International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Generic Method for Prevention of Software Piracy

Nadeem Sajjad[1], Rohit Maheshwari[2]

[1]Integrated M.Tech. Scholar, Mewar University, Rajasthan, India
[2]Assistant Professor, Mewar University, Rajasthan, India

Abstract: ***Software piracy has been major issue for software industries. They have to pay a very large amount to protect their applications. There are several insurance schemes for the protection of software. But they all are very costly and provide services for a limited period of time. This paper will demonstrate a protector tool which can be developed in any platform very easily so that the vendor can protect the software not only for being pirated but also capable of limited period expiration of software. This strategy will provide easy and low cost protection which is more effective than MAC address authentication. This tool is very useful for desktop applications which use internet for their internal working, as it provides server based authentication, but is also feasible for those applications that do not use internet as it has client side authentication also.***

Keywords: Hardware Based Authentication, SMS Authentication, Software Piracy, Software Protection, Low Cost Software Protection

1. Introduction

Computer technology is the integral part of the society. This causes a widespread use of personal computers over a short time period. Software industries have to face very huge loss due to piracy. This can be done by sharing, downloading, copying or installing multiple copies of software onto personal or work computers. Studies have shown that the commercial value of this market of pirated software industry climbed from $58.8 billion in 2010 to $63 billion in 2011, a new record which shows a very high rate of piracy [1].

The piracy is tackled through different protection strategies. Software protection must be made available for a very low cost so that it may be useful for software vendors [2]. This paper demonstrates a protector tool which will provide SMS based authentication of the software to protect it from piracy. Software will be registered on server of the vendor. This registration will include several details (e.g. serial number and manufacturer of BIOS). This paper also describes the drawback of MAC based authentication and the ways to overcome it. The approach of having serial number as the authentication process in both server and client side is very effective and have many advantages over the MAC based authentication.

2. MAC Based Authentication

In MAC (Media Access Control) based authentication software is authenticated according to the MAC address or the physical address of the NIC (Network Interface Card), which is a 48 bit unique number given by the NIC vendor. MAC address is stored on the server so that whenever someone tries to access the software MAC address of client must match the registered address on Server [3]. This is a very effective approach and is generally used in a number of software. This approach has a limitation that software cannot be used with the other internet connecting device or the medium having different MAC address. So if the medium gets tampered or if the client wants another device to connect through internet will be barred. Also this method is not always protective as someone can change the MAC address to the already registered MAC address and use the software in simultaneously two or more machines.

MAC address authentication limitations can be very dangerous if MAC address is spoofed, there are numerous software present on internet which can be used to change the MAC address of the machine as per user requirement. This will ultimately affect the software piracy and may result into huge loss to the software industry.

3. Serial Number Based Authentication

MAC address spoofing is very easy and proves to be harmful for software industries. Software industries require recording the details of each client using the software. If the Hardware serial number is registered with the software and they are stored on server, it will be very difficult for client to spoof these serial numbers. Serial number of hardware present on a system can be easily extracted by using simple programming. This paper will also use the BIOS (Basic Input Output System) keys to register software. This approach will allow developers (vendors of software) to protect software. They can use the distribution file (e.g. jar file in java, DLL in .NET) in any platform and protect their software. This distribution file will contain a class protector which will be instantiated at the very first source code of the software to be protected. This will authenticate the software for piracy on failure of which it will stop the execution of software thus protecting it from being pirated.

3.1 Working

When the object of the Protector class is created it first checks the registration status of the product. If the product is not registered a first time registration is invoked followed by Server Side Authentication else if the product is registered then a network instance is created to check whether the client is connected to internet or not. If the software is connected to internet a server side authentication process is invoked. If this authentication is successful then the software is in verified state and the protector allows software to run. Else the IP address and the MAC Address of the client are stored

on the server which can be verified by the vendor at any time.

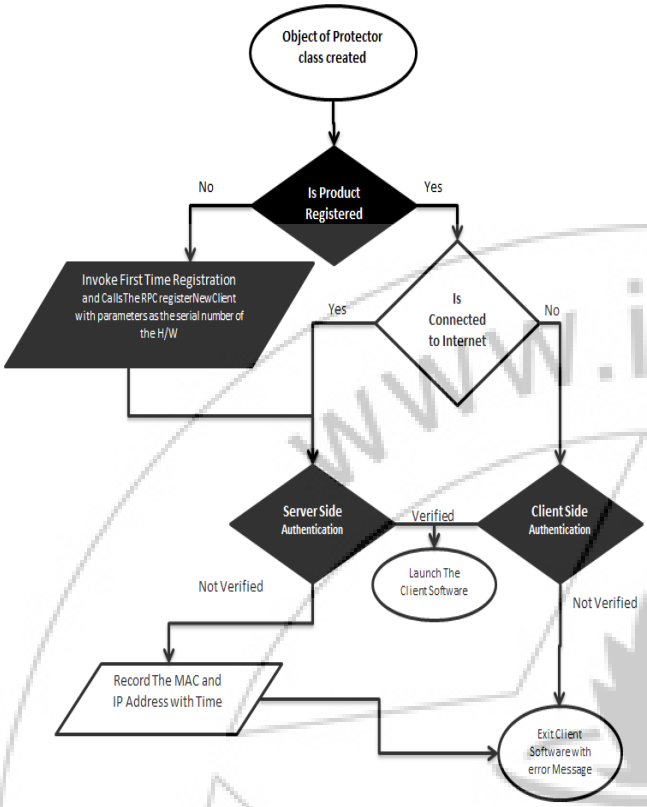

Figure 1: Working of Protector Tool

3.1.1 DB (Date Bit) File

This file stores all the basic information of the software in encrypted format. This encryption will be using message digest algorithm such as md5 so that no one can decrypt the data given except the last accessed time which will be encrypted according to some different approach which can be decrypted for comparisons.

This DB file will contain the following data:

1. Last accessed date.
2. Serial Key provided by the vendor at the time of purchase.
3. BIOS manufacturer, date released, serial number and name

3.1.2 Verification of Product Registration

This is a very simple task for the software that it can check directly for the DB file that must be present in the directory of the software. If the DB file is absent it's for sure that Product is not registered.

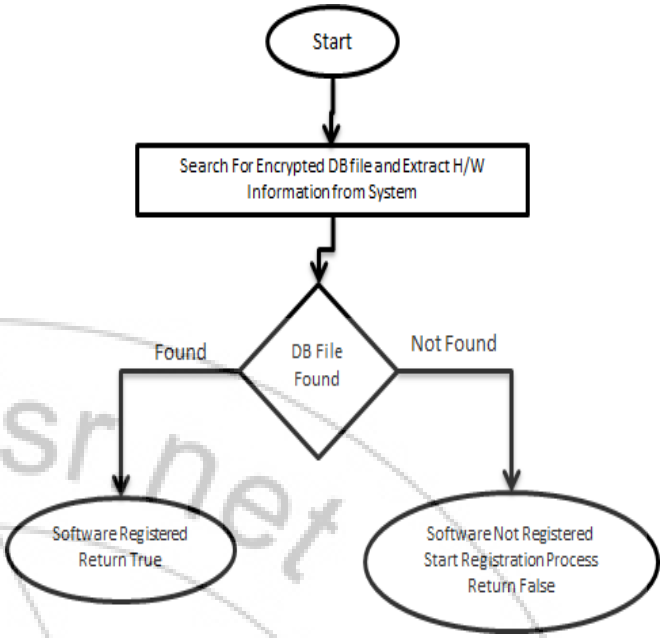

Figure 2: Verification of Product Registration

3.1.3 First Time Registration

In first time registration a registration form is shown to client who asks contact information of the client and also the serial key which was given at the time of purchase. In this registration form mobile number of the user is asked for the authentication process.

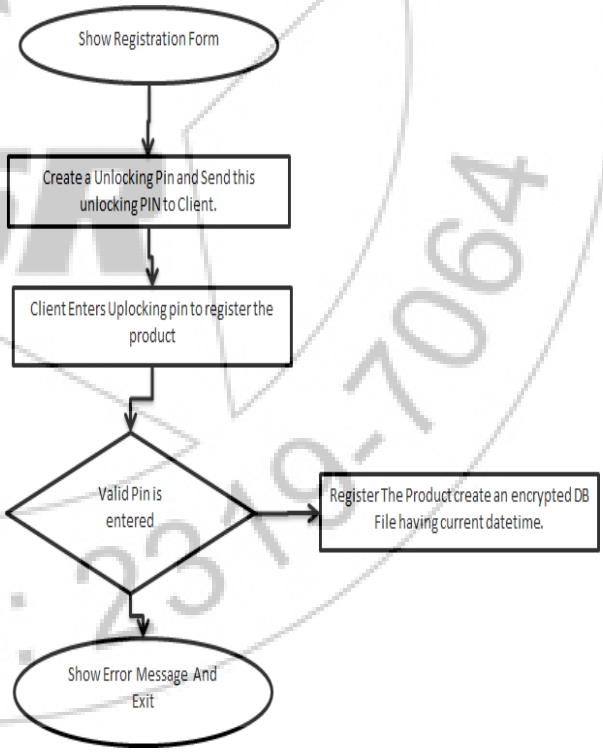

Figure 3: First Time Registration

When a request is generated A 10 digit alphanumeric unlocking pin is created by the protector tool which is sent through SMS to the client Mobile. Client can successfully register this product using the unlocking pin. If the entered pin is valid then an encrypted DB file is created within the software directory which stores last access time of the

software. Else the software Stops and shows an error message.

3.1.4 Server Side Authentication (SSA)

When SSA is invoked an RPC is called with the current Hardware details and also the DB file content. If the Hardware details are of valid user, it returns verified status which allows the S/W to launch. If details are not verified the software stops immediately and shows error message to the client. And also if there is an error while the Server Side authentication a log is created in the server so that vendor can track if any particular user sends multiple non verified SSA requests.

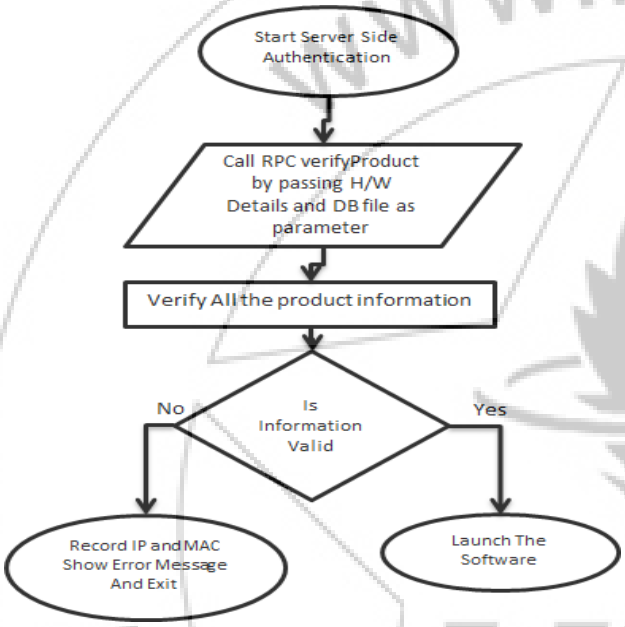

Figure 4: Server Side Authentication

3.1.5 Client Side Authentication (CSA)

CSA is required generally when a client is unable to connect to internet frequently. In this DB file plays an important role which confirms whether the current access time is greater than the last access time or not if the current Access time exceeds the product registration period or is less than the last access time the authentication results in failure which generates an error message and stops the execution of the software.

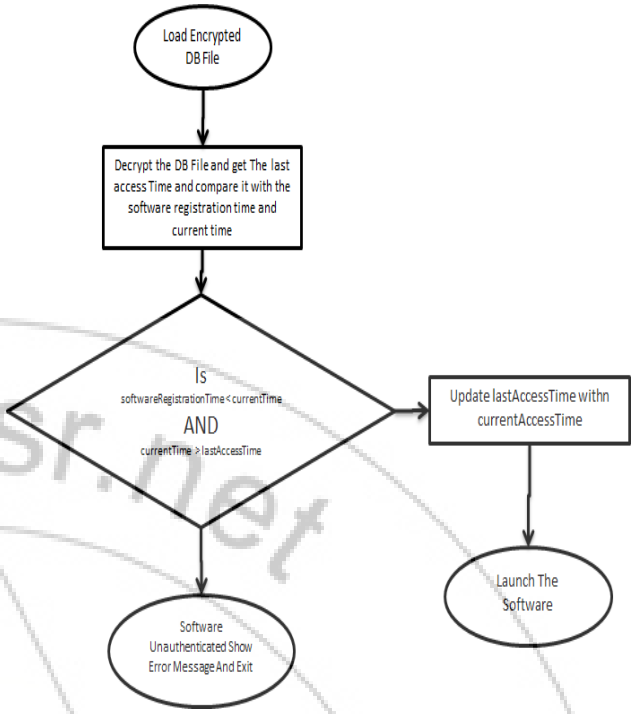

Figure 5: Client Side Authentication

4. Comparison with MAC Based Authentication

Table 1: Comparison with MAC Based Authentication

MAC Based Authentication	*Serial Number Based Authentication*
1. Present on NIC (Network Interface Card) changes on changing NIC.	1. Changing Serial Number of hardware means changing Hardware, which is practically not possible for User.
2. Can be spoofed using MAC spoof software.	2. Practically spoofing of hardware serial is not possible.
3. Can be easily known by simple commands given in command prompt or terminal.	3. Requires an expertise to know the correct serial number and other details.
4. MAC Address is only helpful when the software to be protected must be online software.	4. Can be implemented on a system which is offline.
5. Customer can easily know that software uses MAC authentication as it does not work without Internet connection	5. Customer cannot know that what type of and which hardware serial number is being verified as whenever software runs it does an offline authentication if internet is not available

5. Advantages and Limitations

5.1 Advantages

- Easy implementation in any platform.
- Easy to use and maintain thus helping the developer to integrate the tool very easily.
- Tracking of current clients.
- Tracking of unauthentic users (such that if multiple unauthentic requests are invoked by a particular client it may be blocked by the server)
- Very effective for desktop applications, specially the application which uses internet.
- Can be used for both desktop and web applications.
- Better for periodic expiration software

5.2 Limitations

The tool is less effective if the client uses the software and changes system time frequently. So vendor may provide the software with small periods of expirations. Another limitation of this tool is it requires administrative privilege as it needs information from BIOS of the system which is only provided by the OS if the application has administrative privilege.

6. Implementation on Different Platforms

C# window based Desktop applications have a main method which is invoked at the startup of the application [4]. This tool can be implemented on .NET platform just before the initialization of the first Window Form that is instantiated to run. This tool can be integrated just by instantiating a new object of the class present in the distribution file, which will perform all the operations required for the authentication.

Other .NET technologies can use this tool same as C# window based application. Like Visual C++ can have instantiation of the object in main method. Visual Basic can have instantiation in the default Window form. Java based Desktop applications also have main method in a particular class which is invoked at runtime. We can instantiate the object of the tool in static block of this class, as static blocks in java are executed before main method [5]. All web technologies like JSP, pHp or ASP can have instance of the tool where the common file is used in each web page. Normally a Web application has a common file for database connection [6].

7. Conclusion

I want conclude that Serial Number Based authentication may be used to provide a better protection to the software. The protector tool which is demonstrated can be used for the time based authentication in a smarter way so that a client may not use the software for a longer period to that he purchased the software. Also this model makes it very difficult for a user to judge what type of authentication process is going on so if customer is unknown of the authentication type it decreases the chance of being pirated.

Acknowledgements

I feel highly obliged to a few people who have helped and guided me to the correct path from the initiation to the completion of the dissertation work. First of all I would like to thank **Mr. B. L. Pal**, Head of Department Computer Science and Engineering, Mewar University, Chittorgarh, without whom it would have been a very difficult task. I would also like to thank my guides **Mr. Rohit Maheshwari**, faculty of Computer Science and Engineering, Mewar University.

References

[1] Global Software Piracy, Business Software Alliance, [Online] [Cited: May 5, 2014.] http://globalstudy.bsa.org/2011/.
[2] Conner, Kathleen Reavis, Software Piracy: An Analysis of Protection Strategies, Management Science, 1991, Vol. 37
[3] Mahajan, Surendra, Inhibition to Software Piracy Using Challenging Response Protocol, International Journal of Innovative Research and Development, 2014, Vol. 3.
[4] Main and Other Methods, Microsoft Developer Network, [Online] [Cited: May 1, 2014.] http://msdn.microsoft.com/en-us/library/ms228506(v=vs.90).aspx
[5] Initializing Fields (The Java™ Tutorials <Learning the Java Language> Classes and Objects), Oracle Corporation, [Online] [Cited: May 5, 2014] http://docs.oracle.com/javase/tutorial/java/javaOO/initial.html
[6] Accessing Databases from Web Applications , Oracle Corporation, [Online] [Cited: April 24, 2014] http://docs.oracle.com/javaee/1.4/tutorial/doc/WebApp6.html

Author Profile

Nadeem Sajjad is currently pursuing Masters Degree in Computer Science and Engineering at Mewar University, India.

Rohit Maheshwari, Assistant Professor (Dept. of CSE) Mewar Univerity. He has completed B.E. (IT) from Rajasthan University Jaipur and M.Tech.(CSE) from Rajasthan Technical University Kota.