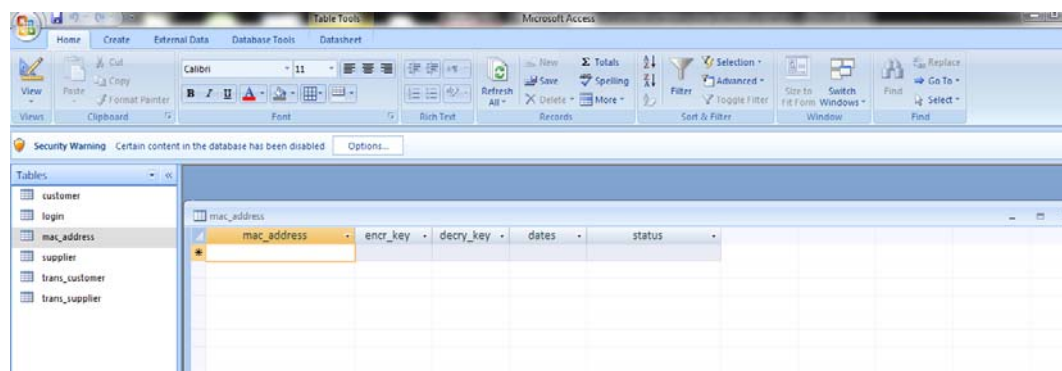
### III. RESULTS

Software License Keys are used in various copy protection schemes. The basic idea is that only users that have acquired the appropriate license will be issued a license key enabling them to install or use the software.

The key itself can be a string of characters entered into the installer or the software itself which by some method of computational comparison verifies the entered key and subsequently continues the installation process or the execution of the software. The key can also be a hardware dongle that physically connects with the computer making the key less vulnerable to copying. Generally speaking, circumventing copy protection schemes based on either software license keys or hardware dongles through reverse engineering of the verification code is not complicated unless rigorous code protection mechanisms are put in place to obfuscate the copy protection itself. Bear in mind that all protection systems can (and will be given enough time and resources) broken.

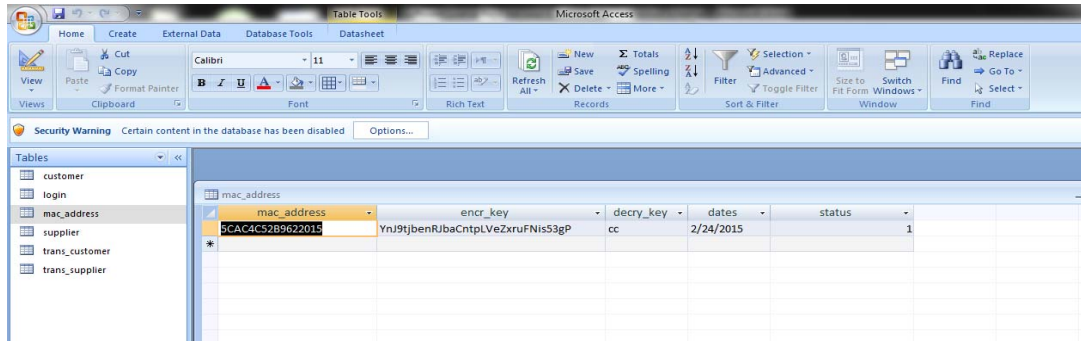


In the above print screen System Date is 24th February 2015. When we enter first time Username and Password the mac\_address table is blank as shown in below print screen.



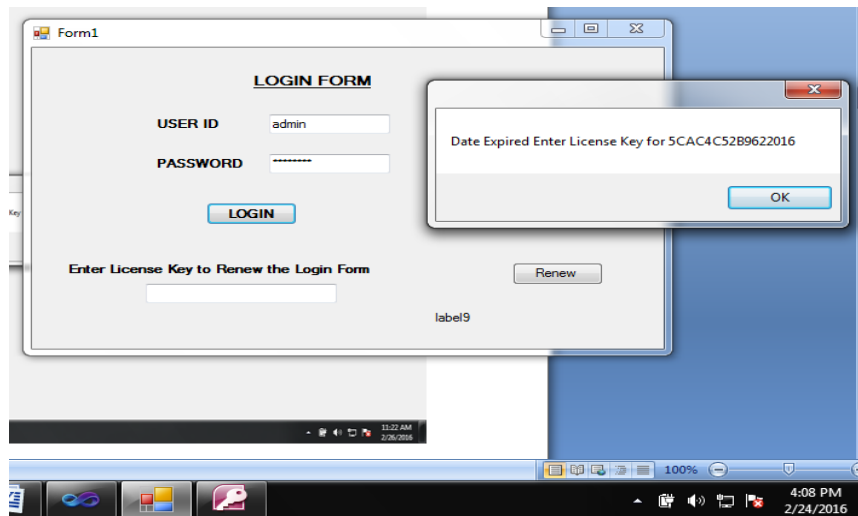
This Print screen shows mac\_address table is blank when we install the software and enter first time username and password.

When we click on submit button of login form main admin form open and the values inserted in mac\_address table as shown below. The mac address value of machine is inserted and the corresponding encryption key is also inserted. The starting date 2/24/2015 is shown in table.

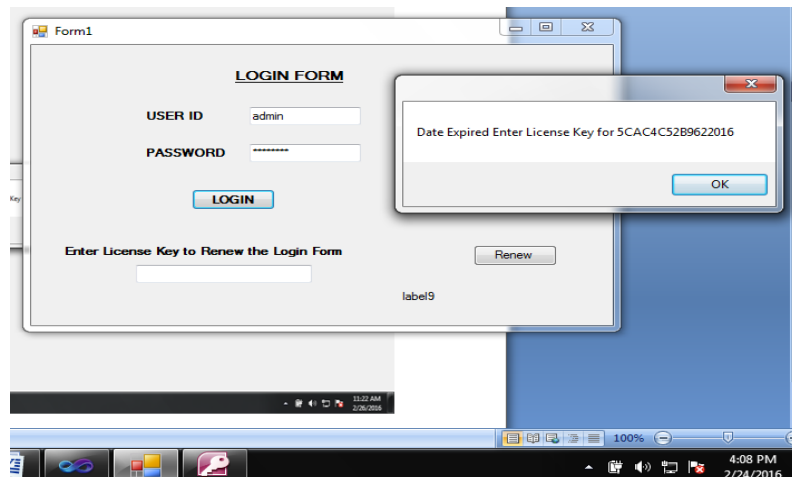


mac_address	encr_key	decry_key	dates	status
5CAC4C52B9622015	YnJ9tJbenRjbaCntpLVeZxruFNis53gP	cc	2/24/2015	1

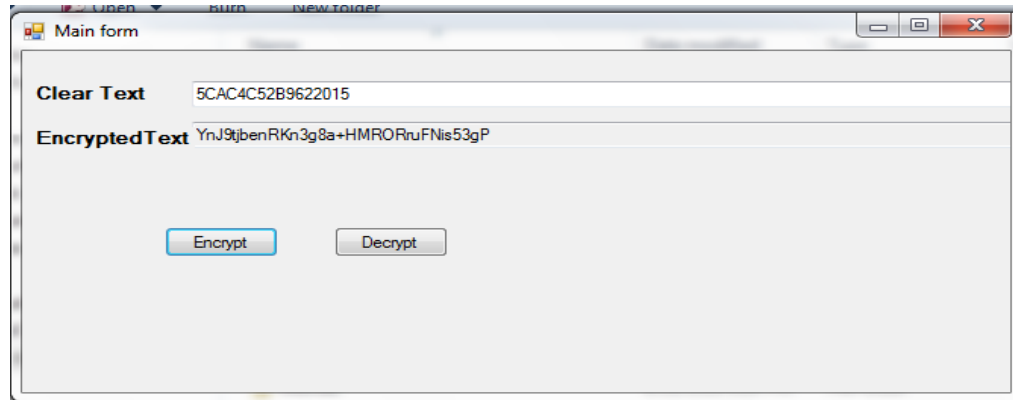
It will work for one year, up to 2/23/2016 its working fine. but on 2/24/2016 its giving error message as shown in below print screen.



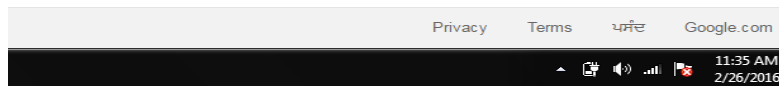
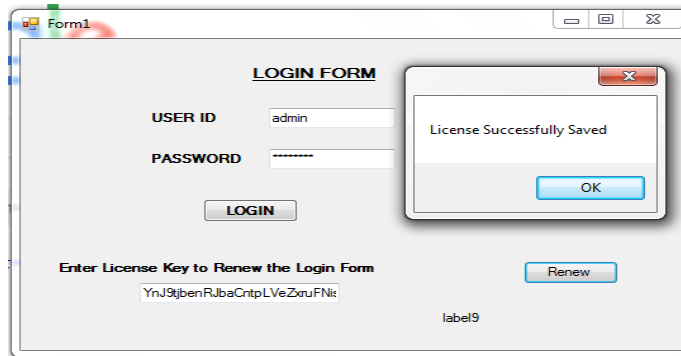
As Date expired after one year, User has to buy license key by sending the values given in message box. After receiving the license key software working for one year as shown in below print screen.



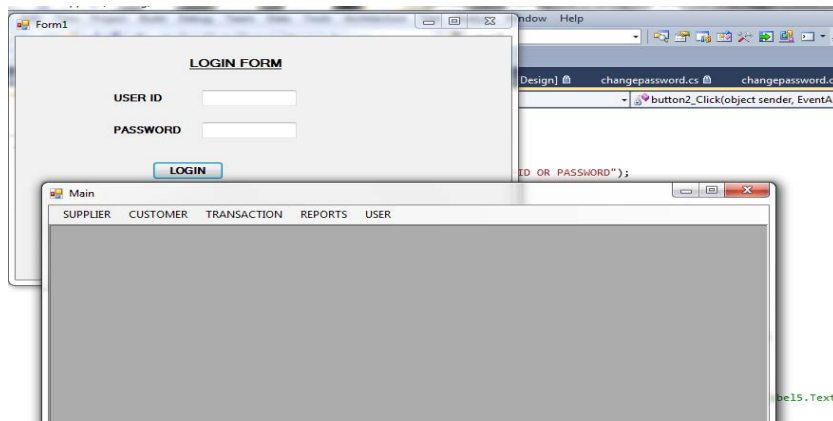
Encryption key generated by administrator on entering the value send by user.



When we entered License key and click on renew button, its renewed for one year



Now It again work for next one year.



#### IV. CONCLUSION

The protection scheme presented in this thesis overcomes the fundamental flaws common to almost all existing technical means for software piracy prevention. The protection mechanism migrates from static nature of defense to a dynamic nature. The marginal cost of using the software decreases. Of the existing technique, software aging is of dynamic nature but the number of forms of software privacy against which it provides protection is too late. The copy rights to run the software on client/customer machine are only available to the software developer company.

The only drawback of the scheme occurs when the user has changed its LAN Card/ Motherboard, the Mac address is also changed and the user has to send the request to software Developer Company to send the License key again. In future we can improve this drawback.

## V. REFERENCE

- [1] Oleg Afonin (2002), "Evaluation of Activation Based Software License Enforcement".
- [2] Laurie E. MacDonald and Kenneth T. Fougere, "Software Piracy: A Study of the Extent of Coverage in Introductory MIS Textbooks", *Journal of Information Systems Education*, Vol. 13(4).
- [3] Susan Athey and Scott Stern(2014), "The Nature and Incidence of Software Piracy: Evidence from Windows".
- [4] Umang Garg, Pushpneel Verma, Yudhveer Singh Moudgil and Sanjeev Sharma(2012), "MAC and Logical addressing (A Review Study)", *International Journal of Engineering Research and Applications (IJERA)*, Vol. 2, Issue 3, pp.474-480.
- [5] Gupta Nishant\* Jamwal Shubhnandan S. Devanand(2013), "Watermark, Hardware Parameters and License Key: An Integrated Approach of Software Protection", *International Journal of Advanced Research in Computer Science and Software Engineering*, Volume 3, Issue 5.