2131 IFW

Attorney's Docket No.: P-9047-US5 *PATENT*

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Patent Application of:	Examiner: Jenise E. Jackson
Daniel Schreiber David Guedaliah	Art Unit: 2131
Application No: 09/595,839	
Filed: June 16, 2000	
For: METHOD AND APPARATUS FOR PREVENTING REUSE OF TEXT, IMAGES, AND SOFTWARE TRANSMITTED VIA NETWORKS	

Mail Stop AMENDMENT
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

AMENDMENT AND RESPONSE TO OFFICE ACTION
UNDER 37 C.F.R. §1.111

Sir:

In response to the Office Action dated September 26, 2005 and pursuant to 37 C.F.R. §1.111, applicants respectfully request that the above-identified application be amended as follows.

IN THE CLAIMS:

Please substitute the following claims for the pending claims with the same number:

12. (currently amended) A method for limiting the operational life of software in a network environment, the method comprising:

transmitting a program applet with a password embedded therewithin from a server computer to a client computer, via a network, the password having a limited operational life, and the program applet including executable code that runs on the client computer;

receiving by the server computer, from said program applet ~~at~~ running on the client computer, via said network, (i) a request for information stored in a restricted access storage area of the server computer, and (ii) said embedded password;

authenticating said embedded password by the server computer, whenever said receiving occurs;

thereafter transmitting said information from the server computer, to said program applet ~~at~~ running on the client computer, via said network, while said embedded password is valid; and

invalidating said embedded password by the server computer, coincident with an invalidation event.

13. (previously presented) A method according to claim **12** wherein said invalidating comprises invalidating said embedded password at a predetermined time.

14. (previously presented) A method according to claim **12** wherein said invalidating comprises invalidating said embedded password after lapse of a predetermined time from when said request was received.

15. (previously presented) A method according to claim **12** wherein said invalidating comprises invalidating said embedded password upon the detection of a loss of communication with said client.

16. (canceled)

17. (canceled)

18. (previously presented) A method according to claim **12** wherein said transmitting a program applet comprises generating said embedded password.

27. (currently amended) A network-based software authentication system comprising a server computer, the server computer comprising:

a password generator;

password validation apparatus;

a restricted-access storage area;

a program applet including executable code that runs on a client computer; and

invalidation apparatus;

wherein said server computer is operative to:

a) cause said password generator to generate a password, the password having a limited operational life;

b) embed said password within said program applet, and transmit said program applet with said password embedded therewithin to ~~a~~ the client computer via a network;

c) receive from said program applet ~~at~~ running on the client computer, (i) a request for information, and (ii) said embedded password for authentication;

d) authenticate said embedded password using said password validation apparatus, whenever information requested is stored in the restricted-access storage area;

e) transmit said information to said program applet ~~at~~ running on the client computer, via said network, while said embedded password is valid; and

f) invalidate said embedded password using said invalidation apparatus coincident with an invalidation event.

28. (original) A system according to claim **27** wherein said invalidation event comprises the arrival of a predetermined time.

29. (previously presented) A system according to claim **27** wherein said invalidation event comprises the lapsing of a predetermined time from when said request was received.

30. (original) A system according to claim **27** wherein said invalidation event comprises the detection of a loss of communication with said client.

31. (canceled)

32. (canceled)

33. (canceled)

REMARKS

Applicants have carefully studied the outstanding Office Action. The present amendment is intended to place the application in condition for allowance and is believed to overcome all of the objections and rejections made by the Examiner. Favorable reconsideration and allowance of the application are respectfully requested.

Applicants have amended claims **12** and **27** to more properly claim the present invention. No new matter has been added. Claims **12 – 15, 18** and **27 - 30** are presented for examination.

In Paragraphs 1 - 7 of the Office Action, claims **12 – 15, 18** and **27 – 30** have been rejected under 35 U.S.C. §103(a) as being unpatentable over Dykes et al, U.S. Patent No. 5,872,915 ("Dykes") in view of Scherpbier, U.S. Patent No. 6,263,365 ("Scherpbier").

The rejections of claims **12 – 15, 18** and **27 – 30** in paragraphs 1 - 7 of the Office Action will now be dealt with specifically.

As to amended independent method claim **12**, applicants respectfully submit that the limitation in claim **12** of:

"*transmitting a program applet with a password embedded therewithin from a server computer to a client computer, via a network, the password having a limited operational life, the program applet including executable code that runs on the client computer*"

is neither shown nor suggested in Dykes or Scherpbier, taken individually or in combination.

In Paragraph 3 of the Office Action, the Examiner has cited Dykes as disclosing transmitting a program applet with a password embedded therein from a server computer to a client computer. Applicants respectfully submit that a program applet is an application that runs on a client computer, whereas Dykes describes an application that runs on a server computer. Specifically, the data flow in Dykes is illustrated in FIGS. **3**, **5** and **6**, and described at col. 7, line 29 – col. 8, line 27, and at col. 8, line 31 – col. 10 line 17, and at col. 14, line 54 – col. 15, line 15, respectively. Following the notation from FIG. **6** of Dykes, input to software application **342** (FIGS. **3** and **5**) flows from

web browser --> web server --> gateway --> software application
CW-->WS-->GCS-->SACS ,

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.