IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Utility Patent Application (Provisional)
Specification

INVENTION NAME

System and Method for Cryptographic Security Functions Based on Anticipated Changes in Computer Minutia

INVENTORS

Paul T. Miller, Irvine California and George A. Tuvell, Thompson's Station, Tennessee; jointly as founders of mSIGNIA, a California corporation

ASSIGNEE

mSIGNIA, a California corporation

BACKGROUND of INVENTION and PRIOR ART

The present invention is in the technical field of computers. More particularly, the present invention is in the technical field of:

- Computers connecting to the internet or other network
- Computers connecting to a network, where computers includes but is not limited to
  - Traditional PC's
  - Non-traditional PC's (i.e. smartphones, smart tablets)
  - Purpose-built network computers (i.e. smart meters, network equipment, appliances)
  - Computers without a user interface (i.e. machine-to-machine functionality)
- Identifying computers which connect to a network
- Identifying computers which connect to each other with or without concurrent connection to a wide-area network
- Authenticating computer connections to an online service
- Authenticating users to an online service
- Encrypting information stored on a computer

Prior patents have identified a computer by calculating a hash of the minutia found on a computer to uniquely identify the computer, often referred to as a computer fingerprint. Computer fingerprints are used, among other things, to 'lock' software to a particular computer fingerprint and identify computers used in online actions to profile the history and potential risk of particular actions.

In existing art, the computer identifier is computed and remains functionally static typically using computer minutia not expected to change (i.e. serial numbers) to ensure reliability. Minutia which changes or evolves naturally with use of the computer is typically not preferred nor are such changes to minutia modeled or predicted for increased functionality. Thus, current computer fingerprints use a relatively small set of reasonably static minutia which may be prone to spoofing.

Prior art and implementations have sought to increase the number of minutia elements used in identifying the computer. However, as more minutia is included in the computation, the probability that changes occurred naturally to the minutia results in a new computer fingerprint. This falsely identifies a computer as 'different' when it is actually the same computer (often referred to as 'false negatives'). These changes to the minutia on a unique computer occur naturally during normal use and should not invalidate the computer fingerprint process or inconvenience the user or service by forcing a re-initialization of the computer fingerprint.

Other inventive work by Paul Miller utilizes predictive manufacturing characteristics to obsolete purpose-built identity tokens. The invention was submitted as a US application 2003/0084311 A1. However, the prior art does not use knowledge of predictive mass production minutia to anticipate changes to a calculated computer identifier.

Prior art cited references appear in the following table:

Patent Number	Issue or Filing Date	First-Named Inventor	Company
US 2008/0244744 A1	Jan 29, 2008	Thomas et al	ThreatMetrix
US 2010/0296653 A1	Sep 14, 2006	Richardson	Uniloc
US 2003/0084311 A1	05/2003	Merrien et al	Gemplus
US 5490216	Sep 21 1993	Richardson	Uniloc
US 7272728	Jun 14, 2004	Peeso et al	ioVation
US 2005/0278542 A1	Feb 15, 2005	Pierson	n/a
US 6148407	Sep 30 1997	Aucsmith	Intel

SUMMARY OF THE INVENTION

Several technologies exist for processing security and assurance claims using static values. These include passwords themselves and static 'seed keys' for functions like one-time-password and challenge-respond security mechanisms. Even public key cryptography is based off a *static* key pair (public & private). mSIGNIA uses a very large numeric representation of the computer minutia (100,000's of bits) to support a range of security functions in a verifiable manner (a cornerstone of security). mSIGNIA's methods, based on the predicable dynamic nature of the computer minutia, allow for verification of the computer minutia (as if they were a single static value) but the entire computer identifier is not required to be static, elements of the minutia can (and are expected to) change and evolve over time. The resultant validation of a dynamic computer identifier based on minutia uses a complex 'confidence scoring' which isolates elements of the computer minutia that have changed and uses confidence weightings against the predictability of such changes.

Layering static minutia, slow-changing minutia and predictably changing minutia creates a very large computer identifier which can be processed as subsets of minutia. These subsets of minutia function as a static identifier over a particular interval and provide increased security while being fault-tolerant to normal and natural anomalies.

To achieve fault tolerance over a possibly changing set of minutia, anticipated changes and multiple subsets that provide back-up to any single subset can be used. By using mass produced computers which both contain a vast array of minutia and predictable evolution paths of computer minutia, a dynamic encryption system of methods based on evolving computer minutia can be maintained for the benefit of nearly any security function. In addition, since the range of minutia is so large, certain cryptographic functions can be performed several times using different subsets of minutia. In this manner, should one subset of minutia change, cryptographic checks using other minutia subsets and the anticipated changes to the minutia can improve fault tolerance.

Assertions regarding a computer's uniqueness, confidence in the computer uniqueness and service-orientated directives (i.e. provision, lock/hold, erase, transfer, blacklist, etc.) are formulated, controlled and directed by the computer identity provider service; computer identifier libraries gather the computer info and act on the computer in response to computer identity provider service directives. The heuristics for the predictive and constantly changing elements of a computer identity are performed in the cloud using data forwarded by the computer identifier libraries AND data gleaned from industry sources. Industry data includes cataloguing publically available data (such as over-the-air upgrades (OS, firmware, applications, etc) and network updates) over the range of possible computers. While nearly infinitely larger than the changes that can occur to a single computer (lending security via a broader search space) it is still finite and, therefore, useful in predictive heuristics regarding computers in use.

The present invention is a system and methods for secure computer identification including:

- Registering online service providers with the computer identity provider service to create custom computer identifier libraries that conduct security functions but are resistant to successful attacks to other services and prohibit profiling users collaborating online service providers
- Collecting and registering the minutia of computers with the computer identity provider system, tying the computer minutia to an online service provider account identifier
- Gathering industry information regarding updates to computer hardware, firmware and software to create a catalogue of industry identifiers which may possible appear on registered computers when they are updated. The catalogued industry minutia data is indexed and the possible minutia and current computer minutia are combined and permutations intelligently stored to anticipate future computer minutia possibilities
- Identifying a computer based on a hash from a subset of minutia taken from a very wide range of minutia found on the computer including hardware, firmware and software. The authentication of the computer can be performed as an intelligent challenge and response which indexes minutia and, when compared to possible responses from anticipated minutia, can ascertain minutia changes on the computer without having to actually exchange the minutia between the computer and computer identity provider service
- Scoring the confidence of a valid response based on the computer minutia used, the anticipated and expected changes to the computer minutia used and non-computer factors such as user PIN entry. Different challenges can be intelligently chosen to achieve a response that yields a higher confidence score.
- Protecting the application and data running on a computer by using the computer minutia in cryptographic functions such as encrypted memory, local identification of the computer and heartbeat to prohibit application self-destruction. Some cryptographic functions are computed using more than one subsets of computer minutia to allow back-up functionality should minutia used in the cryptographic function change. The high number of meaningful minutia enables a more complex interaction between the computer and software computing the identifier. The increased 'chatter', a mix of meaningful and decoy reads of minutia, obscure which minutia is meaningful thereby increasing the difficulty to spoof minutia values and intercept calls intended to counterfeit the original computer
- Notifying a wide range of online service providers should a computer status change. This enables a single event to trigger responses from a wide range of registered online service providers so that security and service continuity are maintained
- Forcing a user to enter a service or computer PIN on a registered computer to increase the confidence score and ensure that a valid user is controlling an identified computer

DRAWINGS - FIGURES

Table of Figures

#	Figure Brief	Figure Title
1	Overview	Change Tolerant Computer Identification System Overview including systems for the Computer, Network, Computer ID Provider, Service Provider, Third Party Software Distributor and Service User
2	App Delivery	Service Provider App Delivery System with Service Provider registration with the Computer ID Provider System, Library Build, Application Build and Application Distribution to the Computer System
3	Register Computer	Registration of Computer System Minutia and Service
4	Catalogue Industry	Catalogue and Model Industry Minutia to Create and Update Anticipated Minutia Databases
5	Auth Computer	Authentication exchanges Using Challenge and Response and Static and Dynamic Computer Minutia
6	Score Auth	Authentication Scoring, Confidence rating and Step-up authentication processing
7	App Security	Application processing for local and update security functions
8	CIDP Lifecycle Management	Computer Identity Provider Lifecycle functionality and services to Service Providers
9	PIN Entry	User PIN Entry System

Table of References

The Referenced items of the invention are shown in the table below. The figures containing the items within the drawing are shown, but the items may be referenced in the specification related to the drawing without necessarily appearing in the figure drawing. The Type and System columns are included for additional information but the items are not necessarily limited to the Type and System mentioned in the table.

Item #	Name	Figure #	Type	System
10	Computer ID Provider System	1-9	System	ID Provider
12	Event Log	1	DB	ID Provider
14	Service Provider System	1-3, 6-8	System	OSP
16	Network	1-9	System	Network
18	Computer System	1-3, 5-9	System	Computer
20	Service User	1-3, 8,9	User	User
22	Third Party Software Distributor	1,2,6	System	3rd Party
30	Service Provider Registration	2	Process	ID Provider
32	Partner Info & IDs	2,3,5,9	DB	ID Provider
34	Customer Library Creation	2	Process	ID Provider
36	Custom CompID Libraries	2	DB	ID Provider
38	Send Custom Library to Service	2	Process	ID Provider
40	Build Application	2	Process	OSP
42	Applicaton Source Code	2	DB	OSP
44	Service Provider App	2,3,5,7	Process	3rd Party

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.