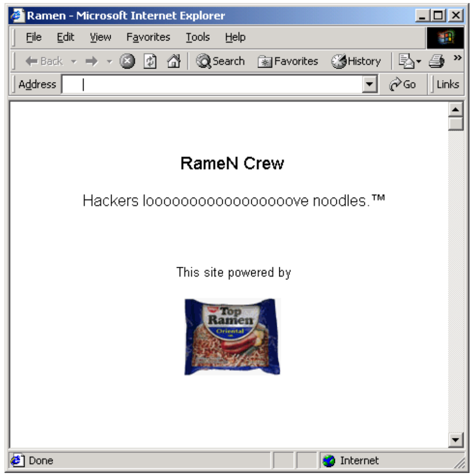
Secure Operating Systems

Practical applications of secure operating systems in E-business

Nigel Edwards
Hewlett-Packard Internet Security Solutions Division
nigel_edwards@hp.com

Secure Operating Systems

Why is security important?


Ramen - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address Go Links
Done
Internet

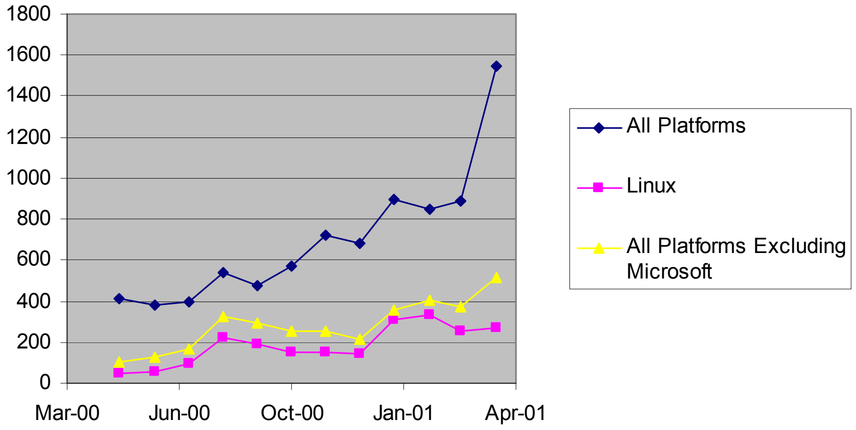
RameN Crew

Hackers looooooooooooooooooove noodles.™

This site powered by

Secure Operating Systems

Web site defacement activity (May 2000 – April 2001)

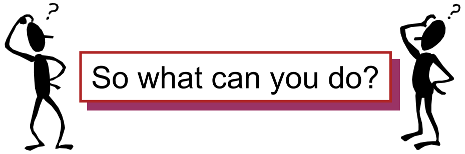


Source: Attrition (http://www.attrition.org/mirror/attrition/os.html)

Secure Operating Systems

Summary of Linux security issues

- In June 2000 Linux was run on 30% of active web sites
  - Source: Netcraft (http://www.netcraft.com/survey/)
- 26.5% of defaced sites ran Linux
- Linux was run on 41.8% of non-Microsoft sites
  - 65.2% of non-Microsoft sites defaced ran Linux
- January 2001 saw the first Linux “Worm” – Ramen
  - Adore and Lion followed
  - Worms may deface your site and/or do other damage

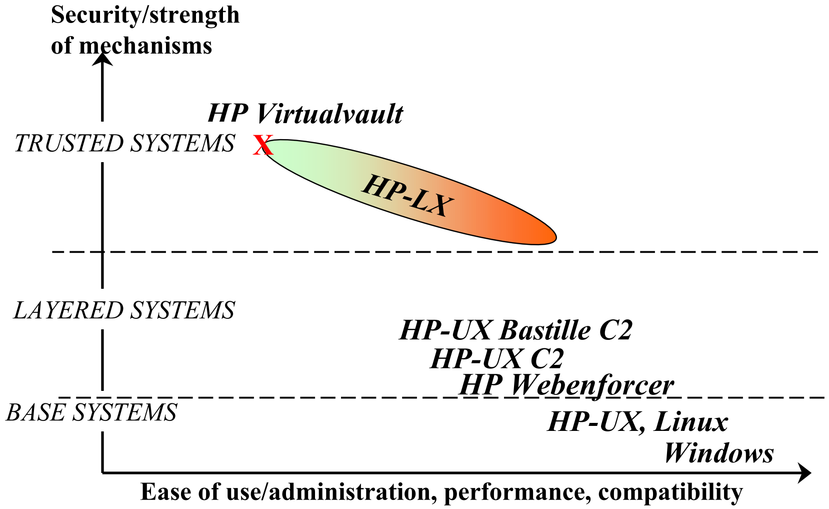


So what can you do?

Possible operating system security strategies

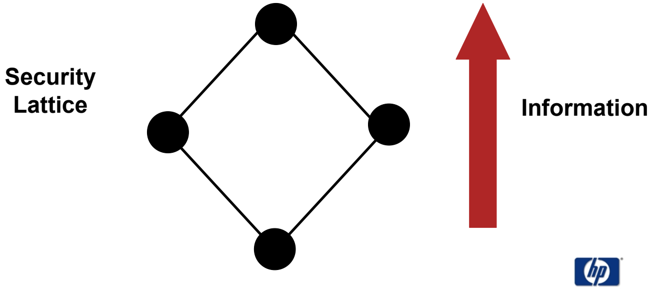
- Wait for the latest patch
  - Will you apply it in time?
  - No protection against administration errors
- Layered security products
  - Minimal protection against attacks exploiting application bugs
- Strengthen the operating system
  - Protects against administration errors
  - Protects and detects attacks exploiting application bugs
  - Enables “safe-sharing” of machines

HP-LX and Virtualvault in context

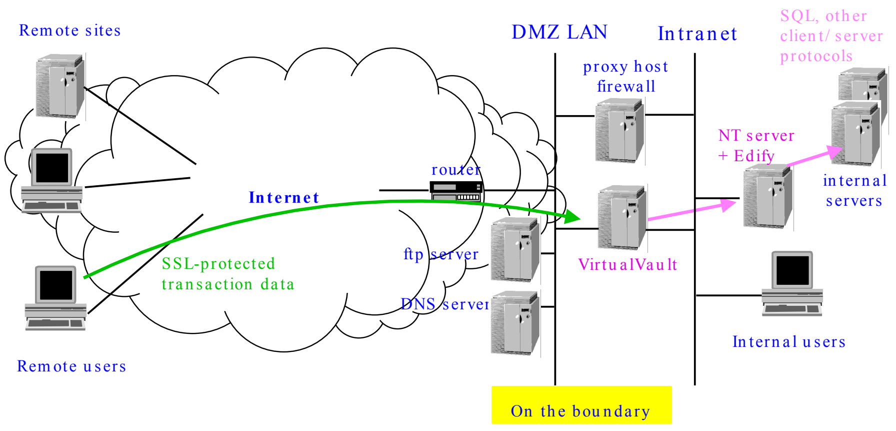


What is HP Virtualvault?

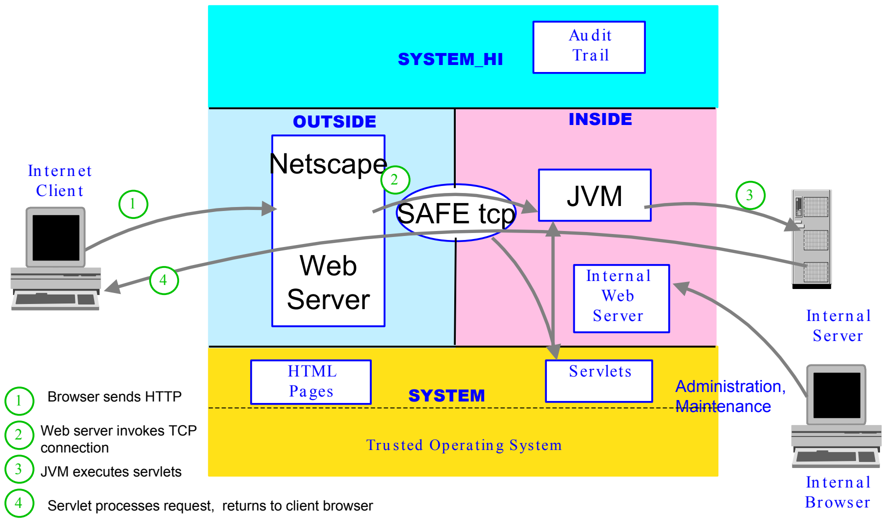
- A highly secure web server
- Six years of installation around the world
- Based on HP-UX Compartmented Mode Workstation
- Implements the Bell and La Padula lattice security model



HP Virtualvault installation



HP Virtualvault internals



1 Browser sends HTTP

2 Web server invokes TCP connection

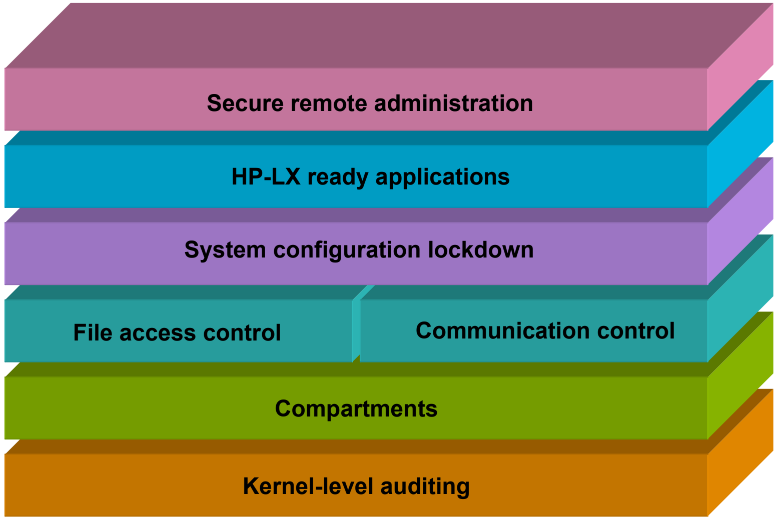
3 JVM executes servlets

4 Servlet processes request, returns to client browser

What is HP-LX?

- A highly secure version of Linux for running applications and services
  - Service provider focus
- Building on the success of HP Virtualvault
  - Balance ease of use with security
  - A new security model focused on Internet services and applications
- Minimal kernel changes
- HP will deliver:
  - Example services (e.g. Apache)
  - SDK and (eventually) integration tools

Review of major HP-LX features



Secure remote administration

HP-LX ready applications

System configuration lockdown

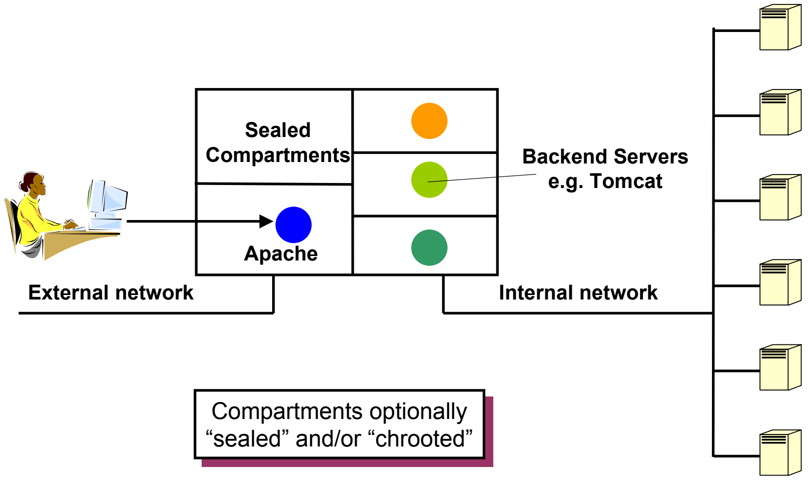
File access control

Communication control

Compartments

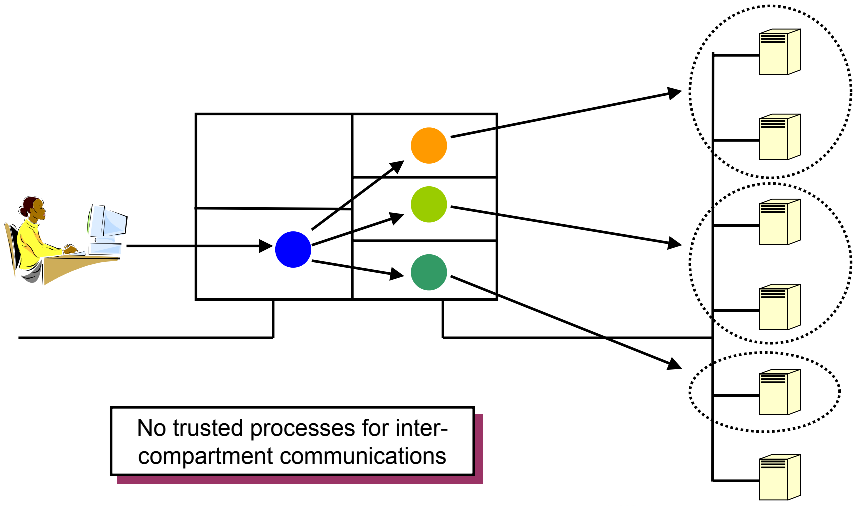
Kernel-level auditing

Compartments



Compartments optionally “sealed” and/or “chrooted”

Communication access control

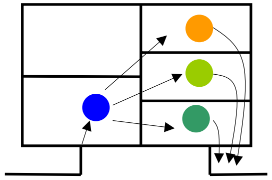


No trusted processes for inter-compartment communications

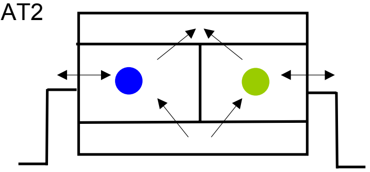
Example of compartment communication rules

```
HOST:* -> COMPARTMENT:WEB
        METHOD TCP PORT 80 NETDEV eth0

COMPARTMENT:WEB -> COMPARTMENT:TOMCAT1
        METHOD TCP PORT 8007 NETDEV lo

COMPARTMENT:WEB -> COMPARTMENT:TOMCAT2
        METHOD TCP PORT 8008 NETDEV lo

COMPARTMENT:TOMCAT1 -> HOST:SERVER1
        METHOD TCP PORT 8080 NETDEV eth1
```

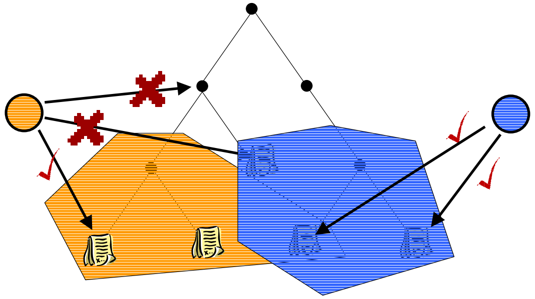
Explicit paths in HP-LX



Implicit paths in Conventional T.O.S.



File access control



- File Control Table specifies: read, write, append
  - Mandatory Access Control (MAC)
  - Prevents web server overwriting the home page
  - Fine-grain control within a sealed compartment
- Coarse grain (MAC) protection also available by using chroot
- Integrity protection
  - Cryptographic hash taken of all immutable files
  - Tripwire

Labels are not used to control access to files
=> No changes to what is written on disk

System configuration lockdown

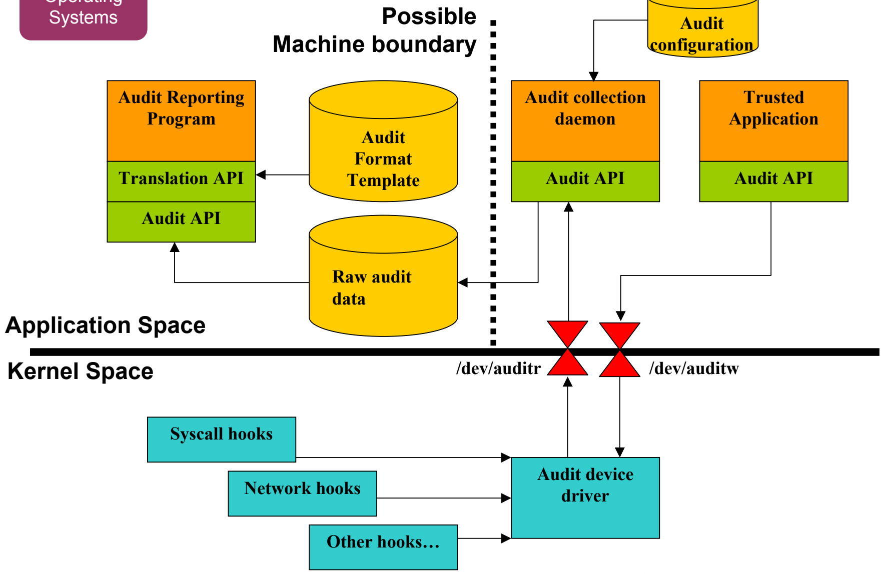
We do:

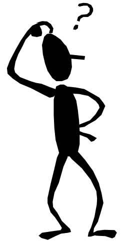
- Removed from sensitive programs Set-UID (and Set-GID)
  - `at`, …
- Enable password aging
- Secure permissions on executables
- Enhance the default system logging
- Etc etc….

We don't:

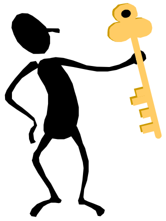
- Remove "unnecessary" programs
  - Ease of use (Diagnosis/maintenance)
  - Anything in Red Hat 7.1 can be installed
  - Rely on containment preventing abuse
  - Use "special" administration compartment

Audit



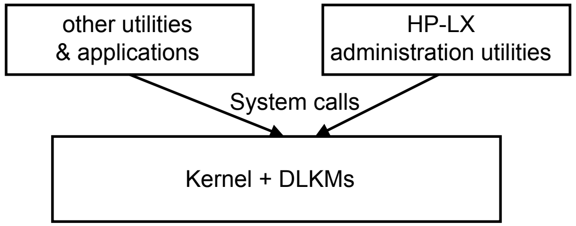


Why is kernel-level Auditing important?



Answer: it is very hard to by-pass

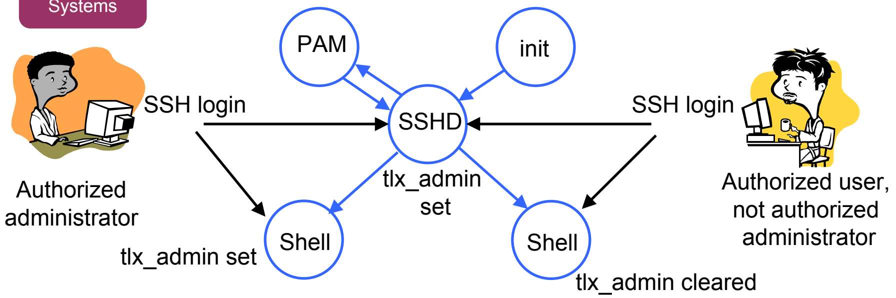
A secure administration model (1/2)



- HP-LX management utilities
  - Create, destroy, start, stop compartments
  - Configure communication rules for compartments
  - Manage audit system

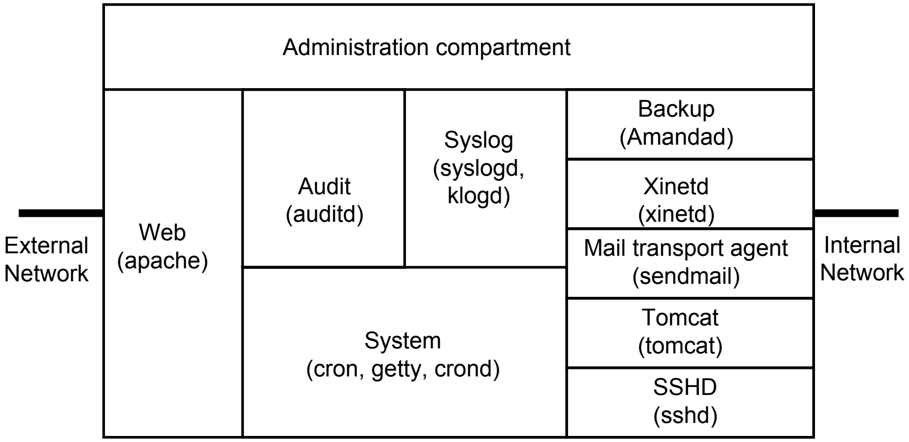
How do we stop the abuse of the system calls used for this?

A secure administration model 2/2



- Each process has an additional attribute
  - The tlx_admin bit
  - Code inside kernel checks for this bit before executing administration functions
- Works in parallel to Linux capability mechanism (which we also use)
  - A more restricted management model than capabilities

Typical HP-LX compartment configuration



Administration compartment

External Network

Web (apache)

Audit (auditd)

Syslog (syslogd, klogd)

System (cron, getty, crond)

Backup (Amandad)

Xinetd (xinetd)

Mail transport agent (sendmail)

Tomcat (tomcat)

SSHD (sshd)

Internal Network

Target platforms and performance

- Which Linux Distributions?
  - Redhat 7.1
  - Will follow up with others including Debian
- Platform
  - Dual processor 700Mhz Pentium III, 2x20GB Disk, 1GB RAM, rack mounted PC (Netserver)
  - Single processor 500 MHZ Pentium III, 10 GB Disk, 500MB Ram
- Performance
  - Currently Apache on HP-LX with auditing-off is within 2% of Apache on Redhat 7.1

Summary

- A new model for trusted operating systems
  - Using our experience of commercial MLS operation
  - Balance ease of use, portability and security
  - Configure communication patterns explicitly
  - Minimal kernel changes
- Main features
  - Compartments provide containment
    - File and communication access control
  - System configuration lockdown
  - Audit
  - Secure administration model

Protects you and your users from many of the most common attacks seen today