



PTAB Oral Argument

April 22, 2024

KEYSIGHT TECHNOLOGIES, INC.

PETITIONER

v.

CENTRIPETAL NETWORKS, LLC

PATENT OWNER

CASE NO.: IPR2023-00445

PATENT NO.: 10,785,266

Overview

- Summary of The IPR Grounds
- The '266 Patent Overview
- Claims 1-27 Patentable over Law
- Claims 1-27 Patentable over Law in View of Wood
- Law in view of Wood and/or Jungck Fails to Render Obvious Dependent Claims

Overview

- **Summary of The IPR Grounds**
- The '266 Patent Overview
- Claims 1-27 Patentable over Law
- Claims 1-27 Patentable over Law in View of Wood
- Law in view of Wood and/or Jungck Fails to Render Obvious Dependent Claims

IPR2023-00445 ('266) – Summary of the IPR Grounds

Ground	Challenged Claims	35 U.S.C. §	References
1	1-27	103	Law
2	1-24	103	Law, Wood
3	6, 13, 19, 26	103	Law, Jungck
4	6, 13, 19, 26	103	Law, Wood, Jungck

Overview

- Summary of The IPR Grounds
- **The '266 Patent Overview**
- Claims 1-27 Patentable over Law
- Claims 1-27 Patentable over Law in View of Wood
- Law in view of Wood and/or Jungck Fails to Render Obvious Dependent Claims

The 266 Patent Overview: Methods and Systems for Protecting a Secured Network

US 10,785,266 B2

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

(10) **Patent No.:** US 10,785,266 B2
(45) **Date of Patent:** Sep. 22, 2020

(54) **METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK**

(71) **Applicant:** Centripetal Networks, Inc., Portsmouth, NH (US)

(72) **Inventors:** Steven Rogers, Leesburg, VA (US); Sean Moore, Hollis, NH (US)

(73) **Assignee:** Centripetal Networks, Inc., Portsmouth, NH (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.:** 16/728,766

(22) **Filed:** Dec. 27, 2019

(65) **Prior Publication Data**
US 2020/0137121 A1 Apr. 30, 2020

Related U.S. Application Data

(63) Continuation of application No. 16/111,524, filed on Aug. 24, 2018, now Pat. No. 10,567,437, which is a (Continued)

(51) **Int. Cl.**
H04L 29/06 (2006.01)
H04L 29/08 (2006.01)

(52) **U.S. Cl.**
CPC — H04L 63/20 (2013.01); H04L 63/0209 (2013.01); H04L 63/0218 (2013.01); (Continued)

(58) **Field of Classification Search**
CPC — H04L 63/20; H04L 63/0209; H04L 63/0218; H04L 63/0236; H04L 67/02
See application file for complete search history.

(56) **References Cited**
U.S. PATENT DOCUMENTS
6,098,172 A 8/2000 Cox et al.
6,147,976 A 11/2000 Shaul et al.
(Continued)
FOREIGN PATENT DOCUMENTS
AU 2006/283136 B2 9/2011
AU 2006/239171 B2 6/2012
(Continued)
OTHER PUBLICATIONS
Xu et al., Source Address Filtering Firewall to Defend against Denial of Service Attacks, Sep. 2004, IEEE 60th Vehicular Technology Conference, vol. 5, pp. 3296-3300 (Year: 2004).
(Continued)

Primary Examiner — Kenneth W. Chang
(74) **Attorney, Agent, or Firm** — Banner & Witcoff, Ltd.

(57) **ABSTRACT**
Methods and systems for protecting a secured network are presented. For example, one or more packet security gateways may be associated with a security policy management server. At each packet security gateway, a dynamic security policy may be received from the security policy management server, packets associated with a network protected by the packet security gateway may be received, and at least one of multiple packet transformation functions specified by the dynamic security policy may be performed on the packets. Performing the at least one of multiple packet transformation functions specified by the dynamic security policy on the packets may include performing at least one packet transformation function other than forwarding or dropping the packets.

27 Claims, 10 Drawing Sheets

(57)

ABSTRACT

Methods and systems for protecting a secured network are presented. For example, one or more packet security gateways may be associated with a security policy management server. At each packet security gateway, a dynamic security policy may be received from the security policy management server, packets associated with a network protected by the packet security gateway may be received, and at least one of multiple packet transformation functions specified by the dynamic security policy may be performed on the packets. Performing the at least one of multiple packet transformation functions specified by the dynamic security policy on the packets may include performing at least one packet transformation function other than forwarding or dropping the packets.

Ex. 1001 ('266), Abstract

The 266 Patent Overview: Methods and Systems for Protecting a Secured Network (cont'd)

- Directed to “[m]ethods and systems for protecting a secured network” because “the path a given packet may take cannot be readily predicted.”

'266 Patent at Abstract, 1:59-60, 5:23-24, 5:23-24

- PSGs placed at each boundary between protected and unprotected network.

Id. at 5:23-34, 3:54-58

- Fig 7 depicting multiple PSG's at boundaries between protected network and one or more networks other than the network protected by the PSGs.

Id. at Fig. 7; id. at 16:44-48, 16:62-17:1.

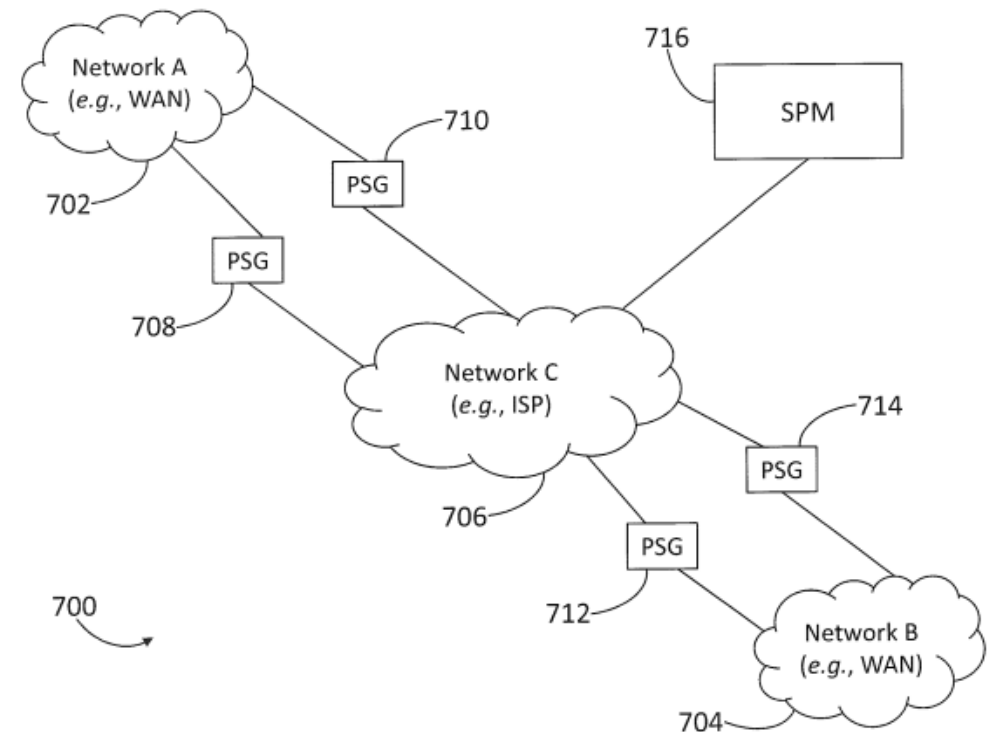


FIG. 7

The 266 Patent Overview: Methods and Systems for Protecting a Secured Network (cont'd)

US 10,785,266 B2

19

management servers A 816 and B 818), one or more operators associated with a single organization that desires to maintain distinct networks (e.g., networks A 802 and B 804) may maintain uniform dynamic security policies at each boundary of their distinct networks, while simultaneously enabling different dynamic security policies to be maintained for each network.

FIG. 9 illustrates an exemplary secure LAN environment protected in accordance with one or more aspects of the disclosure. Referring to FIG. 9, network environment 900 may be a LAN, including hosts A 902, B 904, and C 906. It may also include LAN switch 908. LAN switch 908 may be configured to switch network traffic (e.g., packets) between one or more of hosts A 902, B 904, and C 906. For example, LAN switch 908 may include a switching matrix configured to switch packets received from one or more of hosts A 902, B 904, and C 906 to one or more of hosts A 902, B 904, and C 906. LAN switch 908 may be associated with packet security gateway 910, and network environment 900 may include security policy management server 912.

In some embodiments, packet security gateway 910 may be embodied within LAN switch 908. Alternatively, packet security gateway 910 may be a device distinct from LAN switch 908, and LAN switch 908 may be configured to route network traffic through packet security gateway 910 (e.g., by modifying LAN switch 908's switching matrix). Packet security gateway 910 may be configured to receive one or more dynamic security policies from security policy management server 912. The dynamic security policies received from security policy management server 912 may include one or more rules specifying criteria associated with one or more of hosts A 902, B 904, and C 906, and may further specify one or more packet transformation functions to be performed on packets matching the specified criteria. Packet security gateway 910 may identify packets matching one or more of the criteria specified by the rules and may perform the associated packet transformation functions on the identified packets. By utilizing packet security gateway 910 within network environment 900, an operator of network environment 900 may be able to protect network environment 900 from network attacks, as well as implement one or more services (e.g., blacklist service, allowlist service, VoIP firewall service, phased restoration service, enqueueing service, multi-dimensional routing service, or monitoring service) within network environment 900. Network environment 900 may include multiple LAN switches with embedded or associated packet security gateways, each of the packet security gateways configured to receive one or more dynamic security policies from security policy management server 912.

FIG. 10 illustrates an exemplary method for protecting a secured network in accordance with one or more embodiments. The steps may be performed at each of one or more packet security gateways associated with a security policy management server. For example, each of packet security gateways 112, 114, 116, and 118 may be associated with security policy management server 120, and the steps may be performed at each of packet security gateways 112, 114, 116, and 118. At step 1000, a dynamic security policy is received from the security policy management server. For example, packet security gateway 112 may receive dynamic security policy 300 from security policy management server 120. At step 1002, packets associated with a network protected by each respective packet security gateway are received. For example, packet security gateway 112 may receive UDP packets from a device within network E 110 having an address that begins with 150 and that are destined

20

for port 3030 of a device within network A 102. At step 1004, a packet transformation function specified by the dynamic security policy is performed on the packets. For example, rule 308 of dynamic security policy 300 may specify that packets using the UDP protocol, coming from a source address that begins with 150, having any source port, destined for any address, and destined for port 3030 should have an accept packet transformation function performed on them. Packet filter 214 may identify the UDP packets received from the device within network E 110 as matching the criteria specified by rule 308. Packet transformation function 1 216 may be configured to forward packets, and packet security gateway 112 may utilize packet transformation function 1 216 to perform the accept packet transformation function specified by rule 308 on the UDP packets received from the device within network E 110.

The functions and steps described herein may be embodied in computer-usable data or computer-executable instructions, such as in one or more program modules, executed by one or more computers or other devices to perform one or more functions described herein. Generally, program modules include routines, programs, objects, components, data structures, etc. that perform particular tasks or implement particular abstract data types when executed by one or more processors in a computer or other data processing device. The computer-executable instructions may be stored on computer-readable medium such as a hard disk, optical disk, removable storage media, solid state memory, RAM, etc. As will be appreciated, the functionality of the program modules may be combined or distributed as desired in various embodiments. In addition, the functionality may be embodied in whole or in part in firmware or hardware equivalents, such as integrated circuits, application-specific integrated circuits (ASICs), field programmable gate arrays (FPGAs), and the like. Particular data structures may be used to more effectively implement one or more aspects of the disclosure, and such data structures are contemplated to be within the scope of computer executable instructions and computer-usable data described herein.

Although not required, one of ordinary skill in the art will appreciate that various aspects described herein may be embodied as a method, an apparatus, or as one or more computer-readable media storing computer-executable instructions. Accordingly, those aspects may take the form of an entirely hardware embodiment, an entirely software embodiment, an entirely firmware embodiment, or an embodiment combining software, hardware, and firmware aspects in any combination.

As described herein, the various methods and acts may be operative across one or more computing servers and one or more networks. The functionality may be distributed in any manner, or may be located in a single computing device (e.g., a server, a client computer, etc.).

Aspects of the disclosure have been described in terms of illustrative embodiments thereof. Numerous other embodiments, modifications, and variations within the scope and spirit of the appended claims will occur to persons of ordinary skill in the art from a review of this disclosure. For example, one of ordinary skill in the art will appreciate that the steps illustrated in the illustrative figures may be performed in other than the recited order, and that one or more steps illustrated may be optional.

What is claimed is:

1. A method of filtering packets at a packet security gateway, of a plurality of packet security gateways that collectively provide an entire interface across a boundary of a network protected by the packet security gateway and one

1. A method of filtering packets at a packet security gateway, of a plurality of packet security gateways that collectively provide an entire interface across a boundary of a network protected by the packet security gateway and one

Ex. 1001 ('266), Claim 1

The 266 Patent Overview: Methods and Systems for Protecting a Secured Network (cont'd)

- A PSG receives packets and proactively protects a network from malicious attacks based on dynamic security policies that are automatically created and/or altered by an SPMS based on malicious traffic information received from a malicious host tracker service. '266 Patent at 4:61-5:11, 5:34-53, 13:25-

34, 14:9-39, 19:38-45, Figs. 1, 5, 9

- PSGs placed at each boundary between protected and unprotected network.

Id. at 5:23-34, 3:54-58

- Fig 5 illustrates an exemplary SPMS 120, including processor 500 and memory 502.

Id. at Fig. 5 (annotated below); *id.* at 16:44-48, 16:62-17:1.

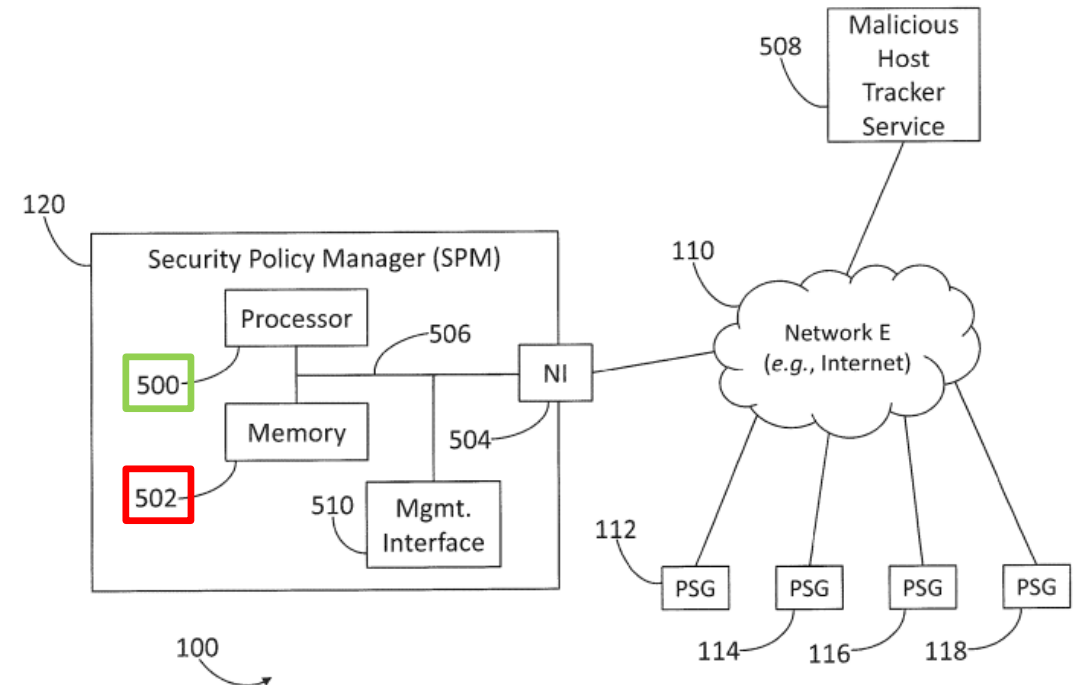


FIG. 5

The 266 Patent Overview: Methods and Systems for Protecting a Secured Network (cont'd)

● The SPMS :

- Automatically creates/alters a first set of packet filtering rules based on aggregated malicious network traffic from malicious host tracker services.
- Sends the first rule set to the PSGs.
- Alters the first rule set based on updates from the malicious host tracker services.
- Sends an updated second set of packet filtering rules to the PSGs.

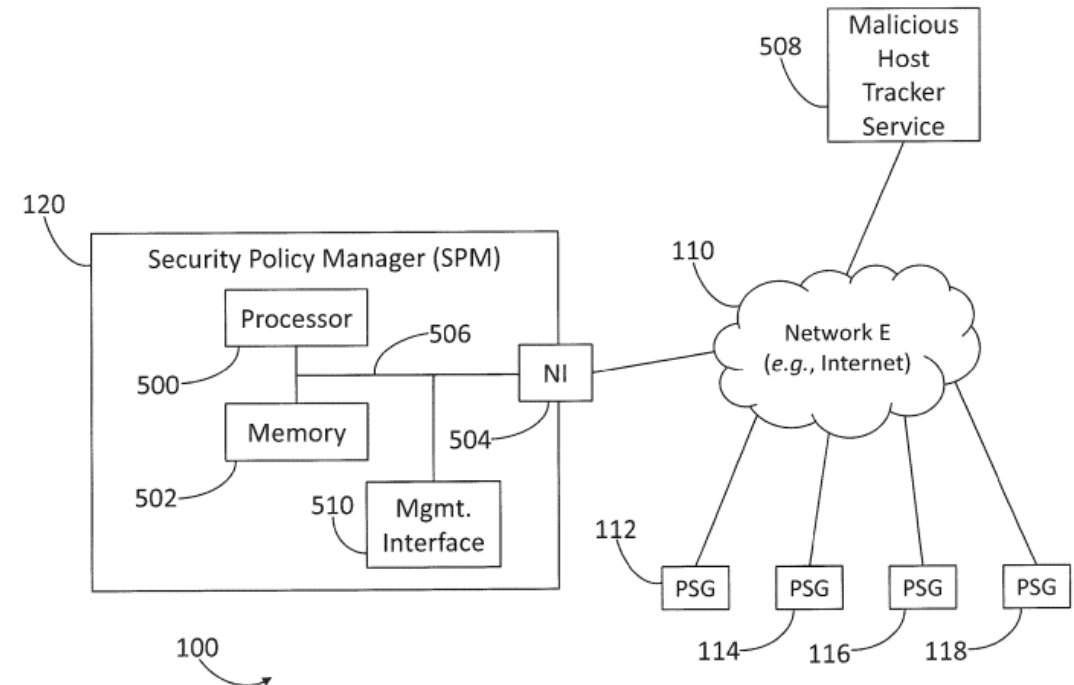


FIG. 5

'266 Patent at 13:18-14:39, *id.* at Fig. 5; see also *id.* at Claims 1, 8, 15, and 21 (the claimed SPMS carrying out these operations).

Overview

- Summary of The IPR Grounds
- The '266 Patent Overview
- **Claims 1-27 Patentable over Law**
- Claims 1-27 Patentable over Law in View of Wood
- Law in view of Wood and/or Jungck Fails to Render Obvious Dependent Claims

Law Does Not Disclose “a plurality of packet security gateways that collectively provide an entire interface across a boundary of a network protected”

- Law’s NAD 149c is a perimeter device that by definition, sits outside of and controls access between the two different networks and moreover fails to teach or suggest applying “a first set of packet filtering rules” to “all network traffic traversing the boundary” therefore the preambles are limiting and Law does not render obvious the preamble limitations.

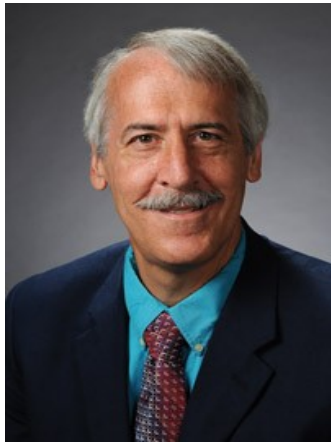
If NAD 149c is outside of the process control network it cannot be simultaneously within the single process control network that the NAD creates

Petitioner’s entire argument relies on the false premise that all of Law’s firewalls apply the same “global” ruleset 147. Reply at 11. However, Law’s reference to a “global” set of rules is one that applies to all of the devices within a single subsystem. POR at 28.

DESCRIPTION

[0051] FIG. 1a is a schematic representation of a process control system 100 including one or more process control sub-systems 105a, 105b within one or more process plants in which external communication between, for example, each subsystem via the Internet or other external source may be secured by a “Unified Threat Management System” (UTMS) including one or more UTMS-configured network devices (e.g., firewalls) 146a, 146b, network devices 152, field devices, 134 smart devices, modules, controllers, components, etc., as herein described. FIG. 1b is a schematic representation of another embodiment of a process control system 100 including one or more process control sub-systems 105a, 105b that may be secured by a UTMS that, in addition to the devices 134, 146, 152 described below, includes a network access device 149 positioned downstream of the firewall 146. The network access device 149 of FIG. 1b may supplement the perimeter UTMS functions of the device 146, or may perform specialized UTMS functions such as the bypass function described below. Each firewall 146 or device 134, 149, 152 may include a ruleset, for example, rulesets 147a, 148a, 147b, 148b, 151a, 151b, 153 defining the communication that may be received or processed by the UTMS-configured device. Where the UTMS-configured device is a perimeter device (i.e., outside of the process control network 150a or 150b), the rulesets 147 and 151 may include a global set of rules for access to any device within the subsystems 105a, 105b. Where the UTMS-configured device is an internal device 134, 152 (i.e., within the process control network 150a or 150b), the rulesets 148, 153 may include a subset of the global set of rules that only defines access to the particular

Law Does Not Disclose “a plurality of packet security gateways that collectively provide an entire interface across a boundary of a network protected”



Dr. Douglas Jacobson
Petitioner's expert

- Law Does Not Disclose a Plurality of PSGs at the Boundary of a Protected Network, and petitioner does not dispute that the preambles of Independent Claims 1, 8, and 15 are limiting.
- Law's Network Access Device 149c does not join together networks 150a and 150b into a single network 150 protected by a plurality of PSGs.
- NAC 149c is not in “Process Control Network 150” because it is, by definition, “outside” of the process control networks. *POR at 19*

1 Q. So looking at the network access
2 device 149c in Figure 3 of Law, this is
3 positioned outside the subsystems of 105a and
4 105b; correct?
5 A. Yeah, it's drawn in between the two
6 boxes, 105a and 105b; correct.
7 Q. So it sits outside of both subsystems;
8 correct?
9 A. Yeah.

Ex. 2018. at 21:1-9 (Dr. Jacobson agreeing that NAD 149c sits outside the process control subsystems and respective networks).

Law Does Not Disclose “a plurality of packet security gateways that collectively provide an entire interface across a boundary of a network protected”

- Law’s “Network 150” is One Process Control Network, not a combination of Network 150a and Network 150b.
- Law only uses the term “a process control network 150” when referring to a single process control network and when it is not necessary to distinguish between two or more different process control networks. See POR at 18; Law ¶¶ 53, 57.

Law at Fig. 3 (annotated)

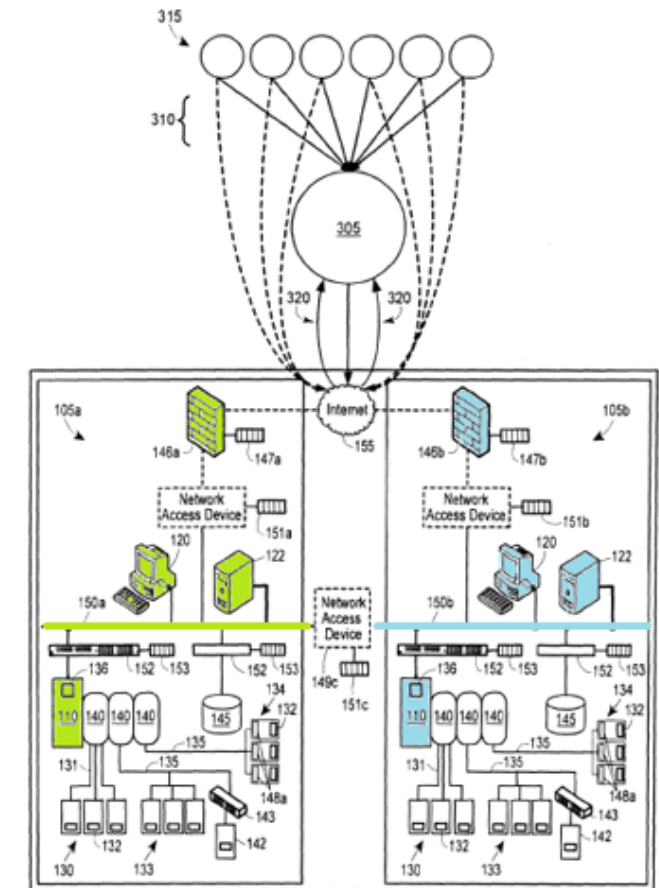


Fig. 3

Law Does Not Disclose “a plurality of packet security gateways that collectively provide an entire interface across a boundary of a network protected”



Dr. Michael Goodrich
Patent Owner's expert

16 THE WITNESS: So to answer your question,
17 the ruleset 146, 147 that is referenced here in
18 paragraph 51, person of ordinary skill in the art
19 would understand that this is referring to
20 generically either the ruleset 147a or 147b, because 09:18:25

A POSITA would understand that a global set of rules (ruleset 147a) is used by subsystem 105a and is separate from global set of rules (ruleset 147b) used by subsystem 105b. Petitioner does not rebut this testimony.

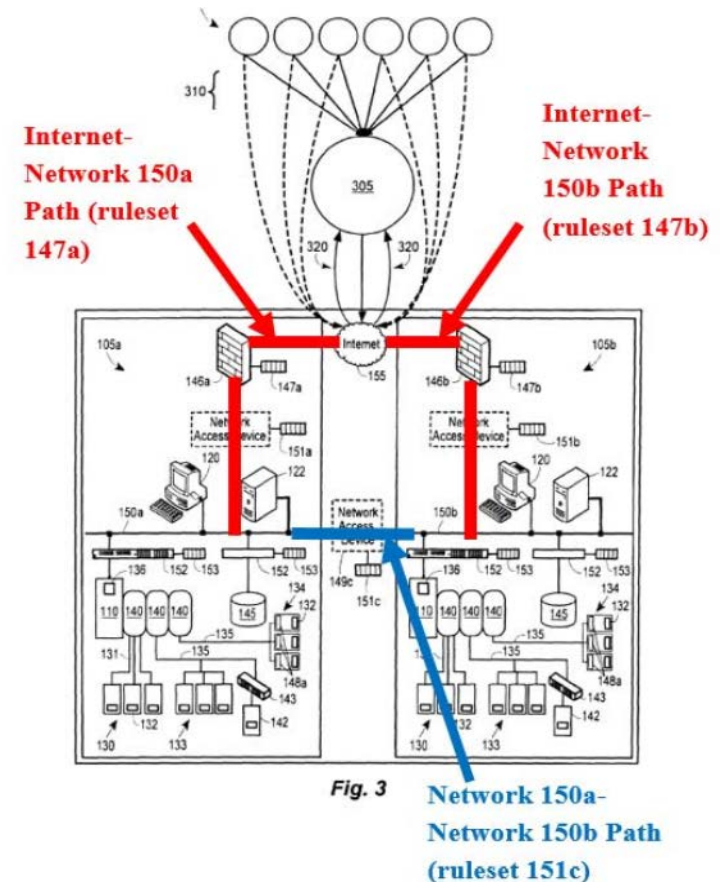
Each Subsystem has its own global set of rules unique to its devices.

Goodrich Tr. at 11:16-20 (emphasis added); see also id. at 9:22-25 (counsel asking whether ruleset 147 “may include a global set of rules”), 11:16-12:23 (Dr. Goodrich explaining that ruleset 147a is associated with firewall 146a while ruleset 147b is associated with firewall 146b).

Law Does Not Disclose “applying “a first set of packet filtering rules” to “all traffic traversing the boundary”

- To the extent that Petitioner suggests that NAD 149c is one of the claimed plurality of PSGs its ruleset is different than the rulesets applied at the other alleged PSGs (Law’s firewalls).

See POR at 31-33



POR at 32 (citing Law at Fig. 3 (annotated)).

Firm 305 is not a “Security Policy Management Server”

- Law’s Firm 305 is not a “Security Policy Management Server” that distributes dynamic security policies.
- Firm 305 is not a “Security Policy Management Server” but a commercial entity. POR at 34-35 (citing Ex. 2011 at 3), Ex. 2014 at 37:2-38:7, Law, ¶ 83, 88.
- Firm 305 does not supply dynamic security policies; it only provides updates to existing policies.
- Firm 305 does not automatically update rulesets as IT personnel are required in the updates. POR at 14-15, 34-35; Law, ¶¶ 16, 88.

Law does not disclose that firm 305 provides automatic updates of rulesets and it is Petitioner’s burden to show that Law discloses firm 305 providing updates without IT personnel involvement. *Dynamic Drinkware, LLC. V. Nat’l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015)

Petitioner therefore fails to demonstrate that firm 305 satisfies the claimed SPMS.

[0088] As previously described, the various rulesets (e.g., rulesets 147, 148, 151, 153) associated with the UTMS configured network devices 146, 134, 149, 152 require updates to remain effective against network threats. With reference to FIG. 3, a third party, cyber security risk management firm 305 such as Wurldtech Security, Inc. of Vancouver, BC Canada, or other entity, may collect threat data 310 from a plurality of various sources 315 to construct the various rulesets 147, 148, 151, 153, validate the rulesets, verify, and distribute the rulesets to the UTMS-configured firewalls 146a, 146b, UTMS-configured network access devices 149c, other UTMS-configured network devices 146, and/or UTMS field devices 134. Ruleset collecting, constructing, validating, and distributing may be performed using any type of information technology methods suitable for performing such actions using electronic data. For example, some of the methods may include collecting the threat data 310 from the World Wide Web using various data collection techniques (e.g., robots, crawling, data feeds, collaborative forums, etc.), constructing data files to convey the rulesets to their destination devices in a device-compatible manner, executing a computer-implemented algorithm to determine if the rulesets effectively secure the process control systems in a desirable manner (e.g., simulation or other testing method), and distributing the rulesets to the UTMS-configured entities via a secure Internet interface or other suitable method.

Ex. 1005 (Law), ¶88; see also ¶¶ 83, 16.

Firm 305 is Not a “Security Policy Management Server”

Petitioner fails to identify with particularity a server within the commercial entity that performs the claimed automatically generating and distributing dynamic security policy functionality

- The parties agree that firm 305 is not a server, and Keysight has not identified any server within firm 305 that automatically generates and distributes dynamic security policies.

“It is of utmost importance that petitioners in the IPR proceedings adhere to the requirement that the initial petition identify ‘with particularity’ the ‘evidence that supports the grounds for the challenge to each claim.’”)

(quoting 35 U.S.C. § 312(a)(3)).

Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd., 821 F.3d 1359, 1369 (Fed. Cir. 2016)

Firm 305 is Not a “Security Policy Management Server”

Firm 305 is a commercial entity consisting of IT personnel and various infrastructure components, not a server.

Firm 305 leverages IT staff and various IT infrastructure components in updating rulesets by “collecting the threat data,” “construction data files,” and “executing [] computer implemented algorithm[s] to determine if the rulesets effectively secure the process control system”

[0088] As previously described, the various rulesets (e.g., rulesets 147, 148, 151, 153) associated with the UTMS-configured network devices 146, 134, 149, 152 require updates to remain effective against network threats. With reference to FIG. 3, a third party, cyber security risk management firm 305 such as Wurdtech Security, Inc. of Vancouver, BC Canada, or other entity, may collect threat data 310 from a plurality of various sources 315 to construct the various rulesets 147, 148, 151, 153, validate the rulesets, verify, and distribute the rulesets to the UTMS-configured firewalls 146a, 146b, UTMS-configured network access devices 149c, other UTMS-configured network devices 146, and/or UTMS field devices 134. Ruleset collecting, constructing, validating, and distributing may be performed using any type of information technology methods suitable for performing such actions using electronic data. For example, some of the methods may include collecting the threat data 310 from the World Wide Web using various data collection techniques (e.g., robots, crawling, data feeds, collaborative forums, etc.), constructing data files to convey the rulesets to their destination devices in a device-compatible manner, executing a computer-implemented algorithm to determine if the rulesets effectively secure the process control systems in a desirable manner (e.g., simulation or other testing method), and distributing the rulesets to the UTMS-configured entities via a secure Internet interface or other suitable method.

[0089] In addition to collecting known threat data 310, the process control system 100 may send domain-specific information 320 back to the firm 305. For example, domain-specific information may include data that indicates information related to the topography of the system 100 (i.e., the manufacturer, model, state, software/hardware versions, etc., of the types of physical devices in the system 100 including pumps, tanks, valves, etc.), protocol and other network 150 infrastructure information, software versions of each physical device, network device, and UTMS-configured device, etc. The firm 305 may then use various analysis techniques to build domain-specific robustness testing tools to continuously identify network vulnerabilities in any device, sub-system, or software program (to name only a few of the possibly identifiable vulnerabilities) using the domain-specific information sent from the process control system 100. The firm 305 may then aggregate the results of the analysis performed by the testing tools into a collection that identifies the specific system vulnerabilities. The collection may be categorized, sorted, and prioritized based on several factors including the security risk of the identified vulnerability, the danger a breach of network security due to the vulnerability might cause, the potential for repeated network breaches, etc. Each of these known vulnerabilities may then be translated into mitigations or rules for the various rulesets 147, 148, 151, 153, and the firm 305 may provide an ongoing remediation update service to the system 100 in the form of UTMS-device updates. In this way, each time a new device or code application is introduced to the system 100, any exposure to bugs or other vulnerabilities may be reduced or eliminated.

US 2011/0072506 A1

13

Mar. 24, 2011

tored and utilized by plant personnel other than operators, such as engineering personnel or management. Graphic elements within the displays that represent the UTMS-configured network devices 134, 146, 149, 152 provide network parameters and security data (as described above) to operators and other plant personnel to monitor and maintain the network security of the process control system 100.

[0088] As previously described, the various rulesets (e.g., rulesets 147, 148, 151, 153) associated with the UTMS-configured network devices 146, 134, 149, 152 require updates to remain effective against network threats. With reference to FIG. 3, a third party, cyber security risk management firm 305 such as Wurdtech Security, Inc. of Vancouver, BC Canada, or other entity, may collect threat data 310 from a plurality of various sources 315 to construct the various rulesets 147, 148, 151, 153, validate the rulesets, verify, and distribute the rulesets to the UTMS-configured firewalls 146a, 146b, UTMS-configured network access devices 149c, other UTMS-configured network devices 146, and/or UTMS field devices 134. Ruleset collecting, constructing, validating, and distributing may be performed using any type of information technology methods suitable for performing such actions using electronic data. For example, some of the methods may include collecting the threat data 310 from the World Wide Web using various data collection techniques (e.g., robots, crawling, data feeds, collaborative forums, etc.), constructing data files to convey the rulesets to their destination devices in a device-compatible manner, executing a computer-implemented algorithm to determine if the rulesets effectively secure the process control systems in a desirable manner (e.g., simulation or other testing method), and distributing the rulesets to the UTMS-configured entities via a secure Internet interface or other suitable method.

[0089] In addition to collecting known threat data 310, the process control system 100 may send domain-specific information 320 back to the firm 305. For example, domain-specific information may include data that indicates information related to the topography of the system 100 (i.e., the manufacturer, model, state, software/hardware versions, etc., of the types of physical devices in the system 100 including pumps, tanks, valves, etc.), protocol and other network 150 infrastructure information, software versions of each physical device, network device, and UTMS-configured device, etc. The firm 305 may then use various analysis techniques to build domain-specific robustness testing tools to continuously identify network vulnerabilities in any device, sub-system, or software program (to name only a few of the possibly identifiable vulnerabilities) using the domain-specific information sent from the process control system 100. The firm 305 may then aggregate the results of the analysis performed by the testing tools into a collection that identifies the specific system vulnerabilities. The collection may be categorized, sorted, and prioritized based on several factors including the security risk of the identified vulnerability, the danger a breach of network security due to the vulnerability might cause, the potential for repeated network breaches, etc. Each of these known vulnerabilities may then be translated into mitigations or rules for the various rulesets 147, 148, 151, 153, and the firm 305 may provide an ongoing remediation update service to the system 100 in the form of UTMS-device updates. In this way, each time a new device or code application is introduced to the system 100, any exposure to bugs or other vulnerabilities may be reduced or eliminated.

[0090] Each ruleset may be a data file that includes known signature, policy, or other rules describing characteristics of network-based threats to the process control system 100. The rulesets may be configured to control both internal and external access to the network 150 for each portion of the process control system 100. Because the UTMS-configured network device 134, 146, 149, 152 is configured as a process variable (as described above), the rulesets 148, 147, 151, 153 may be configurable by an operator or other personnel from a graphic display 129 at a workstation 120. For example, based on various characteristics of the process control system 100 (e.g., the number and type of UTMS-configured devices within the process control system 100, the importance or “sensitivity” of network security to a particular sub-system, entity, or other portion of system 100 to be protected by the rulesets, the likelihood of external network attack, etc.), the user may individually configure and manage the network security of any portion of the process control system 100. In some embodiments, the user’s graphic display may include a number of pre-configured “network security profiles” that employ a subset of the rules that are distributed to the system 100. Depending on the sensitivity of the process being performed by the process control system 100 or other factors, the user may select a profile that best balances the need for network security and the continuing operation of the system 100. Where the ruleset is received by a perimeter UTMS-configured network device, the device may determine which rules of the received ruleset are appropriate for which sub-systems of the process control system. The perimeter device may then distribute the determined rules to the appropriate device within the subsystems. Those subsystems may, in turn, also determine smaller sets of rules and distribute those within the subsystems. Thus, a selected profile or policy may enforce a subset of the total number of rules within one or more rulesets 147, 148, 151, 153 according to the network security needs of the process control system. Alarms may also indicate to a user whether a particular selected profile is adequate for security according to static and dynamic conditions of the network including, but not limited to, detected traffic, a state of the system 100, a length of time a profile has been active, etc. Timers associated with an alarm may also be set by default or configured by a user to limit an amount of time the selected profile is in place. Each timer may include a default setting depending on the rigidity of the selected profile and the sensitivity of the secured entities or devices. For example, a particularly sensitive process for which a user selects a minimal security policy may only be in force for a short period of time before an alarm is indicated, while a particularly secure process for which a user selects a rigid security policy may be in force for a long short period of time.

[0091] Each of the rulesets 147, 148, 151, 153 may define conditions that, if detected, implement some combination of blocking suspected malicious communications or alerting an operator or other plant personnel through an alarm displayed within one or more graphical displays, as previously described. Additionally, each operator may have integrated control over ruleset updates directly from their respective operator displays. For operators with non-supervisory permissions, secondary or supervisory authentication may be enabled to implement a ruleset update (e.g., the two-factor authentication process described above).

[0092] In some embodiments, the UTMS-configured firewalls 146a, 146b, UTMS-configured network access devices 149c, other UTMS-configured network devices 146, and/or

Ex. 1005 (Law), ¶88

Firm 305 is Not a “Security Policy Management Server”

Firm 305 Does Not Automatically Update Rulesets:

Law is clear that IT personnel are “still required to update the ruleset when new threats are discovered”

[0016] Some commercial off-the-shelf (COTS) firewall systems and other network devices are able to provide a partial solution to network security, but still must be managed outside of the operator environment. COTS firewalls are managed by IT personnel specifically trained to integrate the firewall into the needs of the process control system and configure the various rulesets as described above. Even so, COTS firewall systems have a number of disadvantages. For example, the “end of life” for the firewall is controlled by the manufacturer, not the user or by plant floor personnel, which may lead to an unexpected product replacement, lack of manufacturer support, and plant downtime. Further, IT personnel are still required to update the ruleset when new threats are discovered or upgrades to software components of the system are implemented. In a process control system, each ruleset is specific to the system it protects; changes to the system require changes to the rulesets. IT personnel, who are not typically trained to understand the process control system and its upgrades, may not understand how or why the rulesets must also be changed. If left solely as a stand-alone application managed by IT personnel, the rulesets may inadvertently provide less protection for the system than desired. For example, administration, configuration, and management of the firewall typically requires IT personnel to have detailed knowledge of the network architecture that is to be protected.

US 2011/0072506 A1

3

Mar. 24, 2011

[0015] In some particularly high-risk or sensitive process control systems (e.g., nuclear reactors, high-energy processes, major metropolitan area power grids, military and government applications, etc.), restrictive connection policies may demand that all external network connections be completely secure. In practice, these sensitive process control systems have resorted to physically disconnecting all external connections from the network when they are not in use. However, since physically disconnecting external connections is not integrated into the process control system as an object that may be represented within a graphical interface, as described above, it is difficult if not impossible for operators to control the state of the connection (i.e., whether or not the device or system the operator controls is physically connected to an external entity) or to even know whether or not the connection is active from their operator workstations.

[0016] Some commercial off-the-shelf (COTS) firewall systems and other network devices are able to provide a partial solution to network security, but still must be managed outside of the operator environment. COTS firewalls are managed by IT personnel specifically trained to integrate the firewall into the needs of the process control system and configure the various rulesets as described above. Even so, COTS firewall systems have a number of disadvantages. For example, the “end of life” for the firewall is controlled by the manufacturer, not the user or by plant floor personnel, which may lead to an unexpected product replacement, lack of manufacturer support, and plant downtime. Further, IT personnel are still required to update the ruleset when new threats are discovered or upgrades to software components of the system are implemented. In a process control system, each ruleset is specific to the system it protects; changes to the system require changes to the rulesets. IT personnel, who are not typically trained to understand the process control system and its upgrades, may not understand how or why the rulesets must also be changed. If left solely as a stand-alone application managed by IT personnel, the rulesets may inadvertently provide less protection for the system than desired. For example, administration, configuration, and management of the firewall typically requires IT personnel to have detailed knowledge of the network architecture that is to be protected. IT personnel for process control networks typically need to understand the network topology, network business needs related to the network, permitted devices and services that the business requires within and between local networks, and the various external entities that should be permitted to access the local networks. Example internal entities may include multiple workstations within a business that have access to shared file servers and applications. Example external entities may include laptops, workstations, and other communication devices not physically connected to the one or more local networks. Such external entities may be associated with, for example, salespeople that are traveling and require connectivity to sensitive or proprietary nodes of their business network.

[0017] For circumstances in which IT personnel are responsible for protecting networks associated with a control system, the personnel must typically understand which control system devices are permitted to access external network resources and which external network resources are permitted to access the control system devices. Some control systems (e.g., a process control system in a manufacturing plant, test and measurement applications/equipment, etc.) include one or more controllers, such as a Delta™ controller sold by

Fisher-Rosemount Systems, Inc., an Emerson Process Management™ company. The controller may connect to a network and have a designated IP address, one or more communication ports, one or more slots to accommodate input/output (I/O) devices and/or field devices, and/or one or more I/O channels. For some control systems, multiple controllers may be employed, each having a unique IP address with corresponding ports, slots, and/or I/O channels. As such, IT personnel must typically know the IP address of each controller and/or each device connected to the controller, such as field devices (e.g., smart field devices), thermocouples, and/or other devices (e.g., light shields, pressure gauges, pressure transducers, current transducers, etc.).

[0018] In addition to IT personnel having the responsibility of understanding the control system topology and addresses for each control system device, IT personnel must typically set rules and/or access privileges for each of the devices that comprise one or more control systems. Rules may include, but are not limited to, allowing internal network communications between identified devices within the control system, blocking communications from one or more control system devices within the control system, blocking/organizing communications from one or more control system devices having external destination IP addresses, setting one or more communication volume thresholds, and setting communication protocol rules (e.g., a smart field device is not allowed to initiate communications within the control system network unless first requested by a master device).

[0019] Additionally, because control system devices and associated communication protocols used by such devices may include unique and device-specific features, IT personnel typically need to understand details related to control system communications that should be allowed or blocked based on such features. For example, some control systems employ a communication protocol known as Highway Addressable Remote Transducer (HART) HART communications employ a bi-directional industrial field communication protocol that is typically used to implement communications between intelligent field instruments and/or host systems. The host systems, such as Delta™ controllers, communicate with field devices for many reasons including device configuration, device diagnosis, device troubleshooting, receiving device process measurement values, and determining device health status information. HART devices are normally only allowed to communicate on a HART communication network after first being interrogated by the host (such as a Delta™ controller). Another communication feature of the HART communication protocol includes the ability to facilitate a secondary host (e.g., a primary master and a secondary master, each of which may communicate with the field devices). If IT personnel that configure the firewall are unaware of such device and protocol-specific features, the firewall may fail to accommodate for such communication activities that are deemed acceptable or particularly risk-prone. For example, some field devices may be configured in a control system to receive measurement data from a transducer and report the collected measurement data to a specific controller via a specific IP address having a specific port. In the event that the field device also initiates communication to an alternate destination (e.g., a network node, the Internet, an alternate controllers in the control system, etc.), then such activity may be considered a security risk that an operator of the process control system may not fully understand.

Ex. 1005 (Law), ¶16

Firm 305 is Not a “Security Policy Management Server”

Firm 305 Does Not Automatically Update Rulesets:

[0021] One possible solution for network security is described in U.S. Patent Application Publication No. 2007019906 to Byres et al., entitled “NETWORK SECURITY APPLIANCE” and the Tofino™ system manufactured by Byres Security Inc. of Lantzville, BC. These solutions discover and identify network devices and create firewall rules to control the traffic flowing to them by automatically locating devices and generating rules by passively analyzing traffic on the network. When the solution discovers a new device, it prompts the system administrator to accept its deductions and insert the new device into the network inventory diagram, or flag the device as a potential intruder. This way, IT personnel and the network control engineer always have a current network map. While this solution ensures that IT personnel are able to quickly and accurately manage the network, the solution is still left entirely to the expertise and control of separately-trained IT personnel. Operators within a process control system would have no capability to monitor and manage process control network security from operator workstations.

Ex. 1005 (Law), ¶121

Law's discloses ensuring that process control system operators and IT personnel both have control over system security.

Firm 305 is Not a “Security Policy Management Server”

Firm 305 Does Not Automatically Update Rulesets:

Law does not disclose any methods would or even could forego the required manual input of IT personnel.

[0088] As previously described, the various rulesets (e.g., rulesets 147, 148, 151, 153) associated with the UTMS configured network devices 146, 134, 149, 152 require updates to remain effective against network threats. With reference to FIG. 3, a third party, cyber security risk management firm 305 such as Wurldtech Security, Inc. of Vancouver, BC Canada, or other entity, may collect threat data 310 from a plurality of various sources 315 to construct the various rulesets 147, 148, 151, 153, validate the rulesets, verify, and distribute the rulesets to the UTMS-configured firewalls 146a, 146b, UTMS-configured network access devices 149c, other UTMS-configured network devices 146, and/or UTMS field devices 134. Ruleset collecting, constructing, validating, and distributing may be performed using any type of information technology methods suitable for performing such actions using electronic data. For example, some of the methods may include collecting the threat data 310 from the World Wide Web using various data collection techniques (e.g., robots, crawling, data feeds, collaborative forums, etc.), constructing data files to convey the rulesets to their destination devices in a device-compatible manner, executing a computer-implemented algorithm to determine if the rulesets effectively secure the process control systems in a desirable manner (e.g., simulation or other testing method), and distributing the rulesets to the UTMS-configured entities via a secure Internet interface or other suitable method.

US 2011/0072506 A1

13

Mar. 24, 2011

tored and utilized by plant personnel other than operators, such as engineering personnel or management. Graphic elements within the displays that represent the UTMS-configured network devices 134, 146, 149, 152 provide network parameters and security data (as described above) to operators and other plant personnel to monitor and maintain the network security of the process control system 100.

[0088] As previously described, the various rulesets (e.g., rulesets 147, 148, 151, 153) associated with the UTMS configured network devices 146, 134, 149, 152 require updates to remain effective against network threats. With reference to FIG. 3, a third party, cyber security risk management firm 305 such as Wurldtech Security, Inc. of Vancouver, BC Canada, or other entity, may collect threat data 310 from a plurality of various sources 315 to construct the various rulesets 147, 148, 151, 153, validate the rulesets, verify, and distribute the rulesets to the UTMS-configured firewalls 146a, 146b, UTMS-configured network access devices 149c, other UTMS-configured network devices 146, and/or UTMS field devices 134. Ruleset collecting, constructing, validating, and distributing may be performed using any type of information technology methods suitable for performing such actions using electronic data. For example, some of the methods may include collecting the threat data 310 from the World Wide Web using various data collection techniques (e.g., robots, crawling, data feeds, collaborative forums, etc.), constructing data files to convey the rulesets to their destination devices in a device-compatible manner, executing a computer-implemented algorithm to determine if the rulesets effectively secure the process control systems in a desirable manner (e.g., simulation or other testing method), and distributing the rulesets to the UTMS-configured entities via a secure Internet interface or other suitable method.

[0089] In addition to collecting known threat data 310, the process control system 100 may send domain-specific information 320 back to the firm 305. For example, domain-specific information may include data that indicates information related to the topology of the system 100 (i.e., the manufacturer, model, time, software/hardware versions, etc.) of the types of physical devices in the system 100 including pumps, tanks, valves, etc., protocol and other network 150 infrastructure information, software versions of each physical device, network device, and UTMS-configured device, etc. The firm 305 may then use various analysis techniques to build domain-specific robustness testing tools to continuously identify network vulnerabilities in any device, sub-system, or software program (to name only a few of the possibly identifiable vulnerabilities) using the domain-specific information sent from the process control system 100. The firm 305 may then aggregate the results of the analysis performed by the testing tools into a collection that identifies the specific system vulnerabilities. The collection may be categorized, sorted, and prioritized based on several factors including the security risk of the identified vulnerability, the danger a breach of network security due to the vulnerability might cause, the potential for repeated network breaches, etc. Each of these known vulnerabilities may then be translated into mitigations or rules for the various rulesets 147, 148, 151, 153, and the firm 305 may provide an ongoing remediation update service to the system 100 in the form of UTMS-device updates. In this way, each time a new device or code application is introduced to the system 100, any exposure to bugs or other vulnerabilities may be reduced or eliminated.

[0090] Each ruleset may be a data file that includes known signature, policy, or other rules describing characteristics of network-based threats to the process control system 100. The rulesets may be configured to control both internal and external access to the network 150 for each portion of the process control system 100. Because the UTMS-configured network device 134, 146, 149, 152 is configured as a process variable (as described above), the rulesets 148, 147, 151, 153 may be configurable by an operator or other personnel from a graphical display 129 at a workstation 120. For example, based on various characteristics of the process control system 100 (e.g., the number and type of UTMS-configured devices within the process control system 100, the importance or “sensitivity” of network security to a particular sub-system, entity, or other portion of system 100 to be protected by the rulesets, the likelihood of external network attack, etc.), the user may individually configure and manage the network security of any portion of the process control system 100. In some embodiments, the user’s graphical display may include a number of pre-configured “network security profiles” that employ a subset of the rules that are distributed to the system 100. Depending on the sensitivity of the process being performed by the process control system 100 or other factors, the user may select a profile that best balances the need for network security and the confining operation of the system 100. Where the ruleset is received by a perimeter UTMS-configured network device, the device may determine which rules of the received ruleset are appropriate for which sub-systems of the process control system. The perimeter device may then distribute the determined rules to the appropriate device within the subsystems. These subsystems may, in turn, also determine smaller sets of rules and distribute those within the subsystem. Thus, a selected profile or policy may enforce a subset of the total number of rules within one or more rulesets 147, 148, 151, 153 according to the network security needs of the process control system. Alarms may also indicate to a user whether a particular selected profile is adequate for security according to static and dynamic conditions of the network including, but not limited to, detected traffic, a state of the system 100, a length of time a profile has been active, etc. Times associated with an alarm may also be set by default or configured by a user to limit an amount of time the selected profile is in place. Each timer may include a default setting depending on the rigidity of the selected profile and the security of the second entities or devices. For example, a particularly sensitive process for which a user selects a network security policy may only be in force for a short period of time before an alarm is indicated, while a particularly secure process for which a user selects a rigid security policy may be in force for a long short period of time.

[0091] Each of the rulesets 147, 148, 151, 153 may define conditions that, if detected, implement some combination of blocking suspected malicious communications or alerting an operator or other plant personnel through an alarm displayed within one or more graphical displays, as previously described. Additionally, each operator may have integrated control over ruleset updates directly from their respective operator displays. For operators with non-supervisory permissions, secondary or supervisory authentication may be enabled to implement a ruleset update (e.g., the two-factor authentication process described above).

[0092] In some embodiments, the UTMS-configured firewalls 146a, 146b, UTMS-configured network access devices 149c, other UTMS-configured network devices 146, and/or

Ex. 1005 (Law), ¶88

Firm 305 is Not a “Security Policy Management Server”

Firm 305 Does Not Automatically Update Rulesets:

Certain network conditions trigger the Process Control Network to update a rule set, but Firm 305 does not create or automatically alter rulesets.

[0083] Generally speaking, a set of predefined graphic elements may be provided in the configuration application to enable a user to construct process graphic displays that reflect the process plant and the process control system 100 in general and include visual representations of the UTMS-configured devices as described above. These displays have graphic display elements designed to dynamically show on-line measurements and actuators that interface with the control system and, as a result, may present information typically monitored and utilized by operators or other personnel involved in on-line operations. The graphic display elements that represent UTMS-configured elements may dynamically show on-line network security measurements. For example, the UTMS-configured elements within each graphic display may dynamically show a current operating state of the UTMS-configured element, alarms based on detected network conditions (e.g., an unexpected increase in network traffic or type of traffic at the UTMS-configured object, detection of a known fault-inducing attack on the network, etc.), detection of an update (e.g., software, firmware, existing configurations, etc.) of another element or device in the process control system 100 that is in communication with the UTMS-configured object, etc. Detection of certain network conditions may also trigger an automatic update of the rulesets 147, 148, 151, 153 or an alarm to prompt a user to perform a manual update of the rulesets or another action to fully secure the system 100.

US 2011/0072506 A1

12

Mar. 24, 2011

communications networks to allow (as described above), a user may easily configure each UTMS-configured device while reducing the risk of mis-configuration and reduced security. Additionally, a user may define an area of the process control system 100 to protect using the UTMS-configured process object 204. In one embodiment, the user may select one or more process control devices and entities from a graphical display to define which areas or subsystems are protected and monitored by the particular UTMS-configured network device 146, 149, 152. Additional security options may also be configured for the UTMS-configured network device 146, 149, 152 from the UTMS-configured process object 204, including the type of monitoring or protection that may be available for the selected sub-system, entity, or area of the process-control system, which rules are available for the user-defined area, detected conditions that may trigger one or more alarms, etc. Of course, other types of user interfaces other than the drop-down menus 230, 232 described above may assist a user in the configuration of each UTMS-configured process control object. The drop-down menus 230, 232 or other configuration interfaces for the UTMS-configured objects may be tightly integrated into the protected system 100, or available via a secure web page (or similar native page available within the UTMS-configured object 204).

[0082] Access to the one or more user interfaces described above for configuration, update, accepting ruleset updates, etc., for UTMS-configured devices (or access through the device to the protected system via an associated UTMS-configured process control object) may be protected via an inherent, two-factor authentication module that is an inherent part of the device (i.e., an authentication method stored as computer-executable instructions within a secure EEPROM or a secure IC within the UTMS-configured device, as one of the methods 228, etc.). Alternatively, the two-factor authentication method may be a configuration application 200, as described above. An authentication method may also be integrated into user authentication that is native to the system 100 for operator and other user access. For example, the UTMS-configured device and the process control system 100 may both utilize a common Remote Authentication Dial In User Service (RADIUS) authentication server. In some embodiments, the RADIUS server is built into the UTMS-configured device. In other embodiments, the authentication method may include tokens, smart cards, and other known two-factor methods.

[0083] Generally speaking, a set of predefined graphic elements may be provided in the configuration application to enable a user to construct process graphic displays that reflect the process plant and the process control system 100 in general and include visual representations of the UTMS-configured devices as described above. These displays have graphic display elements designed to dynamically show on-line measurements and actuators that interface with the control system and, as a result, may present information typically monitored and utilized by operators or other personnel involved in on-line operations. The graphic display elements that represent UTMS-configured elements may dynamically show on-line network security measurements. For example, the UTMS-configured elements within each graphic display may dynamically show a current operating state of the UTMS-configured element, alarms based on detected network conditions (e.g., an unexpected increase in network traffic or type of traffic at the UTMS-configured object, detection of a

known fault-inducing attack on the network, etc.), detection of an update (e.g., software, firmware, existing configurations, etc.) of another element or device in the process control system 100 that is in communication with the UTMS-configured object, etc. Detection of certain network conditions may also trigger an automatic update of the rulesets 147, 148, 151, 153 or an alarm to prompt a user to perform a manual update of the rulesets or another action to fully secure the system 100.

[0084] In addition to on-line measurements and actuators that interface with the control system 100 and the network parameters of the UTMS-configured elements of the system 100, unmeasured parameters that reflect process operation and unmeasured parameters that reflect network health or security may be calculated using on-line process simulation provided in the UTMS-configured process modules and may be shown as an integral part of the associated graphic displays. In these and other ways, the process graphic displays may provide information typically monitored and utilized by plant personnel other than operators, such as engineering personnel, management, and process control network specialists.

[0085] Additionally, in an office environment that may be used for engineering or training simulation purposes, the process simulation values provided by the UTMS-configured process modules may be used and/or displayed in place of the actual process and network measurement values otherwise provided by the graphic elements and the associated control modules. These simulation values, which may be calculated by the associated process modules or a third-party simulation application (e.g., HYSYS), may be based on actual plant settings (e.g., an actuator position or state, a network configuration or state, rulesets, etc.) as well as user-specified disturbance settings or values that may be established via, and depicted in, the process graphic displays and their respective graphic display elements. To these ends, a content layer of the process graphic display customized for an offline view of the process graphic displays may be generated and made available in, for instance, a training context.

[0086] More generally, the process graphic displays may be used in a variety of contexts involving both on-line or control situations, and off-line or simulation situations, by a number of different types of personnel. To this end, each process graphic display may have a plurality of content layers dedicated to these different contexts, situations and personnel. These dedicated content layers are integrated portions of the objects used to define them, in the sense that the same object or objects have associated therewith the information necessary to generate all of the different content layers. As a result, the content layers of a single process graphic display provide customized views without requiring a configuration engineer, IT network, security specialist, or other design personnel to create a separate display for each of the views.

[0087] Generally speaking, the graphic displays reflect the process control system and the process plant. The graphic display elements within each display are designed to dynamically show on-line measurements and actuators that interface with the control system and, as a result, may present information typically monitored and utilized by operators or other personnel involved in on-line operations. In addition, unmeasured parameters that reflect process operation may be calculated using on-line process simulation provided in the process modules and may be shown as an integral part of the associated graphic displays. In these and other ways, the process graphic displays may provide information typically moni-

Ex. 1005 (Law), ¶83

Firm 305 is Not a “Security Policy Management Server”

Keysight’s reliance on alleged state-of-the-art techniques is unavailing

- Petitioner fails to explain **why** a POSITA would have implemented automatic ruleset updates in firm 305 when Law explains that IT personnel of firms are still required to update rulesets of the process control system or demonstrate **how** automatic updates would have overcome its stated need for manual updates by third-party IT personnel.

“[T]he prior art must be considered for all its teachings, not selectively.”

Henny Penny Corp. v. Frymaster LLC, 938 F.3d 1324, 1331-32 (Fed. Cir. 2019) (citation omitted)

A petitioner must “provide adequately developed explanations when relying on background knowledge based on cited art.”

Ariosa Diagnostics v. Verinata Health, Inc. 805 F.3d 1359, 1366 (Fed. Cir. 2015)

Firm 305 is Not a “Security Policy Management Server”

Keysight’s reliance on alleged state-of-the-art techniques is unavailing

Keysight identifies no state-of-the-art techniques for automatically updating rulesets consistent with Law’s requirement that IT personnel are required to manage process control network.

[0021] One possible solution for network security is described in U.S. Patent Application Publication No. 2007019906 to Byres et al., entitled “NETWORK SECURITY APPLIANCE” and the Tofino™ system manufactured by Byres Security Inc. of Lantzville, BC. These solutions discover and identify network devices and create firewall rules to control the traffic flowing to them by automatically locating devices and generating rules by passively analyzing traffic on the network. When the solution discovers a new device, it prompts the system administrator to accept its deductions and insert the new device into the network inventory diagram, or flag the device as a potential intruder. This way, IT personnel and the network control engineer always have a current network map. While this solution ensures that IT personnel are able to quickly and accurately manage the network, the solution is still left entirely to the expertise and control of separately-trained IT personnel. Operators within a process control system would have no capability to monitor and manage process control network security from operator workstations.

US 2011/0072506 A1

4

Mar. 24, 2011

[0020] In other circumstances, IT personnel have limited or no detailed understanding of the control system details and how the control system is to properly function to meet control objectives (e.g., permitted control communications between controllers and devices, permitted data communications between devices, permitted firmware updates to devices, permitted external access by remote users to the control system, etc.). As such, IT personnel may be at a significant disadvantage regarding proper access controls, permission settings, and/or proper firewall rules configuration for the system. For example, an IT professional may install one or more firewall devices and/or firewall software applications to operate between a control system network boundary and an intranet and/or Internet boundary. However, such firewalls are not typically configured with rules and access permissions that account for the unique needs of the control system that would result in optimum functionality of the control system while maintaining a desired degree of network security. As a result, the IT professional may simply configure the firewall tentatively in response to complaints from control system administrators regarding communication failures and instances of improper control system operation. Such haphazard efforts to configure the firewall results in workforce inefficiency, failures, lost profits, and safety risks.

[0021] One possible solution for network security is described in U.S. Patent Application Publication No. 2007019906 to Byres et al., entitled “NETWORK SECURITY APPLIANCE” and the Tofino™ system manufactured by Byres Security Inc. of Lantzville, BC. These solutions discover and identify network devices and create firewall rules to control the traffic flowing to them by automatically locating devices and generating rules by passively analyzing traffic on the network. When the solution discovers a new device, it prompts the system administrator to accept its deductions and insert the new device into the network inventory diagram, or flag the device as a potential intruder. This way, IT personnel and the network control engineer always have a current network map. While this solution ensures that IT personnel are able to quickly and accurately manage the network, the solution is still left entirely to the expertise and control of separately-trained IT personnel. Operators within a process control system would have no capability to monitor and manage process control network security from operator workstations.

SUMMARY OF THE DISCLOSURE

[0022] The security and management of process control system networks may be enhanced by providing a Unified Threat Management System (UTMS) including a UTMS-configured firewall, UTMS-configured network access device, and UTMS-configured field devices that are capable of defending against both known and “zero day” vulnerabilities and threats to control systems for both embedded, proprietary devices, and standard, commonly-used devices. The UTMS-configured firewall and/or network access devices may include standalone network devices located at the perimeter of the process control network, or devices or software that runs in the controllers or other internal parts of the process control system. The state of the UTMS-configured firewalls and devices is integrated into the process control system as a process control object or variable, thus allowing the state and other UTMS and component network access device parameters and variables to be viewed from an operator or other workstation. The UTMS firewalls and devices

may communicate with a perpetual service that proactively supplies the UTMS-configured firewalls, network access devices, and configured controllers or field devices with rulesets to meet the latest security threats, threat patterns, and control system vulnerabilities found to exist within the network. These updates are managed from within the standard control user interface of the plant (e.g., the DeltaV™ environment) as if the UTMS in general and the UTMS-configured firewalls, network access devices, and field devices were no different than any other control system element or entity. UTMS events and the UTMS-configured firewalls and devices themselves (e.g., status, permissions, threat status, events, settings, state, etc.) may also be managed from within the DeltaV™ environment.

[0023] Operator displays for each component of the UTMS may be displayed within the DeltaV™ environment or another graphical process control environment to allow operators to display the current state of the connection as well as update the settings, rulesets, and other parameters or variables of the UTMS (and its firewalls, network access devices, and field devices if so configured) and perform any other process control system security tasks from the operator display or other workstation. In some embodiments, the rulesets may be created based upon continuous or periodic evaluation of the process control system itself to provide immediate system protection from identified threats. The UTMS and its various network access devices may, thus, protect the process control network from vulnerabilities that are known to exist as well as those that are predicted to exist.

[0024] In one embodiment, a method for securing network traffic in a process control system may comprise instantiating an object having a programmable interface that communicates with a particular process control system device. The object is able to access a ruleset including one or more rules defining a condition to accept or deny network traffic received at the device. The network traffic originates externally from the process control system and also seeks access to one or more of the process control system, a network device of the process control system, and a field device of the process control system. The object then determines which of the one or more rules of the ruleset to apply to the device and secures the device by applying the one or more determined rules to the device. The object then monitors the network traffic received at the secured device and, when network traffic is received, determines if the network traffic received at the secured device violates one or more of the rules applied to the secured device. If the network traffic received at the secured device violates one or more of the rules, the object denies the network traffic access and displays an alarm in an operator interface of the process control system. Alternatively, if the network traffic received at the secured device does not violate one or more of the rules, the object grants the network traffic access.

[0025] In a further embodiment, a network device for securing network traffic in a process control system may comprise a first network connector to communicate network traffic into and out of the network device, and a second network connector to communicate network traffic to a control appliance of the process control system. A ruleset at the network device may include one or more rules defining a condition to accept or deny network traffic received at the network device, where the network traffic originates externally from the process control system and seeks access to the process control system. The network device may also include comparison routine to

Ex. 1005 (Law), ¶121

Firm 305 is Not a “Security Policy Management Server”

Keysight’s reliance on alleged state-of-the-art techniques is unavailing

IT personnel are involved in configuring ruleset updates so as to “account for the unique needs of the control system.”

[0020] In other circumstances, IT personnel have limited or no detailed understanding of the control system details and how the control system is to properly function to meet control objectives (e.g., permitted control communications between controllers and devices, permitted data communications between devices, permitted firmware updates to devices, permitted external access by remote users to the control system, etc.). As such, IT personnel may be at a significant disadvantage regarding proper access controls, permission settings, and/or proper firewall rules configuration for the system. For example, an IT professional may install one or more firewall devices and/or firewall software applications to operate between a control system network boundary and an intranet and/or Internet boundary. However, such firewalls are not typically configured with rules and access permissions that account for the unique needs of the control system that would that will result in optimum functionality of the control system while maintaining a desired degree of network security. As a result, the IT professional may simply configure the firewall iteratively in response to complaints from control system administrators regarding communication failures and instances of improper control system operation. Such iterative efforts to configure the firewall results in workforce inefficiency, failures, lost profits, and safety risks.

US 2011/0072506 A1

Mar. 24, 2011

4

[0020] In other circumstances, IT personnel have limited or no detailed understanding of the control system details and how the control system is to properly function to meet control objectives (e.g., permitted control communications between controllers and devices, permitted data communications between devices, permitted firmware updates to devices, permitted external access by remote users to the control system, etc.). As such, IT personnel may be at a significant disadvantage regarding proper access controls, permission settings, and/or proper firewall rules configuration for the system. For example, an IT professional may install one or more firewall devices and/or firewall software applications to operate between a control system network boundary and an intranet and/or Internet boundary. However, such firewalls are not typically configured with rules and access permissions that account for the unique needs of the control system that would that will result in optimum functionality of the control system while maintaining a desired degree of network security. As a result, the IT professional may simply configure the firewall iteratively in response to complaints from control system administrators regarding communication failures and instances of improper control system operation. Such iterative efforts to configure the firewall results in workforce inefficiency, failures, lost profits, and safety risks.

[0021] One possible solution for network security is described in U.S. Patent Application Publication No. 2007/01906 to Byres et al., entitled “NETWORK SECURITY APPLIANCE,” and the Tofino™ system manufactured by Byres Security Inc. of Lantzville, BC. These solutions discover and identify network devices and create firewall rules to control the traffic flowing to them by automatically locating devices and generating rules by passively analyzing traffic on the network. When the solution discovers a new device, it prompts the system administrator to accept its deductions and insert the new device into the network inventory diagram, or flag the device as a potential intruder. This way, IT personnel and the network control engineer always have a current network map. While this solution ensures that IT personnel are able to quickly and accurately manage the network, the solution is still left entirely to the expertise and control of separately-trained IT personnel. Operations within a process control system would have no capability to monitor and manage process control network security from operator workstations.

SUMMARY OF THE DISCLOSURE

[0022] The security and management of process control system networks may be enhanced by providing a Unified Threat Management System (UTMS) including a UTMS-configured firewall, UTMS-configured network access device, and UTMS-configured field devices that are capable of defending against both known and “zero day” vulnerabilities and threats to control systems for both embedded, proprietary devices, and standard, commonly-used devices. The UTMS-configured firewall and/or network access devices may include stand-alone network devices located at the perimeter of the process control network, or devices or software that runs in the controllers or other internal parts of the process control system. The state of the UTMS-configured firewalls and devices is integrated into the process control system as a process control object or variable, thus allowing the state and other UTMS and component network access device parameters and variables to be viewed from an operator or other workstation. The UTMS firewalls and devices

may communicate with a perpetual service that proactively supplies the UTMS-configured firewalls, network access devices, and configured controllers or field devices with rulesets to meet the latest security threats, threat patterns, and control system vulnerabilities found to exist within the network. These updates are managed from within the standard control user interface of the plant (e.g., the DeltaV™ environment) as if the UTMS in general and the UTMS-configured firewalls, network access devices, and field devices were no different than any other control system element or entity. UTMS events and the UTMS-configured firewalls and devices themselves (e.g., alarms, permissions, threat status, events, settings, state, etc.) may also be managed from within the DeltaV™ environment.

[0023] Operator displays for each component of the UTMS may be displayed within the DeltaV™ environment or another graphical process control environment to allow operators to display the current state of the connection as well as update the settings, rulesets, and other parameters or variables of the UTMS and its firewalls, network access devices, and field devices if so configured and perform any other process control system security tasks from the operator display or other workstation. In some embodiments, the rulesets may be created based upon continuous or periodic evaluation of the process control system itself to provide immediate system protection from identified threats. The UTMS and its various network access devices may, thus, protect the process control network from vulnerabilities that are known to exist as well as those that are predicted to exist.

[0024] In one embodiment, a method for securing network traffic in a process control system may comprise instantiating an object having a programmable interface that communicates with a particular process control system device. The object is able to access a ruleset including one or more rules defining a condition to accept or deny network traffic received at the device. The network traffic originates externally from the process control system and also seeks access to one or more of the process control system, a network device of the process control system, and a field device of the process control system. The object then determines which of the one or more rules of the ruleset to apply to the device and secures the device by applying the one or more determined rules to the device. The object then monitors the network traffic received at the secured device and, when network traffic is received, determines if the network traffic received at the secured device violates one or more of the rules applied to the secured device. If the network traffic received at the secured device violates one or more of the rules, the object denies the network traffic access and displays an alarm in an operator interface of the process control system. Alternatively, if the network traffic received at the secured device does not violate one or more of the rules, the object grants the network traffic access.

[0025] In a further embodiment, a network device for securing network traffic in a process control system may comprise a first network connector to communicate network traffic into and out of the network device, and a second network connector to communicate network traffic to a control appliance of the process control system. A ruleset at the network device may include one or more rules defining a condition to accept or deny network traffic received at the network device, where the network traffic originates externally from the process control system and seeks access to the process control system. The network device may also include comparison routine to

Ex. 1005 (Law), ¶120

Firm 305 is Not a “Security Policy Management Server”

Keysight’s reliance on alleged state-of-the-art techniques is unavailing

- Petitioner attempts to shift the burden to Centripetal to show “explain what role IT personnel would have had, if any, in the constructing of rulesets.” *Reply at 16.*
- Dr. Jacobson admits that the firm 305’s IT personnel would be involved in constructing updates and running tests (for example, executing computer-implemented algorithms) *Ex. 2014 at 38:1-10; POR at 35, 39*



Dr. Douglas Jacobson
Petitioner’s expert

1 have a staff infrastructure -- you have a staff to
2 manage the infrastructure, typically these firms will
3 also have staff that understand, you know, something
4 about the 315s and understand, you know, issues about
5 threats, et cetera. And so you're going to have some
6 security type personnel in the 305 and then, of course,
7 that's all. You know, I mean, I'm going to completely
8 ignore everybody else that you need to run a business,
9 but from a computing standpoint, that's at least off
10 the top of my head what I would put into a 305.

In an inter partes review, the burden of persuasion is on the petitioner to prove ‘unpatentability by a preponderance of the evidence,’ and that burden never shifts to the patentee.”

Dynamic Drinkware, LLC v. Nat’l Graphics, Inc., 800 F.3d 1375, 1378 (Fed. Cir. 2015)

Overview

- Summary of The IPR Grounds
- The '474 Patent Overview
- Firm 305 is Not a “Security Policy Management Server”
- **Law in View of Golnabi Fails to Render Challenged Claims Obvious**
- Neither of Petitioner’s Theories Support a Finding That Law Teaches or Suggests “an Indication of a Feed”

Law Alone Does Not Disclose Altering Rules Based on Correlation Between Portions of Malicious Traffic Information

- It is undisputed that Law does not explicitly disclose this limitation.
- This limitation is non-obvious over Law alone because Petitioner manufactures the “duplicate rules” problem suggests the claimed invention as the solution.
 - Law does not describe the “duplicate rules” problem identified in the Reply. [Sur-Reply at 8-12.](#)
 - Even if Law had identified a problem with “duplicate rules,” the allegedly obvious “solution” to this problem relies on *ex post* reasoning taken from the ‘474 patent, not any disclosure in the prior art or knowledge of the skilled artisan. *See POR at 22*

A patent challenger cannot “use the challenged patent as a roadmap to reconstruct the claimed invention . . . i.e., the impermissible *ex post* reasoning and hindsight bias that *KSR* warned against.”

TQ Delta, LLC v. CISCO Sys., Inc., 942 F.3d 1352, 1361 (Fed. Cir. 2019)

“[K]nowledge of a problem and motivation to solve it are entirely different from motivation to combine particular references to reach the particular claimed method.”)

Innogenetics, N.V. v. Abbott Lab’ys, 512 F.3d 1363, 1373 (Fed. Cir. 2008)

Law Alone Does Not Disclose Altering Rules Based on Correlation Between Portions of Malicious Traffic Information

- **At best, a POSITA would have removed duplicate data from the analyzed threat data, not from the dynamic security policy, as claimed.**
 - 474 Patent at Claims 1, 9, 17 (“wherein one or more of the packet filtering rules **[of the dynamic security policy]** were added, removed or altered”), Claim 25
 - POR at 24-25 (asserting that a POSITA would have analyzed the received threat data and removed duplicate data before constructing updates to rulesets).
 - Reply at 11-12 (Alleging that the threat data includes the duplicate rules); *see also id.* at 13; Ex. 2007 at 48:11-22; POR at 23-24 (In fact, Petitioner does not dispute that Law’s operator-created rulesets e.g., ruleset 147, do not include any duplicate rules.

Ex. 1005 (Law), ¶89

Law in View of Golnabi Does Not Disclose Altering Rules Based on Correlation Between Portions of Malicious Traffic Information

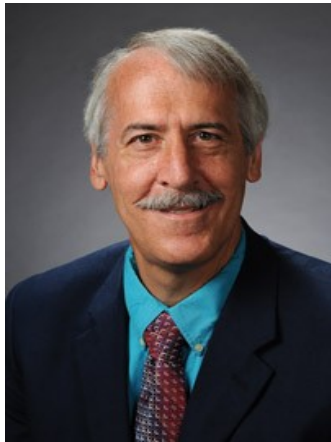
- Petitioner’s allegation that Golnabi “solve[s] the same problem” (reply at 12) does not supply the motivation to combine the references to reach the particular claimed invention.
 - Law does not identify the duplicate rules problem that Golnabi allegedly solves.
 - Petitioner’s combination facially does not satisfy the Challenged Claims requirement of adding, removing or altering rules of the dynamic security policy instead of the alleged threat data. See ‘474 Patent at Claims 1, 9, 17, 25.
 - To the extent that there is any “duplicate” data in Law, the parties agree that the duplicates would be found in the received threat data, not in the dynamic security policy generated by Law’s operator. POR at 23-24, Sur-Reply at 12-13.

Law in View of Golnabi Does Not Disclose Altering Rules Based on Correlation Between Portions of Malicious Traffic Information

- **Petitioner’s allegation that Golnabi “solve[s] the same problem” (reply at 12) does not supply the motivation to combine the references to reach the particular claimed invention.**
- Petitioner’s combination facially does not satisfy the Challenged Claims requirement of adding, removing or altering rules of the dynamic security policy instead of the alleged threat data. See ‘474 Patent at Claims 1, 9, 17, 25.
 - To the extent that there is any “duplicate” data in Law, the parties agree that the duplicates would be found in the received threat data, not in the dynamic security policy generated by Law’s operator. POR at 23-24, Sur-Reply at 12-13.
 - Even if duplicate rules were a known problem, the problem does not provide a sufficient reason for why a POSITA would have been motivated to correlate the threat data and remove packet filtering rules from the dynamic security policy based on the correlated information, as required by the challenged claims.

Obviousness concerns whether a skilled artisan not only *could have made* but *would have been motivated to make* the combinations or modifications of prior art to arrive at the claimed invention.” *Belden Inc. v. Berk-Tek LLC*, 805 F.3d 1064, 1073 (Fed. Cir. 2015)

Claims 1-27 Patentable Over Law (Ground 1)



Dr. Douglas Jacobson
Petitioner's expert

1 BY MS. FULLER:

2 Q. What -- when carrying out that service, like
3 what infrastructure, IT personnel components are
4 involved in firm 305?

5 MR. DETRIXHE: Objection, form.

6 A. I can give you my opinion of what -- what I
7 think a 305 would look like. Law just identifies it as
8 a 305, but it would be -- it would obviously have an IT
9 infrastructure, 'cause it would need to receive data,
10 receive rules and other -- other information from the
11 315s. So it would have to have a place to store that
12 information.

13 It would need then necessary processing power
14 to work with the various -- the information that it got
15 from the 315s in order to process the rules and put
16 them in a -- you know, duplications and et cetera as it
17 needs to do, putting it in a format that can be
18 ingested by the system in Law, so it's going to have to
19 be the, in essence, the post process -- well, the
20 processing in order to go out to be ingested. It will
21 need storage for that.

22 Staff, you know, is what he can say but
23 you're going to need obviously the staff to make sure
24 that the computers all through that -- you know, that
25 the computers are running and they're up to date so you

1 have a staff infrastructure -- you have a staff to
2 manage the infrastructure, typically these firms will
3 also have staff that understand, you know, something
4 about the 315s and understand, you know, issues about
5 threats, et cetera. And so you're going to have some
6 security type personnel in the 305 and then, of course,
7 that's all. You know, I mean, I'm going to completely

Ex. 2014 at 37:2-38:7

Petitioner's expert Dr. Jacobson acknowledges that firm 305 operates as a service comprising various IT infrastructure and staff

This would support the contention that Firm 305 is a commercial entity and not a server, that includes IT personnel staff and various other components involved in updating rulesets.

Claims 1-27 Patentable Over Law (Ground 1)

Term	Proper Construction
“Receiving a Dynamic Security Policy Comprising a First Set of Rules”	PSG must receive the initial dynamic security policy, including a first set of rules, from the SPMS. This construction accounts for the difference between “a dynamic security policy” and updates to a dynamic security policy.

'266 POR at 8-10

Accordingly, the claims and specification limit the first set of packet filtering rules as being included in the dynamic security policy that is sent from the SPMS to the PSG, therefore ascribing a significance to the “first set of packet filtering rules” other than the “common patent-law convention to distinguish between repeated instances of an element or limitation.”

3M Innovative Props. Co. v. Avery Dennison Corp., 350 F.3d 1365, 1371 (Fed. Cir. 2003).

Claims 1-27 Patentable Over Law (Ground 1)

Petitioner's reliance on state-of-the-art techniques is unavailing; petitioner fails to address how Law does not provide state-of-the-art evidence of automatic rule generation because Law explicitly explains how and why IT personnel must be involved in managing access to the process control network

[0021] One possible solution for network security is described in U.S. Patent Application Publication No. 2007019906 to Byres et al., entitled "NETWORK SECURITY APPLIANCE" and the Tofino™ system manufactured by Byres Security Inc. of Lantzville, BC. These solutions discover and identify network devices and create firewall rules to control the traffic flowing to them by automatically locating devices and generating rules by passively analyzing traffic on the network. When the solution discovers a new device, it prompts the system administrator to accept its deductions and insert the new device into the network inventory diagram, or flag the device as a potential intruder. This way, IT personnel and the network control engineer always have a current network map. While this solution ensures that IT personnel are able to quickly and accurately manage the network, the solution is still left entirely to the expertise and control of separately-trained IT personnel. Operators within a process control system would have no capability to monitor and manage process control network security from operator workstations.

[0020] In other circumstances, IT personnel have limited or no detailed understanding of the control system details and how the control system is to properly function to meet control objectives (e.g., permitted control communications between controllers and devices, permitted data communications between devices, permitted firmware updates to devices, permitted external access by remote users to the control system, etc.). As such, IT personnel may be at a significant disadvantage regarding proper access controls, permission settings, and/or proper firewall rules configuration for the system. For example, an IT professional may install one or more firewall devices and/or firewall software applications to operate between a control system network boundary and an intranet and/or Internet boundary. However, such firewalls are not typically configured with rules and access permissions that account for the unique needs of the control system that would result in optimum functionality of the control system while maintaining a desired degree of network security. As a result, the IT professional may simply configure the firewall iteratively in response to complaints from control system administrators regarding communication failures and instances of improper control system operation. Such iterative efforts to configure the firewall results in workforce inefficiency, failures, lost profits, and safety risks.

Claims 1-27 Patentable Over Law (Ground 1)

- Law's Firm 305 is not a "Security Policy Management Server" that distributes initial rulesets and automatically updates the rulesets
 - Firm 305 is not a "Security Policy Management Server" but a commercial entity.
POR at 34-35 (citing Ex. 2011 at 3), Ex. 2014 at 37:2-38:7, Law, ¶¶ 83, 88.
 - Firm 305 does not automatically update rulesets as IT personnel are required in the updates.
POR at 14-15, 34-35; Law, ¶¶ 16, 88.
 - Firm 305 does not distribute "a Dynamic Security Policy Comprising a First Set of Rules"
 - Claim Construction: "Receiving a Dynamic Security Policy Comprising a First Set of Rules"
 - Firm 305 only distributes updates to operator-created initial rulesets

Claims 1-27 Patentable Over Law (Ground 1)

- Law does not disclose automatically creating or altering rulesets. *See Reply at 15-18 (citing paragraphs 83 and 88 of Law, neither of which discloses that firm 305 provides automatic updates of rulesets).* Rather than confronting this determinative fact, Petitioner tries to shift the burden onto Centripetal, claiming that Centripetal failed to “explain what role IT personnel would have had, if any, in the constructing of rulesets.” *Reply at 16.* But it is Petitioner’s burden to show that Law discloses firm 305 providing updates without IT personnel involvement, and that burden does not shift to Centripetal to prove otherwise. *Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015) (“‘In an inter partes review, the burden of persuasion is on the petitioner to prove ‘unpatentability by a preponderance of the evidence,’ 35 U.S.C. § 316(e), and that burden never shifts to the patentee.”) (citation omitted).
- Petitioner fails to explain **why** a POSITA would have implemented automatic ruleset updates in firm 305 when Law explains that IT personnel of firms are still required to update rulesets of the process control system or demonstrate **how** automatic updates would have overcome its stated need for manual updates by third-party IT personnel. *See POR at 38-39 (citing Ariosa Diagnostics v. Verinata Health, Inc.*, 805 F.3d 1359, 1366 (Fed. Cir. 2015) (a petitioner must “provide adequately developed explanations when relying on background knowledge based on cited art”); *see also POR at 14-15 (establishing that Law’s invention still leverages IT personnel of third party firms to perform manual updates).*
- Petitioner selectively cherry-picks Law’s “any type of information technology method” passage to argue that this would have suggested to a POSITA to use automatic techniques *(see Reply at 17)* to the exclusion of Law’s teaching that third-party IT personnel are still required for updating process control system. *Henny Penny Corp. v. Frymaster LLC*, 938 F.3d 1324, 1331-32 (Fed. Cir. 2019) (articulating the “longstanding principle that the prior art must be considered for all its teachings, not selectively.”).

Overview

- Summary of The IPR Grounds
- The '266 Patent Overview
- Claims 1-27 Patentable over Law
- **Claims 1-27 Patentable over Law in View of Wood**
- Law in view of Wood and/or Jungck Fails to Render Obvious Dependent Claims

Claims 1-24 Patentable Over Law in View of Wood (Ground 2)

- Wood Does Not Cure the Deficiencies of Law
 - As explained in the POR, Wood does not cure the deficiencies of Law
 - Petitioner does not dispute this in reply. Therefore Ground 2 does not render obvious the Challenged Claims

Overview

- Summary of The IPR Grounds
- The '266 Patent Overview
- Claims 1-27 Patentable over Law
- Claims 1-27 Patentable over Law in View of Wood
- **Law in view of Wood and/or Jungck Fails to Render Obvious Dependent Claims**

Dependent Claims Patentable Over Law in View of Wood and/or Jungck (Grounds 3/4)

- Wood and/or Jungck Do Not Cure the Deficiencies of Law
 - As explained in the POR, Wood does not cure the deficiencies of Law, nor does Jungck
 - Because Grounds 3 and 4 challenge the dependent claims, these grounds fail for the same reasons Grounds 1 and 2 Fail.