Data Execution Prevention (DEP)

Computer attackers commonly use buffer overflow exploits to gain access to computer systems. Many of these malicious code exploits can be prevented with Data Execution Prevention (DEP), a security feature available in modern operating systems. DEP provides protection for all memory that is not specifically marked as executable code. This guide discusses how to configure and enable DEP.

Enable Hardware Support for DEP

Most personal computers sold today include hardware support for DEP. Hardware support can be enabled or disabled by a BIOS setting. It is recommended that hardware support for DEP always be enabled. BIOS settings vary depending on the manufacturer, but the DEP option can usually be found in the *Security* section. When replacing older systems it is recommended to purchase systems with hardware support for DEP.

Intel® refers to its hardware support as Execute Disable Bit (XD), and AMD™ refers to it as the No-Execute Bit (NX).

Windows® DEP Settings

On Microsoft® Windows XP SP2, Windows Server 2003™ SP1, and Windows Vista™, DEP operates in one of four possible settings: **AlwaysOn**, **OptOut**, **OptIn**, and **AlwaysOff**. It is highly recommended to configure DEP to operate in either the AlwaysOn or OptOut setting.

AlwaysOn protects all applications without exception. This is the preferred setting but is not practical where DEP-incompatible applications are necessary.

OptOut is the next best option and is the default setting for servers such as Windows Server 2003 SP1. OptOut applies DEP protection to all processes on the system except for those specified in an OptOut list.

The final two settings are *not* recommended. OptIn is the default setting on clients such as Windows XP SP2 and Windows Vista and protects only core Windows components. AlwaysOff disables DEP.

The address space layout randomization feature in Windows Vista provides further protection and compliments DEP powerfully.

Enable DEP on Windows XP SP2 and Windows Server 2003 SP1

DEP can be enabled by modifying the system's *boot.ini* file or through the Control Panel. The Control Panel cannot be used to configure the AlwaysOn or AlwaysOff setting. Both methods require Administrator privilege on the system.

To enable DEP through the *boot.ini* file, add one of the following flags to the end of each line in the **`[operating systems]`** section:

```
/noexecute=AlwaysOn
/noexecute=OptOut
```

Save the changes and reboot the system. These changes can also be made using the *bootcfg.exe* tool in Windows XP Professional.

To configure DEP using the Control Panel, launch the *System Properties* applet from the Control Panel. Select the *Advanced* tab, and then click on the *Settings* button in the *Performance* section. Click the *DEP* tab in the Performance Options window (See Figure 1). To select the OptOut setting, check the box labeled "Turn on DEP for all programs and services except those I select." The system must be rebooted before DEP protection is activated.

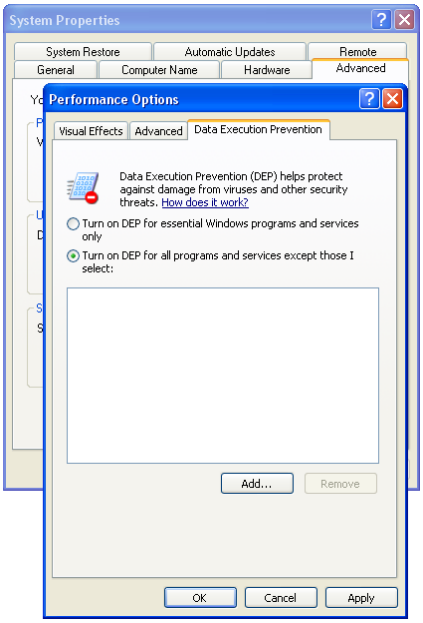

Figure 1: DEP Configuration Window

Enable DEP on Windows Vista

Windows Vista does not use a *boot.ini* file. DEP can be enabled by modifying the system's boot configuration database (BCD). To do this, execute either of the following commands from a command window with Administrator privilege, and then reboot the machine.

```
bcdedit /set nx AlwaysOn
bcdedit /set nx OptOut
```

DEP can also be enabled in the *System and Maintenance* section of the Control Panel. Click *System* → *Advanced System Settings* → *Advanced* tab → click *Settings* in the *Performance* section → *DEP* tab (See Figure 1). To select the OptOut setting, check the box labeled "Turn on DEP for all programs and services except those I select." The system must be rebooted before DEP protection is activated.

Excluding Windows Applications from DEP Protection

Some legacy applications may not run on a DEP-protected system. All enterprise applications should be tested for DEP compatibility. If the vendor cannot supply an updated DEP-compatible version, the product can be excluded from DEP protection when the OptOut setting is selected.

Microsoft's free Application Compatibility Toolkit can be used to create a Custom Compatibility Database file (*.sdb) to omit a program from DEP protection. The file can be easily deployed across an enterprise. 64-bit applications are protected by DEP by default and cannot be exempted.

Red Hat® Linux/Fedora™ Support

Red Hat Enterprise Linux™ version 3 update 3 and later, and Fedora Core 1 and later, provide DEP and address space layout randomization as part of the ExecShield feature. It is enabled by default. To verify, issue:

```
sysctl kernel.exec-shield
```

The expected output is **1**. If the output is not **1**, investigate */etc/sysctl.conf* and startup scripts, to re-enable ExecShield. ExecShield provides hardware-enforced DEP even on older systems by using the code segment limit on all x86 processors. For further protection, install the kernel-PAE package to make use of the processor's XD or NX feature.

Sun™ Solaris™ Support

Sun Solaris supports a non-executable stack on both SPARC® and XD/NX-capable x86 systems. To ensure this feature is enabled, add the following line to */etc/system*:

```
set noexec_user_stack=1
```

Apple® Mac OS® X Support

Mac OS X on Intel processors supports DEP through the processor's XD bit. It is enabled by default. To verify, issue:

```
sysctl kern.nx
```