

XTS-400™ Trusted Computer System

High Assurance Application Platform

As a trusted computer system, BAE Systems' XTS-400 is ideal for hosting trusted guard and server applications. With high-power Pentium® or Xeon™ server hardware, the XTS-400 design is based on its predecessor, the XTS-300™, the only general-purpose computer system in the world rated at the Orange Book B3 level (Mandatory Protection, Security Domains) by the National Security Agency (NSA). This design implements an NSA evaluated mandatory integrity policy that can provide files, data, and applications unparalleled protection from unauthorized tampering by malicious users or rogue software.

The XTS-400 was evaluated at the Common Criteria Evaluated Assurance Level 5 Augmented (EAL 5+). It is one of the few systems that can protect the data and enterprise processing environment from information security risks.

Trusted Applications With High Assurance

The Linux®-like programmatic interfaces of the XTS-400's Secure Trusted Operating Program (STOP™) operating system enable developers to port or develop applications easily on the system. These applications reside, for the most part, outside the system's Target of Evaluation (TOE), making them easier to certify and accredit while deriving a high degree of security and integrity from the underlying mandatory protection mechanisms in the TOE.

Several trusted software applications available for the XTS-400 have been accredited and are operational. These include trusted guard applications that provide strict control over the automated sharing of information among differently classified networks.

Commodity Applications With High Security

The Linux® Application Programming Interface of the XTS allows it to host Linux®-compatible applications, typically requiring no software reengineering. This capability increases the utility of the XTS by taking advantage of the many existing applications that can benefit from the security of being run on a high assurance server.

Life-Cycle Engineering Expertise

BAE Systems has several application development groups that specialize in the development of high assurance guards and other applications that run on the XTS. These groups are experienced in the entire life cycle of development, including requirements analysis, development, documentation, certification, deployment, and support. They

can help field the systems by providing installation, configuration, accreditation support, training, and help desk support to enable the customer's XTS system to meet their mission requirements.

BAE Systems has experience in working both with prime contractors and directly with agencies. BAE Systems can act in every role from product supplier to full development partner through various contract vehicles.

Robust Operating System

The XTS-400's STOP™ operating system incorporates a high-assurance kernel to enforce the system's security and integrity policies.

The multi-level secure kernel ensures that information, processes and devices stored and running on the system at different sensitivity levels cannot intermingle in violation of the system's mandatory security model. The operating system also provides the capability for regrading objects (changing their security or sensitivity level), subject to customer-defined, configurable security policy. Because the XTS is evaluated at such a high level, data can only pass from one security domain to another through the security policy specified by the customer.

The operating system also includes:

- X-Windows graphical user interface
- Linux® programmatic interface
- A multi-level file system
- TCP/IP networking
- Support for the Department of Defense's FORTEZZA® card

Implementation

Email Messaging Guard

BAE Systems' Email Messaging Guard is a robust, configurable boundary device that sits between two or more networks at different classification levels and/or collateral levels (i.e., U.S. Secret and FiveEyes). The Email Messaging Guard ensures compliance with the U.S.'s Secret and Below Interoperability (SABI) and Top Secret and Below Interoperability (TSABI) approaches for messaging. The Email Messaging Guard enforces security policy during the transmission of X.400 & SMTP message traffic and X.500 directory service traffic between multiple enclaves. Email security services include message validation, non-repudiation, content inspection, access control, file type validation, and virus scanning of messages and attachments.

Secure File Server (SFS)

BAE Systems' SFS delivers secure cross-domain file sharing on a multi-level secure, high assurance server. Users have full access to files at their sensitivity levels and read-only access to files at lower levels. Users have no access to higher level shares. The SFS can safely and securely bridge multiple networks, each configured at a distinct security level (0-15) and optionally for up to 64 categories. Further, discretionary access (i.e., user and group permissions) may be configured for individual shares within the security enclaves. The "read-only down" access of the SFS precludes the need for either multiple computers (at differing security levels) or implementing lengthy procedures to move files between sensitivity levels.

Transaction Guard

Transaction Guards are customizable data guards, each tailored to the production environment where it is implemented. A transaction guard can be configured to perform deep content inspection and validation on XML, flat files, database commands (SQL), or virtually any structured data set. Transactions can be either cleansed or rejected outright while passing through the guard, as determined by the security policies implemented. Filtering options include message integrity validation, dirty and clean word searches, access control, and envelope or label matching.

Multi-Level (ML) Chat

ML Chat provides real-time information exchange between users at differing security levels. Users "chat" via an instant messenger/conferencing client application. Messages are filtered for content – passed, cleansed, or redacted completely – on their way to destination users at various security levels.

FOR MORE INFORMATION, CONTACT:

BAE Systems Information Technology
8201 Greensboro Drive
Suite 1200
McLean, VA 22102
(703) 847-5820
www.baesystems.com

2008© BAE Systems, Inc.

Approved for Public Release by BAE Systems 12/2007

0108.31670.CSOG