

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte LUNDY M. LEWIS, JOAO B. D. CABRERA, and
RAMAN K. MEHRA

Appeal 2008-2305
Application 10/138,836
Technology Center 2100

Decided: September 23, 2008

Before HOWARD B. BLANKENSHIP, JAY P. LUCAS, and
ST. JOHN COURTENAY III, *Administrative Patent Judges*.

COURTENAY, *Administrative Patent Judge*.

DECISION ON APPEAL

This is a decision on appeal under 35 U.S.C. § 134(a) from the Examiner's rejection of claims 1-23. We have jurisdiction under 35 U.S.C. § 6(b). An oral hearing for this appeal was conducted on Sept. 11, 2008.

We affirm.

THE INVENTION

Appellants' invention relates generally to network security. More particularly, Appellants' invention is directed to prediction of and prevention of damage from attacks on communications networks supporting video, voice, and data services (Spec. 1).

Independent claim 1 is illustrative:

1. An apparatus for security management in a data, voice, or video network comprising:
 - at least one data collector that collects data during an attack on said network;
 - a precursor discovery module that identifies at least one precursor of said attack on said network among the collected data;
 - at least one monitor that detects the presence of at least one of said identified precursors on said network; and
 - at least one protective module that protects at least one of said network, one or more associated applications, one or more associated systems, and one or more associated network services when said at least one monitor detects the presence of at least one of said identified precursors.

THE REFERENCE

The Examiner relies upon the following reference as evidence in support of the anticipation rejection:

Campbell US 6,839,850 B1¹ Jan. 4, 2005

THE REJECTION

1. Claims 1-23 stand rejected under 35 U.S.C. §102(e) as being anticipated by Campbell.

CONTENTIONS BY APPELLANTS

1. Appellants contend that the Examiner erred in rejecting claim 1 as being anticipated by Campbell under 35 U.S.C. § 102(e) because “Campbell fails to disclose at least the feature of ‘a precursor discovery module . . . [that] identifies at least one precursor of said attack on said network among the collected data,’ as recited in claim 1 . . .” (App. Br. 6).

2. Appellants also contend that the Examiner erred in rejecting claim 1 as being anticipated by Campbell under 35 U.S.C. § 102(e) because “Campbell fails to disclose . . . ‘at least one monitor that detects the presence of at least one of said identified precursors on said network,’ as recited in claim 1 . . .” (App. Br. 7-8).

¹ We note that both the Examiner and the Appellants have referenced the wrong patent number (i.e., 6,398,850) in the Answer and Brief, respectively (*see Ans. 2-3; see also App. Br. 5*). We consider this as a typographical error. U.S. Patent 6,839,850 to Campbell (issued Jan. 4, 2005) is the correct patent reference. Appellants correctly refer to Campbell’s U.S. Patent 6,839,850 on page 1 of the Reply Brief.

ISSUES

1. We consider the question of whether Campbell discloses “a precursor discovery module . . . [that] identifies at least one precursor of said attack on said network among the collected data,” as recited in claim 1.

2. We consider the question of whether Campbell discloses “at least one monitor that detects the presence of at least one of said identified precursors on said network,” as recited in claim 1.

PRINCIPLES OF LAW

In rejecting claims under 35 U.S.C. § 102, “[a] single prior art reference that discloses, either expressly or inherently, each limitation of a claim invalidates that claim by anticipation.” *Perricone v. Medicis Pharm. Corp.*, 432 F.3d 1368, 1375-76 (Fed. Cir. 2005) (citation omitted).

“Anticipation of a patent claim requires a finding that the claim at issue ‘reads on’ a prior art reference.” *Atlas Powder Co. v. IRECO, Inc.*, 190 F.3d 1342, 1346 (Fed Cir. 1999) (“In other words, if granting patent protection on the disputed claim would allow the patentee to exclude the public from practicing the prior art, then that claim is anticipated, regardless of whether it also covers subject matter not in the prior art.”) (Internal citations omitted).

Appellants have the burden on appeal to the Board to demonstrate error in the Examiner’s position. See *In re Kahn*, 441 F.3d 977, 985-86 (Fed. Cir. 2006). Therefore, we look to Appellants’ Briefs to show error in the proffered prima facie case.

FINDINGS OF FACT

The following Findings of Facts (FF) are shown by a preponderance of the evidence.

Campbell

1. Campbell discloses an intrusion detection system for detecting intrusion into and misuse of a computer on a computer network (col. 1, ll. 7-10).
2. Campbell discloses an intrusion detection system that automatically recognizes that certain events have occurred that make an intrusion or misuse likely, so as to provide early indications and warnings of a suspected intrusion or misuse (col. 1, ll. 12-13, 18-19).
3. Campbell discloses an intrusion detection system that identifies “potential threats to the processing system in near real-time, using a system that monitors user actions that interact with barriers and boundaries within the monitored processing system and provides a timely warning that a threat exists” (col. 4, ll. 45-49).
4. Campbell discloses an intrusion detection system that incorporates a “‘Security Indications and Warning Engine’ (SI&W Engine) that is used to determine potential security threats by processing information contained in system audits, which are tokens of user activity on the system” (col. 5, ll. 2-5).
5. Campbell discloses an intrusion detection system where “[u]ser activity is a series of user actions within the monitored computer network environment, as represented by a stream of audit events (e.g.,

- specific records that the Operating System (OS) software records to capture information about each happening)” (col. 5, ll. 5-10).
6. Campbell discloses an intrusion detection system where “[t]he events may be self-contained records with record attributes (date, time, user, machine) or may include links to other events.” (col. 5, ll. 10-12).
 7. Campbell discloses an intrusion detection system where “[s]ystem audits also represent activities performed by the OS on behalf of users. System audits include (1) OS audit trail records; (2) OS log file data; and (3) OS-maintained security state data” (col. 5, ll. 12-15).
 8. Campbell discloses an intrusion detection system where a “barrier is a system-level restriction on user actions” (col. 5, ll. 16-17), and a “boundary is a policy-based limitation on user actions” that “defines limitations of acceptable behavior for a user or group of users within an organization” (col. 5, ll. 24-26).
 9. Campbell discloses an intrusion detection system where the barriers and boundaries are translated into a set of key SI&W events to be monitored (col. 5, ll. 58-60).
 10. Campbell discloses an intrusion detection system where, “[i]n order to provide a measurement mechanism, the barriers and boundaries are represented within the SI&W engine by a set of gauges that measure activity against each of the key SI&W events. A gauge set is associated with every monitored user and machine in the monitored network environment.” (col. 5, ll. 59-65).
 11. Campbell discloses an intrusion detection system where “[i]nformation in the gauges [is] aggregated into other measures

- called criteria and indicators to determine whether a potential threat exists” (col. 6, ll. 2-5).
12. Campbell discloses an intrusion detection system where “[t]he SI&W Engine uses a hierarchical aggregation of information collected in the gauges to ultimately evaluate the potential of a threat to the monitored system and to determine whether to produce a warning” (col. 5, l. 66 through col. 6, ll. 2).
13. Campbell discloses an intrusion detection system where the SI&W Engine is “capable of indicating in near-real time that a potential security threat exists” (col. 6, ll. 8-10).

ANALYSIS

We consider the Examiner’s rejection of claims 1-23 as being anticipated by Campbell. Since Appellants’ arguments with respect to this rejection have treated these claims as a single group which stand or fall together, we select independent claim 1 as the representative claim for this rejection. *See* 37 C.F.R. § 41.37(c)(1)(vii).

Issue I

We decide the question of whether Campbell discloses “a precursor discovery module . . . [that] identifies at least one precursor of said attack on said network among the collected data,” as recited in representative claim 1.

Claim Construction

During prosecution, “the PTO gives claims their ‘broadest reasonable interpretation.’” *In re Bigio*, 381 F.3d 1320, 1324 (Fed. Cir. 2004) (quoting *In re Hyatt*, 211 F.3d 1367, 1372 (Fed. Cir. 2000)).

Here, the Examiner has read the claimed “precursor discovery module” on Campbell’s disclosure of a “Securities Indications and Warning” (SI&W) Engine (Ans., pp. 3, 9). We begin our analysis by broadly but reasonably construing the scope of the claimed “precursor discovery module” (claim 1). When we look to Appellants’ Specification for *context*, we find no specific definition for a “precursor discovery module.” However, Appellants do disclose the identification and discovery of “temporal precursors” or “precursor events,” in several portions of the Specification, as follows:

In one embodiment of the method of the present invention, data is collected during a network attack *in any manner known in the art*. The collected data is analyzed to identify specific *temporal precursors* of the attack. The future network activity is then monitored for the presence of the *precursors*. When the presence of a precursor is detected, appropriate protective action is taken.

(Spec. 5:5-9, emphasis added).

Any suitable algorithm may be used for discovering *precursors* of attacks including, *but not limited to*, statistics-based machine learning algorithms, neural networks and AI-based algorithms. In a typical example, the algorithm utilized will compare the data values collected during the attack state to data values collected during normal network operation, in order to identify those variables that manifest aberrant values or activity levels just prior to the onset of the attack.

(Spec. 5:24-29, emphasis added).

Thus, consistent with Appellants' disclosure, we construe the claimed "precursor discovery module" as broadly but reasonably reading on any software and/or hardware-based module that discovers data values indicative of the onset of a network attack (i.e., "precursors" of the onset of a network attack) using any algorithm.

We note that Campbell discloses an intrusion detection system that incorporates a "Security Indications and Warning Engine" (SI&W Engine) that determines potential security threats by processing information contained in system audits, which are tokens of user activity on the system. (FF 4). Campbell also discloses that the system audits include operating system audit trail records (FF 7). Because audit trails represent data values ("precursors") indicative of the onset of a network attack, we find no error in the Examiner's finding that the claimed "precursor discovery module" broadly but reasonably reads on Campbell's SI&W Engine. In particular, we find that Campbell's SI&W Engine is a software and/or hardware module that processes (i.e., identifies) the audit information (i.e., "precursors") among the collected data (*see* FF 4, 5, and 7). Therefore, we agree with the Examiner that Campbell discloses "a precursor discovery module . . . [that] identifies at least one precursor of said attack on said network among the collected data," as recited in claim 1.

While Appellants support their first contention by arguing that the "SI&W Engine does not analyze data collected during a potential attack to identify 'at least one precursor of said attack,'" we note that the limitation of "analyzing data" is not recited in representative claim 1 (*see* App. Br. 7, ¶2). Appellants also argue that there are no predefined scenarios or profiles used by Campbell's SI&W Engine (*id.*). Again, we note that "predefined

Appeal 2008-2305
Application 10/138,836

scenarios or profiles” are not recited in claim 1. Patentability is based upon the claims. “It is the *claims* that measure the invention.” *SRI Int’l v. Matsushita Elec. Corp. of America*, 775 F.2d 1107, 1121 (Fed. Cir. 1985) (*en banc*). “Moreover, limitations are not to be read into the claims from the specification.” *In re Van Geuns*, 988 F.2d 1181, 1184 (Fed. Cir. 1993) (citing *In re Zletz*, 893 F.2d 319, 321 (Fed. Cir. 1989)). Here, we find Appellants’ arguments directed to unclaimed subject matter to be unavailing.

Issue 2

We decide the question of whether Campbell discloses “at least one monitor that detects the presence of at least one of said identified precursors on said network,” as recited in representative claim 1.

In response, we note that Appellants have merely recited the language of the claim without providing any meaningful analysis (*see* App. Br. P. 7, last two lines, cont’d on p. 8, l. 1). We note that a statement which merely points out what a claim recites will not be considered an argument for separate patentability of the claim. *See* 37 C.F.R. § 41.37(c)(vii); *see also* 37 C.F.R. § 1.111(b). Thus, we find Appellants’ arguments are merely conclusory and do not meet the burden of showing error in the Examiner’s *prima facie* case of anticipation.

Moreover, we note that Campbell discloses an intrusion detection system where the SI&W Engine uses a hierarchical aggregation of information (i.e., precursors) to evaluate the potential of a threat to the *monitored* system and to determine whether to produce a warning (FF. 12, *see also* FF 2, 3, 7-10). Therefore, we find that Campbell discloses “at least

Appeal 2008-2305
Application 10/138,836

one monitor that detects the presence of at least one of said identified precursors on said network,” as recited in claim 1.

CONCLUSION OF LAW

Based on the findings of facts and analysis above, we conclude that Appellants have not met their burden of showing that the Examiner erred in rejecting representative claim 1 (and claims 2-23 that fall therewith) as being anticipated by Campbell under 35 U.S.C. § 102(e). Therefore, these claims are not patentable.

DECISION

We affirm the Examiner’s decision rejecting claims 1-23.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED

pgc

PILLSBURY WINTHROP SHAW PITTMAN, LLP
P.O. BOX 10500
MCLEAN VA 22102