Survey of Multi-Level Security (MLS) Products

Final Report

John Detombe, Darin Cowan, Mike Smith, and John O'Brien

Aepos Technologies Corporation
200 Montcalm Street, Suite 200
Gatineau, Québec
J8Y 3B5

Contract Number: W7714-4-2996

Contract Scientific Authority: Jean Savoie, DRDC Ottawa

Defence R&D Canada—Ottawa
Contractor Report
DRDC Ottawa CR 2004-268
December 2004

AEPOS
Technologies Corporation

Defence Research And Development Canada – Ottawa

Survey Of Multi-Level Security (MLS) Products

Prepared for:

Defence Research and Development - Ottawa

Prepared by:

AEPOS Technologies Corporation
200 Montcalm Street, Suite 200
Gatineau, Quebec
J8Y 3B5

Client Contract No.: CA1785.091
Date: 17 December 2004

Groupe adga Group

This page intentionally left blank

Defence Research And Development Canada – Ottawa
Survey Of Multi-Level Secure Products

DOCUMENT ORIGIN AND APPROVAL RECORD

Prepared by: _____ _____

D. Cowan
Senior IT Security Architect

Date

Prepared by: _____ _____

M. Smith
Senior IT Security Engineer

Date

Reviewed by: _____ _____

J. Detombe
Director, Information Technology Security

Date

Approved by: _____ _____

J. Lyrette
Vice-President, Technical Direction

Date

CHANGE CONTROL RECORD

Version	Date	Description Of Changes	Affected Pages
1.0	November 30, 2004	First Issue	All
1.01	December 8, 2004	Response to customer comments	All
1.02	December 17, 2004	Response to customer comments	All

Executive Summary

Since computers first started to be used to process sensitive information there has existed the situation of information having multiple levels of sensitivity, combined with multiple users having varying security clearances and needs to know the information, creating a security problem. This report refers to this problem as the Multi-Level Security problem.

Multi-level secure computer design began in the late 1960s, and continuing on through the 1970s, the work defined principles of multi-level secure computing: the concept of mandatory and discretionary access control, the Security Reference Monitor, audit, development practices, identification and authentication, formal descriptions, and a requirement that a multi-level secure computer had to be evaluated to assure users that the security features it offered were designed and implemented correctly. It is upon this final requirement that the concept of trust in computing systems is built. This document is focused on products that are trustable, and thus have been evaluated.

That work led to the development of security standards for evaluation. First, the Trusted Computer System Evaluation Criteria (TCSEC, or "Orange Book") laid down a series of standards for functionality and assurance against which a secure computer system could be evaluated. Later, many countries would work to improve on the "Orange Book" and develop their own standards. This ultimately led to the development, by an international consortium of participant nations, to a Common Criteria published in 1999.

The evolution of the evaluation criteria caused a change in focus. The "Orange Book" set out requirements for both total system functionality and assurance. But the later criteria, including the Common Criteria, concentrated on a more granular level of functionality and assurance at the same level of granularity. This leaves no clear modern equivalent class to "Orange Book" multi-level secure systems.

The computer industry also changed greatly over this time. While it was normal in the 1960s to 1980s to have many users with different security clearances processing data with different sensitivity levels all in a single computer, advancing technology led to cheaper hardware. With hardware being more affordable, organizations could separate their information domains onto systems and networks operating at a single sensitivity level with the users all having a need-to-know and an appropriate security clearance. This caused a shift in the types of security products available in the marketplace. Where once there were many multi-level secure operating systems, now there are few. Instead, smaller, point solutions that have limited functionality but can be evaluated to high assurance have come on to the market. These products support multi-level computing by acting as data separators (switches, trusted guards, period processing products) between single level network systems or as sentinels to ensure correct data flow (trusted guards, data protection kits, operating systems). Modern applications are being built with security

functionality included, or designed to take better advantage of security functionality available in underlying infrastructure.

This document presents a survey of the multi-level secure product space, grouping the products with similar functionalities into classes, and allowing the readers to understand the functionalities that are available and compare products of any given class. This document should help readers building new MLS solutions from MLS products.

Table Of Contents

LIST OF TABLES

LIST OF FIGURES

1. INTRODUCTION

1.1. Overview

This document provides primarily a survey of the Multi-Level Secure (MLS) product space to help readers to solve the problem of designing or building MLS computer systems from MLS products.

The "level" in "multi-level secure" refers to levels of information classification. Each classification level has its own special handling requirements, which are documented in government regulations. In particular, no one may have access to classified information at a given level unless he or she has a suitable security clearance. An MLS computer system, then, is one that reliably and accurately supports and enforces these regulations regarding classification levels and security clearances ([AND 1972], page 1; [RYA 1997], Chapter 6, Section F). This is the historic definition of multi-level secure, and it differs slightly from a more modern interpretation of the term (see section 1.2).

AEPOS Technologies has also examined the history of MLS from an evaluated products point of view. Finally, commentary is presented with regard to the direction that the MLS product space seems to be taking as it moves into the future.

This report focuses on trusted products. To be trusted, a product must have had its features formally evaluated and certified by a government agency.

1.2. MLS problem

In this report, the MLS problem is referred as the problem of enforcing security policies for computer systems processing information from many information domains. The notion of information domain and related terms are defined in the Table below.

Throughout this document, a number of terms are used to describe products features and concepts. These terms are defined here:

Table 1 - Terms and Definitions

Term	Definition
Information Domain	A set of commonly and unambiguously labelled information objects with a common security policy that defines the protections to be afforded the objects by authorized users and information management systems [TAF 1996]. This is similar to the historical concept of "level" as noted in Section 2.1, but allows for a non-hierarchical view of information security.
Multi-Level	In this document, the term "multi-level" refers to multiple information domains within the boundaries of a single system.
Multi-Level Secure	A system is said to be Multi-Level Secure when it meets the following criteria: 1. The system must process information for more than one information domain; and 2. The system must be implemented with assurance that the security policies within each domain are enforced.
Multi-Level Secure Product	For the purposes of this document, a product was considered a "multi-level secure product" if: 1. The product was intended by manufacture to function as part of a multi-level secure system; 2. The product has been evaluated by a recognized governmental agency against the Common Criteria, the Information Technology System Evaluation Criteria, or the manufacturer has stated intent to have the product evaluated. It is recognized that it is possible to devise, through engineering, systems that may be capable of multi-level processing solely through the use of products that are not considered multi-level secure products. This document does not include products that may be used in that manner because it is possible that any product on the market could be used in such a design.
Process	A system processes information when it stores, transmits, or receives information.
System	In this document a "system" refers to a computer system, which can be a single processing device or multiple networked processing devices.

1.3. References

[AND 1972] Anderson, James P. *Computer Security Technology Planning Study – Volume II* [online]. Bedford, Massachusetts: [United States Air Force], October 1972 [cited 25 August 2004]. Portable Document Format. Available from World Wide Web: <http://seclab.cs.ucdavis.edu/projects/history/papers/ande72.pdf>.

[AND 2002] Anderson, Shelley. *Common Criteria: An Introduction* [online]. [Ottawa, Canada: 3-Way Street Publications, 2002; cited 25 August 2004]. Presented at the 3rd International Common Criteria Conference, 13-14 May 2002. Portable Document Format. Available from World Wide Web: <http://www.expotrack.com/iccc/proceedings/pdf/proceed/english/track2/t2_s1_e.pdf>.

[APT 2002] Apted, Anthony G.; Carthigaser, Malathi; and Lowe, Chris; *Common Problems with the Common Criteria* [online]. [Ottawa, Canada: 3-Way Street Publications, 2002; cited 25 August 2004]. Presented at the 3rd International Common Criteria Conference, 13-14 May 2002. Portable Document Format. Available from World Wide Web: <http://www.expotrack.com/iccc/proceedings/pdf/proceed/english/track4/p008_e.pdf>.

[BEL 1976] Bell, D.E.; and La Padula, L.J. *Secure Computer System: Unified Exposition and Multics Interpretation* [online]. The MITRE Corporation. Bedford, Massachusetts: United States Air Force, March 1976 [cited 25 August 2004]. Portable Document Format. Available from World Wide Web: <http://seclab.cs.ucdavis.edu/projects/history/papers/bell76.pdf>.

[DOD 1985a] *DoD 5200.28-STD: Department of Defense Trusted Computer System Evaluation Criteria*. [Department of Defense], 26 December 1985 [cited 25 August 2004]. Portable Document Format. Available from World Wide Web: <http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.pdf>.

[DOD 1985b] *CSC-STD-003-85: Computer Security Requirements – Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments* [online]. Department of Defense Computer Security Center, 25 June 1985 [cited 25 August 2004]. Available from World Wide Web: <http://www.radium.ncsc.mil/tpep/library/rainbow/CSC-STD-003-85.html>.

[FAR 2004] TCSEC. In *TheFreeDictionary.com* web site [online]. [Huntingdon Valley, Pennsylvania]: Farlex, Inc. [cited 25 August 2004]. Available from World Wide Web: <http://encyclopedia.thefreedictionary.com/TCSEC>.

[NCS 2000a] Historical EPL [Evaluated Products List]. In *Trusted Product Evaluation Program* web site [online]. [National Computer Security Center], 16 August 2000 [cited 25 August 2004]. Available from World Wide Web: <http://www.radium.ncsc.mil/tpep/epl/historical.html>.

[NCS 2000b] Evaluated Products List Indexed by Rating. In *Trusted Product Evaluation Program* web site [online]. [National Computer Security Center], 18 September 2000 [cited 26 August 2004]. Available from World Wide Web: <http://www.radium.ncsc.mil/tpep/epl/epl-by-class.html>.

[NEU 2004] Neumann, Peter G. *Principled Assuredly Trustworthy Composable Architectures* [online]. Draft. Menlo Park, California: SRI International, 24 August 2004 [cited 25 August 2004]. When completed (before the end of 2004), this report will be deliverable A001, the final report for SRI Project 11459, Contract number N66001-01-C-8040 as part of DARPA's Composable High-Assurance Trustworthy Systems (CHATS) program. Available from the World Wide Web: <http://www.csl.sri.com/users/neumann/chats4.html>.

[NSA 1999] *Labeled Security Protection Profile* [online]. Version 1.b. Fort George G. Meade, Maryland: National Security Agency, 8 October 1999 [cited 25 August 2004]. Portable Document Format. Available from World Wide Web: <http://www.commoncriteriaportal.org/public/files/ppfiles/lspp.pdf>. Also available from <http://www.iatf.net/protection_profiles/file_serve.cfm?chapter=os_labeled.pdf>.

[NSA 2001] *Protection Profile for Multi-level Operating Systems in Environments Requiring Medium Robustness* [online]. Version 1.22. Fort George G. Meade, Maryland: National Security Agency, 23 May 2001 [cited 25 August 2004]. Portable Document Format. Available from World Wide Web: <http://www.iatf.net/protection_profiles/file_serve.cfm?chapter=MLMROSPPVer1_22.pdf>.

[OLS 1997] Olsen, Florence. Sun finds Net creates users for secure OS. In *Government Computer News* web site [online]. [Washington, D.C.]: Post-Newsweek Business Information, Inc., 4 August 1997 [cite 25 August 2004]. Available from World Wide Web: <http://www.gcn.com/archives/gcn/1997/august4/cov2.htm>.

[PFL 2000] Pfleeger, Charles P. *Computer Security from the Trojan Wars to the Present* [online]. [Gaithersburg, Maryland: National Institute of Standards and Technology; cited 25 August 2004]. Presented at the 23rd National Information Systems Security Conference, 16-19 October 2000. Portable Document Format. Available from World Wide Web: <http://csrc.ncsl.nist.gov/nissc/2000/proceedings/papers/920slide.pdf>.

[RYA 1997] Ryan, Daniel J.; and Ryan, Julie J.C.H. *INFOSEC and INFOWAR: The Protection of Information Assets and Systems* [online]. Annapolis, Maryland: Daniel J. Ryan and Julie J.C.H. Ryan, 1997 [cited 25 August 2004]. Available from World Wide Web: <http://www.julieryan.com/BOOK1297.html>.

[RYA 2002] Ryan, Julie J.C.H. *The Effect of Public Budgetary and Policy Decisions on Development of Trusted Systems* [online]. [Washington, D.C]: George Washington University, [October 2002, cited 25 August 2004]. Presented at the 2002 ASEM [American Society of Engineering Management] National Conference, 2-5 October 2002. Available from World Wide Web: <http://www.gwu.edu/~asem_dc/RyanASEM02.html>.

[SSS 1991] System Security Study Committee. Page 143: Chapter 6 – Why the Security Market Has Not Worked Well. In *Computers at Risk: Safe Computing in the Information Age* [online]. Computer Science and Telecommunications Board. Washington, D.C.: National Academy Press, 1991 [cited 25 August 2004]. Available from World Wide Web: <http://www.nap.edu/books/0309043883/html/143.html>.

[SYN 2004] Syntegra. *Common Criteria: An Introduction* [online]. [Common Criteria Project Sponsoring Organizations; cited 26 August 2004]. Portable Document Format. Available from World Wide Web: <http://www.commoncriteriaportal.org/public/files/ccintroduction.pdf>.

[TAF 1996] *Department of Defence Technical Architecture Framework for Information Management.* Version 3.0, 30 April 1996. Available from Defence Information Systems Agency (DISA) World Wide Web site.

2. HISTORY OF MLS

2.1. Introduction

This section provides a review of the key events and ideas in the history of multi-level secure (MLS) computing.

The increasing use and networking of resource-sharing (i.e., multi-user) computers in government and military settings in the 1960s drove the need for MLS computers. Without MLS computers, organizations needed completely isolated computers for different classification levels to separate information of different classification. This was expensive and inefficient. Furthermore, it negated the possibility of automated information sharing between different information domains ([AND 1972], [PFL 2000]).

Theoretical work in MLS computer design began in the late 1960s and continued through the 1970s. This work defined some of the key principles of MLS computing (e.g., [AND 1972], [BEL 1976]):

- The concept of mandatory and discretionary access control
- The Security Reference Monitor
- Audit
- Development practices
- Identification and authentication
- Formal descriptions
- A requirement that a multi-level secure computer had to be evaluated to assure users that the security features it offered were designed and implemented correctly.

Regarding assurance, the greater the difference between the highest classification handled by the system and the lowest clearance of a system user, the greater the assurance had to be ([APT 2002], page 4 of 19). This report focuses on the principle that a multi-level secure computer must be evaluated.

During this period of theoretical development, there were no commercial MLS computers. There was some hope that some technologies of the time, such as virtual machines ([AND 1972], page 17) would be good building blocks for the future development of MLS computers. Some researchers began designing and building early MLS systems ([BEL 1976]).

2.2. The Orange Book

The theoretical work of the 1970s led directly to the publication of [DOD 1985a], commonly referred to as the "Orange Book" because of the colour of its cover, in 1985 (an earlier version

was published in 1983). The Orange Book defined the criteria for evaluating a computer system in terms of its security features. If defined a hierarchy of evaluation classes. Each class had more security features than the class below it and required a higher degree of assurance as to the correct design and implementation of those features ([FAR 2004]).

[DOD 1985b] stated what class of system was required when a computer system was to be used in a multi-level mode. The minimum class for any kind of MLS processing was B1, and this was only acceptable under very limited conditions[1]. True MLS operation required an A1 class system, the highest class in the Orange Book hierarchy.

The Trusted Product Evaluation Program (TPEP) was launched to evaluate computer and related products against the Orange Book criteria. The evaluation process turned out to be long and, for the product manufacturer, expensive ([OLS 1997], [RYA 1997], and [RYA 2002]). The high assurance levels for MLS products required more, and more detailed, design documents from the manufacturers than they would normally produce for a commercial product. Further, the market for MLS was not big enough to justify the expense ([SSS 1991]).

[RYA 2002] analyzed the Evaluated Products Lists (EPL; [NCS 2000a]) and found that 114 products had been submitted for evaluation between 1984 and 2000. Thirty products were withdrawn from the process. Two products were evaluated at class D1, the lowest class, which meant the product offered minimal features with no assurance about those features. Thus, 82 products were successfully evaluated. 44 were evaluated at class B1 or above, and so could be used in MLS environments (with certain limitations for the B1 and B2 classes, as per [DOD 1985b]). Of these 44, fully 28 were evaluated at class B1, the lowest possible MLS class. Only 4 were evaluated at class A1, the highest class.

The TPEP grouped products into four product classes ([NCS 2000b]):

- Operating systems
- Network components
- Trusted applications
- Subsystems

Operating system functions are well understood. Network components included network switches, network interface cards, and network operating systems. Trusted applications were all databases. The only evaluated subsystems were the two D-class products; they were both expansion cards for personal computers designed to provide cryptographically based access control to files on the local hard disk.

[1] Classes below B1 could only be used in "System High" (where every user had a minimum security clearance and all information was treated at the same level of the most sensitive information in the system) or "Dedicated" (where every user had a minimum security clearance and all information was classified at the same level) processing environments.

The Orange Book criteria were tied to the then-current architecture of a monolithic computer system, i.e., systems with a single processor accessed by multiple users from "dumb" terminals. They did not address the security requirements of networks of intelligent, single-user computers sharing information. Various "interpretations" of the Orange Book criteria were released during the 1980s and early 1990s to apply the criteria to different system architectures and to specific security issues (such as audit).

2.3. The Common Criteria

The Orange Book was an American initiative. Canada and Europe developed their own evaluation criteria in the early 1990s. The U.S., Europe, and Canada worked to harmonize these standards through the 1990s. This work resulted in the Common Criteria, first published in 1996 and updated to version 2.1 in 1999 ([AND 2002], [APT 2002]). It was approved as ISO standard 15408 in December 1999. Many countries now use the Common Criteria.

In the Orange Book model, security features and assurance levels were combined; a certain set of security features had to be accompanied by a certain level of assurance, and vice versa. The Common Criteria, by contrast, support "protection profiles", which are collections of security features that are needed to solve defined security problems. The entire universe of features can be combined and re-combined to create different protection profiles for different applications. The set of features is distinct from the desired assurance level. Different products can be designed to offer the same protection profile, but at different assurance levels. This was not possible under the Orange Book scheme.

The Common Criteria are also broader in scope than the Orange Book. The Orange Book criteria aimed mainly at confidentiality issues. The Common Criteria include guidelines for integrity and availability features.

From an MLS perspective, the Common Criteria are less clear that the Orange Book ([NEU 2004], Section 2.3.5). The Orange Book, along with [DOD 1985b], made it clear what class of system was required for MLS operations. There is no equivalent to [DOD 1985b] for the Common Criteria. The Common Criteria does include an equivalence ranking between its evaluation assurance levels (EALs) and the Orange Book evaluation classes. There are seven hierarchical EALs, with 1 being the lowest and 7 the highest. EAL4 is defined as equivalent to the assurance of class B1. EAL7 is equivalent to class A1 ([SYN 2004], page 11). This comparison, though, focuses strictly on the level of assurance and not the functionality of security features.

The U.S. has published protection profiles that equate to Orange Book standards (e.g., [NSA 1999], [NSA 2001]). Nevertheless, an evaluated product could offer MLS features and assurance without being designed to comply with one of these protection profiles. Further, if a product has passed a Common Criteria evaluation with an assurance level of EAL 4 or higher, it does not mean the product is suitable for MLS operations.

2.4. Conclusion

The history of MLS computers is bound up with the history of efforts to evaluate their features. The existence of [NSA 1999] and [NSA 2001] indicates that the U.S. feels that the MLS principles first described around 30 years ago in [AND 1972] and [BEL 1976] are still useful. The relatively small number of products at EAL5 or higher indicates either (1) that it is still hard to make products that embody those principles or (2) that the demand for such products is small. Other, newer security models exist, but manufacturers have not embraced them in their products. The following quotation from [RYA 1997] still seems to apply, even though it dates from 1997: "In actuality, multi-level security is still in its infancy and our most valuable secrets are still protected by isolating our highly-classified systems. We know the [information users] cannot perform their missions effectively or efficiently without timely, accurate and complete information, yet today we cannot even send multi-level secure e-mail within [a single organization], much less solve the larger community-wide MLS problems."

3. PRODUCT CLASSES

3.1. Evaluated Products

The modern market space for multi-level security products is substantially different than it was fifteen years ago. In the late 1980s and early 1990s, MLS was defined by the "Orange Book" and consisted of well-defined criteria by which any product could be judged. Today, products tend toward point solutions that support the concept of linking numerous systems functioning in a System High mode of operation. There is very little that is multi-level secure in the "Orange Book" sense today, even with a somewhat widened definition of the term as presented in section 1.2.

To select products for consideration, the evaluated product lists (EPLs) from Canada, Germany, Japan, France, Australia, United States and the United Kingdom were examined. Efforts were concentrated on the Canadian and US EPLs.

The Common Criteria web site includes a list of evaluated products (http://www.commoncriteriaportal.org/public/consumer/index.php?menu=4). The Common Criteria web site organizes the listing by product type:

- Access control devices and systems
- Boundary protection devices and systems
- Databases
- Data protection
- Detection devices and systems
- Integrated circuits, smart cards, and smart card-related devices and systems
- Key management systems
- Network and network-related devices and systems
- Operating systems
- Other devices and systems

Many of the above product categories have at least some products evaluated at the EAL4 level. Most of the EAL5 products are in the "ICs, smart cards" product category. There is one EAL5 operating system. There are no EAL6 or EAL7 products listed.

The U.S. has its own CC products list at http://niap.nist.gov/cc-scheme/vpl/vpl_type.html. This list uses the following product categories:

- Anti-virus
- Biometrics
- Certificate management
- Firewalls
- Guards
- Intrusion Detection Systems / Intrusion Prevention Systems
- Key recovery
- Miscellaneous
- Mobile code
- Multiple domain solutions
- Network management
- Operating system
- Peripheral switch
- Public Key Infrastructure / Key Management Infrastructure
- Remote access
- Secure messaging
- Security management
- Sensitive data protection
- Single-level web server
- Smart cards
- Switches and routers
- System access control
- Tokens
- Trusted Database Management Systems
- Virtual Private Networks
- Wireless Local Area Networks

No product on the U.S. list is evaluated higher than EAL4. One product is under evaluation at the EAL5 level: XTS-400 STOP 6, an operating system from Digital Net. It is being evaluated under the Labelled Security Protection Profile [NSA 1999]. Some database products and a large number of firewalls are under evaluation at the EAL4 level.

Canada's evaluated product list (http://www.cse.dnd.ca/en/services/common_criteria/trusted_products.html) has only one product at EAL4 or higher: a cryptographic processor. Two firewalls, a PKI product, and the Sun Solaris 9 operating system are under evaluation in Canada for EAL4 or higher.

Most products that have been evaluated have not used a standard protection profile, preferring instead to use a custom protection profile. Thus, although a product might have a high assurance rating, there is no guarantee that the product does anything useful from an MLS perspective – the assurance is that it does what it has been evaluated to do. This is a fundamental difference between modern evaluated products and TCSEC evaluated products of the past.

Complicating the matter of potential products is that the demand for products to work immediately has caused organizations to use unevaluated products, sometimes in creative ways, to layer security onto their IT infrastructures. These Commercial Off-The-Shelf (COTS) products are often difficult to locate, and even more difficult to get a vendor to stand behind on the issue of data security in a Government of Canada context. Unevaluated products cannot be considered trusted and users of such products accept on faith that they function securely as advertised.

3.2. Classes

In order to organize products into groups with similar functionality, the following classes of MLS product have been identified. These classes capture the basic groupings of functionality available in the market for MLS products:

a. Switches – These products typically allow the switching of peripherals between two systems that may be operating with different sensitivities and security policies. The switches are marketed as secure in that they prevent the flow of data between the systems, while allowing a user to access either system. Switches provide separation of data only.

b. Data Protection Kits – These products typically allow the wiping of data between uses of shared resources such as printers and photocopiers. They are designed to give assurance that information is not retained in the device that might leak to another information domain when another user uses the resource. In effect, Data Protection Kits offer object re-use functionality and a type of periods processing functionality.

c. Periods Processing – These products are designed to allow the processing of multiple information domains on a single system, but only a single information domain may be processed at a time and all information is prevented from changing domains when the next processing period is to start. Periods processing products offer data separation and often some identification and authentication of users.

d. Applications – Modern applications may be designed with security in mind and support multiple information domains.

e. Trusted Guards – These products serve to provide assured separation between multiple information domains processing simultaneously. More advanced than switches, trusted guards allow information to flow in very restricted ways, and often support some kind of audit functionality. More advanced guards (e.g. firewalls) can implement complex security policies to control the flow of data between networks.

f. Trusted Operating Systems – These products are more like the traditional "Orange Book" multi-level secure products. They provide a secure operating environment for whatever application the user may choose to run. Typically, an operating system intended for MLS use will offer both mandatory and discretionary access controls, identification and authentication of users, auditing features, and separation of administrative roles.

4. CURRENT MLS PRODUCTS

This section describes a sample of products in each identified class. Most of these products have been evaluated under the Common Criteria or the Information Technology Security Evaluation Criteria (ITSEC), and appear on the various Evaluated Product Lists (EPLs) around the world. It is important to note that commercial products evolve quickly, thus a product that is on the list today may not be available tomorrow due to the release of a new version of the product.

Additionally, a product evaluated in one country may not appear on all countries' EPLs.

4.1. Switches

Switches provide a separation of data between shared resources, allowing the use of components in different information domains by common, shared components. Assurance that the switches do not allow the passage of data between the domains is primary evaluation criterion. The following figure shows the generic switched architecture.

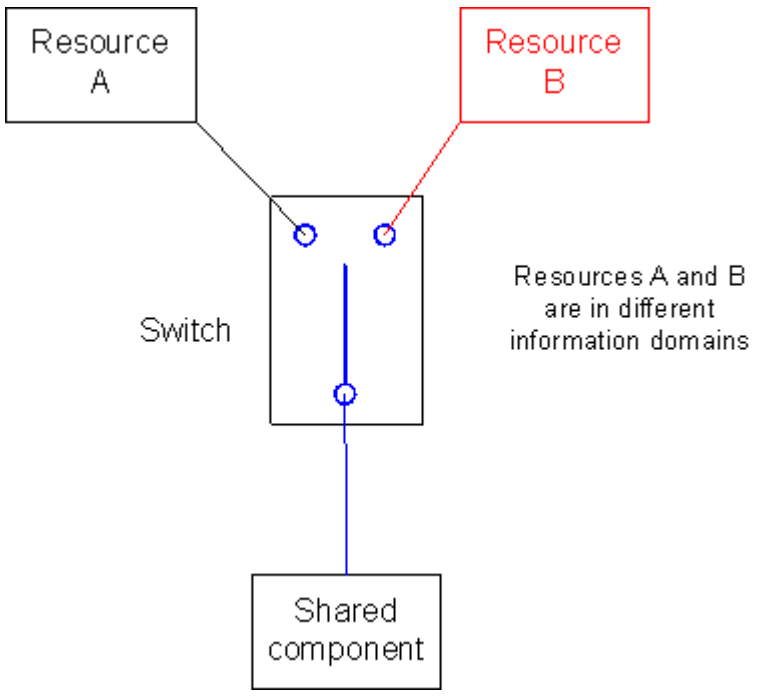

Figure 1 – A switch separating information domains

Switches cannot guarantee that information is not bridged between domains by the components being shared (i.e. a computer connected by a network switch to two secure networks could be

used to collect data in one network, store it, and switch to the other network to retransmit it; a keyboard switched between two computers could be modified to store information from one computer and retransmit it to another computer).

4.1.1 Domain-network Switch

SecureSwitch Dual Network Switch, Model 5000600
Certification Level: EAL4

Contact information:

Market Central Inc.
500 Business Center Drive,
Pittsburgh, PA 15205
USA
Phone: +1-412-494-2800
Fax: +1-412-494-5550

Product Web Site: http://www.mctech.com/secureswitch.html

The SecureSwitch® Dual Network Switch, Model #5000600 is a mechanical switch assembly that controls the connections to two separate networks. It provides the capability to connect to only one of the networks at any given time, and prevents crosstalk, or bleed-over, from one network to the other. This could be used to connect a single workstation to a sensitive and an unclassified network, allowing connectivity to only one network or the other at a given time, or to connect two workstations to two different networks, but only allow one workstation to have network access at a time.

The device consists of two separate mechanical switches, connected with a non-metallic bar that prevents both switches from being either open or closed at the same time. One switch must be open and one closed. The housing of the switch is non-metallic, to prevent conduction of any signal between the two separate networks. Additionally, internal to the device, each of the switch mechanisms is encased in a composite copper/iron shielding, to prevent any electromagnetic coupling of the two networks. The non-metallic housing of the device is assembled with tamper-resistant screws, to reduce the possibility of a user from gaining physical access to the composite copper/iron shielding, switches, and internal wiring.

The following electronic isolation metric shall apply to ensure there is a minimum isolation between two sides of an open switch:

- From 200 kHz to 300 kHz, the device shall show an attenuation greater than 78 dB.
- From 300 kHz to 1.3 MHz, the device shall show an attenuation greater than 78 dB.
- From 1.0 MHz to 11.0 MHz, the device shall show an attenuation greater than 79 dB.
- From 10.0 MHz to 110.0 MHz, the device shall show an attenuation greater than 75 dB.

Certification report: http://www.commoncriteriaportal.org/public/files/epfiles/VID-102-VR.pdf

4.1.2 Peripheral based Switch: (KVM)

Cybex(Avocent) SwitchView SC Series Switches
Certification Level: EAL4

Contact information:

Avocent
4991 Corporate Dr.
Huntsville, AL 35805
Phone: +1-256-430-4000
Fax: +1-256-430-4030
Toll Free: +1-866-286-2368

Product Web Site: http://www.avocent.com/web/en.nsf/Content/SwitchView+SC

This device allows the connection of a single keyboard, monitor, and mouse to many computers that may be processing in different information domains. The switch uses the built-in firmware to ensure that no data is passed to any other channel other than the one selected. The following lists the security features of this product:

- Automatically clears the keyboard buffer. No data is left on the switch.
- Cascading has been disabled to prevent any external device from detecting the presence of Avocent-Cybex SwitchView SC.
- All firmware is installed at Avocent headquarters.
- Firmware is encrypted to protect against tampering

Certification report: http://www.commoncriteriaportal.org/public/files/epfiles/ST_VID2014-VR.pdf

Interactive Link Multiple Computer Switch, V2.0
Certification Level: ITSEC E6 (in evaluation for Common Criteria EAL7)

Contact Information:

Head Office
Tenix Pty Limited,
100 Arthur St.,
North Sydney, NSW, 2060
Phone: +61 2 9963 9600
Fax: +61 2 9963 9690

Product Web Site: http://www.tenix.com/Main.asp?ID=732

This device allows the connection of a single keyboard, monitor, and mouse to many computers that may be processing in different information domains. It is a two-position switch, intended to be used for connecting to two PCs, one in a higher security network and one in a lower security network.

The company notes that using this product in conjunction with their Data Diodes can allow a secure transfer of information between information domains with assurance of no data leakage in the opposite direction.

Certification report:
http://www.dsd.gov.au/library/pdfdocs/EPL%20Listings%20ST&%20CRs/network_security_pdf/Tenix/InterLinkMultipleCompSwitchCR.pdf

4.1.3 Multi-Protocol Network Switch

MPS (Multi-Protocol Switch) 115, 145
Certification Level: EAL4

Contact Information:

Marconi Selenia Communications S.p.A.
Pomezia
Viale dell'Industria, 4
00040 Pomezia RM
Italy
Phone: +39 06 910911
Fax: +39 06 91091339

Product Web Site:
http://www.marconiselenia.com/site/_contentfiles/00005600/5673_mps%20eng.pdf

This product is an ATM switch intended for use in a military environment. It permits the association of security levels that can be assigned to its interfaces to allow security decisions to be made for data switching. Multi-level security is supported with audible notifications if a downgrade situation occurs, or downgrading can be prohibited. The switch provides quality of service/prioritization of traffic as specified in organizational policies.

This product has the following security features:

- Identification and authentication of users

- User data protection
- Intrusion detection
- Auditing
- Protection and recovery

Certification report: http://www.commoncriteriaportal.org/public/files/epfiles/CRP207.pdf

4.2. Data Protection Kits

These kits allow the sharing of peripheral devices between users operating in different information domains by eliminating object re-use issues and thereby reducing the possibility of data flowing from one domain to another.

4.2.1 Printer Kits

7145 Control Software 25.0000 (Konica Minolta)
Certification Level: EAL3

Contact Information:

Konica Minolta Business Solutions Inc.
100 Williams Drive
Ramsey, NJ 07446
Phone: +1-201-825-4000.

Product Web Site:
http://www.kmbs.konicaminolta.us/eprise/main/KMBS/Showroom/Models/960400?info=Features&Category=&PC=

This product is intended for use with the Konica Minolta 7145 series of printer/scanner devices. No description of this product was available beyond that contained in the certification report.

Certification Report: http://www.commoncriteriaportal.org/public/files/epfiles/c0007.pdf

Sharp Data Security Kit AR-FR1, AR-FR2, AR-FR3
Certification Level: EAL2

Contact Information:

Corporate Headquarters
Sharp Electronics Corporation
Sharp Plaza

Mahwah, New Jersey 07430
Phone: +1-201-529-8200

Product Web Site:
http://www.sharpusa.com/products/docsolutions/sharp_data_security_kit/0,2364,,00.html

Encrypts image data and overwrites the copier hard disk drive up to seven times after copy, scan or print jobs. This prevents leakage of data between uses.

Certification Report: http://www.commoncriteriaportal.org/public/files/epfiles/CCEVS-VID201-VR.pdf

Sharp Data Security KIT AR-FR4
Certification Level: EAL2

Contact Information:

Corporate Headquarters
Sharp Electronics Corporation
Sharp Plaza
Mahwah, New Jersey 07430
Phone: +1-201-529-8200

Product Web Site:
http://www.sharpusa.com/products/docsolutions/sharp_data_security_kit/0,2364,,00.html

Encrypts image data and overwrites the copier hard disk drive and memory up to seven times after copy, scan or print jobs. This prevents leakage of data between uses.

Certification Report: http://www.commoncriteriaportal.org/public/files/epfiles/ST_VID2012-VR.pdf

Sharp Data Security Kit AR-FR10
Certification Level: EAL3+

Contact Information:

Corporate Headquarters
Sharp Electronics Corporation
Sharp Plaza
Mahwah, New Jersey 07430
Phone: +1-201-529-8200

Product Web Site:
http://www.sharpusa.com/products/docsolutions/sharp_data_security_kit/0,2364,,00.html

Encrypts image data and overwrites the copier hard disk drive and memory up to seven times after copy, scan or print jobs. This prevents leakage of data between uses.

Certification Report: http://www.commoncriteriaportal.org/public/files/epfiles/c0006.pdf

Toshiba Scrambler Board GP-1010
Certification Level: EAL2

Contact Information:

Toshiba of Canada Limited
191 McNabb Street
Markham, ON L3R 8H2
Phone: +1-905-470-3500
Fax: +1-905-470-3509

Product Website: http://www.toshiba.ca/web/pdf/ScramblerBoard.pdf

This product encrypts information stored on the copier's hard disk drive with TDES encryption in order to protect against disclosure of information across information domains when copying information from different information domains.

Certification Report: http://www.commoncriteriaportal.org/public/files/epfiles/c0005.pdf

4.3. Periods Processing Systems

Periods processing allows the processing of information from multiple information domains on the same hardware, but prevents information from multiple information domains from being on the hardware simultaneously.

4.3.1 Complete Systems

Sentinel Model III
Certification Level: EAL4

Contact Information:

Delta Security Technologies
205 South Whiting Street
Suite 205
Alexandria, VA 22304

Phone: +1-703-751-9515
Fax: +1-703-751-6123

Product Web Site: http://www.delta-sec.com/products/product_overview.htm

This product allows a single IBM PC type computer to be used to process up to three sensitivity levels through the use of smart cards, data labelling to associate users and removable hard drives to information domains, and controlling the power to devices (removable hard drives, USB ports, network etc.) to prevent unauthorized use of the devices to process data.

Certification Report: http://www.commoncriteriaportal.org/public/files/epfiles/CCEVS-VID1000-VR.pdf

Supernet 2000 (G-Series)
Certification Level: EAL4

Contact Information:

Electronic Engineering Systems, Inc.
1403 Greenbrier Parkway,
Suite 400,
Chesapeake, VA 23320
Phone: +1-757-523-2929
Fax: +1-757-523-2455

Product Web Site: http://eescom.com/

This product implements periods processing on a single computer. The product incorporates a non-software dependent electromechanical switch that requires a high security key to manually change data domains. This key cannot be removed while the computer is operating within a sensitive domain. During any transition between states, the switch sends a hardware-reset signal that totally erases all temporary volatile PC memory. Separate hard drives each store a copy of an operating system and boot independently. The two domains are never active concurrently; therefore, no unauthorized user can penetrate the sensitive domain. The workstation also requires a key for the removable sensitive hard drive, to facilitate storage of the sensitive media in a safe. In addition, this product incorporates built-in Identification and Authentication mechanisms to prevent unauthorized access.

Certification Report: http://www.commoncriteriaportal.org/public/files/epfiles/TTAP-VR-0016.pdf

4.4. Applications

These are applications that are designed to be used in environments with multiple information domains.

4.4.1 Databases / Database Add-ons

Oracle Database v9i, Oracle Label Security [Label Security Add-on] for Oracle 9i
Certification Level: EAL 4+

Contact Information:

Oracle
500 Oracle Parkway
Redwood Shores, CA
94065
Phone: +1-650-506-7000

Product Web Site: http://www.oracle.com/technology/deploy/security/ols/index.html

This product can be used to enforce row-level Mandatory Access Control security policies within an Oracle 9i database. The product supports a hierarchical security label (e.g. TOP SECRET, SECRET, CONFIDENTIAL), a horizontal category security label (e.g. CANUS, CAN EYES ONLY), and a group security label that is used to record ownership of records. Users are assigned access rights by the database administrator. User access rights must dominate the sensitivity label of the row to be able to see that row in a query.

Without the Label Security Add-on, Oracle 9i provides highly detailed discretionary access controls to tables and rows.

Certification Reports: http://www.commoncriteriaportal.org/public/files/epfiles/CRP178.pdf, http://www.commoncriteriaportal.org/public/files/epfiles/CRP179.pdf

4.4.2 Message Handling

Thales Message Handling System
Certification Level: EAL3

Contact Information:

Ken Bowering
Director Business Development

Thales Systems Canada
Phone: +1-613-723-7000 ext: 202
Fax: +1-613-723-5600

Product Web Site: http://www.thales-systems.ca/products/mhs/mhs.htm

This product is a multi-user, network-based application that prepares, transmits, receives, and distributes radio teletype messages. The system provides the user with the ability to create, modify, store, distribute, send, and receive messages simultaneously over all channels in the communication system.

The product is a message handling system based on the Allied Communication Publication (ACP) 127 message format, a radio teletype standard, which is widely used in naval systems. However, the product does not support industry-standard e-mail protocols. It is designed to protect its user community against inadvertent or casual attempts to breach system security, and is appropriate for an assumed non-hostile and well-managed user community.

Access to messages is granted based on security labels of the message and the user wishing to have access to the message. The product is not recommended for use in situations where attempts to breach security might be made by hostile and well-funded attackers.

Certification Report:
http://www.commoncriteriaportal.org/public/files/epfiles/thales_mhs_report.pdf

Clearswift Bastion II
Certification Level: ITSEC E4

Contact Information:

Clearswift Corporation
15500 SE 30th Place
Suite 200
Bellevue, WA 98007
Phone: +1-425-460-6000
Fax: +1-425-460-6185

Product Website: http://www.clearswift.com/products/specialist/bastion/default.aspx

This product is intended to run on Trusted Solaris 8 (see section 4.6.1). Clearswift (CS) Bastion II is an application-level e-mail firewall designed for use between incompatible or mutually mistrusting subscriber networks. Its primary goal is to provide assured separation between two subscriber networks, while permitting limited authorized message transfer.

Certification Report: http://www.commoncriteriaportal.org/public/files/epfiles/CRP184.pdf

4.4.3 Web Portals

IBM WebSphere Portal Vesion 5.0.2
Certification Level: EAL2

Contact Information:

IBM Corporation
1133 Westchester Avenue
White Plains, New York 10604
United States

Product Web Site: http://www-306.ibm.com/software/info1/websphere/index.jsp?tab=products/portal

IBM WebSphere Portal 5.0.2 allows authorized users to establish protected portal resources. For example, authorized users can develop, share, and store information of the data types for web modules such as Portlet Application Definitions, Portlets, Content Nodes, User Groups, and URL Mapping contexts. This then allows for fast access to, and transfer of information between members of the team working on the same project.

When a user requests access to a resource from the web browser, WebSphere Portal relies upon WebSphere Application Server (WAS) to perform identification and management of users. The WebSphere Member Manager (WMM) is accessed to provide the group membership and a database for the mapping of users to roles and the actions to resources.

During the evaluation, the evaluation team confirmed the vendor's claims that there is no reliance upon the underlying operating systems for the product to perform its security functions. The difference in the operating system has no bearing upon the product's security functions.

Certification Report: http://niap.nist.gov/cc-scheme/st/ST_VID4038-VR.pdf

4.4.4 Miscellaneous Applications

Interactive Link Data Pump Applications, Version 3.0
Certification Level: ITSEC E6

Contact Information:

Tenix Pty Limited

100 Arthur St
North Sydney, NSW, 2060
Phone: +61 2 9963 9600
Fax: +61 2 9963 9690

Product Website: http://www.tenix.com/Main.asp?ID=734

Interactive Link Data Pump Applications allow client applications to transfer data between networks connected by the Interactive Link Data Diode. E-mail, file transfer, clipboard file transfer and data forwarding are supported. This is not a stand-alone product. The Interactive Link Data Diode Device is required.

This product supports an SMTP interface that can be used with content inspection products.

Certification Report:
http://www.dsd.gov.au/infosec/evaluation_services/epl/network_security/Tenix_InterLink.html

4.5. Trusted Guards

Trusted guards provide assured data flow between networks of differing sensitivity. Data flow may be unidirectional (Data Diodes) or may be based on a comprehensive security policy (Firewalls).

4.5.1 Data Diodes

BAE Systems Australia Trusted Filter
Certification Level: ITSEC E5

Contact Information: na.marketdevelopment@baesystems.com

Product Web Site: http://www.baesystems.com/ocs/australia/c3i2.htm

The BAE Systems Trusted Filter is a filter for asynchronous serial data that can be used in a number of applications, primarily to provide RED/BLACK separation in systems where BLACK equipment is remotely controlled from a RED area via a serial remote control port.

The product provides RED/BLACK separation in systems where control data, which cannot be protected by other means, must cross a RED/BLACK boundary. This is achieved by the filtering of RED data to produce “ORANGE” data. The control data is in the form of arbitrary length strings of characters. The control data is in plaintext.

Data passing from RED to BLACK is filtered in accordance with a table of allowable commands. The filter ensures that only control data of a pre-defined nature are passed. Only valid control data are passed to the BLACK area. Invalid control data are discarded.

The functioning of this devices is shown pictorially in the following figure:

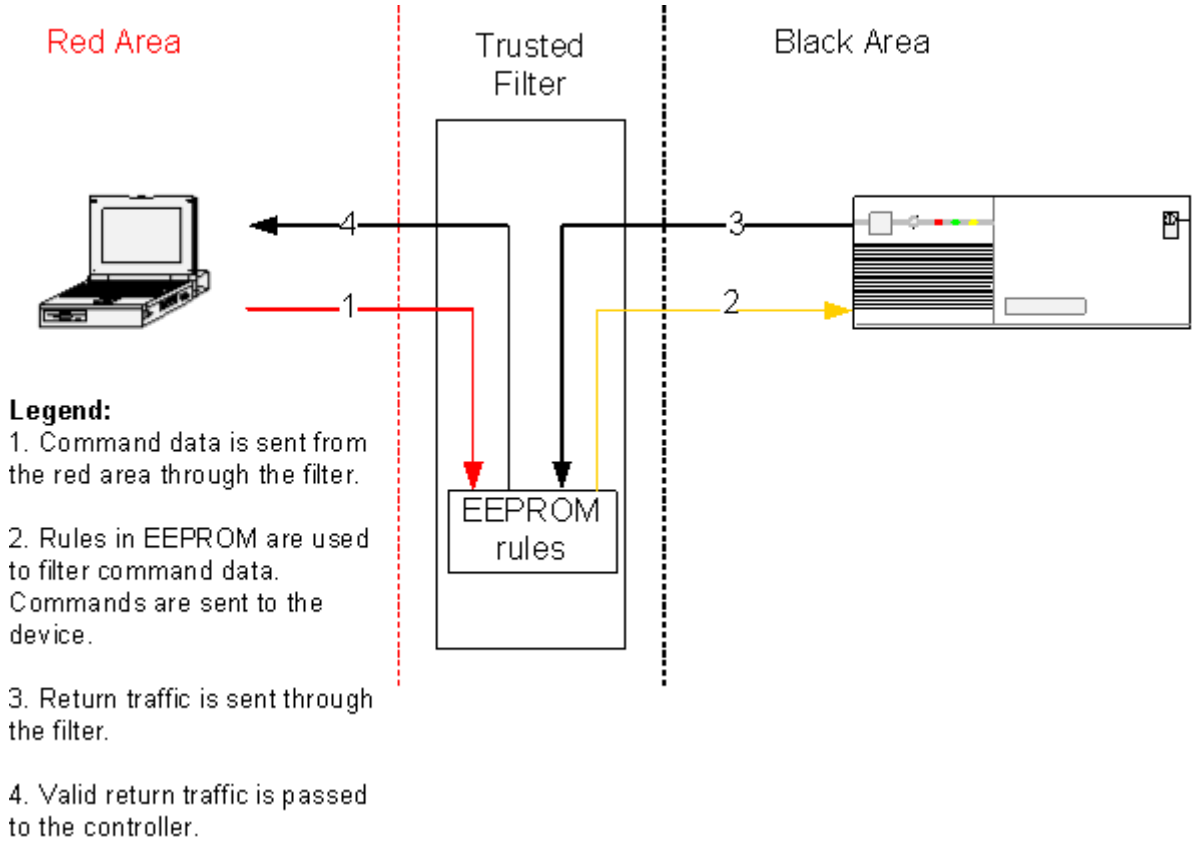

Figure 2 - BAE Trusted Filter operation

Allowable data tables are encoded in EPROM and are not modifiable in the field. There is no operator interface, except for two diagnostic LEDs.

Certification Report:
http://www.dsd.gov.au/infosec/evaluation_services/epl/network_security/BAESystems_TrustedFilter.html

Serial Data Regulator
Certification Level: ITSEC E6

Contact Information:

Compucat Research Pty Ltd
Box 3293,
Belconnen Business Centre
Canberra, ACT, 2616
Phone: +61 2 6253 4344

Product Web Site: http://www.compucat.com.au/images/pdf/SDR.pdf

The Serial Data Regulator provides a trusted method of transferring information, in one direction, between computer networks or communications systems that have different domain security policies. This device protects RS-232 connections only.

Certification Report:
http://www.dsd.gov.au/infosec/evaluation_services/epl/network_security/Compucat_SerialDataRegulator.html

Data Diodes V1.0/2.0
Certification Level: EAL2

Contact Information:

Owl Computing Technologies
P.O. Box 313,
19 North Salem Road (2nd Floor),
Cross River, NY, 10518
Phone: +1-914-763-6281
Fax: +1-914-763-6282

Product Web Site: http://www.owlcti.com/dfts.htm

This device is a combination of hardware and software that allows assured, one-way transfer of files between Microsoft Windows based computers. File transfer is done through a system of mirroring over fibre optic links. Data communication is performed by custom drivers, independent of the TCP/IP stack.

Certification Report: http://www.commoncriteriaportal.org/public/files/epfiles/ST_VID4000-VR.pdf

Interactive Link Data Diode Device, Version 1.2
Certification Level: ITSEC E6

Contact Information:

Tenix Pty Limited
100 Arthur St
North Sydney, NSW, 2060
Phone: +61 2 9963 9600
Fax: +61 2 9963 9690

Product Website: http://www.tenix.com/Main.asp?ID=734

This device is connected between networks of differing sensitivity levels. It allows an assured, one-way path to transfer data between the networks. Typically, this device would be used to allow information to flow from a low sensitivity network to a higher sensitivity network while blocking any information flowing backward from the higher sensitivity network to the lower sensitivity network.

Certification Report:
http://www.dsd.gov.au/infosec/evaluation_services/epl/network_security/Tenix_InterLinkDataDevice.html

4.5.2 Firewalls

Filtre Obligatoire Externe Firewall
Certification Level: ITSEC E4

Contact Information:

Land: Estelle Griton-Saulnier
Tel: +33(0)1 46 13 32 05
e-mail: estelle.griton@fr.thalesgroup.com

Joint / C4ISR: Morten Jarodd
Tel: +33(0)1 46 13 29 01
e-mail: morten.jarodd@fr.thalesgroup.com

Air & Naval: Eric Noel
Tel: +33(0)1 46 13 20 18
e-mail: eric.noel@fr.thalesgroup.com

Product Web Site: http://www.thales-communications.com/communications/portfolio/02_c4isr/06_ISS/04_firewalls/02_06_04.htm

This product is a full-featured TCP/IP firewall.

Certification Report: http://www.ssi.gouv.fr/site_documents/certificats/9905.pdf (French)

4.6. Trusted Operating Systems

These products are intended to be secure operating systems that support multiple users. In each case, security features have been added (or enhanced) to provide greater security.

4.6.1 Evaluated Operating Systems

XTS-400
Certification Level: EAL4+

Contact Information:

BAE Systems Information Technology
2525 Network Place
Herndon, VA 20171
Phone: +1-703-563-7500

Product Web Site:
http://www.digitalnet.com/solutions/information_assurance/xts/xts400_trusted_sys.htm

This product is a UNIX-like operating system with multi-level secure functionality. 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 [BEL 1976]; 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) that 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. The operating system also provides an alarm mechanism to detect the accumulation of events that indicate an imminent violation of the security policy.

Certification Report: http://www.commoncriteriaportal.org/public/files/epfiles/ST_VID3012-VR.pdf

Trusted IRIX/CMW version 6.5.13
Certification Level: EAL3

Contact Information:

SGI
1500 Crittenden Lane
Mountain View, CA 94043
Phone: +1-800-800-SGI1 (7441)

Product Web Site: http://www.commoncriteriaportal.org/public/files/epfiles/CCEVS-VID403-VR020020-SGI_TrustedIRIX.pdf

The Trusted IRIX operating system is a security-enhanced version of the IRIX operating system. In addition to the IRIX identity-based discretionary access control (DAC) on system resources, Trusted IRIX controls access to system resources based on the sensitivity and integrity labels of each resource. Trusted IRIX supports a set of access control policies; an identification and authentication capability to mediate and validate requests for entry into the system; an audit trail capability; and networking capability. The administrator guidance documents and product release notes provide the administrator with specific instructions to ensure that the product is installed in an appropriate environment.

Certification Report: http://www.commoncriteriaportal.org/public/files/epfiles/CCEVS-VID403-VR020020-SGI_TrustedIRIX.pdf

Trusted Solaris 8
Certification Level: EAL4

Contact Information:

Sun Microsystems of Canada Inc.
27 Allstate Parkway, 7th Floor
Markham, Ontario L3R 5L7
Canada

Phone: +1-905-477-6745
Fax: +1-905-477-9423

Product Web Site: http://wwws.sun.com/software/solaris/trustedsolaris/

Trusted Solaris 8 4/01 is a highly-configurable , UNIX-based operating system which has been developed to meet:

- 'Multi-Level' operation through Mandatory Access Control (MAC) functionality, including the use of sensitivity labels; and
- 'System High' operation through Discretionary Access Control (DAC) functionality, including the use of Access Control Lists (ACLs).

It meets the requirements of the Common Criteria (CC) Labeled Security Protection Profile (LSPP) and Controlled Access Protection Profile (CAPP), which are respectively equivalent to those of the B1 and C2 classes of the Trusted Computer System Evaluation Criteria.

Certification Report: http://www.commoncriteriaportal.org/public/files/epfiles/CRP170v3.pdf

4.6.2 Unevaluated Operating Systems

The following operating systems are not evaluated at any certification level; however, they are projects that are working on bringing MLS-type security features to commonly used operating systems. They are backed by several agencies including the NSA, and the Defence Advanced Research Projects Agency.

SELinux

Contact Information: selinux-team@tycho.nsa.gov

Product Web Site: http://www.nsa.gov/selinux/

This version of Linux has a strong, flexible mandatory access control (MAC) architecture incorporated into the major subsystems of the kernel. The system provides a mechanism to enforce the separation of information based on confidentiality and integrity requirements. This allows threats of tampering and bypassing of application security mechanisms to be addressed and enables the confinement of damage that can be caused by malicious or flawed applications.

The work is not intended as a complete security solution for Linux. Security-enhanced Linux is not an attempt to correct any flaws that may currently exist in Linux. Instead, it is simply an example of how mandatory access controls that can confine the actions of any process, including

a superuser process, can be added into Linux. The focus of the work has not been on system assurance or other security features such as security auditing, although these elements are also important for a secure system.

The security mechanisms implemented in the system provide flexible support for a wide range of security policies. They make it possible to configure the system to meet a wide range of security requirements. The release includes a general-purpose security policy configuration designed to meet a number of security objectives as an example of how this may be done. The flexibility of the system allows the policy to be modified and extended to customize the security policy as required for any given installation.

TrustedBSD

Contact Information:

Chris Costello <chris@FreeBSD.org>
Documentation

Chris Faulhaber <jedgar@FreeBSD.org>
Access Control Lists

Brian Feldman <green@FreeBSD.org>
MAC, SEBSD/SELinux

Ilmar Habibulin <ilmar@watson.org>
Capabilities, Mandatory Access Control

Thomas Moestl <tmm@FreeBSD.org>
Capabilities

Andrew Reisse <areisse@nailabs.com>
SEDarwin, Capabilities

Andrew Reiter <arr@FreeBSD.org>
Audit

Tom Rhodes <trhodes@FreeBSD.org>
Documentation

Wayne Salamon <wsalamon@computer.org>
SELinux, SEDarwin, Audit

Chris Vance <cvance@nailabs.com>
MAC, SEBSD/SELinux, SEDarwin

Robert Watson <rwatson@FreeBSD.org>
ACLs, MAC, SEBSD/SELinux, SEDarwin

Product Web Site: http://www.trustedbsd.org/

The TrustedBSD project provides a set of trusted operating system extensions to the FreeBSD operating system, targeting the Common Criteria for Information Technology Security Evaluation (CC). The project is still under development. Targeted features include:

- Extensible and audited authorization framework to support access control modules. This framework provides general-purpose labeling of kernel subjects/objects, centralized policy management, and access to a variety of run-time security events. This will allow the compile-time, boot-time, and run-time extension of the operating system security model based in both TrustedBSD access control modules, and third-party modules that employ the extension framework.
- Mandatory access control modules based on the framework supporting a variety of access control models, including fixed and floating label Biba integrity policies, the MLS confidentiality policy, Type Enforcement, and other customized policies designed for common FreeBSD deployment scenarios. In addition, the SELinux FLASK and Type Enforcement implementations will be provided via an SEBSD module, providing access to the higher level FLASK service abstraction, and mature TE implementation.
- Improvements in system privilege to reduce the level of risk associated with common system management functions.
- Access control lists for the file system and other kernel resources allowing fine-grained and manageable discretionary access control.
- Event auditing support, and single-host modular IDS system to monitor security events and notify administrators in the event of irregularities.

5. PRODUCT COMPARISON

The following table compares the security features of each product in a standardized format. It is important to note that it is not necessary for every product to have every feature, and the lack of a particular security feature is not necessarily indicative of a weaker security product.

Table 2 - Terms used in comparison

Term	Definition
Audit functionality	A product is considered to have audit functionality if it can provide a record of security relevant events in which it has participated.
Certified	A product is certified if it has been evaluated and achieved a rating under the Common Criteria (CC) or the Information Technology System Evaluation Criteria (ITSEC).
Data Separation functionality	A product provides data separation if it can separate the data of many information domains.
Discretionary Access Control functionality	A product provides discretionary access control when it provides security features that can be managed by unprivileged users (e.g. access control lists on operating system objects can be managed by the object's owner).
Hardware	A product is considered hardware if its primary components are physical devices.
Identification functionality	A product provides identification services if it can uniquely identify users.
Intrusion Detection functionality	Intrusion detection refers to the ability of a product to detect and indicate that it has been tampered with. See Tamper Resistance.
Mandatory Access Control functionality	A product provides mandatory access controls when it can identify the sensitivity of data (by labels or other means) and enforce a security policy based on the sensitivity of the data without user intervention.
Object Re-use functionality	A product provides object re-use if it takes steps to ensure that resources are sanitized before being re-used. This capability can be used to prevent leakage of data across information domains.
Roles	A product provides roles when it can provide different access rights for users and administrators based on their identity.

Term	Definition
Roll-back functionality	A product provides roll-back capability when it can reverse events to arrive at a previous state.
Software	A product is considered software if it is a logical program that must be loaded onto a physical device.
Tamper Resistance functionality	A product is tamper resistant if it cannot be modified without leaving traces. See Intrusion Detection.

Table 3 - Product feature comparison

	Product	Certified	HW/SW	Data Separation	Object Re-use	Identification	Discretionary Access Control	Mandatory Access Control	Audit	Roll-Back	Tamper Resistance / Intrusion Detection	Roles
Switches	Secure Switch Dual Network Switch	**EAL4**	**HW**	✓							✓	
	Cybex Switchview SC series	**EAL4**	**HW**	✓	✓						✓	
	Interactive Link Multiple Computer Switch	**E6**	**HW**	✓								

	Product	Certified	HW/SW	Data Separation	Object Re-use	Identification	Discretionary Access Control	Mandatory Access Control	Audit	Roll-Back	Tamper Resistance / Intrusion Detection	Roles
	Multi-Protocol Switch 115, 145	**EAL4**	**HW**	✓		✓			✓	✓	✓	
Data Protectoin Kits	7145 Control Software 25.0000	**EAL3**	**SW**	✓	✓							
	Sharp Data Security Kit AR-FR1, AR-FR2, AR-FR3	**EAL2**	**SW**	✓	✓							
	Sharp Data Security Kit AR-FR4	**EAL2**	**SW**	✓	✓							
	Sharp Data Security Kit AR-FR10	**EAL3+**	**SW**	✓	✓							
	Toshiba Scrambler Board GP-1010	**EAL2**	**HW**	✓	✓							

	Product	Certified	HW/SW	Data Separation	Object Re-use	Identification	Discretionary Access Control	Mandatory Access Control	Audit	Roll-Back	Tamper Resistance / Intrusion Detection	Roles
Periods Processing	Sentinel Model III	**EAL4**	**HW**	✓		✓		✓				
	Supernet 2000 (G-Series)	**EAL4**	**HW**	✓		✓		✓				
Applications	Oracle Database 9i, Oracle Label Security	**EAL4+**	**SW**			✓	✓	✓	✓	✓		✓
	Thales Message Handling System	**EAL3**	**SW**			✓	✓	✓				
	Clearswift Bastion II	**E4**	**SW**	✓								
	IBM Websphere Portal v5.0.2	**EAL2**	**SW**			✓	✓		✓			✓

	Product	Certified	HW/SW	Data Separation	Object Re-use	Identification	Discretionary Access Control	Mandatory Access Control	Audit	Roll-Back	Tamper Resistance / Intrusion Detection	Roles
	Interactive Link Data Pump Applications	**E6**	**SW + HW**	✓				✓				
Trusted Guards	BAE Systems Trusted Filter	**E5**	**HW**	✓				✓			✓	
	Serial Data Regulator	**E6**	**HW**	✓								
	Data Diode v1.0/v2.0	**EAL2**	**HW**	✓								
	Interactive Link Data Diode Device v1.2	**E6**	**HW**	✓								
	Filtre Obligatoire Externe Firewall	**E4**	**HW+ SW**	✓				✓	✓		✓	

	Product	Certified	HW/SW	Data Separation	Object Re-use	Identification	Discretionary Access Control	Mandatory Access Control	Audit	Roll-Back	Tamper Resistance / Intrusion Detection	Roles
Trusted Operating Systems	XTS-400	**EAL4+**	**SW**	✓		✓	✓	✓	✓		✓	✓
	Trusted IRIX CMW 6.5.13	**EAL3**	**SW**	✓		✓	✓	✓	✓			
	Trusted Solaris 8	**EAL4**	**SW**	✓		✓	✓	✓				
	SELinux	**N/A**	**SW**	✓		✓	✓	✓				
	Trusted BSD	**N/A**	**SW**	✓		✓	✓	✓	✓			✓

6. EMERGING TRENDS

There are two trends that appear to be emerging in MLS: the product trend, and the theoretical trend.

In the marketplace, the concept of MLS has factors against it that, over the years, have limited the number and types of product available. Since the primary consumer of MLS-type products has been governments, any company wishing to produce such a product has to expect a low volume of sales. This fact, combined with the high cost of having a product evaluated leads to an end product with a very high price and little opportunity to be sold.

Added to the cost of production, the time lines involved also detract from the marketability of the products. An evaluated version of a product might not reach the market until a year or more after non-evaluated but similar products. This leaves the MLS product behind in terms of technology, and complicates a potential vendor's ability to support the product. It also means that the secure products are not current and may be less capable than a non-evaluated, current version of the same or similar products. Vendors wishing to release evaluated products have to factor in the cost of obtaining an evaluation and the very limited appeal of an expensive evaluated product in the marketplace.

Since the overall price of hardware has dropped substantially over the last 15 years, it has become less necessary to have large, central computers to process multi-level data from a wide community of users if sharing of information is not a crucial concern. The lower cost of hardware has made it advantageous to build small networks of systems working in a Dedicated, or System High mode of operation. This fact has reduced the overall marketability of MLS operating systems and hardware. There remains a market to connect these Dedicated and System High systems that drives the creation of the types of products listed in this report.

Within products, wide media coverage of security issues in mass-marketed products has contributed to an ongoing improvement in vendor awareness of such issues. Microsoft Windows and Solaris 10 (http://www.sun.com/nc/04q4/) have substantial security improvements, for example, even if they are not evaluated under the Common Criteria.

Consequently, market pressure has driven and will probably continue to drive vendors toward very specific, point solutions that are evaluated on custom protection profiles, but this is not satisfactory; standards bodies (IETF, Governments) need to provide protection profiles with good functionality, and customers need to demand (and be prepared to pay for) products that are evaluated to those profiles. Where once large scale MLS systems were marketed, such as SCOMP or the various MLS UNIX releases, to run on secure hardware, now the market has more small devices designed to separate system-high communities and control data flow between them. Organizations wishing large-scale, centralized, TCSEC-style MLS solutions may have to explore having custom work done.

In the theoretical sphere, the trends seem to recognize that where once there were monolithic computers that processed data with multiple sensitivity levels and were used by people with differing security clearances, there are now heterogeneous meshes of hardware and software. The concentration leans toward the development of trust between connections and assurance that the software and hardware used within each domain functions as advertised and has no hidden features. Research continues on security models, security software, and development techniques.

To this end, standards bodies are emerging. The Trusted Computing Group (TCG, http://www.trustedcomputinggroup.org) is attempting to develop a specification to deliver enhanced hardware and OS based trusted computing platforms. Its goal is to define architectures, functions, and interfaces that can be used on a wide variety of computing platforms, including personal computers, cellular phones and other devices. TCG's intention is also to recommend practices and procedures for the operation and maintenance of secure systems in order to maintain trust.

The Information Assurance Technical Framework Forum (http://www.iatf.net) has developed a number of Common Criteria protection profiles, but again, these profiles are for various bits and parts of a heterogeneous system rather than a TCSEC-style MLS solution.

Other papers such as the Flask Design (http://www.nsa.gov/selinux/papers/flask.pdf) look at the requirements on each component of a system in order to meet the goals of a secure computing system.

7. CONCLUSION

Whereas at one time the MLS problem was one of enforcing security policies in a single place, the problem today has evolved into one of enforcing security policies across networks of widely varying equipment. Where once computer security was practically limited to a recognizable monolithic system, today miniaturization has extended the need for computer security into a multitude of new devices with varying capabilities (Personal Digital Assistants, MP3 Players, cellular phones, flash drives and so forth).

While vendors are putting more security functionality into their products, particularly in popular operating systems and applications, the small demand in the marketplace is limiting the number of evaluated products available to customers who prefer certified products. Complicating the issue further is the fact that where once a certification carried not only a guarantee of assurance, but also functionality (TCSEC evaluations), a modern certification only guarantees assurance that the product functions in the manner the vendor has chosen to have certified (ITSEC and CC custom protection profiles). This puts the onus on the customer to shop carefully for the functionality desired and possibly to assume some risk if functionality is not available in an evaluated product.

DOCUMENT CONTROL DATA

(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)

1. ORIGINATOR (the name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g. Establishment sponsoring a contractor's report, or tasking agency, are entered in section 8.)

AEPOS Technology Corporation, 200 Montcalm, Suite 200
Gatineau, Quebec, J8Y 3B5

2. SECURITY CLASSIFICATION (overall security classification of the document, including special warning terms if applicable)

UNCLASSIFIED

3. TITLE (the complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S,C or U) in parentheses after the title.)

Survey of Multi-Level Security (MLS) Products (U)

4. AUTHORS (Last name, first name, middle initial)

Detombe John, Cowan Darin, Smith Mike, and O'Brien John

5. DATE OF PUBLICATION (month and year of publication of document)	6a. NO. OF PAGES (total containing information. Include Annexes, Appendices, etc.)	6b. NO. OF REFS (total cited in document)
December 2004	48	19

7. DESCRIPTIVE NOTES (the category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Contractor Report (final)

8. SPONSORING ACTIVITY (the name of the department project office or laboratory sponsoring the research and development. Include the address.)

DRDC Ottawa, Information Operations Section, 3701 Carling Avenue Ottawa
K1A 0Z4

9a. PROJECT OR GRANT NO. (if appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant)	9b. CONTRACT NO. (if appropriate, the applicable number under which the document was written)
15bf27	W7714-4-2996

10a. ORIGINATOR'S DOCUMENT NUMBER (the official document number by which the document is identified by the originating activity. This number must be unique to this document.)	10b. OTHER DOCUMENT NOS. (Any other numbers which may be assigned this document either by the originator or by the sponsor)
	DRDC Ottawa CR 2004-268

11. DOCUMENT AVAILABILITY (any limitations on further dissemination of the document, other than those imposed by security classification)

(X) Unlimited distribution
( ) Distribution limited to defence departments and defence contractors; further distribution only as approved
( ) Distribution limited to defence departments and Canadian defence contractors; further distribution only as approved
( ) Distribution limited to government departments and agencies; further distribution only as approved
( ) Distribution limited to defence departments; further distribution only as approved
( ) Other (please specify):

12. DOCUMENT ANNOUNCEMENT (any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in 11) is possible, a wider announcement audience may be selected.)

Unlimited distribution of the announcement

13. ABSTRACT (a brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual).

Multi-level secure computer design began in the late 1960s.The work defined principles of multi-level secure computing: the concept of mandatory and discretionary access control, the Security Reference Monitor, audit, development practices, identification and authentication, formal descriptions, and a requirement that a multi-level secure computer had to be evaluated. It is upon this final requirement that the concept of trust in computing systems is built. This document is focused on products that are trustable, and thus have been evaluated.
That work led to the development of security standards for evaluation. First, the Trusted Computer System Evaluation Criteria (TCSEC) laid down standards for functionality and assurance for computer system. Later, many countries developed their own standards. This led to the development of a Common Criteria published in 1999.
The evolution of the evaluation criteria caused a change in focus. The TCSEP set out requirements for both total system functionality and assurance while new criteria focused on a more granular level of functionality and assurance.
The computer industry also changed greatly over this time. With hardware being more affordable, organizations could separate their information domains onto systems and networks operating at a single sensitivity level with the users all having a need-to-know and an appropriate security clearance. This caused a shift in the types of security products available in the marketplace. Where once there were many multi-level secure operating systems, now there are few. Instead, smaller, point solutions that have limited functionality but can be evaluated to high assurance have come on to the market. These products acts as data separators between single level network systems or as sentinels to ensure correct data flow. This document presents a survey of the multi-level secure product space, grouping the products with similar functionalities into classes, and allowing the readers to understand the functionalities that are available and compare products of any given class. This document should help readers building new MLS solutions from MLS products.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus. e.g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus-identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

Multi-Level Security, MLS, MLS products