Red Hat Enterprise Linux Security

Technical Overview

Customer Perspective

"I am a firm believer in trusting highly deployed open source solutions to be more secure, and more responsive to problems than proprietary solutions. Prior to my arrival, the department and the City of Charlottesville was 100 percent Microsoft. Since then, we began a campaign to increase security, save money and address the needs of management. We chose to standardize on Red Hat as our core open source distribution."

-John Lewis, Security Systems Engineer, City of Charlottesville, VA

Aspects of the Security Problem

- **Security is a *technical issue***—New technology can make systems more impervious to common attacks by default. It can also provide organizations with more control over who can access what.
- **Security is a *human issue***—Compliance and failure to keep systems up to date are a major source of security vulnerabilities. Administrators need help understanding the state of their systems and managing the complexity of securing their network.
- **Security is an *economic issue***—In an interconnected environment, you are only as secure as your neighbor. Access to strong security must be affordable enough to be ubiquitous.

Linux Lowers the Cost of Ubiquitous Security

- Cost should not be a prohibitive factor in providing a secure computing environment.
- Traditionally, proprietary “trusted operating systems” have been priced out of reach for most customers. Red Hat is making secure operating system architectures an affordable, mainstream solution.
- You are only as secure as your neigbor: As affordable, secure solutions scale, the entire internet becomes more safe and reliable.

Red Hat Security Evaluations

- **Evaluated Assurance Level (EAL) 3 (August 2004)**
  Red Hat Enterprise Linux WS on x86
  Red Hat Enterprise Linux AS on x86, Intel Itanium, AMD64, IBM zSeries, iSeries and pSeries
- **Common Operating Environment (COE)**
  Certified by the Defense Information Systems Agency (DISA)
  Red Hat Enterprise Linux AS
  32-bit Architecture
- **Section 508 Compliance**
  Red Hat Enterprise Linux 3 WS/ES/AS

redhat

Better Patching and Management Tools

- Red Hat Network makes system upkeep easier and faster to do—visibility, control and automation. Updates are filtered for relevance to the customer's setup.
- Open and clearly explained patches help customers make more informed decisions.
- Tight integration with hardware and software vendors to provide patches that minimize disruption to customer business processes.
- Backporting of key fixes or features to maintain security of systems without unnecessary or unplanned upgrades.

redhat

redhat

Red Hat GPG Keys

- Red Hat use a number of GNU Privacy Guard (GPG) keys to sign software and to communicate securely. This document is designed to tell you which keys we use for which purposes and how to verify those keys.
- It is a good security practice to validate public keys that you receive and to only trust validated keys.
- The Red Hat secalert@redhat.com public key is available from a number of places:
  * From our web site
  * On a public keyserver, such as pgp.mit.edu
- The fingerprint of the secalert@redhat.com key is
  - 9273 2337 E5AD 3417 5265 64AB 5E54 8083 650D 5882

redhat

Security Policy

- Advance Notification
  - Red Hat does not provide advance notification of private security issues to our partners or customers. We also will not inform our partners or customers that an investigation is underway.
  - For issues that are already in the public domain we may notify our partners, customers, or other organizations about our investigations or response process.

Get Notified of New Security Issues

- Subscribe to the Red Hat watch lists to get new security advisories for Red Hat products sent to you by email:
  - For Red Hat Enterprise Linux advisories subscribe to enterprise-watch-list: enterprise-watch-list
  - For Red Hat products that are Red Hat Network enabled you can also use the Red Hat Network to automatically notify you to applicable alerts
  - A RSS (Really Simple Syndication) feed for Red Hat advisories is also available. To take advantage of this service you need a RSS client pointed to the Red Hat Advisory RSS Feed

Errata Support

- Phase 1: Full Support
  - Start Date: General Availability
  - End Date: 2.5 Years from General Availability date
  - Description: During the Full Support phase, new hardware support will be provided at the discretion of Red Hat via Updates, Additionally, all available and qualified errata will be applied to the Enterprise products via Updates (or as required for Security level errata.)
- Phase 2: Deployment
  - Start Date: General Availability
  - End Date: 3 Years from General Availability date
  - Description: During the Deployment phase, all available and qualified security and bug fix errata will be applied to the Enterprise products via Updates. Security Errata will be released as necessary independent an Update.
- Phase 3: Maintenance
  - Start Date: 3 Years from General Availability (end of Deployment)
  - End Date: 2 Years from end of Deployment (5 years from General Availability)
  - Description: During the Maintenance phase, only Security errata and select mission critical bug fixes will be released for the Enterprise products.

Linux Worms

Name	*Date Found*	*Date Fixed*
Slapper	Sep 2002	July 2002
Adore	Apr 2001	Jan 2001
Lion	Mar 2001	Jan 2001
Ramen	Jan 2001	Sep 2000
Noodle		

Customer Perspective

Defense Information Systems Agency

"Open source allows us the opportunity to have a proactive and pre-emptive identification of security holes by friendly analysis. As a result, this early identification and rapid repair of security vulnerabilities has become a major advantage of open source over proprietary approaches to software development."

-Rob Walker, Program Manager, Defense Information Systems Agency

How well does Red Hat Really Do?

- "Critical" issues
  - 13 CVE named vulnerabilities
  - 77% fixed within a day
  - 1.1 days average
- Also include remote attacks that require user interaction
  - 21 issues
  - 76% fixed within a day
  - 1.4 days average
- Also include those issues like privilege escalation, remote Denial of Service, information leaks
  - 47 total issues
  - 57% had a fix within a day
  - 7 days average

Securing the Enterprise with New Technology

- Next version of Red Hat Enterprise Linux will implement SELinux, an NSA initiative to provide more granular access controls.
- Red Hat contributions to the Linux kernel such as ExecShield and PIE (Position Independent Executables) prevent buffer overflow vulnerabilities—the most common kind of attack.
- Fedora Project provides a proving ground for new technologies and innovations.

Technology and Tools

- Network
  - Firewall (iptables)
  - xinetd (and tcp wrappers)
  - IPSec/VPN
  - SSL/SSH

Technology and Tools

- Data
  - File permissions / ACLs
  - Encrypted filesystems

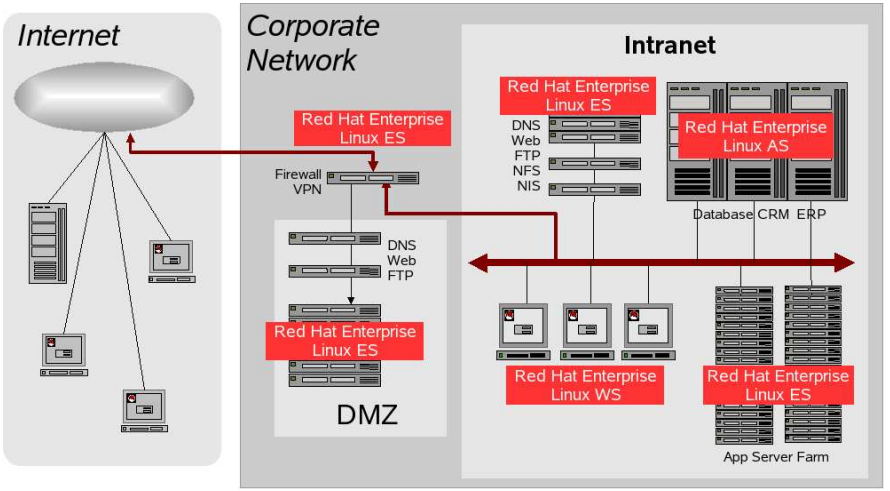
Technology and Tools

- Execution / Exploits
  - PIE, NX, execshield
  - SELinux

Technology and Tools

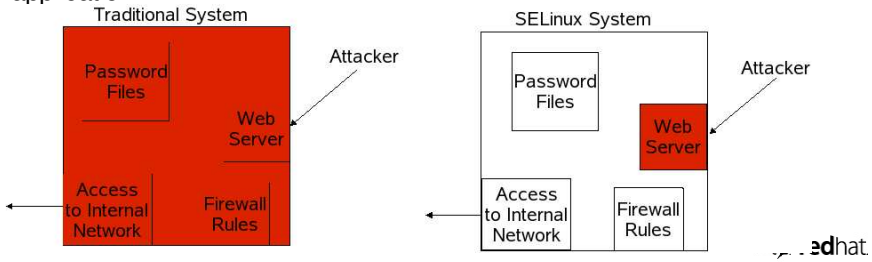
- Auditing
  - Snort
  - Tripwire
  - Logwatch

RHEL Network Configuration



Security Enhanced Linux (SELinux)

- Red Hat Enterprise Linux 4 will include SELinux
  - Leverages 10 years of OS research by the NSA
  - Integrated into standard RHEL versions – full ISV support
  - "Policies" ensure applications have only the minimum access needed
  - Transparent to applications and users – no added administration
  - Role-based access controls available to enhance security
- A successful attack can only use the rights of the compromised application



redhat

Access Control Mechanisms

- **Traditional**
- **Discretionary Method (DAC)**

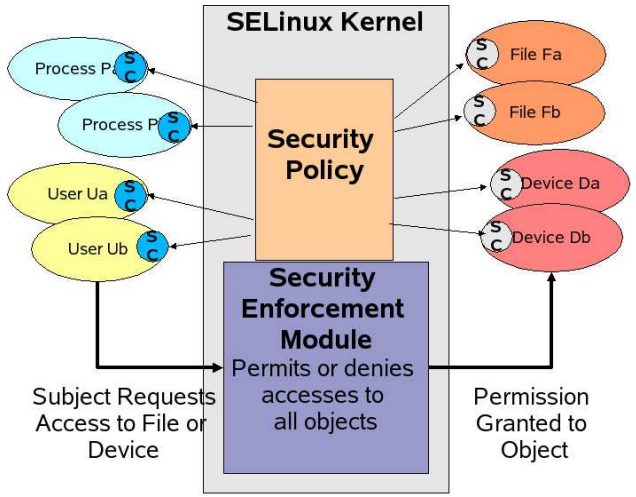
- Traditional OS/Unix mechanism
- Users/programs have complete control
- System security is left to the applications
- Program inherits user's rights
- Root is all powerful
- Any program running as root can be compromised, and therefore the entire system.

- **Trusted Computing**
- **Mandatory Method (MAC)**

- User/Programs has limited privilege
- System and data integrity
- Security policy set by administrator and enforced by the System
- No concept of all powerful root user
- Incorporates program function / trustworthiness into A/C decisions.
- Root compromises confined by policy

redhat

How SELinux Enforces Security Policy



redhat

How SE Linux Enforces Security Policies

- SELinux tags each and every process and file with a security context (SC)
  - Files tagged via extended attributes.
- New files get assigned context via default policy
- Kernel assigns context to processes via policy
- Applications can set the context of files if the policy allows it.
- Applications can exec processes in a specific context if the policy allows it.

redhat

Apache Example

- Apache executable unmodified
- System administrator might have three choices of policy
  - **High** - Apache only can display html pages in /var/www/html
  - **Medium** – Apache can run cgi-scripts in /var/www/cgi-bin
  - **Low** – Apache can display pages in users home directories
- If Apache server compromised with remote shell exploit
- Cracker only has access to files that Apache had access too
- If Apache had read access to /var/www/html that is all cracker can do.

Customer Perspective

Air Force Electronics Systems Command (ESC)

"The Air Force's Electronics Systems Command (ESC) applauds adoption of industry-driven standards. The DoD now can achieve the required level of conformance so vital to joint warfare by embracing the self-governance standards created by the Linux community. This will allow the DoD to remain current with commercial technology innovations while using the self-governance model of the Linux community.

"The [Red Hat Enterprise Linux AS] running on IBM based Intel servers will deliver enterprise capability, proven stability, and flexibility required for C2 systems deployed world-wide In particular the New Tactical Forecast Systems being developed by ESC will be able to field as planned."