Contact Information

Publications@ipcg.com

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

TITLE

Assisted Two Factor Authentication Mechanism via a Trusted External Source

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. The Assisted Two Factor Authentication Mechanism via a Trusted External Source 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 a 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 validity 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.

---

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

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

2. SUMMARY OF INVENTION

Invention Summary

The present invention involves a adding a layer of security to the authentication of new network devices by implementing a two factor authentication mechanism. In addition to validating new hardware via a single authentication methodology, this invention involves a second validation mechanism, driven by external vendor or trusted peer network information. Once the single authentication method has been performed, the OS then performs a second validation check by searching information provided by an external vendor or trusted peer network. If the OS queries a vendor, the vendor site can confirm the safety of the hardware and correlate it with the user for whom it was purchased. Alternatively, the OS can query a peer network to validate that the hardware to be added has been on a peer network before and that it was not harmful to the system. Should either query return a negative result, the OS can prompt the user to ask further validation questions of the sites, deny the new hardware access to the network or allow the user to override the query and authenticate the new hardware.

Unique Concepts

The unique concept of this invention is its use of vendor or peer information to authenticate new hardware. Furthermore, this invention can be used for authentication when a user wants to attach new hardware via cloud computing and/or a virtual server.

3. DESCRIPTION OF THE INVENTION

Figure 1 depicts the system for operation of the Assisted Two Factor Authentication Mechanism via a Trusted External Source

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 OS is an operating system, such as Linux, residing on the Network Server. 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 Trusted External Data Source is a site or list compiled by a trusted vendor (such as Dell or Microsoft)

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

The Identifier is a piece of data that uniquely identifies the New Hardware such as a MAC Address, serial number, or other data. The Identifier can be used to safely authenticate the New Hardware.

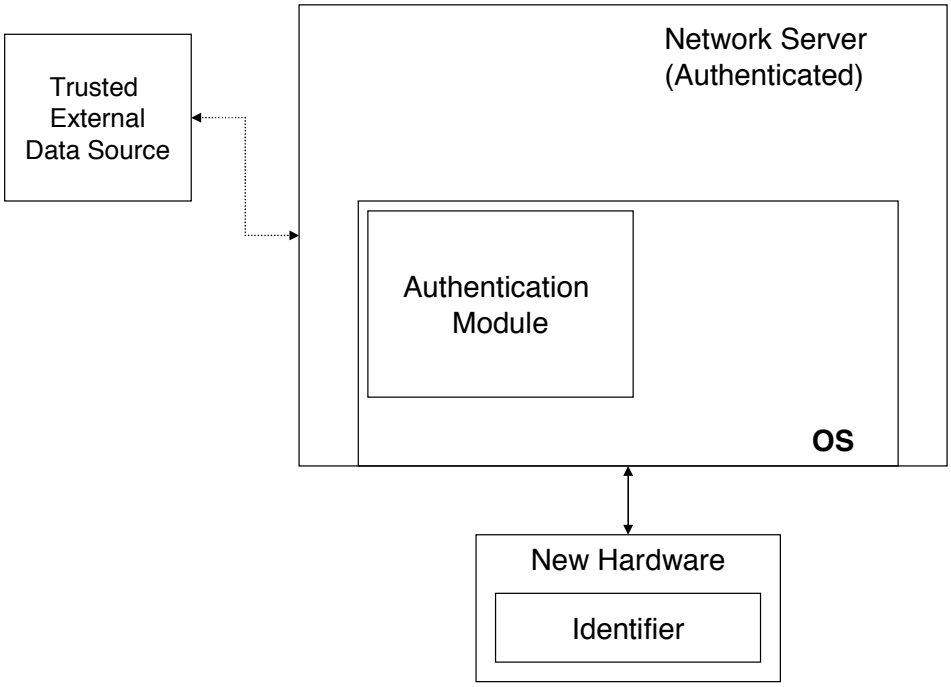

Figure 1. System for Two Factor Authentication Mechanism via a Trusted External Source

Figure 2 shows the methodology for Authenticating a New Hardware Device via an External Trusted Source.

In step 1, the user adds a new hardware device to a secured network via a Network Server and optionally authenticates it via a traditional method.

In step 2, the Network Server queries the New Hardware for the Identifier.

In step 3, the Authentication Module sends the Identifier to a Trusted External Data Source via the internet or network location to determine if the New Hardware can be further authenticated.

In step 4, the Trusted External Data Source attempts to verify the authenticity of the New Hardware using the provided information. If the New Hardware is validated, continue to step 7. If the New Hardware cannot be validated, proceed to optional step 5.

In optional step 5, the Authentication Module prompts the user to send more validation questions to the same or other Trusted External Data Sources. If the user chooses to attempt further validation, proceed to step 4. If the user declines, proceed to optional step 6.

In optional step 6, the User is prompted to override the authentication. If the User chooses to override, proceed to Step 7. If the User does not choose to override, proceed to step 8.

In step 7, access is allowed to the network, and the method ends.

In step 8, access to the network is denied, and the method ends.

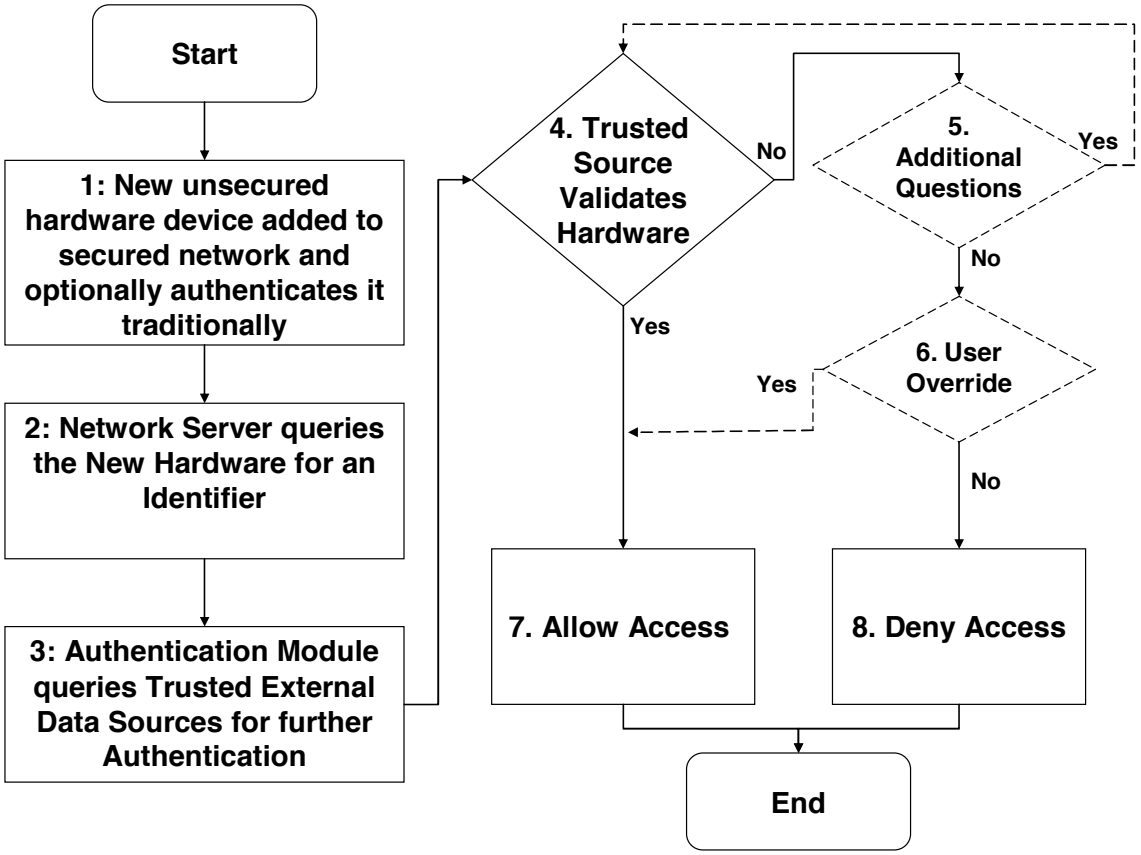

Figure 2. Methodology for Authenticating a New Hardware Device via an External Trusted Source