National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

Microsoft Windows 2003 Server and XP Workstation

Report Number: CCEVS-VR-07-0023
Dated: **April 1, 2007**
Version: **1.1**

National Institute of Standards and Technology
Information Technology laboratory
100 Bureau Drive
Gaithersburg, Maryland 20899

National Security agency
Information Assurance Directorate
9600 Savage Road Suite 6740
Fort George G. Meade, MD 20755-6740

Acknowledgements:

The TOE evaluation was sponsored by:

Microsoft Corporation
Corporate Headquarters
One Microsoft Way
Redmond, WA 98052-6399
USA

Evaluation Personnel:
Science Applications International Corporation (SAIC)
Common Criteria Testing Laboratory
7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046-2554

Shukrat Abbas
Tony Apted
Tammy Compton (Lead Evaluator)
Terrie Diaz
Suzanne Hamilton
Andrea Orellana
Eve Pierre
Quang Trinh
.

Validation Personnel:
Santosh Chokhani, Orion Security Solutions
Geoff Beier, Orion Security Solutions
Armen Galustyan, Orion Security Solutions
Shaun Gilmore, National Security Agency

Table of Contents

1 Executive Summary

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Microsoft Windows 2003 Server and XP Workstation. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

The evaluation of the Microsoft Windows 2003 Server and XP Workstation was performed by the SAIC Common Criteria Testing Laboratory in the United States and was completed during October 2005. The information in this report is largely derived from the Security Target (ST), Evaluation Technical Report (ETR) and associated test report. The ST was written by SAIC. The ETR and test report used in developing this validation report were written by SAIC. The evaluation team determined the product to be Part 2 Extended and Part 3 augmented, and concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL) 4 augmented with ALC_FLR.3 and AVA_VLA.4 have been met.

Windows 2003/XP is an operating system that supports both workstation and server installations. The TOE includes five product variants of Windows 2003/XP: XP Embedded, XP Professional, Server 2003 Server, Server 2003 Enterprise Server, and Server 2003 Data Center. The server products contain Domain controller features including the Active Directory, Kerberos Key Distribution Center, and Internet Information Service (IIS6) for use within the distributed Windows configuration. The Active Directory is also used by the TOE users to store and retrieve information. The discretionary access control capability and data replication capabilities of the Active Directory Service have been evaluated as part of this evaluation. Although the evaluation had no specific requirements addressing the function of the following services, all were evaluated to ensure they did not permit violations of the specific access control, information flow, or authentication policies of the TOE: Certificate Server, File Replication, Directory Replication, DNS, DHCP, Distributed File System service, Removable Storage Manager, and Virtual Disk Service.

The validation team monitored the activities of the evaluation team, participated in Technical Oversight Panel (TOP) meetings, provided guidance on technical issues and evaluation processes, reviewed successive versions of the Security Target, reviewed selected evaluation evidence, reviewed test plans, reviewed intermediate evaluation results (i.e., the CEM work units), and reviewed successive versions of the ETR and test report. The validation team determined that the evaluation team showed that the product satisfies all of the functional and assurance requirements defined in the Security Target for an EAL 4 augmented with ALC_FLR.3 and AVA_VLA.4 evaluation. Therefore the validation team concludes that the SAIC Common Criteria Testing Laboratories (CCTL) findings are accurate, and the conclusions justified.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called CCTLs or candidate CCTLs using the Common Evaluation Methodology (CEM) for EAL 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs and candidate CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	Microsoft Windows Server 2003, Standard Edition (32-bit); SP 1 (hotfixes 899587, 896422, 899588, and 907865) Microsoft Windows Server 2003, Enterprise Edition (32-bit and 64-bit versions); SP 1 (hotfixes 899587, 896422, 899588, and 907865) Microsoft Windows Server 2003, Datacenter Edition (32-bit and 64-bit versions); SP 1 (hotfixes 899587, 896422, 899588, and 907865) Microsoft Windows XP, Professional; SP 2 (hotfixes 896423, 899587, 899588, 896422, 890859, 873333, 885250, 888302, 885835, and 907865) Microsoft Windows XP, Embedded; SP 2 (hotfixes 896423, 899587, 899588, 896422, 890859, 873333, 885250, 888302, 885835, and 907865)
Security Target	Microsoft Windows 2003/XP Security Target, Version 1.0, 01 April 2007
Evaluation Technical Report	Evaluation Technical Report for Microsoft Windows 2003/XP, Version 1.0, 30 September 2005.
Conformance Result	CC Part 2 Extended, CC Part 3 augmented, EAL 4 augmented with ALC_FLR.3 and AVA_VLA.4 Compliant with Control Access Protection Profile (CAPP), Version 1.d, National Security Agency, 8 October 1999
Sponsor	Microsoft Corporation Corporate Headquarters One Microsoft Way Redmond, WA 98052-6399

Item	Identifier
Common Criteria Testing Lab (CCTL)	Science Applications International Corporation 7125 Columbia Gateway Drive, Suite 300 Columbia, MD 21046-2554
CCEVS Validator(s)	Santosh Chokhani, Geoff Beier, and Armen Galustyan Orion Security Solutions 1489 Chain Bridge Road, Suite 300 Mclean, Virginia 22101 Shaun Gilmore National Security Agency

3 TOE Security Services

The security services provided by the TOE are summarized below:

- **Security Audit** – Windows 2003/XP has the ability to collect audit data, review audit logs, protect audit logs from overflow, and restrict access to audit logs. Audit information generated by the system includes date and time of the event, user who caused the event to be generated, computer where the event occurred, and other event specific data. Authorized administrators can review audit logs.

- **Identification and Authentication** – Windows 2003/XP requires each user to be identified and authenticated (using password or smart card) prior to performing any functions. An interactive user invokes a trusted path in order to protect his identification and authentication information. Windows 2003/XP maintains a database of accounts including their identities, authentication information, group associations, and privilege and logon rights associations. Windows 2003/XP includes a set of account policy functions that include the ability to define minimum password length, number of failed logon attempts, duration of lockout, and password age.

- **Security Management** – Windows 2003/XP includes a number of functions to manage policy implementation. Policy management is controlled through a combination of access control, membership in administrator groups, and privileges.

- **User Data Protection** – Windows 2003/XP protect user data by enforcing several access control policies (discretionary access control, WEBUSER and web content provider access control) and several information flow policies (IPSec filter information flow control, Connection Firewall); and, object and subject residual information protection. Windows 2003/XP uses discretionary access control methods to allow or deny access to objects, such as files, directory entries, printers, and web content. Windows 2003/XP uses information flow control methods to control the flow of IP traffic and packets. It authorizes access to these resource objects through the use of security descriptors (which are sets of information identifying users and their specific access to resource objects), web permissions, IP filters, and port mapping rules. Windows 2003/XP also protects user data by ensuring that resources exported to user-mode processes do not have any residual information.

- **Cryptographic Protection -** Windows 2003/XP provides additional protection of data through the use of data encryption mechanisms. These mechanisms only allow authorized users access to encrypted data.

- **Protection of TOE Security Functions** – Windows 2003/XP provides a number of features to ensure the protection of TOE security functions. Windows 2003/XP protects against unauthorized data disclosure and modification by using a suite of Internet standard protocols including Internet Protocol Security (IPSEC) and Internet Security Association and Key Management Protocol (ISAKMP). Windows 2003/XP ensures process isolation security for all processes through private virtual address spaces, execution context and security context. The Windows 2003/XP data structures defining process address space, execution context, and security context are stored in protected kernel-mode memory.

    - Resource Utilization – Windows 2003/XP can limit the amount of disk space that can be used by an identified user or group on a specific disk volume. Each disk volume has a set of properties that can be changed only by a member of the administrator group. These properties allow an authorized administrator to enable quota management, specify quota thresholds, and select actions when quotas are exceeded.

    - Session Locking – Windows 2003/XP provides the ability for a user to lock their session immediately or after a defined interval. It constantly monitors the mouse and keyboard for activity and locks the workstation after a set period of inactivity. Windows 2003/XP allows an authorized administrator to configure the system to display a logon banner before the logon dialogue.

4 Assumptions

4.1 Physical Security Assumptions

- The processing resources of the TOE will be located within controlled access facilities that will prevent unauthorized physical access.
- The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

4.2 Personnel Security Assumptions

- Authorized users possess the necessary authorization to access at least some of the information managed by the TOE and are expected to act in a cooperating manner in a benign environment.
- There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
- The system administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the administrator documentation.

4.3 Connectivity Assumptions

- All connections to peripheral devices reside within the controlled access facilities. The TOE only addresses security concerns related to the manipulation of the TOE through its authorized access points. Internal communication paths to access points such as terminals are assumed to be adequately protected.
- Any other systems with which the TOE communicates are assumed to be under the same management control and operate under the same security policy constraints. The TOE is applicable to networked or distributed environments only if the entire network operates under the same constraints and resides within a single management domain. There are no security

requirements that address the need to trust external systems or the communications links to such systems.

5 Architectural Information

The diagram below depicts components and subcomponents of Windows 2003/XP that comprise the TOE. The components/subcomponents are large portions of the Windows 2003/XP OS, and generally fall along process boundaries and a few major subdivisions of the kernel mode OS.

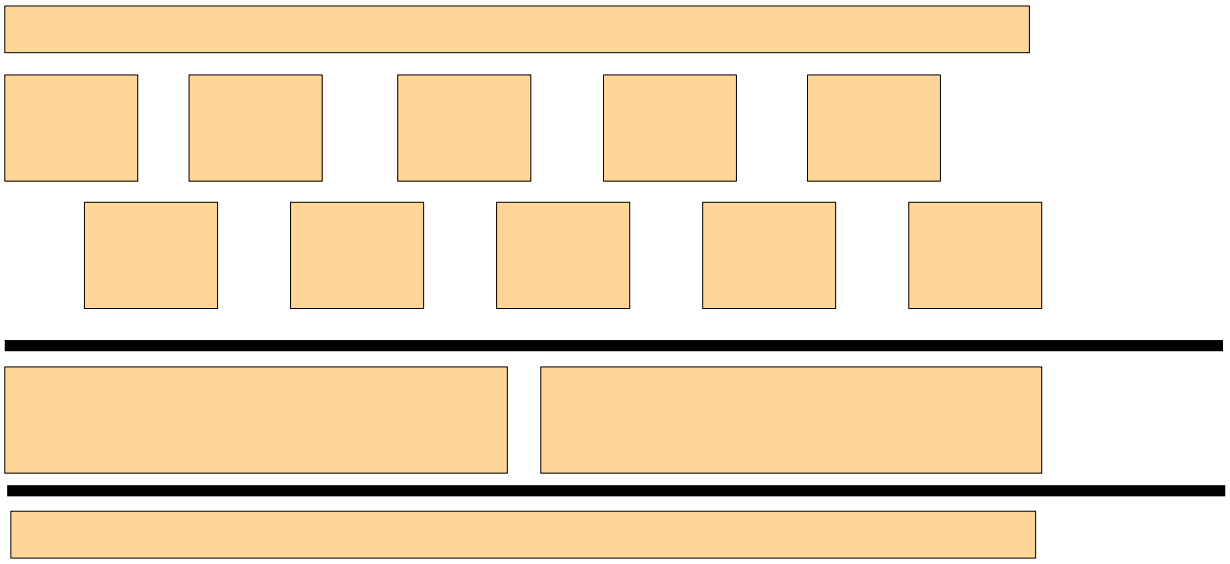

Figure 1: TOE Components

The system components are:

- Administrator Tools Module
    - Administrator Tools Component (aka GUI Component): This component represents the range of tools available to manage the security properties of the TSF.
- Certificate Services Module
    - Certificate Server Component: This component provides services related to issuing and managing public key certificates (e.g. X.509 certificates). However, no certificate server related security functions have been specified or evaluated in the TOE.
- Embedded Module
    - Embedded Component: The embedded component provides a variety of applications that facilitate the OS functioning in devices that require an embedded OS.
- Firewall Module
    - Windows Firewall Component: This component provides services related to information flow control.

Certificate Server Component

Embedded Componen

- Hardware Module
    - Hardware Component: This component includes all hardware used by the TSF to include the processor(s), motherboard and associated chip sets, controllers, and I/O devices.
- Kernel Software Module
    - Executive Component: This is the kernel-mode software that provides core OS services to include memory management, process management, and inter-process communication. This component implements all the non-I/O TSF interfaces for the kernel-mode.
    - I/O System: This is the kernel-mode software that implements all I/O related services, as well as all driver-related services. The I/O System is further divided into:
        - I/O Core Component
        - I/O File Component
        - I/O Network Component
        - I/O Devices Component
- Miscellaneous OS Support Module
    - OS Support Component: This component is a set of processes that provide various other OS support functions and services
- RPC and Network Support Module
    - Network Support Component: This component contains various support services for Remote Procedure Call (RPC), COM, and other network services.
- Security Module
    - Security Component: This component includes all security management services and functions.
- Services Module
    - Services Component: This is the component that provides many system services as well as the service controller.
- Web Services Module
    - IIS Component: This component provides services related to web/http requests.
- Win32 Module
    - Win32 Component: This component provides various support services for Win32 applications and the command console application.
- WinLogon Module
    - WinLogon Component: This component provides various interactive logon services to include interactive authentication, trusted path, session management and locking.

6 Documentation

Following is a list of the evaluation evidence, each of which was issued by the developer (and sponsor):

Assurance Class	Document Title
ASE	Microsoft Windows 2003/XP Security Target, Revision 1.0, September 28, 2005
ACM	Windows Configuration Management (CM) Manual, Version 1.9, 2 August 2005
ADO	• Windows XP and Windows Server 2003, Delivery Procedures, Version 0.2, 3 August 2005 • Windows Server 2003 Security Configuration Guide, Version 1.0, September 22, 2005 • Windows XP Professional Security Configuration Guide, Version 1.0, September 22, 2005

ADV	• System Decomposition, Rev: 5, 7/22/2005
	• Informal TOE Security Policy Model Design Specification, Rev: 7, 8/25/2005
	• Functional Specification Completeness Rationale, Rev: 5, 1/27/2005
	• API Correspondence Rules, Rev 3, 2/18/2004
	• Implementation Subset Representation
	  • Embedded: Enhanced Write Filter
	  • Executive: Security Reference Monitor *and* Object Manager
	  • Internet Information Server: Internet Information Services
	  • IO Core: Mount Manager
	  • IO Devices: IDE/ATAPI Port Driver *and* FIPS Crypto Driver
	  • IO File: NPFS Driver *and* NT File System Driver
	  • IO Network TCP/IP Protocol Driver
	  • Network Support: Domain Name Service
	  • OS Support: Session Manager
	  • Security: LSA Audit and Secondary Logon Service
	  • Services: Service Controller
	  • Win32: Client Server Runtime Process
	  • Windows Firewall Application Layer Gateway Service
	  • WinLogon: WinLogon/GINA
	• Component and Subcomponent Design Specification (see Appendix A of ETR)

AGD	• Windows Server 2003 Evaluated Configuration Administrator's Guide, Version 1.0, September 21, 2005 • Windows XP Professional Evaluated Configuration Administrator's Guide, Version 1.0, September 21, 2005 • Windows XP Professional Evaluated Configuration User's Guide, Version 1.0, September 8, 2005
ALC	• Assurance Life Cycle (ALC) for Windows 2003/XP, Version 0.2, August 2, 2005

ATE	• Test Documents
	  o ACL Test Suite, Rev 2.8, 09/01/2005
	  o Admin Access Test Suite, Rev 2.8, 09/01/2005
	  o Authentication Provider Test Suite, Rev 2.8, 09/01/2005
	  o Certificate Server Test Suite, Rev 2.8, 09/01/2005
	  o COM+ Test Suite, Rev 2.8, 09/01/2005
	  o COM+ Event System Service Test Suite, Rev 2.8, 09/01/2005
	  o DCOM Test Suite, Rev 1.7, 09/16/2005
	  o Devices Test Suite, Rev 1.3, 06/26/2005
	  o DS Replication Test Suite, Rev 1.6, 09/30/2005

Assurance Class	Document Title
	o GDI Test Suite, Rev 1.3, 06/26/2005 o Handle Enforcement Test Suite, Rev 2.9, 09/14/2005 o HTTP Client Test Suite, Rev 2.9, 09/14/2005 o IA32 Hardware Test Suite, Rev 1.4, 08/12/2005 o IA64 Hardware Test Suite, Rev 1.2, 08/12/2005 o Impersonation Test Suite, Rev 1.9, 09/14/2005 o IPSEC Test Suite, Rev 3, 08/25/2005 o KDC Test Suite, Rev 3, 08/25/2005 o LDAP Test Suite, Rev 3, 08/25/2005 o MAPI Test Suite, Rev 3, 08/25/2005 o Miscellaneous Test Suite, Rev 3, 08/25/2005 o Net Support Test Suite, Rev 1.0, 08/28/2005 o Object Reuse Test Suite, Rev 1.0, 08/28/2005 o Privilege Test Suite, Rev 2.0, Rev 1.0, 08/28/2005 o Server Driver Test Suite, Rev 0.7, 08/12/2005 o Special Access Test Suite, Rev 2.6, 09/14/2005 o Test Plan, Rev 2.2, 7/08/2005 o Token Test Suite, Rev 1.7, 08/24/2005 o User Test Suite, Rev 1.12, 09/23/2005 o Windows Firewall Test Suite, Rev 1.3, 07/22/2005 o Windows Firewall Test Suite, Rev 1.3, 07/22/2005 • GUI Tests o Active Directory Domains and Trusts GUI, Version 0.8, 09/26/05 o Auditusr.exe GUI, Version 0.2, 09/09/2005 o Backup and Restore GUI, Version 0.4, 03/22/2005 o Certification Authority GUI, Version 1.2, 09/23/05 o COM+ Apps Test Plan/Procedures, Rev. 1.0, 08/01/2005 o Date and Time GUI, Version 0.3, 09/26/2005 o Device Manager GUI, Version 0.2, 09/09/2005 o Disk Quota GUI, Version 0.2, 03/22/2005 o Event Viewer GUI, Version 1.2, 09/03/05 o Explorer GUI, Version 0.3, 09/21/2005 o IIS Mgr Test Plan/Procedures", Rev. 1.0, 9/23/2005 o Network ID GUI, Version 0.3, 09/12/2005 o OU Delegation GUI, 06/06/2005 o Printers GUI, Version 0.2, 09/22/2005 o Registry Editor GUI, Version 0.2, 03/22/2005 o Services GUI, Version 0.2, 03/22/2005 o Session Locking GUI, Version 0.3, 09/26/2005 o Share a Folder Wizard, Version 0.2, 09/08/2003 o Users and Groups GUI, Version 0.8, 09/26/2005 o WinLogon/GINA, Rev. 1.6, 09/22/2005 o Security Policy GUI, v.1.7, 08/09/2005 • Test Code for each Test Suite • Test Results as referenced by test cases
AVA	• Windows 2003/XP Misuse Analysis, Version 0.2, August 4, 2005 • Strength of Function (SOF) Support Documentation, Version 0.2, August 3, 2005 • Microsoft Windows Server 2003/XP Professional Vulnerability Analysis, Version 0.3, September 6, 2005

7 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team.

7.1 Developer Testing

The developer tested the interfaces identified in the functional specification and mapped each test to the security function tested. The scope of the developer tests included all TOE Security Functions and the entire TSF Interface (TSFI). Where testing was not possible, code analysis was used to verify the TSFI behavior. The evaluation team determined that the developer's actual test results matched the vendor's expected results. It should be noted that the TSFI testing was limited to testing security checks for the interface. The TSFI input parameters were not exercised for erroneous and anomalous inputs.

7.2 Evaluation Team Independent Testing

The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. Specifically, the evaluation team ensured that the developer test documentation sufficiently addresses the security functions as described in the security target and the TSFI as described in the Functional Specification.

The evaluation team performed a sample of the developer's test suite and devised an independent set of team tests. The evaluation team determined that the vendor's test suite was comprehensive. Thus the independent set of team tests was limited. A total of twenty (20) team tests were devised and covered the following areas: Residual Information Protection, TSF Security Functions Management, TOE Security Banners, Session Locking, Identification & Authentication, TOE Access Restriction, and Access Control on Encrypted Files.

The evaluation team confirmed that the developer's vulnerability analysis was comprehensive in terms of examining the evaluation evidence and search for vulnerabilities from public domain sources. The developer's vulnerability analysis also included examination of Microsoft Knowledge base maintained based on the security flaws reported from Microsoft internal research, external consumers, and external security research and testing organizations. The evaluation team augmented the developer's vulnerability analysis by researching and analyzing the following open sources for Windows 2003/XP vulnerabilities: CVE from http://www.cve.mitre.org Web Site.

The evaluation team also conducted twenty (20) penetration tests. The penetration tests fall in the following areas: cached logon, access to special accounts and resources, registry settings, erroneous IP packets, configuration settings, audit, Obsolete TSFI, Shatter Attack, and invalid TSFI inputs.

7.3 Highly Resistant Vulnerability Analysis

Additional testing to address the AVA_VLA.4 requirements was performed by the National Security Agency (NSA) and completed in April 2007. Using the results of the evaluation by the CCTL evaluation team, the NSA evaluation team installed the TOE evaluated configuration and conducted AVA_VLA.4 vulnerability testing. The NSA team utilized the same category of tools used by the CCTL for penetration testing, as well as in-house developed tools, which enabled the team to determine that the TOE was resistant to penetration attacks performed by attackers with high attack potential.

8 Evaluated Configuration

The evaluated configuration identified in this section was also the test configuration. The evaluation results are valid for the various realizable combinations of configurations of hardware and software listed in this section. A homogeneous Windows system consisting of various Servers, Domain Controllers, and Workstations using the various hardware and software listed in this section maintains its security rating when operated using the secure usage assumptions listed in Section 4 of this validation report, including the connectivity assumptions listed in Section 4.3 of this validation report.

TOE Hardware – The evaluation results are valid for the following hardware platforms. The TOE testing was conducted on these platforms.

- HP ProLiant DL380 G3 X2.8GHz
- HP rx2600 1.5GHz CPU Server Solution
- HP Workstation ZX2003/XP
- Dell Optiplex GX270
- Unisys ES700-420 (64-bit)
- Unisys ES7000-540-G3 (32-bit)
- Infineon SICRYPT Smart Cards
- IBM xSeries 346

TOE Software Identification – The evaluation results are valid for the following Windows Operating Systems when security updates listed in this section are applied. The TOE testing was conducted for these Operating Systems after applying the security updates listed in this section:

- Microsoft Windows Server 2003, Standard Edition (32-bit); SP 1
- Microsoft Windows Server 2003, Enterprise Edition (32-bit and 64-bit versions); SP 1
- Microsoft Windows Server 2003, Datacenter Edition (32-bit and 64-bit versions); SP 1
- Microsoft Windows XP, Professional; SP 2
- Microsoft Windows XP, Embedded; SP 2

The following security updates must be applied to the above Server products:

- MS05-042 – Vulnerabilities in Kerberos Could Allow Denial of Service (DoS), Information Disclosure, and Spoofing (899587)
- MS05-039 – Vulnerability in Plug and Play Could Allow Remote Code Execution and Elevation of Privilege (899588)
- MS05-027 – Vulnerability in Server Message Block (SMB) Could Allow Remote Code Execution (896422)
- A hotfix that updates the IPSec Policy Agent is available for Windows Server 2003 and Windows XP (907865)

The following security updates must be applied to the above XP products:

- MS05-043 – Vulnerability in Print Spooler Service Could Allow Remote Code Execution (896423)
- MS05-042 – Vulnerabilities in Kerberos Could Allow DoS, Information Disclosure, and Spoofing (899587)

- MS05-039 – Vulnerability in Plug and Play Could Allow Remote Code Execution and Elevation of Privilege (899588)
- MS05-027 – Vulnerability in SMB Could Allow Remote Code Execution (896422)
- MS05-018 – Vulnerability in Windows Kernel Could Allow Elevation of Privilege and DoS (890859)
- MS05-012 – Vulnerability in Object Linking and Embedding (OLE) and Component Object Model (COM) Could Allow Remote Code Execution (873333)
- MS05-011 – Vulnerability in SMB Could Allow Remote Code Execution (885250)
- MS05-007 – Vulnerability in Windows Could Allow Information Disclosure (888302)
- MS04-044 – Vulnerabilities in Windows Kernel and Local Security Authority Subsystem Service (LSASS) Could Allow Elevation of Privilege (885835)
- MS07-006: Vulnerability in Windows Shell Could Allow Elevation of Privilege (928255)
- MS07-007: Vulnerability in Windows Image Acquisition Service Could Allow Elevation of Privilege (27802)
- A hotfix that updates the IPSec Policy Agent is available for Windows Server 2003 and Windows XP (907865)

9 Validator Comments

The TOE developer and sponsor, and the Evaluation Team are commended for their effort to develop tests for such a complex system. The Evaluation Team is commended for their painstaking efforts to validate the evaluated configuration during team testing.

The security functional testing activities were limited to verifying that the security checks at each TSFI are enforced. The TSFI input parameters were not exercised for erroneous and anomalous inputs during security functional testing or during penetration testing.

While no specific security functional requirements or TSFI are listed for the following components of the TOE, the TOE was not evaluated in the following areas and is known to be not compliant with applicable standards and hence can cause security and interoperability problems:

- The Microsoft Cryptographic Applications Programming Interface (CAPI) does not perform X.509 certification path validation in accordance with applicable ISO and Internet standards.

- The Internet Information Server (IIS) Transport Layer Security (TLS) and Secure Socket Layer (SSL) do not perform X.509 certification path validation for client authentication in accordance with applicable ISO and Internet standards

10 Security Target

See Table 1 in this validation report.

11 List of Acronyms

ACM	Configuration Management (Assurance Class)
ADO	Delivery and Operations (Assurance Class)
ADV	TOE Development (Assurance Class)
AGD	Guidance Document (Assurance Class)
ALC	Life Cycle (Assurance Class)
API	Application Programming Interface
ASE	ST Evaluation (Assurance Class)
ATE	TOE Testing (Assurance Class)
AVA	Vulnerability Analysis (Assurance Class)
CAPI	Cryptographic **API**
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme (US CC Validation Scheme)
CCIMB	Common Criteria Implementation Board
CCTL	Common Criteria Testing laboratory
CEM	Common Evaluation Methodology
COM	Component Object Model
DHCP	Dynamic Host Control Protocol
DNS	Domain Name Service
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standard
FLR	Flaw Remediation
GUI	Graphic User Interface
HP	Hewlett Packard
I/O	Input/Output
IBM	International Business Machine
IIS	Internet Information Service
IPSEC	Internet Protocol Security
ISAKMP	Internet Security Association and Key Management Protocol
ISO	International Organization for Standards
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
OS	Operating System
RPC	Remote Procedure Call
SAIC	Science Application International Corporation
SSL	Secure Socket Layer
ST	Security Target

TLS	Transport Layer Security
TOE	Target Of Evaluation
TOP	Technical Oversight Panel
TSF	**TOE** Security Function
TSFI	**TSF** Interface
URL	Universal Resource Locator
VR	Validation Report

.

12 Bibliography

The validation team used the following documents to prepare the validation report.

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated January 2004, Version 2.2.

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated January 2004, Version 2.2.

[3] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated January 2004, Version 2.2.

[4] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated January 2004, Version 2.2.

[5] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated January 2004, Version 2.2.

[6] Common Evaluation Methodology for Information Technology Security, dated January 2004, Version 2.2.

[7] Final Evaluation Technical Report for Windows 2003/XP Product, Version 1.0, September 30, 2005.

[8] Microsoft Windows 2003/XP Security Target, V 1.0, September 28, 2005.

[9] Common Criteria Evaluation and Validation Scheme for IT Security, *Guidance to Validators of IT Security Evaluations*. Scheme Publication # 3, Version 1.0, January 2002.

[10] Evaluation Team Test Plan for Microsoft Windows 2003/XP, Version 3.0, September 30, 2005

13 Interpretations

13.1 International Interpretations

The evaluation team performed an analysis of the international interpretations and identified those that are applicable and had impact to the TOE evaluation. The table summarizes the set of interpretations determined to have an impact on the evaluation and identifies the impact.

Impact on Security Target Requirement	Impact on ETR Work Unit	Interpretation Identification (ID)
New element added after ACM_CAP.3.3C		RI-3
ACM_SCP.1.1D and ACM_SCP.1.1C changed		RI-4
	ASE_OBJ.1.2C and ASE_OBJ.1.3C changed (no work unit change indicated)	RI-43
ADO_IGS.1.1C and AVA_VLA.1.1 – 1.3C changed		RI-51
FMT_SMF.1 introduced		RI-65
	ASE_REQ.1-20 work unit changed	RI-84
	ASE_REQ.1.10C (ASE_REQ.1-16 work unit changed)	RI-85
FDP_ACF.1 changed		RI-103
FIA_USB.1 changed		RI-137
	ADO_DEL.1-2 work unit deleted	RI-116
FAU_STG.1 changed		RI-141
FMT_REV.1 changed		RI-201
FAU_GEN.1 changed		RI-202
	All portions of the CC and CEM should be considered "Normative" unless specifically denoted as "Informative.	RI-222

13.2 NIAP Interpretations

Neither the ST nor the vendor's evidence identified any National interpretations. As a result, since National interpretations are optional, the evaluation team did not consider any National interpretations as part of its evaluation.

13.3 Interpretations Validation

The Validation Team concluded that the Evaluation Team correctly addressed the interpretations that it identified.