US010055576B2

(12) **United States Patent**
Milner et al.

(10) **Patent No.: US 10,055,576 B2**
(45) **Date of Patent: *Aug. 21, 2018**

(54) **DETECTION OF MALICIOUS SOFTWARE PACKAGES**

(71) Applicant: **Red Hat, Inc.**, Raleigh, NC (US)

(72) Inventors: **Steve Bradford Milner**, Tallahassee, FL (US); **James Robert Bowes**, Remote, OR (US)

(73) Assignee: **Red Hat, Inc.**, Raleigh, NC (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **15/729,304**

(22) Filed: **Oct. 10, 2017**

(65) **Prior Publication Data**

US 2018/0032720 A1 Feb. 1, 2018

Related U.S. Application Data

(63) Continuation of application No. 12/898,876, filed on Oct. 6, 2010, now Pat. No. 9,792,429.

(51) **Int. Cl.**

G06F 21/00	(2013.01)
G06F 21/51	(2013.01)
G06F 21/56	(2013.01)

(52) **U.S. Cl.**

CPC ***G06F 21/51*** (2013.01); ***G06F 21/564*** (2013.01)

(58) **Field of Classification Search**

CPC G06F 21/51; G06F 21/564

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,324,647	B1 *	11/2001	Bowman-Amuah	H04L 63/0227 709/223
6,438,749	B1	8/2002	Chamberlain	
7,240,336	B1	7/2007	Baker	
7,512,939	B2	3/2009	Brookner	

(Continued)

OTHER PUBLICATIONS

Seth Ketby Vidal, "Systems and Methods for Initiating Software Repairs in Conjuction With Software Pac Kage Updates", U.S. Appl. No. 12/714,200, filed Feb. 26, 2010.

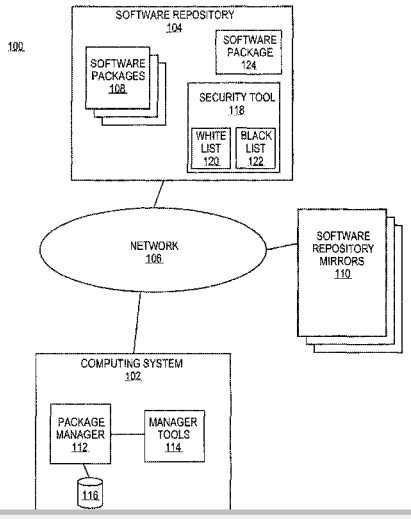
(Continued)

Primary Examiner — Mahfuzur Rahman
Assistant Examiner — Narciso Victoria
(74) *Attorney, Agent, or Firm* — Lowenstein Sandler LLP

(57) **ABSTRACT**

Systems and methods for a security tool that verifies the security of a software package. An example method may involve identifying a plurality of components contained in a software package comprising one of a JAR file, an Android application package, a docker image, a container file, or a virtual machine image; comparing the components contained in the software package to a list of known components; classifying the software package as insecure when at least one of the components matches an insecure component, or as secure when each of the compared components matches a corresponding secure component on the list of known components; preventing addition of the software package to a software repository when the software package is classified as insecure; and when insecure, providing an interface to enable a user to request the components of the software package be added as a secure component on the list of known components.

20 Claims, 7 Drawing Sheets



(56) **References Cited**

U.S. PATENT DOCUMENTS

7,624,393	B2	11/2009	Egan et al.	
7,657,885	B2	2/2010	Anderson	
7,836,341	B1	11/2010	Krishnan	
2003/0051235	A1	3/2003	Simpson	
2003/0229890	A1	12/2003	Lau et al.	
2005/0210459	A1	9/2005	Henderson et al.	
2006/0190773	A1	8/2006	Rao et al.	
2006/0230398	A1	10/2006	Yokota	
2007/0038991	A1	2/2007	Schuff et al.	
2007/0157192	A1	7/2007	Hoefler et al.	
2007/0169075	A1	7/2007	Lill et al.	
2007/0180490	A1*	8/2007	Renzi	G06F 21/577 726/1
2008/0134165	A1	6/2008	Anderson et al.	
2008/0141240	A1	6/2008	Uthe	
2008/0201705	A1	8/2008	Wookey	
2009/0013319	A1	1/2009	Williams et al.	
2009/0037897	A1	2/2009	Dull et al.	
2009/0083852	A1*	3/2009	Kuo	G06F 21/564 726/22
2009/0300595	A1	12/2009	Moran et al.	
2010/0023933	A1	1/2010	Bryant et al.	
2010/0058308	A1	3/2010	Demshur et al.	
2010/0058314	A1	3/2010	Wang	
2010/0083243	A1	4/2010	Miocarelli et al.	
2010/0114939	A1*	5/2010	Schulman	G06F 11/3672 707/769
2011/0166969	A1*	7/2011	Hughes	G06F 8/20 705/30

OTHER PUBLICATIONS

Seth Kelby Vidal, Manager, U.S."Systems and Methods for Diagnostic Notification Via Package Update", U.S. Appl. No. 12/714,258, filed Feb. 26, 2010.

Seth Ketby Vidal, "Systems and Methods for Managing Software Package Updates Using Commubication Pipes", U.S. Appl. No. 12/714,208, filed Feb. 26, 2010.

Seth Ketby Vidal, "Systems and Methods for Generating and Storing Translation Information as Package Manager", U.S. Appl. No. 12/714,171, filed Feb. 26, 2010.0.

Seth Kelby Vidal. "Systems and Methods for Generating Predictive Diagnostics Via Package Update Manag Er", U.S. Appl. No. 12/714,222, filed Feb. 26, 2010.

James Antill, "Systems and Methods for Defining and Enforcing Access Poucy for Package Update Proces Ses", U.S. Appl. No. 12/873,850, filed Sep. 1, 2010.

Seth Kelby Vidal, Systems and Methods for Generating Cached Representations of Encoded Package Profile, U.S. Appl. No. 12/788,139, filed May 26, 2010.

Seth Kelby Vidal, Systems and Methods for Generating Cached Representations of Host Package Inventories in Remote Package Repositories, U.S. Appl. No. 12/790,699, filed May 28, 2010.

Seth Kelby Vidal, "Systems and Methods for Generating Package Profiles in Software Package Repositories Using Selective Subsets of Packages",U.S. Appl. No. 12/873,557, flied Sep. 1, 2010.

Se!h Kelby Vidal, Systems and Methods for Generating an Encoded Package Profile Based on Executing Host Processes, U.S. Appl. No. 12/787,104, filed May 26, 2010.

Seth Kelby Vidal, "Systems and Methods for Restoring Machine State History Related to Detected Faults in Package Update Process", U.S. Appl. No. 12/788,036, filed May 26, 2010.

Seth Kelby Vidal, "Systems and Methods for Generating Cuent Quaufication to Execute Package Update Manager", U.S. Appl. No. 12/788,458, flied May 27, 2010.

Seth Kelby Vidal, "Systems and Methods for Determining When to Update a Package Manager Software", U.S. Appl. No. 12/790,752, filed May 28, 2010.

Seth Kelby Vidal, "Systems and Methods for Generating Exportable Encoded Identifications of Networked Machines Based on Installed Package Profiles", U.S. Appl. No. 12/758,416, flied Apr. 27, 2010.

Seth Kelby Vida!, "Systems and Methods for Tracking Computing Systems Utiuz!ng Software Repositories", U.S. Appl. No. 12/955,671, filed Nov. 29, 2010.

Seth Kelby Vidal, "Systems and Methods for Automatic Upgrade and Downgrade in Package Update Operations", U.S. Appl. No. 12/892,227, filed Sep. 28, 2010.

Seth Kelby Vidal, "Systems and Methods for Managing Versions of Software Packages", U.S. Appl. No. 13/037,363, filed Mar. 1, 2011.

Seth Kelby Vidal. "Systems and Methods for Space Efficient Software Package Management", U.S. Appl. No. 12/610,006, filed Oct. 30, 2009.

Spybot—Search & Destroy, Overview, http://www.safer-networking.org/enlspybotsd/index.html, 4 pages.

LANDesk Patch Manager 9, LAN Desk Software, Inc., 4 pages.

Security for File Servers, Kaspersky Lab, http://usakaspersky.com/products-services|business/security-for-file-servers.

"About Symantec Scan Engine", Symantec, 2008, 12 pages.

"Symantec™ Scan Engine Software Developer's Guide", Symantec, 2008, 103 pages.

"Symantec™ Scan Engine Management Pack Integration Guide", Symantec, 2008, 18 pages.

"Symantec198 Scan Engine Implementation Guide", Symantec, 2008, 247 pages.

* cited by examiner

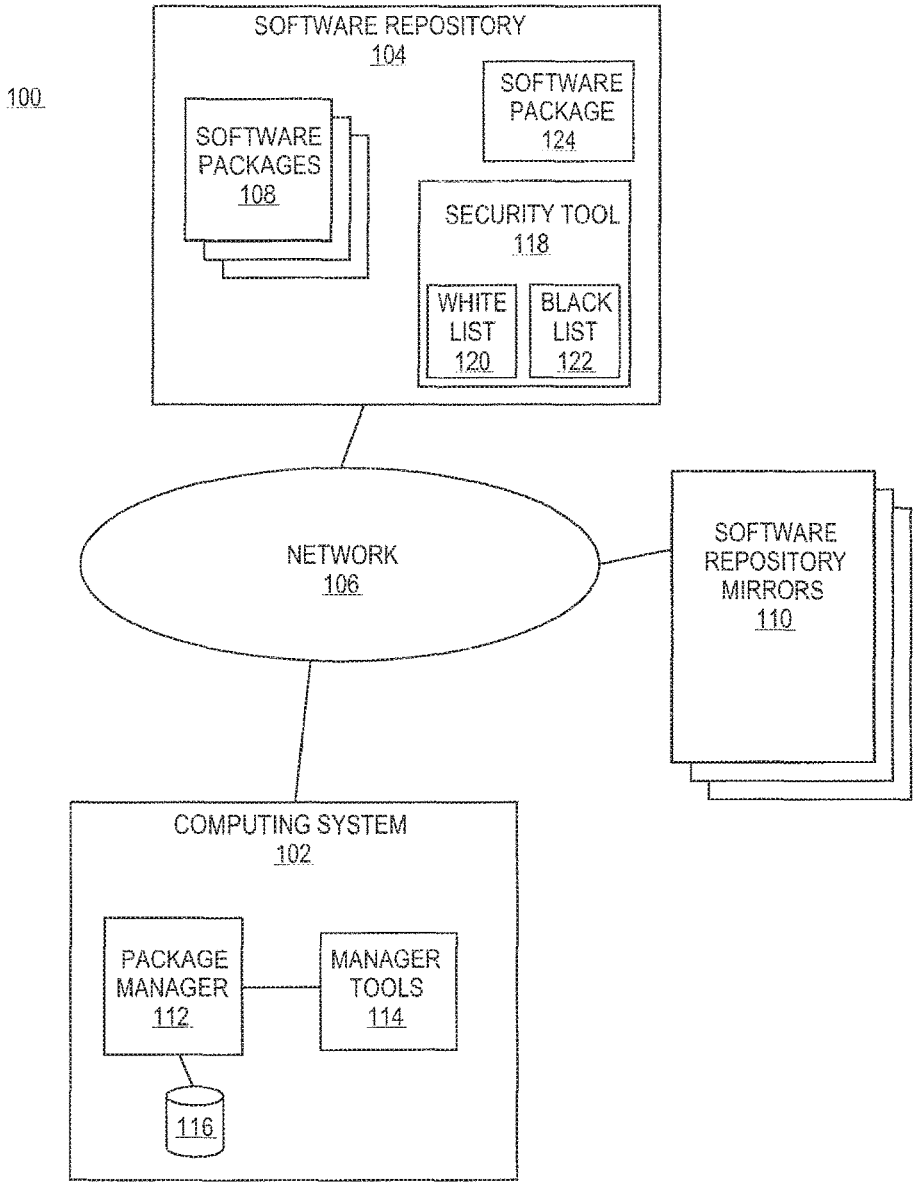


FIG. 1A

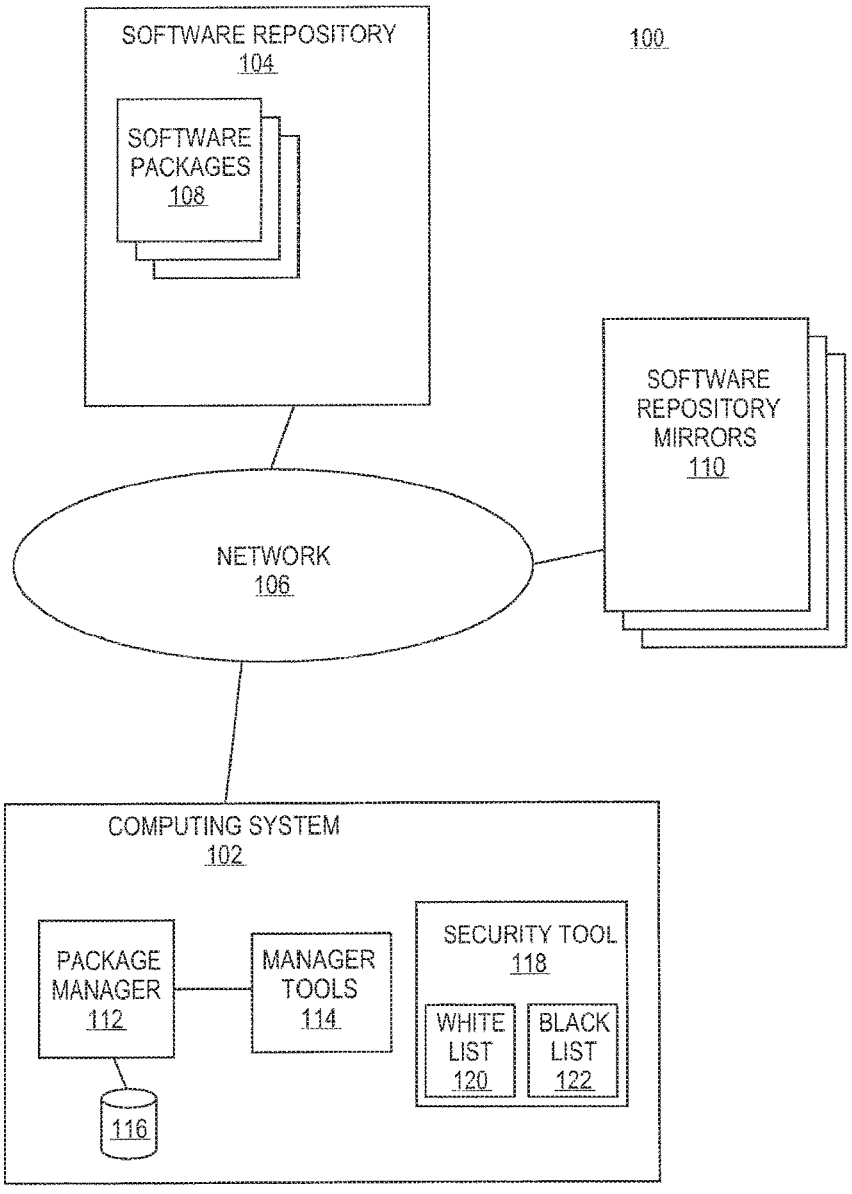


FIG. 1B

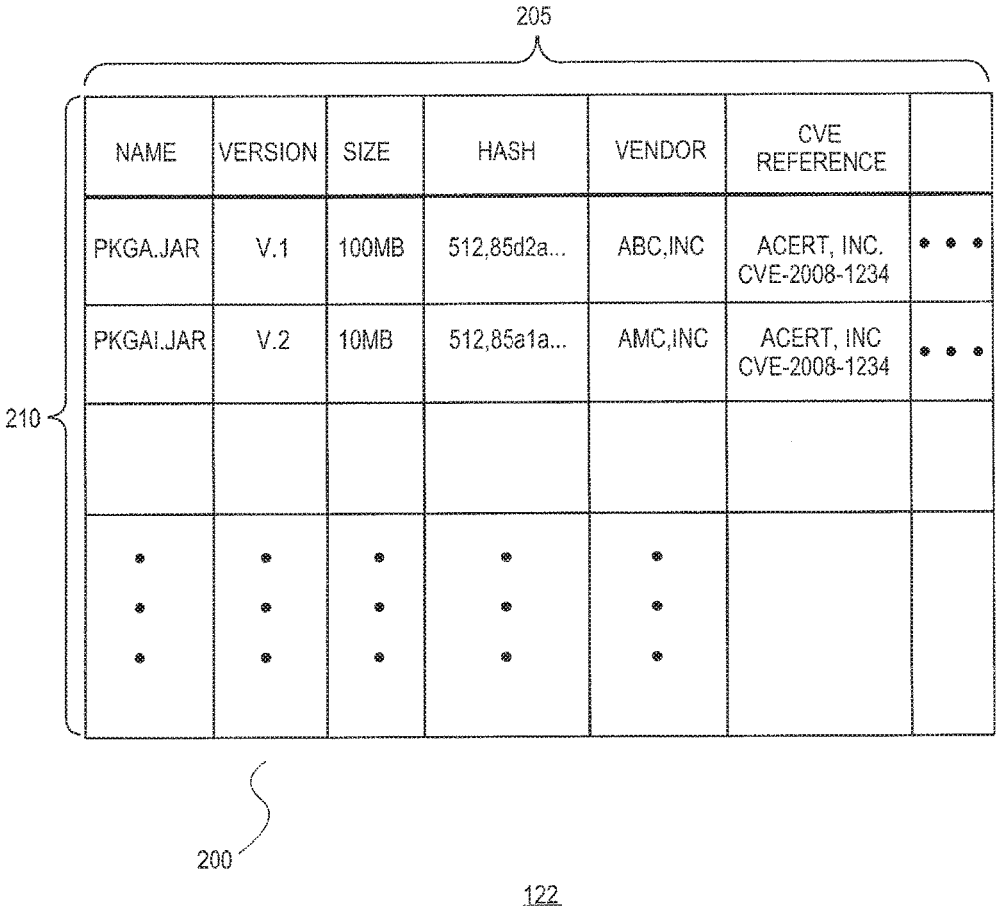


FIG. 2

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.