US008621639B1

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

(10) **Patent No.: US 8,621,639 B1**
(45) **Date of Patent: *Dec. 31, 2013**

(54) **USING FUZZY CLASSIFICATION MODELS TO PERFORM MATCHING OPERATIONS IN A WEB APPLICATION SECURITY SCANNER**

(75) Inventors: **William Pennington**, San Jose, CA (US); **Jeremiah Grossman**, San Jose, CA (US); **Robert Stone**, Mountain View, CA (US); **Siamak Pazirandeh**, San Diego, CA (US)

(73) Assignee: **WhiteHat Security, Inc.**, Santa Clara, 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.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **13/307,382**

(22) Filed: **Nov. 30, 2011**

Related U.S. Application Data

(63) Continuation of application No. 11/864,736, filed on Sep. 28, 2007, now Pat. No. 8,087,088.

(60) Provisional application No. 60/827,405, filed on Sep. 28, 2006.

(51) **Int. Cl.**
G06F 21/00 (2013.01)

(52) **U.S. Cl.**
USPC **726/25**; 713/175; 709/206; 709/227; 705/3; 705/26; 380/30

(58) **Field of Classification Search**
USPC 726/25
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

7,237,265	B2	6/2007	Reshef et al.	
2002/0120685	A1*	8/2002	Srivastava et al.	709/203
2003/0233581	A1*	12/2003	Reshef et al.	713/201
2004/0019658	A1*	1/2004	Plastina et al.	709/217
2004/0023666	A1*	2/2004	Moon et al.	455/456.1
2004/0103315	A1	5/2004	Cooper et al.	
2005/0207361	A1*	9/2005	Rosenberg et al.	370/282
2006/0048214	A1	3/2006	Pennington et al.	
2006/0242104	A1	10/2006	Ellis et al.	
2007/0016563	A1*	1/2007	Omoigui	707/3
2007/0016615	A1	1/2007	Mohan et al.	
2007/0016960	A1*	1/2007	Glaser et al.	726/27
2007/0043702	A1	2/2007	Lakshminarayanan et al.	
2007/0079379	A1	4/2007	Sprosts et al.	
2007/0156820	A1*	7/2007	Peters	709/206
2007/0192709	A1	8/2007	Popp et al.	
2007/0299915	A1*	12/2007	Shraim et al.	709/206
2008/0010535	A1	1/2008	Dasgupta	
2013/0036476	A1*	2/2013	Roever et al.	726/27

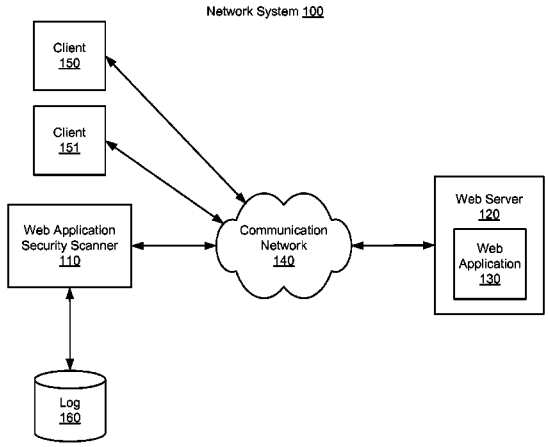
OTHER PUBLICATIONS

Fuzz-Web: A Methodology Based on Fuzzy Logic for Assessing Web Sites|http://www.mirlabs.org/ijcisim/regular_papers_2013/Paper88.pdf|2013|p. 126-136| Kalle et al.*

* cited by examiner

Primary Examiner — Mahfuzur Rahman
(74) *Attorney, Agent, or Firm* — Davis Wright Tremaine LLP; Philip H. Albert

(57) **ABSTRACT**

A system provides for fuzzy classification in comparisons of scanner responses. A web application test suite performs tests against a web application by sending client requests from a testing computer to the server running the web application and checking how the web application responds. A thorough web application security scan might involve thousands of checks and responses. As a result, some sort of programmatic analysis is needed. One such evaluation involves comparing one response against another. Response matching that compares two HTTP responses might use fuzzy classification processes.

17 Claims, 5 Drawing Sheets