Global Information Assurance Certification Paper

Muli-Level Security: Reality or Myth

Douglas D. Zellmer

GSEC Practical Requirements v.1.4.b

March 26, 2003

Abstract

A multi-level security (MLS) system is one where a single device is used to communicate or process data at different security classifications. Since the 1960's, Government and Intelligence agencies have sought a system that could access data from separate security classifications. They have a significant interest in the development and deployment of MLS networking as they can significantly reduce costs, ease administration functions, and provide significant efficiency improvements to the access of data.

This paper will provide descriptions of the various MLS technologies that have been developed as well as example products of each. Government agencies as well as commercial companies have developed a significant number of MLS products over the past several years. A representative sampling of these devices for each MLS technology is described in this paper to provide the reader with a sense of the MLS capabilities that exist today.

1 Introduction

"(MLS) Guards are the promise of the future…
unfortunately, they will always be."
Speaker at the March 1998 NSFF[1]

Just how far have we come in the area of multi-level security in the past five years? Are MLS products available today that can be successfully utilized in a network architecture that can be certified and accredited? This paper attempts to address these questions by providing an overview of multi-level security technologies and the products that have been developed to implement these technologies.

Multi-level security (MLS) is an overloaded term and can be used in various ways depending upon the source and context of the term. This can pose problems when discussing this topic as unique individuals often have different definitions and backgrounds when referring to MLS. It is imperative that a complete concept of operations of a project be fully defined and understood so that the MLS requirements can be clearly defined. This paper will describe some of the

[1] Network Security Framework Forum

technologies that support a multi-level security approach using products that are available today.

This paper will use the terms system-high and system-low to refer to two separate security enclaves when describing MLS technologies. In the commercial environment, system-high may refer to the internal corporate security enclave and system-low may refer to the external security enclave available from the World Wide Web (WWW). In the military environment, system-high may refer to a security enclave that processes data classified as Secret and system-low may refer to a security enclave that processes data that is unclassified.

2 Multi-Level Security Overview

Multi-level security, or MLS, is a capability that allows information with different classifications to be available in an information system with users having different security clearances, authorizations, or need-to-know, while preventing users from accessing information for which they are not cleared, do not have authorization, or do not have a need to know. MLS capabilities help overcome the operational constraints imposed by traditional approaches where security enclaves are separated by an airgap or connected only by *sneaker net*.

A discussion of multi-level security would not be complete with a discussion of the security models used in the design of MLS architectures. The Bell-LaPadula model concentrates on the confidentially aspects and defines two security axioms:

1. A subject cannot read information for which it is not cleared, often referred to as "*no read-up*" [1].
2. A subject cannot move information from system-high to system-low, often referred to as "*no write-down*" [1].

One of the limitations of the Bell-LaPadula model is that it deals only with confidentiality and does not account for the integrity of the information. The Biba Model [1] attempts to address this limitation by defining the following security axioms:

1. A subject may modify an object if the security level of a subject is at least as high as the security level of the object. [1]
2. A system-low object may not be passed to a system-high object. This prevents the corruption of system-high information by system-low information [1].

Why build and use an MLS system? Each of the MLS technologies described in this paper attempts to provide solutions to the multiple network approach. The multiple network approach requires the use of separate network infrastructures for each security enclave: one for system-high and one for system-low.

Military and Intelligence network architectures have historically segregated data based upon its security classification; for example Secret or Unclassified. In this architecture, devices are connected to networks based upon the classification of data that they process. A user that is required to access both system-high and system-low data would be required to use a unique device to access each type of data. Users working on system-high devices would be isolated from users working on system-low devices, which constrains users and reduces productivity. Also, the multiple network approach scenario requires redundant network infrastructures at additional cost.

MLS technologies have been developed to provide solutions to the multiple network approach. The benefits of each of the MLS solutions along with available products that provide these solutions will be described in the sections below.

3 Multi-Level Security Products

A thorough understanding of project requirements, communication paths and data types must be understood prior to the investigation of suitable MLS products. The MLS technologies in the sections below have been developed to meet the needs of specific MLS requirements. For example, if your requirement is to transmit e-mail between system-high and system-low enclaves, an MLS mail guard may be utilized in your architecture to meet this requirement.

It is also imperative that network architects understand the certification and accreditation requirements of their projects. In military MLS implementations, a certifying agent must approve the use of MLS devices and require the products to complete an extensive certification and accreditation process. INFOSEC provides assurance and certification services for MLS products and provides a catalogue of the products that they have certified [2]. Government agencies such as NSA and SABI also provide accreditation services for MLS products for military applications.

Most of the certification agencies follow a formal evaluation and certification process based upon a clearly defined set of criterion that is conducted by independent testing laboratories. One set of criteria is called the Common Criteria (CC) that has been ratified as ISO standard 15405 [2] and identifies the level of compliance as EAL1 through EAL7. ITSEC is another set of criteria used in Europe for the evaluation of products and systems and identifies the level of compliance as E1 through E6.

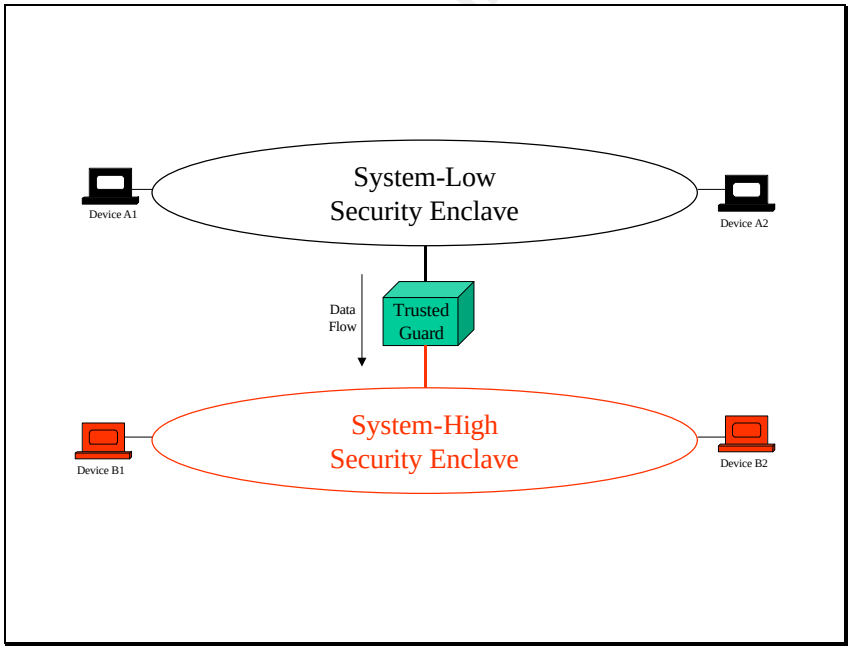
Another set of evaluation criteria used by the Department of Defense (DoD) is defined in DoD 5200.28-STD [3], also known as the "*Orange Book*" because of its orange cover. The level of compliance is identified by a combination of divisions (A, B, C, D) and classes within each division (1-3). MLS products are associated with divisions A and B. The orange book identifies the following classification levels shown in descending levels of assurance: A1, B3, B2, B1, C2, C1, and D.

3.1 MLS Trusted Guard Technology

A Trusted Guard is a device that is connected between two networks of different security classifications and provides a controlled data flow between these networks. Figure 3.1 shows two security enclaves connected via a trusted guard. In this scenario, files located in the system-low enclave could be transferred to the system-high enclave via the trusted guard product. [4]

A trusted guard is used when it is necessary to "*ride-up*" files from a system-low security enclave to a system-high security enclave. This type of MLS product has the capabilities to move large quantities of practically any type of data including imagery files, maps, and documents. It must be clearly understood that a trusted guard of this type will not allow data transfer from the system-high enclave to the system-low enclave. This mechanism is called "*write-down*" and it is not allowed by the Bell-LaPadula or Biba security models, not even to acknowledge receipt of data from the system-high device. This is to prevent a covert timing channel from the system-high enclave to the system-low enclave. A communication channel is covert if it is neither designed nor intended to transfer information at all. [5]

Figure 3.1 – Trusted Guard Technology



3.1.1 Trusted Gateway System (Trusted Computer Solutions)

The Trusted Gateway System (TGS) is a trusted guard MLS product available from Trusted Computer Solutions [6] and provides a secure one-way transfer of data from one network to another higher classification network. This system also provides the ability to virus scan selected file types prior to transferring the files to the system-

high enclave. If any virus is found, the file is automatically deleted and not transferred to the system-high enclave [6].

The TGS is software that is executed on a Trusted Computing Base (TCB). A TCB is a system that includes a trusted operating system and associated server hardware. A trusted operating system provides Mandatory Access Control (MAC) as well as other security features. MAC is access control that is not at the discretion of the user or operator but is mandated by the operation system. This ensures that users cannot accidentally or purposely circumvent the access control features of the operating system. In the case of the TGS, the TCB includes the Trusted Solaris Operating System ™ supported on the Sun UltraSPARC ™ family of servers [6].

The TGS contains an unclassified file system that is shared via NFS-mount to provide shared data space. File servers in the system-low enclave NFS-mount the TGS file system with read and write privileges while a file server in the system-high enclave NFS-mount the TGS file system with read privileges only. This prevents the high security file server from accidentally or intentionally writing classified data into this unclassified file system.

Users or applications in the system-low enclave place files on the unclassified file system of the TGS. A daemon on the TGS periodically checks the file system for new files and when it determines a new file is present it starts up a new process to transfer the file. The new process determines if the file requires a virus scan and if so, completes this action. The file is then transferred to the file server in the system-high enclave and the transfer is complete.

The security accreditation status is currently in process by the Secret and Below Interoperability (SABI) Program Office [6].

3.1.2 Radiant Mercury (Lockheed Martin)

Another Trusted Guard solution is the Radiant Mercury application developed by Lockheed Martin [7] for the United States Navy. This application also must run on a Trusted Computer Base. This application was developed to solve a specific problem where imagery data collected in a system-high enclave and needed to be downgraded and released under lower classification levels [7]. Note that in this case the data is transferred from the system-high enclave to the system-low enclave.

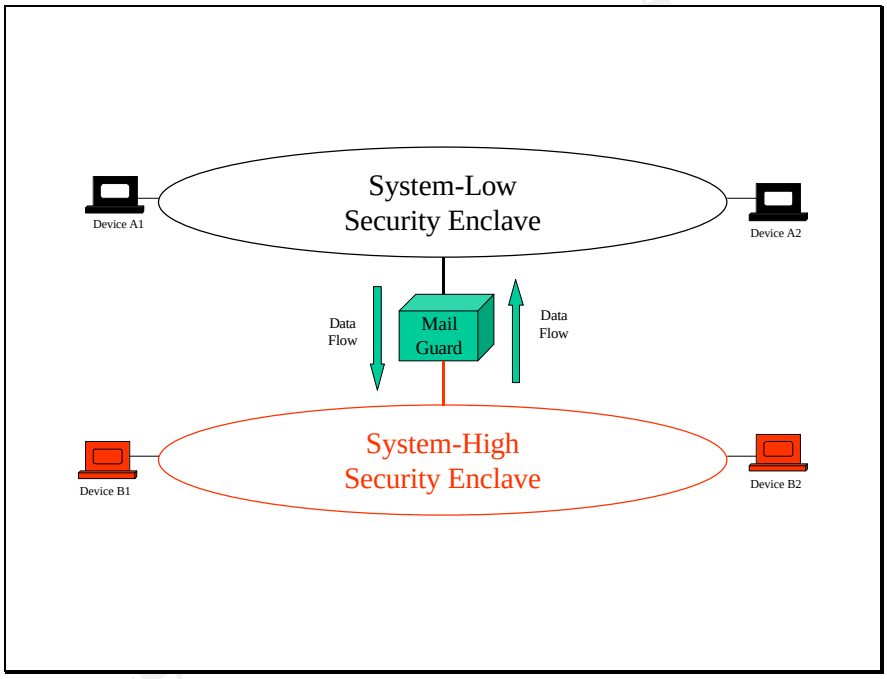
The Radiant Mercury application is designed to automatically sanitize and downgrade formatted classified files based on operator-modifiable rules. The automation of the sanitization and downgrade process decreases the time needed to perform the transfer and also eliminates human error. The system utilizes header information included in the classified files to determine classification status [7]. It has been suggested that this technology can be expanded to other automated multi-level security sanitization and redaction applications [7].

The National Security Agency (NSA) has accredited radiant Mercury for operational use [7]. It is quite an undertaking to develop a system that passes data from a system-high enclave to a system-low enclave. This device does not adhere to the Bell-LaPadula or Biba security models.

3.2 MLS Mail Guard Technology

A Mail Guard is a device that is connected between two security enclaves that provides controlled bi-directional flow of e-mail between these enclaves. Figure 3.2 shows two security enclaves connected via a Mail Guard. This allows users inside a secret enclave to communicate via unclassified electronic mail with users outside the enclave.

Figure 3.2 – Mail Guard Technology



E-mail connectivity has become so important that users working in a secret environment cannot be isolated without suffering significant disadvantages related to productivity, which is a common fate for groups operating in system-high security enclaves. The purpose of the Mail Guard is to solve this isolation problem and thereby enhance productivity.

3.2.1 Secure Network Server Mail Guard (SMG)

The Secure Network Server Mail Guard (SMG) is a MLS product available from Secure Computing Corporation [8] and provides a bi-directional transfer of electronic mail between security enclaves. The SMG is an application that must be executed

on a Trusted Computing Base (TCB) and provides the filters and logic to ensure the e-mail messages are “approved” for transfer between the security enclaves.

Filters provide the ability to configure the SMG based upon the security policy of the facility. Each e-mail and attachment must successfully traverse all configured filters before the e-mail message is delivered to the destination recipient. These filters are individually configured and each makes a message release decision based on detecting specific types of information in the e-mail message submitted for reclassification. The filters provided within the SMG include [8]:

- Sender/Recipient Address Filter – Source and destination address of the SMTP message must be included in a database of approved addresses.
- Classification Label Filter – The sender must include text in the body of the message indicating the security classification of the message contents.
- Attachment Type Filter – Any attachments to the message must be of a type approved by the filter.
- Attachment Review Filter – This filter will verify that attached files include a special tag and checksum indicating that the attachment was reviewed and approved.
- Digital Signature Filter – This filter verifies that the body of the message is formatted correctly and is signed using a digital signature and that the signature belongs to the authorized sender.
- Encryption Filter – This filter verifies that the body of the message is formatted correctly and is encrypted and signed using a digital signature and that the signature belongs to the authorized sender.

The configuration of the SMG requires the e-mail client of the sender as well as the e-mail client of the recipient to be configured appropriately or the filters will prevent the successful transmission of the message. These filters can be configured with very liberal or very strict filter policies and seem to provide great flexibility for the administrator.

Although e-mail traffic is not time critical, this author was surprised at the latency of a message as it traverses the SMG. Testing has indicated that an average latency of 52 seconds [8] was measured with no security filters enabled. With all filters enabled, an additional 53% latency [8] was observed.

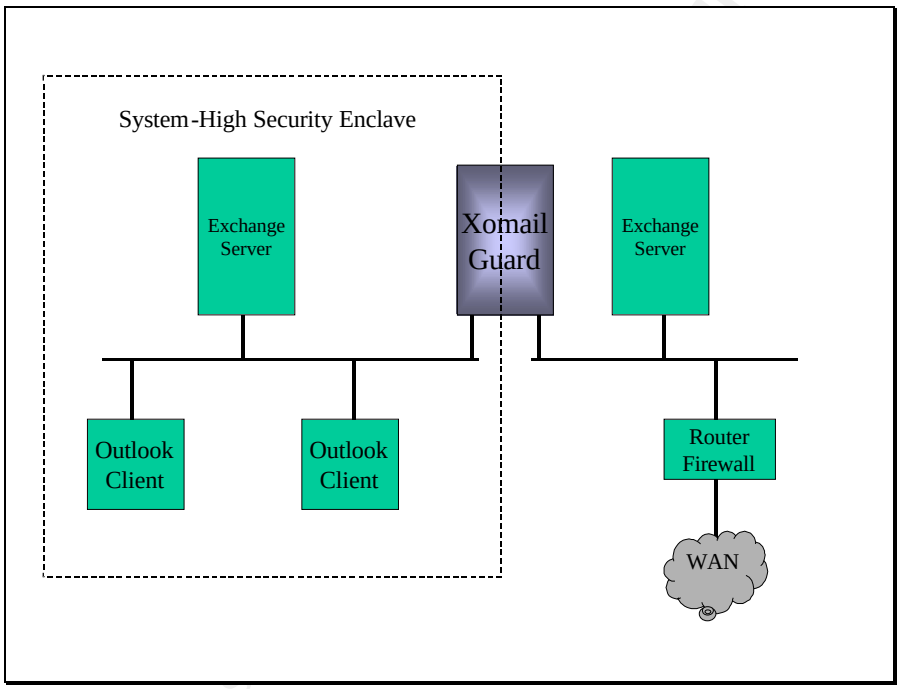
3.2.2 XOmail Guard (Thales Communications)

The XOmail Guard is an MLS product available from Thales Communications [9] and is focused on military applications for a secure messaging gateway guard between networks of different security classifications. This product has been certified according to the “Trusted Computer Systems Evaluation Criteria” TCSEC, sometimes referred to as the *Orange Book* [3]. The XOmail Guard is designed to use Security Labels that are contained in each message and allows only properly

labeled messages to pass through the device. Data other than properly formatted e-mail is disallowed.

Figure 3.2.2 is similar to a diagram in the product literature for the XOmail Guard [9] found on the Thales Communications web site. It depicts the network configuration required to utilize the product where an Exchange server is located in the system-high enclave and communicates to an external Exchange server through the XOmail Guard. Clients in the system-high enclave send and receive e-mail from Microsoft Outlook client software running the Windows operating system. Product literature indicates that an XOmail add-on to the Outlook client is required [9].

Figure 3.2 – XOmail Network Configuration



Although the product literature indicates that this product is certified, this author was unable to locate information regarding the certifying agency.

3.3 MLS Web Server Technology

An MLS Web server allows organizations to maintain a single web server that connects to multiple security enclaves avoiding the need to maintain multiple servers and data, one for each enclave. This single server can potentially support multiple organizations where there is a requirement to restrict access to information based upon classification levels.

3.3.1 MLS Web Server (Trusted Computer Solutions)

The MLS Web Server is an MLS Web Server available from Trusted Computer Solutions [10] that provides the ability to consolidate content previously maintained on separate servers and connects to multiple security enclaves. Users on remote hosts are granted access to data and information based upon their access authorizations. Additional options include extensions to support MLS database capabilities and SSL certificates for strong identification and authentication.

The MLS Web Server has been certified by the certified by the Defense Intelligence Agency (DIA) and security tested by the National Security Agency (NSA) [10].

3.3.2 Trusted Web Server (Trusted Systems Laboratories)

The Trusted Web Server available from Trusted Systems Laboratories is a multilevel web server built on a Trusted Solaris ™ TCB [11] that accesses and distributes data based upon the sensitivity of the information requested and the authorization of the requestor. It also provides the capability to securely vary the content of Web pages based on user authorizations and responds to standard HTTP and FTP requests compatible with standard Web browsers while providing customizable security policies for data at different levels of sensitivity.

The Trusted Web Server has been evaluated at an ITSEC E3 level [11].

3.3.3 Multilevel Secure (MLS) Web Server (Network Associates)

The Multilevel Secure (MLS) Web Server available from Network Associates [12] protects against unauthorized attempts by users to modify web data and protects against attempts to gain unauthorized access to sensitive information. It is supported on the Trusted Mach ™ (Tmach) systems Trusted Computing Base (TCB) [12].

This product achieves multi-level security by executing multiple instances of the web server program, one for every security enclave to which the device is connected. The result is that the web server program offering service to clients within a particular security enclave can only read data that is accessible to that enclave and any attempt to access data for other security enclaves is denied.

3.4 MLS Workstation Technology

MLS workstations are workstations that can separate and protect data of different security classifications. An MLS workstation is typically configured with two network connections, one for system-high connectivity and another for system-low connectivity with the intent to provide improved capabilities to the user because it supports both system-high and system-low functionality at a single workstation.

MLS workstations utilize a windowing environment where each window allows access to a single security enclave at a time. Cut and paste capabilities can be used to transfer data from the system-low to the system-high enclave or from system-high to system-low if the user has the appropriate privileges.

3.4.1 Ops/Intelligence Workstation (Trusted Computer Solutions)

The Ops/Intelligence Workstation (OIW) is a MLS Workstation available from Trusted Computer Solutions [13]. This workstation is designed to provide a user who requires access to data of differing classification levels and sources. This workstation is based on the Sun Trusted Solaris ™ operating system that has been approved to the ITSEC E3 level of assurance [13].

The OIW was designed to provide a secure environment for executing numerous applications at multiple security classification levels. These include word processing, spreadsheet and graphics applications, and full Microsoft Office compatibility. Web access to both system-high and system-low web servers is available simultaneously. The OIW can be used to re-label files (upgraded or downgraded) to different security classifications in their native format.

The Ops/Intelligence Workstation has been certified by the certified by the Defense Intelligence Agency (DIA) and security tested by the National Security Agency (NSA) [13].

4 Conclusion

MLS technology is real and in use today as evidenced by the numerous products available in the marketplace. Each of the MLS technologies described in this paper will continue to evolve with the computer and communications industry and will provide users with ever-increasing effectiveness in the work environment. MLS is an enabling technology as it enhances the availability of information while maintaining security. It is imperative that network architects understand what capabilities MLS can provide and to integrate these capabilities into network architectures when they provide enhanced effectiveness.

Although numerous MLS products exist today, it is clear that the addition of these security products will add complexity to a network infrastructure. I heard it stated that “security is the inverse of convenience”. MLS does not appear to be an exception to this axiom in 2003.

References:

1. Bosworth, Seymour. Computer Security Handbook. John Wiley & Sons, Inc. 2002. 17:12-21.

2. INFOSEC. "Directory of INFOSEC Assured Products 2002." 2002. URL: http://www.cesg.gov.uk/publications/media/brochures/directory.pdf (21 Mar. 2003).

3. Department of Defense, Trusted Computer System Evaluation Criteria, 1985, URL: http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.txt (12 Mar. 2003).

4. Epstein, Jeremy. "Architecture and Concepts of the ARGuE Guard.", 1999. URL: http://www.acsac.org/1999/papers/wed-b-1030-epstein.pdf. (2 Feb. 2003).

5. National Computer Security Center. "A Guide to Understanding Covert Channel Analysis of Trusted Systems." Nov. 1993. URL: http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-030.html. (15 Mar. 2003).

6. Trusted Computer Solutions, "Trusted Gateway System." 2001. URL: http://www.tcs-sec.com/products/trusted-gateway-system/trusted-gateway-system.html (2 Feb. 2003).

7. Pike, John. "Intelligence Resource Program." 26 Jan 2000. URL: http://www.fas.org/irp/program/disseminate/radiant_mercury.htm (16 Feb. 2003).

8. Smith, Richard E. "Constructing a High Assurance Mail Guard." URL: http://www.smat.us/crypto/docs/mailguard.pdf. (12 Feb. 2003).

9. Thales Communications. "XOmail/Guard." 27 Feb. 2001. URL: http://www.xomail.com/dl/xomail-guard.pdf. (27 Feb. 2003).

10. Trusted Computer Solutions, "TCS Secure Web Server." 2002. URL: http://www.tcs-sec.com/products/mls-web-server/mlsservr.pdf. (1 Mar. 2003).

11. Trusted Systems Laboratories. "Trusted Web Server." 2000. URL: http://www.trustedsyslabs.com/pdf/trusted_webserver.pdf. (10 Mar. 2003).

12. Network Associates. "A High Assurance, Multilevel Secure Web server." 2003. URL: http://www.nai.com/research/nailabs/finished-projects/a-high-assurance.asp. (14 Mar. 2003).

13. Trusted Computer Solutions, “Ops/Intelligence Workstation.” 2001. URL: http://www.tcs-sec.com/products/ops-intelligence-workstation/ops-intelligence-workstation.html. (2 Feb. 2003).