EXHIBIT 7

Attorney Docket No.: 60644-8007.US01 PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Patent Application of: Shlomo TOUBOUL	Examiner: Christopher A. Revak
Application No: 10/838,889	Art Unit: 2131
Filed: May 3, 2004	Confirmation No.: 5334
Title: METHOD AND SYSTEM FOR CACHING AT SECURE GATEWAYS	

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

AMENDMENT ACCOMPANYING REQUEST FOR CONTINUED EXAMINATION (RCE)

Sir:

In response to the Office Action dated October 4, 2007 ("the Office Action"), the following amendments and remarks are submitted for consideration, together with a Request for Continued Examination (RCE).

Amendments to the specification begin on page 2 of this paper.

Amendments to the claims are reflected in the claim listing that begins on page 3 of this paper.

Remarks begin on page 11 of this paper.

AMENDMENTS TO THE SPECIFICATION

Please amend page 11, second paragraph, as follows:

Use of security profiles and security policies are described in Applicant's US Patent No. 6,092,194 entitled SYSTEM AND METHOD FOR PROTECTING A COMPUTER AND A NETWORK FROM HOSTILE DOWNLOADABLES, US Patent No. 6,154,844 entitled SYSTEM AND METHOD FOR ATTACHING A DOWNLOADABLE SECURITY PROFILE TO A DOWNLOADABLE, US Patent No. 6,167,520 entitled SYSTEM AND METHOD FOR PROTECTING A CLIENT DURING RUNTIME FROM HOSTILE DOWNLOADABLES, [[and]] US Patent No. 6,480,962 entitled SYSTEM AND METHOD FOR PROTECTING A CLIENT DURING RUNTIME FROM HOSTILE DOWNLOADABLES, US Patent No. 6,804,780 entitled SYSTEM AND METHOD FOR PROTECTING A COMPUTER AND A NETWORK FROM HOSTILE DOWNLOADABLES, US Patent No. 6,965,968 entitled POLICY-BASED CACHING, and US Patent No. 7,058,822 entitled MALICIOUS MOBILE CODE RUNTIME MONITORING SYSTEM AND METHODS.

Please amend page 14, second paragraph, as follows:

Otherwise, if the gateway computer determines at step 270 that the web page is to be blocked, then at step 280 the gateway computer takes an alternate action. Preferably, the alternate action is defined within the client computer's security ~~profile~~ policy, and includes alternatives such as sending a notification to the client computer, sending a notification to a system administrator, sending only a portion of the requested web page, or allowing the intranet computer to decide whether or not to trust the suspicious web page.

CLAIM LISTING

1. (Currently Amended) A computer gateway for an intranet of computers, comprising:

a scanner for scanning incoming files from the Internet and deriving security profiles for the incoming files ~~therefor~~ , wherein each of the ~~and the~~ security profiles comprises ~~being lists~~ a list of computer commands that [[the]] a corresponding one of the incoming files is ~~files are~~ programmed to perform;

a file cache for storing files that have been scanned by the scanner for future access, wherein each of the stored files is indexed by a file identifier; and

a security profile cache for storing the security profiles derived by the scanner, ~~for files;~~ wherein each of the security profiles is indexed in the security profile cache by a file identifier associated with a corresponding file stored in the file cache; and

a security policy cache for storing security policies for intranet computers within [[an]] the intranet, the security policies each including a list of restrictions for files that are transmitted to a corresponding subset of the intranet computers.

2 – 4. (Canceled)

5. (Currently Amended) The computer gateway of claim [[4]] 1 wherein each of the file identifiers comprises a hash value derived from a corresponding one of the stored files ~~the file IDs are hash values of files~~.

6. (Currently Amended) The computer gateway of claim 5 wherein the file cache and the security profile cache use the file identifiers ~~IDs are used~~ to ensure that duplicate files are not scanned and not cached more than once.

7 – 11. (Canceled)

12. (Currently Amended) A method of operating ~~for operation of~~ a network gateway for an intranet of computers, the method comprising:

receiving a request from an intranet computer for a file ~~on the Internet~~;

determining whether the requested file resides within a file cache at the network gateway;

if said determining is affirmative:

retrieving a security profile for the requested file from a security profile cache at the network gateway, the security profile including a list of at least one computer command that the requested file is programmed to perform; and

if said determining is not affirmative:

retrieving the requested file from the Internet;

scanning the retrieved file to derive a security profile including a list of computer commands that the retrieved file is programmed to perform; ~~determine computer commands that the file is programmed to perform;~~

~~deriving a security profile for the retrieved file;~~

storing the retrieved file within the file cache for future access; and

storing the security profile for the retrieved file within [[a]] the security profile cache for future access.[[;]]

~~retrieving a security policy for the intranet computer from a security policy cache at the network gateway, the security policy defining restrictions for transmitting files to the intranet computer; and~~

~~comparing the security profile for the requested file vis a vis the security policy for the intranet computer, to determine whether transmission of the requested file to the intranet computer is to be restricted.~~

13 - 14. (Canceled)

15. (Currently Amended) The method of claim 12 further comprising indexing the ~~file~~ security profile cache so that security profiles of files are indexed according to file identifiers (IDs).

16. (Original) The method of claim 15 wherein the file IDs are hash values of files.

17. (Currently Amended) The method of claim 16 further comprising managing the file cache and the security profile cache using the file IDs so that duplicate files are not scanned and not cached more than once.

18 - 23. (Canceled)

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.