 Express Mail Label No. EL844453103US
Date of Deposit: June 14, 2002

STATEFUL DISTRIBUTED EVENT PROCESSING AND ADAPTIVE SECURITY

CROSS-REFERENCE TO RELATED APPLICATIONS

This application claims priority to provisional U.S. application Serial No. 60/298,592 filed June 14, 2001 and entitled Stateful Distributed Event Processing and Adaptive Security, the disclosures of which are incorporated herein by reference.

This application is also related to co-pending U.S. application Serial No. 10/071,328 filed February 8, 2002 and entitled Stateful Reference Monitor, the disclosures of which are incorporated herein by reference.

BACKGROUND

This invention relates to computer network security, and more particularly to methods and apparatus for securing one or more nodes on a computer network.

Conventional network security systems can be said to provide either "active" or "passive" protection. Active security systems provide real-time barriers to intrusions, via software- or hardware-based pre-programmed intrusion detection measures. "Passive" systems provide the ability to detect and recover from previously observed security breaches, by examining data gathered about previous system access activity, so as to improve static access controls and policies over time. Active systems, then, function primarily to prevent intrusions, and passive systems function primarily to report on and examine data about previous intrusions to prevent future intrusions.

Examples of conventional active security systems include access control tools, content filtering tools, and system auditing tools. Access control tools, such as network firewalls, can be deployed on dedicated machines, usually at a network perimeter, to control inbound and outbound access using pre-configured permission levels. Content filtering tools, like computer virus scanners, typically execute on either an e-mail server or a workstation, and function by screening incoming content, like e-mail and attached files, for potentially threatening matter, based on known signatures of previously observed attacks. System auditing tools, like reference monitors, may provide either stateless or state-based monitoring (such as the state-based monitoring provided by the

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

stateful reference monitor described in U.S. Patent Application Serial No. 10/071,328 and incorporated by reference herein) of individual workstations or servers, by identifying variations from either pre-determined settings or a dynamic machine state.

Examples of conventional passive security systems include activity logging tools and auditing tools, which may be employed in conjunction with one another. Activity logging tools track the activity of one or more computers and transcribe observed system activity to a series of log files as individual entries. Auditing tools typically examine those log entries to discern breaches, attacks, or other potentially threatening activity, occurring either across machines or within individual machines.

Both types of security systems provide useful intrusion detection and prevention functions. However, both generally rely on pre-programmed network administration policy, business rules, or other parameters, and so neither (particularly passive systems) provides the adaptation capability sometimes necessary to counter novel types of attacks as they occur. Also, conventional active systems are unable to observe and correlate seemingly innocuous activity as it occurs across nodes to determine that an intrusion is in progress. Given the growing ubiquity of computer networks and the value of electronic assets, commensurate growth of network security threats is to be expected. Therefore, a security system which provides adaptive countermeasures in real time to localized (i.e., limited to one node) or non-localized intrusions would provide tremendous value to operators of computer networks.

SUMMARY OF THE INVENTION

A first embodiment of the invention provides a method of maintaining a networked computer system including first and second nodes and an event processing server, comprising the first and second nodes detecting changes in state, the event processing server receiving notification of the changes in state from the first and second nodes, the event processing server correlating changes in state detected in the first and second nodes, and the event processing server executing a maintenance decision which affects the first and second nodes, wherein the detecting, transmitting, correlating, and executing occurs without human intervention.

This embodiment may be practiced wherein the changes in state are a result of at least one of an event and the absence of an event, wherein the changes in state are recognized by a reference monitor, and/or wherein the event processing server receiving

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

the report is the result of one of the first and second nodes reporting to the event processing server and the event processing server polling the first and second nodes. The embodiment may further include the event processing server updating an operating policy on the network, and updating the operating policy may include at least one of requesting security policy changes on at least one node, requesting changes to privileges to access system resources on at least one node, tuning system parameters on at least one node, and modifying network firewall parameters. At least one node may further enact the updated operating policy. Also, the embodiment may further include notifying an external entity of actions taken, and the external entity may be a network administrator or a software application executing on the network.

A second embodiment of the invention provides a method for maintaining a networked computer system including at least one node detecting a change in state, an event processing server on the network receiving notification of the at least one change in state from the at least one node, and the event processing server responding to the notification by executing a maintenance decision, wherein the detecting, receiving, and responding occurs without human intervention.

This embodiment may be practiced wherein the change in state is a result of at least one of an event and the absence of an event, wherein the change in state is recognized by a reference monitor, wherein the event processing server receiving the report is the result of one of the node reporting to the event processing server and the event processing server polling the node, and may be practiced wherein the maintenance decision affects the at least one node detecting the change in state, and/or wherein the maintenance decision affects at least one node other than the node detecting the change in state. The embodiment may further include the event processing server updating an operating policy on the network, wherein updating the operating policy may include at least one of requesting security policy changes on at least one node, requesting changes to privileges to access system resources on at least one node, tuning system parameters on at least one node, and modifying network firewall parameters. The embodiment may still further include at least one node enacting the updated operating policy, and/or notifying an external entity of actions taken, wherein the external entity is a network administrator or a software application executing on the network.

A third embodiment of the invention provides a method for maintaining a node on a networked computer system including at least one node detecting a change in state,

Find authenticated court documents without watermarks at docketalarm.com.

and the at least one node reacting to the change in state, wherein the at least one node detecting and reacting occurs without human intervention.

The embodiment may be practiced wherein the change in state is a result of at least one of an event and the absence of an event, and/or wherein the change in state is recognized by a stateful reference monitor. The embodiment may further include at least one node notifying an event processing server on the network, the event processing server responding to the notification by updating an operating policy on the network, wherein updating the operating policy includes at least one of requesting updates to security policy on at least one node, requesting changes to privileges to access system resources on at least one node, tuning system parameters on at least one node, and modifying network firewall parameters. The embodiment may further include the at least one node enacting the updated operating policy, and/or notifying an external entity of actions taken, wherein the external entity is a network administrator and/or a software application executing on the network.

A fourth embodiment of the invention provides a computer-readable medium having instructions recorded thereon, which instructions, when executed, enable at least one processor in a networked computer system to detect a change in state of a node, and process instructions defining reacting to the detected change in state.

The embodiment may further include instructions defining communicating the change in state to an event processing server, instructions defining processing maintenance instructions received from the event processing server, and/or instructions defining transmitting notification to a network administrator of actions taken.

A fifth embodiment of the invention provides a computer-readable medium having instructions recorded thereon, which instructions, when executed, enable at least one processor in a networked computer system to maintain an operating policy for the network, receive notification of a change in state from at least one node, and update the operating policy based on the change in state.

The embodiment may further include instructions defining storing received notifications of changes in state in memory, instructions defining correlating notifications received from a plurality of nodes, instructions defining storing received notifications in electronic file storage, and/or instructions defining notifying an external entity of actions taken, wherein the external entity is a network administrator or a software application executing on the network.

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

A sixth embodiment of the invention provides a method for maintaining a networked computer system including at least one node detecting a change in state, an event processing server on the network receiving notification of the at least one change in state from the at least one node, and the event processing server responding to the notification by dispensing a maintenance decision.

The embodiment may further comprise executing, by a human operator, the maintenance decision on at least one node on the networked computer system, or executing, without human intervention, the maintenance decision on at least one node on the networked computer system. A human operator may be prompted and allotted a predetermined period to execute the maintenance decision before it is executed without human intervention.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a functional block diagram depicting the interaction of system components which define aspects of at least one embodiment of the invention;

Figure 2 is a functional block diagram depicting the interaction of system components which define aspects of at least one other embodiment of the invention;

Figure 3 is a functional block diagram depicting the interaction of system components which define aspects of at least a third embodiment of the invention;

Figure 4 is a block diagram of an exemplary computer system on which aspects of embodiments of the invention may be implemented; and

Figure 5 is a block diagram depicting exemplary computer system components with which aspects of embodiments of the invention may be implemented.

DETAILED DESCRIPTION

Aspects of embodiments of the present invention provide methods and apparatus for securing a networked computer system through the coordinated execution of reference monitor and event agent software on individual nodes, and event processing server software on a network server, for achieving active security measures, administrative control, and the ability to correlate potentially threatening activity across multiple nodes in real time.

Computer system 400, shown in Figure 4, with which aspects of these embodiments, either individually or in combination, may be implemented, may include

Find authenticated court documents without watermarks at docketalarm.com.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.