Prevention of Data Ex-Filtration through Endpoint Protection

Snehal Nemade[1], Prachi Patil[2], Nikita Nikrad[3]

[1]*STUDENT, Dept. of Computer Engineering, Pune University, Maharashtra, India*

[2]*STUDENT, Dept. of Computer Engineering, Pune University, Maharashtra, India*

[3]*STUDENT, Dept. of Computer Engineering, Pune University, Maharashtra, India*

---***---

Abstract - *Now a days there is a growing problem of data extortion from private offices, industries, government organizations, which should be prevented. As USBs are most easiest devices to use and endpoints are an easy target thus many people preferred usb only to steal the data or hack the data which ultimately slows down the PC and degrades it's performance. In this paper we are focusing on DLP (Data Loss Prevention) and preventing our systems from unauthorized access via USBs through endpoints.*

Key Words: **USB, Endpoint protection, Data security, Data loss prevention, Data theft prevention from unauthorized USB device.**

1. INTRODUCTION

USB is a standard for a connection between two electronic devices, including a mobile phone and a desktop computer.

Data exfiltration, also called as data extrusion, is the unauthorized copying or retrieval of information from a target's network to a location which is controlled by a threat agent. Because data usually moves in and out or within a networked enterprise, data exfiltration can act like normal network traffic which detects exfiltration attempts challenging for IT security groups.

Data Loss Prevention (DLP) is a computer security term referring to systems that identify, monitor, and protect data-in-motion (network security), data-at-rest (storage security) and data-in-use (endpoint security). These systems achieve their goals through advanced content-aware inspection capabilities, contextual security analysis of transactions and robust management consoles with a centralized framework. Cloud and software-as-a-service (SAAS) delivery models have now joined traditional delivery systems for DLP.

2. RELATED WORK

In [1] authors used Threat analysis of portable hack tools from USB storage devices and protection solutions. According to authors their proposed solution is aimed at providing the most important and concise solution for enterprise administrators to secure their system from portable hack tools.

In [2] authors proposed Data theft prevention and endpoint protection from PnP devices. Author presents 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.

In [3] authors Behavior model for detecting data exfiltration in network environment author have presented a behavior based model for detecting data-exfiltration attacks, the issue of data-exfiltration over the network is or addressed and solution the same is provided.

3. PROPOSED SYSTEM

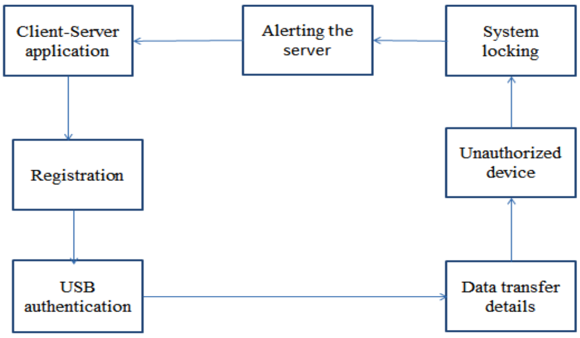


Figure: End point protection cycle for USB

The vision of this project is to track record and limits the use of USB devices in a secured environment (network) thus maintains confidentiality and integrity to meet information security standards. We are proposing to keep a centralized repository of allowed devices such as USB key board, mouse, and printer etc. based on organization's security standards. Along with centralized repository, system should keep a distributed repository of devices in each local system.

4. IDENTITY AND ACCESS MANAGEMENT

Identity management (IDM) describes the management of individual identifiers, their authentication, authorization, and privileges/permissions within or across system and enterprise boundaries with the goal of increasing security and productivity while decreasing cost, downtime, and repetitive tasks. [4]

4.1 Implementation of Security

In an organization there is many ways to authenticate uniquely e.g. employee id, full name, face etc., but in digital word same has been done by digital identity.

Digital identity is a psychological identity that prevails in the domains of cyberspace, and is defined as a set of data that uniquely describes a person or a thing (sometimes referred to as subject or entity) and contains information about the subject's relationships to other entities [5].

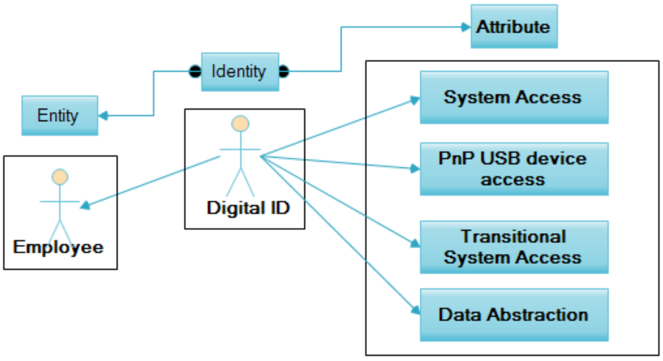


Figure: Identity and Access Management

5. Motivation

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.

USB devices are the popular source of computer virus and other harmful malware software that harms and degrades performance of workstation.

6. Objectives

Following things are necessary in order to solve a problem of unauthorized USB access and data transfer:-

(1) Device identification and authentication.

(2) Maintain logs of data transfer.

(3) Blocking of unauthorized USB device.

(4) Generate alert and send to the admin.

7. Applications

This software would be helpful in following areas:-

- Military organizations where the information is confidential.
- Government organization.
- Bank systems where the data must be confidential.

8. ARCHITECTURAL DESIGN

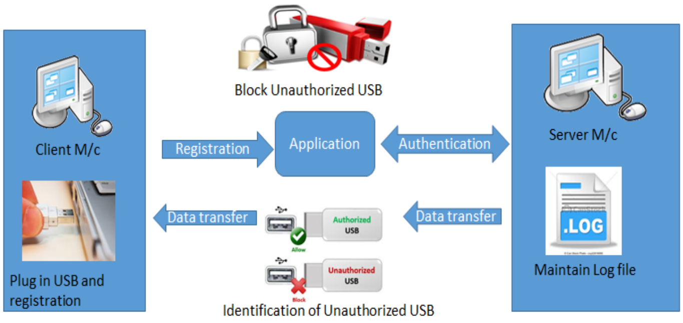


Figure 8.1: Architecture diagram

Device Detection:

This means workstation on which USB device plugged in is connected to a system. In this scenario authentication and authorization will take place from database repository. In device detection mode, if plugged in device is authorized; the event log will be created on central event log server, else device will be locked and an instant security alert as e-mail will be generated for administrator and then event log will be created.

Device Identification:

We identify that plugged in device is authorized or not. Every USB device comprises a set of VID (Vendor ID) and PID (Product ID). These set of two IDs make a key by which we can identify similar type of devices. These IDs are 4 characters hexadecimal ID; e.g. a typical VID looks like VID xxxx and PID looks like PID yyyy, where xxxx and yyyy is a hexadecimal number. On the basis of VID and PID we block and allow USB devices to communicate with workstation.

Device Authentication:

Devices are authenticated by a Whitelist (a list of authorized USB devices) located on a remote server database. Devices should be authenticated directly from server whitelist. The system should keep a local copy of remote whitelist in encrypted format to authenticate devices and maintain security. At this place we take decision to lock or allow USB device to communicate with workstation.

Allow Authorized Devices:

If organizations security policy allow some devices e.g. USB keyboard, PnP printer devices etc. then we can add them into repository of allowed devices and rather than raising block even we will install drivers to make it communication with computer and user will allow to use that device.

9. PROPOSED ALGORITHM

A. Design Considerations:

DEFAULT USB ACCESS ALGORITHM:

INPUT:

VID: VENDOR ID OF USB DEVICE

PID: PRODUCT ID OF USB DEVICE

PORT: VIRTUAL PORT ON WHICH DEVICE COMMUNICATING WITH SYSTEM

Output: Give Access/ Install Drivers

B. Description of the Proposed Algorithm:

```
ALGORITHM:
IF VID ≠ 0 AND PID ≠ 0 PORT ≠ 0
LIST L: LIST OF ALL VID AND PID FROM LOCAL .INF FILE FROM ROOT DIRECTORY
    FOR EACH ITEM IN L (|L| >= 1), DO
        IF ITEM [VID] == VID AND ITEM [PID] == PID THEN B ←GIVE ACCESS
IF B == GIVE ACCESS THEN
    COMMUNICATE WITH PLUGGED USB
ELSE
    Install desired drivers then Communicate with plugged USB.
```

10. PSEUDOCODE

```
Step 1: First, we will create a client server based standalone application or web based application
Step 2: User should register their USB devices with the help of its Configuration and Specification details.
Step 3: After registration server side should recognize the device is valid and records different logs.
Step 4: Validation of device
    If device is valid
    {
        Data transfer allowed
    }
    Else
    {
        System is locked
    }
Step 5: End.
```

11. SIMULATION RESULTS

System will create a web based application then the appropriate usb's will get registered on it so that the system will be ready for the future use, whenever any usb device will be plugged to our system it's validation will take place and after validation if the device is found authorized it will be able to interact with the system otherwise system will get locked.

12. SYSTEM GUI

User interface is the front-end application view to which user interacts in order to use the software. User can manipulate and control the software as well as hardware by means of user interface. Today, user interface is found at almost every place where digital technology exists, right from computers, mobile phones, cars, music players, air planes, ships etc. User interface is part of software and is designed such a way that it is expected to provide the user insight of the software. UI provides fundamental platform for human-computer interaction. UI can be graphical, text-based, audio-video based, depending upon the underlying hardware and software combination. UI can be hardware or software or a combination of both.

UI is broadly divided into two categories:

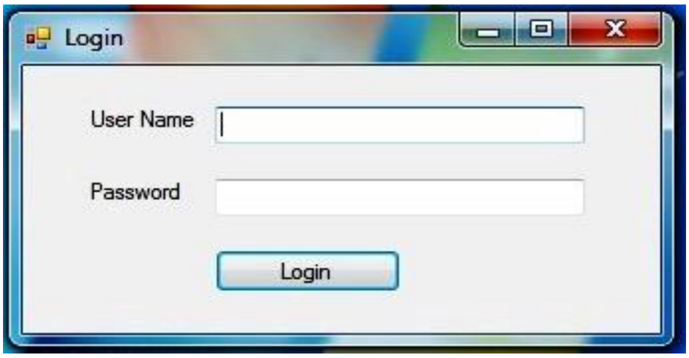
- Command Line Interface
- Graphical User Interface

Graphical User Interface

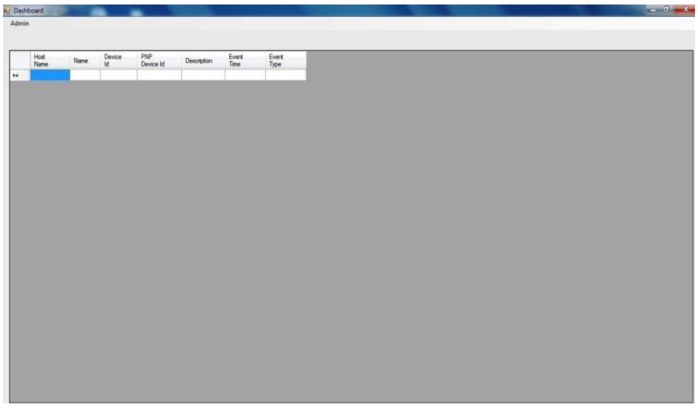
Graphical User Interface provides the user graphical means to interact with the system. GUI can be combination of both hardware and software. Using GUI, user interprets the software. Typically, GUI is more resource consuming than that of CLI. With advancing technology, the programmers and designers create complex GUI designs that work with more efficiency, accuracy and speed.

12.1. Screen Outputs for Proposed System

1. User Login

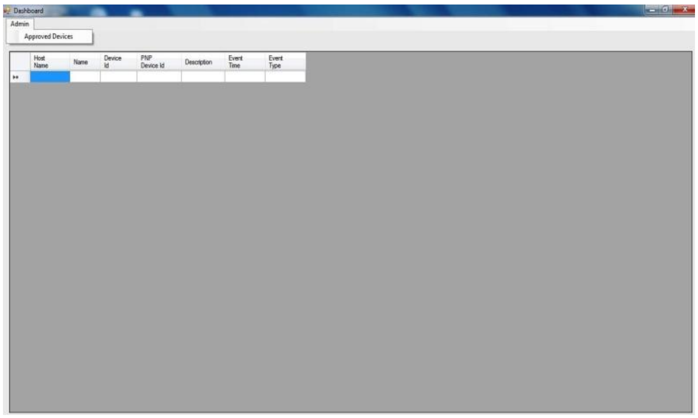


2. Admin Dashboard



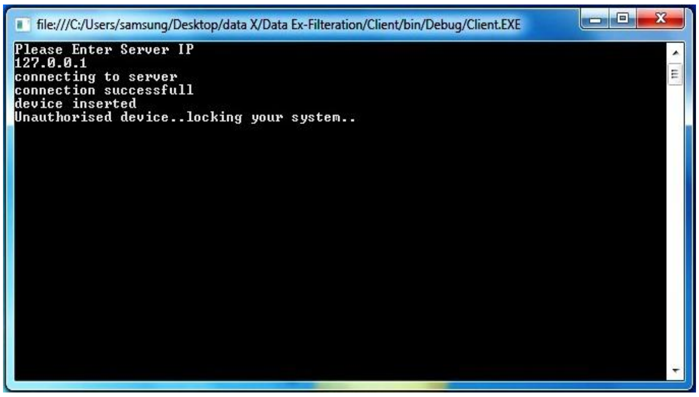
	Host Name	Name	Device Id	PNP Device Id	Description	Event Time	Event Type
▸*							

3. Approved Devices



	Host Name	Name	Device Id	PNP Device Id	Description	Event Time	Event Type
▸*							

4. System Locking


file:///C:/Users/samsung/Desktop/data X/Data Ex-Filteration/Client/bin/Debug/Client.EXE

```
Please Enter Server IP
127.0.0.1
connecting to server
connection successfull
device inserted
Unauthorised device..locking your system..
```

13. CONCLUSION AND FUTURE WORK

There are very few detection methods for data exfiltration which has led to extraction of highly confidential data by the intruders. There is a need for various tools and techniques that will detect the unwanted data extraction. To detect the data exfiltration, a technique has been developed by researchers and is still in work. Thus in this paper we have concluded that with the help of this project we can provide Endpoint protection and data theft prevention from unauthorized USB devices in a network.

Future work could be detection of the intruder, what the intruder extracted from the data. As we are providing best solution for Data Exfiltration through endpoints, this application would be useful in Military organizations where the information is confidential, Government organization, Bank systems where the data must be confidential.

14. ACKNOWLEDGEMENT

It gives us great pleasure in presenting the preliminary project report on '**Prevention of Data Ex-Filtration through Endpoint Protection**'.

We would like to take this opportunity to thank our internal guide Prof. S. P. Jadhav for giving us all the help and guidance we needed. We are really grateful to them for their kind support. Their valuable suggestions were very helpful.

We are also grateful to Prof. N. D. Kale, Head of Computer Engineering Department, PVPIT for his indispensable support, suggestions.

In the end our special thanks to Mrs. Prerna Mishra (Sc 'C') and Mr. Sunil Jaiswal (Sc 'D') for providing various resources such as laboratory with all needed software platforms, continuous Internet connection, for Our Project.

15. REFERENCES

[1]. “Threat analysis of portable hack tools from USB storage devices and protection solutions” Ali Syed, Azeem Mohammad.

[2]. “Data theft prevention and endpoint protection from PnP devices”, Saurabh Verma, Amitesh Verma

[3]. “Behaviour model for Detecting data Exfiltration in Network Environment”, Rajamenakshi Ramachandran , Subramani, Neelakantan , Ajay Shankar Bidyarthy

[4]. IoanaBazavan 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.

[5]. Phillip J. Windley, Digital Identity, O'Reilly Media, Inc., 2005, p.

[6].” Data theft prevention & endpoint protection from Unauthorized USB devices – Implementation”, CONFERENCE PAPER · DECEMBER 2012. Saurabh Verma, Abhishek Singh