Report Number: I743-009R-2006

NSA Windows XP Security Guide Addendum

Operational Network Vulnerability Office

Updated: Sept. 12, 2006
Version: 1.0

National Security Agency
9800 Savage Rd. Suite 6704
Ft. Meade, MD 20755-6704

XPGuides@nsa.gov

Background

As part of a change in our development strategy for security guidance, the National Security Agency is no longer maintaining and updating security guides for Windows XP Professional beyond what was produced as a cooperative effort between the vendor and the security community. The "Specialized Security – Limited Functionality" (SSLF) security settings in Microsoft's "Windows XP Security Guide" track closely with the security level historically represented in the NSA guidelines. It is our belief that this guide establishes the latest best practices for securing the product and recommend that traditional customers of our security recommendations use the Microsoft guide when securing Windows XP.

Users of NSA's original guide, "Guide to Securing Windows XP," will notice differences in security recommendations as compared to those in the Microsoft guide. Microsoft's Windows XP guide includes new security features available in Windows XP Service Pack 2 not originally addressed in NSA's guide, such as the Windows Firewall. Furthermore, NSA has worked with the vendor in assessing threat and operational constraints in addition to security issues in order to reach agreement on security recommendation guidelines**. If original NSA guidelines are currently being used and are working within the environment, there is no need to change these to match those in Microsoft's guidance unless desired.** The original "Guide to Securing Windows XP" will be archived, but no longer maintained and updated.

A Note on File and Registry Permissions:

NSA's original Windows XP guide recommended many changes to file and registry permissions. Typically, these changes were similar to the default operating system permissions, except the Everyone and Power Users groups were removed from the access control lists (ACLs).

However, NSA now believes that for Windows XP, the default file and registry ACLs are generally sufficient given the following assumptions:

- Within Group Policy or Local Security Policy, **the "Network access: Let Everyone permissions apply to anonymous users"** security option is set to be **Disabled**.
- The Power Users group has a restricted membership (preferably restricted to no members) set via Group Policy or Local Security Policy.

The Microsoft Windows XP guide's discussion on "Securing the File System," lists optional security permissions for executables located primarily within the %SystemRoot%\system32 directory, stating that these permissions should be set only if one of the above-mentioned options is not configured. However, **NSA recommends setting these permissions regardless.**