HP WORLD ’96

Implementing Security Audit and Intrusion Detection in an Environment

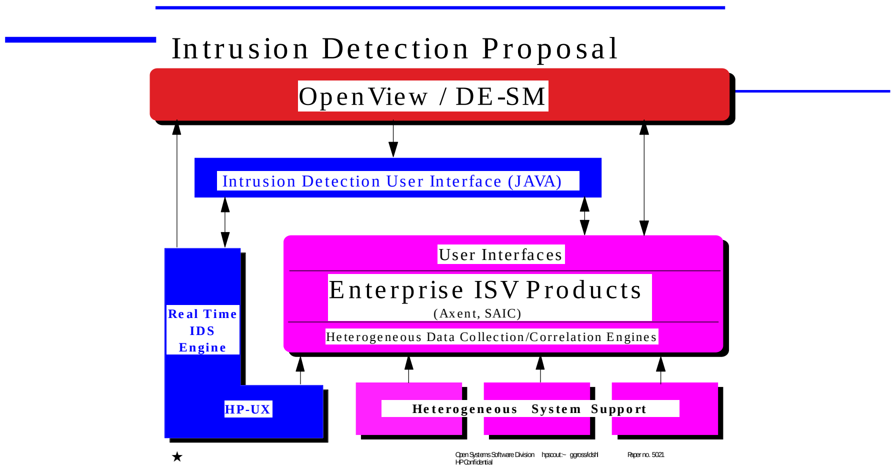
Presentation Number 5021

Bob Schwehr

Hewlett-Packard Co.
c/o Liz Ynegas

Phone: 408/447-3213
Fax: 408/447-4916
Email: liz_ynegas@hp-cupertino-om5.om.hp.com

Security Guard - the security inside


Intrusion Detection Proposal
OpenView / DE-SM
Intrusion Detection User Interface (JAVA)
User Interfaces
Enterprise ISV Products
(Axent, SAIC)
Heterogeneous Data Collection/Correlation Engines
Real Time
IDS
Engine
HP-UX
Heterogeneous System Support
★
Open Systems Software Division hpscout:~ ggross/idsh1
HP Confidential
Paper no. 5021

Goal of the Product:

To provide a software security window launched from OpenView, which displays Security Status across a networked set of computers and applications (e.g. on the intranet).

To enhance security conscious personnel’s ability to see threats to the security policy in real-time at a summary level, and to extract threat details on request.

Misuse and intrusion events are defined, and can be displayed as they happen. Event definitions are available as templates with the system, and additionally, can be custom designed by the user. The user interface itself can be used as-is, expanded, or replaced to reflect the production environment (Java Toolset Expansion Kit).

Role:

Security Guard expands Policy to include a random series of surveillance strategies which detect misuse and intrusions, and demonstrate visible security presence, while insuring minimum network and host system overhead for these activities (<10%).

Target Market and Customer:

Any set of systems where security is important to the operation of the software.

The Financial and Telecom markets are used as the primary measures of success.

Where security is important, and definitive, quick response to intrusions is necessary (rather than after-the-fact).

Complex environments where efficient surveillance is required.

Target User:

People in charge of applications, charged with protecting data integrity, a security person, or a person charged with maintaining system and network availability and integrity.

Functionality and Connectivity:

Event Notification is supported via:

OpenView High Level Alerts

- Via Distributed Enterprise - Smart Monitor (DE-SM) for Security
- Email
- Pager
- Display

OpenView Threat Details

- Java GUI Application (launched from OpenView)

The types of systems monitored:

HP systems are monitored in real time and support:

Rule Based Events

Interpretive and Behavior Event Detection via Genetic Programing and

AI modeling --- These are handled and displayed in real time.

HP Secure Web Platform running B1 rated HPUX-CMW

HPUX Computers running C2/ITSEC rated HPUX Trusted Mode

User Identification

User Logins (direct and network)

File System and Data Access/Integrity

Access to System Calls and Accesses to Processes

Access to Root

Access Control Violations

Networking ...**Non-HP systems are monitored based on Log-File Data and linked to the HP Intrusion Package via the Raxco Axent product family or customized with SAIC CMDS.**

Firewalls

*

*

*

WINNT Based Systems

Sun Systems

Dec

IBM

User Interfaces:

System Display is provided via the HP OpenView Product.

Detailed visualization displays can be local, centralized, or remote (Anywhere on the network), any platform which supports multithreading and a JAVA interpreter.

The product display can be:

HPUX Systems/Workstations

SUN Systems

WINNT

X-Terminals

Product Capability Details:

Notification Features

Notifications can be sent to any user as a "pop up" display

Notifications at any heterogeneous platform (JAVA interface) supporting JAVA or JAVA-compatable net browsers including multithreading

Notification can be observed within Netscape or a JAVA application with no additional user interface

All notifications are expandable by using the Companion Module Toolkit

Notification messages are secure

"Notify me if"..

File System

when a user switches to a directory where he doesn't belong

Optionally record all additional file system activities for this user for a "period".

when a user attempts to open a file for read when he shouldn't

when a user attempts to open a file for write when he shouldn't

when a user attempts to create a file larger than a specified size

if my anonymous ftp area is filling up

if a file is left open for read for longer than a specific time

if a file is left open for write longer than a specific time

Processes

when dynamic data memory allocation exceeds a specified amount

when the priority of this process exceeds a specified value

when this process' overhead exceeds a raw cpu percentage for a specified period of time

this process sleeps or waits longer than the specified period of time

if the nice value exceeds the specified range

if the total size of the process exceeds a specified value

if this process resides in a specific state longer than a specified time

Identity

when a user of specified identity connects with this system

(IP address only, unless Companion Detector Modules are used. Direct logins, okay)

Users (multiple processes)

when the raw cpu overhead for a user or process exceeds a specified quantity for a specified period of time

a user executes any of a list of specified processes

System wide

if the load average goes above a specified value for a specified period of time

if the idle average goes below a specified value

if the system wide interrupt overhead goes above a specified percentage

if the real or virtual memory usage goes above a specified value

Application Specific

Application specific notifications are completely customizable by using the Security Guard Companion Module Toolkit. In-kernel Detector Modules, which generate triggers and manage context dependent actions, can be dynamically inserted and removed from the application audit data stream.

Product Description

Security conscious personnel want to be notified immediately, when intranet hosts are being compromised. Security problems can be characterized as notification events caused by misusing one or more applications, memory, process resources, the file system, or network connection resources. In HP-UX, the events can be caught by collecting and routing audit messages to Detectors which catch the anomalies and report alerts to the management platform.

This product offers the following components:

1. an extensible heterogeneous (JAVA) user interface (prerequisite: Netscape 2.0 or other Net browser; JAVA support is required) for IDS configuration and Intrusion/Misuse notifications

2. a set of STREAMS-based real-time Detector modules

3. base HP-UX IDS functionality, which includes audit data quantity control, and audit data routing

Contact

Gary Gross (408-447-6966)