# SYSTEM AND METHOD FOR DEVICE AUTHENTICATION WITH BUILT-IN TOLERANCE

[0001] This application claims priority to U.S. Provisional Application No. 61/252,960 which was filed October 19, 2009 and which is fully incorporated herein by reference.

## BACKGROUND

### 1. Field of the Invention

[0002] The present invention is directed toward a method and system for building tolerance into comparisons of device fingerprints when authenticating a device.

### 2. Description of the Related Art

[0003] Controlling access to a secured network is one of the biggest challenges for critical infrastructure. Since the majority of existing infrastructures use computers to connect to the Ethernet or Internet, there is an increased possibility for security breaches into such infrastructures. One way to reduce security breaches is to strictly enforce authentication methods such as comparison of password, personal information, secret question, machine identifier, etc. against various stored data and password information. However, in certain approaches, if there is even a slight or minor difference between a device identifier or fingerprint for a device that seeks to be authenticated versus a database of known fingerprints corresponding to known authorized devices, then the request for authentication is rejected or denied.

[0004] From a practical standpoint, it is quite possible for a user of given known device (e.g., a device that is known and authorized to access a secured network), to upgrade, replace, or otherwise modify one or more components of the device. If the device fingerprint may be based on or generated from various device components, including upgraded or modified components, it is quite possible that the known device may no longer have a fingerprint or identifier that will be recognized by the authentication system. For example,, a valid device and machine may inadvertently be denied an authenticated status because of upgrade(s) to typical components such as memory, video card, etc. Accordingly, it would be desirable to provide an authentication method with built in flexibility or tolerance to allow for some upgrades or changes to the device.

## SUMMARY

[0005] The following presents a simplified summary of one or more embodiments in order to provide a basic understanding of such embodiments. This summary is not an extensive overview of all contemplated embodiments, and is intended to neither identify key or critical elements of all embodiments nor delineate the scope of any or all embodiments. Its sole purpose is to present some concepts of one or more embodiments in a simplified form as a prelude to the more detailed description that is presented later.

[0006] In accordance with one or more embodiments and corresponding disclosure thereof, various aspects are described in connection with a method for allowing tolerance in the authentication process of a digital fingering of a device. By building in tolerance into the authentication process, the risk of rejecting a valid device is reduced. Some tolerance is needed because users may upgrade their hardware and/or software, thus changing the environment of their devices. Once the environment is changed, the authentication software/client one the device may generate a different digital fingerprint. Thus, without built in tolerance, a valid device may be rejected once an upgrade is made to the device.

[0007] In accordance with one or more embodiments and corresponding disclosure thereof, various aspects are described in connection with a method for building tolerance into authentication of a device, the method comprising: receiving and storing first digital fingerprint of the device during a first boot of an authenticating software on the device, the first digital fingerprint being based on a first set of device components; receiving a second digital fingerprint from the device at a subsequent time; comparing the second digital fingerprint with a plurality of stored digital fingerprints of known devices; in response to the comparison indicating a mismatch between the second digital fingerprint and the plurality of stored digital fingerprints, generating a request code comprising instructions for the device to generate a third digital fingerprint using the first set of device components; sending the request code to the remote device; receiving the third digital fingerprint from the remote device in response to the request code; and authenticating the device based on a comparison of the first and third digital fingerprints.

[0008] In the foregoing method, the first digital fingerprint may be generated using specific components, such as a typical-upgrade list and a non-typical-upgrade list. The typical-upgrade list may comprise one or more components such as graphic card, random access memory, sound card, network adaptor, hard drive, CD/DVD drive, and Ethernet controller. The non-typical-upgrade list may comprise one or more components such as motherboard, USB host controller, central microprocessor, PCI Bus, and System CMOS Clock.

[0009] The foregoing method may also include the process of receiving component list of the device at the first boot of the authenticating software on the device. This list of components may be used to generate the request code, which may exclusively comprise components from the list. In this way, a control digital fingerprint may be generated to be compared with the first digital fingerprint.

[0010] In one embodiment, the authentication process may further include: generating a control metric by comparing differences between the first and second digital fingerprints. The control metric may identify fingerprint portions and their respective components of the device that generated the differences between the first and second digital fingerprints. The control metric may help identify components missing and/or was upgraded in the device. A second metric may also be generated by comparing differences between the first and third digital fingerprints. Each metric may comprise data identifying a fingerprint portion and associated component that caused the difference. The device may be validly authenticated when the associated component of the control metric and the associated component of the second metric are identical. This means the difference found in the comparison may be caused by a single component. When this is the case, there is a high probability that the changed in the digital fingerprint is caused by an upgrade rather than being caused by an entirely different device.

[0011] In the foregoing method, in one embodiment, the authentication server may be configured to parse out the digital fingerprint into a plurality of logical portions. Each logical portion may represent a component corresponding to a fingerprint portion. During the comparison of a received digital fingerprint from the device with stored digital fingerprints of known devices, the authentication server may flag each portion for which it failed to find a match. When the comparison process is completed, the device may be validly authenticated if there are matching portions for at least 75% of the logical portions of the received fingerprint. It should be noted that other percentages could be implemented.

[0012] In accordance with yet another embodiment of the present invention a computer readable medium is provided. The computer readable medium having stored thereon, computer executable instructions that, if executed by a device, cause the device to perform a method comprising: receiving a first digital fingerprint from a device having a plurality of digital fingerprint portions, each fingerprint portion being associated with a component of the device; authenticating the received digital fingerprint against stored digital fingerprints; flagging each digital fingerprint portion creating an error during authentication; categorizing associated component of each fingerprint portion as a typical-upgrade component or a non-typical-upgrade component; and granting the digital fingerprint a valid authenticated status when the flagged fingerprint portions have a predetermined typical-upgrade/non-typical-upgrade ratio.

[0013] In accordance with yet another embodiment of the present invention, a computer readable medium is provided. The computer readable medium may have stored thereon, computer executable instructions that, when executed by a device, cause the device to perform a method comprising: receiving and storing first digital fingerprint of the device during a first boot of an authenticating software on the device, the first digital fingerprint being based on a first set of device components; receiving a second digital fingerprint from the device at a subsequent time; comparing the second digital fingerprint with a plurality of stored digital fingerprints of known devices; in response to the comparison indicating a mismatch between the second digital fingerprint and the plurality of stored digital fingerprints, generating a request code comprising instructions for the device to generate a third digital fingerprint using the first set of device components; sending the request code to the remote device; receiving the third digital fingerprint from the remote device in response to the request code; and authenticating the device based on a comparison of the first and third digital fingerprints.

[0014] In accordance with one or more embodiments and corresponding disclosure thereof, various aspects are described in connection with a method for authenticating a device, the method comprising: comparing the received digital fingerprint with stored digital fingerprints of known devices; flagging each digital fingerprint portion that creates an error during authentication; categorizing associated component of each fingerprint portion as a typical-upgrade component or a non-typical-upgrade component; and  granting the digital fingerprint a valid authenticated status when the flagged fingerprint portions exceed a predetermined typical-upgrade/non-typical-upgrade ratio.

[0015] To the accomplishment of the foregoing and related ends, the one or more embodiments comprise the features hereinafter fully described and particularly pointed out in the claims.  The following description and the annexed drawings set forth in detail certain illustrative aspects of the one or more embodiments.  These aspects are indicative, however, of but a few of the various ways in which the principles of various embodiments may be employed and the described embodiments are intended to include all such aspects and their equivalents.

## BRIEF DESCRIPTION OF THE DRAWINGS

[0016] The present invention, in accordance with one or more various embodiments, is described in detail with reference to the following figures.  The drawings are provided for purposes of illustration only and merely depict typical or example embodiments of the invention. These drawings are provided to facilitate the reader’s understanding of the invention and shall not be considered limiting of the breadth, scope, or applicability of the invention.

[0017] FIG. 1 is a block diagram illustrating an exemplary environment within which a method for authenticating remote devices may be implemented according to one embodiment of the present invention.

[0018] FIG. 2 is a block diagram representing memory allocation for a device identifier used in accordance with principles of the present invention.

[0019] FIG. 3A is a process flow chart illustrating one embodiment of a method according to the invention for device authentication with built-in tolerance.

[0020] FIG. 3B is a continuation of the process flow diagram of FIG. 3A.

[0021] FIG. 4 is a process flow chart illustrating another embodiment of a method according to the invention for device authentication with built-in tolerance.

DOCKET ALARM

# Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

## Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

## Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

## Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

## API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

### LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

### FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

### E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

**WHAT WILL YOU BUILD?** | **sales@docketalarm.com** | **1-866-77-FASTCASE**

fastcase®
Smarter legal research.