Contact Information

Publications@ipcg.com

ipCapital Group, Inc.
400 Cornerstone Drive, Suite 325
Williston, VT 05495
United States of America
(802) 872-3200

TITLE

A Novel Methodology for Physically Authenticating a New Hardware Device

ABSTRACT

New hardware devices added to secure networks require authentication to verify that the devices belong on the secure network. When an administrator needs to add a new piece of hardware to the network, the rights and privileges for the new hardware must be validated, using a variety of authentication protocols. A Novel Methodology for Physically Authenticating a New Hardware Device is a new secure method for adding hardware to a secure network.

1. BACKGROUND

Problem or Opportunity

Frequently, computers and networks of computers need to increase capacity or add hardware to accommodate user requirements. Due to the potential of interlopers to hijack unsecured hardware and cause damage to or interfere with the network, it is preferred that any added hardware is secured upon installation.

Typically a secure network contains a security system designed to prevent unauthorized access to said network. In order to add hardware to the network, a user with administrative privileges must verify the authenticity of the new hardware.

Currently, the process of authenticating a piece of hardware involves creating a communication network from the hardware to network (i.e. through DCP (dynamic addressing) or through a static IP address). Once the network is communicating with the new device, the network then prompts the new device for credentials verifying that the device should be allowed on the network. The network server or an authentication tool built into the OS then checks the credentials against the network permissions and either allows or denies the device's request to join. If the hardware is approved, it is added to a hardware control list which contains a unique identifier for all approved network devices.

One limitation of this authentication method is the difficulty of adding hardware to a virtual network or via cloud computing. Additionally, while methods do exist to add hardware to virtual networks, they may not require two factor authentication ("As the name implies, two-factor authentication adds a second security method, typically 'something you have,' to the standard practice of requiring a password, 'something you know'"[1]).

Background Publications

Described below are systems and methods that attempt to provide a solution to the problem described above. These systems and methods are unable, however, to fully address the problem of authenticating the security of a new hardware device over a cloud computing network.

US Patent Number 5764890 describes a method and system for adding a secure network server to an existing computer network. The authentication process involves "connecting as separate nodes on a common communications link at least one client workstation, a network server and an authenticating agent; logging in by the network server as a user connection to the authenticating agent, which includes a database of valid client credentials; receiving a request at the network server for access thereto from the client workstation, the request including authentication credentials of the user; verifying the request by passing the credentials of the user through the network server to the authenticating agent by modifying the form of the request from a request for access to a request for authentication verification; receiving a response from the authenticating agent at the network server, the response including information indicative of the validity or invalidity of the credentials; granting the user access to the network server when the response indicates the request contained valid credentials of the user, and; logging off by the network server as a user connection to the authenticating agent when the connection has not been in use for a pre-defined duration of time." However this invention does not involve authentication from more than one source.

Matthias Rechenburg in his paper for the UKUUG Spring 2009 Conference entitled Instant Cloud Computing with openQRM describes a potential solution. He states that in a virtual setting, one solution is to clone the server settings or authentications and download these to added hardware. "[T]he Cloud can be set to automatically or manual approve new Cloud request, automatically create new virtual machines if not enough existing one are available, enable or disable the clone-on-deploy features etc. It also consist [sic] of a Cloud Ip-manager which is used to automatically configure the external network-interfaces of the provisioned machines."[2] However, one limitation to cloning the server setting is that the cloned machine needs to be identical to the server for the settings to work.

United States Patent Application 20060129797 describes systems and methods for establishing an authenticated and encrypted network connection in a boot protocol, and

---

1 http://www.prnewswire.co.uk/cgi/news/release?id=144246

2 http://www.ukuug.org/events/spring2009/programme/instant-cloud-computing-paper.pdf

specifying the boot image to be loaded by a client. This invention entails using a hardware token or other portable medium, such as a USB drive or device, CD, mini-CD, or floppy diskette, to store authentication and/or identification information for a server. A client then uses the information on the token to authenticate the network server upon initial connection to the network and request a boot image.[3] A limitation of this solution is that an interloper need only acquire one token that contains an authorization code to validate an unauthorized hardware device.

2. SUMMARY OF INVENTION

Invention Summary

The present invention involves a Novel Methodology for Physically Authenticating a New Hardware Device. This is done by creating a trust relationship between the added device and the network using two or more USB drives (or other capable devices) that each contain individual tokens. The individual tokens are then married together on a third party device.

The device containing the first token is inserted into the new device and activated, and a connection to the Network Server is established. The device containing the second token is then inserted into the network server and activated. The network server and the User Machine then communicate to determine if the encryption keys contained in the tokens match. If they match, the new device is then authenticated. This allows the second device to be validated from anywhere in the world where it can communicate with the server. For security purposes, both tokens must be concurrently active in their respective devices.

Unique Concepts

The unique concept embodied in this invention is the ability to easily and physically authenticate a new hardware device in a secure fashion, even when the device to be added is contained at a physically disparate location.

3. DESCRIPTION OF THE INVENTION

Figure 1 depicts the system for operation of the Novel Methodology for Physically Authenticating a New Hardware Device.

The User Machine consists of any personal computing device, such as a desktop computer, laptop, or mobile device.

The I/O Devices are input and output devices through which the user and User Machine may communicate. I/O Devices may include a keyboard, mouse, monitor, or removable disk drive.

---

[3] http://www.freepatentsonline.com/y2006/0129797.html

The OS is an operating system, such as Linux, residing on the User Machine. The OS manages interactions with hardware, applications, and the user.

The Authentication Module is part of the OS that validates the authenticity of hardware on the network.

The New Hardware is a computer or peripheral device to be added to the network.

The Network Server consists of any personal computing device, such as a desktop computer, laptop, or mobile device that processes requests and delivers data to other (client) computers or hardware devices over a local network or the Internet.

The Universal Serial Bus (USB) flash drive is a removable disk drive that stores information that the User Machine can understand.

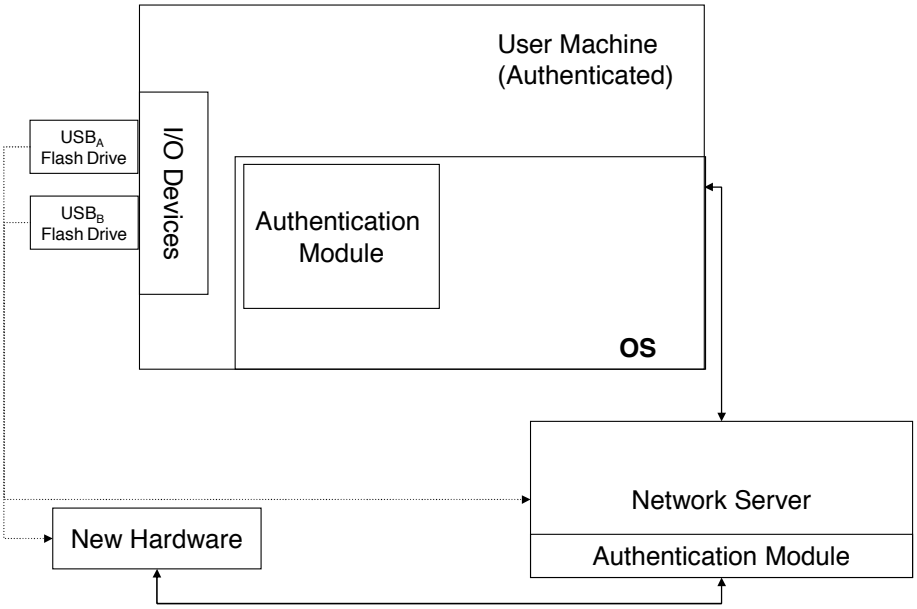

Figure 1. System for a Novel Methodology for Physically Authenticating a New Hardware Device

Figure 2 summarizes the method used by the Novel Methodology for Physically Authenticating a New Hardware Device.

In step 1, the user connects an unsecured New Hardware to a secured network via a network server.

In step 2, the user puts two USB drives, USB_A and USB_B, in an authenticated User Machine, where USB_A contains a set of rights/privileges via a third party token.

In step 3, the user tells the User Machine to encode USB_B with the same privileges that are contained on USB_A (user knowledge of the codes is not necessary).

In step 4, the user then takes the USB_A and plugs it into the Network Server.

In step 5, the user plugs USB_B into the unsecured New Hardware to be authenticated.

In step 6, the user machine sends the token to the network server. The authentication module on the server compares the tokens and if valid, authenticates the new device and adds it to the secured network. Additionally, if the device to be authenticated was in a virtual space or remote location, the user could send one of the USB drives to another user or the token via email to allow for authentication of the hardware device.

The method ends.

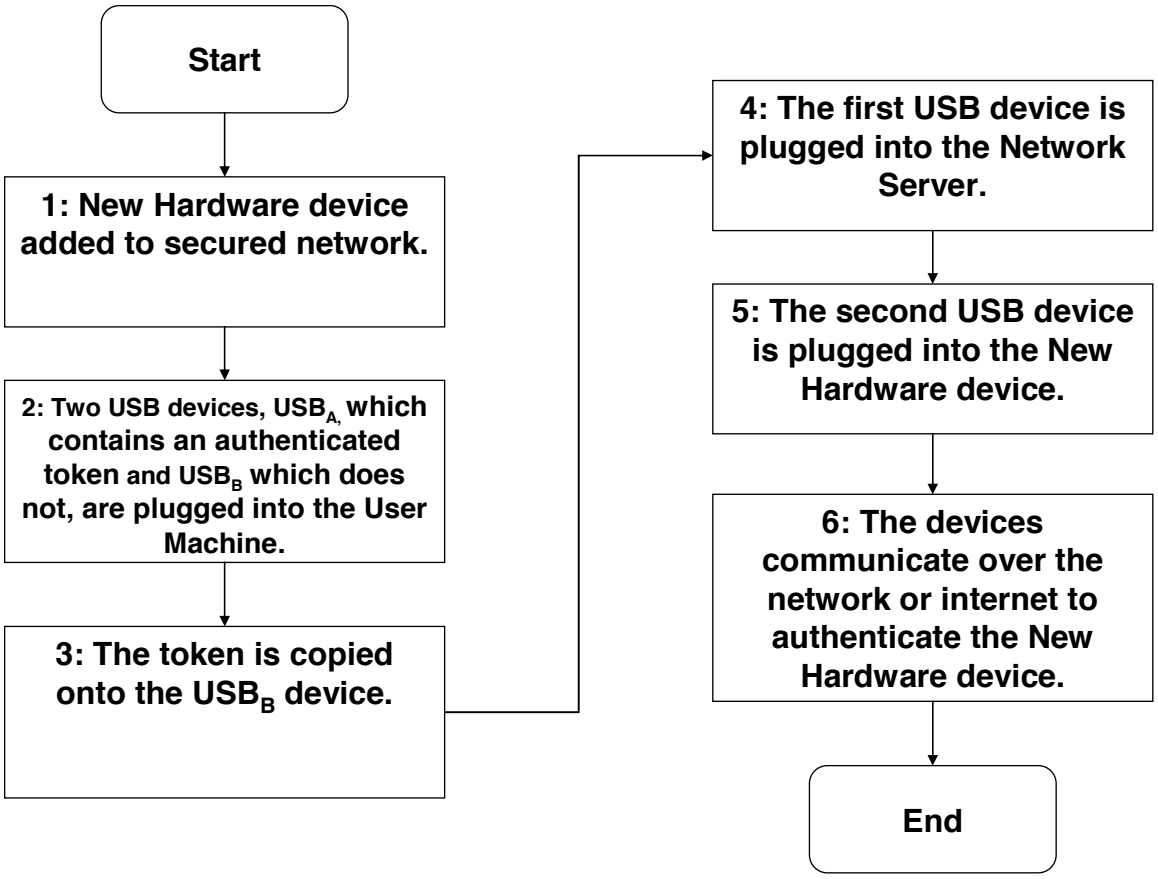

Figure 2. Methodology for Physically Authenticating a New Hardware Device