National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Common Criteria Evaluation and Validation Scheme
Validation Report

BAE Systems Information Technology, LLC

XTS-400 / STOP 6.1.E

Report Number: CCEVS-VR-05-0094
Dated: 1 March 2005

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

Dr. Jerome Myers
The Aerospace Corporation
Columbia, Maryland

Margaret T. Webster-Butler
National Security Agency
Linthicum, Maryland

Common Criteria Testing Laboratory
CygnaCom Solutions
McLean, Virginia 22102-3350

Table of Contents

1 EXECUTIVE SUMMARY

This report documents the NIAP Validators' assessment of the CCEVS evaluation of BAE – IT's XTS-400™/ STOP™ 6.1.E, a multilevel secure operating system based upon a BAE - IT-supplied x86 hardware base, at EAL5 augmented with ALC_FLR.3 and ATE_IND.3. It presents the evaluation results, their justifications, and the conformance result.

The evaluation was performed by CygnaCom Solutions, McLean Virginia, with supplemental support for the vulnerability analysis by the National Security Agency and was completed 1 March, 2005. The information in this report is largely derived from an Evaluation Technical Report (ETR) held by the NSA which combines a proprietary ETR written by CygnaCom with a proprietary NSA report documenting the vulnerability analysis. The combined evaluation determined that the product conforms to the CC Version 2.1, Part 2, and Part 3 to meet the requirements of Evaluation Assurance Level (EAL) 5 augmented with ALC_FLR.3, Systematic Flaw Remediation, and ATE_IND.3, Independent Testing - Complete, resulting in a "pass" in accordance with CC Part 1 paragraph 175. The evaluation determined that the product conformed to the *Labeled Security Protection Profile (Version 1.b)* [12] and the *Controlled Access Protection Profile (Version 1.d)* [9].

The XTS-400 product is a combination of STOP revision 6.1.E, a multilevel secure operating system, and a BAE - IT-supplied x86 hardware base. STOP is a 32-bit, multiprogramming, multi-tasking, operating system that can support multiple concurrent users. In addition to proprietary interfaces for secure administration, STOP provides a Linux®-like user environment and programming interface (API/ABI) that allows many programs written for Linux to be copied to the XTS and run without change while benefiting from the designed-in security STOP and the XTS-400 provide.

An X-windows graphical user interface (GUI) is included within the Target of Evaluation and is available at the console for work by untrusted users. Trusted path initiation causes suspension of the GUI and trusted commands can not be run from the GUI. All windows on the display are at the same level and multi-level cut-and-paste is not supported.

Network connectivity on up to 16 different networks is allowed in the evaluated configuration. TCP/IP and Ethernet are included in the TOE, but not network servers (e.g., SMTP). Within an evaluated configuration, network attachments must be made according to rules in the Trusted Facility Manual (e.g., the network must be single-level while multiple networks can each be at a different level). The TOE can not be

compromised by remote users or unusual network traffic, but the TOE itself does not prevent disclosure of (or loss of integrity by) data on the network.

The system provides mandatory access control that allows for both a security and integrity policy. It provides 16 hierarchical sensitivity levels, 64 non-hierarchical sensitivity categories, eight hierarchical integrity levels, and 16 non-hierarchical integrity categories. The mandatory security policy (MAC) enforced by the XTS-400 is based on the (formal) Bell and LaPadula security model; the mandatory integrity policy (MIC) is based on the (formal) Biba integrity model. The system implements discretionary access control (DAC) and provides for user identification and authentication needed for user ID-based policy enforcement.

Individual accountability is provided with an auditing capability. Data scavenging is prevented through residual data protection mechanisms. A trusted path mechanism is provided by the implementation of a Secure Attention Key (SAK) which provides trusted communications between users and the system.

The separation of administrator and operator roles is enforced using the integrity policy. The system enforces the "principle of least privilege" (i.e., users should have no more authorization than that required to perform their functions) for administrator and operator roles. All actions performed by privileged (and normal) users can be audited. The audit log is protected from modification using integrity and subtype mechanisms. STOP also provides an alarm mechanism to detect the accumulation of events that indicate an imminent violation of the security policy.

STOP was designed from the ground up with strong internal architectural characteristics (minimization, modularization, layering, and data hiding) to resist penetration and minimize the chance of bugs. STOP uses hardware privilege level and memory protection mechanisms to protect itself from tampering and to isolate processes from one another. XTS-400/STOP 6.1.E is the most recently evaluated descendant in a chain of products that began with the Secure Communications Processor (SCOMP) and evolved sequentially into XTS-200, XTS-300, STOP 3.1.E, STOP 3.2.E, STOP 4.1, and STOP 5.2.E. Each of those predecessors was evaluated under the U.S. Trusted Product Evaluation Program with the SCOMP receiving an A1 rating in 1984 and the subsequent systems receiving B3 ratings. The XTS-400 and STOP 6.0.E received an EAL4 Augmented evaluation in March of 2004.

STOP consists of the TSF software and a body of untrusted application code and commands. The XTS-400/STOP TSF consists of the hardware and four major software components:

- the Security Kernel, which operates in the most privileged domain and provides all mandatory, subtype, and a portion of the discretionary, access control;
- the TSF System Services, which operate in the next-most-privileged domain, and implement a hierarchical file system, supports user I/O, and implements the remaining discretionary access control;
- Operating System Services (OSS), which operates in a less privileged domain and provides the Linux-like interfaces; and
- Trusted Software, which provides the remaining security services and user commands.

The XTS-400 is available on Intel Pentium (PIII) and Xeon (P4) based server class systems, available in tower, and rack-mount chassis. All components are commercial-off-the-shelf (COTS). The XTS-400 uses specific Intel-brand motherboards and industry standard ISA or PCI peripheral cards or chips built into the motherboard. Additional hardware components may be optionally included in the evaluated configurations.

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 desire 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 CCEVS' 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

Evaluation Identifiers for BAE - IT XTS-400 / STOP 6.1.E	
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	BAE - IT XTS-400/STOP 6.1.E
Protection Profile	Labeled Security Protection Profile (Version 1.b) [12] and the Controlled Access Protection Profile (Version 1.d)[9]
Security Target	BAE - IT XTS-400 Version 6 Common Criteria Security Target, Version 1.11, December 2004
Evaluation Technical Report	Evaluation Technical Report (ETR) for a Target of BAE - IT XTS-400 Version 6.1.E, dated Sept 24, 2004 [11] and XTS-400/STOP 6.1.E Vulnerability Assessment ETR, dated 1 March 2005 [14]
Conformance Result	Part 2 conformant, Part 3 conformant, and EAL5 augmented with ALC_FLR.3, Systematic Flaw

Evaluation Identifiers for BAE - IT XTS-400 / STOP 6.1.E	
	Remediation and ATE_IND.3, Independent Testing – Complete.
Version of CC	CC Version 2.1 [1], [2], [3], [4] and all applicable NIAP CCEVS and International Interpretations effective on March 1, 2003
Version of CEM	CEM Version 1.0 [5], [6], Supplement: ALC_FLR - Flaw Remediation [13], and all applicable NIAP CCEVS and International Interpretations effective on March 1, 2003
Sponsor	BAE - IT Government Solutions, LLC 2525 Network Place Herndon, VA 22171
Developer	BAE - IT Government Solutions, LLC 2525 Network Place Herndon, VA 20171
Evaluator(s)	**CygnaCom Solutions** Debra Baker Elise Berger Peter Kukura Herb Markle Jean Petty **National Security Agency**
Validator(s)	**NIAP CCEVS** Dr. Jerome Myers Margaret T. Webster-Butler

3 Security Policy

The TOE is the XTS-400™ product, which is a combination of STOP™ revision 6.1.E (a multilevel secure operating system), and a BAE - IT-supplied x86 hardware base. The STOP™ is a 32-bit, multiprogramming, multi-tasking, operating system that provides these features:

- Associate sensitivity labels with all objects and all its users will have an associated clearance level identifying the maximum security level of data that they may access;
- Allow simultaneous use of the system by multiple users, all with different clearances and needs-to-know;
- Allow simultaneous network connectivity to networks of differing sensitivities/classifications;
- Mandatory integrity protection of files;
- An untrusted operating environment that includes common Linux commands and tools;
- An Application Programming Interface/Application Binary Interface which is suitable for running most Linux applications in their binary format (no recompilation required).

The TOE implements the following security policies.

3.1 Identification and Authentication Policy

The TSF ensures that each user is uniquely identified and authenticated prior to being able to perform any TSF-mediated functions. The identification and authentication policy ensures that sufficient information is available for the TOE to bind user attributes (e.g. sensitivity clearance, role, integrity level) to user sessions for the purpose of implementing the other security policies described below. The identification and authentication policy also enforces a lockout policy that locks out users based upon an administratively specified number of failed login attempts.

3.2 Mandatory Access Control Policy

The TSF implements a Bell-LaPadula style Mandatory Access Control (MAC) based on user clearance (level and category(ies)) of the subject and classification (level and category(ies)) of the object. The MAC policy is enforced over all identified system resources (i.e., subjects, storage objects, and I/O devices) that are accessible, either directly or indirectly, to subjects external to the TSF. The TSF provides 16 hierarchical sensitivity levels and 64 non-hierarchical sensitivity categories. The combination of mandatory sensitivity hierarchical and non-hierarchical levels is called the *Mandatory Access Control (MAC) label*.)

The TOE provides a *dominates* function that is used to compare sensitivity labels; this comparison is done whenever a subject external to the TSF accesses an object. Every user has an identification and authentication database record that specifies the MAC

label of the user's clearance. The TSF enforces the restriction that any subject created on behalf of a user has a current MAC label dominated by the user's clearance.

The kinds of access that are relevant are read and write – execute is considered the same as read. The MAC level of processes and some objects can not be modified. Only administrators can change the MAC level of an object, except that a user (who has been granted an appropriate capability) can change the level of objects that s/he owns. A MAC level change to an object will take effect immediately, even if that means denying access to the object by a process which already has the object "open".

Mandatory security control is used internally by the TSF to prevent viewing of sensitive TSF data, including the audit trail and authentication data.

3.3 Mandatory Integrity Control Policy

The TOE implements a Biba style Mandatory Integrity Control (MIC) Policy which enforces an integrity policy on all authorized users and TOE resources to prevent malicious entities from corrupting data. The TOE provides 8 hierarchical integrity levels and non-hierarchical integrity categories. The combination of mandatory integrity hierarchical and non-hierarchical levels is called the *Mandatory Integrity Control (MIC) label*. Some of the hierarchical integrity levels are used by the system to provide role separation, and the others are available to users.

The MIC is based on user clearance, user integrity level of the subject, and integrity level of the object. The TSF enforces a MIC policy over all identified system resources (i.e., subjects, storage objects, and I/O devices) that are accessible, either directly or indirectly, to subjects external to the TSF. The TOE provides a *dominates* function that is used to compare integrity labels; this comparison is done whenever a subject external to the TSF accesses an object. Every user has an identification and authentication database record that specifies the MIC label of the user's clearance. The TSF enforces the restriction that any subject created on behalf of a user has a current MIC label that dominates the user's MIC clearance.

The types of access that are relevant are read and write – execute is considered the same as read. The MIC level of processes and some objects can not be modified. Only administrators can change the MIC level of an object, except that a user (who has been granted an appropriate capability) can change the level of objects that s/he owns. A MIC level change to an object will take effect immediately, even if that means denying access to the object by a process which already has the object "open".

Mandatory integrity control is used internally by the TSF to prevent modification or deletion of TSF data, including the audit trail and configuration parameters for "alarm" mechanisms (such as low disk space, low audit trail space, excessive failed login attempts).

3.4 Discretionary Access Control Policy

The TOE implements a Discretionary Access Control Policy (DAC) which restricts access to objects based on the identity of subjects and/or groups to which they belong, and allows authorized user to specify protection for objects that they control;

The TOE allows owning users to define and control access to named objects through the use of an Access Control List (ACL). Every subject has associated with it an effective user and group; every named object has an ACL. Each ACL contains permissions that specify the allowable access for the owning user, the owning group, up to seven other user or groups, and any user or group not explicitly listed. These permissions can either grant or deny a particular form of access to a named object. When a subject introduces an object into its address space, the ACL is checked to ensure that the subject can access the object.

The types of access that are controlled are read, write, and execute. Write does not imply the ability to delete and some objects cannot be executed.

Only administrators can introduce new users and groups to the system, establish the group membership of users, or set the default group for users. Normal users can change the discretionary attributes of only the objects they own, but administrators can change the attributes of any object.

3.5 Audit Policy

The TOE implements and audit policy which allows authorized administrators to detect and analyze potential security violations. The audit policy mandates that the TOE:

- Provide a means to generate audit records of security-relevant events
- Allow only authorized administrator to define the criteria used for the selection of events to be audited, include or exclude auditable events from the set of audited events based on specified attributes,
- Recognize and creates an audit record resulting from a change of management functions,
- Provide mechanisms to prevent audit data loss such as loss of audit records due to audit storage failure.

Audit events are generated by the Trusted Software, Operating System Software, TSF System Services, and the Kernel and include the following types of events:

- Startup and shutdown of the operating system
- Use of special permissions that circumvent the access control policies
- Login attempts
- Logout commands issued
- Opens and closes of file system objects
- Creates and deletes of file system objects
- Operator commands issued
- Administrator commands issued
- Print request issued with no markings

The Audit policy also mandates that all audit records include the following attributes: date and time of the event, type of event, process ID of the process causing the audit event, MAC and MIC label of the process, effective privileges of the process, real user ID, and real group ID.

3.6 Separation of Roles Policy

The XTS-400 product provides pre-defined “operator”, and “administrator” roles. The separation of administrator and operator roles is enforced using the integrity policy. The system enforces the "principle of least privilege" (i.e., users should have no more authorization than that required to perform their functions) for administrator and operator roles.

3.7 Management Policy

The TSF implements a policy that regulates the management of TSF data. A combination of MAC, DAC, MIC, and roles are used to specify which users are authorized to initialize, view, modify, or delete the security attributes maintained by the TSF.

3.8 Residual Information Protection Policy

The TOE implements a policy that prevents the scavenging of residual data. The TSF ensures that all previous information content of a resource is made unavailable before the resource is reallocated to an object.

3.9 Trusted Path Policy

The TOE implements a trusted path policy that permits a user to be sure s/he is interacting directly with the TSF during sensitive operations. Note that “remote” users, i.e., across a network, are not supported. Users on serial terminals are considered local users. The <Break> key invokes the Trusted Path key for serial terminal users. On the console the sequence is <Ctrl-Alt-SysRq>. These are known as the SAK (Secure Attention Key). Any invocation of the SAK leads to a Trusted Path.

SAK must be used to initiate a login. Any time SAK is used, the user will obtain a prompt from a part of the TSF known as the Secure Server. If the terminal is not already handling a login session, a login is initiated; otherwise the user can request running of any trusted command. Use of SAK when processes are already running, returns the display to a known state and severs access by those processes to the display. Access to the display by those processes can be restored with the trusted “reattach” command.

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

The evaluation made a set of assumptions concerning the product usage that characterize the physical protection of the system as well as the training and behavior of system administrators and users. The following is a listing of those usage assumptions stated in the ST.

Physical protection of the communications to the system is adequate to guard against unauthorized access or malicious modification by users.

System Administrators follow the policies and procedures defined in the TOE documentation for secure administration of the TOE.

System administrators are fallible and occasionally make errors that compromise security.

Procedures exist for granting users authorization for access to specific security levels. This includes procedures for establishing one or more operators and administrators.

System administrators are competent to manage the TOE and the security of the information it contains.

Users cooperate with those responsible for managing the TOE to maintain TOE security, follow TOE user guidance, protect TOE secrets, and follow site procedures.

System Administrators properly dispose of user data after access has been removed (e.g., due to job termination, change in responsibility).

Procedures exist for how sensitive, classified, and high-integrity data and secrets are to be handled when they are in possession of an authorized user. Procedures also exist for pick-up and distribution of hardcopy output at multi-user or multi-level printers.

System Administrators are trusted not to abuse their authority.

The TOE is subject to deliberate attack by experts with advanced knowledge of security principles and concepts employed by the TOE. These experts are assumed to have substantial resources and high motivation.

System Administrators follow password management policies and procedures to ensure users comply with password policies.

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 located within controlled access facilities that prevent unauthorized physical access by outsiders.

The TOE involved in security policy enforcement will be physically protected from unauthorized modification by potentially hostile outsiders.

System Administrators review audit logs regularly.

Procedures exist for how to restrict other system users, or non-system users, from viewing terminal output on an authorized user's terminal. This includes considerations such as "looking over the shoulder", an authorized user leaving his or her terminal unattended, and terminal-specific instructions to erase terminal-local data following a logout.

Procedures exist for establishing the security attributes of all information imported into the system, for establishing the security attributes for all peripheral devices (e.g., printers, tape drives, disk drives) attached to the TOE, and marking a sensitivity label on all hardcopy output generated.

Authorized users are trusted not to compromise security.

Users are fallible and occasionally make errors that compromise security.

It is assumed that appropriate physical security is provided within the domain for the value of the IT assets protected by the operating system and the value of the stored, processed, and transmitted information.

Networks are single-level and unlabeled at layers 3 and below.

4.2 Clarification of Scope

The XTS-400 product release and corresponding ST for this evaluation was revised between the EAL4 and EAL5 evaluations to reflect the differences in the levels, as well as to address issues that were identified during the course of the EAL-5 evaluation.

The product that a customer would purchase directly from BAE - IT matches with the evaluated TOE. The TOE does not provide a particular trusted application out-of-the-box, but is a general-purpose system that can support many kinds of highly trusted applications. BAE - IT and its customers have developed a number of trusted applications which rely on the security features provided by the XTS-400. In particular, the XTS is often used as an application host platform for programs that provide automated filtering of an information flow. Information which meets the security policy criteria will pass through the filter and can safely flow between networks of differing sensitivity/classification. These filters are often called Guards because they guard against inadvertent release of sensitive information. These applications are not part of the TOE addressed by this ST. In particular, the following BAE - IT provided products are not covered by this evaluation:

- A Software Development Environment (SDE) package that allows programming of trusted and untrusted applications for use on the XTS. Frequently, initial programming and debug is done on a "real" Linux system and the binary copied to the XTS for execution. The SDE includes library functions to allow the security enforcing XTS API (separate from the Linux API used for UNIX® functions).
- A middle-ware package called Secure Automated Guard Environment (SAGE™) which provides transaction processing support for many of the tasks common to file-oriented filtering applications. SAGE reduces the risk and expense of developing custom applications by providing pre-written and pre-tested functions so the application developer can focus on the "security filter" logic.

- Turn-key applications programmed by BAE - IT to provide specific filtering or Guard capability.

This report makes no claims with regards to the trust associated with those applications. Installation of these applications could invalidate the security rating of the TOE due to the presence of privileged software. Customers should use sources other than this report to determine the trust associated with those applications.

The XTS-400/STOP 6.1.E system also provides an additional policy mechanism, "subtypes," which can be used in a customer-specific way in conjunction with MAC, MIC and DAC controls. Although the implementation of the subtype mechanism is within the TOE, there are no specific security policies associated with that mechanism that have been included in this evaluation. However, the subtype mechanism has been reviewed by the evaluators as it is used in the TOE to supplement protection for audit records.

The vendor has designed the product for a generic hardware platform that meets a well documented set of specific criteria. The basis for the platform is the x86 architecture. The vendor has a process in place for determining whether specific hardware configurations meet their specifications and to incorporate additional hardware into evaluated configurations. However, the specific hardware platforms listed for this evaluation (the Model 500 and the Model 2800) with the associated list of optional hardware additions are the only platforms for which this specific evaluation applies.

The TOE does not include multi-processor hardware platforms, but the evaluated configurations do support concurrent use by multiple users.

The evaluated configuration includes the device driver for the MSCU, a cryptographic device that plugs into the PCI bus and was not included within the scope of this evaluation. The MSCU interfaces to the TOE in a manner that would require design, implementation, and testing details about the MSCU that were not available to BAE - IT for inclusion in the evaluation. Customers that need to use the MSCU in conjunction with XTS-400/STOP 6.1.E will need to rely upon other means to determine the impact of incorporating MSCU hardware into their application environment.

The evaluated configuration supports up to eight network interfaces. Each network interface is treated as a single-level interface. The TOE is not a distributed system, though it can be attached to multiple Ethernet 10baseT and 100baseT networks concurrently.

The user identification and authentication mechanism utilizes one-way encryption to store passwords and to compare provided passwords against the stored passwords. The strength of the actual cryptographic algorithm used is not within the scope of this evaluation.

5 Architectural Information

The TOE consists of the following architectural components.

(a) the Kernel, TSS, OSS, and Trusted Application Domain Software components described below

(b) some BAE - IT-written untrusted software to ease use of the untrusted environment; This software executes in Ring 3, the application domain.

(c) some third-party untrusted software that is shipped with XTS systems to customers by BAE - IT to ease installation by the customer and to provide the look and feel of a Linux system;

(d) BIOS software to perform certain kinds of hardware configuration or diagnostics;

(e) the hardware platforms Model 500 and Model 2800.

The BAE - IT XTS-400 operating system was designed using strong architectural principals including layering, modularity, and data hiding. As a candidate EAL5+ product, the evaluation team looked at internal architecture of the XTS-400, in particular modularity, and the team developed strong evidence that the product met its EAL5 architectural requirements.

The high level design of the XTS-400 decomposes the TOE into four layered subsystems that utilize the ring architecture of the x86 processor family to support the separation of the layers. The allocation of TOE functionality to the four basic software components is described below. The software within the layers exhibits further characteristics of layering and modularity. The four subsystems of the software components are:

Kernel: The Security Kernel software occupies the innermost and most privileged ring and performs all Mandatory Access Control (MAC), and Mandatory Integrity Control (MIC). The kernel provides a virtual process environment, which isolates one process from another. The kernel implements a variation of the reference monitor concept. When a process requests access to an object, the kernel performs the access checks, and, given that the checks pass, maps the object into the process' address space. Subsequent accesses are mediated by the hardware. The Security Kernel also provides I/O services and an Inter-process Communication (IPC) message mechanism. The Security Kernel is part of every process' address space and is protected by the ring structure supported by the hardware.

TSS: The TSS software executes in Ring 1. TSS provides trusted system services required by both trusted and untrusted processes. The Kernel, TSS and OSS have the responsibility for creation and loading of both trusted and untrusted programs, respectively, in XTS-400, Version 6.1.E. TSS software enforces the Discretionary Access Control (DAC) policy to file system objects.

OSS: The OSS executes in Ring 2. OSS provides a UNIX-like Linux interface for user-written and trusted and untrusted software applications. The purpose of OSS is to make the multilevel security execution environment hidden to software running in the Application Domain (Ring 3).

Application Domain: Ring 3 is the Application Domain, in which all applications, both trusted and untrusted, execute. Software is considered trusted in XTS-400, Version 6.1.E if it performs functions upon which the system depends to enforce the security policy (e.g., the establishment of user authorization). This determination is based on integrity level and privileges. Untrusted software runs at a low integrity level. Some processes require

privileges to perform their functions. An example of a process that requires privileges is the Secure Server, which needs access to the User Access Authentication database, kept at system high access level, while establishing a session for a user at another security level.

6 Delivery and Documentation

The hardware and software for the TOE are purchased as a single item. The evaluated product is available on two basic hardware platforms – the Model 500 and the Model 2800. There is some optional hardware that may be included in the base hardware for the evaluated platform. The hardware options are described in further detail in the Security Target.

The software is installed by the BAE - IT prior to delivery. However distribution media are also provided with the product. The following items are included in the media distribution:

STOP 6.1.E Model 500 Base Operating System tape
STOP 6.1.E Model 500 Installation diskette
STOP 6.1.E Model 500 Recovery diskette
-or-
STOP 6.1.E Model 2800 Base Operating System tape
STOP 6.1.E Model 2800 Installation diskette
STOP 6.1.E Model 2800 Recovery diskette
-and-
STOP 6.1.E Applications CD-ROM
STOP 6.1.E Base RPM Support Tape

The following product documentation is provided in softcopy on the CD-ROM.(XTDOC0093-01):

Title/Description	Order No.
XTS-400 STOP 6.1.E Trusted Facility Manual	XTDOC0004-07
XTS-400 STOP 6.1.E User's Manual	XTDOC0005-07
XTS-400 Software Release Bulletin	XTDOCC0001-08
XTS-400 Installation and Setup Manual (Pentium III Model 500 Systems), (Bios Revision 7.2)	XTDOC0054-04
XTS-400 Installation and Setup Manual (XEON Model 2800 Systems), (Bios Revision 1.00)	XTDOC0051-04

In addition, the product distribution includes a "checksum" delivery that is made under separate cover. The Installation Guide explains the procedure for using the checksums to verify the integrity of the distribution.

The only printed documentation that is delivered with the hardware is a hardcopy of the *XTS-400 Installation and Setup Manual* that is also provided on the distribution media.

7 IT Product Testing

7.1 Developer Testing

The developer maintains a suite of tests for confirming that the XTS-400 product meets its advertised functional requirements. Testing was performed at a developer facility in Herndon, VA. Since the vendor considers the evaluated configuration to be the base platform for many of their hosted applications, the vendor's normal functional testing was directly applicable to the TOE. Although some test documentation and tests may have initially been developed to support the product evaluation, all of that documentation and testing has been incorporated into the regular product test suite. The developer tested the STOP operating system on a combination of configurations that includeed both of the platform models and each of the optional hardware components.

The developer has categorized its testing into "programmatic" and "scripted" tests. The test package includes a programmatic test driver and a scripted test driver with procedures designed to verify each identified security relevant rule. There are essentially three types of functional tests: "automated", "interactive", and "manual". The vast majority of the testing is automated with no human interaction required once the automated test suite is started. The "automated" tests are included in the programmatic test suite. Thorough logs of the automated tests are maintained so the results many be retained and manually reviewed. Interactive tests require a human to perform an action at some point, but do not require further human activity or interpretation of the results to determine whether the tests were successful. Examples of interactive tests are those that pause and prompt the tester to insert a tape as part of the test. Manual tests require a tester to observe the behavior of the system, such as the clearing of a screen or the presentation of other visual information to interpret the test results. The interactive and manual tests are contained in the scripted test suite. Logs are also maintained for the interactive and manual tests.

The developer provided the evaluators with a CD-ROM containing documentation evidence in electronic form. Hyperlinks were provided between all related evidence. The developer's Test Plan, Test Procedures, Test implementation code, expected results, and test coverage documentation were included on the CD-ROM. The CD-ROM also included the functional specifications, design documentation, and a hypertext representation of the implementation code. The evaluators reviewed the developers tests and test results to ensure that the developers testing and test results were appropriate for the evaluated configuration. The developer's test documentation showed that the external interfaces were thoroughly tested. At least one test case was mapped to every external interface. Many of the interfaces were exercised by multiple tests. An evaluation team review of all of the security functions and the mapping between security functions and tests confirmed that security functions were appropriately tested by the developer tests.

7.2 Evaluator Testing

CCTL evaluation team testing was conducted at the BAE - IT development facility in Herndon, VA. NSA evaluator testing was conducted at the NSA facilities in Linthicum, MD. The CCTL evaluation team testing was performed on STOP 6.1.E rc1, which was

the version of the product that was originally submitted for EAL 5 evaluation. The NSA evaluators performed testing and related analysis on STOP 6.1.E rc1 and the resulting evaluated product, STOP 6.1.E (also referenced as STOP 6.1.E rc2).

The CCTL evaluation team performed the following activities during testing:

1. Execution of all of the developer's functional tests for STOP 6.1.E rc1
2. Independent Testing on STOP 6.1.E rc1
3. Vulnerability Testing (AVA_VLA.2)

The NSA evaluation team performed the following activities during testing:

1. Installation of the TOE in its evaluation configuration.
2. Testing of changes from STOP 6.1.E rc1 to STOP 6.1.E
3. Vulnerability Testing for AVA_VLA.3

The test configuration consisted of two instantiations of the TOE attached to an ethernet network. Most of the tests were installed, executed, logged, and analyzed directly on the individual hardware platforms. The Ethernet connection between the two platforms was used to drive a couple of tests that exercised the network interface. A third host was also attached to the network, but was only used to download test evidence, in particular the test logs, and to archive those logs. The one instantiation of the TOE used the Model 500 hardware platform and the other instantiation of the TOE used the Model 2800 platform. The CCTL testing for STOP 6.0.E was run on both hardware configurations while the STOP 6.1.E rc1 tests were only performed on Model 2800 platform. The NSA evaluator testing for STOP 6.1.E rc1 and the final evaluated product, STOP 6.1.E was performed on both hardware configurations. The specific configurations of the tested platforms were as follows:

Model 2800 (Xeon-based) system had;
- PCI Cards
  - Adaptec SCSI controller
  - Zynx network card (2-port and 4-port)
- Peripherals
  - Spyrus PC card readers (2)
  - Optional Serial Port
  - APC UPS
  - HP 4100 Printer
  - Wyse Terminal
  - Seagate SCSI-160 hard drives (2)
  - Toshiba DVD reader used as a CD reader
  - HP DDS-3 tape drive
  - SHARP 17" LVD monitor
  - Keytronics keyboard
  - Microsoft Mouse
  - XTS400-1UBLACK KVM (sometimes)

Model 500 (Pentium 3 based) system had:

PCI Cards
- Adaptec SCSI controller (2 optional cards)
- Zynx network card (2-port and 4-port)

Peripherals
- Adtron PC card Reader
- APC UPS
- HP 4100 Printer
- Wyse Terminal
- IBM LVD SCSI hard drives (2)
- Toshiba CD reader
- CipherServer PC card reader
- Wangdat DDS2 tape drive
- MAG CRT monitor
- Keytronics keyboard
- Logitech Mouse

Most of the developers test procedures were automated. There were only a few dozen interactive or manual tests. Although the tests did not require much interaction with the tester, the analysis of the test results was very time consuming. The test logs were recorded on the systems that were being evaluated. The MAC, DAC, and MIC security policies protected the test logs. Although those logs could be exported for archival purposes and printouts of some of the log information could be obtained, a significant portion of the review of the logs and the analysis of the test results was easiest when performed on the XTS-400. The evaluator spent a significant portion of the testing period reviewing the evidence online and documenting the observations in evaluation records Although the analysis of the test results included extensive online work, the source material that was analyzed was all archived in a manner that it could be retrieved and reviewed if further verification of the analysis was required.

The evaluation team performed all of the installation, setup, testing, and test result analysis. Vendor representatives were available to answer questions and assist in the archiving of test results. The evaluators' testing included all of the tests found in the developer test plan and procedures. All security functions were tested, as well as all external interfaces. Testing of internal subsystem interfaces was done implicitly.

The evaluators devised additional tests to augment and supplement the vendor tests. The evaluation team obtained help from the BAE - IT developers to code some of the independent tests that evaluation team designed. Those tests that could be automated were added to the developers automated test suite. Hence, some of the evaluation team's tests were actually conducted at the same time as the team exercised the vendor test suite. A few independent tests were manual tests.

Finally, the evaluators performed tests for hypothesized vulnerabilities. The CCTL evaluation team determined that the vendor's own vulnerability analysis was very thorough and appropriately tested. As a result, there were only a few additional vulnerabilities hypothesized and tested by the CCTL evaluators. The NSA evaluation team expanded upon the vendor and CCTL vulnerability analysis to perform additional penetration testing.

Tools employed by the NSA evaluation team for independent testing included the same category of tools employed by the CygnaCom evaluation team, as well as in-house developed tools, which assisted in determining that the TOE was resistant to penetration attacks performed by attackers possessing a moderate attack potential.

The initial National Security Agency vulnerability testing on STOP 6.1.E rc1 revealed several design and code flaws that needed correction and the final Evaluated product was retested by the NSA team to assure that those problems were successfully corrected. STOP 6.1.E contains the "fixed" product and should be used to replace any prior 6.0.E or 6.1.E rc1 products or products labeled "beta". STOP 6.1.E is bit for bit the same code as the STOP 6.1.E rc2 that was tested. Only the media labels and documentation references were changed between 6.1.E rc2 and 6.1.E so, if you are already using 6.1.E RC2, there is no need to "upgrade" to 6.1.E.

The end result of the CCTL and NSA testing activities on the evaluated product was that all tests gave expected (correct) results. The final evaluator testing did not reveal any residual problems with the TOE. The testing found that the product was implemented as described in the functional specification. The CCTL and NSA evaluation team tests and penetration tests substantiated the security functional requirements claimed in the Security Target.

8 Evaluated Configuration

The TOE includes the entire XTS-400 and the underlying hardware platform. The TOE hardware consists of the Model 500 (Pentium III) and the Model 2800(XEON) platforms, available in tower and rack-mount chassis. All components are commercial-off-the-shelf (COTS). The XTS-400 uses specific Intel-brand motherboards and industry standard ISA or PCI peripheral cards or chips built into the motherboard.

In addition to these basic platform components the evaluated configuration allows:

- CD-ROM drive
- 4mm DAT tape drive
- PC card readers
- Add-in Ethernet cards
- Add-in SCSI host adapters
- parallel, PCL-5 printer
- serial terminal
- touchpads
- flat panel displays

The specific identifiers of the evaluated hardware components are provided in the ST[10].

Other hardware that are not part of the evaluated configuration, but which are software supported within the TOE include:

- APC Smart-UPS uninterruptible power supply.
- Mission Support Cryptographic Unit (MSCU): a proprietary PCI board that supports type 1 cryptography. Further information on this product, including a

security analysis of this product, may be available to customers with the appropriate need-to-know through the developer.

:

9 Results of the Evaluation

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC, Version 2.1; CEM, Version 1.0, and all applicable NIAP CCEVS and International Interpretations in effect on March 1, 2003.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 5 assurance component and for the augmented assurance components: ALC_FLR.3 and ATE_IND.3. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of issues requiring resolution or clarification within the evaluation evidence.

In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict. Section 4, Results of Evaluation, from the document *Evaluation Technical Evaluation Technical Report (ETR) for a Target of BAE - IT XTS-400 Version 6.1.E, 24 September 2004 [11]* and the supplemental report *XTS-400/STOP 6.1.E Vulnerability Assessment ETR, dated 1 March 2005 [14]* contain the verdicts of “PASS” for all the work units.

The evaluation determined the product to be Part 2 conformant and, as well, meeting the requirements for Part 3, and EAL 5 augmented by Flaw Remediation (ALC_FLR.3) and Independent Testing – Complete (ATE_IND.3). The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which combines a proprietary ETR controlled by CygnaCom Solutions together with a proprietary supplemental AVA_VLA.3 Evaluation Report that is controlled by the National Security Agency.

10 Validator Comments

The TOE included two very explicitly defined hardware platforms. However, the vendor has designed STOP for a fairly generic x86 based platform. The vendor maintains a list of hardware characteristics that are required for a porting of STOP 6.1.E to meet the CC requirements in the Security Target. As part of this evaluation, the explicit hardware platforms included in this evaluation were determined to meet the vendors’ criteria. The generic requirements were not included as part of this evaluation because of evaluation constraints imposed by the LSPP and CAPP protection profiles. The vendor has procedures in place for incorporating changes to the evaluated platforms into future updates to this evaluation.

The analysis for this product was definitely facilitated by the architectural design as well as the automated HTML-presentation documentation and testing evidence that was prepared by the vendor for the evaluation.

11 Security Target

The Security Target, "BAE - IT XTS-400 Version 6 Common Criteria Security Target, Version 1.11, dated December 2004" [10] is included here by reference.

12 Glossary

12.1 Definition of Acronyms

CAPP	Controlled Access Protection Profile (Version 1.d)[9]
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Evaluation Testing Laboratory
CEM	Common Evaluation Methodology
CI	Configuration Items
CM	Configuration Management
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FTP	File Transfer Protocol
GUI	Graphical User Interface
I&A	Identification and Authentication
I/O	Input/Output
IP	Internet Protocol
IPC	Interprocess Communication
IT	Information Technology
LSPP	Labeled Security Protection Profile (Version 1.b) [12]
MAC	Mandatory Access Control
MIC	Mandatory Integrity Control
MSCU	Mission Support Cryptographic Unit
NIAP	National Information Assurance Program
NIST	National Institute of Science & Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
OR	Observation Report
OSS	Operating System Services
PP	Protection Profile
SAK	Secure Attention Key
SAR	Security Assurance Requirement
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirements
STOP	Secure Trusted Operating Program
SOF	Strength of Function
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

TSS	TSF System Services
UDP	User Datagram Protocol
XTS	Extended Trusted System

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] NIAP Common Criteria Evaluation and Validation Scheme for IT Security, Guidance to Common Criteria Testing Laboratories, Version 1.0, March 20, 2001.

[8] Common Criteria Evaluation and Validation Scheme for Information Technology Security Guidance to Validators of IT Security Evaluations, Scheme Publication #3, Version 1.0, February 2002

[9] Controlled Access Protection Profile (Version 1.d)

[10] BAE - IT XTS-400, Release 6 Common Criteria Security Target, Version 1.11, dated December 2004

[11] Evaluation Technical Report (ETR) for a Target of BAE - IT XTS-400 Version 6.1.E, dated Sept 24, 2004

[12] Labeled Security Protection Profile (Version 1.b)

[13] Supplement: ALC_FLR - Flaw Remediation, CEM-2001/0015, Version 1.0, August 2001

[14] XTS-400/STOP 6.1.E Vulnerability Assessment ETR, dated 1 March 2005