Linux Security Capabilities: Perspective

Summary

Linux increasingly finds favor as an alternative to commercial server operating systems. Several initiatives aim to create a secure Linux, but the enhancements have yet to appear in popular distributions.

Table of Contents

Technology Basics

Technology Analysis

Business Use

Benefits and Risks

Selection Guidelines

Technology Leaders

Technology Alternatives

Insight

List Of Tables

Table 1: Technology Leaders: Mainstream Linux Distributions

Table 2: Technology Leaders: Secure Linux Distributions and Enhancements

Table 3: Technology Alternatives

Entire contents © 2002 Gartner, Inc. All rights reserved. Reproduction of this publication in any form without prior written permission is forbidden. The information contained herein has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Gartner shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice.

Technology Basics

The Linux Operating System

Linux is a Unix-like operating system (OS) that was designed to provide personal computer users a free or very low-cost OS comparable to traditional and usually more expensive Unix systems.

The Linux OS comprises the Linux kernel developed by Linus Torvalds at the University of Helsinki in Finland and programming utilities and standard commands from the Free Software Foundation (FSF) GNU project. (Hence, Linux is properly "GNU/Linux.") Most of the system and network administration tools in Linux come from the Berkeley Software Distribution (BSD).

Linux is distributed using the FSF's "copyleft" stipulations. Any copy or modifications are in turn freely available to others. Unlike Windows and other proprietary systems, Linux is publicly open and extensible by contributors — and bugs can be fixed quickly and easily. Linux comes in versions for all the major platforms, including Intel, SPARC, Alpha and even IBM S/390 and zSeries mainframes. There are nearly 50 Linux distributions, including a number of commercially supported distributions.

Security Capabilities

Linux is not a Unix OS: even though it "looks and feels" like Unix, it has no code that is based on Unix, but was built from the ground up with new code. Nevertheless, the base security capabilities of Linux are very much the same. Linux was originally developed for personal, rather than corporate, use. Commercial Unix OSs, however, have been developed to meet the needs of corporate use, including the need for more advanced security capabilities.

Commercial Unix OSs have been evaluated at the U.S. Federal Trusted Computing Security Evaluation Criteria (TCSEC or "Orange Book") C2 levels, at the European Information Technology Security Evaluation Criteria (ITSEC) F-C2 level and against the Common Criteria (CC) Controlled Access Protection Profile (CAPP). Although no open-source Unix OSs have been evaluated, some of the development groups also seek to provide similarly advanced security capabilities; OpenBSD, in particular, openly expresses a belief in strong security and aspires to be "No. 1" in the industry for security.

As organizations increasingly consider Linux as an alternative to Unix and other commercial OSs, at least the commercial distributions of Linux will be expected to provide the same robust security capabilities as a commercial off-the-shelf (COTS) OS.

Core Security Capabilities of a Commercial Off-the-Shelf Operating System

Any COTS OS should provide a range of capabilities that at least meet the security needs of its users, whether they are commercial organizations or "mainstream" government agencies. Such capabilities have been documented in the various computer security evaluation criteria and most recently in two International Standards Organization (ISO) 15408, or Common Criteria (CC), protection profiles:

- Controlled Access Protection Profile (CAPP), roughly equivalent to TCSEC C2.
- Labeled Security Protection Profile (LSPP), roughly equivalent to TCSEC B1.

Core COTS OS security capabilities fall into four areas:

Identification and Authentication

Copyright 2002

Linux Security Capabilities: Perspective

User identification and authentication are crucial to resource access control and auditing services: everything hinges on the true identity of the user. If users are not uniquely and unambiguously identified and those identities are not properly verified, an organization has no assurance that access to resources is properly controlled. Similarly, without properly authenticated identities, audit trails will be unreliable and provide no accountability.

Linux follows the same paradigm as commercial Unix and BSD OSs. Each user is assigned a unique login name, conventionally based on the user's common name, and a numerical user ID ("uid"). An administrator can specify a uid; otherwise, the next available uid is used. A uid can be nonunique, but this is exceptional, as users sharing a uid share access privileges.

Linux natively authenticates each user with a password. As with Unix OSs, the default action is to store encoded passwords in the /etc/passwd file. The encoding mechanism is very secure, using a one-way hash function (typically Data Encryption Standard [DES]) with a two-byte "salt" that "randomizes" the encoding to frustrate dictionary attacks. The /etc/passwd file, however, is world-readable and so available to an attacker.

Some Linux distributions also support an /etc/shadow file that only privileged users can read, to keep encoded password information secret from normal users. Red Hat and Debian Linux use shadow passwords by default; other distributions can make use of the Shadow Password Suite. To use shadow passwords, a system administrator needs to make sure all utilities that need access to password information are recompiled to support them. Shadow passwords might not be needed in some instances: for example, where the Linux machine is running on a LAN and is using Network Information Services (NIS) to get or supply user names and passwords to other machines on the network.

Linux supports a pluggable authentication module (PAM), which allows a system administrator to change authentication methods and requirements on the fly and encapsulate all local authentication methods without recompiling any executables. PAM can be used, for example, to substitute another encryption algorithm for DES, to enable shadow passwords on the fly and to allow specific users to log in only at specific times from specific places.

Resource Access Control

Users' access to data and services must be controlled to ensure the confidentiality and integrity of corporate information and the platform itself. CC CAPP (and earlier criteria) requires the OS to enforce a discretionary access control (DAC) policy. A DAC policy is one based on user identities and group membership, and their authorizations to resources, so that it can control precisely *who* can do *what* to *which* resources.

Linux again follows the same paradigm as commercial Unix and BSD OSs. Each file or directory is associated with an individual user, the "owner," and a group (by default, the owner's default group). The owner or a privileged user (administrator) can set which file access modes (read, write or execute) are permitted to the owner, to other users in the group and to everyone else. These permissions are stored as an octet, but normally are represented by a character string: for example, "-rw-r——x" indicates the owner has read and write access, and the group and "others" have only execute access.

The owner or a privileged user can change the owner or group associated with a file. Users can belong to one or more groups, as listed in the /etc/group file, and users belonging to more than one group enjoy the access permitted to all of those groups.

The "self/group/public" mechanism is simple to implement, flexible enough to allow for most common needs and generally reliable. While it does not meet the requirements of the TCSEC C2 or ITSEC F-C2

evaluation criteria — which call for the use of access control lists (ACLs) — it does conform with the current CC CAPP.

Linux, however, generally cannot enforce a Mandatory Access Control (MAC) policy required by the CC LSPP. Linux's access control capabilities can, however, be extended using the general-purpose Linux Security Module (LSM) framework. LSPP-conformant controls can be implemented via LSM using, for example, Security-Enhanced Linux (SELinux) from the U.S. National Security Agency (NSA) or Linux Intrusion Detection System (LIDS).

Security Audit

An OS must record information needed to establish accountability of users initiating or participating in security events and actions — logon and logoff, resource access, configuration changes. An OS must also ensure the security of this record, the "audit trail," and should also provide suitable reporting tools.

The Linux system daemon syslogd can be used to log system events such as kernel messages, login or logout messages and general system messages. The syslogd daemon can be configured to automatically send log data to a central syslog server, but generally without encryption, data integrity checking or data origin authentication. Variants such as metalog and syslog-ng offer more granular control of what events are logged.

None of these, however, meet the formal requirements for event-logging facilities. These logs do not provide an audit record of all auditable events listed in the CC CAPP nor do they associate each event with the identity of the user that caused the event. This is a fundamental lack and one that will likely hamper Linux deployment in large security-conscious organizations. Some vendors and development groups are addressing this issue. For example:

- Hewlett-Packard offers HP Secure OS Software for Linux. Among other security enhancements, this offers a kernel-level auditing mechanism that maintains a full audit trail and allows organizations to ensure full user accountability.
- InterSect Alliance offers System iNtrusion Analysis & Reporting Environment (SNARE). SNARE is designed to form the basis of a host-based intrusion detection system (IDS) and a "C2-style" event-logging facility.
- The Secure Auditing for Linux (SAL) project is also developing a kernel-level auditing facility to monitor all security-relevant events — conformant with CC CAPP — and to securely store audit-trail data to ensure admissibility in a court of law.

Security Management

An OS must provide a mechanism that ensures only designated persons — "authorized administrators" — can make changes to system configurations and the security policies for authentication, access control and audit. An OS should also provide a suitable interface and reporting tools.

Linux enforces the same restrictions as Unix OSs: only privileged users can change system configurations; users can change only their own passwords; privileged users can change any user's password; and file owners and privileged users can modify file ownership and permissions. Users work through the terminal window's command-line interface to execute familiar Unix commands — passwd, chmod, chown and so on.

Secure Configuration

Linux Security Capabilities: Perspective

The most important thing for an administrator to do after installing Linux is to disable unnecessary services and daemons. Many network services are automatically enabled in most Linux distributions to make it easy to set up servers, but many of these are unnecessary and might give rise to serious security problems.

A system administrator should, at least, remove or delete any unused boot-time Linux processes (such as sendmail, named, routed and hppd) and consider using secure shell (SSH) rather than the telnet remote access user interface or r-commands (rsh, rlogin and rexec).

Additional Security Capabilities

A secure system, however, does not rely on the security of the OS alone. There are a number of areas where additional security capabilities may be desirable, if not essential: for example, user identification and authentication, authorization, administration and perimeter security (firewalls, intrusion detection). Some Linux distributions may build in these additional capabilities; most will be provided by third-party software.

Any organization considering Linux as an alternative to a Unix or other commercial OS needs to consider both the native security capabilities of the OS itself and the quality and availability of additional security software. What is needed will depend on the organization's requirements and a balance of costs against risks, but consideration should be given at least to the following areas:

- **Authentication** — Authentication is required to confirm that either a user or a machine has a valid identity and legitimate access to a system. Linux's native user authentication mechanism is not particularly robust, especially where users are logging on over open networks where passwords can easily be "sniffed." Secure remote authentication mechanisms can overlap with virtual private networks (VPNs). Kerberos can also be used.
- **Access Control** — Access control mechanisms provide a way of restricting which users can use which system resources. Linux's native controls are not particularly flexible or robust. Confidence in the security of a system is based in part on confidence in the way that users and access controls have been set up: good administration — that is, good reporting and good management — is essential.
- **Encryption** — Even with good access control, data on a computer's hard drive is vulnerable to attacks that bypass the OS: for example, by physically removing the hard drive and installing it on another machine. Data encryption can ensure that an attacker comes away empty-handed. Linux kernel 2.4 provides the ability to encrypt file systems.
- **Virtual Private Networks** (**VPNs**) — VPNs use cryptography to allow users to communicate via a public network in a way that is secure against intrusion or surveillance. VPNs can overlap with either firewalls or authentication mechanisms. Linux kernel 2.4 provides the ability to create VPNs via its cryptographic extensions.
- **Antivirus** — Although Linux itself is quite resistant to viruses, good antivirus software is an important safeguard. Furthermore, it is possible for, say, a Windows client to be infected with a virus via a Linux server.
- **Firewalls** — Firewalls protect networks by providing a "perimeter defense," restricting access by combinations of IP addresses and service types (for example, File Transfer Protocol [FTP], Simple Mail Transfer Protocol [SMTP], telnet). Firewalls often overlap with VPNs.

Linux Security Capabilities: Perspective

- **Vulnerability Assessment** — Scanners probe for open ports and known security holes. They provide assurance that computers and networks are, as far as possible, free from vulnerabilities. Other software can be used to verify host security.
- **Intrusion Detection** — Port-scan detectors look for port scans and can simply log the attack or retaliate in some way, such as blocking all access from the attacker's address. Other software can detect intruders by their "footprints," for example, variations in file integrity. A "honeypot" is a lure to attackers that gives the illusion of common vulnerabilities; any activity on these dummy ports or networks has to be from an intruder, so it is trivial to identify when an attack is taking place.

Technology Analysis

Business Use

Although it used to be education and research organizations and computer hobbyists that were drawn to Linux, commercial organizations are warming to Linux technology. Although Microsoft Windows still prevails in terms of installed base, Linux is the fastest-growing server OS. For application development, file-sharing and print-sharing tasks, and intranet/Web hosting, Linux is competing in the Windows server space.

Organizations must, however, be aware of the security capabilities of Linux, especially where limitations of the preferred distribution — for example, a lack of CC CAPP-compliant auditing — may be a barrier to its use for security-critical applications.

Benefits and Risks

Benefits

Linux Is Continuously Scrutinized and Actively Improved

Proprietary OS vendors must rely on laborious internal testing to find and fix bugs, and few are prepared to make a big investment in proactively eliminating vulnerabilities. Linux, like the open-source BSD variants, is open to the scrutiny of thousands of developers who are free to examine and improve the current code base. And as many of those developers approach the task with security in mind, the time required to find a bug is significantly decreased.

Furthermore, rather than waiting for computer emergency response teams (CERTs) to report a new bug being exploited, open-source development groups are likely to ferret out and fix bugs *before* they can be exploited. An experienced Linux developer might take only minutes to verify a bug and only hours to develop a fix for the bug and share it with the world. Commercial Linux distributors' response times are somewhat longer, say one to two weeks, but this is substantially less than the months-long response time that can be expected from commercial Unix OS vendors. Nevertheless, the organization is still faced with the challenge of keeping up to date with all fixes.

Linux Is Less Vulnerable to Viruses and Other Malicious Code

The basic OS structure of Linux (and open-source and commercial Unix OSs) makes it less susceptible to viruses than Microsoft Windows OSs. Viruses must insert code somewhere to be executed, but unless the code has purposely been given permission, Linux automatically prevents code execution. Furthermore, a Linux user (other than root) cannot write to system files, confining the damage that the virus can do to files the user can write to.

Nevertheless, viruses and other malicious code attacks on Linux are not unknown. As Linux becomes more popular, virus writers increasingly target it, and the number of known Linux viruses is now in the

Copyright 2002

hundreds (although this is still a fraction of the number of known Windows viruses). Organizations should also note that a Linux machine can be a vector for Windows viruses, for example, if it is an e-mail server.

Risks

Linux Is Not "Secure By Default"

To achieve CC CAPP-conformant, C2-like security, a system administrator needs to properly configure the system. In common with most commercial and open-source OSs, few major Linux distributions are shipped in a "secure by default" mode. Exceptions are Turbolinux Server, with its "only what's needed" default configuration, and Mandrake Linux, with its "Paranoid" configuration (although this is only optional).

Many of the "secure" Linux distributions — EnGarde Secure Linux, HP Secure OS Software for Linux and Trustix Secure Linux — do aim to be "secure by default." In addition, Bastille Linux allows administrators to easily harden Red Hat, Mandrake and Debian distributions.

Open Source Enhancements and Tools

A huge number of enhancements and tools are available for Linux — and anyone can develop his or her own enhancement or tool as an alternative to the rest. Linux system administrators have a wide choice.

While Linux enthusiasts insist that this is "a good thing," it may be a concern when Linux is to be used by commercial organizations. These enhancements and tools generally do not have any kind of warranty; the perceived quality of a tool rests on the reputation of the development group in the Linux community. Nor do they have support from commercial vendors. This does not mean that the support is necessarily poor — it is often excellent, with the benefits of open-source development mentioned before. Organizations will not, however, have the customer service agreements that they would expect with proprietary software, and for security-critical software in particular, this may be unacceptable.

Limited Support by Proprietary Security Software

A number of commercial vendors offer a variety of proprietary security software for Linux, but many are niche players rather than market leaders. The situation is improving, so that organizations can easily find Linux versions of leading proprietary network security products, such as antivirus software, firewalls, vulnerability scanners and IDSs. Not all major vendors in each market will support Linux, however, and this can limit an organization's choice. For example, of the three current leaders in the IDS market, two can monitor Linux hosts and only one can use Linux for its management console. And sometimes a Linux version may not have the full features of a Unix or Microsoft Windows version.

This limitation is more severe in high-end security software, for example, in the identity and access management (IAM) space. Linux is often supported as a target system for password management or provisioning products, but very few IAM products can sit on a Linux server.

Linux Vulnerabilities Are Exposed to Attackers

The availability of Linux source code allows a malicious person to examine it for vulnerabilities that can be exploited in an attack. This is the corollary of the first benefit above. It is quite possible that a potential attacker will discover — and exploit — a vulnerability before others find and fix it. On balance, however, more vulnerabilities will be found and fixed by "people of goodwill."

Copyright 2002

Selection Guidelines

While security is an important criterion, any organization will make its decisions on whether or not to move to Linux and, if so, which distribution to choose, on a range of criteria. These selection guidelines address only the security issues.

Good-Enough Security

Most organizations are likely to choose one of the mainstream Linux distributions. If it has freedom to choose between them, it should look for either:

- A distribution that provides sufficient security to meet its needs.
- A distribution that can be beefed up using suitable enhancements.

In either case, the organization must consider the effort that will be required to install and securely configure the OS and any enhancement(s).

CAPP-Conformant Auditing Requirements

None of the mainstream Linux distributions provides event logging that meets the CC CAPP requirements. An organization must first decide if this poses a problem within the framework of its information security policy and its technical architecture. Comprehensive event logging is increasingly important not just to maintain individual accountability, but also to provide a basis for enterprise IT security management. If full auditing is required, an organization should look for either:

- A “secure” distribution that embeds auditing or is packaged with a suitable enhancement.
- A mainstream distribution that can be augmented with a suitable enhancement.

LSPP-Conformant Access Control Requirements

None of the mainstream Linux distributions supports a MAC policy that meets the CC LSPP requirements. This will not pose a problem for many organizations, but an organization may have to meet regulatory requirements for B1-like security, or it may be imposed by its own information security policy. Such a requirement will create a challenge for the organization, as Linux enhancements that support MAC (for example, LIDS and SELinux) do not meet the C2-like CAPP auditing requirements — that is, it must layer enhancements on a mainstream distribution. In this situation, unless there are other compelling reasons to choose Linux over a commercial Unix OS, the organization may be better off using a “secure” commercial Unix OS.

Established Security Software Infrastructure

An organization must also consider how a particular (or any) Linux distribution will fit with its existing security software. While many network security and identity and access management products do support Linux as a target system, some do not. If an organization cannot “see” Linux machines using existing software, it faces the dilemma of either acquiring Linux-specific solutions and managing these separately or migrating to different software enterprise wide. Neither is really tenable.

Copyright 2002

Linux Security Capabilities: Perspective

Technology Leaders

Table 1: Technology Leaders: Mainstream Linux Distributions	
The SCO Group (SCO), OpenLinux (Internet: www.sco.com)	SCO (formerly Caldera) is a member of the UnitedLinux project. OpenLinux 64 and OpenLinux Server include intrusion detection software to check for port intrusions and to advise the administrator of potential attacks. An OpenLinux system is installed with all unnecessary processes, ports and access points closed or turned off.
Debian Project, Debian GNU/Linux (Internet: www.debian.org)	Debian GNU/Linux includes OpenSSH for secure remote login. Debian claims that most security problems brought to its attention are corrected within 48 hours. Debian's security Web page addresses Debian's status to known security holes. Debian tracks security bugs until a version with the fix is released, and the company recommends using the latest version to avoid security problems.
MandrakeSoft, S.A., Mandrake Linux (Internet: www.mandrakesoft.com)	Mandrake Linux 9.0 provides several security features: • Four security levels, from "Standard" to "Paranoid," depending on the intended use of the system. • Shorewall 1.3.7, a firewalling subsystem based on the netfilter/iptables project. • Cryptographic functions: GnuPG, OpenSSH, SSL certificate management tools, a special Linux Kernel Secure, encrypted file systems and e-mail encryption. • User authentication via Lightweight Directory Access Protocol (LDAP), NIS or Windows authentication servers as well as local files.
Red Hat Inc., Red Hat Linux (Internet: www.redhat.com)	Red Hat is the dominant commercial Linux distribution and is the most common basis for third-party secure Linux distributions. Red Hat Linux 7 includes OpenSSH for secure remote login.
SuSE AG, SuSE Linux (Internet: www.suse.com)	SuSE is a member of the UnitedLinux project. SuSE Linux includes the SuSE Firewall package and a "Harden SuSE" utility that cleans up file permissions and turns off daemons. It supports encryption for e-mails (GnuPG, OpenPGP) and for file systems.
Turbolinux Inc., Turbolinux (Internet: www.turbolinux.com)	Turbolinux is a member of the UnitedLinux project. The Turbolinux distribution bundles ipchains-firewall as well as the Amanda backup program for disaster recovery. In Turbolinux Server, most services and ports are disabled by default, and the distribution includes: • 128-bit SSL library for secure network communication. • Software to monitor, prevent and identify all file changes.

Table 2: Technology Leaders: Secure Linux Distributions and Enhancements	
Hewlett-Packard Co., HP Secure OS Software for Linux (Internet: www.hp.com/security/products/linux)	Based on the Linux 2.4 kernel and Red Hat Linux 7.1. Its security enhancements include: • Application and data containment — preventing unauthorized communication between programs to minimize the damage from an attack. • System configuration lockdown — automatically disables unnecessary services and secures enabled services. • System event auditing — provides a full security audit trail. • File system integrity — via Tripwire Open Source, Linux Edition.

Table 2: Technology Leaders: Secure Linux Distributions and Enhancements	
Trustix AS, Trustix Secure Linux (Internet: www.trustix.net)	Trustix intends Trustix Secure Linux to be a secure version of Linux for server use. It does not offer any security enhancements, but offers "secure defaults for everything," minimizing the number of packages installed and using the most secure package where options are available.
U.S. National Security Agency (NSA), Security-Enhanced Linux (SELinux) (Internet: www.nsa.gov/selinux/index.html)	SELinux is an implementation of flexible and fine-grained nondiscretionary access controls in the Linux kernel, based on the Flask security architecture developed by Ray Spencer and others. It was released under GNU General Public License (GPL) in 2001. It was originally implemented as its own particular kernel patch, but now uses the generalized Linux Security Module (LSM) kernel patch. It is a demonstration implementation of mandatory access controls in Linux and does not address system assurance or other necessary features such as security auditing.
Guardian Digital Inc., EnGarde Secure Linux (Internet: www.engardelinux.org)	EnGarde's design philosophy is based around the principle of least privilege: each program runs with only the privileges it needs. Furthermore, nonessential programs are either disabled by default or omitted altogether. EnGarde Secure Linux also includes security software, such as Snort and Tripwire, and the OpenWall kernel security patch.
InterSect Alliance, System iNtrusion Analysis & Reporting Environment (SNARE) (Internet: www.intersectalliance.com/projects/Snare)	SNARE provides three complementary applications: • A dynamic kernel module (auditmodule.o), which captures information about critical system calls. • A user-space audit daemon (auditd), which writes event data to a log. • A graphical configuration and reporting tool (snare). InterSect Alliance provides SNARE binaries for Red Hat Linux 7.x and source code that can be recompiled for other Linux kernel 2.4 distributions, such as Debian, Mandrake and SuSE.
Secure Auditing for Linux (SAL) (Internet: http://secureaudit.sourceforge.net)	SAL is a research project funded by the Defense Advanced Research Projects Agency (DARPA). The project will develop a kernel-level auditing package for Red Hat Linux conformant with CC CAPP. It will also provide cryptographic features to protect logged information from unauthorized modification. As of June 2002, the project was at the design/code stage.
Linux Intrusion Detection System (LIDS) (Internet: www.lids.org)	LIDS is *not* an intrusion detection system as such, although it embodies a port-scan detector and can generate kernel-level security alerts. LIDS comprises a kernel patch and an administrative tool that enhances the core security capabilities of Linux. It provides MAC and robust protection of files and processes.
Bastille Linux (Internet: www.bastille-linux.org)	The Bastille Hardening System attempts to harden the Linux OS. It currently supports Red Hat, Mandrake and Debian distributions. Bastille Linux was developed with three major goals: • Comprehensiveness — drawing from "every available major reputable source" on Linux security and the project manager's own experience with Solaris and Linux. • Instructiveness — designed to educate the installing administrator about the security issues involved. • Community — the specification and hardening script are published under a GPL.

Linux Security Capabilities: Perspective

Technology Alternatives

Technology alternatives include a variety of OSs from different vendors and development groups, for different platforms and with different security capabilities.

Table 3: Technology Alternatives	
Microsoft's Windows 2000 and Windows .NET Server OSs (Internet: www.microsoft.com)	Windows 2000 Server SP3 has recently (September 2002) been certified against the CC CAPP at Evaluation Assurance Level 3 (EAL3). Although it has yet to be evaluated, Windows .NET Server 2003 encapsulates the same CAPP-conformant features as Windows 2000 Server SP3. Windows 2000 server OSs offer significant improvement over Windows NT 4.0 in security functionality with Active Directory (AD) directory services, Kerberos user authentication, built-in support for public key infrastructure (PKI), VPNs, smart-card-based user authentication and so on. Windows .NET Server 2003 offers further improvements in the robustness of the core platform and extensions to the additional security capabilities.
Novell NetWare (Internet: www.novell.com)	NetWare, now at version 6, is a widely installed network server OS. NetWare includes advanced security features such as public key cryptography and Secure Authentication Services (SAS), based on technology licensed from RSA Security. An earlier version, Novell IntranetWare (NetWare 4.11 Server) with IntranetWare Support Pack 3A and Directory Services Update, was evaluated as a TCSEC C2 network component.
Open-Source Unix OSs • FreeBSD (Internet: www.freebsd.org) • NetBSD (Internet: www.netbsd.org) • OpenBSD (Internet: www.openbsd.org)	Open-source Unix OSs include three variants of BSD: FreeBSD, NetBSD and OpenBSD. No open-source Unix OSs have been rated. This does not, however, mean that these systems cannot meet commercial security requirements, only that they have not been evaluated. OpenBSD puts the strongest focus on security: the development group openly expresses a belief in strong security and aspires to be No. 1 in the industry for security. No *BSD, however, provides native support for ACLs, although Trusted BSD aims to provide Posix.1e support in FreeBSD.
Proprietary Unix OSs • Apple Computer Mac OS X Server (Internet: www.apple.com) • Hewlett-Packard HP-UX (www.hp.com) • IBM AIX (Internet: www.ibm.com) • Silicon Graphics (SGI) IRIX (Internet: www.sgi.com) • Sun Microsystems Solaris (Internet: www.sun.com)	AIX, HP-UX and Solaris are the three dominant proprietary Unix OSs, with Solaris having over half the market. SGI's IRIX is a niche offering for high-performance environments. Apple Computer's BSD-based Mac OS X Server is the newest product and competes directly with Linux as an alternative to Microsoft Windows server OSs in the small and midsize business (SMB) market. Unix OSs are mature and technically superior with a proven track record for performance, reliability and security in a server environment. Many commercial Unix OSs and platforms — including AIX, HP-UX and Solaris — have been evaluated at TCSEC C2 or ITSEC F-C2. Unix OSs that have been evaluated against CC PPs include: • Solaris 8CAPP EAL4 • Trusted Solaris 8 — LSPP EAL4 • IRIX 6.5 CAPP — EAL3 • Trusted IRIX 6.5 — LSPP EAL3 (EAL4 provides a higher level of assurance than EAL3.) Apple has recently submitted Mac OS X Server (and Mac OS X) for CC CAPP evaluation.

Table 3: Technology Alternatives	
Mainframe OSs • IBM z/OS (Internet: www.ibm.com)	Mainframe OSs have a different architecture and code heritage. The leader is IBM's z/OS, the 64-bit successor to OS/390. z/OS differs from Unix by having an external security manager, either IBM's own Resource Access Control Facility (RACF) (part of the SecureWay Security Server) or CA's eTrust CA-ACF2 or eTrust CA-Top Secret. z/OS is a robust platform and a benchmark for good security.

Insight

Linux is more than a niche operating system and is driving toward mainstream acceptance. It shares the basic security capabilities of commercial and open-source Unix OSs. In common with the open-source BSDs, Linux benefits from rapid bug identification and remediation: it is not inherently more secure than a commercial OS, but will tend to achieve a given level of security more quickly. Mainstream Linux distributions do not yet have the auditability necessary for C2-like CSPP conformance or the more advanced security capabilities required for B1-like LSPP conformance. Secure Linux distributions, or enhancements for mainstream distributions, are available, but these do not have the same level of support as the mainstream distributions. There is an abundance of free, open-source security tools for Linux, but, while the situation is improving, organizations can be limited in their choice for commercial security software for Linux. In the short term, however, organizations that put a premium on good security should stay with better-established commercial Unix OSs or other commercial OSs.

Copyright 2002