National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

Microsoft Corporation
Windows 2000

Report Number: CCEVS-VR-02-0025

Dated: 25 October 2002

Version: 2.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Aerospace Corporation

Columbia, Maryland

Common Criteria Testing Laboratory

Science Application International Corporation

Columbia, Maryland

Table of Contents

1. EXECUTIVE SUMMARY

This report documents the NIAP validators' assessment of the evaluation of Microsoft Corporation Windows 2000 operating system. It presents the evaluation results, their justifications, and the conformance results. This validation report is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

The evaluation was performed by SAIC, and was completed during October 2002. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, both written by SAIC. The evaluation determined the product to be **Part 2 conformant, Part 3 conformant,** and to meet the requirements of **EAL 4**, augmented with ALC_FLR.3 (Systematic Flaw Remediation). Additionally, the product was found to be conformant to the *Controlled Access Protection Profile* (CAPP), Version 1.d, October 8, 1999.

The Windows 2000 operating system is a general-purpose, distributed operating system. It supports networked operations and provides controlled access protection (traditionally referred to as *discretionary access control,* or DAC) between subjects (i.e., user processes) and objects (e.g., data and system resources). It provides a number of security and security-relevant services, such as support for VPN, encryption of user data, and single logon capability.

In terms of what is required by the CAPP, the primary security features of the Windows 2000 operating system are:

- Fundamental protection mechanisms for multiple domains of execution, virtualization of memory, and separation of process address spaces;
- Extensive and flexible access controls;
- Auditing of user actions;
- Support for roles;
- Trusted path;
- Extensive security management capabilities.

User profiles are maintained in a globally-accessible database (i.e., Active Directory) such that users possess the same identity, access authorizations, and capabilities regardless of where they logon in the network. The global user database also provides a single focus for security management actions.

The validation team monitored the activities of the evaluation team, participated in team 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 showed that the product satisfies all of the functional requirements and assurance requirements defined in the Security Target (ST) and is conformant with the requirements of the CAPP. Therefore, the validation team concludes that the SAIC findings are accurate, the conclusions justified, and the conformance claims correct.

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 Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (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 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 evaluation. Upon successful completion of the evaluation, the product is added to 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 Protection Profile to which the product is conformant;
- 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 2000 Operating System
Protection Profile	Controlled Access Protection Profile, V1.d, 8 October 1999
Security Target	*Windows 2000 Security Target;* Version 2.0, 18 October 2002
Evaluation Technical Report	*Evaluation Technical Report for the Windows 2000 Product;* Version 1.0, October 4 2002
Conformance Result	Part 2 conformant, Part 3 conformant, EAL 4 augmented (ALC_FLR.3)
Sponsor	Microsoft Corporation
Developer	Microsoft Corporation
Evaluators	SAIC
Validators	The Aerospace Corporation

3. SECURITY POLICY

The Windows 2000 product enforces the following security policies:

1.1 Role Differentiation Policy.

The Windows 2000 product provides several pre-defined administrative groups; the Administrator role is defined as any user account that is assigned any of the security-relevant privileges or is made a member of one of these pre-defined administrative groups (e.g., Administrators).

More generally; a role is realized by assigning group accounts and privileges to a given user account. Windows 2000 provides a number of policies and security features that require appropriate management (see below); the control of these management functions is accomplished by creating user accounts with the appropriate authorizations and/or privileges. In general, an arbitrary set of roles can be defined through the association of the requisite authorizations and privileges with the desired user accounts.

1.2 Identification and Authentication Policy.

Each user must be identified and authenticated prior to being able to perform any TSF-mediated functions. Four types of logon are provided:

- interactive—logon to the local machine
- network—logon to a machine remotely; from elsewhere in the network
- batch—logon as a batch job; intended for batch servers
- service—logon as a service

Each of the logon types has a corresponding user logon right that can be assigned to user and group accounts. This provides control over the logon methods available to specific users.

For the initial interactive logon, a trusted path must be invoked. This ensures the protection of identification and authentication information.

1.3 Audit Policy

Windows 2000 supports the collection of audit data, provides for the review and management of audit logs by an authorized administrator, and implements mechanisms that prevent loss of audit data due to overflow of the audit logs. The access control mechanisms limit access to the audit data only to authorized administrators. Audit logs include date and time of the event, user on whose behalf the event occurred, the specific computer in the network on which the event occurred, as well as other event-specific data.

1.4 Access Control Policy

Windows 2000 implements a *Discretionary Access Control (DAC)* policy; the TSF mediates access between subjects (user processes) and named objects (system resources and data objects). Access decisions are made by comparing the attributes associated with the requesting user and the attributes associated with the object being accessed. User attributes include a security identifier (SID) for the user, identifiers for any groups to which the user is a member, and privileges associated with the user. Object attributes include the SID for the owner and, optionally, an access control list that contains the access authorizations for each user or group that may access the object.[1] Access to an object may be explicitly granted or denied at the granularity of specific users or user groups.

An additional access control check is made when a user chooses to utilize the optional encryption capability for NTFS file objects. If a file is encrypted, Windows 2000 performs additional checks to those described above; the encrypted file will be made available only to users who possess a valid decryption key for the file.

1.5 Security Management

The Windows 2000 product provides security management functions for the following security policies and features:

- Audit policy—enable/disable auditing, management of the audit database, and definition of audit parameters and events;
- Account policy—define password constraints and characteristics, account lockout parameters, and Kerberos key usage parameters;
- Account database—define, assign, or remove security attributes for user and group accounts, both locally and for a domain;
- User rights policy—manage the association of user and group accounts with logon rights and privileges;
- Domain policy—manage the association of specific computers with domains, and manage the trust relationships among domains;
- Group policy—define accounts, user rights, system security settings for a group of TSFs or accounts within a domain;
- IPSEC policy—define whether and how IPSEC will be used to protect communications among distributed machines.
- Encrypted file system (EFS) policy—enable or disable EFS on an NTFS volume;
- Disk quota—manage and define parameters for disk quotas for NTFS volumes.

[1] The set of access control parameters associated with subjects and objects is fairly extensive, and the access control mechanism is reasonable flexible. A more detailed and complete a description is provided in the Security Target for this product.

4. ASSUMPTIONS

1.6 Usage Assumptions

The system is expected to be used in what has traditionally been known as “a relatively benign environment.” That is, all the information on the system is at the same level of sensitivity, all users are authorized for that level of information (although do not necessarily have access to all the data). However, users are not expected to be trustworthy; they may make attempts to bypass system security controls or otherwise exceed their authorizations to data and system resources.

Administrators are assumed to be trusted (i.e., non-malicious) and competent to carry out their responsibilities.

For networked or distributed operations, it is assumed that all elements of the network operate under the same security rules and constraints and are subsumed under a single management domain.

1.7 Environmental Assumptions

The system is presumed to be located within controlled facilities such that physical access to workstations and/or servers is limited only to those allowed to access the system.

Additionally, it is presumed that all connections to peripheral devices are within the controlled facilities, and that the communications paths are adequately protected.

5. ARCHITECTURAL INFORMATION

Windows 2000 runs on a hardware base that provides at least two domains of execution—user-mode and executive-mode[2] (in the Windows 2000 product it is the kernel-mode processes that execute in the privileged[3], or “executive mode.”). Additionally, the system provides virtualization of memory, and separation of address spaces for user-mode processes. These mechanisms provide isolation of user-mode processes from each other.

The system architecture is layered; running on the hardware is the kernel-mode software, consisting of the Executive and Primitive Kernel Component and the I/O component[4]. Above the kernel-mode software is the user-mode software that includes the Security Process Component, Winlogon Process Component, and Administrator GUI, as well as components for Win32 applications and network support. These components execute in the hardware state that is the user-mode domain.

[2] The complete list of hardware bases that are included in the evaluation is provided in the Security Target

[3] Unfortunately, the term “privilege” has been used in several ways in computer systems. As used here it refers to the scope of execution of processes rather than the authorizations (or “privileges”) that can be assigned to them by an administrator. That is, processes that execute in kernel-mode can typically access all of memory and execute instructions that are normally unavailable to processes executing in the user-mode domain.

[4] The I/O component includes the networking as well as the device sub-components.

Each workstation or server consists of an Intel X86 machine (or equivalent processor) with, possibly, up to eight processors (for the Advanced Server product). A set of devices may be attached:

- Monitor
- Keyboard
- Mouse
- Floppy disk drive
- CD_ROM drive
- Fixed disk drives
- Printer
- Audio adaptor
- Network adaptor

6. DOCUMENTATION

The following product documentation is provided to consumers:

- Windows 2000 Security Configuration Guidance Document, Version 1.0, dated 10/04/02
- Windows 2000 Administrative Guidance Document, Version 1.0, dated 10/04/02
- Windows 2000 User's Guidance Document, Version 1.0, dated 10/04/02

During the course of the evaluation, the CCTL had access to an extensive amount of documentation and evidence[5], covering:

- Design details and system internals;
- Configuration management and lifecycle documentation;
- Delivery procedures and operation guidance;
- Vendor test plans and configurations, test suites, and test results;
- Vulnerability assessment documentation and strength of function analyses;
- Security Target

7. IT PRODUCT TESTING

1.8 Developer Testing

The developer's approach to security testing is essentially focused on the testing of the interfaces. For each TFSI, security checks and effects are identified, and tests devised for each. Test documentation includes a high-level test plan that describes the philosophy of testing, and provides a mapping between the system components and specific test suites.

[5] A complete list of the documentation used during the evaluation is included in Section 8 of the *Evaluation Technical Report for the Windows 2000 Product, Part 1 (Non-Proprietary)*, Version 1.0, October 4 2002.

The developer testing is extensive, including, but not limited to, tests for:

- Use of tokens
- Privileges
- Object reuse (i.e., FDP_RIP requirement)
- Ipsec
- Access control
- Authentication
- Security policy GUI
- Security configuration Editor GUI
- Device Manager GUI
- Session locking GUI

The evaluation team concluded that for the vast majority of interfaces test procedures had been defined to directly invoke the interface and test the security functions and/or effects. In cases for which interfaces could not be tested directly, procedures were devised to test the interface indirectly; for example, by testing the low-level function upon which the interface built.

Each of the developer's functional test suites includes a high-level design document that describes the intent of the test suite, the APIs addressed, the testing approach (including expected test results), any special considerations, and instructions for using the test suite.

1.9 Evaluator Testing

Prior to testing, the evaluation team verified that the TOE was as identified in the ST, and then proceeded to install and configure the TOE as described in the installation guide. The following configurations were installed:

- Domain controller;
- Server in a domain
- Stand-alone Server;
- Windows 2000 Professional workstation (as a member of a domain);
- Stand-alone Windows 2000 Professional workstation.

The entire automated test suite was executed on each of these configurations.

The developer's manual test suite was also executed. For these, each test was run on only one of the configurations, although several configurations were used during testing in order to obtain representative samples.

The evaluation team also devised a set of independent tests, in part covering areas that were felt to be missing from, or inadequately covered by the developer's test suites. The evaluation team's conclusion is that between team and vendor testing, the entire TSF is addressed.

8. EVALUATED CONFIGURATION

The evaluated configurations of this product were Windows 2000 Server, Advanced Server, and Professional, each with Service Pack 3 and Q326886 Hotfix. The hardware base, as indicated above, is any of the identified Intel X86 (or equivalent) processors.

9. RESULTS OF THE EVALUATION[6]

The evaluation determined the product to be **Part 2 conformant, Part 3 conformant,** and to meet the requirements of **EAL 4**, augmented with ALC_FLR.3. Additionally, the product is conformant to the *Controlled Access Protection Profile (CAPP)*, Version 1.d, 8 October 1999. This implies that the product satisfies the security technical requirements specified in *Windows 2000 Security Target, Version 2.0*, 18 October 2002.

10. EVALUATOR COMMENTS

There are no Evaluator Comments.

11. SECURITY TARGET

The ST, *Windows 2000 Security Target;* Version 2.0, 18 October 2002 is included here by reference.

[6] The terminology in this section is defined in CC Interpretation 008, specifying new language for CC Part 1, section/Clause 5.4.

12. GLOSSARY

CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Evaluation Testing Laboratory
CEM	Common Evaluation Methodology
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards & Technology
NSA	National Security Agency
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
TSFI	TOE Security Function Interface

13. BIBLIOGRAPHY

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 1999, Version 2.1.

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 1999, Version 2.1.

[3] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated August 1999, Version 2.1.

[4] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 1999, Version 2.1.

[5] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated 1 November 1998, version 0.6.

[6] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated August 1999, version 1.0.

[7] Windows 2000 Security Target, Version 2.0, dated 18 October 2002.

[8] Controlled Access Protection Profile, Version 1.d, 8 October 1999.

[9] Evaluation Technical Report, for the Windows 2000 Product, Part 1, Version 1.0, October 4 2002.

[10] Evaluation Technical Report, for the Windows 2000 Product, Part 2 (Proprietary), Version 1.0, October 4 2002.

[11] Evaluation Team Test Plan for the Windows 2000 Product, ETR Part 2 Supplement (Proprietary), Version 1.0, October 4 2002.

APPENDIX

Relevant Decisions

Although there were several Observation Reports (ORs) that were raised during the course of the evaluation, two in particular had visible impact on the issue of conformance with the *Controlled Access Protection Profile* (CAPP), and thus deserve to be summarized.

A.1 The Audit Issue:

The CAPP requirements for audit capabilities include both FAU_SAR.3 and FAU_SEL.1, although the ST for the Windows 2000 product identifies the FAU_SAR.3 requirement as the one that is satisfied; the capabilities defined in the FAU_SEL.1 requirement are not provided by the product.

Both FAU_SAR.3 and FAU_SEL.1 deal with the issue of how desired audit events are collected and made available to the audit administrator. Traditionally, one of two methods have been acceptable:

- Collect all auditable events, and employ database processing tools (e.g., sorts, searches) to display those events that are of interest. This is referred to as *post-selection*, and is captured in FAU_SAR.3.
- Implement a filter that allows the audit administrator to capture only the auditable events that are of interest. This is referred to as *pre-selection*, and is captured in FAU_SEL.1. This approach has traditionally been taken where the storage for audit records is limited.

The vendor and the CCTL raised the issue of having to implement both techniques in the product; this is what a strict reading of the CAPP would require.

The decision was that the intent of the CAPP was to require either—but not necessarily both—of the audit selectivity approaches. The CAPP authors had included both auditing techniques with the intent that they be understood as "either/or" choices. However, the formats for CC specifications (i.e., PPs and STs) do not provide the vocabulary for either/or choices. In short, the decision was that only one of the approaches need be implemented, and that satisfying either of the requirements was sufficient for conformance with the CAPP.

The full text of this decision may be found in the NIAP Precedent Database at http://niap.nist.gov/cc-scheme/PD/0067.html.

A.2 Abstract Machine Testing

The CAPP includes the requirement FPT_AMT.1 (Abstract Machine Testing), which does not appear in the ST for the Windows 2000 product.

The wording of FPT_AMT.1 is such as to require testing to "demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF." The intent of the requirement is that mechanisms be implemented to verify that any assumptions about properties (e.g., correct operation) of any abstract machine (e.g., operating system, hardware) upon which the TSF depended. This provides assurance that the TSF, in turn, is providing the security attributes and capabilities that are defined in the ST.

However FPT.AMT.1 presumes that the underlying hardware on which the TSF runs is not part of the TOE, but part of its environment. As such, the vendor and CCTL argued that this requirement did not apply because the TOE included the hardware, and thus there was no “abstract machine” upon which the product depended. After considerable discussion, NIAP eventually agreed with the vendor position; the FMT_AMT.1 requirement was considered to be satisfied.

The full text of this decision may be found in the NIAP Precedent Database at http://niap.nist.gov/cc-scheme/PD/0069.html.