International Journal of Information and Computation Technology.
ISSN 0974-2239 Volume 3, Number 8 (2013), pp. 833-840

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

Software Piracy Prevention Using Image Splitting

Shweta Kamble

EXTC, Mumbai University, Versova , Mumbai , India.

Abstract

Software piracy continues to be a major economic concern for organizations. Given the high cost of producing software, development of technology for prevention of software piracy is important for the software industry. After identifying the fundamental weakness of existing piracy prevention, I propose a Software Activation Algorithm using image splitting technique; in which image is sliced into two parts, one part will be with the client and the other part will be with the trusted server. When user wants to activate the software; both parts of the image are made available to the server as well as the machine fingerprint (Hash codes of serial numbers of 'n' devices) of the users machine are sent to the server. After joining both parts, it will be matched with the original image using DCOS technique. This DCOS technique requires 100% matching of two images. Even if a single pixel is changed then the user is not authenticated by DCOS technique. In case of system failure Shamir's Secret Sharing technique is used to identify authenticated Users machine. Encryption/Decryption techniques will be used for Overall Security. This method not only makes It harder to create an additional available copy based on diversity, but also prevents illegal use of the Software.

1. Introduction

Today most of companies are affected by software piracy because of that it affects to their economic condition. In 2009 the piracy costs software industry near about $51 billion. Software piracy becomes major economic concern in today's life hence software anti-piracy is important. Antipiracy is attempt to prevent Copyright which is set of exclusive rules granted to author, Infringement means violation of rules &agreement of software, Counterfeiting is imitation of original manufacturer product and other violations of intellectual - property rights.

1.1Existing systems:

Software activation by product key or CD key. As a customer, you can activate your Software via a variety of methods. It's fast, secure, simple and anonymous. Product is activated using

- Online (Internet)
- Self service(for those with firewalls or proxy servers)
- Offline (email/phone licensing)
- License

Software piracy prevention techniques via software-splitting on client: In the software-splitting approach, the extracted critical segments refer to some codes. The developer may release a trial version of the software along with a key generator. When the user decides to purchase the full-function version, he could send the machine-related key back to the developers. The key is calculated in accordance with some machine characteristics like MAC address so that every key is user-relative and unique. When the developer receives the key, he could generate a last key and encrypt critical extracted contents, maybe critical resources or critical codes. After that, the developer sends the entire software back to the end user, including the main program; the extracted encrypt contents and the last key. When the user runs the software, the main program could decrypt those critical contents with the last key. When the key is valid, the contents decrypted would make the program continue executing normally, which represents that the software is authorized lawfully. Otherwise, contents decrypted with a wrong key would crash the main program or render some unreadable information.

Split Software into open and hidden components: splits software modules into open and hidden components. The open components can be installed and executed on an unsecure machine while the hidden components are installed on a secure machine.

The conventional methods to prevent software piracy fail largely because they rely on one method for the prevention of software piracy.eg CD key etc .Diversity in our project refers to the use of multiple methods to provide one solution to prevent software piracy, Furthermore each software is unique i.e. the crack for one copy of a software does not work on another copy of the software.

Me and my colleagues have made an innovative software which combines the elements of the existing antipiracy systems. Our approach has more than one piracy prevention techniques like key generation, computer identification and image splitting(innovation).Software is identified using an image rather than a key, and the image is split for security. As split image has no extension retrieving it is impossible. Also generating an exact replica of the image is not possible. The original image always stays with the server.

2. Concepts

It is important to understand a few concepts first to understand the algorithm.The concepts are explained below.

2.1 Diversity:

Our software identifies the fundamental weaknesses of existing approaches, resulting from the static nature of defense and the impossibility to prevent the duplication of digital data. A new scheme is presented that unravels a more dynamic nature of defense and makes it harder to create an additional, equally use full copy. Furthermore it enables a fine grained control over a distributed software. Its strength is based on diversity: each installed copy is unique and updates are tailored to work for one installed copy only. The importance of diversity is that it makes every software unique, uses different instance for every update ,Crack of one software does not work on other and it is useful against patches. Diversity in this project is achieved by using different concepts and combining it to together to make one unbreakable software.

2.2dcos technique:

The cosine similarity measure formula is used in our project to compare 2 images, after the second part of the image is received from the client and is then joined from the first part of the image from the server side, this reconstructed image is then compared with the original image from the server database. The cosine similarity measure formula gives values in the range from 1 to 0,0 indicating absolute similarity and a higher value i.e. a value near one indicating a large dissimilarity

$$\mathrm{Dcos}(A, B) = 1 - \left[\frac{\sum_{i=1}^{i=N} (ai \bullet bi)}{\sqrt{\left[\sum_{i=1}^{i=N} (ai)^2 \bullet \sum_{i=1}^{i=N} (bi)^2 \right]}} \right]$$

Figure 1: This diagram shows the formula used to implement Dcos Technique.

Here ai is one pixel in frame A and bi is the corresponding pixel in frame B. The value of Dcos varies from 0 to 1. A large value of Dcos indicates dissimilarity and a small value indicates similarity. While implementing Dcos in the program using C# the image file is first converted into bits and each bit is compared using the formula. 100% match is achieved when Dcos value is 0.

2.3 Shamir's Secret:

Shamir's Secret Sharing is an algorithm in cryptography, developed by Adi Shamir .It is a form of secret sharing, where a secret is divided into parts, giving each participant its own unique part, where some of the parts or all of them are needed in order to reconstruct the secret. We divide some data D (e.g., the safe combination) into n pieces in such a way that, Knowledge of any k(threshold number) or more pieces makes D easily computable.Knowledge of k-1 or fewer pieces leaves D completely undetermined (in the sense that all its possible values are equally likely). For example if there 4 keys and if we set the thresh hold number at 3 then only if 3 keys are combined then only the entire secret will be revealed If there are less than 3 keys which are combined the secret will not be revealed.

2.4 The AES:

Advanced encryption standards, is the algorithm we have used to encrypt our files before sending them across the server or client.Developed by Joan Daemen and Vincent Rijmen, who submitted a proposal which was evaluated and approved by the NIST i.e.national institue of standards and technology. AES is based on a design principle known as a substitution-permutation network, and is fast in both software and hardware,similar to the DES algorithm. The AES algoritthm has not been cracked till today. Microsoft visual studio has a build in function to implement AES . The keyword used to invoke this function is *Rijndael.* Thus the task to peform this algorithm becomes very easy and gives maximum security.

3. Algorithm

The developer may releases of the software along with CD key and Second part of image (say SPI).The SPI will be embedded with CD key. The server will have Original image, CD key and first part of image (say FPI).When user clicks on activate button registration form window will be display and it takes a device id's (Machine fingerprints) of system and convert it into hash code.Then it generate one key file containing hash code of device id's ,content of SPI and registration information of user.This encrypted key file is send to server.The server will decrypt the key file and extract the CD key.From CD key the server will find the original image and FPI from server database.After getting FPI, it is joined with SPI to get the full image.The image is then compared with original image associated with CD key using DCOS technique. This DCOS technique is used for comparison between two images which requires 100% matching. If the match is found then it generates one license file. This license file contains user information, content of SPI and hash code of device numbers i.e. f(x). Term f(x) is used because algorithm uses shamir's secret sharing scheme. basically it is used when user want to reinstall his software after formatting or after system crash due to some reason or in case of change any device from his system like Ram, Hard disk, Motherboard etc.In this case it checks some fixed number of device numbers with device number taken at the time of registration and if they matches then user is authenticated for using the software.Then after generating the license file it checks whether it full version or trial version. If it is for full version then it directly send the license file to the user else it show payment option window for trial version and then activate the software.Every time software starts it checks for device id's(machine fingerprints) and with hash code of device id's i.e. and f(x) and using Lagrange Interpolation it evaluates secret 'S' and compare it with secret 'S' in license file which is used in Shamir's secret sharing method .

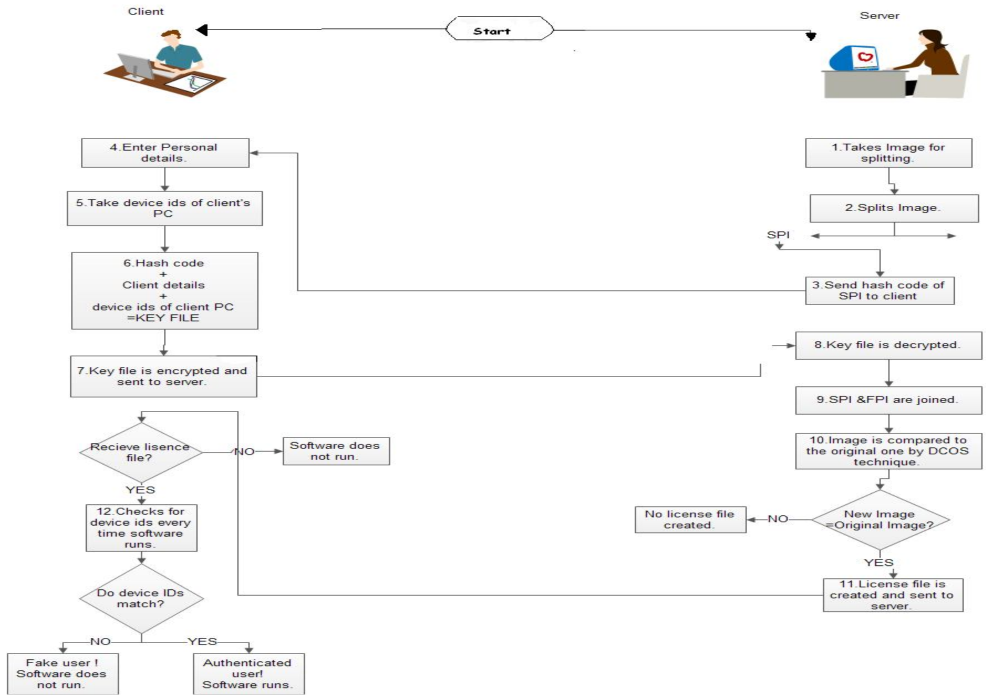
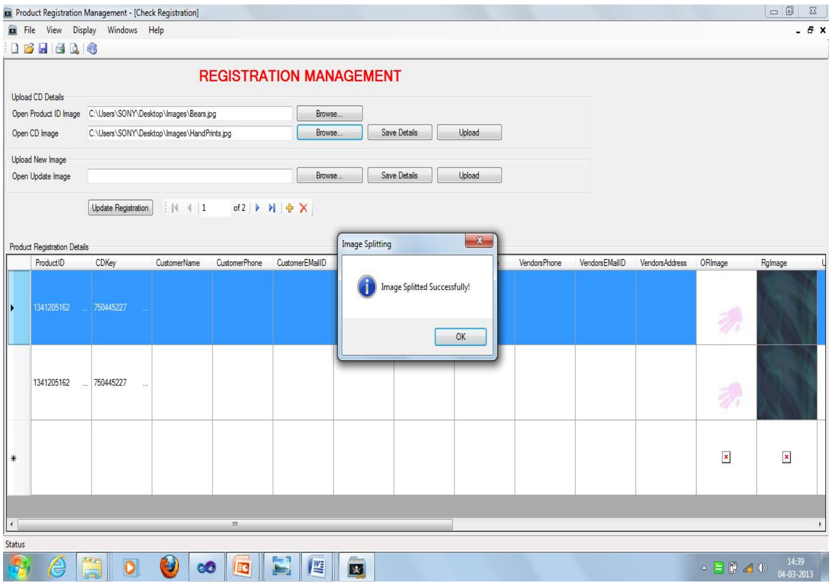

Client
Start
Server
4.Enter Personal details.
5.Take device ids of client's PC
6.Hash code + Client details + device ids of client PC =KEY FILE
7.Key file is encrypted and sent to server.
Recieve lisence file?
NO
Software does not run.
YES
12.Checks for device ids every time software runs.
Do device IDs match?
NO
YES
Fake user ! Software does not run.
Authenticated user! Software runs.
1.Takes Image for splitting.
2.Splits Image.
SPI
3.Send hash code of SPI to client
8.Key file is decrypted.
9.SPI &FPI are joined.
10.Image is compared to the original one by DCOS technique.
New Image =Original Image?
NO
No license file created.
YES
11.License file is created and sent to server.

Figure2: Diagram showing steps undertaken to know whether a user is authenticated or not.

4. Implementation

The project was implemented using the c# language in visual studio. Microsoft Visual Studio is an integrated development environment (IDE) from Microsoft and was so chosen as it can be used to develop console and graphical user interface applications along with Windows Forms applications, web sites, web applications, and web services in both native code together with managed code for all platforms supported by Microsoft Windows. Other built-in tools include a forms designer for building GUI applications, web designer, class designer, and database schema designer. It accepts plug-ins that enhance the functionality at almost every level—including adding support for source-control systems The coding was done in C-sharp language, C# language was chosen because it supports .net and SQL and is a multi paradigm language allowing usage of both classes and methods.



Product Registration Management - [Check Registration]

REGISTRATION MANAGEMENT

Upload CD Details

Open Product ID Image: C:\Users\SONY\Desktop\Images\Bears.jpg

Open CD Image: C:\Users\SONY\Desktop\Images\HandPrints.jpg

Upload New Image

Open Update Image:

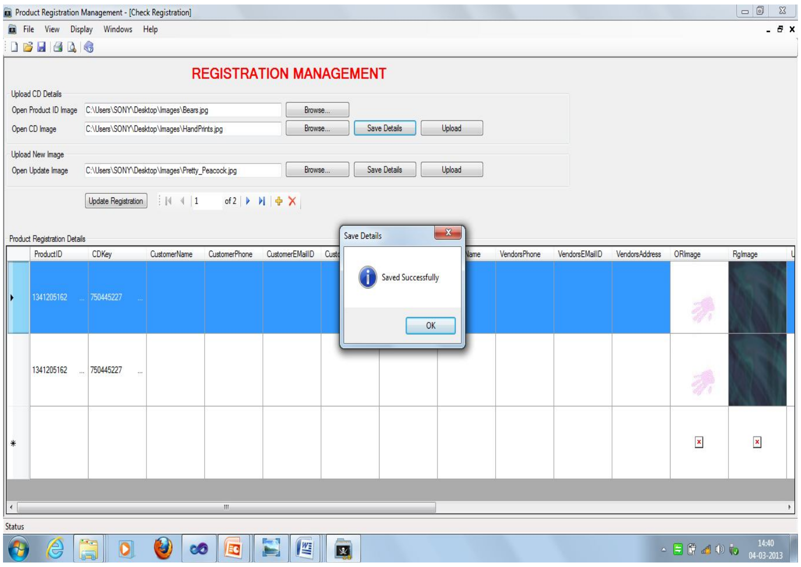
Image Splitting

Image Splitted Successfully!

Product Registration Details

ProductID	CDKey	CustomerName	CustomerPhone	CustomerEMailID	VendorsPhone	VendorsEMailID	VendorsAddress	ORImage	RgImage
1341205162 ...	750445227 ...								
1341205162 ...	750445227 ...								

Figure 3: This is the server screen,from this screen the software maker can choose which image he wants to split,for implementing the SIA. In this screen we have provided options for the loading of multiple images to be split and also to save them,for easy refrence a table of all the images in circulation and used for splitting is also provided. After the software maker has choosen which image he wants to use,the image gets splited into 2 parts,this screen shows the choosen image has been split successfully.



Product Registration Management - [Check Registration]

REGISTRATION MANAGEMENT

Upload CD Details

Open Product ID Image: C:\Users\SONY\Desktop\Images\Bears.jpg

Open CD Image: C:\Users\SONY\Desktop\Images\HandPrints.jpg

Upload New Image

Open Update Image: C:\Users\SONY\Desktop\Images\Pretty_Peacock.jpg

Save Details

Saved Successfully

Product Registration Details

ProductID	CDKey	CustomerName	CustomerPhone	CustomerEMailID	VendorsPhone	VendorsEMailID	VendorsAddress	ORImage	RgImage
1341205162 ...	750445227 ...								
1341205162 ...	750445227 ...								

Figure 4: After the user clicks on the save details button ,the two images called SP.001 and SP.002 are saved.

5. Conclusion

In this paper I have presented a technique to prevent software piracy using the algortithm involving splitting and recombing of an image and then checking if the software is running on a valid computor using Shamirs Secret Sharing algorithm.ME and my Colleagues have been able to achieve a technique which prevents sodtware piracy at the same time allowing miminum inconvinece to the end user of the software,we would also like to work towards making our method more robust and efficient.

The salient Features of this project would be that the Image cannot be generated An image is unlike text is extremely difficult to guess and create,hence a software pirate can never create or generate the entire original image.Sliced Image cannot be opened because of unknown extension The sliced images generated are given extension 001 and 002 thus there is no way to open them and view their original contents.Multiple authentications by image, CD key and activation remark.The split image algorithm works perfectly and the DCOS technique assures 100 percent accuracy i.e no tampering with the image is allowed.

References

[1] Basic Considerations for Preventing Software Piracy *Andre Armstrong and Vic Lu*

[2] Secuirty System For application copyright protection Makrand U Rahane Aushitosh K Patil

[3] Software piracy prevention through Diversity- Bertrand Anckaert,Bjorn De Sutter,Koen De Bosschere.Electronics and information’s department Ghent University.

[4] How to share a Secret Adi Shamir Massachusetts institute of technology Edited By R.Rivest

[5] Singhal, Amit (2001). "Modern Information Retrieval: A Brief Overview". Bulletin of the IEEE Computer Society Technical Committee on Data Engineering 24 (4): 35–43.

[6] Software Piracy Prevention: Splitting on Client Yawei Zhang, Lei Jin, Xiaojun Ye Dongqing Chen

[7] Advanced Cryptographic Protocols Marius Portmann

[8] ”Fourth annual BSA and IDC global software piracy study”Conducted by IDC May @007

[9] Software Security through Targeted Diversification Mantadelis TheofrastosDu Xiaodai

[10] Software Piracy Prevention Miichael Follk Research in Computer Science SeminarFebrruary 26, 2006

[11] Software Security through Targeted Diversification Nessim Kisserli Jan Cappaert Bart Preneel Katholieke

[12] Discrete Mathematics for CS Fall 2006 Papadimitriou & Vazirani.