



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/685,784	11/27/2012	Joshua Lukas	XROC920110123US2	6076
127893	7590	11/30/2016	EXAMINER	
Streets & Steele - Lenovo (Singapore) Pte. Ltd. 13100 Wortham Center Drive Suite 245 Houston, TX 77065			ANDERSON, MICHAEL D	
			ART UNIT	PAPER NUMBER
			2433	
			MAIL DATE	DELIVERY MODE
			11/30/2016	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte JOSHUA LUKAS, GARY R. RICARD,
and TIMOTHY L. THOMPSON

Appeal 2015-003610
Application 13/685,784
Technology Center 2400

Before CARL L. SILVERMAN, MELISSA A. HAAPALA, and
MONICA S. ULLAGADDI, *Administrative Patent Judges*.

HAAPALA, *Administrative Patent Judge*.

DECISION ON APPEAL

This is a decision on appeal under 35 U.S.C. § 134(a) from a final rejection of claims 1–6 and 8–10.¹ We have jurisdiction under 35 U.S.C. § 6(b).

We reverse.

¹ Claim 7 was canceled. App. Br. 23.

INVENTION

Appellants' invention is directed to network intrusion detection in a network that includes a distributed virtual switch fabric. Spec. ¶ 2. Claim 8 is exemplary of the subject matter on appeal:

8. A computer-implemented method for detecting network intrusions in a networked computer system that includes a plurality of networks interconnecting a plurality of systems, the plurality of systems including a distributed virtual switch fabric that provides a virtual view of the plurality of networks and the plurality of systems, the method comprising the steps of:

(A) configuring a network intrusion detection system by performing the steps of:

querying the distributed virtual switch fabric to determine from the virtual view network topology and configuration of the networked computer system;

defining a plurality of attack signatures that specify characteristics of network intrusions;

defining a plurality of service actions that each may be performed automatically without input from a human system administrator when a network intrusion that matches at least one of the plurality of attack signatures is detected by the network intrusion detection system;

(B) running the network intrusion detection system, which performs the steps of:

monitoring network traffic in the networked computer system;

detecting a network intrusion in the networked computer system that matches at least one of the plurality of attack signatures; and

in response to detecting the network intrusion that matches the at least one of the plurality of attack signatures, when a corresponding action for the detected network intrusion is to notify a human system

administrator, notifying the human system administrator of the network intrusion, and when the corresponding action for the detected network intrusion is to perform a specified service action, automatically performing the specified service action and notifying the system administrator, wherein the specified service action comprises performing at least one of the following steps:

monitoring a compromised host that originated network traffic detected as the network intrusion;

quarantining the compromised host;

moving to a different network the compromised host; and

shutting down the compromised host.

REJECTIONS ON APPEAL

Claim 8 stands rejected under 35 U.S.C. § 102(b) as being anticipated by Mualem (US 7,463,590 B2; issued Dec. 9, 2008).

Claims 1–6, 9, and 10 stand rejected under 35 U.S.C. § 103(a) as being obvious over the combination of Mualem and Aybay (US 8,442,048 B2; issued May 14, 2013)

ISSUE

Appellants' contentions present us with the following dispositive issue: Did the Examiner err in finding Mualem discloses *querying the distributed virtual switch fabric to determine from the virtual view network topology and configuration of the networked computer system* (“querying” limitation) as recited in independent claim 8?

ANALYSIS

We have reviewed the Examiner's rejections in consideration of Appellants' contentions. Appellants have persuaded us the Examiner has failed to establish that the claims are unpatentable over the cited prior art.

Appellants contend Mualem does not disclose the "querying" limitation recited in claim 8. App. Br. 5, 7–10. Specifically, Appellants argue the portions of Mualem cited by the Examiner refer to various network protocols and that a query/response for ARP (address resolution protocol) does not read on the disputed limitation. *Id.* at 10. Appellants further argue the different network protocols are unrelated to any distributed virtual switch fabric. *Id.* Appellants also argue that even if the Examiner establishes Mualem discloses the recited distributed virtual switch fabric, nothing in Mualem queries the distributed virtual switch fabric as claimed. *Id.*

The Examiner construes a "virtual switch fabric" as "a software/virtual based switching system that would move data coming into a network node by the correct port to the next network node." Ans. 4. The Examiner finds Mualem explicitly discloses a switch/hub switching system. *Id.* at 5. The Examiner further finds Mualem's description of query/response for ARP discloses the "querying" limitation. *Id.* (citing Mualem 4:65–67).

Mualem describes a protocol anomaly detection module that looks for a number of anomalies, including a packet with Ethernet protocol of ARP that is not large enough to contain an ARP Header and an ARP packet that is not large enough to carry its advertised data. Mualem 3:60–63. The network packets that are received are stored in a session cache for analysis by the individual threat analysis modules. *Id.* at 4:40–44. In the section of Mualem cited by the Examiner as disclosing the querying limitation,

Mualem describes in at least one embodiment, TCP, UDP, ICMP, and ARP are tracked and that each maintain their own pool of specific session types, but all share a common pool of IP's, which includes query/response for ARP. *Id.* at 4:61–67. We agree with Appellants that the Examiner does not establish the described ARP query discloses the disputed limitation. Even assuming, *arguendo*, that we were to agree with the Examiner's construction of "virtual switch fabric" as encompassing Mualem's switch/hub, the cited section of Mualem does not describe the ARP query is to the switch/hub, nor does the Examiner provide any explanation that the ARP query implicitly or inherently queries the virtual switch fabric (switch/hub) as required by the claim. Furthermore, the Examiner does not sufficiently establish or explain how an ARP query determines both the recited network topology *and* the configuration of the networked computer system.

For the reasons stated above, Appellants persuade us the Examiner has not established Mualem discloses the "querying" limitation. Accordingly, we do not sustain the 35 U.S.C. § 102(b) rejection of claim 8.

Independent claims 1 and 9 also recite the "querying" limitation, for which the Examiner similarly relies on Mualem in the obviousness rejection of these claims. *See* Final Act. 7, 10. We, therefore, do not sustain the 35 U.S.C. § 103(a) rejection of claims 1, 8, and 9, and their dependent claims 2–6, and 10.

Appeal 2015-003610
Application 13/685,784

DECISION

We reverse the Examiner's decision to reject claims 1–6 and 8–10.

REVERSED