Висновок

Таким чином, зроблено крок у сторону покращення роботи з базами даних. Цей крок є надзвичайно важливим, оскільки велика частина функціональності СКБД вважається вже максимально оптимізованою і важко знайти ще щось, щоби могло пришвидшити її роботу.

Ось чому будь-який крок в цьому напрямку є надзвичайно важливим та потрібним.

[1] Кнут Д. Искусство программирования для ЭВМ. Сортировка и поиск.-М.:Издательський дом «Вильямс», 2000.-832с

[2] Мартин Дж. Организация базах даних в вичислительных системах.М.:Мир,1980.-644с.

[3] Цегелик Г.Г. – Организация и поиск информации в базах даних,-Львов:Вища школа,1987.-176с.

[4] Цегелик Г.Г. – Системы распредельонных базах даних.-Львов:Свит,1990.-168с.

[5] http://www.postgresql.org

Anti-Forensic Tool Using Double Encryption Scheme

Avtar Singh, Kuldip Singh

Electronic and Computer Science Department, Indian Institute of Technology Roorkee, Roorkee, India, E-mail: avtarpec@iitr.ernet.in, ksconfcn@iitr.ernet.in

Abstract – In this paper we are implementing an Anti-Forensic tool that is used in data hiding approaches of the Anti-Forensic technology. This tool will encrypt a secret file twice: firstly it is encrypted with the XOR and then by the powerful AES (Advance Encryption Standard). To make XOR strong we have used three files that are selected by user. These files will create a mess with the plain text before encryption making the cipher text more secure and harder to break.

Keywords - component; network security; forensic; anti-forensic; encryption.

I. Introduction

According to Saferstein, forensics is ‘‘the application of science to those criminal and civil laws which are enforced by police agencies in a criminal justice system’’ [1]. The dictionary definition of the word “anti” is “opposed to” or “against”. So now if we define Anti-Forensic it resembles the methods used to prevent or act against to the application of science to those criminal and civil laws that are enforced by police agencies in a criminal justice system. Peron and Legary pinpoint Anti-Forensics as the attempt to “limit the identification, collection, collation and validation of electronic data” so that the crime investigation is hindered [2]. This definition is not complete however, since it disregards the analysis of the evidence. Evidence analysis is essential to the forensic process; therefore, we must include it if we list each phase in our definition. Another definition by Grugq identifies Anti-Forensics as “attempting to limit the quantity and quality of forensic evidence” [3]. This definition is useful as well, but it only considers the evidence and completely ignores the forensic process. According to Ryan Harris Anti-Forensic is considered to be to be any attempts to compromise the availability or usefulness of evidence to the forensics process. Compromising evidence availability includes any attempts to prevent evidence from existing, hiding existing evidence or otherwise manipulating evidence to ensure that it is no longer within reach of the investigator. Usefulness maybe compromised by obliterating the evidence itself or by destroying its integrity.

In this paper we will focus mainly on data hiding approaches used in the Anti-Forensic process. There are various forensic tools like EnCase [2], FTK [3], and etc., and they have powerful functionalities relevant to computer forensics. However, the situation is different from the past. Criminals are no more in the level of “script kids” about computers and anyone can get various Anti-Forensics (AF) tools [4] from Internet. Dr. Marcus Rogers classified AF into four categories in [4]: data hiding, data wiping, trial obfuscation, and attacks against the computer forensic process or tools. The first can include encryption and Steganography.

II. Related work

The proposed scheme in the paper [5] consists of three stages. In the first stage, a user encrypts his own private file, P, using available cipher algorithm, E, and its key, KE. The encrypted file, C1, can be expressed as C1 = E(P, KE). In the second stage, the user selects some files and copies data block with the same size as C1 from each file. No one but the user has knowledge about the files. The copied data blocks are XORed with each other, and its result, kXOR, is encrypted into KXOR by the same manner as used on P. Thus, KXOR can be expressed as KXOR = E(kXOR, KE).

The problem found in this scheme was the double encryption algorithm that to by AES is time consuming. So we decided to propose an idea that can efficiently decrease the consumption of time and even increase the security. Therefore we have proposed a new idea by modifying its approach. Our proposed scheme is explain in the next section.

III. Our proposed scheme

Our scheme also consists of three stages. In the first stage, a user encrypts the three files, F1, F2 and F3 by XORing them together to make kXOR. Then with the help of key kE generated by the password specified by the user, we create a digest using MD5 with SHA-1 hashing technique for this kXOR. This digest obtained is called KXOR. In second stage this KXOR is XORed with the plain text to get the encrypted plain text and then is encrypted using AES with the help of key KE generated again with the same password.

This generated Crypt Text C is the final encrypted message for the corresponding plain text P as input.

The Encryption process used in our scheme is diagrammatically shown as below:

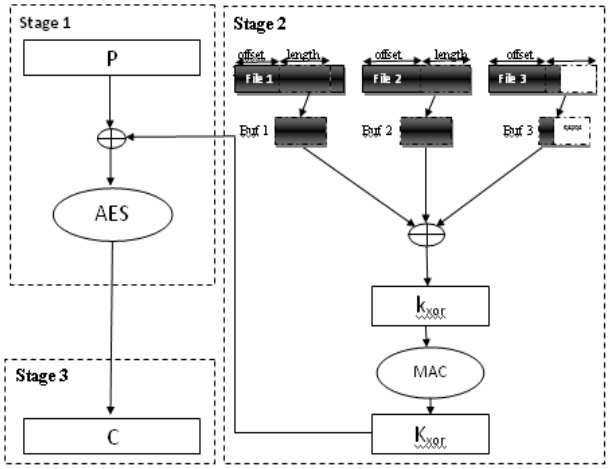

Figure1. Encryption Procedure

The Decryption processs also can be described as the reverse of Stage 1 and Stage 3 as below:

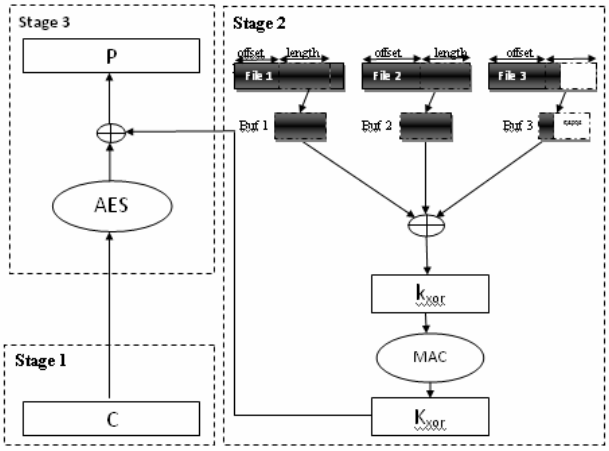

Figure 2. Decryption Procedure

IV. Prepare Your Paper Before Styling

Before you begin to format your paper, first write and save the content as a separate text file. Keep your text and graphic files separate until after the text has been formatted and styled. Do not use hard tabs, and limit use of hard returns to only one return at the end of a paragraph. Do not add any kind of pagination anywhere in the paper. Do not number text heads-the template will do that for you.

Finally, complete content and organizational editing before formatting. Please take note of the following items when proofreading spelling and grammar:

Abbreviations and Acronyms

The results are compared with the algorithm used in [5]. It proves the new approach is optimized with respect of time, speed and security.

The results are evaluated by varying the file size used for encryption. The execution time of the process is calculated for each file and the results are evaluated.

The results of both the New Algorithm and the Old Algorithm implemented in [3] are shown below in the table.

TABLE 1

COMPARISON RESULTS OF TWO ALGORITHMS

File Size (in MB)	Execution Time (in Seconds)	
	New Algorithm	Old Algorithm
1	29.1	39.7
5	214.9	341.4
25	872.3	1257.9
50	1872.6	2693.4
100	3219.5	4270.4

The Results shows that the Execution time of the Old Algorithm is high as compared to the New Algorithm. This shows the performance in comparison of speed of the New Algorithm is better than that of Old Algorithm. These results are shown in the graphical form as below.

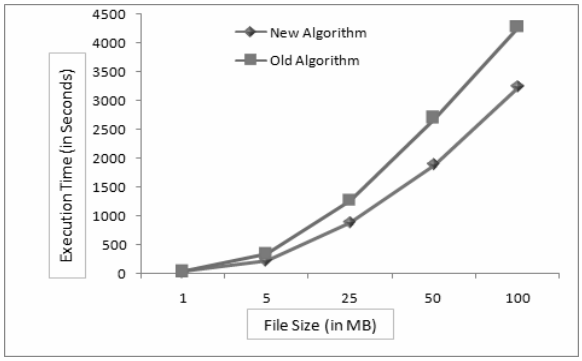

Fig 3 : Comparison Results of Two Algorithms

These results can be proven theoretically also as the Old Algorithm and New Algorithm uses same specification but the only difference is the no. of time it does the encryption and no. of hashing. This difference can be shown in the table as below.

TABLE 2

ALGORITHM SPECIFICATIONS

Comparison criteria	New Algorithm	Old Algorithm
Size of key	128 bit	128 bit
No. of Encryption (AES)	1	2
No. of hashing (MAC)	1	0

As we can see in the table above that the no. of Encryption that is AES encryption in Old Algorithm is 2 times whereas New Algorithm uses Encryption once and hashing once. Time taken for the process depends on AES and MAC algorithm. Since MAC is much faster than AES. Therefore the execution time of the New Algorithm is faster.

In implemented scheme in which a secret file is encrypted twice: one by a common encryption algorithm like AES and another by XOR. Despite the first key is revealed by guessing or dictionary-based attack, the attacker cannot

reconstruct the original secret until knows the files used to derive the second key block according to our scheme.

References

[1] Saferstein RE, "Criminalistics: An Introduction to Forensic Science", 6th ed. Upper Saddle River, NJ: Prentice Hall, 1998.

[2] Peron CSJ, Legary M, "Digital Anti-Forensics: emerging trends in data transformation techniques", 2002.

[3] Grugq, "The Art of Defiling: Defeating Forensic Analysis", Blackhat briefings, 2005.

[4] Ryan Harris, "Arriving at an Anti-Forensics Consensus: Examining How to Define and Control the Anti-Forensics Problem", DFRWS, 2006.

[5] Sang Su Lee, Ku-Young Chang, Deokgyu Lee, Dowon Hong, "A new anti-forensic tool based on a simple data encryption scheme", FGCN, 2007.

Методи аналізу функціонування Веб-форумів

Юрій Сєров, Руслан Кравець, Віктор Сівокозов

Кафедра інформаційних систем та мереж, Національний університет "Львівська політехніка", УКРАЇНА, м.Львів, вул.С.Бандери, 12, E-mail: syerov@ridne.net, rkravets@ua.fm

Abstract – Article considers actual problem of Web-forum efficiency analysis research and developing. Methods of analysis of Web-forum members quantity increasing and amount of content growth are described.

Key words – Web-community, forum, members, content, web-forum, efficiency analysis methods.

I. Вступ

Для кожного власника та адміністратора важливою є задача моніторингу та аналізу стану та процесу життєдіяльності його Веб-форуму. Проте жодна з перелічених СУІН не забезпечує адміністратора якісними засобами моніторингу та аналізу. У переважній більшості випадків за допомогою СУІН адміністратор Веб-форуму може отримати лише дуже обмежений набір статистичних даних (кількість повідомлень за день, кількість учасників, які відвідали форум протягом доби, загальну кількість повідомлень та дискусій Веб-форуму, найактивніші дискусії, найатрактивніші дискусії, найактивнішого учасника за день, множину учасників, які сьогодні святкують день народження і т.д.), але жодна СУІН не надає можливості спостерігати велику кількість важливих показників(позицію форуму, динаміку створення повідомлень та дискусій, динаміку зростання інформаційного наповнення Веб-форуму, найактивніші підфоруми, динаміку активності учасників, наповнення підфорумів, розподіл аудиторії учасників по підфорумах і т.ін.).

II. Аналіз стану Веб-форуму

Аналіз стану Веб-форуму зводиться до визначення його показників ефективності. Чотири з наведених критеріїв ефективності, а саме: кількість зареєстрованих учасників, об'єм інформаційного наповнення, швидкість приросту інформаційного наповнення, швидкість приросту кількості учасників, можна визначити на основі даних, що містяться в базі даних форуму, однак для цього треба розширити функціональність існуючих СУІН. Розширення функціональності полягає у доопрацюванні програмної частини СУІН з метою вирішення задач визначення ефективності Веб-форуму. Розробка нових програмних засобів, у свою чергу, передбачає розширення схеми бази даних для проведення необхідного аналізу стану Веб-форуму, визначення показників ефективності Веб-форуму, а також моніторингу та можливого прогнозування його розвитку.

Аналіз стану Веб-форуму згідно з критеріями ефективності будемо проводити у двох напрямках – окремо будемо аналізувати учасників Веб-форуму та його інформаційне наповнення. У свою чергу аналіз учасників Веб-форуму можна проводити у двох напрямках – аналіз появи нових учасників та діяльність існуючих. Аналіз збільшення інформаційного наповнення будемо проводити з точки зору його поділу на типи, тобто зростання кількості повідомлень та зростання кількості дискусій. Усі ці показники діяльності Веб-форуму є взаємозалежними. Скажімо, зростання кількості учасників вказує на актуальність та атрактивність інформаційного наповнення Веб-форуму, і в свою чергу веде до збільшення кількості інформаційного наповнення. І навпаки, збільшення кількості цікавого контенту призводить до збільшення кількості відвідувачів, і як наслідок – учасників. У свою чергу зменшення приросту нових учасників призводить до зменшення активності існуючих.

Для забезпечення стабільної діяльності та розвитку Веб-форуму необхідно, щоб показники ефективності на великих часових проміжках були неспадними.

A.Аналіз приросту учасників Веб-форуму та їх діяльності

Аналізуючи Веб-форум з точки зору його учасників і їх діяльності почнемо з аналізу приросту учасників. Першою дією людини, яку їй потрібно зробити для того, щоб стати учасником Веб-форуму є реєстрація. У більшості випадків процедура реєстрації є типовою – необхідно задати своє ім'я та пароль, а також інші дані, які можуть бути обов'язковими або ні - такі як електронна пошта, дата народження, тощо.

Аналіз приросту учасників

Досліджувати учасників Веб-форум почнемо з аналізу їх приросту. Людська природа така, що одна людина дуже рідно може постійно бути активним учасником Веб-форуму, як правило, з часом активність