US009749349B1

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

(10) **Patent No.: US 9,749,349 B1**
(45) **Date of Patent: Aug. 29, 2017**

(54) **COMPUTER SECURITY VULNERABILITY ASSESSMENT**

(71) Applicant: **OPSWAT, Inc.**, San Francisco, CA (US)

(72) Inventors: **Benjamin Czarny**, San Francisco, CA (US); **Jianpeng Mo**, Burlingame, CA (US); **Ali Rezafard**, Millbrae, CA (US); **David Matthew Patt**, Kansas City, MO (US)

(73) Assignee: **OPSWAT, Inc.**, San Francisco, CA (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.

(21) Appl. No.: **15/275,123**

(22) Filed: **Sep. 23, 2016**

(51) **Int. Cl.**
H04L 29/06 (2006.01)
G06F 17/30 (2006.01)
G06F 21/57 (2013.01)

(52) **U.S. Cl.**
CPC ***H04L 63/1433*** (2013.01); ***G06F 17/30289*** (2013.01); ***G06F 21/577*** (2013.01); ***H04L 63/1425*** (2013.01)

(58) **Field of Classification Search**
CPC H04L 63/1433; H04L 63/1425; H04L 29/06904; G06F 21/577; G06F 17/30289
USPC 726/25
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

8,127,354	B1 *	2/2012	Bettini	G06F 21/577 726/22
8,474,004	B2 *	6/2013	Leone	G06F 21/51 380/59
8,654,340	B2 *	2/2014	Girard	G01Q 20/02 356/484
8,813,222	B1	8/2014	Codreanu et al.	
8,850,583	B1 *	9/2014	Nelson	H04L 63/1416 380/44
8,863,288	B1 *	10/2014	Savage	G06F 21/56 713/188
9,304,980	B1 *	4/2016	Hartsook	G06F 21/577
2004/0006704	A1 *	1/2004	Dahlstrom	G06F 21/577 726/25

(Continued)

OTHER PUBLICATIONS

Mellor, FlashMate hybrid hard drive works without Windows, InfoWorld, Oct. 11, 2007. pp. 1-2.

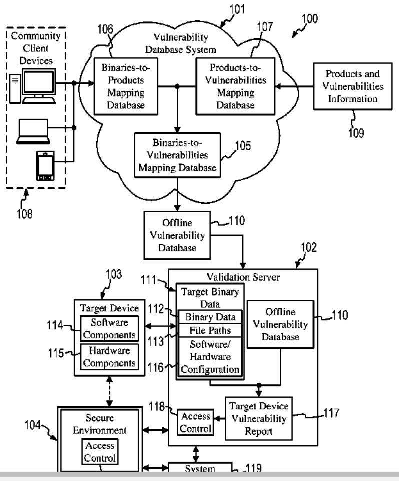
(Continued)

Primary Examiner — Hadi Armouche
Assistant Examiner — Shahriar Zarrineh
(74) *Attorney, Agent, or Firm* — The Mueller Law Office, P.C.

(57) **ABSTRACT**

Computer security vulnerability assessment is performed with product binary data and product vulnerability data that correspond with product identification data. A correspondence between the product binary data and the product vulnerability data is determined, and a binaries-to-vulnerabilities database is generated. The binaries-to-vulnerabilities database is used to scan binary data from a target device to find matches with the product binary data. A known security vulnerability of the target device is determined based on the scanning and the correspondence between the product binary data and the vulnerability data. In some embodiments, the target device is powered off and used as an external storage device to receive the binary data therefrom.

10 Claims, 8 Drawing Sheets


100
101
Vulnerability Database System
106
107
Community Client Devices
Binaries-to-Products Mapping Database
Products-to-Vulnerabilities Mapping Database
Products and Vulnerabilities Information
109
Binaries-to-Vulnerabilities Mapping Database
105
108
Offline Vulnerability Database
110
102
Validation Server
103
111
Target Binary Data
112
Binary Data
File Paths
113
Software/ Hardware Configuration
116
Offline Vulnerability Database
110
Target Device
Software Components
114
Hardware Components
115
118
Access Control
Target Device Vulnerability Report
117
104
Secure Environment
Access Control
System
119

(56) **References Cited**

U.S. PATENT DOCUMENTS

2005/0022021	A1 *	1/2005	Bardsley	G06F 21/577 726/4
2005/0132206	A1 *	6/2005	Palliyil	G06F 21/566 713/188
2007/0067846	A1 *	3/2007	McFarlane	H04L 63/1433 726/25
2007/0271360	A1 *	11/2007	Sahita	G06F 21/577 709/223
2010/0083346	A1 *	4/2010	Forman	G06F 21/55 726/1
2011/0179477	A1 *	7/2011	Starnes	G06F 21/52 726/9
2013/0191919	A1 *	7/2013	Basavapatna	G06F 21/577 726/25
2014/0173737	A1 *	6/2014	Toback	G06F 21/57 726/25
2015/0127607	A1 *	5/2015	Savage	G06F 17/30194 707/610
2015/0207811	A1 *	7/2015	Feher	G06F 21/577 726/25
2015/0213272	A1 *	7/2015	Shezaf	H04L 63/1433 726/25
2015/0363294	A1 *	12/2015	Carback, III	G06F 8/37 717/132
2016/0112444	A1	4/2016	Palumbo et al.	
2016/0188882	A1 *	6/2016	Mahrous	G06F 21/577 726/25
2016/0232358	A1 *	8/2016	Grieco	G06F 21/577
2016/0300063	A1 *	10/2016	Daymont	G06F 21/566

OTHER PUBLICATIONS

Mitchell, Web Security Pop-Up Trojan Making Rounds Again, This Time Attacking Both Windows and Macs, The Internet Patrol, May 9, 2011, pp. 1-4, Accessed on May 30, 2016, https://www.theinternetpatrol.com/websecuritypopuptrojanmakingroundsagainthistimeattackingbothwindowsandmacs/.

OS X EI Capitan [OT], NeoGAF, May 27, 2016, p. 34, 3 pages, Accessed on May 30, 2016, http://www.neogaf.com/forum/showthread.php?p=204835278.

* cited by examiner

Fig. 1

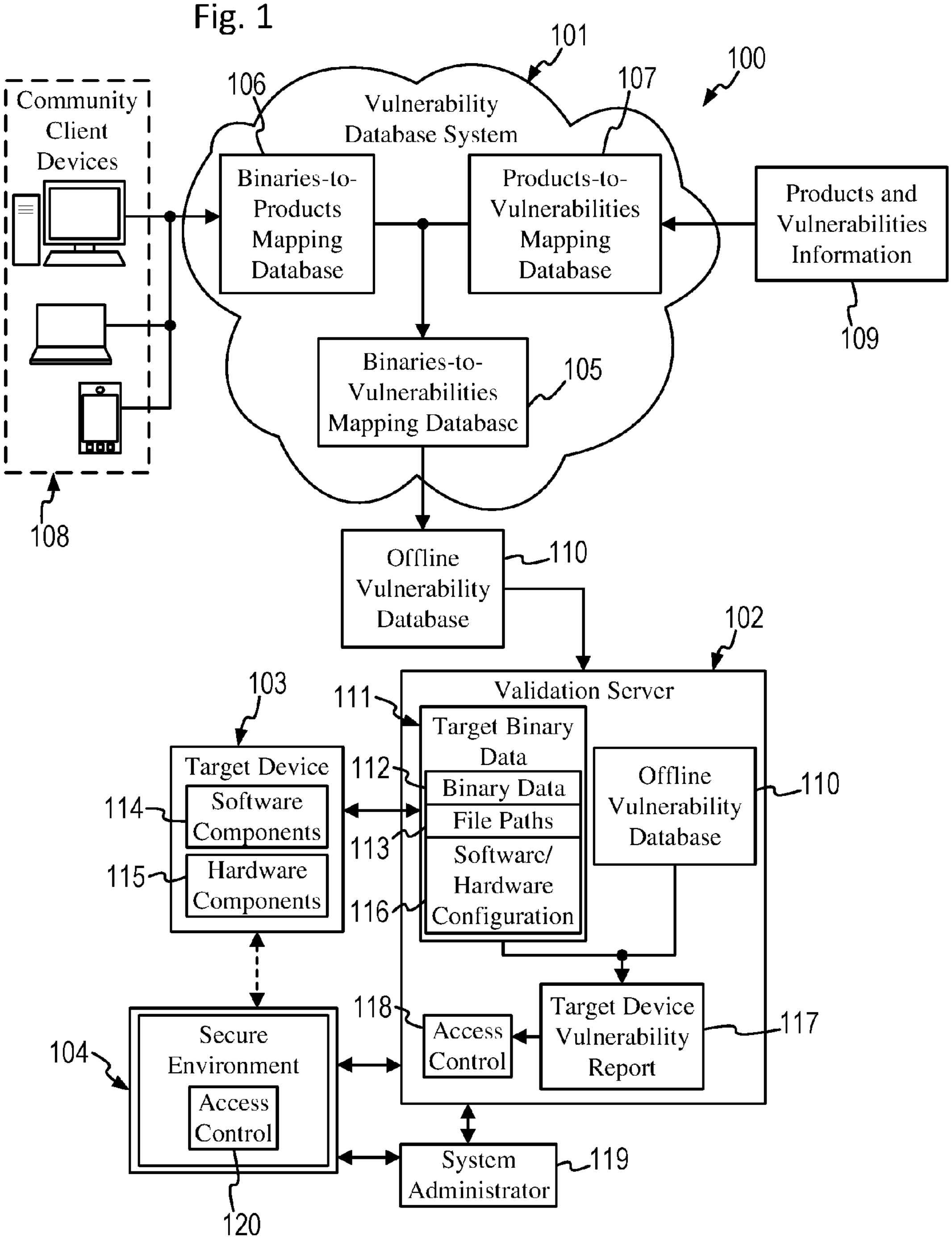

101
100
106
107
Vulnerability Database System
Community Client Devices
Binaries-to-Products Mapping Database
Products-to-Vulnerabilities Mapping Database
Products and Vulnerabilities Information
109
Binaries-to-Vulnerabilities Mapping Database
105
108
Offline Vulnerability Database
110
102
103
111
Validation Server
Target Binary Data
Target Device
Software Components
Hardware Components
114
115
112
Binary Data
File Paths
113
Software/ Hardware Configuration
116
Offline Vulnerability Database
110
118
Access Control
Target Device Vulnerability Report
117
104
Secure Environment
Access Control
System Administrator
119
120

Fig. 2

106

Product	Version	Binary Files
ESET Endpoint Security	5.0.2214.4	Exe1_sha256, Exe2_sha256, Dll3_sha256, ...
ESET Endpoint Security	5.0.1055.2	Exe1_sha256, Exe4_sha256, Dll5_sha256, ...
ESET Endpoint Security	4.2.3330.1	Exe1_sha256, Exe2_sha256, Dll5_sha256, ...
ESET Endpoint Security	4.0.1211.2	Dll3_sha256, Dll5_sha256, Exe1_sha256, ...
JAVA	7.11	Dll9_sha256, Dll12_sha256, Dll13_sha256, ...
…	…	…

Fig. 3

107

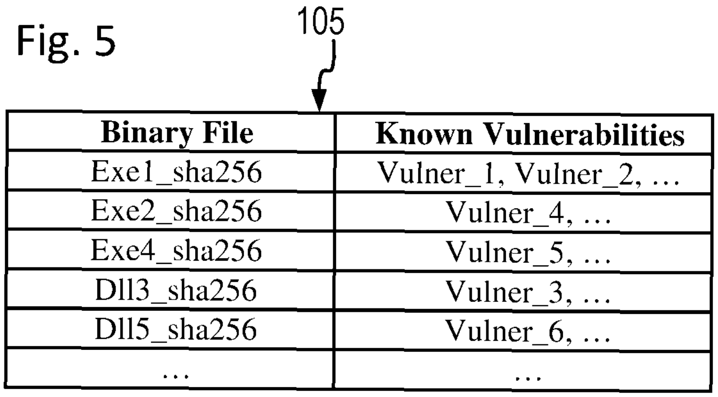
Product	Version	Known Vulnerabilities
ESET Endpoint Security	5.0.2214.4	Vulner_1, Vulner_2, Vulner_3, Vulner_4, ...
ESET Endpoint Security	5.0.1055.2	Vulner_1, Vulner_2, Vulner_5, Vulner_6, ...
ESET Endpoint Security	4.2.4230.1	Vulner_1, Vulner_2, Vulner_7, Vulner_8, ...
ESET Endpoint Security	4.0.1211.2	Vulner_1, Vulner_2, Vulner_3, Vulner_6, ...
Adobe Flash	3.0.5	Vulner_2, Vulner_9, Vulner_10, …
…	…	…

Fig. 4

400

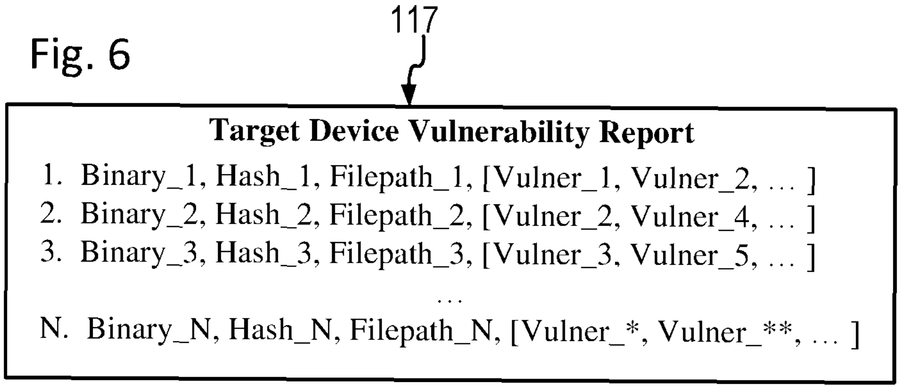
Product	Version	Binary Files	Known Vulnerabilities
ESET Endpoint Security	5.0.2214.4	Exe1_sha256, Exe2_sha256, Dll3_sha256, ...	Vulner_1, Vulner_2, Vulner_3, Vulner_4, ...
ESET Endpoint Security	5.0.1055.2	Exe1_sha256, Exe4_sha256, Dll5_sha256, ...	Vulner_1, Vulner_2, Vulner_5, Vulner_6, ...
ESET Endpoint Security	4.2.3330.1	Exe1_sha256, Exe2_sha256, Dll5_sha256, ...	Vulner_1, Vulner_2, Vulner_4, Vulner_6, ...
ESET Endpoint Security	4.0.1211.2	Dll3_sha256, Dll5_sha256, Exe1_sha256, ...	Vulner_1, Vulner_2, Vulner_3, Vulner_6, ...
JAVA	7.11	Dll9_sha256, Dll12_sha256, Dll13_sha256, ...	
Adobe Flash	3.0.5		Vulner_2, Vulner_9, Vulner_10, …
…	…	…	…

Fig. 5



Binary File	Known Vulnerabilities
Exe1_sha256	Vulner_1, Vulner_2, …
Exe2_sha256	Vulner_4, …
Exe4_sha256	Vulner_5, …
Dll3_sha256	Vulner_3, …
Dll5_sha256	Vulner_6, …
…	…

Fig. 6



Target Device Vulnerability Report

1. Binary_1, Hash_1, Filepath_1, [Vulner_1, Vulner_2, …]
2. Binary_2, Hash_2, Filepath_2, [Vulner_2, Vulner_4, …]
3. Binary_3, Hash_3, Filepath_3, [Vulner_3, Vulner_5, …]

…

N. Binary_N, Hash_N, Filepath_N, [Vulner_*, Vulner_**, …]

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.