Data Theft Prevention and Endpoint Protection from PnP Devices

Saurabh Verma
Assistant Manager
IT Department
Fareportal India PVT LTD

Rahul Lamba
Software Engineer
IT Department
Fareportal India PVT LTD

Abhishek Singh
Associate Director
IT Department
Fareportal India PVT LTD

Amitesh Verma
Trainee
IT Department
Fareportal India PVT LTD

ABSTRACT

Podslurping 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]

Many organizations are unaware of, or choosing to ignore, the threat presented by portable devices in their network environment until some event, ranging from unfortunate to catastrophic, happens. In hard economic times, cybercrime and data leakage increase, finding an easy target in endpoints. 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 need and implementation of access and identity management for endpoint protection and data security from PnP USB devices to maintain information security in a corporate network.

General Terms

Endpoint protection; Data security; IT security; Data theft prevention; Access and identity management.

Keywords

Data theft prevention from unauthorized USB device; End point security, How to control USB devices in corporate network, Plug and Play (PnP) devices.

1. INTRODUCTION

USB (Universal Serial Bus) is a specification to establish communication between devices and a host controller.

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, iPods and even digital cameras.[2]

Since employees often spend a considerable amount of time developing confidential and copyrighted information for the organization they work for; they often feel, they have some right to the information and are inclined to copy and/or delete part of it when they leave the company, or misuse it while they are still in employment.

Sometime organization may undergo heavy loss in business due to unauthorized access to confidential information of organization transmitted through their personnel USB modems and other network devices under highly firewalled and secure network.

Now a day USB devices are the popular source of computer virus and other harmful malware software that harms and degrades performance of workstation. There is also an increased risk of malicious and other illegal software introduction to organizations network through these devices.

So the goal of this project is to prevent organizations from unauthorized USB device access by blocking communication of unauthorized USB device from network endpoint to sensitive data and alert administrator about intrusion and allowing only white listed or authorized USB devices.

2. PROCESS DESCRIPTION

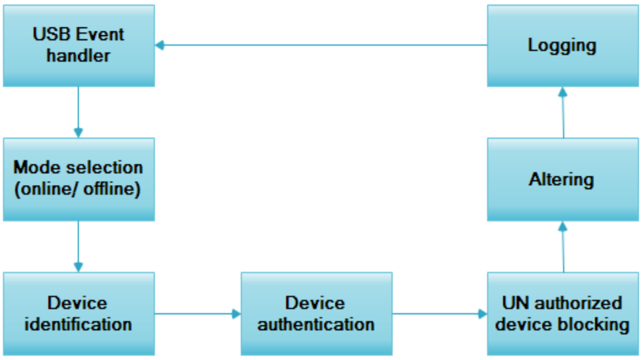

Fig. 1: End point protection cycle for USB

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, and it should be keep up to date by sort of sync mechanism to let system work if central repository is not reachable (system is off line).

2.1 Device DetectionModes

2.1.1 Online detection

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

2.1.2 Offline detection

This means workstation on which USB device plugged in is isolated or disconnected from network. In this scenario authentication and authorization will take place from local repository maintained by the system. In offline mode, if plugged in device is authorized; the event log will be stored locally, and sync with remote server when came online, else device will be blocked and security alert and event log will be stored locally and alert will be sent to administrator when system became online.

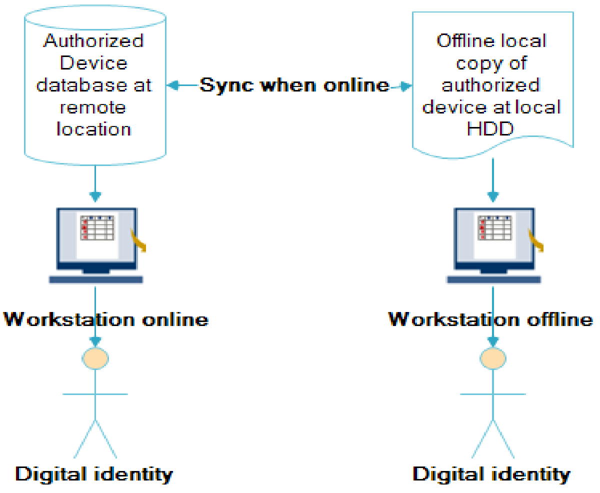
Authorized Device database at remote location
Sync when online
Offline local copy of authorized device at local HDD
Workstation online
Workstation offline
Digital identity
Digital identity

Fig. 2: Device Authentication mode (Online/offline)

2.2 Device Identification

We identify that plugged in device is authorized or not. Every USB device comprises a set of VID (Vendor ID)[3]and PID (Product ID). These set of two ID's make a key by which we can identify similar type of devices. These ID's 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.

2.3 Device Authentication

Devices are authenticated by a Whitelist (a list of authorized USB devices) located on a remote server database. In online mode devices should authenticated directly from server whitelist. If device is offline it should keep a local copy of remote whitelist in encrypted format to authenticate devices and maintain security. This authentication process is called 2-way authentication.

At this place we take decision to block \ allow USB device to communicate with workstation.

2.4 Allow Authorized Devices

If organization's 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.

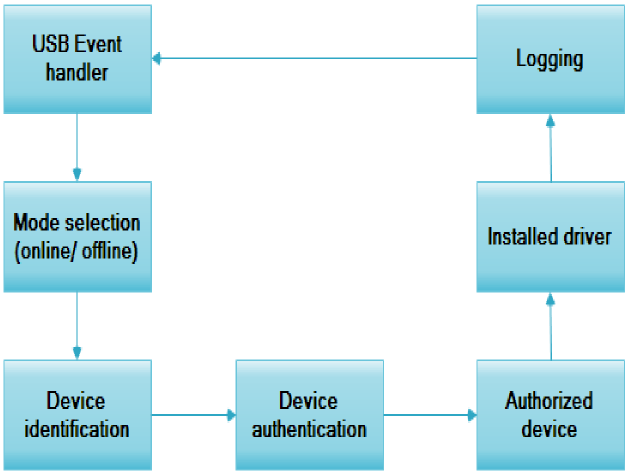

Fig. 3: End point protection cycle for authorized USB device

3. 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]

3.1 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].

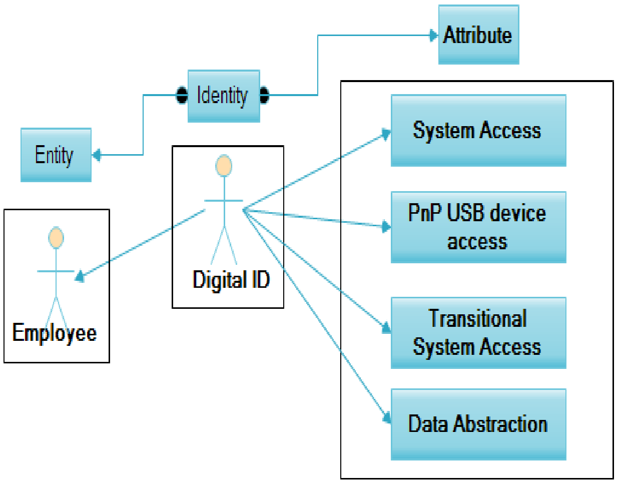

Fig. 4: Identity and Access Management

In our implementation we have logged all events (Refer: Fig.-1). In logging information we have proposed to fetch all possible digital identities (e.g. entities' login ID, Host Name or serial number of workstation etc.) by which we can extract pattern of employee by which he plugin devices (Authorized \ Un authorized) and prevent data theft.

4. ACKNOWLEDGMENTS

We would like to acknowledge and extend our heartfelt gratitude to the following persons who have made the completion of this application possible: our Vice president (Technology) Mr. Nikunj Dhawan for his vital encouragement and support, Mr. Ajay Kohli (Sr. Manager IT) for his guidance, Mr. Anand Tanti (Manager IT) for his valuable suggestions.

5. REFERENCES

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

[2] Julius Baer CEO, Reuter US edition, August 27 2012.

[3] USB.org, vendors and products.

[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.