Implementation of Clipboard Security using Cryptographic Techniques

Gaurav Pathak
Department of Computer
Science and Engineering
Lovely Professional University
Phagwara, India

Gaurav Kumar Tak
Department of Computer
Science and Engineering
Lovely Professional University
Phagwara, India

ABSTRACT

In the present scenario malicious authors are rapidly growing and now other than internet users they are also targeting the loophole in operating system application level security. Transferring data between applications is common user activity. Since data in a clipboard is freely delivered between arbitrary programs capable of using a format of the data, a simple text, a rich text, a picture, and information having a particular format may be delivered between programs capable of using such information. Information delivery made between programs through a clipboard is undoubtedly an efficient method of properly using a multitasking function of an operating system, but as the security of important data is increasingly demanded, data transmitted between independent programs through the clipboard needs to be protected. Any malicious application with get through from the protection system can easily watch the content of our clipboard and can modify the content during copy paste operation. In this paper implementation of a prototype model for clipboard security of operating system is presented, as we know that whole operating system has a common clipboard which acts as channel for inter-application operability. In our approach we prevent the clipboard data by encrypting the content at the time of copying & cutting and decrypting at the time of pasting, for this we use cryptographic techniques.

Keywords

Clipboard Data Security, Copy-Paste Operation, Operating System Security Enhancement.

1. INTRODUCTION

In present time internet is backbone of our society. From a child to old man all are somehow connected to internet, because internet is like ocean of information. Everybody needs internet, as it is growing with exponential rate and web applications are also growing. On the other side malicious author are also making internet users as their prime target.

People used to perform copy/cut and paste operation much frequently then typing anything making the use of clipboard. The clipboard is the common operating system component which enables application to transfer data among other. An application places data into the clipboard with the cut or copy operations and other applications can retrieve the data from the clipboard with the paste operation [1]. So user’s habit to cut/ copy paste provides malicious application and malware a loophole in security at client based system [4]. So security of important data is increasingly demanded, data transmitted between independent programs through the clipboard needs to be protected. There can be many attack or applications which can register themselves as clipboard event viewer and observe the clipboard content and can capture to modify it [2]. In attack name Hitchbot [2] they deliver malicious content by getting the clipboard content and modify it with similar looking malicious content. So security to clipboard content is issue of concern and need to enhance the functionality of operating system by which we can protect our clipboard data from being got watched.

From the study of recent papers and market reports, clipboard security becomes important issue of concern in data security. According to the google forum [6] there is being the great threat to the clipboard security in which they talk about ClipNote that can monitor the system clipboard and collect all clipboard entries. That ClipNote application does not require any special permission to run. That means any malware can steal passwords by just monitoring the system clipboard in the background, which become great threat to the client’s system. In this client is unaware of monitoring process going on clipboard in background. In Security threat report 2013 [12] they have reported Morcut/Crisis, a very sophisticated and potentially dangerous spying malware, which can remotely monitor user’s communication like: mouse events, clipboard content, IM, running applications, keystrokes monitoring, web URLs etc.

In a Technical White Paper [11] about Reversal an Analysis of Zeus and SpyEye Banking Trojans provide a technical analysis of Bot’s advanced hooking and injection mechanism and functionality how it hijack and steals user information. This malware make use of windows API & hooks to steal the content of clipboard also by hooking the GetClipboardData function, it can only able to hook if clipboard data is text, by hooking it store text in encrypted log file and if data is not text, this function returns normally. It means if we place data on clipboard in encrypted form then no malware can steal our data.

In [7] [8] & [14] there has been recent news about a malware who hijack the clipboard and put a weblink which lead the user to selling fake software. The attack on the clipboard has hit both Windows and Mac users of the Firefox web browser. In Clipboard Snooping Malware [9] also describe about how they snoop the clipboard operations by hooking SetClipboardData and GetClipboardData to steal the user information from clipboard. In this they register themselves as the clipboard viewer and get notification whenever data of clipboard changes. In [13] Bromium vSentry they talk about protection of system clipboard with the help of IT policies, access control and format conversion restriction, but still if any application register itself as clipboard viewer can easily access the clipboard data.

In this paper implementation of a prototype approach for system clipboard security using cryptographic techniques is presented. We are proposing an enhancement for clipboard security so that copy/cut and paste operation can be made more secure. We have implemented this approach in which we encrypt the copying data to the clipboard and decrypt on paste operation.

2. PROBLEM DEFINITION

After analysis of above mentioned Attacks and Malware regarding clipboard we need to provide a mechanism which can prevent our clipboard being hijacked and monitor, because if any unauthorized application can register itself as the clipboard viewer and can monitor the clipboard content.

In [14] they restricted through help of policies, access control but still there is need of some mechanism which can provide security on data itself so that any unauthorized user can't be able to watch our original data on clipboard.

3. RELATED TECHNOLOGY PRINCIPLES

3.1 What are Clipboard and its Working?

Clipboard is the special memory zone which is used in the operation of transferring data. In this user copy the selected data into the clipboard and copy that data from clipboard to somewhere in memory or disk that user specified called as paste operation [5]. There are distinct mechanisms for interfacing to the Clipboard that is Windows Clipboard API the most common method used. Windows clipboard in the inter-process communication mechanisms are: If an application needs to pass data to another application, then the application of providing data first need to create a global memory space by calling the function OpenClipboard, and then by calling EmptyClipboard function empty the memory space.

SetClipboardData is the function which is called when data is provided by any source application (e.g. 1) and store that in global memory. The application (e.g. 2) of receiving data (which may be multiple) must first obtain the address of this piece of the global memory space by calling the same function OpenClipboard. And then it can take the appropriate read operation to the data information in the memory space by the function GetClipboardData [3]. Working of clipboard using SetClipboardData and GetClipboardData functions is shown below:

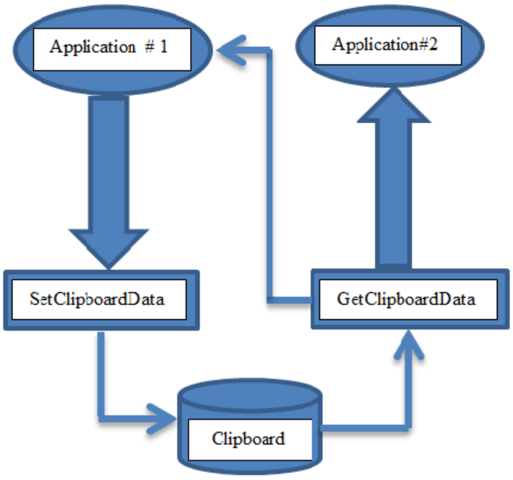


Fig 1: Working Mechanism of Clipboard

3.2 Encryption Processes and Techniques.

Encryption is the process to converting plaintext information into cipher text or in hidden form. Encryption techniques can be distinguished on the basis of key used. If the same key is being used for encryption and decryption process then it is called secret key or symmetric cryptography, and if different key is being used for both processes then it is called public key or asymmetric cryptography. Symmetric algorithm include DES, Double DES, AES, 3DES etc. and asymmetric algorithm include RSA, Digital signature, Message Digests etc. [10]

In our application we have implemented with both symmetric algo and asymmetric algo using DES and RSA respectively. DES (Digital encryption Standard) is a symmetric algo which use the block cipher of 64 bit and 56 bit key. It uses the concept of substitution and permutation. It's a 16 round process. RSA is asymmetric algo which use the concept of public and private key [10][15]. We use encryption at the time of copy/cut and at paste operation we use decryption process, so that during the mean time when data is at clipboard, remain in encrypted form.

4. APPLICATION OF CLIPBOARD SECURITY USING CRYPTOGRAPHIC TECHNIQUES

4.1 Proposed Methodology and Solutions

In order to get prevention from above mentions malware monitoring of clipboard and hijacking of text from clipboard some enhancements are proposed in operating system functioning like:

1. Operating system should restrict accessing API hook, access should be under some IT policy. Malicious application should be restricted at application level only.
2. Operating system should secure the clipboard content with the help of encryption algos.
3. Conversion of encrypted data into original text should perform by operating system for application separately.
4. Clipboard data access for should be only accessible to internal function of operating system.

Implementation of solution to make system clipboard secure against malicious applications by encrypting the clipboard content is shown. Our algorithm is as follows:

Step 1: Open any application (e.g. Editor Application)

In editor application we have functionality of copy/cut & paste over text.

Step 2: Select text for copy or cut.

Step 3: Perform Encryption using Cryptographic algo.

3(a) when we select any amount of text for copy execution of DoEncryption ( ) function encrypt the selected data using DES, AES or RSA.

3(b) After DoEncryption ( ) function encrypted data is placed at system clipboard by using function clipboard.setContent( ).

Step 4: Check the encrypted system clipboard.

4(a) Open start menu of OS.

4(b) Go to run.

4(c) Type clipbrd.exe

By these we can see encrypted system clipboard.

Step 5: Paste the selected data on application

When we paste selected data into the application we get decrypted data in original text form.

4.2 Application of clipboard security in system

Clipboard security system using cryptographic techniques achieves security of clipboard content from watching of unauthorized application, encryption technique has been used so that whenever there is any content for copying it first get encrypted and then it got placed over system clipboard, so that any malicious application registered as clipboard viewer cannot able to get original data from clipboard. And on the pasting time it gets decrypt first and then data is pasted on the application. In this application focus is made on the copy/cut operation of windows operating system, in this application we encrypt all the copied text using algos and secure clipboard from unauthorized clipboard viewer.

Emphasis is made on the copy/cut operation using keyboard shortcuts Ctrl+C, Ctrl+X & Ctrl+V because computer users use these shortcuts frequently rather than using button for copy paste. In our application we customize the windows API for copy/cut in such a way that whenever any text data is being copied from our application it first encrypt all the selected text and place that encrypted data on clipboard, so that no unregistered clipboard viewer application cannot watch the content of clipboard in text form, which provides protection from the various attack on clipboard as mentioned in [11]. Flowchart for the system clipboard security is shown below.

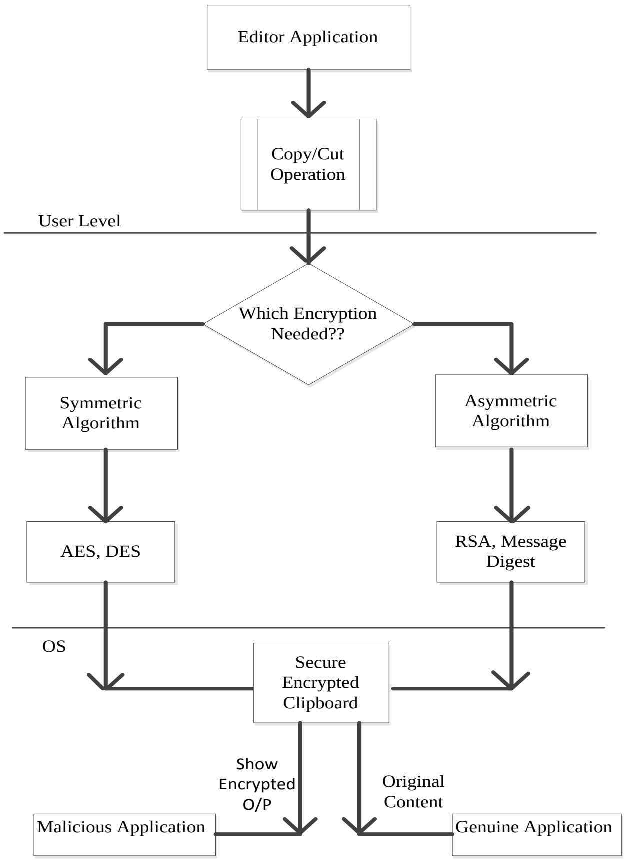


Fig 2: Flowchart of System Clipboard Security

In above figure flowchart is shown that when we copy any text from our application at user level then with any one cryptographic technique we have apply encryption to the system clipboard and secure clipboard contents from malicious applications in operating system, on system clipboard we get data in encrypted form in case of DES it'll be in binary form and in case of RSA it'll be in integer form.

Implementation of a prototype for operating system is shown to designer, they should implement this security of clipboard for whole system applications so that whenever there is any inter-operability among applications via clipboard then content placed at clipboard will be secured. When malicious application hook the clipboard function GetClipboardData, it get only encrypted data whereas when authorized system

Application hook SetClipboardData and GetClipboardData to access the clipboard it can access normal original content.

In our application when we select text to being copy then selected text first get encrypted by user defined DoEncryption ( ) function and placed in encrypted form at clipboard until DoDecryption ( ) function is being called by user for pasting the text into application.

4.3 Features of Clipboard Security Application

In order to provide security to clipboard from malicious applications from being watched, this prototype approach should be implemented as a feature of further coming operating system. Operation of copy/cut & paste which involve clipboard functioning as major part is now made secure. Clipboard security application can be use basis platform for most security needed enterprises like online trading, banking systems, intelligence & military systems where security is the atmost requirement. In these areas a small loophole can cause severe threat to security. Here inter-application communication is done through copy/cut & paste operation via clipboard, so clipboard need to be most secure from all kind of online and offline attacks. Figure below showing the interaction between two applications of operating system.

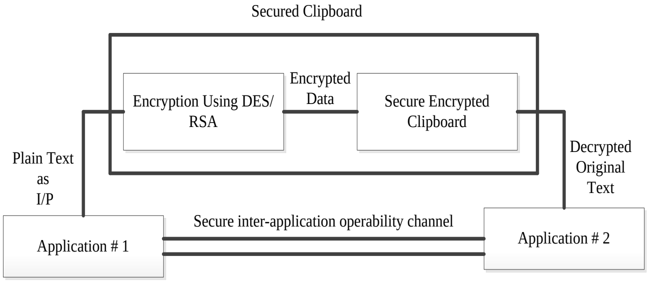
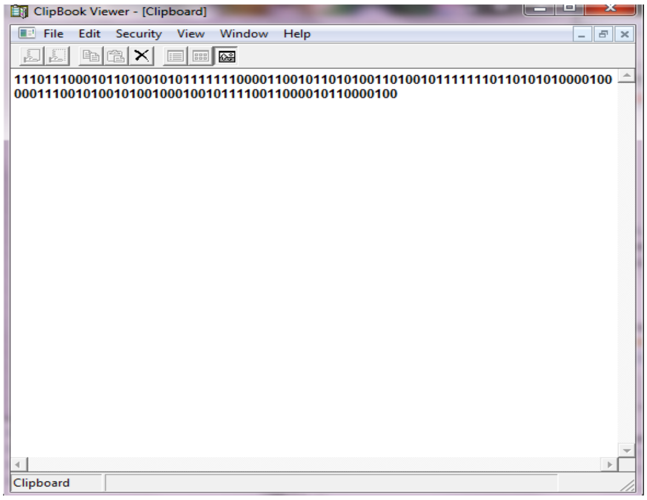


Fig 3: Interaction between two applications through secure channel

In above figure we have implemented secure clipboard approach between two applications of OS through secure channel within the system, if such functionality is implemented as system functionality then no external malicious application can play with system clipboard and we can get prevention from Zeus and SpyEye Banking Trojans which catch the text present in clipboard [11] In which if this Trojan get data in text form it'll capture else it will return normally.

5. Implementation & Results

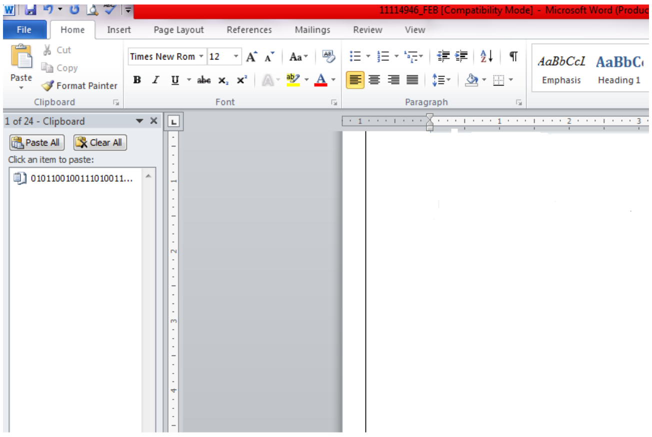
Implementation of this clipboard security application is done on windows 7 operating system, processor 2.00 Ghz, RAM 2.00 Gb using java as platform. We successfully encrypted the system clipboard. When any malicious application register itself into clipboard viewer list then it can able to watch only encrypted data in clipboard. After performing encryption for clipboard, we can access the clipboard in windows in just three steps: ① Go to start menu; ② Type run in search; ③ Open Clipbrd.exe, by opening clipboard we can watch encrypted system clipboard. Figure of system clipboard containing encrypted data is shown below:



```
111011100010110100101011111110000110010110101001101001011111110110101010000100
000111001010010100100010010111100110000101100000100
```

Fig 4: Encrypted Content in System Clipboard

In above figure we can see system clipboard is being secured with the use of encryption algo, it means if any malicious application as clipboard viewer want to watch the clipboard data it can only get encrypted content. For example: if suppose unfortunately any malicious application named svc.exe bypass through antivirus scanner of user's system and register as clipboard viewer, when this application view clipboard content, it can view only encrypted data. We can also watch encrypted system clipboard at Microsoft Word, which has functionality to watch clipboard content as shown below:



0101100100111010011...

Fig 5: Encrypted system clipboard at MW

In above figure we can see encrypted system clipboard through very common editor application Microsoft Word (MW), as which is showing that whole systems clipboard is being secured from any malicious eavesdropper. We have successfully protected our clipboard data from malicious application because malicious application will only able to watch encrypted data. DES, AES and RSA has different amount of encryption and decryption time and memory usage which vary with the different data size and machine. On our machine AES and DES both come up with less execution time (in milliseconds) encryption and decryption while RSA has also high memory usage in terms of bytes.

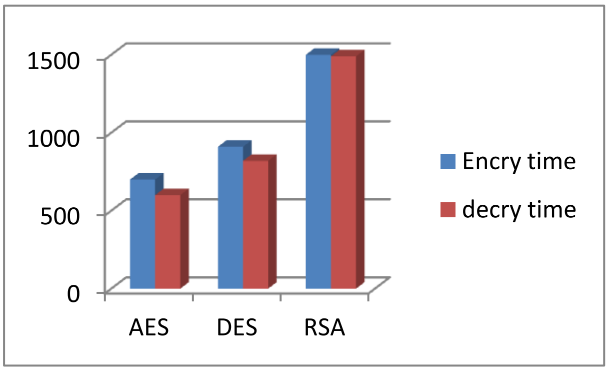


Fig 6: Comparison of computation time among AES, DES and RSA

6. CONCLUSION AND FUTURE WORK

In this paper Implementation of a prototype approach is successfully done for enhancement of windows operating system for clipboard functioning. In this we have successfully encrypted the system clipboard with the help of cryptographic techniques with prevent the data of clipboard being leaked or eavesdrop by any malicious application register as clipboard viewer. By doing this we can enhance the operating system security from malware which aims to hijack the text from the clipboard. In this AES, DES and RSA are used for encryption purpose. This approach is implementation for windows and in future we'll going to implement such for other operating system also and for other encoding like UTF-8, 16, 32, EBCDIC, so this can be used as global language compatible.

7. REFERENCES

[1] "Clipboard Operations", http://msdn.microsoft.com/en-us/library/ms649016(VS.85).aspx

[2] K. C. Lam, W. C. Lau, O. Yue "Hitchbot - Delivering Malicious URLs via Social Hitch-hiking" published in IEEE Globecom 2011 Proceedings.

[3] S. Li, S. Lv, X. Jia and Z. Shao "Application of Clipboard Monitoring Technology in Graphic and Document Information Security Protection System" published in Third International Symposium on Intelligent Information Technology and Security Informatics, IEEE 2010.

[4] K.T. Stolee, S.Elbaum, and G. Rothermel "Revealing the Copy and Paste Habits of End Users" Symposium on Visual Languages and Human-Centric Computing (VL/HCC) IEEE 2009.

[5] M.Wang and Z.Qui "Research of Anti-copy and Plagiarism Monitoring System" First International Workshop on Education Technology and Computer Science, IEEE 2009.

[6] "GoogleForum" https://groups.google.com/forum/#!topic/keepassdroid discuss/w1x6pFUSexw

[7] "MALWAREHELP.org" http://www.malwarehelp.org/malware-new-attack-hijacks-the-clipboard-2008.html

[8] "Clipboards hijacked in web attack" http://news.bbc.co.uk/2/hi/technology/7567889.stm

[9] "Clipboard Snooping Malware" http://www.infosecisland.com/blogview/22429-Detecting-Window-Stations-and-Clipboard-Monitoring-Malware-with-Volatility.html

[10] A. Kumar, S. Jakhar and S.Makkar "Comparative Analysis between DSA and RSA" IJARCSSE Volume 2, Issue 7, July 2012.

[11] Technical White Paper "Reversal and Analysis of Zeus and SpyEye Banking Trojan" 2012

[12] Sophos Security Threat report 2013.

[13] Bromium vSentry *Defeat the Unknown Attack.pdf*

[14] *"MalwareCity News"* Adobe Flash ads launching clipboard hijack attack. 2009

[15] S.Mehrotra, R.Mishra "Comparative Analysis of Encryption Algorithms For Data Communication" IJCST Volume 2 , Issue 2, June 2011.