GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

LT Gary McKerrow

Multilevel Security Networks

An explanation of the problem

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Abstract

Processing electronic information of multiple security classifications has long been a goal of warfighters. While major strides have been taken in recent years in increasing the ability to fuse National information at levels above Top Secret (TS) with the shipboard tactical picture, the process remains primarily a manual one with the onboard Shipboard Sensitive Equipment Space (SSES) detachment and off-board National Sources providing contact and identification information to the Combat Information Center (CIC). Examples of this are Trap Tree, a General Security (GENSER) rebroadcast of Top Secret and Sensitive Compartmented Information, and Radiant Mercury, a method and process in which classified information is sanitized for use at a lower level.

This paper addresses the current efforts within the Department of Defense (DoD) to develop a Multi-Level Security (MLS) system. The regulations, requirements and processes for developing an MLS system within the DoD will be reviewed to illustrate their complexity, cost, and schedule constraints. Next, a look into the current technology on the Evaluated Product List will show that it can be structured to develop an MLS system for use with several new Navy acquisitions, Common Command and Decision (C&D), and DD 21. A top-level description of a MLS network is then developed from the components discussed. The ability to transition MLS systems such as these into the Fleet will require commitment, buy-in, and acceptance by other organizations within the Department of the Navy. While we call out the DoD solution, the same methodology and principles hold with in industry. While this paper deals with the Department of Defense requirements, the same methodology and practice can be applied to other networks with similar requirements.

© SANS Institute 2000 - 2005 Author retains full rights.

Introduction

The ability to process electronic information of multiple security classifications has long been a goal of warfighters. The process of Fusing National information at levels above Top Secret (TS) with the tactical picture being generated onboard the ship has been greatly improved in recent years, but remains primarily a manual one with the onboard Ship Sensitive Equipment Space (SSES) and off-board National Source detachments providing contact and identification information to the Combat Information Center (CIC). The aggressive manning goal stated by the DD 21 Operational Requirements Document (ORD) [1] requires that these functions be preformed only once. The Department of Defense goal for Multilevel security divides the different processing levels by classification, industry could very well divide the different level along the lines of products, financial, divisions, etc. There are currently two processes to obtain certification to meet multilevel security requirements, the first in the Trusted Product Evaluation Program also known as DoD 5200.28-STD [2], the second is a program known as the Common Criteria. This program involves multiple countries, and government agencies to develop standards and benchmarks to validate Information technology security.

The Standard

The history of organization-wide computer security within DoD dates back to 1967 when a task force was formed to provide guidance and recommendations on how to use computers and maintain security. This effort preceded the release of the first edition of DoD 5200.28 in 1972. The National Bureau of Standards and the Mitre Corporation [5, 6, 7, 8] continued the groundbreaking work of the task force. This work provides the foundation of the DoD 5200.28-STD [2]. These requirements and objectives can be broken down into three major headings: Security Policy, Accountability, and Assurance [2]. The goal of the requirements given in the Standard is to ensure that classified information stored in an electronic form has the same level of control and protection as classified information stored in a paper format. The foundation that this protection is based on is the Trusted Computer Base (TCB). The TCB includes those elements of hardware, firmware, and software that ensure the computer system provides the protection requirements of DoD 5200.28-STD.

What exactly are these protection requirements? Let us start by looking at an example with which we are all familiar, the classified library. When we enter the Library, the librarian asks us who we are and requests some sort of photographic identification. The librarian then checks the information against the library access database that provides the librarian with the levels of access we have been granted, as well as providing some indication of our "need to know". This process satisfies two requirements: security policy- a procedure (rule) to allow people access to the library and identification- information from you, such as your name and proof of that name, in the form of an identification card. A third requirement, marking, is familiar to all who have handled classified documents; this is the classification stamp at the top and bottom of each page, along with the cover sheet. When we request a document from the librarian, he or she produces the

© SANS Institute 2000 - 2005 Author retains full rights.

document along with a checkout form; this is accountability, yet another requirement. The procedures that are followed when we photocopy the document or take notes on the information are derived from the accountability requirement. All of these items are noted or logged so that the librarian has a record of who has had access to a particular document and what has happened with that document. There are two additional requirements assurance and continuous protection that are harder to see in our classified library example. The assurance requirement includes the spot checks, inventory, and user training performed by the organization that oversees the librarian. Continuous protection include those polices and procedures which the organization that controls the library has put in place to ensure that the librarian cannot change the operating procedures without a thorough security review of the changes requested. In this example, people provided the MLS framework. The goal is to provide this same degree of MLS for computer-based information and processes.

In review, the TCB must provide a security police function that controls access to information and must possesses the ability to mark or label the information such that classification is known to the computer system. The TCB must positively identify the user, and track what the user, or process invoked by the user, does with the information that is accessed. Further, there must be assurance in the design and production that the TCB cannot be compromised and that the upgrade process of the TCB allows for the continued protection of the information handled by the TCB and its computer system.

This Standard can be applied in two different ways. The first way excludes the application layer and focuses on the individual components. The second method focuses on the system and includes the application layer. The former is preformed by the Computer Security Center through the Commercial Product Evaluation Process. The latter, also preformed by the Computer Security Center, is known as a Security Evaluation. The result of either evaluation is the assignment of one of the following ratings: D, C1, C2, B1, B2, B3, or A1. When applied to an entire system, a rating gives a level of assurance that the system must meet. However, the Designated Approval Authority (DAA) retains responsibility for the overall security of their individual systems.

The lowest level of classification is Class D; this class is reserved for those systems that failed a higher level of testing. The only way products can be placed in this class is through evaluation by the Computer Security Center and failing. The second category is Class C, which is divided into two subclasses. In class C1 there are decretory controls allowing separation of users and data. However, there is an assumption within this class that all users are trusted. Depending on the application this may or may not be the case. The second subclass, C2, increases the rigor behind its separation of users and data and includes auditing of data actions. Windows NT 4.0 is an example of a C2 accredited Operating System. The next class B, further strengthens and adds requirements over Class C. Class B is divided into three subclasses. The B1 subclass improves on the requirements of C2 and strengthens the security policy and data marking requirements to include marking of exported data either by tagging the exported electronic media or including printed labels on a hard copy. Subclass B2 starts with a well-defined security policy incorporating all six-security requirements. In addition, this

© SANS Institute 2000 - 2005 Author retains full rights.

subclass starts addressing covert communications. Covert communications are communications between processes that violate the security polices of the TCB. In addition, life cycle issues are addressed for the first time in the B2 class. Subclass B3 further increases Class B2 requirements and ensures that the models are tamper proof. There is one subclass within class A, which is Class A1. Class A1 is functionally the same as class B3 the difference is in the formal design disclosure and insight into the design of the system.

The requirements to perform the necessary testing for the different categories are strict and expensive. The test team consists of at least two people with degrees in Computer Science and experience in assembly language programming and computer security testing theory. The team will independently verify the industry test program and results. Additionally, the test team must have sufficient understanding and insight into the system being tested to develop their own test program. The principal product that comes from this evaluation is the security users manual. This manual provides network administrators and system administrators the ability to set up and configure the system in a secure manner.

The differences between the categories (C, B, A) in the level of experience of the team members, the number of tests the test team must develop, and the amount of time the evaluation takes are extensive. For a Category C rating the test team, consisting of at least 2 people, must have bachelors degrees, develop and perform 5 tests, and spend not more than 3 months with 21 hands-on hours in testing. For a Category B rating, the team consists of at least 2 people with at least one having a Masters in Computer Science, both fluent in the source code language of the system, who develop and implement 15 tests, spending not more than 4 months with 30 hands-on hours testing the system. The team for a Category A system must have at least 2members, both with Masters Degrees, both being fluent in the source code language for the system, and both having a thorough understanding of design details to include maintenance and diagnostic programs. They must develop 25 tests and spend not more than 6months with 50 hands-on hours in testing. The times listed are all for testing. The test team could spend several years gaining the background understanding of the system before the test program actually begins.

The Commercial Product Evaluation Process has three different processes: Preliminary Product Evaluation, Formal Product Evaluation, and the Evaluated Product List. The Preliminary Product Evaluation is a process that allows the manufacturer to bring in the government test team to exchange early design information and to allow the test team to help with design decisions that relate to security. All information obtained on the system in development is proprietary to the vendor doing the design work. The Formal Product Evaluation is conducted on a system that is ready for production. The test team provides feedback during testing to allow the vendor to correct as many problems as possible before the report is complete. Once the Formal Product Evaluation is complete, the product is placed on the Evaluated Product List. As seen in Table 1, there have not been many products developed to meet DoD 5200.28–STD. The number of vendors with suitable products is also very small, because there is little incentive in the commercial market for new companies to produce products that meet the requirements

© SANS Institute 2000 - 2005 Author retains full rights.

listed in this section. [4]

Table 1. Number of Elements By Class

Class	Operating Systems	Network Components	Applications	Vendors
A1	0	2	0	2
B3	6	0	0	1
B2	2	3	0	2
B1	16	3	4	11
C2	15	3	4	10
C1	No longer evaluated at this class			

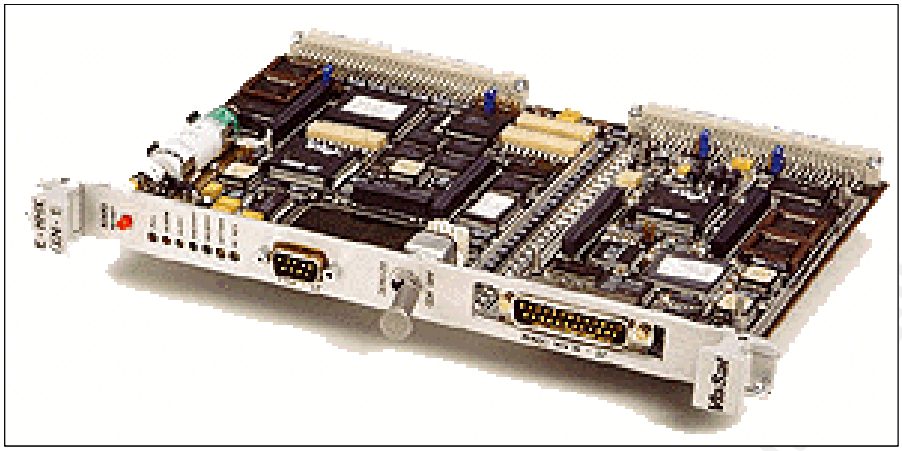
Common Criteria

A joint venture by the United States, United Kingdom, Germany, France, Canada, and the Netherlands to establish international requirements for security, the product of their work is the Common Criteria for Information Technology Security Evaluation (CCITSE) or Common Criteria. The Common Criteria loosely follows the DoD 5200.28 Standard; change the names from trust level to protection profiles. There are two primary differences between the two standards, first the Protection Profiles of the Common Criteria allow different features and assurances to be bound together in any combination, the other difference is that there are unlimited number of Protection Profile combination, vice the fixed number in the DoD 5200.28-STD [4]. The Common Criteria has not yet gained wide spread approval through the Government, and most of the products are still required to be evaluated under the DoD 5200.28-STD processes. The NSA is working on mapping the Trust Levels of the Standard to the Protection Profiles of the Common Criteria. As an example, the NSA has published a Controlled Access Protection Profile, which is based on the DoD 5200.28-STD C2 level of trust [4]. The most common example of a C2 system is that of Microsoft Windows NT 4.0 when configured as specified in the "C2 Administrator's and User's Security Guild Revision 1.1" [11].

Technologies

Technology, both hardware and software, is developing at a rate that follows Moore's Law and, as such, must be continually monitored with respect to the availability of new technologies and improvements in old technologies. In this section, we will address several technologies that have ratings from the Evaluated Product List. These products can be used separately or together to develop an MLS computer system.

© SANS Institute 2000 - 2005 Author retains full rights.



Network Interface Cards (NIC)

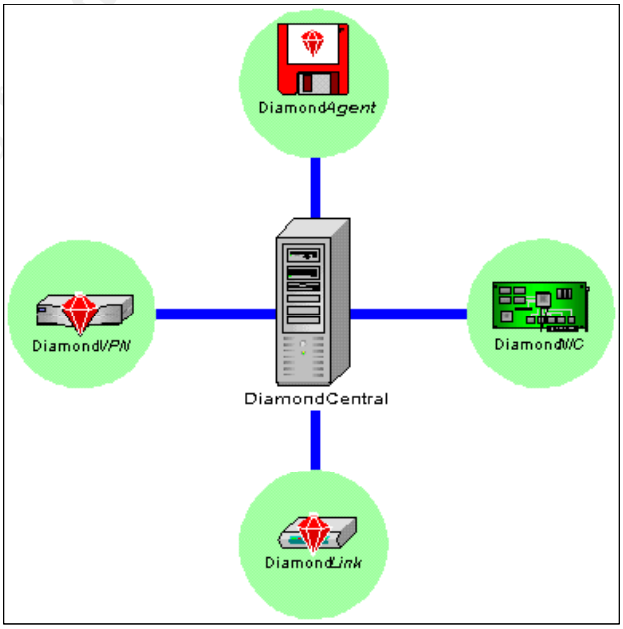
Figure 1. ViaSat Embeddable INFOSEC Product

The National Security Agency (NSA) has entered into a corporate business arrangement with two companies to develop Internet Protocol (IP) or Asynchronous Transfer Mode (ATM) network interface cards with onboard Type I encryption and decryption ability.

The first company is ViaSat, headquartered in Carlsbad, California [10]. ViaSat has developed a flexible device for a VME chassis. The Embeddable INFOSEC Product (EIP) fully supports the Transmission Control Protocol / Internet Protocol (TCP/IP) at T1 rates (1.544 Mbps). The device, shown in Figure 1, has the ability to handle 64 different traffic encryption keys.

Figure 2. Cryptek DiminodCentral

The second product is from Cryptek Secure Communications located in Chantilly,



© SANS Institute 2000 - 2005 Author retains full rights.



Virginia. Cryptek offers a complete system called DiamondTek to manage security [11]. This product is on the Evaluated Product List, at the B2 level. DiamondTek is currently undergoing testing for the approval of Type 1 encryption keys for use within the different components of the system. Type 1 encryption keys are those keys utilized by the DoD for transmit of classified information from one point to another. The heart of the system is a server called Diamond Central. This product allows for the centralized control of Information Security, audits and alarms, and updates to the other components. Diamond NIC is the network card for the client machines. The NIC provides filtering similar to a firewall as well as supporting Internet Protocol Security (IPSec) protocols. The NIC communicates with DiamondCentral allowing for central controlling on the network cards, freeing the user from some of the responsibility. In addition, other part of the

DiamondTek system are the DiamondLink an external network adapter, DiamondVPN providing for site to site virtual private network encryption, and DiamondAgent a windows operating software application that allow mobile users to access the DiamondTek system from outside the network (see Figure 2). All of the elements work with the DiamondCentral to provide a robust security network geared towards commercial products and standards. With the B2 rating from the Computer Security Center, the system has the ability to be the core of a network's MLS communications system at the transport and physical layers.

Operating Systems

One of the few certified operating systems from Wang Government Services, Inc, is a system called the XTS-300, which is a computer running an Intel Pentium II/III processor (see Figure 3). The operating system is called STOP 5.2.E and has four components - Security Kernel, TCB System Services, Trusted Software, and Commodity Application Systems Services (CASS). The first three components, Security Kernel, TCB System Services, and Trusted Software, along with the hardware make up the Trusted Computer Base of the XTS-300. The Security Kernel, as the name implies, is the kernel of the operating system and provides for all mandatory, subtype access control functions. The TCB System Services provides for the file system, handles user input / output operations and implements, along with part of the Security Kernel, the

© SANS Institute 2000 - 2005 Author retains full rights.



discretionary access control. The Trusted Software layer provides for user commands and the remaining security requirements. The final layer, the CASS, supports both the UNIX System V and INTEL 386 Family Binary Compatibility Specification 2 interface specifications, allowing for third party software utilization. This means that a windows type environment is supported within XTS-300, modeled on either the UNIX-X window or the Microsoft model, supported by Graphical User Interface (GUI) development. The hardware of the XTS-300 is a standard Pentium II / III processor with Intel motherboards and chip sets.

Figure 3. XTS 300 [13]

The hardware supports Integrated Systems Architecture (ISA), Product Configuration Identification (PCI), and Small Computer Systems Interface (SCSI) interfaces. The hardware also supports the Personal Computer Memory Card Interface Association (PCMCIA / PC) card reader for Fortezza type encryption devices, hard disks to 36.4 GB, Super Video Graphics Array (SVGA) video cards, and CD Rom drives with both parallel and serial ports.

The XTS-300 holds a B3 rating in accordance with reference [2]. The system can support 2 processors, 19 users, and 200 processes running at different classification levels. While network protocols are supported, they are outside the TCB, and must be handled by a different security method. The system is currently being accredited in several different MLS situations. A weakness of this system is that the network interface is outside the TCB; however, using a network card, from either the ViaSat or Cryptek, would allow a network of several XTS-300s to be incorporated together as we will see in the next section.

Network Design

With the information provided in the above sections, let us look at how a network could be configured to allow for Multi-Level Access to information in support of an R&D activity. The network we build will has the following top-level requirements. The information will consists of information classified at the Sensitive but Unclassified (SBU),

© SANS Institute 2000 - 2005 Author retains full rights.

Confidential, and Secret levels. The SBU network will have the ability to connect to the World Wide Web. Due to the interconnection between the other two classification levels (Networks), a SIPERNET connection is not provided for. A server is provided in each classification level, providing for data storage. For each user or resource within the network, an access type will be assigned. The Types provided for are shown in Table 2 below. The bold entries indicate the native classification for the type.

Table 2 . Access Levels

	SBU	Confidential	Secret
Type 1	**X**		
Type 2		**X**	
Type 3	X	**X**	
Type 4			**X**
Type 5	X	X	**X**

A lower type is not allowed to access a higher type. A higher type may access a lower type, and the information will be stored at accessing machines native classification level. To the maximum extent possible, the differences between type 1, 2 and 4 computers will be logical, vice physical. In other words, the different types will be collocated and connected to the same network infrastructure.

An Implication

An implementation, such as that shown in Figure 4, will consist of several nodes. The nodes could be interconnected via the Navy Marine Corp Internet, a building Local Area Network, or the Internet. There are two types of nodes, Central and Processing Nodes. Within each node, the workstations and servers will all be interconnected via a switch. The connection point to the node will consist of three systems, router, DiamondVPN, and a firewall. The router will have fixed routes assigned to the different nodes of the network. The firewall will be configured in accordance with the Navy Firewall Policy, and modified for local conditions. The DiamondVPN will provide additional protection and encryption for the traffic between nodes.

© SANS Institute 2000 - 2005 Author retains full rights.

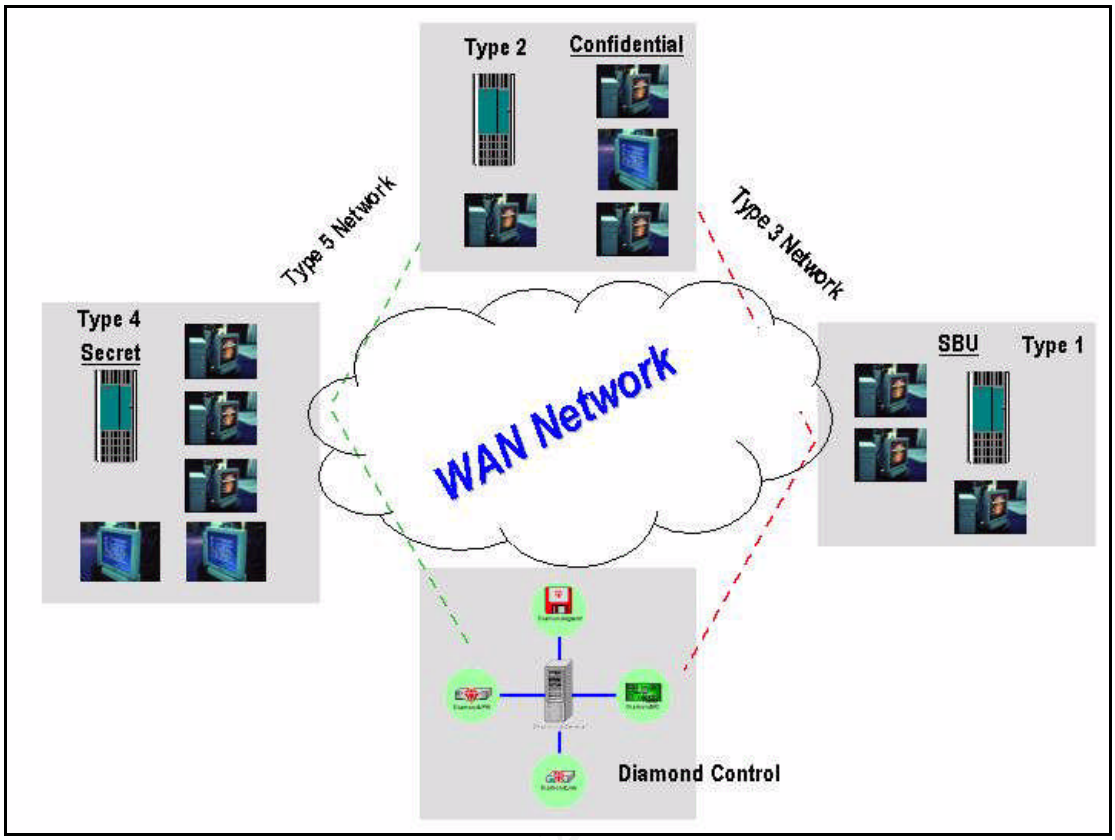


Figure 4. MLS Network

The implementation provides for two types of workstations. The first, will operate at a given type (1, 2, or 4), is a Windows NT 4.0 workstation configured in accordance with Microsoft's C2 Administrator's and User's Security Guild Revision 1.1, [12]. The workstation will be clearly marked as to the access type supported. The second type of workstations is the Wang Federal XTS-300 from the proceeding section. On the XTS-300, each user and process will have an access type assigned (3 or 5) allowing him the ability to access the different primary types. The ability to work on documents and save documents at the primary levels is easily supported on the XTS-300, as well as the ability to move data from lower to higher access types. Movement of information from High to Low is not supported at this time.

There will be a minimum of one server (Windows NT 4.0) in each node per type supported within the node. This server proposes is to provide for domain control within the node. Further, the server will be available to back up the servers in the other nodes. In addition to this, a node may have data servers, which house the information or application for the network. These servers will maintain an image of the data on the master servers.

There are two basic types of nodes. First is the control node. This node houses

© SANS Institute 2000 - 2005 Author retains full rights.

the DiamondCentral server for the network. The main servers are located in this node as well. The second type of node is the processing node. Each processing node consists of the connection point; a minimum of one server per access type supported with in the node (for domain control), and as many workstations (type 1 or 2) as required to support the node requirements.

This network has been described, and the parts can be easily assembled, there is still much work that needs to be accomplished. We presuppose that Cryptek has received the Type 1 crypto keys for the DiamondTek system. After that, the rest of the DITSCAP processes must be completed.

Conclusion

While the example shown above states requirements related to a government activity, namely classified information, a similar network can be set up in a corporate level, see Table 3. While the needed for the separation of information is currently not there in today's environment, the further expansion of e-business may well benefit from this type of approach.

Table 3. Industry example

	Project	Finical	Management
Type 1	**X**		
Type 2		**X**	
Type 3	X	**X**	
Type 4			**X**
Type 5	X	X	**X**

The ability to develop systems to handle MLS security with state-of-the art technology is currently available within the DoD. The drawbacks are the amount of time that the different evaluation, certification, and accreditation tasks require; the limited number of solutions currently available from the Evaluated Product List to build IA systems; and the different organizations responsible for the various functions. There is very little incentive for commercial products to undergo the stringent testing required for inclusion on the Evaluated Product List, both from a financial and technical standpoint. The insight that the Computer Security Center needs to perform Formal Technical Evaluation is extensive; insight needs to start at product conception. This requires the Government's "help" throughout the design process, and while there are non-disclosure agreements in place, industry is not comfortable with these practices.

The amount of time required to perform an evaluation should be yet another

© SANS Institute 2000 - 2005 Author retains full rights.

concern for the Government, and industry. Currently the Formal Technical Evaluation, depending on the level sought, takes between 2 and 6 months to complete. However, the amount of time that the evaluators need to become knowledgeable in the design and software of the systems in question can run into several years. This means that the systems fielded with an Evaluated Product rating is between one and two generations behind commercial products. The program office/vendors may wish to involve the Computer Security Center early in the design to keep the delay of introduction to a minimum. The other option is to include the Computer Security Center on the program office team so that the test and evaluation of the system in development includes the required test to support the Evaluated Product Evaluation.

As seen in the example the development of and implementation of a MLS network is possible today, the biggest disadvantage to this network is the inability to support high to low data translation. A good deal of research and development is documented in some sort of an Office Suite product, document, spreadsheet, or presentation. One of the biggest examples of this is the Microsoft Office suite. All of these tools store the information contained in them in proprietary binary files. Further, there are mechanisms built into these products to allow the recovery of pervious versions. The result is that it is not possible to just manually go in, remove classified information from these sources, and then deem them unclassified. Tools must be developed to remove the recovery information from these documents, which takes the corporation of the vendor. With Microsoft as an example, they have stated that they do not see the business case for MLS systems. This makes getting the proprietary information to develop and remove the hidden content of the documents a challenge.

© SANS Institute 2000 - 2005 Author retains full rights.

Bibliography

1. *Operational Requirements Document for Land Attack Destroyer* (DD 21), 5 November 1997

2. *Department of Defense Trusted Computer System Evaluation Criteria* (DoD 5200.28-STD), 26 December 1985

3. *DoD Information Technology Security Certification and Accreditation Process (DITSCAP)* (DODI 5200.28), 30 November 1999

4. Common Criteria Web Site. http://www.radium.ncsc.mil/tpep/library/ccitse/index.html

5. Evaluated Product Web Site. http://www.radium.ncsc.mil/tpep/epl/epl-by-class.html

5. Federal Information Processing Standards Publication (FIPS PUB) 39, *Glossary for Computer Systems Security*, 15 February 1976.

6. Lee, T. M. P., et al. "Processors, Operating Systems and Nearby Peripherals: A Consensus Report," in *Audit and Evaluation of Computer Security II: System Vulnerabilities and Controls*, Z. Ruthberg, ed., NBS Special Publication #500-57, MD78733, April 1980.

7. Lipner, S. B, *A Comment on the Confinement Problem*, MITRE Corp., Bedford, Mass.

8. Nibaldi, G. H, *Proposed Technical Evaluation Criteria for Trusted Computer Systems*, MITRE Corp., Bedford, Mass., M79-225, AD-A108-832, 25 October 1979.

9. OMB Circular A-123, *Internal Control Systems*, 5 November 1981.

10. ViaSat Web Site. http://www.viasat.com

11. Cryptek Web Site. http://www.cryptek.com

12. Microsoft Corporation, "*C2 Administrator's and User's Security Guild Revision 1.1*", Microsoft Corporation, 1998

13. Naval Postgraduate School Website. http://cisr.nps.navy.mil/Lab_Tour/Thesis.html

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.