



PTAB Oral Argument

April 22, 2024

KEYSIGHT TECHNOLOGIES, INC.

v.

CENTRIPETAL NETWORKS, LLC

PETITIONER

PATENT OWNER

CASE NO.: IPR2023-00448

PATENT NO.: 11,012,474

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”

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”

IPR2023-00448 ('474) – Summary of the IPR Grounds

Ground	Challenged Claims	35 U.S.C. §	References
1	1-3, 5-7, 9-11, 13-15, 17-19, 21-23, 25-27, 29-31, 33	103	Law, Golnabi
2	2, 10, 18, 26	103	Law, Golnabi, Wood
3	4, 12, 20, 28	103	Law, Golnabi, Ke
4	5, 13, 21, 29	103	Law, Golnabi, Jungck
5	7, 8, 15, 16, 23, 24, 31, 32	103	Law, Golnabi, Johnson

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”

The 474 Patent Overview: Methods and Systems for Protecting a Secure Network

US011012474B2

United States Patent Rogers et al.

(10) Patent No.: US 11,012,474 B2
(45) Date of Patent: *May 18, 2021

(54) METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK

(71) Applicant: Centripetal Networks, Inc.,
Potsdam, NY (US)

(72) Inventors: Steven Rogers, Leeburg, VA (US);
Sean Moore, Hollis, NH (US); David
K. Ahn, Winston-Salem, NC (US);
Peter P. Gremia, Potsdam, NY
(US)

(73) Assignee: Centripetal Networks, Inc.,
Potsdam, NY (US)

(*) Notice: Subject to any disclaimer, the term of this
patent is extended or adjusted under 35
U.S.C. 154(b) by 0 days.

This patent is subject to a terminal dis-
claimer.

(21) Appl. No.: 17/027,436

(22) Filed: Sep. 21, 2020

(65) **Priority Publication Data**

US 2021/0014277 A1 Jan. 14, 2021

Related U.S. Application Data

(60) Continuation of application No. 16/909,327, filed on
Jan. 23, 2020, and a continuation-in-part of
(Continued)

(51) **Int. Cl.** (2006.01)

H04L 29/06

H04L 29/08

(52) **U.S. Cl.** (2006.01)

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 63/0218; H04L 63/0263;
H04L 67/02; H04L 63/425;

(Continued)

(56) References Cited

U.S. PATENT DOCUMENTS

6,098,172 A 8/2000 Cosa et al.

6,147,976 A 11/2000 Shand et al.

(Continued)

FOREIGN PATENT DOCUMENTS

AU 2005328336 B2 9/2011

AU 2006230171 B2 6/2012

(Continued)

OTHER PUBLICATIONS

Jul. 26, 2018 (US) Declaration of Kevin Jeffrey, PhD in Support of
Second Petition for Inter Partes Review of U.S. Pat. No. 9,137,205—
IPR2018-01444.

(Continued)

Primary Examiner — Cheng-Feng Huang

(74) Attorney, Agent, or Firm — Banner & Witcoff, L.L.P.

(57) ABSTRACT

Methods and systems for protecting a secured network are
presented. For example, one or more packet security gate-
ways 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 manage-
ment 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.

33 Claims, 13 Drawing Sheets

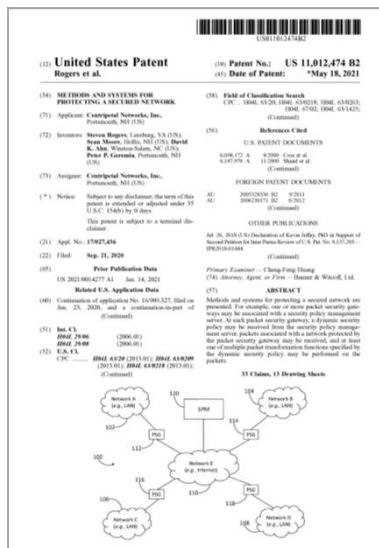
(57)

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.

Ex. 1001 ('474), Abstract

The 474 Patent Overview: Methods and Systems for Protecting a Secure Network (cont'd)



Plurality of networks

Packet Security Gateways

Ex. 1001 ('474), Figure 1 (annotated), 4:46-67

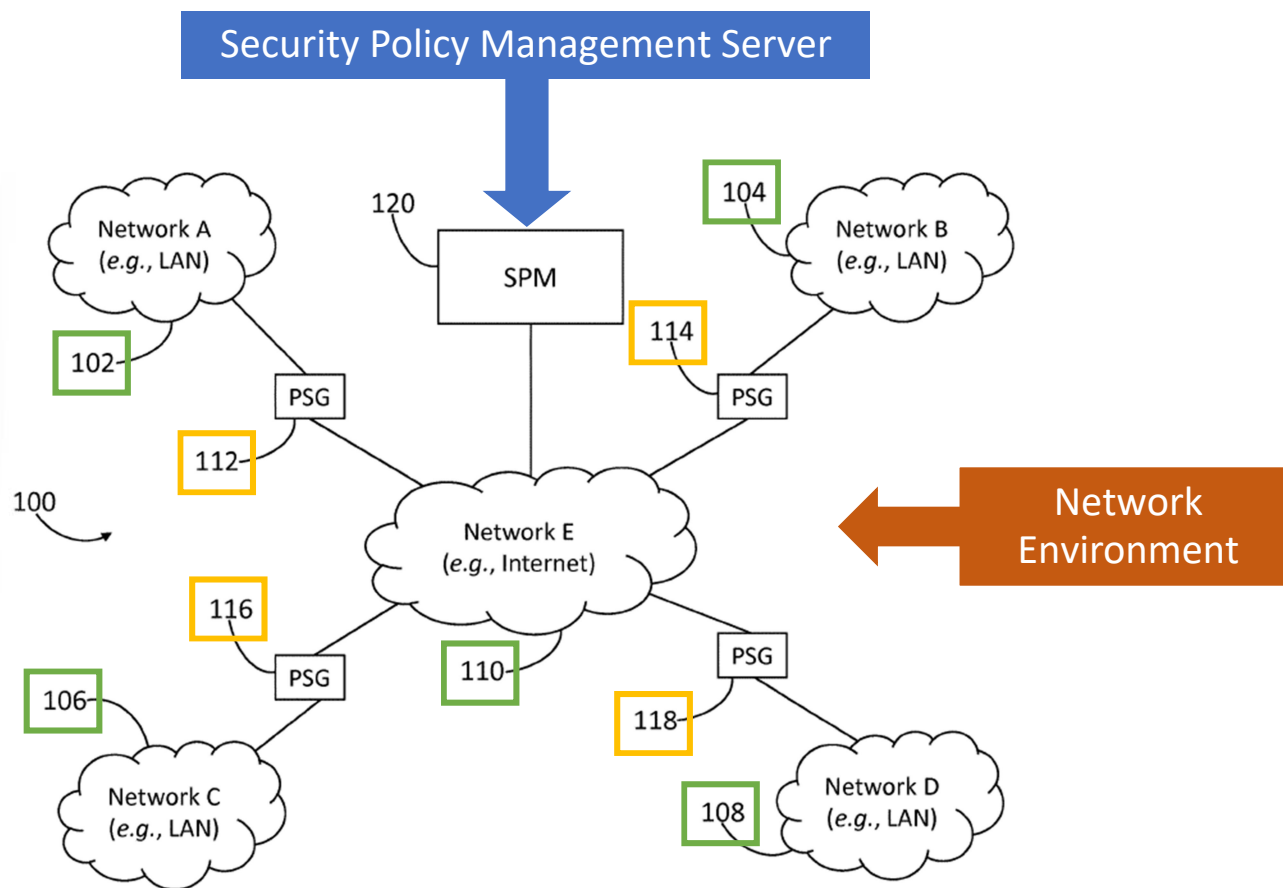
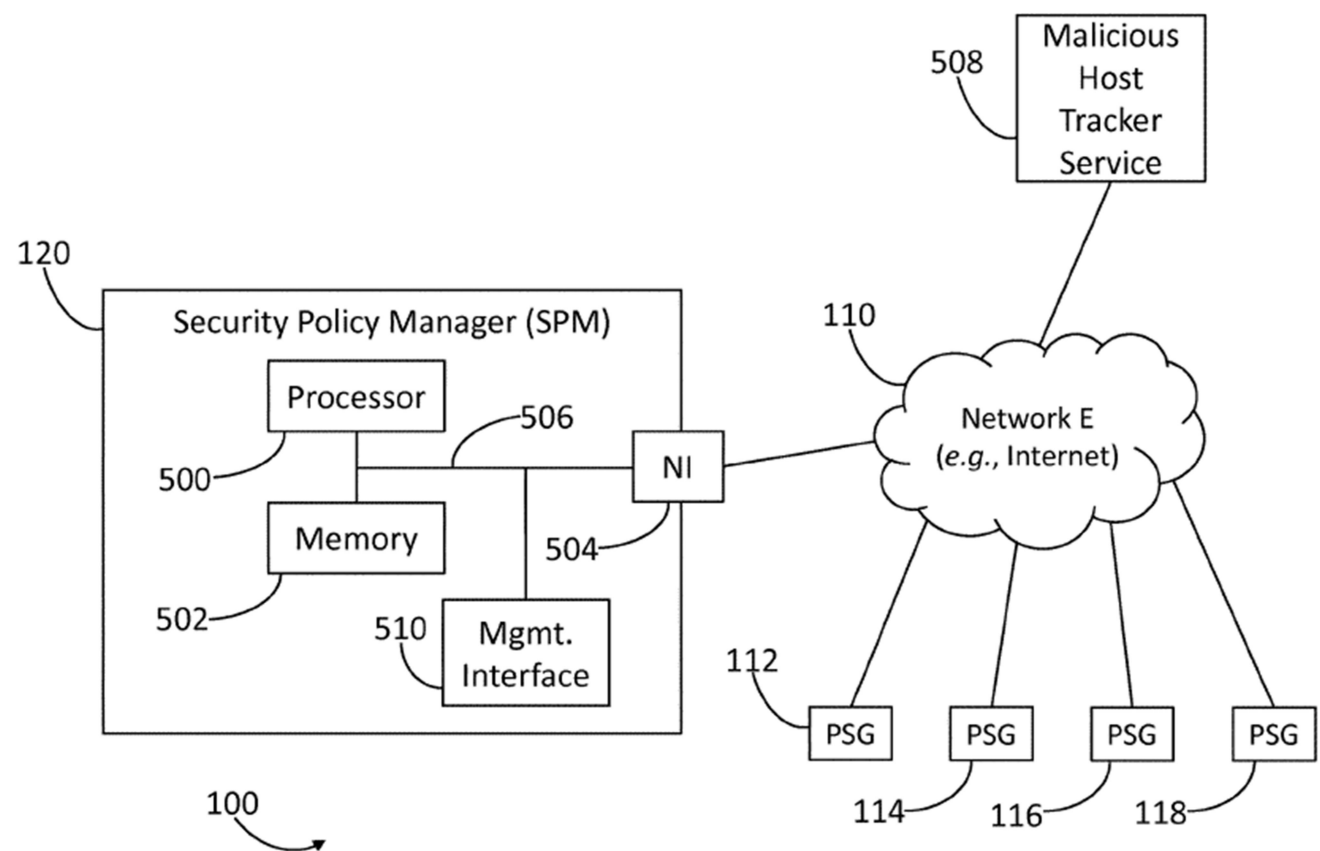


FIG. 1

The 474 Patent Overview: Methods and Systems for Protecting a Secure Network (cont'd)



Ex. 1001 ('474), Figure 5, 15:7-55

FIG. 5

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”

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,” “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 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 device 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 device 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 manufacture, 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 subdomain 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 not 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 updateservice 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 configured 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. These subsystems may, in turn, also determine smaller sets of rules and distribute these 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. 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 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.

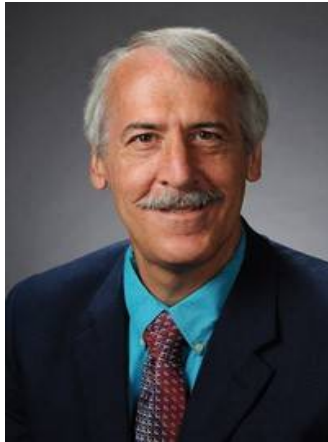
[0091] Each of the rulesets 147, 148, 151, 153 may define conditions that, if detected, implement some combination of blocking suspected malicious communications or alerting an operator or other plant personnel through an alarm displayed within one or more graphical displays, as previously described. 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), ¶188

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.



**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

*Excerpt from
Ex. 2006 at 37:2-38:7*

Firm 305 is Not a “Security Policy Management Server”

Firm 305 Does Not Automatically Update Rulesets:

- Law explains how and why IT personnel must be involved in managing access to the process control network. *See POR at 18-19 (citing Law at ¶ 21 (“‘[S]eparately-trained IT personnel’ are required to ‘quickly and accurately manage’ the industrial environment”))*
- Firm 305’s IT personnel are involved in updating rulesets, i.e. constructing the updates and running tests. *Ex. 2006 Jacobsen Tr. at 38:1-10; POR at 13, 18-19.*
- Petitioner does not explain how or why a POSITA would have modified Law in order to reach a system that operates automatically, without the IT personnel that Law says are required. *Law (Ex. 1005) at ¶16, 88; Ariosa Diagnostics, 805 F.3d at 1366; Reply at 6.*

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 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 as 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.



Dr. Douglas Jacobson

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.

Ex. 2006 at 38:1-10

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 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.

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 topology 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 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 offline 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), ¶183

Firm 305 is Not a “Security Policy Management Server”

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

- Law’s disclosure of creating rulesets using “any type of information technology method” does not suggest automatically updating rulesets because that overbroad reading conflicts with Law’s requirement for IT personnel are required this task. *See Reply at 6.*

“[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 have the control system 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 tentative 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., 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 deployed 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 Hytes et al., entitled “NETWORK SECURITY APPLIANCE,” and the Tofino™ system manufactured by Hytes 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 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 comprises 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 second device and, when network traffic is received, determines if the network traffic received at the second device violates one or more of the rules applied to the secured device. If the network traffic received at the second 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 second 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 5; Sur-Reply at 5-6.*
- It is Petitioner’s burden to prove that a POSITA would have had a reasonable expectation of success in implementing any “state of the art” techniques to reach the claimed invention. *Sur-Reply at 5-6.*
DEMONSTRATIVE EXHIBIT – NOT EVIDENCE
- Dr. Jacobson admits that the firm 305’s IT personnel would be involved in updating rulesets.

POR at 13, 18-19; Ex. 2006 at 38:1-10.

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), ¶189

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)

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”**

Neither of Petitioner's Theories Support a Finding That Law Teaches or Suggests "an Indication of a Feed"

- Petitioner's theory that Law's protocol 130s indicates a feed is unsound because Petitioner also cites this information as the claimed "packet matching criterion." *See. Pet. At 38-39, 42-43; Reply at 17; see also POR at 28-29; see also '474 Patent at Claims 1, 9, 17, 25, See also Paper 7, Institution Decision at 45-46.*

Where a claim provides for two separate elements, such as for "second portion" and a "return portion," these two elements "logically cannot be one and the same."

Engel Indus., Inc. v. Lockformer Co., 96 F.3d 1398, 1404-05 (Fed. Cir. 1996)

Rejecting petitioner theory as improper because it relied on same prior art component for multiple claim elements.

Cisco Sys., Inc. v. Egnera, Inc., No. IPR2017-01341

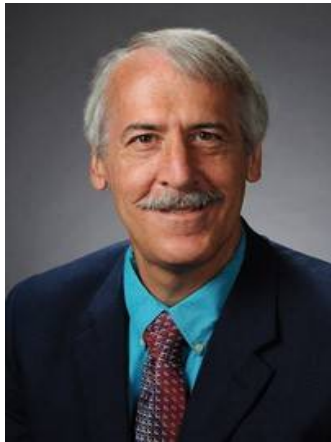
Affirming PTAB determination that petitioner failed to demonstrate unpatentability when it mapped two distinct limitations to same element in prior art

Comcast Cable Comm'ns, LLC v. Promptu Sys. Corp., 838 F. App'x 551, 553-554

"Where a claim lists elements separately, 'the clear implication of the claim language' is that those elements are 'distinct component[s]' of the patented invention.

Becton, Dickinson & Co. v. Tyco Healthcare Grp., LP, 616 F.3d 1249, 1254 (Fed. Cir. 2010)

Neither of Petitioner's Theories Support a Finding That Law Teaches or Suggests "an Indication of a Feed"



Dr. Douglas Jacobson
Petitioner's expert

4 Q. So the SCPI protocol is still used
5 for -- in a condition field to indicate a
6 specific packet matching criterion; is that
7 correct?
8 A. Yeah, that's -- yeah.
9 Q. And what is the SCPI protocol used
10 for?
11 A. Boy, I'd have to research. That's not
12 one that I'm intimately familiar with. Given
13 that Law referenced it, I would speculate that
14 it is some type of a process protocol.
15 Q. A process protocol for the process
16 control system?
17 A. Yeah. He talks about the Hart
18 protocol, that's the one that he mentions in his
19 documents. And --
20 Q. But sitting here today, you don't have
21 a recollection of what the SCPI protocol is?
22 A. No, I don't.

Admitting that he
did not even know
what the SCPI
protocol is used for
let alone how it is
less common so as
to identify a
particular field

Ex. 2007 at 42:9-22

Neither of Petitioner's Theories Support a Finding That Law Teaches or Suggests “an Indication of a Feed”

- **The record evidence establishes that the existence of a certain protocol in a rule does not indicate the feed that the rule was based on:**
 - Ex. 2006 at 20:5-22, 22:17-24:23 – Dr. Jacobson testifying that there is a “high likelihood” that various sources provide duplicate rules with the same protocol, including SCPI.
 - Ex. 2007 at 48:11-24; 43:23-45:9 – Dr. Jacobson testifying that because of the “high likelihood” that a number of sources provide duplicate rules under a particular protocol type, there is no factual basis for Petitioner’s assumption that Law’s protocol would, or even could, identify a particular feed from one source. See Reply at 18-19.
 - Dr. Jacobson Reply Declaration (Ex. 1017 at ¶29) – Parroting the Reply’s conclusory argument without any supporting explanation or citation to corroborating evidence.
 - Reply at 18 – Petitioner admitting that different sources provide rules with the same protocol, such as SCPI recognizing that it is “not always . . . The case that one of the sources 315 of a plurality of sources would have been the only source providing rules under a particular protocol (such as SCPI)”, id. at 19 (conceding that rules are attributable to several sources).

“The cited declaration testimony is conclusory and unsupported, adds little to the conclusory assertion for which it is offered to support, and is entitled to little weight.”

Neither of Petitioner's Theories Support a Finding That Law Teaches or Suggests “an Indication of a Feed”

- **Petitioner has not established that it would have been obvious to modify Law to include “an Indication of a feed”:**
 - Petitioner's rationale lacks any motivation for modifying rule table or firm 305's rules *See Pet. At 42-43; Reply at 20, 22.*
 - The combination would further require firm 305 to modify the rules it provides in order to populate Law's rule table with the claimed indication.
 - Petitioner has made no effort to explain how and why a POSITA would have made that modification, and there is no record evidence supporting such a modification.
 - **Petitioner's Reply improperly introduces a new rationale based on the “possibility of errors” in the threat data. *See Reply at 20, 22.***
 - The Board should not consider this new rationale. *Intelligent Bio-Sys.*, 821 F.3d at 1369-70 (the Board is not permitted to entertain an ‘entirely new rationale’ in reply).
 - Like its previous rationale, this one is constructed entirely from hindsight with no teaching or suggestion in the prior art. *See POR at 34.*
 - That certain benefits of the claimed invention are appreciable in hindsight (e.g., the ability to identify whether a rule came from a particularly trustworthy or untrustworthy feed), is not evidence of its obviousness when there is no evidence of the limitation (or its benefit) being known in the art.

Neither of Petitioner's Theories Support a Finding That Law Teaches or Suggests “an Indication of a Feed”



Dr. Michael Goodrich
Patent Owner's expert

- Petitioner relies on reliability and trustworthiness as reason to modify rule table, however this rationale would not have prompted a POSITA to make any modification to the rule table, much less firm 305's rules. *See Pet. At 42-43; Reply at 20, 22.*

12 Do you think a person of skill in the art
13 might find the threat data or the threat identified
14 by the six sources to be a more reliable indicator of
15 a threat than the one identified by only one source? 12:13:58
16 A. No.
17 Q. Why is that?
18 A. Because a threat is a threat. How many
19 people say it as a threat doesn't make it worse or
20 better. 12:14:13