Linux as a Trusted Operating System: A Secure and Cost-Effective Choice for Government Systems

EXECUTIVE SUMMARY
Sponsored by: IBM
Shawn P. McCarthy
August 2006

INTRODUCTION

"Trusted" is moving to open source. Work is under way by members of the open source community to make Linux a trusted operating system.

Computers that run "trusted" operating systems (OSs) have long found a home in select government agencies because of the government's unique need to protect and share data and establish secure connections. Secure operating systems and trusted systems play important roles in many niches throughout the government, but historically, the Department of Defense and intelligence organizations have shown the strongest interest in these systems. Growing demand, in other parts of the government and in the private sector, for increased security and integrity of systems should expand the usage of trusted operating systems.

Until now, a trusted operating system has been a distinctive version of a standard OS that has been enhanced with special security mechanisms and services to allow a computer to compartmentalize data and protect information and connections. The acceptance of the work now under way by the open source community will make Linux a trusted operating system. Organizations will have the option of running Linux in their traditional manner or with configured trusted options.

The debut of trusted Linux will move trusted OS solutions firmly into the open source community, making the trusted OS a more mainstream solution for government users.

Implementation results may vary by organizations, but federal, state, and local government IT managers may find this open source offering a friendly and affordable solution for their secure system needs.

This IDC Government Insights Executive Summary explores the benefits of trusted Linux in the government IT space and looks at why it is likely to become a favorite of the large systems integrators (SIs) that serve this space. It also looks at how IBM, Red Hat, and Trusted Computer Solutions are working together to put trusted Linux on the fast track.
**Key Government IT Market Drivers**

Before we delve into the particulars of trusted Linux, it's important to understand the key issues that drive government IT spending today. These issues are as follows:

- **Government budgets are tightly constrained.** There is substantial pressure from the Office of Management and Budget to reduce costs and consolidate IT systems. Events such as the wars in Iraq and Afghanistan and natural disasters such as Hurricanes Katrina and Rita have consumed government resources and made all government spending, including IT budgets, extremely tight.

- **Demands are increasing for improved and integrated government services.** Constituents are demanding better-performing and more reliable online interactions, effective handling of security threats, and better collaborative environments.

- **Accountability for compliance and efficiency is increasing.** Agencies must track and report on how they are complying with a variety of laws and government reporting structures, including those aimed at streamlining costs. Secure, reliable data sources are needed if these reports are to be reliable.

- **Emphasis on security continues, but with a requirement for improved accessibility.** A system can be made so secure that it fails to share data in a timely manner with those who need it most. A system is most valuable when it is both secure and quickly accessible to the right people.

- **Innovative buying models are being developed.** From packaged solutions to new pricing structures that reach across multiple levels of government, costs are being driven down while new higher expectations for performance are being set.

**What Is the Definition of Trusted Linux?**

The standard open source Linux operating systems will become trusted operating systems with the trusted Linux enhancement. A trusted Linux is being developed in response to the needs and demands of government agencies for a secure, mainstream operating system capable of addressing system access and other security concerns. This response from open source technology providers heeds the government's call by using open source Linux as the platform for delivering a highly secure operating system to the marketplace.
Government IT infrastructures are being challenged today to meet very stringent security requirements by business, citizens, and various government regulations. In addition, government systems managers must find new methods to efficiently handle interenterprise and interagency information flows across security boundaries while meeting the ongoing operational and business challenges of their organizations.

If organizations are to accomplish this goal, then the underlying platform must provide a certain level of trust. Traditional architectures, which support only discretionary access control (DAC), have proven to be inadequate solutions to emerging threats and high-connectivity requirements. They are unable to provide the fine-grained access control necessary to support trusted platforms.

A trusted platform then must support some form of mandatory access control (MAC) capability. In its most general form, a MAC capability is an access control mechanism that enforces a system security policy that cannot be altered at the discretion of the system user. This enforcement of a system-level security policy provides much of the "trust" in the trusted platform.

In addition to providing the trusted functionality, the trusted platform must provide a level of assurance for this functionality. This assurance is normally achieved through security certifications, such as the Common Criteria Evaluation and Validation Scheme (CCEVS). Such capabilities have been built into the standard Linux infrastructure, leading to a "trusted" Linux.

**Security Enhanced Linux**

As a first step, organizations must understand the baseline Security Enhanced Linux, also known as SELinux.

SELinux is a set of capabilities adopted by the open source community. It is used with the Linux kernel available in some Linux distributions (e.g., Red Hat Enterprise Linux 4). It forms the foundational baseline for trust and is important to understand.

An outgrowth of National Security Agency (NSA) research projects, SELinux capabilities are built around the Linux kernel, with several additional utilities. Its security functions provide MAC, plus details on how such controls should be built into Linux.
SELinux is not a "trusted" operating system by itself. A trusted OS (which is what trusted Linux will be) includes support for multilevel security and complies with government requirements that literally fill a whole book. It includes a layered extension of the standard Linux OS at the kernel level (with user-level support) and specific containment properties to guard against application intrusion and compromise. It has security mechanisms and services to allow systems to protect, distinguish, and separate or compartmentalize classified government data or sensitive corporate information. Such systems should also have detailed development, documentation, and testing requirements to ensure that the security features have been properly implemented.

The NSA has been very supportive of efforts to bring trusted Linux into the open source realm.

The value of trusted Linux is that it provides the foundation to allow:

- Access to secure information across different domains — system to system, agency to agency
- Information sharing between different security levels without compromising protected data
- Transfer of information across domains using the security protocols required

**The Certification Process for Trusted Linux**

In the case of trusted Linux, the term "trusted" also refers to an operating system that has been evaluated under the CCEVS with an evaluation assurance level (EAL) of 4 or higher under specific protection profiles. A trusted operating system must have security functionality that includes MACs, role-based access, and labeled security access. The labeled security access is enforced by MACs utilizing multilevel security (MLS).

CCEVS is the result of a multiyear effort by the governments of the United States, Canada, the United Kingdom, France, Germany, and the Netherlands to develop harmonized security criteria for IT products.

Details on who is pushing the development of a solid trusted Linux OS can be found in the Vendor Synergy section of this document.

Other vendors and operating systems are also going through the CCEVS process. Government systems administrators will need to make a choice as to whether they will install and support multiple trusted systems or whether they will standardize on a single enterprise trusted solution. In such cases, price point may be a major deciding factor.
Where Does Trusted Linux Fit In?

Any security-conscious organization, public or private, may have a need for trusted Linux. However, government agencies, especially those with a strong need to protect classified data or to protect any sort of data or system from hackers, have a particularly strong need. Trusted Linux addresses the same security requirements that have been addressed by traditional, more expensive operating systems over the past 10 years. Thus, the scope of this cost-effective open source solution could be very extensive if adopted by government agencies.

The types of government applications, environments, and networks that would use trusted Linux are numerous and varied. They include financial management systems, human resources systems that need to protect personal records, transaction processing systems, and, of course, intelligence agencies, defense installations, and homeland security data and systems that are needed to help keep the country secure.

Virtually any organization that adheres to the National Information Assurance Partnership (NIAP), the CCEVS, or the Defense Information Systems Agency Common Operating Environment (COE) should pay attention to trusted Linux as it matures.

Drivers and Pain Points

The events of 9/11 drove home the need for government agencies to securely collaborate and share relevant data. In fact, the 9/11 Commission report specifically mentions this need and a presidential directive mandates better security. Some of the pain points driving the need for trusted Linux include:

- Abuse of system privilege to gain access to protected system resources
- Undermining application-enforced access controls to bypass application security rules
- Supply of bogus security decision-making information
- Illegitimate use of unprotected system resources

A properly installed and configured trusted Linux system can address each of these issues because of the way it's designed.
The Cost Factor: Cost-Effective Licensing and Access to Commodity Architecture Servers

One of the largest pain points for trusted systems has been high cost; they have been significantly more expensive than traditional systems. Trusted Linux should address this issue because it plugs into the open source Linux model that requires OS enhancements to be made available to all.

However, it's unlikely that many government customers will download, install, and manage trusted Linux systems by themselves. Servers (and occasional client machines) running trusted Linux will usually be integrated into larger systems and solutions. As such, the SIs that build and manage these systems for the government will often install them.

Because trusted Linux can run on commodity Intel architecture servers, further cost savings may be realized. Performance should not be a significant issue because systems can be configured to achieve top-level performance on machines with higher-end processors (e.g., symmetric multiprocessors [SMPs] and blades).

The Function Factor

Leveraging Linux for trusted applications brings all the power of a current open operating environment to the equation. This power includes key functions, assumed as normal work tools in most environments today, such as video streaming and high-bandwidth presentation graphics or visualization applications. These work tools can be difficult to provide in current implementations. In addition to these new functions, Linux offers true hardware and software independence, providing a level of choice not previously available in this trusted applications market space.

Vendor Synergy

Building on the NSA's efforts, Trusted Computer Solutions is working to establish significant pieces of the trusted Linux system. IBM and Red Hat also play key roles as the driving forces behind this development. The three companies are working together with the open source community to establish higher security for Linux. The results of the collaboration will be submitted to the open source community for incorporation into standard, mainstream Linux.
Each company is leading initiatives to bring trusted Linux to the marketplace. Trusted Computer Solutions ported its application suite to run on trusted Linux. Red Hat is incorporating the trusted Linux changes into its standard release of Red Hat Enterprise Linux 5 (RHEL5). IBM is certifying that Red Hat RHEL5 will meet the government's Trusted Standards on its Intel- and Opteron-based System x platforms as well as its System z and System p platforms. Thus, Trusted Solutions will be available across the broad range of IBM platform offerings.

In September 2005, IBM entered CCEVS evaluation with trusted Linux for the label security protection platform, role-based access control profile, and the controlled access protection profile at the EAL4 level. This evaluation is being conducted across IBM's System server line of products. Evaluation is expected to be completed in the first quarter of 2007.

Other major players waiting in the wings include the SIs that have increasingly leveraged Linux in recent years. The Linux operating system has proven to be a cost-effective solution for everything from government Web sites to database and application servers driving back-office government solutions. A trusted Linux should support expanded usage in the government sector.

IDC's Government Insights believes not only that trusted Linux will give SIs another powerful tool in their system development arsenals but also that trusted Linux has the potential to become one of the more popular operating systems installed for government solutions that will be built by many SIs.

**Summary of Trusted Linux Benefits**

Organizations using trusted Linux will be able to:

- Share information across domains more freely but with security controls in a multilevel, trusted environment
- Protect resources from internal and external threats through tightly configured permissions
- Increase productivity by consolidating on a single, more secure platform
- Increase both system-level and application-level security
- Decrease operating costs by reducing OS licensing fees and hardware costs
- Improve accuracy of auditing and reporting for secure applications and data
Challenges

The gauntlet to trusted Linux certification is stringent, as it should be, and the current efforts by IBM, Red Hat, and Trusted Computer Solutions must continue to be focused to meet the timelines planned. Maintaining focus and the synergy of purpose is challenging within the four walls of any organization and even more challenging across three organizations. Discussions with all three organizations were held separately and at the same time and indicate that the challenge is being met.

Essential Guidance

Government IT shops can and should prepare themselves for the arrival of trusted Linux by familiarizing themselves with its properties and deciding which of their systems are most in need of this secure solution. They should also look at the existing secure operating systems within their organizations and determine if long-term costs can be trimmed by migrating to trusted Linux platforms.

Such evaluations can begin now, with a plan to migrate toward the end of 2006 and beyond, as trusted Linux becomes available.

IDC's Government Insights believes that the decision to migrate to trusted Linux should account for the costs associated with porting applications to a new system, personnel, and ongoing maintenance, as well as other factors.

Such a decision can usually be quantified, and the calculations can help clearly identify the right decision. IDC's Government Insights believes that trusted Linux will be an attractive option for many government organizations and the SIs that serve them.

With strong interest and support from the IT vendors mentioned, government-oriented SIs, and a robust government end-user community, trusted Linux is well positioned to have a major impact on government IT shops in the very near future.

Copyright Notice

Copyright 2006 Government Insights, an IDC company. Reproduction without written permission is completely forbidden. External Publication of Government Insights Information and Data: Any Government Insights information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate Government Insights Vice President. A draft of the proposed document should accompany any such request. Government Insights reserves the right to deny approval of external usage for any reason.