

# Interworks 2000

1/14/2000

[Click here to start](#)

## Table of Contents

[Interworks 2000](#)

[Abstract](#)

[Abstract](#)

[Abstract](#)

[Contents](#)

[Contents](#)

[Contents](#)

[An Intranet Enabled Application](#)

[Adding the Internet](#)

[What is the Virtual Vault?](#)

[Internet Security Goals](#)

[Associated Risks](#)

[Risk Mitigation Strategies](#)

[Risk Mitigation Strategies \( continued \)](#)

[Virtual Vaults Implementation of: Internet Traffic Filtering](#)

[Virtual Vaults Implementation of: User Authentication](#)

[Virtual Vaults Implementation of: User Authorization](#)

[Virtual Vaults Implementation of: User Authorization \( continued \)](#)

[Virtual Vaults Implementation of: Directory Concealment](#)

[Virtual Vaults Implementation of: Data Partitioning](#)

[Virtual Vaults Implementation of: Data Partitioning \( continued \)](#)

[Virtual Vaults Implementation of: Data Partitioning \( continued \)](#)

[Virtual Vaults Implementation of: Integrity Checking](#)

[Virtual Vaults Implementation of: Use of Least Privilege](#)

[Virtual Vaults Implementation of: Use of Least Privilege \( continued \)](#)

[Virtual Vaults Implementation of: System Surveillance](#)

[Virtual Vaults Implementation of: System Surveillance \( continued \)](#)

[Virtual Vaults Implementation of: System Surveillance \( continued \)](#)

[Virtual Vaults Implementation of: System Alarms](#)

[Virtual Vaults Implementation of: Simple Security Administration](#)

[Virtual Vaults Implementation of: Simple Security Admin. \( continued \)](#)

[Virtual Vaults Implementation of: Simple Security Admin. \( continued \)](#)

[Virtual Vaults Implementation of: Simple Security Admin. \( continued \)](#)

[Virtual Vaults Implementation of: Simple Security Admin. \( continued \)](#)

[Virtual Vaults Implementation of: Clear Site Security Policy](#)

**Author:** Stan M. Zitello

**Company:** Hewlett Packard

**Address:** 20 Perimeter Summit Blvd

Atlanta, Georgia 30019

**Voice:** (404) 648-5000

**Fax:** (404) 648-5450

**Email:** stan\_zitello@hp.com

[The Information Separation Paradox](#)

[Solution: The Trusted Gateway Agent](#)

[Solution: The Cross-Boundary IPC Mechanism](#)

[Solution: The Trusted Gateway Proxy](#)

[Solution: The TGP \( continued \)](#)

[Solution: The Java Servlet Proxy](#)

[Solution: The Java Servlet Proxy \( continued \)](#)

[Summary 1: Are you a candidate?](#)

[Summary 2: VV Definition Revisited](#)

[Questions and Answers](#)

# Interworks 2000

## Using Hewlett Packard's Virtual Vault for E-BUSINESS

presentation #75

*Stan M. Zitello*

*Hewlett Packard*



Slide 1 of 45

# Abstract

When your company allows your customers to conduct business across the internet, your doing e-business. This may take many different forms, among the most common being those that involve the use of web applications. These applications may be CGI applications launched by a web browser, Java applets downloaded from web-browsers, standalone Java applications, or other types of programs. These applications can be used to allow customers to order products, to purchase stocks, to pay utility bills, perform on-line banking; the possibilities are many and varied. What they have in common is that they are providing your customers with access to internally stored data and processes. If this access is allowed to occur outside of the strict boundaries that you intend, substantial risk to your company will occur. How can you be sure that this will not happen? How can you mitigate this risk? The Virtual Vault is a Hewlett Packard product that addresses these issues. It supports the most common types of applications that are being used by businesses today to provide internet connectivity to their customers. It is a unique solution in that it brings many layers of security to bear upon this problem. These include a security enhanced version of the HP-UX operating system, Fire-walling, mandatory access control, directory concealment, user authorizations, compartmentalization, and others. This presentation will teach the attendee what the virtual vault is, how it solves the problem of opening up your enterprise to the internet, and how and when it would be appropriate for your organization.



Slide 2 of 45

# Abstract

## Notice

This document was prepared by Stan Zitello for the purpose of a live tutorial to be presented at Interex 2000 in Las Vegas during April, 2000. As such, it does not contain enough information to be accurately interpreted as a standalone document. For technical details regarding the Virtual Vault product, or any other HP products mentioned during the tutorial, please refer to the web site <http://www.docs.hp.com>. If you are interested in attending courses offered by HP Education for the Virtual Vault, or any other HP products mentioned during the tutorial, please refer to the web site <http://education.hp.com>

## Biographical Sketch

Stan Zitello has been in the computer industry for over 20 years, and is presently a Senior Consultant for HP Education. He has been teaching virtual vault seminars since the early days of the vault (1996). For HP Education he teaches a variety of classes, specializing in Security, Network Systems Management (The Openview Family), and Windows NT. He holds a variety of industry certifications including HP's HP-UX System and Network Administration and Microsoft's MCP, MCSE and MCT certifications.



Slide 3 of 45

# Abstract

## Copyright

This document contains proprietary information which is protected by copyright. All rights are reserved. Reproduction, adaptation, or translation without prior written permission is prohibited, except as allowed under the copyright laws.



# Contents

An Intranet Enabled Application  
Adding the Internet  
What is the Virtual Vault?  
Internet Security Goals  
Associated Risks  
Risk Mitigation Strategies  
Risk Mitigation Strategies (continued)  
Virtual Vaults Implementation of Traffic Filtering  
Virtual Vaults Implementation of User Authentication  
Virtual Vaults Implementation of User Authorization  
Virtual Vaults Implementation of User Authorization (contd)  
Virtual Vaults Implementation of Directory Concealment  
Virtual Vaults Implementation of Data Partitioning  
Virtual Vaults Implementation of Data Partitioning (contd)  
Virtual Vaults Implementation of Data Partitioning (contd)  
Virtual Vaults Implementation of Integrity Checking  
Virtual Vaults Implementation of Use of Least Privilege  
Virtual Vaults Implementation of Use of Least Priv. (contd)



Slide 5 of 45

# Contents

Virtual Vaults Implementation of System Surveillance  
Virtual Vaults Implementation of System Surveillance (contd)  
Virtual Vaults Implementation of System Surveillance (contd)  
Virtual Vaults Implementation of System Alarms  
Virtual Vaults Implementation of Simple Security Admin.  
Virtual Vaults Implementation of Simple Security Adm. (contd)  
Virtual Vaults Implementation of Simple Security Adm. (contd)  
Virtual Vaults Implementation of Simple Security Adm. (contd)  
Virtual Vaults Implementation of Simple Security Adm. (contd)  
Virtual Vaults Implementation of Clear Site Security Policy  
The Information Separation Paradox  
Solution: The Trusted Gateway Agent  
Solution: The Cross Boundary IPC Mechanism  
Solution: The Trusted Gateway Proxy  
Solution: The Trusted Gateway Proxy (contd)  
Solution: The Java Servlet Proxy  
Solution: The Java Servlet Proxy (contd)



Slide 6 of 45



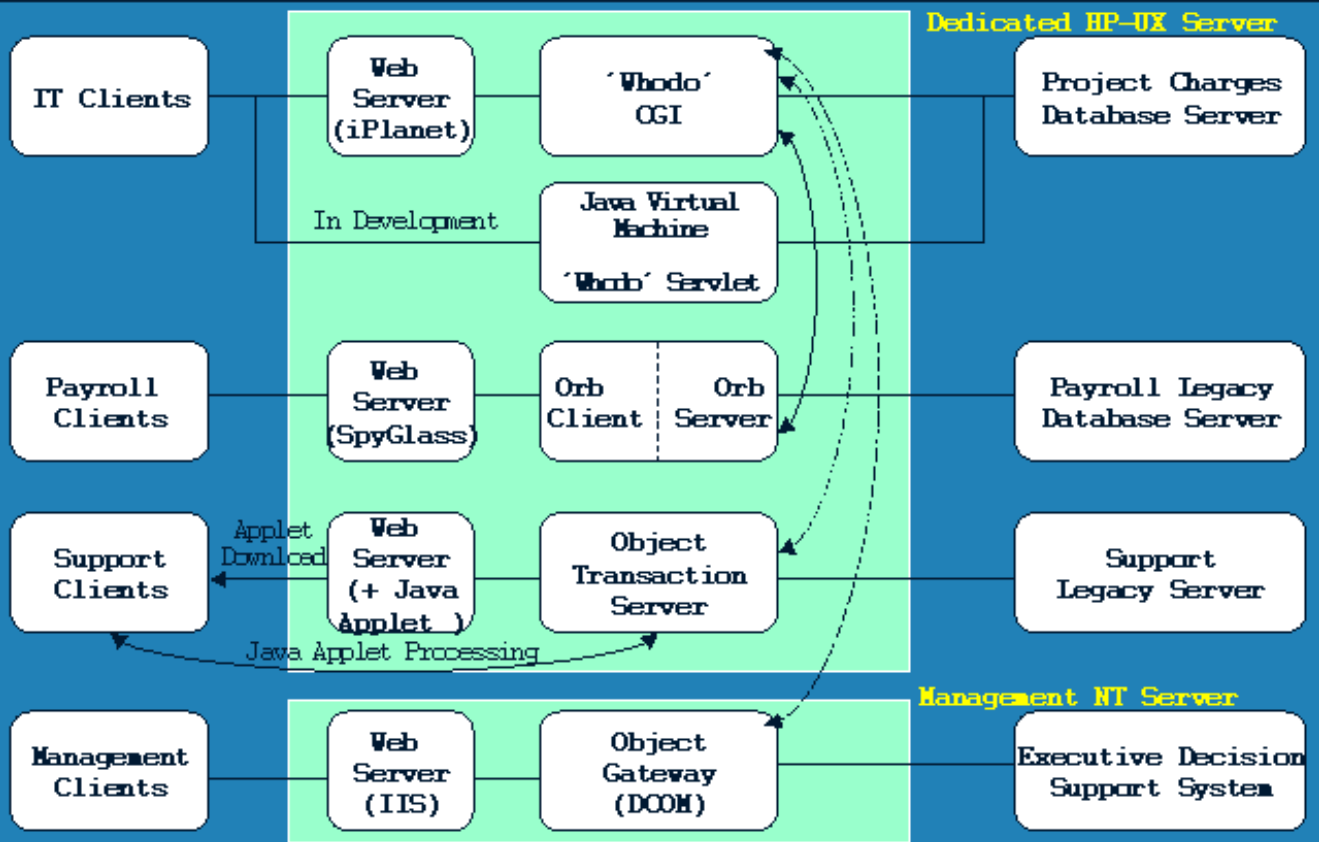
# Contents

Summary 1: Are You a Candidate?  
Summary 2: VV revisited  
Questions & Answers

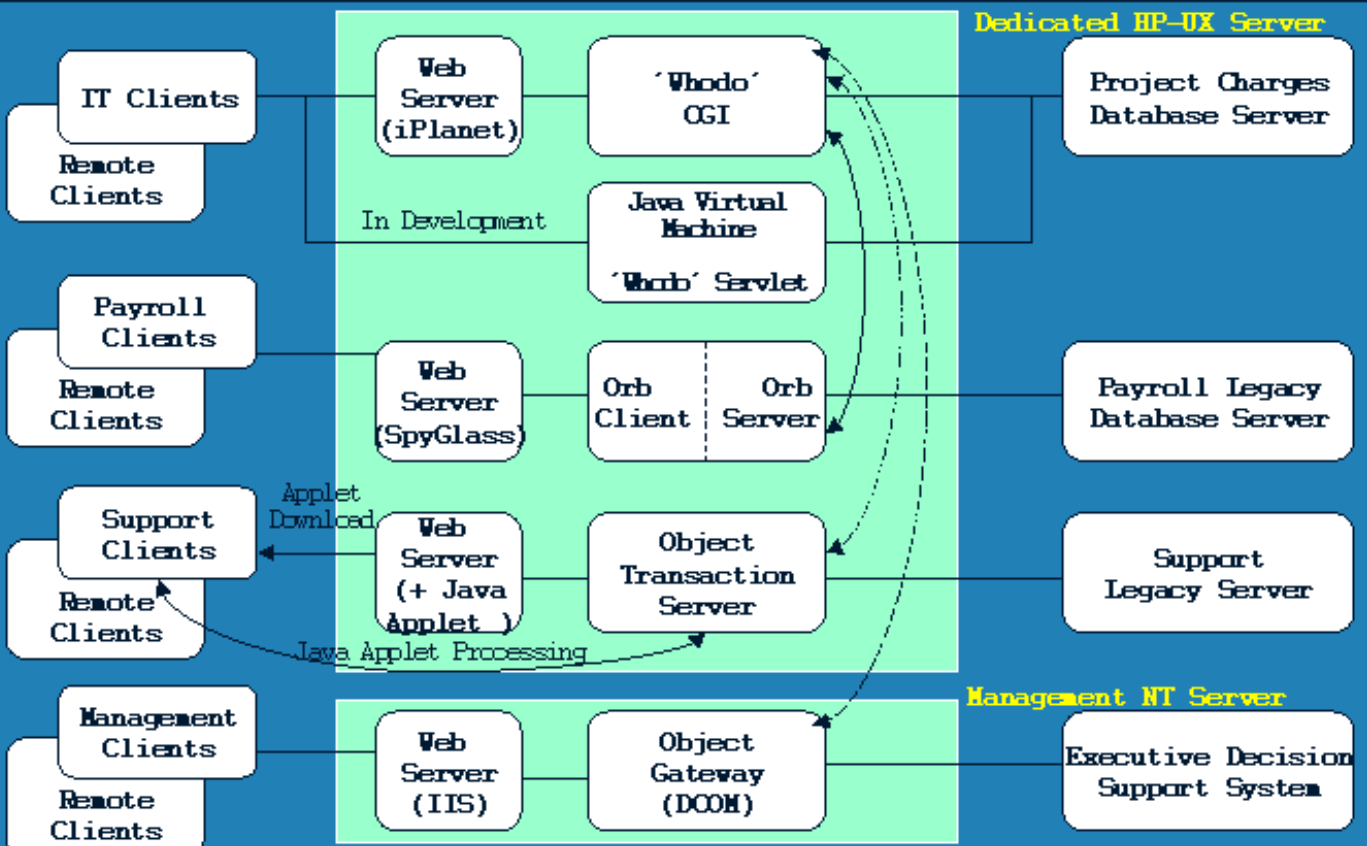


Slide 7 of 45

# An Intranet Enabled Application



# Adding the Internet



# What is the Virtual Vault?

- **A Secure, run-time environment for middle-tier applications. An application 'Front End'.**
- **Runs on "VVOS" - a military-grade security hardened version of HP-UX.**
- **Contains layers of protection to greatly mitigate the security risks of allowing internet connectivity to your enterprise.**



# Internet Security Goals

- **Maintaining Privacy**
- **Maintaining Secrecy**
- **Maintaining Integrity**
- **Maintaining Access to Service**
- **Limiting Abuse**
- **Identifying Problems**
- **Assuring Security**
- **Maintaining Security Policy**



# Associated Risks

- **Maintaining Privacy**
- **Maintaining Secrecy**
- **Maintaining Integrity**
- **Maintaining Access to Service**
- **Limiting Abuse**
- **Identifying Problems**
- **Assuring Security**
- **Maint. Security Policy**
- **Unlawful Disclosure**
- **Industrial Espionage**
- **Destruction of Data**
- **Denial of Service**
- **Misuse of Privilege**
- **Stealth (penetration)**
- **Spoofing**
- **Security Erosion**



# Risk Mitigation Strategies

- ⊗ **Internet Traffic Filtering**
- ⊗ **User Authentication**
- ⊗ **User Authorization**
- ⊗ **Directory Concealment**
- ⊗ **Data Partitioning**
- ⊗ **Integrity Checking**



# Risk Mitigation Strategies

[ continued ]

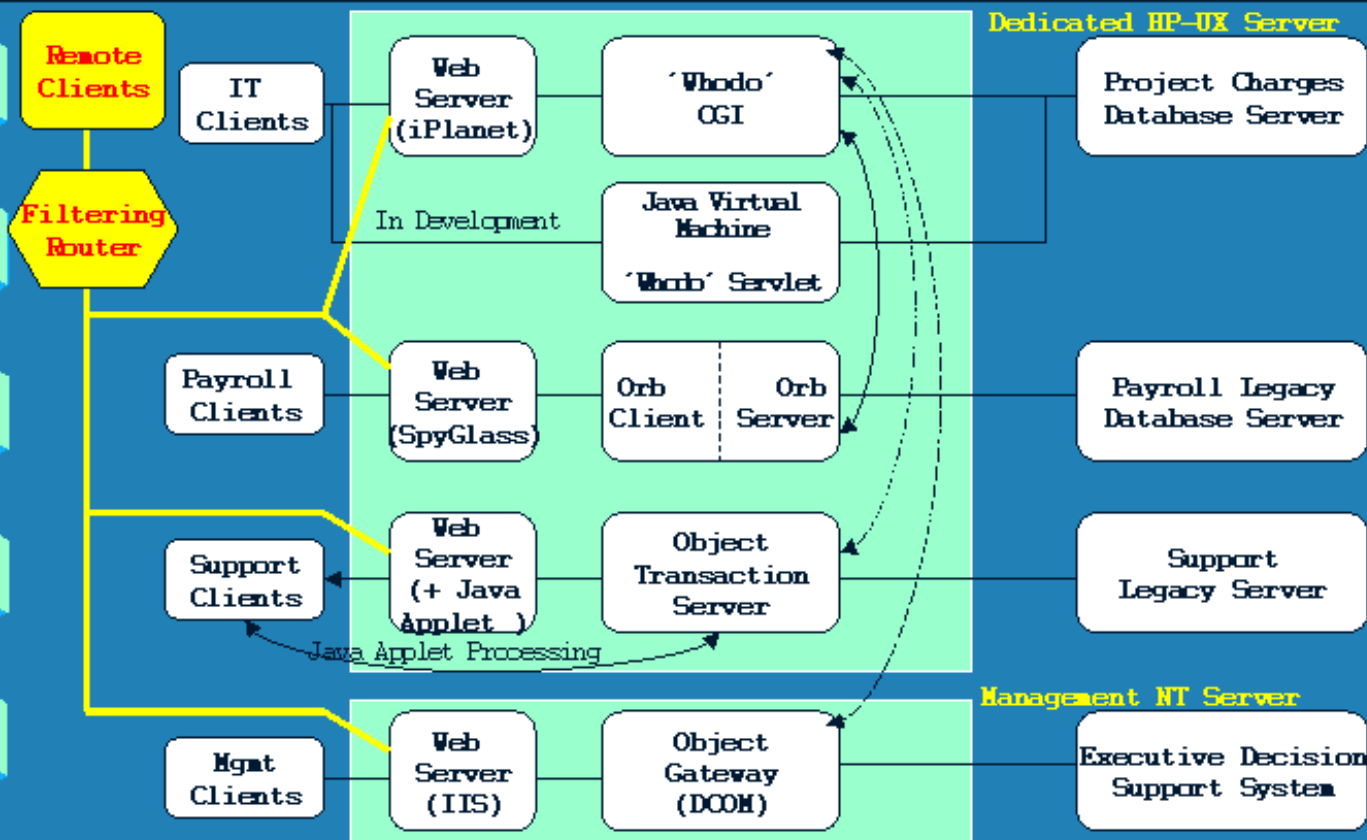
- **Use of Least Privilege**
- **System Surveillance**
- **System Alarms**
- **Simple Security Administration**
- **Clear Site Security Policy**



Slide 14 of 45



# Virtual Vaults Implementation of: Internet Traffic Filtering



# Virtual Vaults Implementation of: User Authentication

- **SSL support within the Web Servers:**
  - Server Certificate to authenticate servers
  - Client Certificates to authenticate users
- **VVOS password features:**
  - Password time limits
  - Clearing from memory of programs requesting clear-text passwords immediately after use
  - Stores encrypted passwords in protected files



Slide 16 of 45

# Virtual Vaults Implementation of: User Authorization

## • **VVOS Access Control Policies**

- **Discretionary Access Control**
  - Real, Effective and Login User IDS
  - Real and Effective Group IDS
- **Mandatory Access Control**

## • **Access Control Lists**

- **Standard**
- **WildCard / Null**



# Virtual Vaults Implementation of: User Authorization

[ continued ]

## • **VVOS Command Authorizations**

- **Distribute the Vaults Administrative Rights**
- **Increased Accountability**
- **Support “Administrative Roles” Definition**
- **Extendable**



Slide 18 of 45

# Virtual Vaults Implementation of: Directory Concealment

## • **CHROOT**

- Alters the “apparent” root directory
- Limits the damage a program can do by hiding the vast majority of system files from it

## • **Web Servers “chroot”**

- Limits damage from unknown exploits or web server malfunction

## • **Application “chroot”**

- Isolate application from server and other apps



# Virtual Vaults Implementation of: Data Partitioning

## • Information Separation from “MAC”

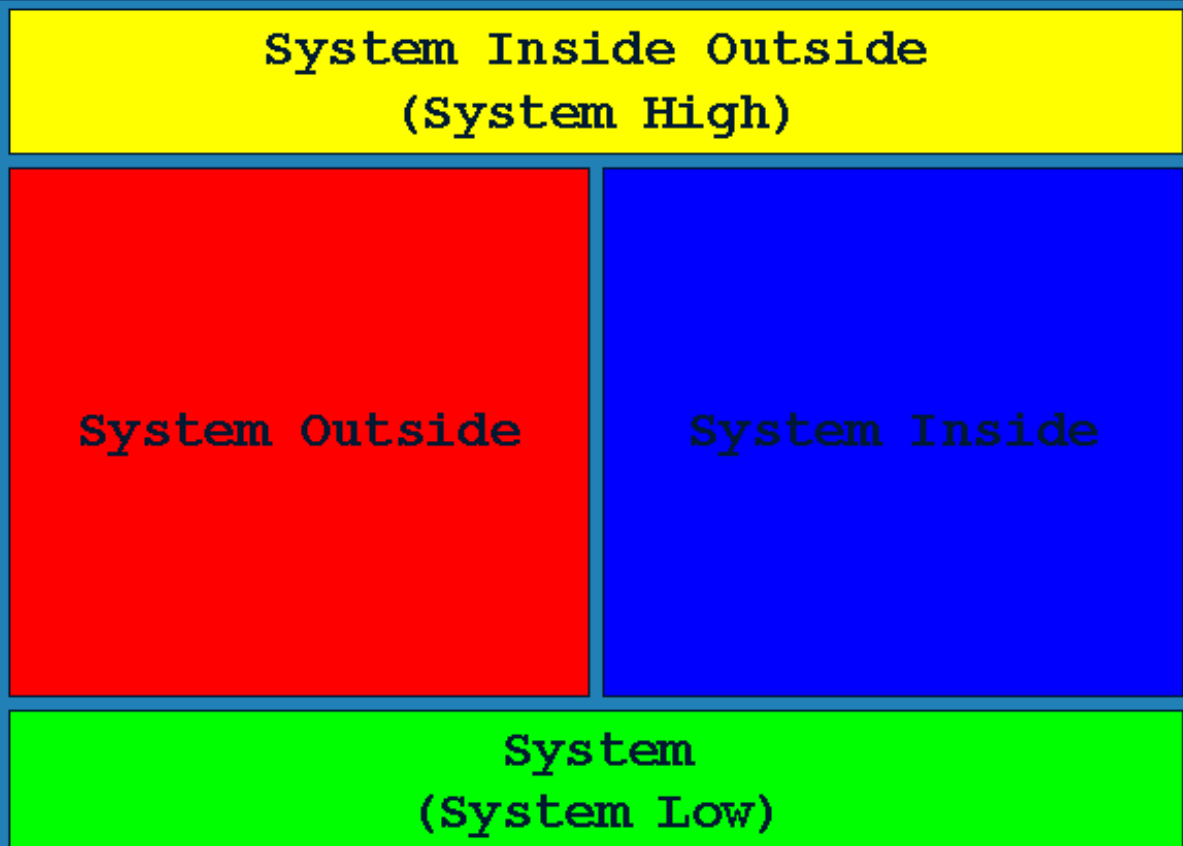
- Separates application processes from system and application files
- Partitions middle-tier app. processes into compartments separated by a strong policy
- Enforcement via the VVOS Kernel
  - Every process and file system object has a mac sensitivity label
  - Communication policy strictly enforced by label:
    - ◆ No Read Up
    - ◆ No Write Down



Slide 20 of 45

# Virtual Vaults Implementation of: Data Partitioning

[ continued ]



# Virtual Vaults Implementation of: Integrity Checking

## • **File Control Databases**

- **Maintain attributes of all critical system files**
- **Maintain attributes of desired application files**
  - Owner, Group, Mode, Size, ACL's, Label, Privileges
  - Can be extended to include checksum and times

## • **Integrity and Setfiles System Utilities**

- **Check and Fix erroneous attributes**
- **Run manually and automatically during boot**



Slide 23 of 45



# Virtual Vaults Implementation of: Use of Least Privilege

- **A process should have no more privilege than is required to perform intended tasks, and for only the minimum required time**
- **VVOS splits up the power of the traditional UNIX super user account into 50 individual privileges**
- **There is no check for UID=0**



Slide 24 of 45

# Virtual Vaults Implementation of: Use of Least Privilege

[ continued ]

- **Privilege “sets” are associated with**
  - **Users**
    - In effect for everything a user does
  - **( Program ) Files**
    - In effect for everyone who executes the program
  - **Processes**
    - The only set checked by the kernel, determines what operations a process will be allowed to do
- **Privileges can be “raised” as needed**
  - **For as little time as needed, only as required**



Slide 25 of 45

# Virtual Vaults Implementation of: System Surveillance

## • **VVOS Audit System**

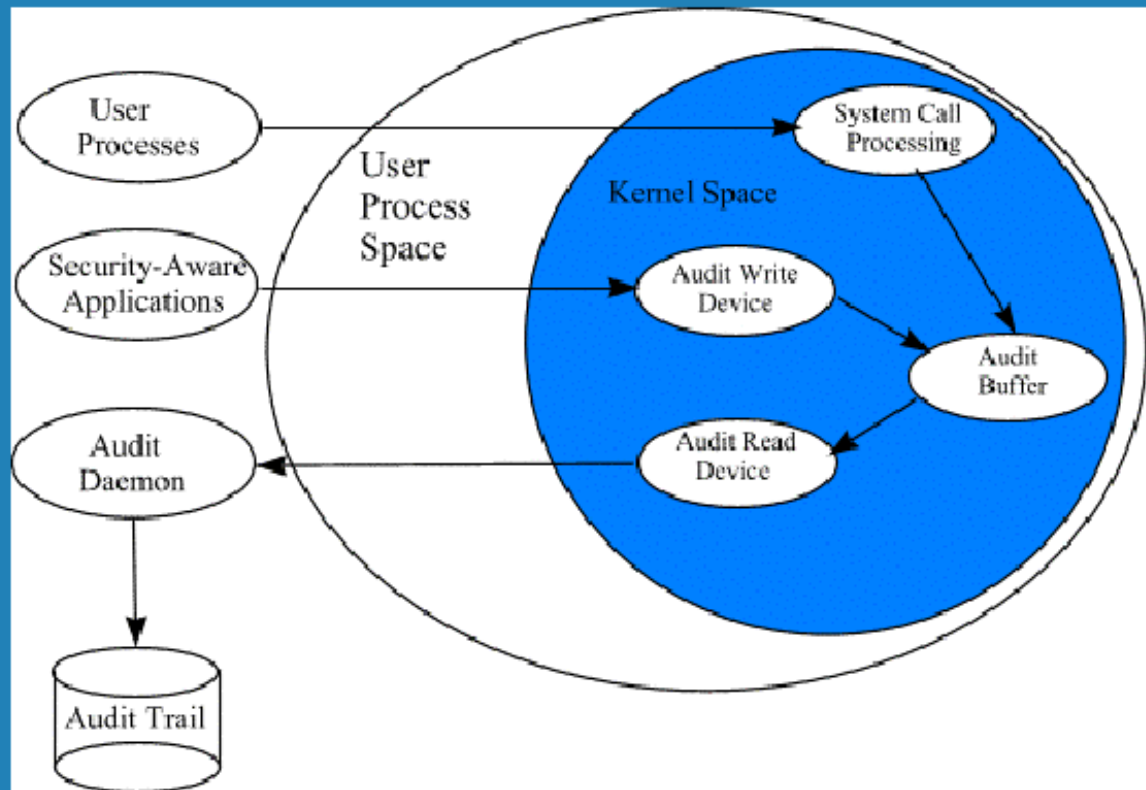
- **Kernel implemented, at the system call level**
- **Customizable by the Audit Administrator**
  - **Type of events to audit**
  - **Size, Location, rollover time of audit files**
  - **Action to take should audit file system fill up**
  - **System Resources consumed by Audit subsystem**
- **Tracks events by Login UserID**
  - **Accurate accountability in Audit Trail**



Slide 26 of 45

# Virtual Vaults Implementation of: System Surveillance

[ continued ]



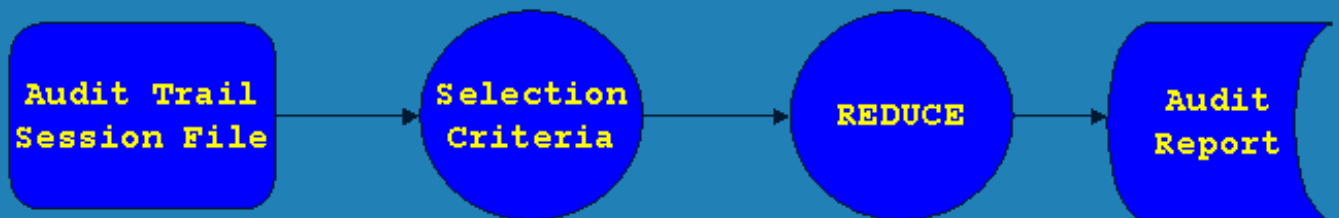
Slide 27 of 45

# Virtual Vaults Implementation of: System Surveillance

[ continued ]

## • “Reduce”

- Audit Reporting Tool
- Allows selection of subset of session data



Slide 28 of 45

# Virtual Vaults Implementation of: System Alarms

## • **VVOS Alarm System**

- **Scans the Audit Trail for “special events”**
  - Events configurable by Name, Time-of-Day, Results, Threshold, Period, Severity and Text Patterns
- **Notification Actions**
  - Log to any file, Email any user, Execute any Command or Send and Alarm to OpenView
- **Protection Actions**
  - Execute any (or no) Command, Shutdown the System, Inside or Outside NW I/F, Outside Web Server



Slide 29 of 45

# Virtual Vaults Implementation of: Simple Security Administration

## • **Out-of-the-Box Security**

- **Preconfigured conservative security stance**
  - Does not require user to
    - Pick an Operating System
    - Disable IP Forwarding or Source Routing
    - Remove Network Services or Unnecessary Accounts
    - Modify Kernel or Application Code
    - Modify Device or other File Attributes
- **Only internet to intranet communication allowed is that expressly supported by user integrated applications**



Slide 30 of 45

# Virtual Vaults Implementation of: Simple Security Admin. [ continued ]

- **Step-by-step instructions for initial configuration and deployment**
- **Web Based Gui for Administrative functions**
  - **Web Server Config, Audit and Alarm Config, Integrity Management, Backup, Restore, etc...**
- **Tools for Integrating applications securely**



Slide 31 of 45



# Virtual Vaults Implementation of: Simple Security Admin. [ continued ]



The image shows a menu screen for VirtualVault. At the top, there are two Hewlett-Packard logos and the VirtualVault logo in the center. Below the logos are four icons representing different sections: a person pointing at a greenboard for 'Getting Started', a red lamp over an open book for 'Documentation', a server rack for 'Administration', and a computer monitor with a mouse for 'Applications'. A horizontal dashed line separates the top two sections from the bottom two. At the bottom of the screen, there is a copyright notice: 'Copyright © 1996, 1997 Hewlett-Packard Company, all rights reserved.'



# Virtual Vaults Implementation of: Simple Security Admin. [ continued ]

**VirtualVault** [Help](#)

### VirtualVault Administration

---

<b>Personal Account Functions</b> <ul style="list-style-type: none"><li><a href="#">Display Account Information</a></li><li><a href="#">Modify Account Preferences</a></li><li><a href="#">Invoke X-Terminal Window</a></li></ul>	<b>Account Administration</b> <ul style="list-style-type: none"><li><a href="#">Create Account</a></li><li><a href="#">Modify Account</a></li><li><a href="#">Retire Account</a></li><li><a href="#">Modify Account Defaults</a></li></ul>
<b>Operator Functions</b> <ul style="list-style-type: none"><li><a href="#">Back Up and Restore Files</a></li><li><a href="#">Verify System Integrity</a></li></ul>	<b>Audit and Alarm Administration</b> <ul style="list-style-type: none"><li><a href="#">Configure Audit and Alarms</a></li><li><a href="#">Generate Reports</a></li><li><a href="#">Manage Audit Sessions</a></li></ul>
<b>System Administration</b> <ul style="list-style-type: none"><li><a href="#">Modify or Display System Defaults</a></li><li><a href="#">Notify or Display Message of the Day</a></li><li><a href="#">Manage Administration Server</a></li><li><a href="#">Set File Attributes</a></li><li><a href="#">Shut Down Entire System</a></li></ul>	<b>VirtualVault Component Administration</b> <ul style="list-style-type: none"><li><a href="#">Message Remoteise Server Administration</a></li></ul>

Go To:

Copyright © 1997, 1998 Hewlett-Packard Company, all rights reserved



# Virtual Vaults Implementation of: Simple Security Admin. [ continued ]

The screenshot shows the VirtualVault Application Integration Tools interface. At the top left is the Hewlett-Packard logo. The title "VirtualVault" is centered at the top, with a help icon (lightbulb) to its right. Below the title is the heading "VirtualVault Application Integration Tools". A section titled "Integrator Tool Selection:" contains a list of tools: "Import Application Files", "Classify Application Files", "Install Application Files", "Configuration File Editor", "chroot() Assistance", and "Miscellaneous Utilities". The "Miscellaneous Utilities" section includes "Device Manager", "Generate MDS Hash for file", "Build System File Control Database", and "Set File Attributes". Below this list is a link "Set Integration Tool Configuration Preferences". At the bottom, there is a "Go To" field with a dropdown menu showing "VirtualVault Application Integration Tools".



Slide 34 of 45

# Virtual Vaults Implementation of: Clear Site Security Policy

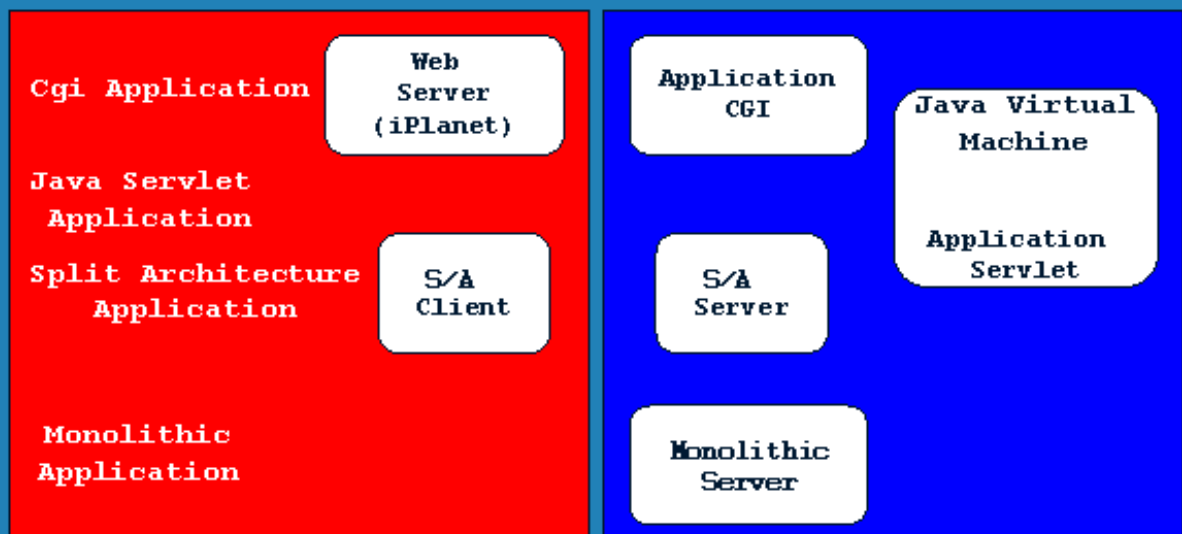
- **The Virtual Vault is part of a Site Security Policy. A policy should include:**
  - **Physical Handling of Media and Hardcopy**
  - **Physical Access Rules and Procedures**
  - **Handling of Emergencies**
  - **Handling of Known or Suspected Penetration Attempts**
- **Establish Your Procedures in Advance!**



Slide 35 of 45

# The Information Separation Paradox

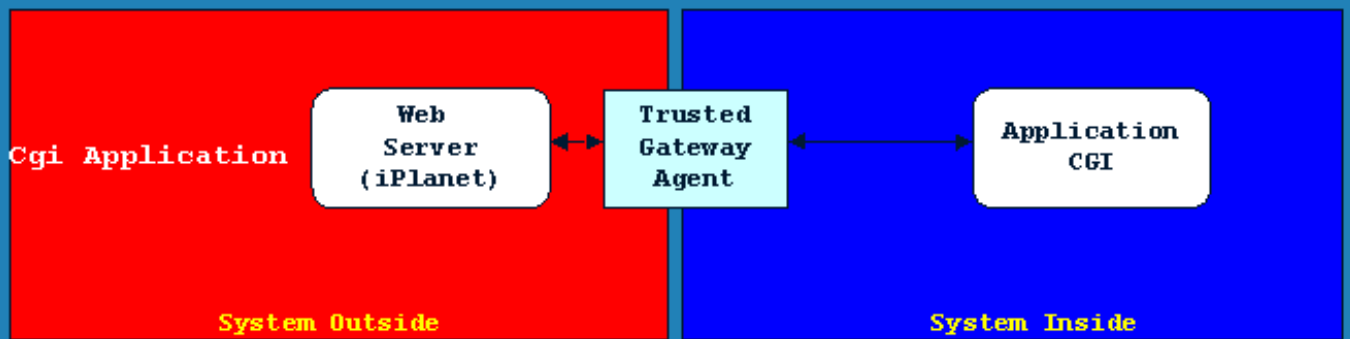
- Separately Compartmented Application Tiers are Necessary for Protection!
- They must, but Can Not Communicate!



# Solution: The Trusted Gateway Agent

## • The Trusted Gateway Agent

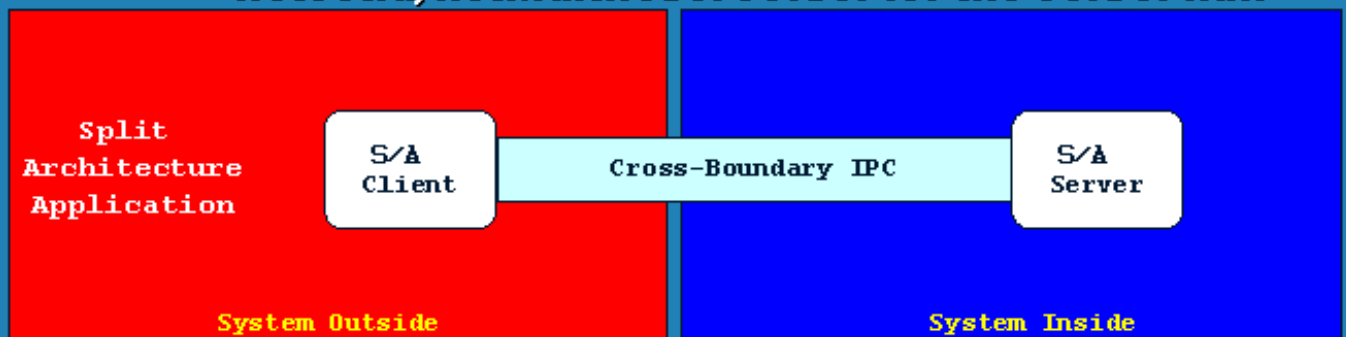
- Provides the needed **Web Server to CGI** Communication Mechanism
- Is the only process trusted to do this task
- Is configured to support only secured Apps



# Solution: The Cross-Boundary IPC Mechanism

## • The Cross-Boundary IPC Mechanism

- Provides the needed **Application to Application** Communication Mechanism
- Is a privilege based mechanism
  - netprivsession for the client half
  - netsetid, netmultilevel server for the server half

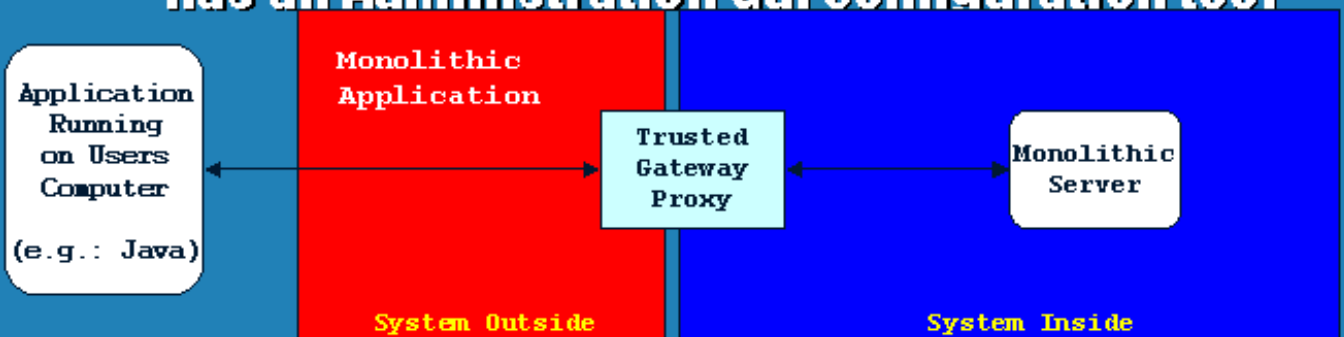


Slide 38 of 45

# Solution: The Trusted Gateway Proxy

## • The Trusted Gateway Proxy

- Provides the needed **"Remote" Application to Monolithic Application** Comm. Mechanism
- Is a privilege based mechanism
  - netprivsession for the inside application
- Has an Administration Gui configuration tool





# Solution: The TGP

[ continued ]

**Configure Trusted Gateway Proxy Ports**

**Create New Service Entry**

Service Name:

Service State:  Enable  Disable

	Address	Port	Sensitivity
Listening Endpoint:	<input type="text" value="0.0.0.0"/>	<input type="text" value="8081"/>	<input type="text" value="SYSTEM INSIDE"/>
Connecting Endpoint:	<input checked="" type="radio"/> <input type="text" value="http"/>	<input type="text" value="8081"/>	<input type="text" value="SYSTEM INSIDE"/>
	<input type="radio"/> <input type="text"/>		

Listen Queue:  connections

End Of Transmission Timeout:  seconds

Audit Inbound Data Offset:  bytes

Audit Inbound Data Length:  bytes

Audit Outbound Data Offset:  bytes

Audit Outbound Data Length:  bytes

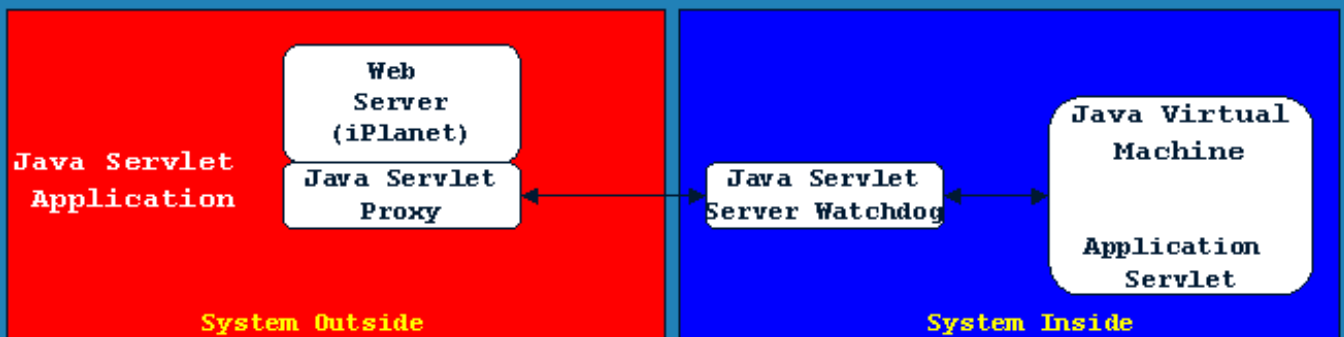


Slide 40 of 45

# Solution: The Java Servlet Proxy

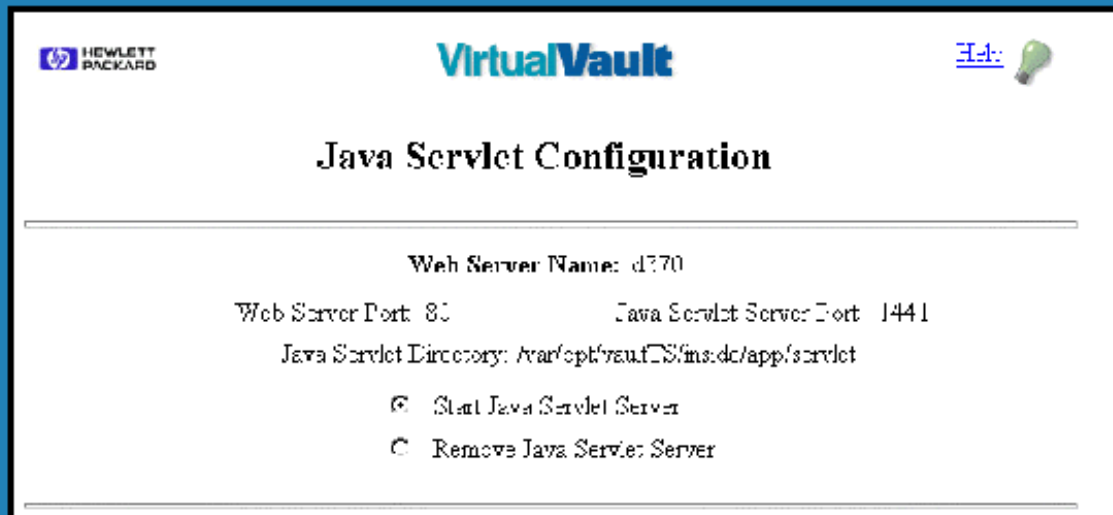
## • The Java Servlet Proxy

- Provides the needed **Web Server to Java Servlet** Communication Mechanism
- Is implemented as an NSAPI module
- Relies on a Privileged Inside “Watchdog” App



# Solution: The Java Servlet Proxy

[ continued ]



The screenshot shows a web interface for configuring a Java Servlet. At the top left is the Hewlett-Packard logo. The title "VirtualVault" is centered at the top, with a help icon (lightbulb) to its right. Below the title is the heading "Java Servlet Configuration". A horizontal line separates the heading from the configuration details. The details include: "Web Server Name: d370", "Web Server Port: 80", "Java Servlet Server Port: 1441", and "Java Servlet Directory: /var/opt/vault/CS/ins.dc/app/servlet". At the bottom, there are two radio buttons: "Start Java Servlet Server" (which is selected) and "Remove Java Servlet Server".



Slide 42 of 45

# Summary 1: Are you a candidate?

- **Do you need to provide Internet to Intranet Connectivity for**
  - **Web Servers with CGI Applications**
  - **Java Applets**
  - **Split Architecture Applications**
  - **Java Servlets**
  - **Other middle-tier applications**
- **Do you need to minimize the chances of and the damages from an Internet attack?**



# Summary 2: VV Definition Revisited

## ⚙ **The Virtual Vault is designed for reality**

- Provides a secure run-time environment for middle-tier applications
- Isolates applications to protect them from attack and to mitigate damage to the system from compromised apps
- Minimized the privilege an attacker can gain if they manage to take over an application
- Reduces config. errors that lead to compromised apps
- If an attacker attempts penetration, an audit trail can capture the effort, and an alarm system can notify the administrator(s) and take automated responses
- Detects integrity problems resulting from unauthorized changes and restores from a known good configuration



# Questions and Answers



Slide 45 of 45