IBM is a leader in Linux security

Imagine: You've managed to maintain an incident-free security history. Your confidence is at an all-time high, and the possibility of an attack on your system seems remote. To argue for stronger security measures is a "negative case" scenario, since the logic of security is only ever proven in the aftermath of an attack.

Many assume that outside infections like viruses, trojans, and worms, or eavesdropping through IP spoofing, phishing, and pharming, pose the worst risks to information security. But the doorway to systems security is often left open from the inside through poorly-programmed or misconfigured software, or by weak passwords or sloppy system administration. These factors can be exploited by anyone from "script kiddies" pursuing a personal challenge to serious thieves targeting the confidential data that assures your corporate market advantage.

Fundamental features of Linux® can help mitigate security threats — the broad development base and rapid patching of Open Source, integrated auditing and encryption features — and there is a virtually non-existent history of Linux-targeted virus attacks. However, these advantages alone provide no guarantee against the ingenuity of malicious intent.

Linux lays a secure foundation

Linux-based platforms leverage numerous built-in security features:

- The *Principle of Least Privilege*, which provides applications and users only as much access to system resources as they require.
- Built-in static and runtime buffer overflow protection that blocks security exploits and preserves system integrity for compilers, applications, and the kernel.
- Mandatory Access Control, which uses granular authorization rules to enforce system-wide security policies on all applications.
- Integrated block device and file system layer encryption that protects data confidentiality when media is lost or stolen.
- Fewer defects per lines of code than proprietary products, per independent confirmation.

IBM offers expert Linux security support

In 1999, IBM® established the Linux Technology Center (LTC) with four goals for Linux community participation:

- Make Linux better.
- Expand the Linux reach for new workloads.
- Enable IBM products to operate with Linux.
- Increase collaboration with customers to innovate beyond what IBM can do by itself.

IBM has provided more than 600 developers to over one hundred Open Source projects and remains one of the top commercial contributors to the enablement of Linux as an enterprise platform.

The LTC Security Team works to apply these goals by integrating security features and design principles into the Linux kernel, file systems, networking, and hardware. By leveraging both broad and deep experience in systems design and development, LTC security professionals help ensure Linux is secure enough for our clients' business-critical workloads.

But security goes beyond sound design and development practices. The LTC security team studies the exploitability of system processes, seeking ways to bypass, attack, or break components. With this knowledge, they make improvements to eliminate vulnerabilities, focusing on detection, protection, and prevention.

Building a base through security standards

IBM's leadership in security starts with fundamental assumptions about the importance of security standards. The Common Criteria for Information Technology Security Evaluation (CC) is an international standard that measures the function, structure, method, and design of an IT product's security. In order to certify at one of CC's standard Evaluated Assurance Levels (EAL1 to EAL7), the product must qualify to the security objectives and requirements of a corresponding protection profile specification that is implementation-independent.

The LTC worked collaboratively to obtain EAL certification of Linux at a time when some industry experts speculated that CC certification might be hindered by a perceived lack of developmental structure. In open-community style, IBM led an alliance of more than 60 business peers, customers, and other members who represented at least 15 contributing organizations. This community developed vital CC resources — the security target, high level design, functional specification, and test cases — required for a satisfactory documentation of the Linux development process.

In 2003, IBM achieved the first ever Common Criteria certification of a Linux distribution. This certification represented a win for IBM, its Linux distribution partners, other peer community members, and customers. The LTC continues to help obtain and maintain Common Criteria certifications that enable the U.S. Government to invest in economically sound Linux solutions on secure IBM products. (For more information, see *IBM leads Common Criteria Linux security certifications* below.) When using the same IBM products, customers from other industries join the government sector in leveraging the benefits assured by this internationally recognized security standard.

IBM leads Common Criteria Linux security certifications

IBM has led the pursuit of Common Criteria certification for Linux. Using multiple protection profiles, including the Controlled Access Protection Profile (CAPP) and Labeled Security Protection Profile (LSPP), LTC-guided teams have documented the security-rich Linux development process for levels EAL2, EAL3, and EAL4.

IBM has:

- Elevated IBM products to first in class among competitors to gain EAL certification for Linux distributions.
- Set the precedent and trend among other enterprise participants in the community toward certification.
- Led the way to making Linux the most Common Criteria certified operating system in the world.
- Enabled the U.S. Government to invest in economically-sound Linux solutions on secure IBM products.

CERTIFIED	LINUX DISTRIBUTION	PROTECTION PROFILES	LEVEL
Aug 2004	RHEL[1] 3 U2 AS and WS	CAPP	EAL3+
Jan 2006	RHEL 4 U1 AS and WS	CAPP	EAL4+
Jun 2007	RHEL 5 GA	LSPP RBACPP CAPP	EAL4+
Jul 2003	SLES[2] 8 GA	-- --	EAL2+
Jan 2004	SLES 8 SP 3 RC 4	CAPP	EAL3+
Mar 2005	SLES 9 GA	CAPP	EAL4+
Aug 2005	SLES 8 SP 3	CAPP	EAL3+
Jun 2006	SLES 8 SP 3 Recertification	CAPP	EAL3+
Oct 2007	SLES 10 SP 1	CAPP	EAL4

[1] Red Hat Enterprise Linux [2] Novell SUSE Linux Enterprise Server

Sources:

- Elevated National Information Assurance partnership (NIAP): http://www.niap-ccevs.org/
- Set Federal Office for Information Security (BSI, Germany): http://www.bsi.bund.de/

Contributions by IBM's Linux Technology Center to Linux security

The LTC has contributed security enhancements to support many facets of the Linux processing environment.

Security Certifications

IBM is a leader in championing Linux Security certifications. IBM's contributions to the audit subsystem, labeled IPsec, and namespaces technologies help Linux to meet government security standards. The Common Criteria documentation and tests that IBM has developed and Open Sourced are reused throughout the industry.

Trusted Computing

IBM's Open Source Trusted Computing Software Stack (TrouSerS) extends the reach of Trusted Computing technology, which uses system hardware and software to enforce consistent and specific system behavior, into Linux environments. TrouSerS enables IBM clients to use the Trusted Platform Module (TPM) in IBM System x™ and IBM Power Systems® servers to ensure the integrity of mission critical servers.

Cryptography

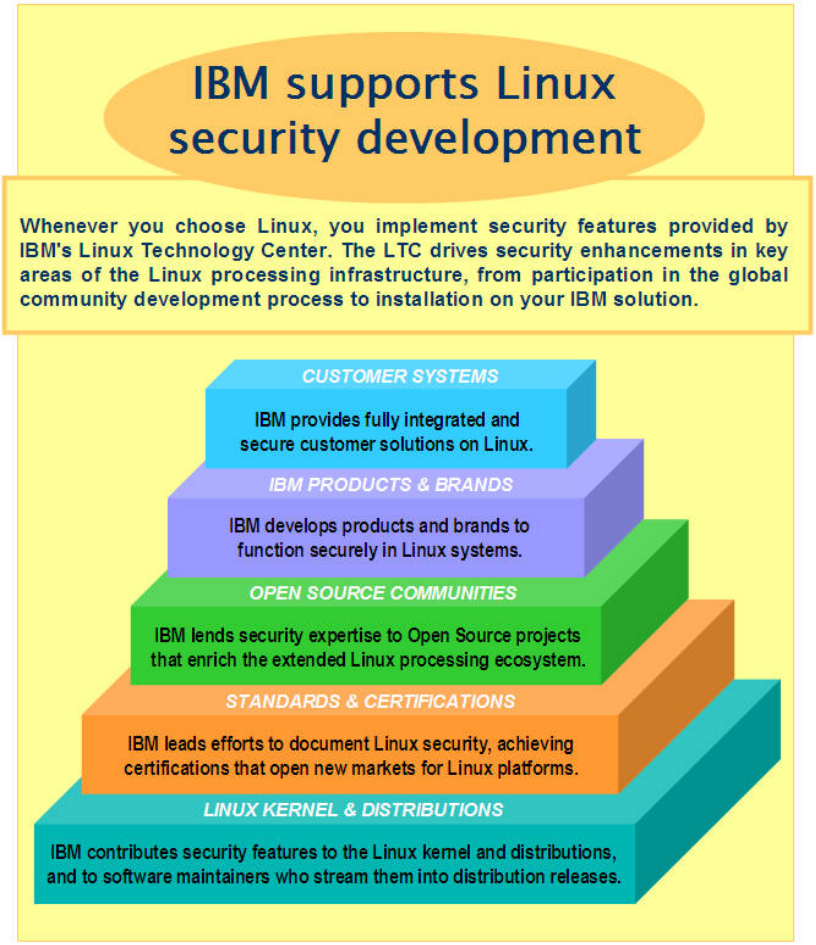
Linux cryptography provides data integrity and confidentiality on an enterprise scale. As a key contributor, IBM has:

- Created eCryptfs, a stacked cryptographic file system for Linux that offers the flexibility to encrypt sensitive data on a per-file basis.
- Contributed Linux kernel cryptographic software modules and hardware drivers that enable scalable security applications, such as VPNs.
- Co-sponsored the cross-company evaluation of OpenSSL against the FIPS 140-2 government standard.
- Supported ongoing consolidation of cryptographic libraries to achieve Linux Standard Base 4.0 compliance.
- Developed openCryptoki, an Open Source implementation of PKCS #11 standard interface to Hardware Security Modules and smart cards.

Networking Security

IPsec, or Internet Protocol Security, protects data as it travels across networks. This standard was driven by collaboration among industry leaders. IBM has:

- Developed features to enable IPsec compliance with current IPv6 RFCs to meet standards for U.S. Department of Defense use.
- Driven the implementation of leading edge Labeled IPsec to support the exchange of government classified information.



Core Linux security building blocks

To enhance end-to-end security of your system at the most fundamental level, IBM has:

- Contributed to the Linux Security Module (LSM) extensible security framework.
- Helped create the Common Criteria certified auditing system for tracking Linux Kernel security events.
- Contributed to Kerberos, the industry standard distributed authentication service.
- Developed a Linux PAM namespace module allowing private namespace for a session with polyinstantiated directories.

Systems hardening

System hardening means protecting critical IT resources against security threats through careful configuration of systems settings. IBM supports Bastille, a hardening tool shipped by numerous Linux distributors, with product enhancements by identifying security vulnerabilities and refining by way of product codefixes.

Providing direct customer security on Linux

Customers gain valuable security features on Linux thanks to many avenues of LTC investment. When a security feature developed in the LTC gains community acceptance, the code is accepted by upstream maintainers and incorporated into enterprise Linux distributions. The LTC also works within IBM to ensure IBM brands and products use Linux security features effectively. For example, IBM Power Systems and IBM System x have adopted TPM to extend the benefits of Trusted Computing to customers. Also, IBM System z® customers can take advantage of industry-leading specialized hardware for accelerating business-critical cryptographic workloads and secure key storage. As part of a special project, IBM worked with the UK government and a healthcare provider to use SELinux policy for IBM WebSphere® to carefully restrict the use of confidential information.

IBM collaborates extensively with our Linux distribution partners, Red Hat® and Novell, on Linux security customer issues. Recently, Red Hat sought to create an SELinux policy for the IBM Java™ Virtual Machine™, at the same time IBM was working to integrate SELinux labeling into the IBM Java Runtime Environment™ installer. LTC security engineers coordinated the results of these efforts to enable an embedded JRE, such as those shipped with products like IBM Lotus Notes®, to be installed to arbitrary file system locations.

By achieving CC certifications with Linux, IBM can offer all customers the same product security on Linux that has been approved for U.S. Government usage. The LTC works to ensure up-to-date CC certifications for IBM hardware platforms, and works with software product teams to create SELinux MLS (multilevel security) policies which enable IBM DB2®, WebSphere Application Server, WebSphere MQ, WebSphere Message Broker, and WebSphere Process Server to work on CC-certified Linux.

Choosing secure IBM and Linux

Information is one of the most important assets of your business. Choosing a secure operating system, trusted hardware, SELinux-aware middleware, and other system components is a critical step toward protecting that asset.

Where many industry providers list security proficiencies and skills, IBM has earned the reputation of being an industry standard-bearer for Linux security technologies. The involvement of the LTC in vital Open Source security initiatives enables IBM to provide industry-leading Linux security solutions.

For more information, visit the IBM Linux Security forum on IBM developerWorks®:

→ http://ibm.com/developerworks/forums/forum.jspa?forumID=1271

To learn more about IBM's commitment to Linux, see:

→ http://ibm.com/linux

IBM operates as a partner and a peer in every aspect of the Linux open source development community.

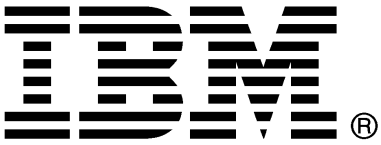
IBM has contributed, and will continue to contribute significant resources to developing and testing Linux for its customers, its business, and in partnership with the industry as a whole.

IBM ensures that its hardware and software products work seamlessly with Linux and the associated technologies.

IBM backs Linux with 24/7 support and its full services business.

IBM collaborates extensively with others in the community to ensure that Linux remains a robust, enterprise-ready platform.

With its extensive commitment to Linux and the open source community, IBM is the premier partner to provide your Linux and open source solutions.



IBM Corporation

Route 100
Somers, NY 10589

Produced in the United States of America
11-2008