Implement Data Security in Today's Operating System

Saad Bashir **Muhammad Aleem** **Muhammad Tahir**

Usman Abid **Muhammad Tayyab**

Department of Information Technology

University of Lahore (Gujrat Campus)

Gujrat, 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. This framework provides security mechanism with simple permission checks between user application interactions with cloud services.

INTRODUCTION

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 a 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).

In this paper we introduce a security policy framework which prevent our system from disclosure of data and information when system user 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.

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.

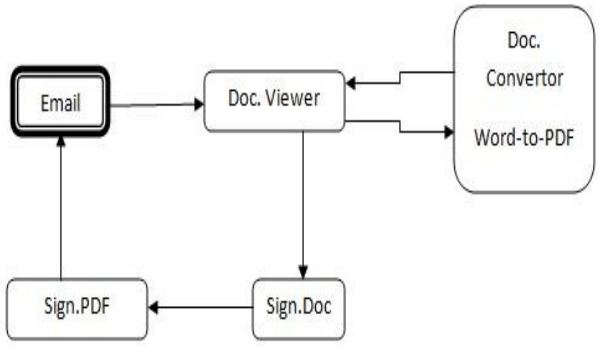

Figure:1

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.

Purposed 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.

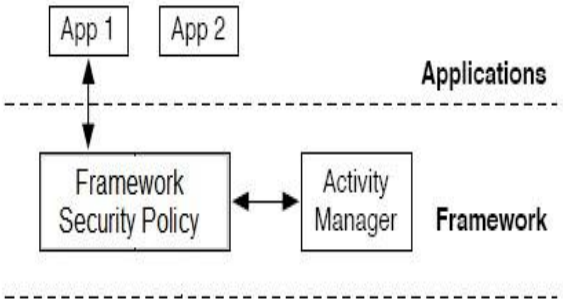

Figure: 2

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.

References:

[1] A Capability Based Client: The DarpaBrowser. http://www.combex.com/papers/darpareport/html/.

[2] 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.

[3] T. Wyatt, "Security alert: Android trojan ggtracker charges premium rate sms messages," *http:// blog.mylookout.com/ 2011/ 06/ security-alertandroid-trojanggtracker-charges-victims-premiumratesms-messages/* .

[4] L. Badger, D. F. Sterne, D. L. Sherman, K. M.Walker, and S. A. Haghihat. A domain and type enforcement UNIX prototype. In *Proc. of the USENIX Security Symposium*, Salt Lake City, 1995. [5] D. E. Bell and L. J. LaPadula. Secure computer systems: Mathematical foundations and model. Technical Report M74-244, Mitre Corporation, Bedford MA, 1973.

[6] J. L. Berger, J. Picciotto, J. P. L. Woodward, and

[1] P.Derrin, K. Elphinstone, G. Klein, D. Cock, and M.M. T Chakravarty. Running the manual: An approach to high-assurance microkernel development.