RED HAT ENTERPRISE LINUX 5 SECURITY

By Karl Wirth

ABSTRACT

Red Hat® Enterprise Linux® has been designed by, and for, the most security-conscious organizations in the world. Accordingly, security has always been a central focus of the Red Hat Enterprise Linux family. This paper will show how Red Hat has led the way in developing new security technology– making a secure operating system architecture an affordable, mainstream solution. We will discuss how the strength of open source development lowers the cost of security maintenance and how Red Hat continually looks for potential security exposures and delivers tested security updates through Red Hat Network. We will discuss how the company works closely with partners to make sure customers have a choice in building a secure, integrated environment. And finally, we will show how Red Hat has combined these strengths to produce a platform that offers customers world-leading security: Red Hat Enterprise Linux 5.

Innovation, part 1: Red Hat Enterprise Linux 5

Security is not just about technology, but technology is important. The following major technical innovations are built into Red Hat Enterprise Linux 5, delivering real security benefits to customers:

NEW FEATURE	FUNCTION	BENEFIT
Common Criteria EAL 4+ Certification	First OS to ship with native support for functionality necessary to meet Common Criteria for Trusted Operating Systems: EAL 4 CAPP, RBAC, and LSPP.	Provides assurance that platform is designed, reviewed, and tested to the government's most rigorous security standards.
Virtualization	OS level compartmentalization and rapid guest system deployment.	Enables: (i) Application isolation by deploying each on a separate OS, (ii) Rapid deployment of honeypots, (iii) Rapid redeployment of compromised systems.
Expanded SELinux coverage and usability	200+ core system services protected by default via targeted policies. SELinux management tools.	Simplifies process of creating, customizing, managing, and troubleshooting SELinux policy.
Native smart card integration	Leverage smart cards for certificate based login (including kerberos ticket acquisition).	Increased authentication security.
Additional attack protection	Fortify Source on all packages, Stack smashing protection, Pointer encryption, SELinux memory protection.	Additional buffer overflow and memory attack protection.
Enhanced Auditing	Complete, configurable local audit subsystem.	Gives ability to centrally track (on a local system) events from logins to low level system events.

COMMON CRITERIA EAL4+ CERTIFICATION

Enterprise Linux 5 is the first operating system to ship with native support for the functionality necessary to meet Common Criteria for Trusted Operating Systems. This includes all functionality to enable EAL 4+ certification under the following protection profiles: CAPP (Controlled Access Protection Profile), RBAC (Role Based Access Control), and LSPP (Labeled Security Protection Profile).

For customers outside of the government, this provides assurance that the platform is designed, reviewed, and tested to the government's most rigorous security standards.

For government customers required to run Common Criteria for Trusted Operating Systems, Enterprise Linux 5 provides an open source solution that natively supports multi-level security. This is an exciting mainstream option for customers previously forced to depend on high priced, proprietary solutions.

VIRTUALIZATION

Enterprise Linux 5 ships with built-in support for virtualization. Virtualization enables organizations to run multiple applications on one box in such a way that each application has its own OS. This has the benefit of isolating the applications from one another – blocking one problem application from reaching or crashing other applications on the system.

Virtualization also allows IT organizations to much more rapidly add and remove systems to their network. The rapid deployment of honeypots, as well as the rapid redeployment of systems which have become compromised are two examples of the security-enhancing roles that virtualization can play.

EXPANDED SELINUX COVERAGE AND USABILITY

SELinux (Security Enhanced Linux) enables granular policy-based control over programs' access to data and kernel resources, preventing a compromised program from acting outside its policy. SELinux was developed in coordination with the open source community and the National Security Agency (NSA) to provide the highest levels of security for the Linux operating system.

By default, over 200 core system services in Enterprise Linux 5 are protected by targeted policies. This enables organizations to quickly benefit from the security provided by SELinux.

Enterprise Linux 5 also includes enhanced SELinux management tools that simplify the process of creating, customizing, managing, and troubleshooting SELinux policy.

NATIVE SMART CARD INTEGRATION

Customers can increase the level of security used for authentication with Enterprise Linux 5 systems from a one-factor password-based authentication scheme, to two-factor smart card-based authentication. When enabled, the end user inserts their smart card into a smart card reader attached to the system. The end user then authenticates with their PIN and smartcard to gain access.

Once the user authenticates via the Pluggable Authentication Module (PAM), the system can leverage this smart card authentication to generate a Kerberos ticket for the user that enables single-sign on to kerberos-aware applications like SSH, SCP, and Fedora Directory server. Firefox and Thunderbird can use the end-user's certificate to perform SSL client authentication to a web server that supports this. And Red Hat Certificate System can be used to create and manage the end user's certificate.

ADDITIONAL ATTACK PROTECTION

Enterprise Linux 5 includes four major innovations that protect systems against attack, particularly in the area of buffer overflow and other memory-based attacks. These new features are:

- **Fortify Source.** This check is now run on all selected packages. When the compiler knows the size of a buffer, it is possible to ensure the buffer will not overflow.
- **Stack Smashing protection (canary values).** The system will place a canary value at a randomized point above the stack. This canary value is verified during normal operation. If the stack has been smashed, the canary value will have been overwritten, indicating that the stack has indeed been smashed. This method can detect buffer overflows early.
- **Pointer encryption.** Function pointers are encrypted with unique random values. This is intended to detect an overwrite of a pointer in memory, and prevent the subsequent redirect of execution.
- **SELinux memory protection.** This enhancement can prevent any memory that was writable from becoming executable. This prevents an attacker from writing his code into memory and then executing it.

ENHANCED AUDITING

A complete, configurable local audit subsystem is included with Enterprise Linux 5, giving organizations the ability to centrally track (on a local system) events from logins to low-level system events. It includes the ability to audit users, processes, and files as well as search and reporting utilities that quickly see when security events occur. Sample CAPP/LSPP rule sets are included.

Innovation, part II: A history of innovation

Red Hat leads the way in developing new security technology for Linux. Secure operating system architectures are now an affordable, mainstream option. The following chart illustrates some of the technologies included with Enterprise Linux, and the date of their introduction.

SECURITY FEATURES		RED HAT ENTERPRISE LINUX		
		v.3	v.4	v.5
DESCRIPTION	BENEFIT	2003 OCT	2005 FEB	2007 MAR
Make data memory non-executable and program memory non-writable	Prevent certain types of buffer overflow exploits from working as expected	since 2004Sep	Y	Y
Put program code at a different address each time it starts.	All parts of process (heap, stack, data, DSOs) are laid out randomly in the address space	since 2004Sep	Y	Y
Enable randomization of load address of executables	Attackers cannot predict where the application will start, making it very hard to exploit.	since 2004Sep	Y	Y
Cryptographic signing of update RPMs	Prevent installation of fake updates	Y	Y	Y
Cryptographic signing of kernel modules	Detect/prevent installation of fake kernel modules		Y	Y
Special case of ASLR for the vDSO	Same as ASLR but specific to vDSO	no vDSO	Y	Y
Restrict how the kernel memory can be overwritten.	Prevents several rootkits from functioning		Y	Y
Granular policy-based control over program's access to data and the kernel	Prevents compromised program from acting outside its policy		Y	Y
Default enable system with targeted MAC policy -Role Based Access Control and TE	Prevents compromised program from acting outside its policy		Y	Y
By default, check heap memory for corruption and incorrect links	Detect heap corruption early		Y	Y
When the compiler knows the size of a buffer, functions operate on the buffer to make sure it will not overflow	Prevents buffer overflows		Y	Y
	Prevents buffer overflows			Y
Automatically reorganize location of ELF data to be before program data	Prevent .bss and .data overflows from affecting other program data		Y	Y
Verification of randomized canary value indicates if stack has been smashed	Detects buffer overflows early			Y
Encrypt function pointers with unique random values	Detect overwrite of pointer in memory and subsequent redirect of execution			Y
Prevent any memory that was writable from becoming executable.	Prevent attacker writing his code into memory and then executing it			Y
Enable multi layer security polices in SELinux	Implement "need to know" policy			Y

Each of the above listed features is included in Red Hat Enterprise Linux, and contributes to its security. An equally important component of the Red Hat Enterprise Linux security story is that its security mechanisms are open source.

Transparency

The innovations in Enterprise Linux 5 are due in no small part to the power of the open source development model, which combines the input of customers, partners, developers, end-users, and administrators. Features which drive security further into the environment can more quickly and accurately be addressed and developed by harnessing the collective interests of the community.

The availability of the source code for Enterprise Linux makes it a better alternative for creating secure systems than proprietary code. This kind of transparency has many benefits, including:

- **Increased scrutiny.** With many people looking at the code, vulnerabilities can be spotted before they can be used by viruses or worms. Not only are Red Hat engineers constantly working to find potential security issues in the software, but thousands of developers around the world are doing so as well, while looking for ways to improve security even more.
- **Flexibility.** Not only does open source development help fix flaws, but the flexibility of open source allows customers to match security technology to their processes. Security mechanisms are available for everyone to see and understand, allowing customers and partners to extend or enhance security functions to meet their needs.
- **Modularity.** The modular package-based design of Linux makes it easy to identify, resolve, and trace dependencies surrounding security issues – compare this to the monolithic designs of other operating systems, where a single problem can have far-reaching and difficult-to-identify consequences.

Studies, including a recent survey by Evans Data, show that Linux systems have fewer viruses and security breaches than competing operating systems. This higher level of security translates into direct value for customers:

- Less employee downtime from computer viruses and worms
- Secure web sites that are resistant to attacks
- IT budgets can be spent enabling productivity and infrastructure, not defending it

Red Hat also adheres to and promotes several standards meant to increase transparency and tracking of vulnerabilities, including:

- **CVE Compatibility.** Red Hat adheres to the Common Vulnerabilities and Exposures standard, which allows customers to trace a vulnerability through multiple vendors with consistent naming.
- **OVAL Compatibility.** Red Hat helped create--and supports--the Open Vulnerability and Assessment Language patch definitions, providing a machine-readable version of our security advisories.

Vigilance

Red Hat continually looks for potential security exposures, certifies each package, delivers tested security updates through Red Hat Network, and supports our customers through Red Hat services and support.

SECURITY RESPONSE TEAM

Red Hat's Security Response Team provides customers with a single point of contact for expert, integrated responses to emerging security threats. The team constantly tracks and investigates security issues affecting Red Hat customers, providing timely and clearly explained patches designed to help customers evaluate and manage their risk. By leveraging strong relationships with hardware and software vendors, Red Hat optimizes fixes for compatibility and performance across applications and configurations. Backporting of critical security fixes provides organizations with a predictable and stable means of maintaining secure systems on earlier releases of Enterprise Linux--without unnecessary or unplanned upgrades.

To aid in maintaining a secure environment, Red Hat provides a variety of resources, including configuration guides and technology whitepapers. Red Hat security experts and security training are also available.

UPDATE MANAGEMENT

Customers can easily take advantage of the work of the Security Response Team through Red Hat Network. Red Hat Network provides functionality to reduce exposure to exploits, including:

- Tested fixes that are authorized and digitally signed by Red Hat.
- Email notification or automatic updating when fixes are available.
- Customized notifications that address a customer's specific environment.
- Management features that allow customers to easily manage and deploy updates across an entire enterprise.
- The capability to apply updates selectively to different computing groups within an environment.
- The functionality to facilitate internal testing before an update is deployed in an organization.
- Security updates that are checked for over one million dependencies, maintaining the integrity of the customer's systems.

SUPPORT

Red Hat Enterprise Linux allows customers to take advantage of the performance and security of Linux, while receiving the support they need to run their enterprise. Red Hat offers a single point of accountability for the hundreds of open source projects and applications that make up the Enterprise Linux offering. Red Hat's support staff—all of whom are Red Hat Certified Engineers® —are dedicated to helping customers address any issues that arise.

CERTIFICATION

In order to make sure that Enterprise Linux "just works," Red Hat takes extensive measures to ensure the integrity of the products and services they offer. Red Hat developers inspect and test packages to ensure they work as intended, and examine the code for backdoors that could jeopardize the integrity of a customer's network. Then, the software is run through a rigorous quality assurance process.

Inclusiveness

Red Hat works closely with partners to make sure customers have choices when building a secure, integrated environment.

The Open Source Architecture is Red Hat's vision of a standards-based system that allows customers the freedom to choose the components that work best for them. Security is a key part of the Open Source Architecture, enabling integrity across system components.

Red Hat partners provide solutions that complement a secure environment, such as access management, anti-virus, and encryption solutions. Red Hat's close relationship with its partners and Red Hat's solid reputation in the platform community combine to improve the performance and functionality of products delivered by both Red Hat and its partners.

In addition to low vulnerability rates, Red Hat Enterprise Linux has a partner support model that has been built on a collaborative and inclusive philosophy. All community members, customers, hardware, and software partners are part of an ecosystem that identifies security issues--often before they become exploit targets.

Red Hat has partnered with IBM and HP for accreditations such as the Common Criteria EAL4+ CAPP profile Security Evaluation, which certifies that Red Hat Enterprise Linux meets stringent product and process standards for security. These certifications assure government customers that Enterprise Linux meets their requirements for highly secure environments.

Summary

Platform security must be a pervasive and fundamental part of the platform—not just an add-on. It must be continually reviewed and maintained to ensure platform integrity, and organically include the partner ecosystem and the larger platform community. For these reasons, Red Hat Enterprise Linux 5 stands out as a state-of-the-art, industry-leading choice for settings where security really matters.

At Red Hat, the values of innovation, transparency, vigilance and inclusiveness are not mere words, but business processes that combine to produce and maintain the most secure product possible, while also delivering the best value to customers. That's why Red Hat has consistently appeared at or near the top of the CIO Insight Survey for three years in a row.