



# Security in a Networked World

By Mike Ferris, Product Manager, Red Hat Security Solutions

Linux was born in networked world. In fact, its success is due in large part to the collaborative development model that proliferated as the Internet became globally accessible.

Open source development communities evolve with common goals—to innovate the correct solutions to the challenges presented by increasingly complex technical and political demands. This highly collaborative environment—open to all on the Internet—includes a focus on security as part of the development process. As Eric Raymond said in the Cathedral and the Bazaar, the open source process implements a principal that “Given enough eyeballs, all bugs are shallow.” Security “bug” identification and correction is an inherent part of this process.

Open source developers build technologies, and thousands of their peers can scrutinize the source code. As solutions are proposed, they are immediately vetted for technical merit including an analysis of their security capabilities. Just as local neighborhood watch groups grow to include nations and international alliances with the increasing threat of global terrorism, so do the communities of developers continuously evaluating the security of the solutions in the open source community.

Both immediacy and evolution drive this process. As soon as a solution is offered, everyone has the opportunity to review it. There are no market driven deadlines. If a solution is judged to include insufficient security mechanisms, immediate revision is initiated.

Conversely, closed software development models create an environment where a specified group controls the level of security that their solutions provide. This group may include every developer within a large corporation; however, this is still a group continually under the pressures of market and financial requirements. Even the largest corporate environments are beholden to the contemporary desires of stockholders and customers. This conflict may result in the pressure to focus on user features in one release and building security process and mechanisms into future releases. In short, security becomes another feature of proprietary releases rather than an integrated process in the development model.

Proprietary development models will certainly evolve to address the concerns and challenges presented by ever increasing security requirements. However, unlike open source, these models must adapt their core principles to a networked environment. Open source, and those enterprises and vendors which embrace the community development model, become part of an existing, networked security framework and benefit from its evolution and extension.

## **The relevance of security today**

Security in an enterprise environment has now become a top priority for CIOs and CEOs, and is driving fiscal and policy decisions on every corporate board and advisory committee.

Ubiquitous network connectivity is the driving force behind the increasing requirements for security.

With the Internet and communication channels reaching every aspect of our lives, customers continuously demand better access, services, and applications from their providers. The best solutions will be those that provide these networked services in the most secure manner possible.

## **Accessibility**

Mobile devices such as PDAs, wireless Internet access points, and even technologies built to provide increased physical security such as building access scanners all create additional touch points to enterprise environments, and they all must be secured. The challenge for enterprise companies is to provide the most accessible services to their customers yet protect both their own and their customers' intellectual property through a growing maze of connection points. A highly accessible vendor must continually adapt security procedures and technologies to remain as secure as possible. As access to a vendor's products and services increases, so must their vigilance and focus on security.

## **Applications and information aggregation**

Likewise, the increase in customer services, such as online self-service account information, creates an environment where the enterprise must not only protect their internal networks from rogue users but also protect the growing information about customers and partners, which has become a focal point of security. Storage is increasingly inexpensive, and enterprise companies continually grow the information they store about customers to provide better services. Yet this information must be protected and retained only by those authorized under security policies that the enterprise creates and to which customers agree.

Privacy rights, industry and government regulatory requirements, phishing, and fraud all drive the corporate decision makers to focus on security as a vital component of their businesses. Security is no longer about merely providing a locked-down, firewalled environment. Security is now in the domain of bringing an enterprise company's community of users together under a security framework which continually evolves to meet ever-changing environmental, business, regulatory, and privacy requirements.

## The Red Hat approach

In the tradition of the open source development model, Red Hat approaches security as part of every aspect of technology and service development. At the core, this includes working with the open source community to identify and build the “correct” solutions to security issues. Red Hat focuses on four key areas in this arena: technology, services, content, and process.

### Technology

- **Security is not passive**—Red Hat builds security into every aspect of our product development and evolution. Our engineering and product management teams work with the community, customers, and partners to ensure that if and when issues arise that we have the correct technologies available as quickly as possible for everyone.
- **Entrenched in the platform**—Red Hat coordinates with the open source development communities to create new technologies which address security within the solutions themselves rather than providing extra products which must be purchased to protect inherently insecure technologies. Security-Enhanced Linux, ExecShield, PIE, and recent gcc and glibc extensions are prime examples of communities and Red Hat working together to build security into the platform.
- **Consistency across all networked devices**—Red Hat remains focused on building a flexible, modular, enterprise computing platform whose security infrastructure can be leveraged in every aspect of a corporate network. From mainframe to desktops, from databases to devices Red Hat builds technologies which can be used as part of an extended, protected network.
- **Scalable security management**—Growing from hundreds to tens of thousands of connected platforms requires a focus on security to maintain a consistent, protected environment. Red Hat invests heavily in the management of these highly scaled environments—offering solutions to better manage heterogeneous systems, users, and applications as enterprise deployment complexities continue to grow.
- **Focus on compliance and standards**—As our customers must focus on compliance and certifications, our technologies must comply with both industry and government security standards to meet the ever-increasing demands on security ecosystems. By leading the open source community in meeting key certification standards such as Common Criteria and security components within the Federal Information Processing Standard, Red Hat brings the value of the highest degree of government security requirements to all our customers.

### Services

- **Invest in the customer**—By providing the industry-leading certifications with a training curriculum which integrates security technologies and processes, Red Hat is committed to building an extended community of innovators collaborating to maintain the security of our customers. Self-sufficiency is a key goal and having highly qualified customers who can configure and maintain security infrastructures builds additional value into both Red Hat solutions as well as the extended community.
- **Assist and extend**—Red Hat and our partners’ service organizations provide key security assessments, penetration testing, design, configuration and implementation, and policy development services to ensure an integrated, aggressive approach to the security of our customers’ deployments.

- **Secure delivery of our offerings**—In a networked world, security is also about trust, including trust that the software that you receive from Red Hat is authentic. To ease not only the management of secure environments but also the delivery of software to customers through protected mechanisms Red Hat developed Red Hat Network. Red Hat Network provides a cryptographically signed and secure software delivery mechanism to your enterprise as well as offering proactive notification of updates for issues as they arise.
- **Service the secure deployment**—Even the most secure offering can be reconfigured into an insecure link in an otherwise secure environment. To assist, our highly-trained Red Hat support team can work with customers to ensure that deployments meet the flexibility required within the secure requirements of every networked organization.

## Content

- **Subscription services for continuous security**—Any deployment of software or hardware can be vulnerable, and as such Red Hat views our customers' deployments not as deployed products but as services which must be constantly maintained with the highest degree of security and updates possible. All Red Hat solutions are offered as subscriptions not licenses, emphasizing and encouraging a continuous relationship with our customers.
- **Content across all environments**—The proliferation of the networked environment has created a vast array of information stored across heterogeneous platforms. Red Hat is committed to providing information about those networks, systems, applications, and data in a form that can easily be reported, managed, and controlled to ensure the security of the entire environment, not just Red Hat solutions.

## Policy and process

- **Commitment to open source**
  - Red Hat is committed to working with the open source development community on every technology our customers deploy, investing in the continuous evolution of security as part of the open source process.
  - Red Hat adapts technologies to the open source development model to ensure that they are part of the continuous improvement of not only our products and services but even those of our open source competitors because security is not proprietary.
- **Security response center**—Security is a top priority for all our employees from engineering to customer service representatives, and we have extended this process to work with the leading security organizations to ensure that our Security Response Team remains constantly aware of impending vulnerabilities and that we have appropriate ranking, responsive notification, and rapid updates for customers and the open source community as security issues occur.
- **Meeting security concerns with our partners**—A large component of the success of Linux has been the open paths of communication among multiple vendors. Red Hat constantly works with an extended ecosystem of partners to ensure immediate, clear, and consistent communication as well as testing and certification paths in the event of any security concern with either our or our partners' technologies.

## Red Hat security solutions

Red Hat is the leading provider of security solutions to the enterprise today. Over the past five years Red Hat has made significant investment and prioritized security as the top consideration in the development of Red Hat® Enterprise Linux®. We continue to extend this investment with additional offerings, services and the integration of features and capabilities across our entire set of solutions to provide flexible security infrastructures.

### What's new

- Red Hat Network Monitoring module
- Integration of Red Hat Certificate System
- Build out of Certificate System Ecosystem: integration of libraries with Mozilla, Firefox, and Apache for network-wide user and data protection

### I. Red Hat Network

- Red Hat Network was built alongside Red Hat Enterprise Linux to ensure that enterprise customers would have a management tool to update and secure thousands of systems while keeping costs down. Additionally, Red Hat Network provides immediate notification when updates to address vulnerabilities are available.
- Since its inception, Red Hat Network has been implemented to provide a secure and trusted end-to-end delivery mechanism to protect even the most tightly secured environments. Red Hat Network Satellite is a widely-used solution that allows customers to keep vital information behind company firewalls while not comprising the ability to quickly and efficiently update thousands of systems at once.
- Recently, Red Hat announced the next step in Red Hat Network protection: Monitoring. With the Red Hat Network Monitoring module, customers can monitor systems, network functionality, and applications.
- Red Hat Network provides updates across the entire Open Source Architecture—a single way to receive notification of issues, a single way to get updates across everything we do, from the OS to the applications.

### II. Red Hat GFS

- Red Hat Global File System was added to the solutions portfolio to provide customers with a networked storage solution.
- GFS provides customers with simple storage management, making storage appear as one networked storage solution.
- Red Hat GFS protects the data in an enterprise by simplifying management and consistency of access to key data resources. Customer information can be centrally available to authorized users within an organization, reducing data replication and potential loss.

### III. Red Hat Enterprise Linux with SELinux

- Red Hat worked with the NSA to develop Security-Enhanced Linux (SELinux) to provide the highest levels of security available in any operating system.
- SELinux provides a Mandatory Access Controlled (MAC) infrastructure that complements the existing Discretionary Access Control security features provided by the standard Linux environment. In a MAC-based environment, application capabilities and privileges are set by predefined policies and enforced by the kernel. This prevents errant applications from compromising system security.

- Red Hat Enterprise Linux was the first enterprise operating system to include SELinux turned on by default to protect all users for ultimate system, application, and data protection.
- Red Hat is working with key software and service solution providers to extend the capabilities of SELinux to provide even more compartmentalized security capabilities. By segmenting the resources, applications, and data which a desktop user can access, Red Hat will provide solutions for high-security and privacy-sensitive environments whether driven by government or commercial requirements.

#### **IV. Red Hat Directory Server**

- User identity is a central component of any security infrastructure. Red Hat's security focus evolved from an operating system to a networked infrastructure solution, extended by the introduction of Red Hat Directory Server as the scalable identity solution for organizations both large and small.
- Red Hat acquired the widely-used Netscape Directory Server technology in 2004 then released it under the GPL in June 2005 to build a broad community for the further development of this enterprise-class technology.
- Red Hat Directory Server centralizes application settings, user profiles, group data, policies, and access control information into an operating system-independent, network-based registry.
- Forming the central repository for an identity management infrastructure, Red Hat Directory Server improves security by storing policies and access control information. Red Hat Directory Server creates a single authentication source across an entire enterprise for both intranet and extranet applications.

#### **V. Red Hat Certificate System**

- Authentication of users, devices, and applications is an extended mechanism to ensure that your environment is accessible only by trusted users and resources in a networked environment. Red Hat Certificate System is the leading authentication system for ensuring that customers have the confidence that everyone and everything accessing their network is a trusted entity.
- Red Hat is now taking the next step in enterprise security by officially launching a smart card management system and an integrated component of Red Hat Certificate System.
  - Certificate System was acquired with Netscape enterprise assets in 2004. Today, Red Hat is extending its capabilities to include automatic authentication across multiple client platforms.
  - Red Hat has worked with the Mozilla Foundation to include libraries for smart card detection with versions of Mozilla and the upcoming Firefox 1.1.
- Red Hat Certificate System utilizes the open source Network Security Services (NSS) libraries, technology that has received Federal Information Processing Standards (FIPS) certification. Renewed certification for new requirements and releases of our key technologies are planned for the near future.
- Additionally we are working with key partners and customers to enable end-to-end solutions government compliance with the FIPS 201 in response to Homeland Security Presidential Directive 12.
  - The directive mandates that all federal agencies standardize on one security identification with a smart card chip. Red Hat Certificate System today provides the ability for government entities to meet these requirements.

## Future

Where is Red Hat working to take security in the future? Working with the open source community, we are driving standards-based security process for the networked enterprise.

Ultimately Red Hat sees security as a proactive environment composed on integrated yet open technologies, services, content, and process built around a community of users where security communication and corrective actions are part of every aspect of delivery. This is the evolution of the open source community building security into the process, rather than an after-thought.

As evidenced by our strong commitment to the open source model and customer service, there are many capabilities evolving in the open source development model today that will address security in a proactive mode rather than reactive.

The networked world is here, and security requirements have never been greater. With the proactive, integrated approach to security embedded in the open source development model, Red Hat's focus on driving security consistently through innovative technology, services, content, and policies, we strongly believe that the immense complexities of security in a networked world will be addressed and vendors will be able to refocus their effort on delivering what every customer expects, increased value.

**For more information, visit <http://www.redhat.com> or call 866-2-REDHAT.**