International Journal of Enhanced Research in Management & Computer Applications
ISSN: 2319-7471, Vol. 6 Issue 2, February-2017, Impact Factor: 1.544

Study on Cryptography Analysis in Security Softwares using Media Access Control Address

Shashi Bala

M. Tech Student, Dept. of CSE, R N College of Engg., Rohtak, Haryana

ABSTRACT

Software Security is built to protect the privacy of its users. The software typically works in conjunction with Internet usage to control or limit the amount of information made available to third parties. The software can apply encryption or filtering of various kinds. Most retail programs are licensed for use at just one computer or for use by only one user at any time. By buying the software, you become a licensed user rather than an owner. You are allowed to make copies of the program for backup purposes, but it is against the law to give copies to friends and colleagues. In this paper License file generator using MAC address of the system that will provide security against piracy of the software application has been studied.

Keywords: cryptography, security, software, MAC.

INTRODUCTION

Software verifies activation every time it starts up, and sometimes while it is running. Some software even "phones home", checking a central database (across the Internet or other means) to check whether the specific activation has been revoked. Some software might stop working or reduce functionality if it cannot connect to the central database.

Computer software, or simply software, is that part of a computer system that consists of data or computer instructions, in contrast to the physical hardware from which the system is built. In computer science and software engineering, computer software is all information processed by computer systems, programs and data. Computer software includes computer programs, libraries and related non-executable data, such as online documentation or digital media. Computer hardware and software require each other and neither can be realistically used on its own.

Due to piracy and other forms of unauthorized use, users cannot always be sure that they have a genuine copy of software. The goal of product activation is to reduce a form of piracy known as casual copying. Casual copying is the sharing and installation of software that is not in compliance with the software's end user license agreement and is estimated to contribute to half of all pirated installations. Product Activation helps ensure that each copy is installed in compliance with the end-user license and is not installed on more than the limited number (usually one) of computers allowed by the product license.

At the lowest level, executable code consists of machine language instructions specific to an individual processor—typically a central processing unit (CPU). A machine language consists of groups of binary values signifying processor instructions that change the state of the computer from its preceding state. For example, an instruction may change the value stored in a particularstorage location in the computer—an effect that is not directly observable to the user. An instruction may also (indirectly) cause something to appear on a display of the computer system—a state change which should be visible to the user. The processor carries out the instructions in the order they are provided, unless it is instructed to "jump" to a different instruction, or is interrupted (by now multi-core processors are dominant, where each core can run instructions in order; then, however, each application software runs only on one core by default, but some software has been made to run on many).

The majority of software is written in high-level programming languages that are easier and more efficient for programmers, meaning closer to a natural language. High-level languages are translated into machine language using a compiler or an interpreter or a combination of the two. Software may also be written in a low-level assembly language, essentially, a vaguely mnemonic representation of a machine language using a natural language alphabet, which is translated into machine language using an assembler.

An online license management system helps reduce both forms of piracy by ensuring that each copy of the software product being installed is legal and has been installed on a PC in compliance with its license terms. Installations beyond those allowed in the license agreement will fail to activate, thus preventing both casual and intended piracy. 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. Another way is Product Activation. Product activation is a license validation procedure required by some proprietary computer software programs. Product activation prevents unlimited free use of copied or replicated software. Inactivated software refuses to fully function until it determines whether it is authorized to fully function. Activation allows the software to stop blocking its use. Activation can last "forever", or it can have a time limit, requiring a renewal or re-activation for continued use.

Software that has been installed but not activated does not perform its full functions, and/or imposes limits on file size or session time. Some software allows full functionality for a limited "trial" time before requiring activation. Inactivated software typically reminds the user to activate, at program startup or at intervals, and when the imposed size or time limits are reached. (Some inactivated software has taken disruptive actions such as crashing or vandalism, but this is rare.)

Some 'inactivated' products act as a time-limited trial until a product key—a number encoded as a sequence of alphanumeric characters—is purchased and used to activate the software. Some products allow licenses to be transferred from one machine to other using online tools, without having to call technical support to deactivate the copy on the old machine before reactivating it on the new machine.

LITERATURE REVIEW

Dr. Mohammed Abbas Fadhil Al-Husainy committed that in computer networking, the Media Access Control (MAC) address is a unique value associated with a network adapter. MAC addresses are also known as hardware addresses or physical addresses. TCP/IP and other mainstream networking architectures generally adopt the OSI model. MAC addresses function at the data link layer (layer 2 in the OSI model). They allow computers to uniquely identify themselves on a network at this relatively low level. In this paper, suggested data encryption technique is presented by using the MAC address as a key that is used to authenticate the receiver device like PC, mobile phone, laptop or any other devices that is connected to the network. This technique was tested on some data, visual and numerical measurements were used to check the strength and performance of the technique. The experiments showed that the suggested technique can be used easily to encrypt data that is transmitted through networks.

Ram D. Gopa G. Lawrence Sanders said that in an attempt to protect their intellectual property and compete effectively in an increasingly dynamic marketplace, software publishers have employed a number of preventive and deterrent controls to counter software piracy. Conventional wisdom suggests that reducing piracy will force consumers to acquire software legitimately, thus increasing firm profits. We develop an analytical model to test the implications of antipiracy measures on publisher profits. Our results suggest that preventive controls decrease profits and deterrent controls can potentially increase profits. Empirical results are also presented that support the proposition on the impact of deterrent controls on the extent of software piracy derived from the analytical model.

Laurie E. MacDonald et al. 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. 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.

Dag discussed that he provide an implementation of the Data Encryption Standard highly optimized for the Intel Pentium processor. His implementation improves DES encryption speed by more than 7.9% versus the best known previous result on the Pentium. Key setup speed is improved by more than 19%. This is achieved without increasing the size of lookup tables; a total of 4 kilobytes of lookup tables are used by his implementation.

Calloway discussed that this literature review looks at the research that has been published in the area of cryptography as it relates to network data and global communications security. It compares and contrasts the research pointing out overall trends in what has already been published on this subject. It analyzes the role that cryptography has played and will play in the future relative to security. This review addresses cryptography around the central theme of the security that it provides or should provide individuals, corporations, and others in the modern age of computing technology, networking, and Web-based ecommerce. By reviewing both scholarly and non-scholarly works, its objective to make a case that continuing research into the use of cryptography is paramount in preserving the future of electronic data security and privacy as well as the continuing development of Web-based applications that will permit the growth of ecommerce business worldwide to be conducted over the Internet.

Bin discussed that in view of Chua's circuit's characters and the deficient in DES algorithm, the paper presents a new image encryption scheme based on DES algorithm and chaotic encryption. The chaotic sequence is implemented in the DES algorithm to improve the initial keys and the iterating operations, so that the chaotic encryption is combined with DES algorithm. Theory analysis and simulation results show that the presented scheme can expand the initial key space, improve the security and anti-attack ability of the algorithm effectively. It is more propitious to image information transmission as this scheme insures the security and confidentiality of image information.

Ling et al. discussed that the initial sensitivity of chaotic map makes its application more and more widely. The image encryption algorithm based on chaotic theory is a hot researching field recently. Confusion and diffusion are necessary methods to realize the image encryption. However, using the initial sensitivity and randomness of chaotic map can realize the purpose of confusion and diffusion. S-DES system can encrypt the input binary flow of image, but the fixed system structure and few keys will still bring some risks. However, the sensitivity of initial value that Lu chaotic map can be well applied to the system of S-DES, which makes S-DES have larger random and key quantities. A dual image encryption algorithm based on S-DES and Lu map is proposed. Compared to traditional methods, it has some merits such as easy to understand, rapid encryption speed, large keys and sensitivity to initial value.

Alani discussed that the Data Encryption Standard (DES) has shown noticeable signs of aging during the last two decades. In this paper he develops a system that is a DES-varient with more resistance towards the possible attacks against DES. The develop system has a sub key generation algorithm that is completely different from original DES. The develop system uses 84-bit initial key instead of 56-bit key originally used. It has substitution boxes inside the key generation algorithm and mod2 additions. The choice of arrangement of substitution boxes in the main algorithm for each round is sub key dependent. The result of the design is a DES variant cryptographic system that has higher resistance against brute force attack, differential cryptanalysis linear cryptanalysis. The proposed system design also cancelled the weak keys and complement keys properties of the DES.

Hamami et al. discussed that Data Encryption Standard (DES) is a block cipher that encrypts data in 64-bit blocks. A 64-bit block of plaintext goes in one end of the algorithm and a 64-bit block of cipher text comes out of the other end. Blowfish is a block cipher that encrypts data in 8-byte blocks .Blowfish consists of two parts: a key-expansion part and a data-encryption part. Key expansion converts a variable-length key of at most 56 bytes (448 bits) into several subkey arrays totalling 4168 bytes. Blowfish has 16 rounds, such as DES. In this research the fusion philosophy will be used to fuse DES with blowfish and Genetic Algorithms by taking the strong points in all of these techniques to create a proposed Fused DES-Blowfish algorithm. The proposed algorithm is presented as a modified DES depending on the advantage in key generation complexity in blowfish and advantage of optimization in Genetic Algorithm to give the optimal solution. The solution will be the depended tool for creation of the strong keys.

CRYPTOGRAPHY SOFTWARE ANALYSIS

It is very important to have strong Product Keys and Activation Codes that could not be broken. One of the worst problems experienced by software developers is a possibility of appearance of so called 'key generators', or 'keygens'. Key

generators are created by hackers or hacker teams, and produce fake software licenses that are positively validated by the products they target.

For weak key generation schemes the hackers use reverse engineering in order to figure out an algorithm of validating a software license. After that they reverse the algorithm, and obtain the ability to produce fake license keys.
In order to counter this type of attack, we used a strong open key cryptography for license key generation. We implemented strong open key crypto software based on the HFE algorithm that uses a private key to generate license keys, and a public key to verify them. This is the opposite of the classical open crypto, with private keys used for decryption and verification, and public keys for encryption and signing. Our approach guarantees that it is impossible to reverse the license key verification algorithm to make a key generator, or produce a valid license code without knowing a private key.

Our Product Keys are generated as cryptographic signatures of a customer's name (all characters are converted to capitals, spaces and punctuation removed). Such a signature is a one-way function of a string, also known as a 'hash function'.

A cryptographic hash function is a special class of hash function that has certain properties which make it suitable for use in cryptography. It is a mathematical algorithm that maps data of arbitrary size to a bit string of a fixed size (a hash function) which is designed to also be a one- way function, that is, a function which is infeasible to invert. The only way to recreate the input data from an ideal cryptographic hash function's output is to attempt a brute-force search of possible inputs to see if they produce a match, or use a rainbow table of matched hashes.Bruce Schneier has called one-way hash functions "the workhorses of modern cryptography". The input data is often called the message, and the output (the hash value or hash) is often called the message digest or simply the digest.

The ideal cryptographic hash function has five main properties:

- It is deterministic so the same message always results in the same hash
- It is quick to compute the hash value for any given message
- It is infeasible to generate a message from its hash value except by trying all possible messages
- A small change to a message should change the hash value so extensively that the new hash value appears uncorrelated with the old hash value
- It is infeasible to find two different messages with the same hash value

Most cryptographic hash functions are designed to take a string of any length as input and produce a fixed-length hash value.

Encode Readable License Keys

The string encoding of product keys should omit confusing characters like. Using such characters in the key encoding makes it very easy for the user to enter the wrong key and then call the technical support department complaining that the purchased key does not work. For the same reason, product keys should also be case-insensitive, if possible. One possibility is to use a Base32-like encoding (each character encodes 5 bits) with the alphabet "ABCDEFGHJKLMNPQRSTUVWXYZ23456789".

A sensible solution, adopted by Microsoft, is to use 2346789BCDFGHJKMPQRTVWXY as alphabet, leaving 015AEILNOSUZ unused (Licenturion, 2001). In addition to what has been said, 5 could easily be confused with S, Z with 2 and using two lowercase n in a row could look like a m; these are therefore removed. Vowels AEIOU are avoided to cancel out the possibility of generating meaningful word in most Latin languages. Altogether, this alphabet has a base of 24. It might however be convenient to relax the readability constraints slightly to reach base 32 since it obviously maps easier into binary data, and a larger base will allow more information to be stored in the key.

License Reader

Vendor of product is considering as administrator and the administrator should have the power to view the license file. Application will provide two types of license reader i.e. virtual reader and real reader, virtual reader accept license file from the user as well as it will ask for MAC address and after the successful comparison of given MAC with the MAC address of license file, it will show the complete information of license file on the screen. Real reader will not work exactly as virtual reader but it is little different, real reader will be one of the module of the any product developed by vendor and when the product (application software) starts running it will read MAC address from the machine and compares the machine's MAC address with the decoded MAC address of file and after successful completion of this comparison it will allow user to access application.

Software Piracy

Software piracy is the unauthorized copying, reproduction, use, or manufacture of software products. On average, for every authorized copy of computer software in use, at least one unauthorized or "pirated" copy is made. In some countries or regions, up to 99 unauthorized copies are made for every authorized copy in use. Software piracy harms everyone in the software community including you, the end user. Piracy results in higher prices for duly licensed users, reduced levels of support, and delays in the funding and development of new products, causing the overall selection and quality of software to suffer.

Piracy harms all software publishers, regardless of their size. Software publishers spend years developing software for the public to use. A portion of every dollar spent in purchasing original software is funneled back into research and development so that better, more advanced software products can be produced. When you purchase pirated software, your money goes directly into the pockets of software pirates instead.

Software piracy also harms the local and national economies. Fewer legitimate software sales result in lost tax revenue and decreased employment. Software piracy greatly hinders the development of local software communities. If software publishers cannot sell their products in the legitimate market, they have no incentive to continue developing programs. Many software publishers won't enter markets where the piracy rates are too high, because they will not be able to recover their development costs.

CONCLUSIONS

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. 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. Also, a technique for data encryption has been presented which employ the MAC address of the receiver device to use it as a key for encryption. This technique made a good immunity for the data that is transmitted through networks.

REFERENCES

[1]. Alaa A.H, Mohammad A., Soukaena H.H, 2011. "A proposed Modified Data Encryption Standard algorithm by Using Fusing Data Technique", World of Computer Science and Information Technology Journal, Vol. 1, No. 3, pp. 88-91.
[2]. Said F.Z, Y.A.Nada, A.A. Abdo, 2011. "How Good Is The DES Algorithm In Image Ciphering", Int. J. Advanced Networking and Applications, Vol.02, pp. 796-803.
[3]. Visual Basic .NET Black Book by Steven HolznerW.Stallings, "Cryptography and Network Security" 2nd Edition, Prentice Hall,1999
[4]. W.Diffie; M.E.Hell man, " New Directions in Cryptography" IEEE Transactions Information Theory, Nov, pp 644-654.
[5]. Garfinkel, S.L; "Public Key Cryptography" , Computer, IEEE, Volume: 29, Issue:6, June 1996
[6]. V. Miller; "Uses of Ellptic Curves in Cryptography. In advances in Crptography, Springer Verlag Crypto 95.
[7]. An Open IP Encryption Flow Permits Industry-Wide Interoperability Published By:-Synopsys, Inc. Synplicity Business Group 600 West California Avenue,Sunnyvale, CA 94086 USA
[8]. Sumedha Kaushik and Ankur Singhal(2012), "Network Security Using Cryptographic Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 12.
[9]. 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).
[10]. Susan Athey and Scott Stern(2014), "The Nature and Incidence of Software Piracy: Evidence from Windows".
[11]. Thai Duong and Juliano Rizzo(2011), "Cryptography in theWeb: The Case of Cryptographic Design Flaws in ASP.NET", IEEE Symposium on Security and Privacy.
[12]. Walt Scacchi and Thomas Alspaugh, "Addressing Challenges in the Acquisition of Secure Software Systems with Open Architectures".
[13]. Daniel, L.C, 2008. "Literature Review of cryptography and its role in Network security", Principles and Practice , Capella University, pp. 1-20.
[14]. Bin G. and Qian, 2009. "A new image encryption scheme based on DES algorithm and Chua's circuit", International Workshop on Imaging Systems and Techniques, South university of Technology, Shenzhen, pp. 168-172.
[15]. Bin, L., Lichen, L., Jan Z., 2010. "Image encryption algorithm based on chaotic map, and S-DES", Advanced Computer Control (ICACC), 2nd International Conference, Information & Computer Engineering College, Northeast University, Harbin, China. pp. 41-44.
[16]. Alani M.M., 2010. "DES96-Improved DES Security", 7th International Multi conference on Systems, Signals & Devices, Gulf Univ., Gulf, Bahrain, pp. 1-4.