ISSN 2395-1621

Obviation of Data Ex-filtration through End-point users

[#1]Apurva Kulkarni ,[#2]Revati Pathak ,[#3]Ankita Kokane,[#4]Prof. Rachna Satao

[1]kulkarniapurva1995@gmail.com
[2] revatip999@gmail.com
[3]ankitadkokane21@gmail.com

[#123]Department of Computer Engineering,
[#4]Assistant Professor, Department of Computer Engineering,

Smt Kashibai Navale College of engineering,
Pune 411041, India

ABSTRACT

Pod slurping consider as the act of using portable devices for downloading large amounts of data on an unauthorized basis. Pod slurping, data hacking, data theft can be prevented by various security products, but there is possibility that authorized or trusted employees, contractors or visitors may be able to steal large amounts of information with a simple connection, often a USB connection to a workstation or other hardware component. Data theft is a growing problem in many organization using unauthorized USB portable devices, mobile devices, digital cameras. These actions are responsible to violate organizations standards and confidentiality of company data. So in order to solve the problem of unauthorized USB access and data transfer, we develop a system or application which will automatically block an unauthorized USB device at the time of data transfer. And at the server side, each and every information will be recorded in log file. As soon as an unauthorized user is recognized, then system will generate an alert.

Keywords: Client/server architecture, Distributed file systems, End point Security and reliability, Multithreading.

ARTICLE INFO

Article History

Received: 11th February 2017

Received in revised form :

11th February 2017

Accepted: 13th February 2017

Published online :

14th February 2017

I. INTRODUCTION

Now-a-days there is a growing problem of accessing data by unauthorized user from private offices, industries, government organisations, we should have to be prevented From this problem. USB (Universal Serial Bus) is a specification to establish communication between devices and a host controller [1]. Data theft is currently facing problem for desktop application. Data theft is a growing problem primarily perpetrated by office workers with ease to technology such as desktop computers and hand-held devices capable of storing digital information such as flash drives, mobile devices and even digital cameras. Now a day USB devices are the popular source of computer virus and other harmful malware software that harms and degrades performance of workstation. Data theft problem through employee confidentially data will be going to be access by unauthorized user this user will be damage or corrupt the data and illegal use of it. So from preventing this we have to develop the application which is providing protection to our desktop computer.

The purpose of application is to provide security and protect confidential data from unauthorized devices. We are designing admin module to take care of desktop. Admin gives permission to access only authorized user and maintain all data log of user. If user attaches unauthorized removable disk or USB devices then system is lock until user removes it .So we are developing such system which protect our confidential data from unauthorized USB devices. In this system we use ex-filtration technique for protecting confidential data.

II. LITERATURE SURVEY

A] Different themes of Security culture

© 2016, IERJ All Rights Reserved

"There is increasing interest from regulators and government departments concerned with enhancing security in organisational culture, more specifically the notion of security culture. Culture is essentially a "set of common understandings, expressed in language" , or "shared patterns of meaning" , or "shared values and beliefs that interact with an organisation's structures and control systems to produce behavioural norms" . Culture is of interest in a security context if it can be proven to affect security outcomes. Three main techniques were used in the gathering of qualitative data. These were: the Twenty Statements Test (TST) [5], repertory grids technique [6], and critical incidents technique [7]. The analysis of the data gathered by these techniques yielded nine categories or themes relating to security culture.

The themes, listed below, could support the creation of an item bank for the development and trialling of the security culture audit tool. The themes demonstrate the content of security culture: what is contained within it. The emergent themes are: 1 External Influences; 2 Human Resource Activities; 3 Impact on Business; 4 Infrastructure; 5 Information Security; 6 Management; 7 Organizational Staff; 9 Physical Security; 10 Working with External Others. As a result of this work a working definition of security culture has been derived, and is stated as: "Security culture is indicated in the assumptions, values, attitudes and beliefs, held by members of an organisation, and behaviours they perform, which could potentially impact on the security of that organisation, and that may, or may not, have an explicit, known, link to that impact". This paper will suggest implications of these findings for Aviation Security. Some aspects of an organisation's security culture have evolved as a logical response to security threats, and are espoused by the management of the organisation.

B] Basic concept of Pod slurping through USB

"Pod slurping is the intentional or unintentional use of a portable USB mass storage device, such as a USB flash drive (or "thumb drive"), to illicitly download and store confidential and proprietary data from network endpoint [1]. There are many establishments and organization that are unaware of, or choose to remain ignorant about the threat that can be caused by portable devices in their network setting until some events that can be from a minor unfortunate incident to a complete catastrophe. In the information age, cybercrime and information leakage increase, because endpoints are an easy target [2]. The key to managing portable devices in business environment is to give administrator direct control over what devices are in use on your network. In this paper we present the implementation of access and identity management for endpoint protection and data security from USB devices to maintain information security and data theft prevention in a corporate environment."

C] Architecture of USB and interfacing technologies

"The Universal Serial Bus (USB) is a communications architecture that gives a PC the ability to interconnect a variety of devices via a simple four-wire cable. One such device is the printer. Traditionally, printers have been interfaced using the following technologies: • Unidirectional parallel port • Bi-directional parallel port • Serial port • SCSI port • Ethernet/LAN There are other, more sophisticated printer interfaces, but the ones previously listed are the most popular. USB offers a much greater throughput capability than the serial port and is comparable in speed to the parallel port. This makes both parallel and serial printers good candidates for interfacing with USB."

D] Detection of data theft using endpoint

"Obtaining another's personal information and using it without his/her knowledge or consent to commit fraud for financial gain or for another criminal purpose. A thief does not need much information to steal and seriously disrupt someone's life: often a name, address, and date of birth are enough to get started."

Sr. No	Title Of Paper	Author Name	Published Year	Keypoint
1.	"A breach in nuclear security."	Zagorin, Adam	19 April 2011.	Endpoint protection
2.	"70% of security breaches using pen drives: Indian army", PTI, New Delhi, Mon,	Press Trust of India	01 Oct 2012	Podslurping through USB
3.	"Definition of Universal Serial Bus". 1394 Newsletter 2 (4): 7-9.	Paul Polishuk	03 Nov 2010	Uniqueness of USB
4.	"Client data theft" Reuter US edition	Julius Baer CEO	27 August 2012	Data theft using end point

Table.1 Review on Exiting Technique's

III. SYSTEM ARCHITECTURE

In this system, we are going to use client server architecture .So client will be responsible for USB plugging and registration of that device. And Server will maintain logs of data transfer taking place in the system. Authentication is a necessary step in order to transfer any kind of data.

© 2016, IERJ All Rights Reserved

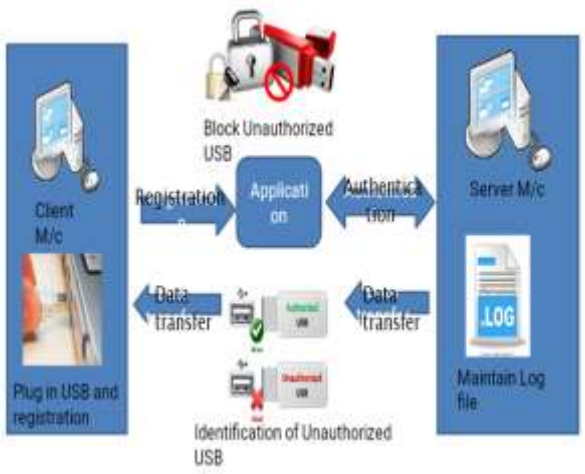
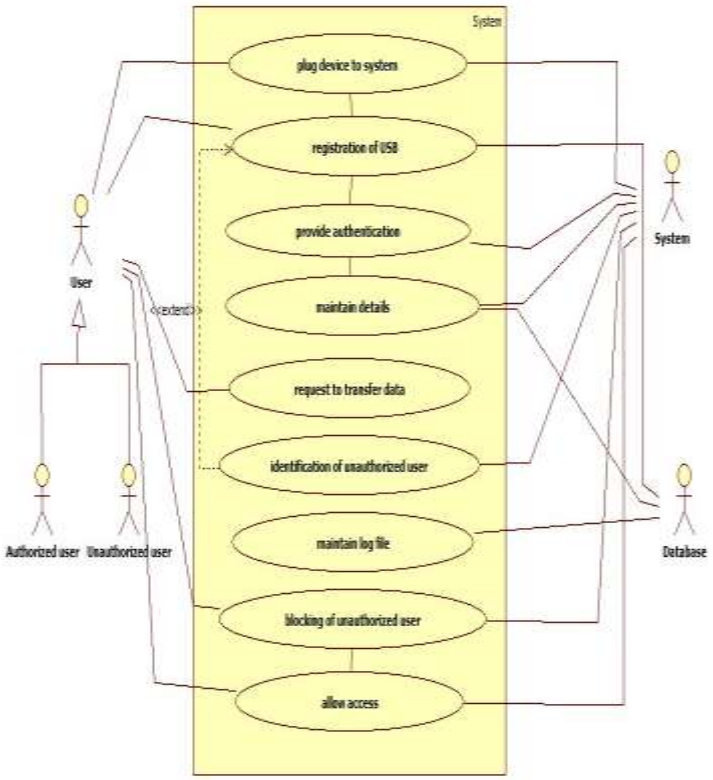


Fig 3.1 Proposed Data System Architecture

IV. USE CASE DIAGRAM



V. CONCLUSION & FUTURE DIRECTIONS

We can conclude that, System provide security to each LAN cycles .We conclude that whenever any user connects unauthorized cables to the system. To develop a desktop/web application which will provide protection to data at endpoint by locking and recognizing unauthorized USB access.This project would be useful in Military organizations where the information is confidential, Government organization, Bank systems where the data must be confidential.

In terms of future scope, this can be a platform independent system .Scope of this project can be extending to cloud system. It can be extended for antivirus detection, cybercrimes, malicious files and checking of originality of files. Additionally, VDR records can also be helpful for recognizing that unauthorized user.

VI. ACKNOWLEDEMENT

With due respect and gratitude we take the opportunity to thank all those who have helped us directly and indirectly. We convey our sincere thanks to Prof. P. N. Mahalle, HoD, Computer Dept. and Prof. Rachna A. Satao for their help in selecting the project topic and support. Our guide Prof .Rachna A. Satao has provided us help with immense support and guidance for the same. She has always encouraged us and given us the motivation to move ahead. She has put a lot of time and effort in this project along with us and given us confidence. We wish to extend a very big thank you to her for the same.

Also we wish to thank all the other people who have helped us in any smallest way in the successful completion of this project.

REFERENCES

[1]Zagorin, Adam "A breach in nuclear security." Time, April 19, 2007. Retrieved April 21, 2007.

[2]Press Trust of India, “70% of security breaches using pen drives: Indian army”, PTI, New Delhi, Mon, 01 Oct 2012.

[3]Hui Pan, Editor; Paul Polishuk, Editor (April 1998). "Definition of Universal Serial Bus". 1394 Newsletter 2(4): 7–9. Retrieved 2010-03-11.

[4]Julius Baer CEO, BAER.VX, “Client data theft” Reuter US edition, August 27 2012.

[5]Pham, D.V. “Threat analysis of portable hack tools from USB storage devices and protection solutions,” IEEE ISBN: 978-1-4244-8001-2 [2010 International Conference on, vol., no., pp.1-5, 14-16 June 2010].

[6]Lynn, K., "Universal serial bus (USB) power management," Wescon/97.Conference Proceedings, vol., no., pp.434-441, 4-6 Nov 1997.

[7] Steven C. Mills, “Using the internet for active teaching and learning,” ISBN 0-13-110546-9

[8] Bai Xiaoping; Wei Yuanfeng; , "Study on the signal detection and simulation of universal serial bus 2.0 IP core circuit system," SoutheastCon, 2007. Proceedings. IEEE , vol., no., pp.59-62, 22-25 March 2007

© 2016, IERJ All Rights Reserved

[9] Ioana Bazavan Justus (18). "Identity Management Series – Role- and Rule-Basing Part 1: Introduction". THE SECURITY CATALYST helping people effectively communicate value. Michael Santarcangelo. Retrieved 23 May 2012.

[10] Phillip J. Windley, "Digital identity", O'Reilly Media, Inc., 2005, p.

[11] Saurabh Verma, Abhishek Singh, "Data theft prevention & end point protection from PnP Devices" ISBN: 978-93-81583-71-5, National Conference on Communication Technologies & its impact on Next Generation Computing 2012.

© 2016, IERJ All Rights Reserved