Defense Enterprise Linux: The DoD Computing Platform

Roy S. Keene

October 12, 2011

1 Introduction

1.1 What is an Enterprise Platform ?

An enterprise platform is an operating system that provides more than just basic services that applications can use to access hardware, it also provides services for managing large numbers of servers running diverse applications centrally.

1.2 Defense Enterprise Linux

Defense Enterprise Linux will be an enterprise platform based on the Linux kernel and in-house and GNU user-land, as well as Open Source Software. It will be the combination of the best-of-breed tools and ideas from various existing enterprise platforms as well as several innovations unique to Defense Enterprise Linux.

1.3 Why ... ?

1. Why now ?
   (a) Right now may not seem like an excellent time for a divergent Linux Distribution[1], but due to several market factors it is:
      i. Oracle recently bought Sun Microsystems and Solaris;
      ii. RedHat Enterprise Linux is enjoying great success in the enterprise space, but the enterprise tools are still somewhat primitive;
      iii. Microsoft Windows NT is being preferred by many institutions due to its formal (if not standard) interfaces for managing enterprise systems
2. Why me ?

[1] A Linux Distribution is an Operating Environment based on the Linux kernel (think hardware drivers, and process isolation) and some user applications.

(a) I have a unique combination of experience and expertise;

   i. System Administration for UNIX as well as Windows NT systems
   ii. Systems programmer and analyst for UNIX as well as Windows NT systems
   iii. Experience with creating and maintaining Linux distributions

(b) I have worked for the Department of Defense since 1999 (GS-1, Step 1) with several different organizations (US Naval Research Laboratory (NRL), US Special Operations Command (USSOCOM), US Army Corps of Engineers (USACE))

(c) I have personally experienced the benefits and shortfalls of various modern operating systems and have the ability to create a solution that meets real world demands

2 Comparison to Existing Enterprise Platforms

2.1 RedHat Enterprise Linux

For the past several years Linux is taking over from UNIX platforms such as Oracle's Solaris, HP's HP-UX, and IBM's AIX both within the Department of Defense and in the private sector. RedHat Enterprise Linux is by far the most popular Linux distribution used within the Department of Defense, but it is still missing some of the more advanced enterprise features of the UNIX distributions that have been undergoing modern engineering (e.g., Oracle's Solaris).

Defense Enterprise Linux will leverage several key advantages of RedHat Enterprise Linux:

1. Large library of Open Source Software;
2. Tight integration of large library of software component;
3. Up-to-date development and production tools to make application developers and vendors support easier;
4. Low rate-of-change for critical components of the operating system

2.2 Oracle Solaris

Self-healing, easily debugged, well engineered.

2.3 Microsoft Windows NT

The Microsoft Windows NT family of operating systems have been traditionally undervalued by UNIX and Linux vendors and administrators. This is largely due to superficial flaws in the design, or fundamental flaws in the implementation however the fundamental design offers significant improvements over many

traditional UNIX approaches in an enterprise environment. That is to say an enterprise Linux distribution probably has the most to learn about the enterprise from Microsoft Windows NT.

Defense Enterprise Linux will incorporate many of the design goals of Microsoft Windows NT, while learning from implementation mistakes, such as:

1. Closed standards
2. Proprietary security and communications protocols
3. Poor layering of system and diagnostics tools

Some of the many advantages that Defense Enterprise Linux will incorporate from Microsoft Windows NT are:

1. Standardized API for making changes to the system configuration
   (a) Traditionally, UNIX configuration has been done by modification of configuration files while Microsoft Windows NT has had a more pragmatic database (the "registry");
   (b) Defense Enterprise Linux will implement an API that allows applications to manage configuration for any application using the same interface (just as is done with the Windows NT "registry") but will use translation guides included with each package to make the changes in the configuration files - these translation guides will likely be a significant amount of work to implement but will provide the single largest advantage for Defense Enterprise Linux over other UNIX and Linux enterprise platforms
2. Management API exposed to remote systems for standardized remote system management
3. Built-in "domain" capabilties enabled by default so that systems can be managed commonly

3 Unique Features

1. Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG) Compliant out of the box
   (a) This simply saves DoD customers time and money by ensuring that the system meets the minimum requirements during its entire life cycle.
2. Patching for compliance and not for "latest"

(a) The patching situation for most modern operating systems is relatively primitive and coarse. When new patches are released, there is very little information about the patch itself included as a part of the patch - at best whether it is a "Bugfix" or "Security Patch". This creates a system management burden when attempting to patch systems for compliance to various requirements. One must either decide which patches are needed on a per-system basis, or patch everything with the latest patches which can introduce unnecessary risk.

(b) The Defense Enterprise Linux approach is to provide a mechanism for fine control of patch metadata called "Patch Streams". Briefly, "Patch Streams" are arbitrarily defined feeds of patch requirements to be a member of that "Stream". When a new patch comes out, a Defense Enterprise Linux technician will add it to the appropriate "Patch Streams". A system can be in any number of "Patch Streams", and to be in compliance must meet the requirements of all the "Patch Streams". Some examples:

   i. An "IAVA" (Information Assurance Vulnerability Assessment) patch stream would include items that restrict the use of software that would cause the system to be vulnerable to a particular IAVA finding.

   ii. A "CVE" (Common Vulnerabilities and Exposures) patch stream would include items that restrict the use of software with known vulnerabilities

4 Market Opportunities

4.1 Investment Cost

1. Timeline:

   (a) Incubation:

      i. Month 0: $60,000 for Overhead/Startup Expenses and Retainer

      ii. Months 1-24: $10,000/mo ($240,000) for Software Development

      iii. Month 14: $150,000 for Common Criteria evaluation (EAL4+)

      iv. Month 18: $100,000 for Marketing, Test and Training Materials, and Large Scale Product Testing

   (b) Delivery

      i. Intermittent or not required

   (c) Maturity

      i. No investment funding needed, self-sufficient

4.2 Return on Investment

RedHat Inc. is predicted to have $1 billion dollars in revenue for Fiscal Year (FY) 2011. For an investment of $550,000 paid in small amounts over time to ensure that adequate progress is made minimal risk can be assured while great returns are possible.