Novelty Journals

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 1, Issue 1, pp: (1-5), Month: September-December 2014, Available at: www.noveltyjournals.com

Implement Data Security in Today's Operating System Group Members

[1]Muhammad Aleem, [2]Muhammad Tahir, [3]Nasir Jamal

[1]MSCS-20, [2]MSCS-06, [3]MSCS-01 Department of Information Technology, University of Sargodha (Gujranwala Campus) Gujranwala, Pakistan

Abstract: **Today's operating systems such as Windows 8 and Android make a change in the way of user interaction with computer devices. Due to cloud computing every task is completed with the collections of software in today's operating systems those are purposed as user application such as document viewer, social network application, online supporting tools etc. Operating system interaction workflow between these applications is difficult to understand as per security point of view. During completion of a task it is also hard to know what result occurs at every step when operating system interacts with cloud services. As per data security importance operating systems interaction with cloud services become a cause of data disclosure. In this term paper we are going to present a framework for data prevention when our operating system interacts with cloud services. Framework manages inbound and outbound traffic of user operating system when user interacts with cloud services to prevent data from disclosure on internet.**

Data disclosure is occur when user system interact with cloud services to complete a long term task define by user. During it system interacts with multiple applications available in cloud services. Framework will provide secure interaction between user system and cloud services. It's allow only those cloud applications which are reliable and secure for data interaction with user system and complete all long term task one by one. This framework provides security mechanism with simple permission checks between user application interactions with cloud services.

Keywords: **Computer Devices, Document Viewer, Social Network Application, Online Supporting Tools Etc.**

I. INTRODUCTION

In today's operating system data disclosure is weak point of Windows 8 and Android. Especially in Android operating system this issue is raising up when user system interact with third parties tool or cloud services but in Windows Microsoft almost cover up this issue in its new released version Windows 8.1 and upcoming. Microsoft tries to remove its operating system bugs with online suggestion and its reach center but in Android this issue is still that when user system interact with third parties tools or using cloud services. Today mostly research is going on operating system security especially in cloud services domain, different researchers provide different solution regarding data disclosure. But mostly could not focus on data disclosure when user system interacts with cloud services using mail servers. In our term paper we especially focus on this problem such as already explain a example 1) open a attachment file in document viewer 2) chose option online convertor from word to PDF 3) select an social network application for communication this modularity strikes a balance between simple UNIX tools.

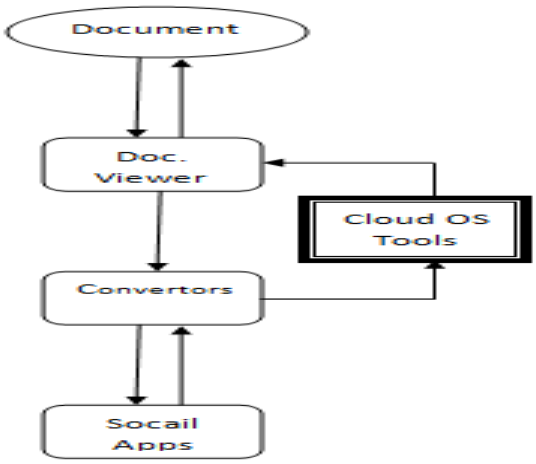

Figure: 1

In our term paper we introduce security policy framework which prevent our system from disclosure of data and information when system use cloud services. Framework is specially developed for prevention of data disclosure such as office documents, audio and video data, official pictures relevant to secret projects etc. This framework play security role when user system interacts with cloud services as a middle security policy between system interactions. Third party tools or cloud services cannot directly interact with system at user level. Only authenticate applications can interact with user system those are define in framework for sharing or converting data of user system, no application can interact during a task up till completion and authentication of framework. Framework work like a middle man between interacted system and application. Our term paper point out the problems during system interaction with cloud services and data disclosure weak points when system share it with others by using third party tools in community of operating system security and lack of security in application development due to which data exposed.

II. LITERATURE REVIEW

Today's operating systems architectures are under observation and organizations make a fundamental change. Windows 8 and Android rapidly make change in their operating systems [2], such as Microsoft take suggestions regarding its product (Windows) on operating system security and make change in its today operating system [5][8]. Security mechanism change with fine grained security policies in application interaction with cloud services [3] [11].Android security mechanism is not too much strong as compare to other [4][9] so that's why data disclosure is raising up in it such that in Android platform an application develop work together with other application to complete a larger user define task for example 1) open a attachment file in document viewer 2) chose option online convertor from word to PDF 3) select an social network application for communication this modularity strikes a balance between simple UNIX tools (e.g., sed, grep) and monolithic GUI applications (e.g., MS Office).

III. PROBLEM STATEMENT

Data is the most important in user system so its security is also too much important like as data. Prevent data from expose is important in operating system security. In today's operating systems data accidently expose with cloud services interaction in our system. Such as an Email generate with attachment file in .doc format and send to target system. After receiving that mail user click on attachment file for view .doc format file. For it system call online document viewer to view document from cloud services and also purpose to convert .doc to PDF format with online application. When user accept take the advantages of online converting tools, user system data is disclose. During all upper process it's not easy to understand what's up at each step or result of each step. Major drawback in it, system digital signature of user system a hacker can easily can hack during completion of task and take a miss use of digital signatures. In this example document viewer and word to PDF convertor both tools are used by user system from cloud services.

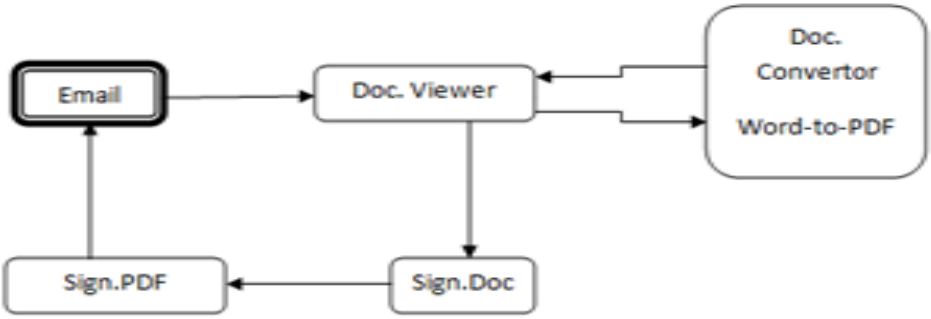

Figure: 2

In a business environment people generate mails for communication and consider it a best way to pass a contract or make a deal between two parties so, data security of this mechanism in operating system is also important. As per Figure: 1 a mail with attachment file become a cause of data disclosure when user system interact with cloud services for document viewer or using online convertor and third parties tools .

IV. PROPOSED SOLUTION

We introduce a security policy framework which prevent our system from disclosure of data and information when system use cloud services. Framework is specially developed for prevention of data disclosure such as office documents, audio and video data, official pictures relevant to secret projects etc. Framework monitor all inbound and out bound traffic regarding cloud services. As per Figure: 1 when our system share it's document for viewing on cloud for document viewer, after that system control on data is out of order and our data is disclose. In framework we manage our security mechanism on system which interacts with cloud services. Every traffic regarding cloud services passed through this framework on cloud. System will interact only those applications those are authenticate in framework. Framework perform large tasks step by step authentication. Our system interacts at a time one application of cloud services, not start next till completion of first task. Framework check whole traffic with security checks policy and manage all activities with activity manager of framework.

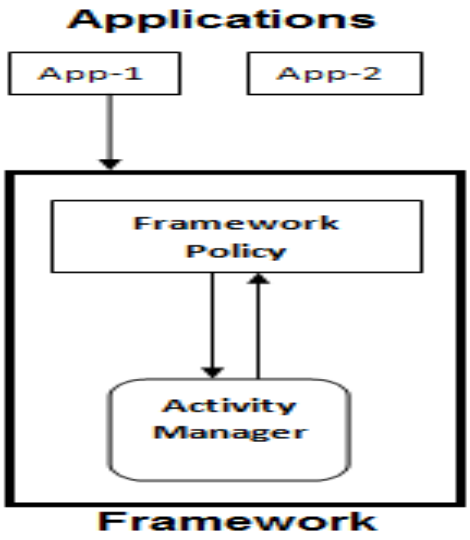

Figure: 3

As per Figure: 2 every activity will be record in activity manager and every task will be perform through framework security policy. User system interacts at a time one application and cannot interact second till completion of first application task.

Framework allows only those applications or cloud services those are authorized by system. Any attachments file which user system received will not be open directly in document viewer, first framework shows it in zip or compressed form to user and makes an option to download and then open in user system. If user try to open it directly framework stopped and blocked this process. For online view or using cloud services framework complete this task with define grained security policy and perform each task through framework policy and activity manager. Work Flow between application process and framework policy is show in Figure: 4.Framework complete each user system task one by one.

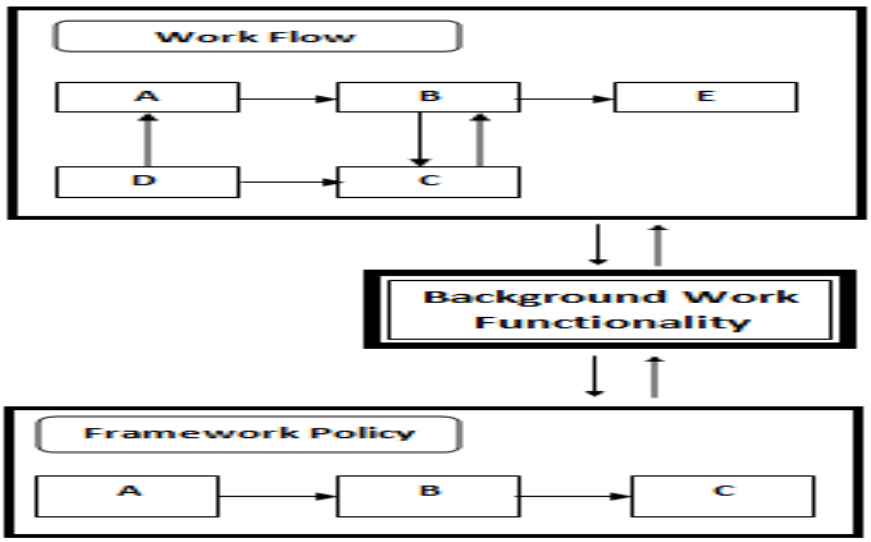

Figure: 4

As per Figure: 4 user systems want to interact with applications A to E but framework stopped it and manage it as per define policy. First system will interact with one application or task A then next B and C. after completion of first task A then framework allow to interact with next B or C.

V. CONCLUSION

Today's operating systems specially Microsoft and Android OS disclose data when user system interact with third parties tools or using cloud services. To prevent it we introduce a framework which manages whole processes with security checks when system interacts with cloud services. Framework defines inbound and outbound rules for user systems and makes a security check on traffic when system interacts with cloud services. If the interacting source is reliable then framework allow user system for using third parties tools or cloud services and block when refer interacting source is not reliable.

VI. FUTURE WORK

Data disclosure is the major issue of operating systems security especially when systems use cloud services. This concluded work is part of semester term paper in limited time. Due to time constraint our proposed framework will develop and be implementing in future. This framework will play security role when user system interacts with cloud services as a middle security policy between system interactions. Framework will define inbound and outbound rules for user systems and makes a security check on traffic when system will interacts with cloud services.

REFERENCES

[1] O. Arden, M. D. George, J. Liu, K. Vikram, A. Askarov, and A. C. Myers. Sharing Mobile code Securely With Information Flow Control. In Proceedings of the IEEE Symposium on Security and Privacy, 2012.

[2] D. Barrera, H. G. Kayacik, P. C. van Oorshot, and A. Somayaji. A Methodology for Empirical Analysis of Permission-Based Security Models and its Application to Android. In Proceedings of the ACM Conference on Computer and Communications Security, Oct. 2010.

[3] S. Bugiel, L. Davi, A. Dmitrienko, T. Fischer, A.-R. Sadeghi, and B. Shastry. Toward Taming Privilege-Escalation Attacks on Android. In Proceedings of Network and Distributed System Security Symposium, 2012.

[4] M. Conti, V. T. N. Nguyen, and B. Crispo. CRePE: Context-Related Policy Enforcement for Android. In Proceedings Information Security Conference, 2010.

[5] J. A. Solworth and R. H. Sloan. A layered design of discretionary access controls with decidable properties. In Proc. IEEE Symp. Security and Privacy, pages 56–67, 2004.

[6] Wheeler 2001: David A. Wheeler, Counting Source Lines of Code (SLOC), (Self) 2001,

[7] Colp, P., Nanavati, M., Zhu, J., Aiello, W., Coker, G., Deegan, T., Loscocco, P., Warfield, A.: Breaking up is hard to do: security and functionality in a commodity hypervisor. In: SOSP (2011)

[8] Kim, T., Zeldovich, N.: Making Linux Protection Mechanisms Egalitarian with UserFS. In: USENIX Security Symposium 2010 (2010)

[9] Santos, N., Rodrigues, R., Gummadi, K.P., Saroiu, S.: Policy-Sealed Data: A New Abstraction for Building Trusted Cloud Services. In: USENIX Security (2012)

[10] H. J. Wang, C. Grier, A. Moshchuk, S. T. King, P. Choudhury, and H. Venter. The Multi-Principle OS Construction of the Gazelle Web Browser. In Proceedings of the USENIX Security Symposium, 200