International Journal of Information and Computation Technology.
ISSN 0974-2239 Volume 3, Number 4 (2013), pp. 303-310

http://www. irphouse.com /ijict.htm

Digital Media Piracy & Control

Deepak Vashisht[1] and Megha Agarwal[2]

[1,2]Department of Information Technology,
Dronacharya College of Engineering, Gurgaon.

Abstract

The paper is meant to create a discussion on techniques developed for prevention of piracy in digital media which can be regarded as one of the biggest obstruction in the growth of digital media sector. The duplication caused by piracy has innumerable problems which are indispensable. Thus it is need of the hour to staidly understand the importance of preventing piracy so as to ensure unhindered growth of the staggering flourishing market of digital media. The fact that it is becoming relatively easy to access anyone's confidential data without any legal permission has led us to carefully think of some kind of innovative ways to protect ourselves and so this paper talks of some of the most effective counter measures. Here described an architecture integrated with different forms i.e. tamper proofing, obfuscation and watermarking that can shield digital media. These techniques are built with the purpose of controlling ever increasing piracy which and are undoubtedly capable of fighting against the hazardous consequences causes by the toughest rival of economy sector. This three layered technique enable us to withstand all most all types of attacks and prevent from Zero Day attacks. These techniques cover both hardware/manufacture level and software/user level protection, and are most affordable, reliable and everlasting counter measures.

Keywords: Tamperproofing, obfuscation, watermarking.

1. Introduction

Even after being aware of the fact that use of computers has increased 2 folds over the past three decades, we have no clue that piracy in digital media has increased million times. Focusing on this fact, we should understand that number of people involved

have gained more or less the same amount of knowledge on such facts and thus are able to hit their targets more frequently. With the advent of networked appliances, mobile code, and pervasive access to the Internet, software protection has gained increasing importance. Digital media has become an inevitable part of our technologically active lives and piracy comes as an inhibitor drug that is an obstruction to unhindered growth. The authors survey current and promising new techniques designed to reliably preserve and protect digital media vital to our privacy and security.

Personal privacy, national security, and other fundamental values hinge on the ability to protect data from unauthorized access. As computing becomes pervasive, concerns about data protection have taken on new urgency. For example, obtaining unauthorized access to someone's medical history once would have required physically breaking into a doctor's office, searching through one or more filing cabinets, and extracting the patient's folder. Today, it is often possible to obtain such records by breaking into the doctor's computer from a remote location. What makes securing digital data difficult is that it is rarely static—rather, data is manipulated by software, often in a networked environment.

Software itself is a form of data and as such is vulnerable to theft and misuse. Given the enormous investment of time, money, and intellectual capital in software development, piracy has long been—and continues to be—a major threat to the software industry The problem, however, extends well beyond that of software piracy. Software is increasingly being distributed as mobile code in architecture-independent formats. Most such formats are essentially equivalent to source code, which makes the software susceptible to recompilation and reverse engineering. Malicious parties can steal the intellectual property associated with such code with relative ease. Clearly, there is a strong need for developing more efficient and effective mechanisms to protect software. Unfortunately, none of the major approaches currently used by software developers and vendors provide adequate protection, especially on today's open computing platforms. However, three promising techniques under development—tamper proofing, obfuscation, and watermarking.

2. Technologies to Prevent Piracy:

The various methods in which piracy control can be carried out in different economic sectors are given as follows:

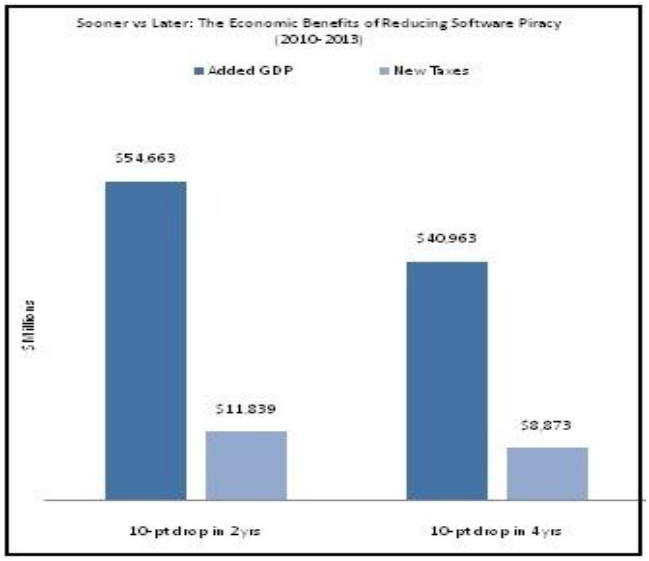
A. TAMPERPROOFING
B. OBFUSCATION
C. WATERMARKING

2.1 TAMPERPROOFIING

It is a technique to prevent any kind of modification done in the original code, which may be done through manual coding(user) or may be automated(virus).After detecting

the modification, the mechanism behind tamper proofing will sometimes disable the whole program functionality or sometimes partially.

Several technologies to provide defence in depth:



A plot showing the economic benefits of reducing software piracy

A.1 Checksum

It is not easy to conceal the nature of checks and so an attacker can easily patch around them once they are detected. To overcome this, checksum is a straight forward tamperproofing technique under which it examines the software program by comparing it with the original one right before it runs.

A.2 Guard

Guard is the mixture of many small program units which work together to prevent one another in the system. The main motive behind this was to prove wrong that the tamperproofing technology depends upon single module whose only purpose is to tamper the whole program, Hoi Chang and Mikhail atallah.[1] argues on this technique.By using number of guards, we prevent the program from running. Only by removing all guards can an attacker gain the program's full functionality which is highly improbable.

A.3 Assertion checking

It is based upon checking of intermediate program result. Let us take the situation of FIFO (first in first out). .[2] In this, the program fails if we try to enter more entries after a specified limit.

Some of the disadvantages under this are-

- Programs cannot recover from many bugs.
- A large number of intermediate checking can result in slow speed.
- This technology may be labour intensive
- There is no guarantee that after tampering, the program will always produce invalid intermediate results.

A.4 Cryptographic techniques

Cryptography scrambles a message so that it cannot be understood. It is a technique which ensures that the code will be decrypt only after it is loaded to XOM. .[4] It jumps to the decrypted part according to the sequence of pseudorandom values which is generated by the cryptographic key but this technique does not lend itself well to type safe .[3] languages like JAVA. David lie and his colleaguesadvocate added a new feature named as execute only memorywhich contains code that the machine user can only execute but not view.

2.2 OBFUSCATION

Obfuscation refers to the practice of disguising other software based protection mechanisms. This is created keeping in mind that the attacker should not be able to distinguish the program code that performs tamperproofing operations from other parts of the code through either manual inspection or tool assisted analysis.The practical goal of obfuscation is therefore to make reverse engineering uneconomical. Although obfuscation results in less efficient code, it is relatively cheap to perform and has aroused increased in interest in the past two years.

Types:

B.1 Lexical obfuscation

This involves renaming program identifiers to avoid giving away clues to their meanings but alone it is not sufficient as a determined attacker can infer the meaning of programs identifiers from the content.

B.2 Data obfuscation

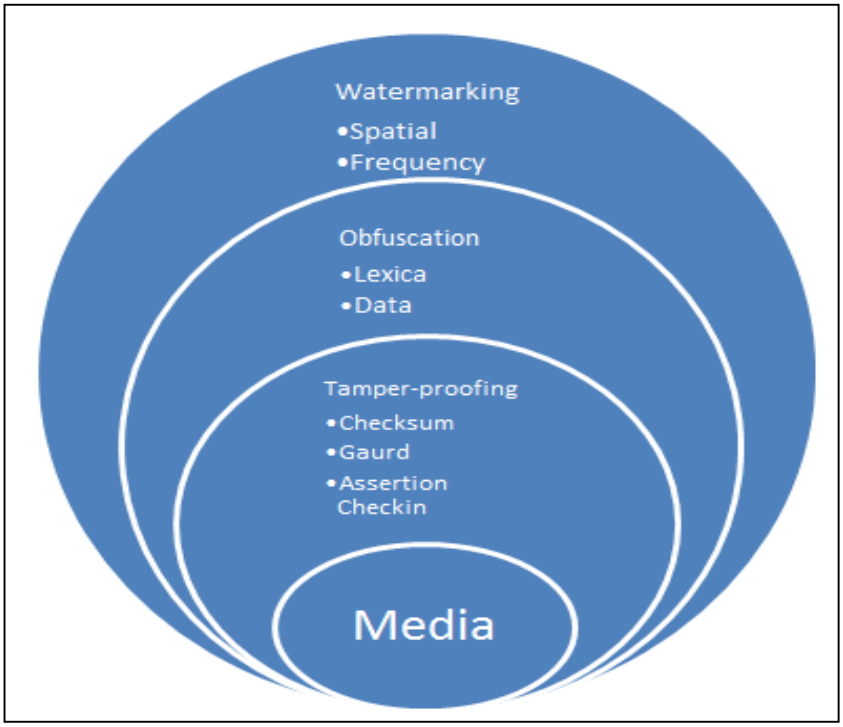
This approach obscures the purpose of program data fields. For example it is possible to replace an integer variable in the program with two integer variables in such a way that the original variable values at any point can be determined by adding the two new variable values.

Most recently, we have proposed more potent data type techniques that aim to obscure high level designs of object oriented programs by breaking the abstractions of classes.

1.It merges arbitrary classes into single class

2.It splits an arbitrary class into two classes related by inheritance.

3.It substitutes numerous interfaces for an arbitrary class, whenever possible, to obscure its purpose in the program design, specifies for JAVA with its concept of lightweight data structures.



2.3 WATERMARKING

It is a digital signature that is embedded in the media and is perceptually undetected. An effective watermark must have the following property:

1. It must be embedded in such a way that the quality of the media is not hampered.
2. It should be maintain the accuracy of the owner identification on its retrieval.
3. Watermark should be such that its removal or its editing is not possible for an attacker. It should be embedded in such that attempting or destroying the watermark should create notable deprivation in the quality of the media.

Digital media watermarking techniques are classified into these two categories:

C.1 Spatial-domain technique:

In this a watermark is embedded in least significant bits of randomly selected pixels. The watermark is actually invisible to human eye. However watermark will be destroyed if some common image operation like low-pass filtering is applied to the watermarked image. So to make the image unaffected we got to increase the bits of watermark, which as a result reduce the quality of image or cause hindrance. To meet both obscure and robust requirement we will adaptively modify the intensities of some

selected pixels as large as possible such that this modification is not visible to human eyes. The robustness is increased by using Darven and Scott proposed fractal-based steganography method. The watermark is also scrambled to digital watermark before it is inserted into an image.

C.2 Frequency-domain:
In this technique image is transformed into a set of frequency domain coefficients. Then the watermark is embedded in this transformed image coefficient with taking care that it is almost invisible. At last the coefficients are again changed into watermarked image.

3. TCPA

It stands for trusted computer platform alliance and is a collaborative initiative by a number of hardware, software and technology vendors to define specifications for a hardware assisted OS based, trusted subsystem that would become an integral part of computing platforms. It would use public-key cryptography and an enabling public-key infrastructure to assign a reliable identity to each pc or computing device. The TCPA subsystem would use public-key cryptography and an enabling public-key infrastructure to assign a reliable identity to each PC or computing device.This capability, combined with secure storage,trusted paths within the system, and a secure coprocessor for performing cryptographic primitives and random number generation, would let software vendors verify the trustworthiness of the environment within which their software is running. The subsystem could be used to grant access to sensitive data only to signed and trusted applications and could also protect applications from tampering. Although the eventual standardization and widespread availability of TCPA-enabled systems would go a long way toward protecting data and software on computing devices, several potential drawbacks may prevent universal adoption. Some object that vendors could use it to unfairly prevent consumers from switching to alternate products, while others fear that governments could use such a powerful mechanism for political censorship.Digital fingerprints can be used to identify individual copies of pirated software programs.

4. Conclusion

Considering the above mentioned advantages, we can solemnly conclude that it is our sheer responsibility to be a part of this never-foreseen campaign for encouraging use of piracy control techniques.The method is less talked about and less known to people at this point of time. This may be attributed to the fact that the methods discussed have some shortcomings that hackers take advantage of and do their tasks but even they have to admit that their job is made difficult It aims not only at eliminating piracy, but increasing the efficiency to such an extent that it will actually be impossible for us to even think of looking back.

We aim at diminishing piracy completely so we can have a piracy free digital sector for us and our future generations.

References

[1] H.Chang and M.J..Atallah,"seventh annual BSA Global Software PiracyStudy,"june2002;www.bsaa.com.au/media/FINAL7thAnnuaGlobalSoftwarePiracyStudyJune2002.pdf.

[2] D.Auscsmith,"Tamper Resistant Software:An Implementation,"proc.1st Int'l Workshop Ingormation Hiding,LNCS 1174,Springer-verlag,1996,pp.317-333.

[3] [3] Cummings et al., Simulation and Synthesis Techniques for Asynchronous FIFO Design with Asynchronous Pointer Comparisons, SNUG San Jose 2002.

[4] [4] D.Lie et al.,"Architectural Support For Copy and Tamper Resistant Software,"proc.9th Int'l Conf. Architectural Support for Programming Languages and Operating Systema,ACM Press 2002p,pp.168-177.