1993-06

Multilevel security within the Army Tactical Command Control System: an implementation strategy

Loper, Kathleen Schmidt

Monterey, California. Naval Postgraduate School

http://hdl.handle.net/10945/27145

Multilevel Security within the Army Tactical Command and Control System: An Implementation Strategy

by

Kathleen S. Loper
Captain, United States Army
B.S., United States Military Academy

Submitted in partial fulfillment
of the requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS TECHNOLOGY

from the

NAVAL POSTGRADUATE SCHOOL
June 1993

Command, Control and Communications Academic Group

Inclassified
ecurity Classification of this page

REPORT DOCUMENTATION PAGE

1a Report Security Classification: Unclassified		1b Restrictive Markings			
2a Security Classification Authority		3 Distribution/Availability of Report Approved for public release; distribution is unlimited.			
2b Declassification/Downgrading Schedule					
4 Performing Organization Report Number(s)		5 Monitoring Organization Report Number(s)			
6a Name of Performing Organization Naval Postgraduate School	6b Office Symbol *(if applicable)* 39	7a Name of Monitoring Organization Naval Postgraduate School			
6c Address *(city, state, and ZIP code)* Monterey CA 93943-5000		7b Address *(city, state, and ZIP code)* Monterey CA 93943-5000			
8a Name of Funding/Sponsoring Organization	6b Office Symbol *(if applicable)*	9 Procurement Instrument Identification Number			
Address *(city, state, and ZIP code)*		10 Source of Funding Numbers			
		Program Element No	Project No	Task No	Work Unit Accession Nc

11 Title *(include security classification)* MULTILEVEL SECURITY WITHIN THE ARMY TACTICAL COMMAND AND CONTROL SYSTEM: AN IMPLEMENTATION STRATEGY

12 Personal Author(s) Loper, Kathleen Schmidt

13a Type of Report Master's Thesis	13b Time Covered From To	14 Date of Report *(year, month, day)* June 1993	15 Page Count 87

16 Supplementary Notation The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

17 Cosati Codes			18 Subject Terms *(continue on reverse if necessary and identify by block number)*
Field	Group	Subgroup	Multilevel Security, Computer Security, TCSEC, ATCCS, Trusted Workstation, Trusted DBMS Trusted Host, Trusted LAN, BLACKER, CANEWARE, ASAS

19 Abstract *(continue on reverse if necessary and identify by block number)*

As U.S. Forces continue to operate in coalition environments, the need to incorporate Multilevel Security into the ATCCS becomes more apparent. While Army doctrine requires the ATCCS to be MLS to the B2 level, there is currently no product or technology developed to fulfill this requirement, nor is there any implementation strategy devised to address this issue. This thesis proposes two strategies to implement MLS within the ATCCS: a target and near term implementation strategy. These two strategies are derived from the DoD Joint MLS Technology Insertion Program Target Architecture and Implementation Strategy, which provides the vehicle for assessing the current and in development MLS products and capabilities.

20 Distribution/Availability of Abstract _x_ unclassified/unlimited __ same as report __ DTIC users	21 Abstract Security Classification Unclassified	
22a Name of Responsible Individual Myung Suh	22b Telephone *(include Area Code)* (408) 656-2637	22c Office Symbol AS/Su

83 APR edition may be used until exhausted

All other editions are obsolete

security classification of this pag

Unclassifie

ABSTRACT

As U.S. forces continue to operate in coalition environments, the need to incorporate Multilevel Security into the ATCCS becomes more apparent. While Army doctrine requires the ATCCS to be MLS to the B2 level, there is currently no product or technology developed to fulfill this requirement, nor is there any implementation strategy devised to address this issue. This thesis proposes two strategies to implement MLS within the ATCCS: a target and near term implementation strategy. These two strategies are derived from the DoD Joint MLS Technology Insertion Program Target Architecture and Implementation Strategy, which provides the vehicle for assessing the current and in development MLS products and capabilities.

TABLE OF CONTENTS

I. INTRODUCTION 1

A. BACKGROUND & SCOPE 1

B. ORGANIZATION 2

II. COMPUTER SECURITY 4

A. INTRODUCTION TO THE ORANGE BOOK 4

B. DEFINITION OF COMPUTER SECURITY 5

1. Trusted Computing Base and Reference Validation Mechanism . . 6

2. Security Models 7

C. TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA . . . 9

1. Fundamental Computer Security Requirements 9

a. Security Policy 9

(1) Mandatory Access Control (MAC). 10

(2) Discretionary Access Control (DAC) 10

(3) Marking (Labels) 10

(4) Object reuse. 10

b. Accountability 11

c. Assurance 11

d. Documentation 12

2. Four divisions of security protection 13

a. D, Minimal Security 15

b. C, Discretionary and Controlled Access Protection 15

c. B, Mandatory Protection 16

d. A, Verified Protection 17

D. SECURITY OPERATING MODES 17

1. Dedicated Security Mode 17

2. System High Security Mode 18

3. Multilevel Security Mode 18

4. Controlled Security Mode 18

5. Compartmented Security Mode 19

E. RISK INDEX 19

F. SECURITY ENVIRONMENT 22

G. DETERMINING A SYSTEM'S SECURITY REQUIREMENT 23

H. NETWORK SECURITY 23

III. ARMY TACTICAL COMMAND AND CONTROL SYSTEM (ATCCS) . . 28

A. INTRODUCTION 28

B. BACKGROUND 28

C. ATCCS ARCHITECTURE- CCS2 30

1. BFA Control Systems 30

a. Force Level Control System 31

b. Functional Control System 32

(1) Maneuver 32

(2) Intelligence/Electronic Warfare (IEW). 33

(3) Fire Support 33

(4) Air Defense. 34

(5) Combat Service Support. 34

(6) Subordinate Systems. 35

2. Communications 35

a. Area Common User System (ACUS) 38

b. Combat Net Radio System (CNR) 38

c. Army Data Distribution System (ADDS) 38

D. REQUIREMENT FOR MLS 39

1. Host Computers 39

2. Local Area Networks 40

3. Wide Area Networks 40

E. SECURITY POLICIES AND REQUIREMENTS FOR THE ATCCS 41

IV. MLS Product Technology Assessment 46

A. BACKGROUND 46

B. TARGET ARCHITECTURE--2000 48

1. Trusted Local Area Network (LAN) 50

2. Untrusted LAN 50

3. Wide Area Network (WAN) 51

C. NEAR-TERM ARCHITECTURES 52

1. Guard Architecture 54

2. Workstation Architecture 58

3. LAN Architecture 59

4. Database Management System Architecture 60

5. Host Architecture 62

V. MLS IMPLEMENTATION WITHIN THE ATCCS 68

A. BACKGROUND 68

B. AN MLS ATCCS TARGET ARCHITECTURE 69

1. MLS Internal to ATCCS 69

2. MLS External to ATCCS 70

C. AN MLS ATCCS NEAR TERM ARCHITECTURE 70

1. MLS Internal to ATCCS 70

2. MLS External to ATCCS 70

a. WAN connectivity 70

b. Untrusted LAN connectivity 71

VI. CONCLUSION 72

LIST OF REFERENCES 74

INITIAL DISTRIBUTION LIST 76

LIST OF TABLES

TABLE I RATING SCALE FOR MINIMUM USER CLEARANCE 20

TABLE II RATING SCALE FOR MAXIMUM DATA SENSITIVITY 21

TABLE III COMPUTER SECURITY REQUIREMENTS FOR OPEN SECURITY ENVIRONMENTS 26

TABLE IV EVALUATION STRUCTURE FOR NETWORK SECURITY SERVICES 27

TABLE VI SELECTED GUARD OVERVIEW 64

LIST OF FIGURES

Figure 1 **Monitor Model of Access** 8

Figure 2 **Trusted Computer System Criteria** 14

Figure 3 **ACCS System Environment** 29

Figure 4 **CCS2 Vertical Architecture** 31

Figure 5 **CCS2 Needlines Representation** 36

Figure 6 **Vertical synchronization through CCS2** 37

Figure 7 **Target Architecture--2000** 49

Figure 8 **Workstation Architecture** 65

Figure 9 **LAN Architecture** 66

Figure 10 **Database Management System Architecture** 67

I. INTRODUCTION

A. BACKGROUND & SCOPE

As U.S. forces continue to operate in coalition environments, the need to incorporate Multilevel Security (MLS) into the ATCCS becomes more apparent. MLS within tactical communications is a necessity. Tactical units have a requirement to exchange information with adjacent units, unified command elements, senior components of the armed services and with national and allied agency information systems. This information exchange must be timely, efficient and protected to the proper security classification level to support all types of operations. Critical information, to include classified with compartmented caveats, often must be exchanged between allied force elements. Current tactical operations do not use automated multilevel security technology for data storage or transfer except in a very limited fashion. Dedicated equipment is used to create and store information for each level of security needed. Information is transferred using either dedicated (point-to-point) circuits or using a combination of bulk and/or end-to-end encryption. These methods fragment information, forcing the use of redundant databases which are manpower intensive, often inaccurate and outdated. Manual human review interfaces used to bridge this information gap are slow and error prone. MLS will facilitate the seamless data handling and communications capability required for Army operations. The Army Field Manual 24-7, *ATCCS System*

Management Techniques specifies the MLS requirements but does not include a plan on how it will be implemented.

The objective of this thesis is to present an MLS implementation strategy for the ATCCS.

The ATCCS is by definition a WAN but will be considered as a LAN in this thesis since it is viewed within the context of the Target architecture used by the Joint MLS Technology Insertion Program Target Architecture and Implementation Strategy (discussed shortly). The WAN represents the DCS and represents an external interface to the ATCCS. The LAN distinction is used merely for pedological purposes, and it does not change the nature of the ATCCS. This thesis will not try to justify or replace existing systems within the ATCCS in an attempt to make an MLS solution more convenient or easier. Rather, this thesis will attempt to apply the MLS and trusted products available or in development to bring the ATCCS closer to a fully MLS system.

B. ORGANIZATION

The second chapter, Computer Security, provides an executive summary of DoD 5200.28, the National Computer Security Center Trusted Computer System Evaluation Criteria, often referred to as the Orange Book. Of the 28 volumes, 27 are explanatory to the one primary volume, the Orange Book. This chapter provides an explanation of the basic security principles and not the finer details that are elaborated upon in the remaining explanatory volumes. This chapter serves as a primer to the reader unfamiliar with the security principles referred to throughout the remainder of the thesis.

The third chapter, Army Tactical Command and Control System (ATCCS), introduces the ATCCS architecture. The five Battlefield Functional Areas (BFAs) that compose the ATCCS are explained in terms of their functions. The operating systems that support these functions are mentioned but not explained in detail. These operating systems are relevant to this thesis only in terms of how they provide security to the ATCCS. The ATCCS security requirements as described in Field Manual 24-7. The requirements for MLS outlined in the document *Multilevel Security Operational Concept*, a product of the Combat Developments Center, U.S. Army Signal School, are provided as well.

The fourth chapter, MLS Product Technology Assessment, introduces an MLS technology assessment IAW the Joint MLS Technology Insertion Program Target Architecture and Implementation Strategy. The strategy provides a target architecture and five near term architectures for implementing MLS. The target architecture is discussed in terms of LANs (trusted and untrusted) and WANs. The near term architectures include: guard, workstation, LAN, database management system and host. These architectures serve as the vehicle for categorizing different methods of providing MLS for the ATCCS.

The fifth chapter, MLS Implementation within the ATCCS, presents two solutions: the first provides for a near term strategy and the second describes a target strategy.

II. COMPUTER SECURITY

The purpose of this chapter is to provide an executive summary of the material in the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC) (hereafter cited as the Orange Book).[1] This summary is intended to familiarize the reader with the military computer concepts and terms referred to throughout the thesis so that he will understand what Multilevel Security (MLS) is and how it is applied in subsequent chapters.

A. INTRODUCTION TO THE ORANGE BOOK

The National Computer Security Center (NCSC) published the Trusted Computer System Evaluation Criteria (TCSEC) in 1983. In 1985, the TCSEC was published with revisions as the DoD 5200.28-STD, which is also known as the "Orange Book". The TCSECs focus is disclosure protection of information and modification protection of system resources. In 1982, the NCSC began evaluating products developed by computer and computer software manufacturers under the Trusted Products Evaluation Program. The objectives of the program include:

[1] The Department of Defense TCSEC is a DoD standard which includes 28 different volumes and is commonly referred to as the "Rainbow Series" because each volume is a different color. The Orange Book is the main volume while the other volumes provide the details and explanations for the requirements stated in the Orange book.

1. Ensure widespread availability of commercial off-the-shelf (COTS) trusted products for use by the government.

2. Advance the state of the art in information system security (designing, building and evaluating trusted systems).

3. Transfer of computer security technology, specifically an understanding of techniques for constructing trusted computer systems, to government program managers and planners and to established computer manufacturers to assure an inventory of trusted computer product lines for application to government needs.[Ref. 1:p. 64-65]

B. DEFINITION OF COMPUTER SECURITY

A computer system can never be completely secure. A person, with enough time and tools, can penetrate any computer security system. A computer system can be physically secured with locks behind a locked door, for example, but for this thesis computer security is defined in terms of the degree of trust the computer system can provide. The Orange Book defines a trusted system as:

> a system that employs sufficient hardware and software integrity measures to allow its use to simultaneously process a range of sensitive unclassified or classified (e.g., confidential through top secret) information for a diverse set of users without violating access privileges.[Ref. 2:p. 116]

A trusted system is the manifestation of a security policy, which defines the set of rules and practices that determine how an organization manages, protects and distributes sensitive information. The Orange Book defines a security policy as:

> Given identified subjects and objects, there must be a set of rules that are used by the system to determine whether a given subject can be permitted to gain access to a specific object.[Ref. 2:p. 3]

Thus a security policy is stated in terms of subjects and objects. A subject is defined as something active in the system such as a user, process or program. An object is defined as something passive that a subject acts upon, such as files, devices and windows. Systems with lower levels of trust express their security policies informally while systems with high levels of trust are required to formally state their security policy in mathematical terms.

1. Trusted Computing Base and Reference Validation Mechanism

The concept of the Trusted Computing Base (TCB) is fundamental to the operation of a trusted system. The TCB is the mechanism that enforces security in a system. The Orange Book defines the TCB as follows:

> The totality of protection mechanisms within a computer system-- including hardware, firmware, and software-- the combination of which is responsible for enforcing a security policy. A TCB consists of one or more components that together enforce a unified security policy over a product or system. The ability of a trusted computing base to correctly enforce a security policy depends solely on the mechanisms within the TCB and on the correct input by system administrative personnel of parameters (e.g., a user's clearance) related to the security policy.[Ref. 2:p. 116]

The higher levels of trust require well-defined TCB's that are implemented in accordance with the reference monitor concept. The reference monitor concept enforces the authorized access relationships between subjects (users) and objects (data) of a system. The mechanism that implements this concept validates each reference between data and users, hence the name reference monitor (i.e., validation) mechanism.

The Orange Book references the Anderson report, a 1972 Air Force Base study, that lists three design requirements that the reference monitor mechanism must meet: isolation, completeness and verifiability. Isolation requires that the TCB be tamperproof. To meet completeness, the TCB must always be invoked for every access decision and must be impossible to bypass. Verifiability is accomplished when the TCB is small enough to be able to be analyzed and tested, and its completeness must be assured.

2. Security Models

As a result of the Anderson report, research was initiated into formal models of security policy requirements and into the mechanisms to implement and enforce those policy models. Models are developed to identify the essential components of secure systems. A security model expresses a system's security requirements precisely and without confusion.[Ref. 3:p. 108] From these models the user can study the interactions between the components.

From a security policy the first step is to determine how to control access to the system. The simplest model of access control which enforces the authorized access relationships between subject and objects is the reference monitor concept(see Figure 1).

The Orange Book criteria for trusted computer systems are based on the Bell-Lapadula model, the first mathematical model of a multi-level secure computer system. It is defined by the Orange Book as:

> A formal state transition model of computer security policy that describes a set of system access rules. In this formal model, the entities in a computer system are divided into abstract sets of subjects and objects. The notion of a secure state is defined and it is proven that each state transition preserves security by moving from secure state to secure state; thus inductively proving that the system is secure. A system state is deemed to be "secure" if the only permitted access modes of subjects to objects are in accordance with a specific security policy.[Ref. 2:p. 111]

Operating systems are at the heart of security systems for computers and must provide the mechanisms for separation and sharing of information in order to conform to a specific security model. The operating system mechanism that implements the monitor concept is known as the security kernel. This security kernel is the heart of the TCB. The Orange book defines a security kernel as:

> The hardware, firmware, and software elements of a Trusted Computing Base that implement the reference monitor concept. It must mediate all access, be protected from modification, and be verifiable as correct.[Ref.2:p. 115]

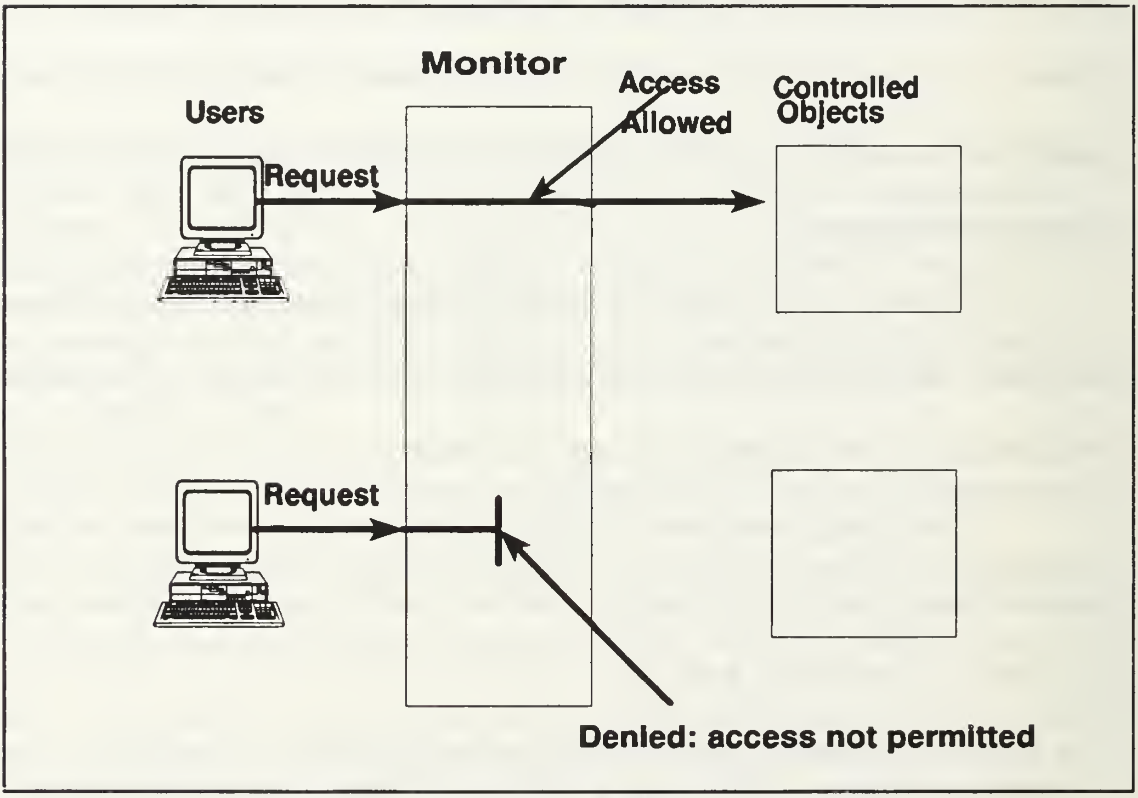


Figure 1 Monitor Model of Access

C. TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA

For a computer system to obtain NCSC accreditation within any of the seven classes of security protection (discussed below), the system must meet the NCSC criteria established for that class. The objectives of the criteria are threefold: to provide guidance, measurement, and acquisition standards. Guidance provides a standard to manufacturers as to what security features to build into their new and planned commercial products in order to satisfy trust requirements for sensitive applications. Measurement provides users with a metric with which to evaluate the degree of trust that can be placed in computer systems for the secure processing of classified and other sensitive information. Acquisition provides a basis for specifying security requirements in acquisition specifications.[Ref. 4:p. 2]

1. Fundamental Computer Security Requirements

The TCSEC lists six requirements that a system must meet to be awarded a rating within any class of security: security, identification, marking, accountability, assurance and documentation.

a. Security Policy

The requirements of a security policy represent the fundamental needs of an organization to protect the information on its system. These needs are translated into a framework in which a system provides trust. The framework provides a set of rules and practices that regulate how an organization manages, protects and distributes its information. The specifics include the following:

(1) Mandatory Access Control (MAC). This capability allows the system to enforce a label-based policy modeled after DoD Security Policy. A user can read only the information for which it has a clearance (also called sensitivity label). The clearance consists of a hierarchical and non-hierarchical classification level. The former includes unclassified, secret, top-secret while the latter includes codeword categories (nuclear, crypto, etc.). The system program can thus read information only at or below the clearance label in which it is operating. It also can write information only at or above the clearance in which it is operating. This write policy protects against software penetration such as a trojan horse from being able to downgrade information.

(2) Discretionary Access Control (DAC). This capability allows the users to protect the information they create in files. The user has the authority to grant or deny access to information (including read, write, create, delete) to individual users or groups of individuals.

(3) Marking (Labels). This capability, together with MAC, ensures that clearances associated with users and objects accurately reflect the security levels of these subjects and objects. It includes printing these labels on hardcopy output.

(4) Object reuse. This capability ensures that the storage elements such as disks are cleared prior to their assignment to a user so that no intentional or unintentional data can be retrieved.

b. Accountability

Accountability within a computer system lets the system know who its users are and what they are doing. The first requirement is to identify and authenticate the user. The next requirement of trusted path authenticates the TCB. This guarantees that the user is communicating with trusted software to insure that passwords are revealed only to the TCB. An example of a check to the TCB might be a type of interrupt (control break or character sequence) from the terminal as a request to communicate with the TCB. Next the system must decide whether a user is authorized to access information, and then keeps track of what the user does. This is needed, for example, to support the requirements of MAC and DAC. Finally, the audit capability requirement is necessary to allow the TCB to record the security-relevant events such as logins/outs within a protected file. Auditing involves the processes of recording, examining and reviewing of security related activities in a trusted system. Auditing enables the system to perform two security functions: surveillance and reconstruction. Surveillance is the monitoring of user activity. Reconstruction is the ability to put together a record of what happened in the case of a security violation.

c. Assurance

Assurance is the guarantee that the security policy of a trusted system has been implemented correctly and that the system's security features accurately carry out the security policy. The Orange Book identifies two types of assurance: operational and life-cycle. Operational assurance focuses on the system architecture and features of the system to ensure that the security policy is enforce during system operation (includes the features of system integrity, covert channel analysis, trusted facility management, and trusted recovery). Life-cycle assurance focuses on controls and standards for building and maintaining the system (which includes security testing, design specification and verification, configuration management and trusted distribution).

d. Documentation

This last set of requirements includes four categories: Security Features User's Guide (SFUG), Trusted Facility Manual (TFM), Test documentation and Design documentation. Additionally, a system security policy is required.

The Security Features User's Guide requirements are the same for all classes of security. It is written for the ordinary user who has no special privileges. Topics include how to log in to the system, how to protect files, how to import files into the system and how to export files into other systems, and how to understand and deal with system restrictions.

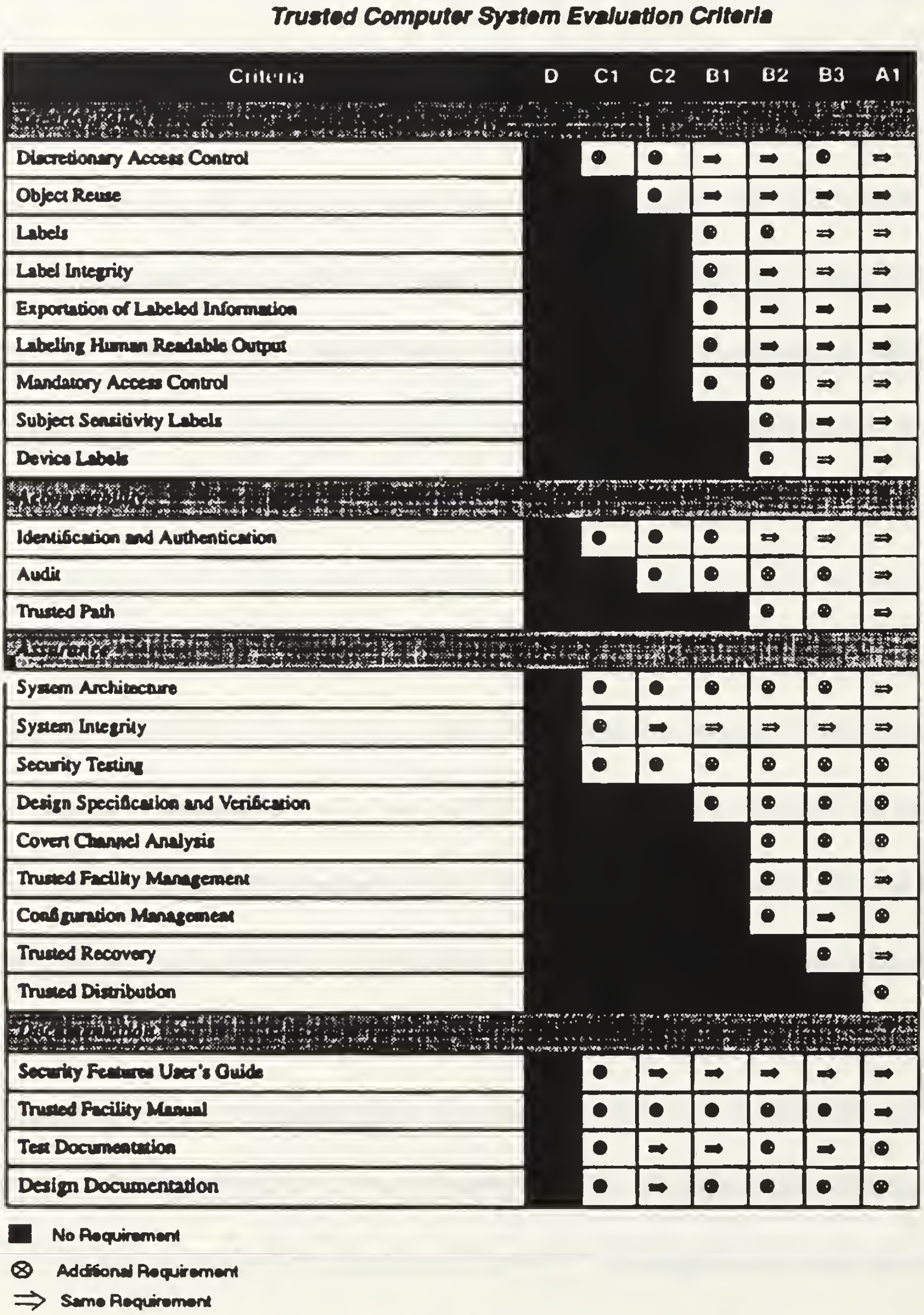
The Trusted Facility Manual requirements are for the system administrators and security administrators. It tells them how to set up a secure system, how to enforce system security, how to interact with user's requests and how to make the system function at its best.

Test documentation must show how the security mechanisms were tested as well as the results of the functional testing. The system developer is left to decide how to present his tests and results. The documentation, however, must contain a test plan, assumptions used, test procedures, expected results and actual results.

Design documentation chronicles the internal workings (the TCB) of the system's hardware, software and firmware. There are two goals of design documentation. The first goal is to prove to the evaluation team that the system fulfills the evaluation criteria. The manufacturer must delineate his philosophy of protection and how it is translated into the TCB. The second goal is to help the team define the system's security policy so that the team can then determine how well that policy is implemented. The design must be able to distinguish between security-relevant portions and non-security-relevant portions of the system. As with the other criteria, as the level of security increases, the requirements (in this case the description) become increasingly more formal.

2. Four divisions of security protection

The TCSEC specifies four divisions of security protection criteria (in increasing levels of security): D, C, B, A. Division D is for systems that have been evaluated but fail to meet the requirements for a higher NCSC evaluation rating. Division C has two classes: C1 and C2, which require discretionary access control protection. Division B has three classes: B1, B2, B3, which require support for sensitivity labels. Division A has only one class A1 which requires additional assurance through formal verification methods. For a consolidated view of the criteria associated with each security class, see Figure 2.



Trusted Computer System Evaluation Criteria

Criteria	D	C1	C2	B1	B2	B3	A1
[illegible]							
Discretionary Access Control		●	●	⇒	⇒	●	⇒
Object Reuse			●	⇒	⇒	⇒	⇒
Labels				●	●	⇒	⇒
Label Integrity				●	⇒	⇒	⇒
Exportation of Labeled Information				●	⇒	⇒	⇒
Labeling Human Readable Output				●	⇒	⇒	⇒
Mandatory Access Control				●	●	⇒	⇒
Subject Sensitivity Labels					●	⇒	⇒
Device Labels					●	⇒	⇒
Accountability							
Identification and Authentication		●	●	●	⇒	⇒	⇒
Audit			●	●	●	●	⇒
Trusted Path					●	●	⇒
Assurance							
System Architecture		●	●	●	●	●	⇒
System Integrity		●	⇒	⇒	⇒	⇒	⇒
Security Testing		●	●	●	●	●	●
Design Specification and Verification				●	●	●	●
Covert Channel Analysis					●	●	●
Trusted Facility Management					●	●	⇒
Configuration Management					●	⇒	●
Trusted Recovery						●	⇒
Trusted Distribution							●
Documentation							
Security Features User's Guide		●	⇒	⇒	⇒	⇒	⇒
Trusted Facility Manual		●	●	●	●	●	⇒
Test Documentation		●	⇒	⇒	●	⇒	●
Design Documentation		●	⇒	●	●	●	●

■ No Requirement

⊗ Additional Requirement

⇒ Same Requirement

Figure 2 Trusted Computer System Criteria

a. D, Minimal Security

This class has no security characteristics associated with it. It is reserved for systems that have been evaluated for a higher category but have failed.

b. C, Discretionary and Controlled Access Protection

Class C1 is defined by discretionary security protection. This class is intended for use in an environment where users operate at the same level of classification. This system provides a separation of users from data. It is intended primarily to keep users from making honest mistakes and damaging the system or interfering with others' work (assurance criteria). The security features are not sufficient to keep a determined intruder out. The security policy criteria includes discretionary access control. Accountability criteria includes identification and authentication. Here a user must use a password or some other mechanism to identify and authenticate himself to the TCB. The assurance criteria includes providing a system architecture that is capable of protecting system code from tampering by user programs. System integrity must be provided to ensure that the system works properly and that the security features cannot be bypassed in any obvious manner. Documentation criteria includes a Security Features User's Guide which describes the protection mechanism provided by the TCB, guidelines on their use, and how they interact with one another. A Trusted Facility Manual is required for use by the system administrator to present cautions about functions and privileges that should be controlled when running a secure facility. Test documentation must provide the evaluators a document that describes the test plan, test procedures to show how the security mechanisms were tested, and results of the security mechanisms' functional testing. Finally, design documentation must be available that provides a description of the manufacturer's philosophy of protection and an explanation of how this philosophy is translated into the TCB.

Class C2 is defined by controlled access protection. In addition to all of the features addressed for C1, C2 provides DAC by providing access controls capable of distinguishing between individual users or as the Orange Book states, including or excluding to the granularity of a single user. Thus, through access control lists or some other mechanism, the system must be able to specify, for example, that individuals A and B can read a file and that only individual C can change it. Another security policy requirement includes the object reuse feature. The accountability requirement specifies that the system must be able audit selectively by user. The documentation requirement requires the system to delineate how it administers the auditing capabilities.

c. B, Mandatory Protection

Class B1 is defined by labeled security protection. It has the following requirements in addition to those described for C2. In the area of security policy it has the requirement of labels and MAC. Under accountability requirements it has the audit feature specified. B1 has an additional design specification and verification requirement for the assurance category and additional Trusted Facility Manual and design documentation requirements for the documentation category.

Class B2 is defined by structured protection. It has the added features of subject security labels and device labels. It must have a trusted path feature to meet the accountability requirement. Under assurance, it has the added features of covert channel, trusted facility management and configuration management. It also has an additional test documentation requirement for the documentation category.

Class B3 is defined by security domains. The added features include DAC for the security policy; additional audit and trusted path features for accountability requirements and trusted recovery and trusted distribution for assurance requirements.

d. A, Verified Protection

Class A1 is defined by verified design. It has all of the features provided by the B3 class as well as the following: security testing, design specification and verification, covert channel, configuration management and trusted distribution to meet the assurance criteria. It also has additional test documentation and design documentation to fulfill the documentation criteria.

D. SECURITY OPERATING MODES

Not only are trusted computer systems classified at different levels of security protection, but they are also defined by different security operating modes. These five modes allow for different levels of service required by the users.

1. Dedicated Security Mode

The dedicated security mode is specifically and exclusively dedicated to and controlled for the processing of one particular type or classification of information, either for full-time operation or for a specified period of time.[Ref. 4:p. 2]

2. System High Security Mode

The system high security mode is defined by system hardware/software only trusted to provide need-to-know protection between users. In this mode, the entire system, to include all components electrically and/or physically connected, must operate with security measures commensurate with the highest classification and sensitivity of the information being processed and/or stored. All system users in this environment must possess clearances and authorizations for all information contained in the system. All system output must be clearly marked with the highest classification and all system caveats, until the information has been reviewed manually by an authorized individual to ensure appropriate classifications and caveats have been affixed.[Ref. 4:p. 2]

3. Multilevel Security Mode

The multilevel security mode allows two or more classification levels of information to be processed simultaneously within the same system when some users are not cleared for all levels of information present.[Ref. 4:p. 2]

4. Controlled Security Mode

The controlled security mode is a type of multilevel security mode in which a more limited amount of trust is placed in the hardware/software base of the system, with resultant restrictions on the classification levels and clearance levels that may be supported.[Ref. 4:p. 3]

5. Compartmented Security Mode

The compartmented security mode allows the system to process two or more types of compartmented information (information requiring a special authorization) or any one type of compartmented information with other than compartmented information. In this mode, all system users need not be cleared for all types of compartmented information processed, but must be fully cleared for at least Top Secret information for unescorted access to the computer.[Ref. 4:p. 3]

E. RISK INDEX

A computer system is classified into one of the seven security classes depending upon its intended security operating mode and its risk index. The risk index is defined as the disparity between the minimum clearance or authorization of system users and the maximum sensitivity of data processed by a system.[Ref. 5:p. 6] The minimum clearance is also defined as the maximum clearance of the least cleared system user. The risk is determined by rating the system's minimum user clearance R_{min} and the system's maximum data sensitivity R_{max}. Minimum users clearance are rated according to Table I. The rating scale for maximum data sensitivity is categorized by Table II. If R_{min} is less than R_{max} then the risk index is calculated by subtracting R_{max}- R_{min}. If $R_{min} \geq R_{max}$ then the risk index is characterized as 1 if there are categories on the system which some users are not authorized access, or it is characterized as 0 otherwise, i.e., no categories on the system or if all users are authorized to all categories.[Ref. 5:p. 5]

TABLE I RATING SCALE FOR MINIMUM USER CLEARANCE

MINIMUM USER CLEARANCE	RATING
Uncleared (U)	0
Not cleared but authorized for sensitive unclassified (N)	1
Confidential (C)	2
Secret (S)	3
TS/ Current BI	4
TS/ Current Special BI	5
One Category (1C)	6
Multiple Categories (MC)	7

TABLE II RATING SCALE FOR MAXIMUM DATA SENSITIVITY

MAXIMUM DATA SENSITIVITY RATINGS WITHOUT CATEGORIES (R_{MAX})	RATING (R_{MAX})	MAXIMUM DATA SENSITIVITY WITH CATEGORIES	
Unclassified	0	Not Applicable	
Not Classified but Sensitive	1	N With 1 or More Categories	2
Confidential (C)	2	C With 1 or More Categories	3
Secret (S)	3	S With One or More Categories With No More than 1 Category Containing Secret Data	4
		S With 2 or More Categories Containing Secret Data	5
Top Secret (TS)	5	TS With 1 or More Categories With No More Than 1 Category Containing Secret or Top Secret Data	6
		TS With 2 or More Categories Containing Secret or Top Secret Data	7

F. SECURITY ENVIRONMENT

The security environment is categorized into two types: open and closed. A system whose applications are not adequately protected is referred to as being in an open environment. If the applications are adequately protected, the system is in a closed environment. Most systems are in open environments. The applications are protected through the Trusted Computing Base (TCB). The Yellow Book of the rainbow series defines an open security environment as characterized by two conditions:

1. Application developers (including maintainers) do not have sufficient clearance (or authorization) to provide an acceptable presumption that they have not introduced malicious logic. Sufficient clearance is defined as follows: where the maximum classification of data to be processed is Confidential or below, developers are cleared and authorized to the same level as the most sensitive data; where the maximum classification of data to be processed is Secret or above, developers have at least a Secret clearance.

2. Configuration control does not provide sufficient assurance that applications are protected against the introduction of malicious logic prior to or during the operation of system applications.[Ref. 5:p. 31]

Similarly, a closed security environment is characterized by the two following conditions:

1. Applications developers (including maintainers) have sufficient clearances and authorizations to provide an acceptable presumption that they have not introduced malicious logic.

2. Configuration control provides sufficient assurance that applications are protected against the introduction of malicious logic prior to and during the operation of system applications.[Ref. 5:p. 32]

G. DETERMINING A SYSTEM'S SECURITY REQUIREMENT

The class of trust required of a system is determined from three factors: the security operating mode, the risk index and the security environment. Once these are determined, the minimum class of security can be determined from Table III. Since most systems are open, only the open systems table will be shown.

H. NETWORK SECURITY

The material discussed thus far addresses single system security. A network involves many systems that are often not compatible in terms of their architectures and security vulnerabilities. The Red Book, titled Trusted Network Interpretation (TNI) and its companion, Trusted Network Interpretation Environments Guideline (TNIEG), is an NCSC effort to extend the TCSEC evaluation classes to trusted network systems and components. The Red Book distinguishes between two types of networks: an interconnection of accredited automated information systems (AIS) and a unified network. The definitions are as follows: an interconnection of AIS is

> an assembly of computer hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information.[Ref. 6:p. 5]

while a unified network is:

> Some networks may be accredited as a whole without prior accreditation of their component AIS. It is necessary to treat a network as unified when some of its AIS subsystems are so specialized or dependent on other subsystems of the network for security support that individual accreditation of such subsystems is not possible or meaningful with respect to secure network operation.[Ref. 6:p. 10]

Like trusted systems, trusted networks have network TCB's (NTCB), a security policy, architecture, and system design (NSAD, network security architecture and design). The NSAD identifies how the NTCB is partitioned and how the trusted system requirements are met. The NCSC evaluates network products as it does for stand-alone operating systems, through the Trusted Products Evaluation Program (TPEP).

The Red Book divides its discussion of security requirements into two parts: minimum security requirements, which interprets the TCSEC for networks; and qualitative evaluations of security services in terms of functionality, strength of mechanism, and assurance. These security services evaluated include compromise protection, denial of service, and unauthorized modification (communications integrity).

Part one, determining the minimum security requirements for a network is nearly the same as for a stand-alone system. The risk index is calculated to determine which rating is required to provide adequate security. The same tables used for stand alone systems are used for networks; specifically, Table I for determining the rating scale for minimum user clearance, Table II for determining maximum data sensitivity, and Table III for determining computer security requirements for open security environments.[2] Additional factors such as communications security, distance between devices, number of subsystems, and encryption are considered in determining the minimum security requirement.

[2] Limited Access Mode and Compartmented Mode fall under the heading of Partitioned Mode. Controlled Mode comes under the heading Multilevel.

Part two, qualitative evaluations of security services are concerned with functionality, strength of mechanism, and assurance. Functionality refers to the objective and approach of a security service. Strength of mechanism refers to how well a specific approach may be expected to achieve its objective. It has two components, inadvertent threat and malicious threat. Both should be analyzed separately. Assurance refers to a basis for believing that the functionality will be achieved.[Ref. 6:p. 26] The evaluation rating terms used for each are none, minimum, fair, and good. None is used to mean the security service fails to distinguish the strength of mechanism. Table IV identifies a set of security services as well as the evaluation rating terms (discussed above) for each service. The problem with this table as it appears in the TNIEG is that the qualitative ratings are useless to an accreditor or system builder. Protocol structures would provide the specifications required or these system builders and vendors. The TNIEG is a criteria for evaluation and thus avoids specific protocol references.

TABLE III COMPUTER SECURITY REQUIREMENTS FOR OPEN SECURITY ENVIRONMENTS

RISK INDEX	SECURITY OPERATING MODE	MINIMUM CRITERIA CLASS
0	Dedicated	No Min - C1
0	System High	C2
1	Limited Access, Controlled Compartmented, Multilevel	B1
2	Limited Access, Controlled Compartmented Multilevel	B2
3	Controlled, Multilevel	B3
0	Multilevel	A1
5	Multilevel	* protection beyond state of current technology
6	Multilevel	*protection beyond state of current technology
7	Multilevel	*protection beyond state of current technology

TABLE IV EVALUATION STRUCTURE FOR NETWORK SECURITY SERVICES

Network Security Service	Criterion	Evaluation Range
Communications Integrity Authentication	Functionality Strength Assurance	None present None-good None-good
Communications Field Integrity	Functionality Strength Assurance	None-good None-good None-good
Non-repudiation	Functionality Strength Assurance	None present None-good None-good
Denial of Service Continuity of Operations	Functionality Strength Assurance	None-good None-good None-good
Protocol Base Protection	Functionality Strength Assurance	None-good None-good None-good
Network Management	Functionality Strength Assurance	None present None-good None-good
Compromise Protection Data Confidentiality	Functionality Strength Assurance	None present Sensitivity level None-good
Traffic Flow Confidentiality	Functionality Strength Assurance	None present Sensitivity level None-good
Selective Routing	Functionality Strength Assurance	None present None-good None-good

III. ARMY TACTICAL COMMAND AND CONTROL SYSTEM (ATCCS)

A. INTRODUCTION

A network security model cannot be constructed without first understanding the architecture of the system, what its security policies must be, and any other requirements necessary to operate. The format of this chapter will be to introduce the ATCCS architecture, explain its security policies and requirements, and describe the operational requirements for Multilevel Security within the ATCCS.

B. BACKGROUND

The Army Command and Control Master Plan's (AC2MP) primary purpose is to structure the Army Command and Control System (ACCS) doctrine, training, leader development, organizations and material projects and programs and communicate definitive guidance to Battlefield Functional Area (BFA) proponents in managing the development of their C2 and their C2 related capabilities.[Ref. 7:p. 10] The ACCS is a system as well as a concept. "It is the aggregate means by which Army commanders employ and sustain military forces in a theater of operation." [Ref. 7:p. 6] Figure 3 depicts the ACCS system environment. From Figure 3 the Army Tactical Command and Control System (ATCCS) represents the Echelons Corps and Below (ECB) portion of the ACCS.

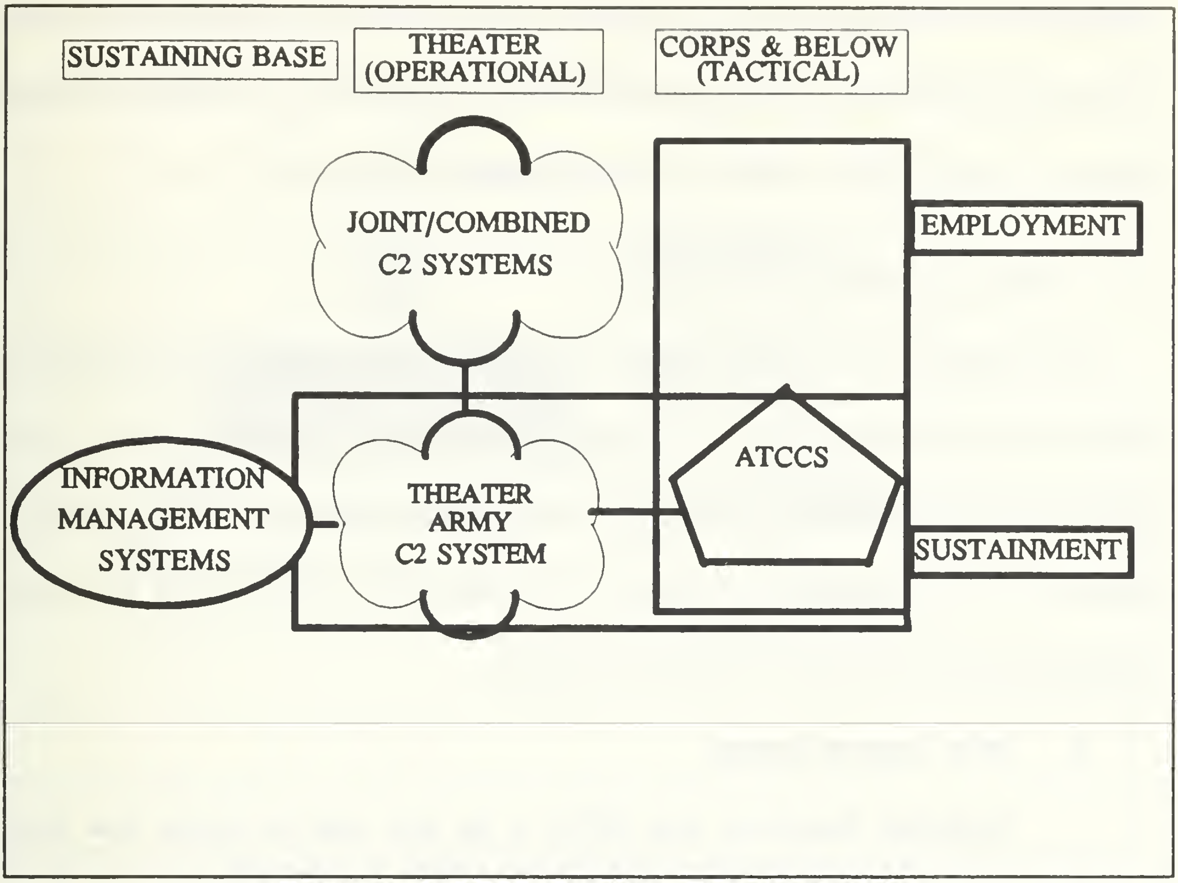


Figure 3 ACCS System Environment

The ATCCS architecture is the focus of this chapter. ATCCS is an integration of automated systems, each of which collects, processes, and distributes information in support of one or more Battlefield Operating Systems (BOS) (each BFA is implemented through its own BOS). It is intended to operate as a single seamless system integrating command post facilities, communications, automation equipment and functions.[Ref. 8:p. 1] ATCCS exists to provide the commander and his staff with the information they need to effectively plan, coordinate, control, and direct the battle. To be effective, a unit's ATCCS devices must be linked together into a network which allows for the free and timely flow of information.[Ref. 8:p. 1] The goal of ATCCS is to "provide commanders at corps level and below with near-real-time data from several Unix-based information systems, all feeding into a maneuver control system."[Ref. 9:p. 41]

C. ATCCS ARCHITECTURE- CCS2

The Command and Control Subordinate System (CCS2) architecture defines the tactical automation architecture for the ATCCS. It consists of the five BFA Control Systems (BFACS), interfaces to the three communications systems, and the command posts and facilities supporting the exercise of force level control on the battlefield. Command posts and facilities will not be addressed.

1. BFA Control Systems

Battlefield Functional Area (BFA) is the term used to express how Army battlefield automated systems should interoperate. There are five BFA's: Maneuver Control, Fire Support, Air Defense, Combat Service Support System (CSSCS) and Intelligence/Electronic Warfare (IEW). The control systems applicable to each BFA will be discussed with each BFA. Information must flow continually within and among the BFA's. The CCS2 partitions each BFA into three classes of interconnected subsystems: the force level control system (command), functional control systems (control), and subordinate systems (see Figure 4).

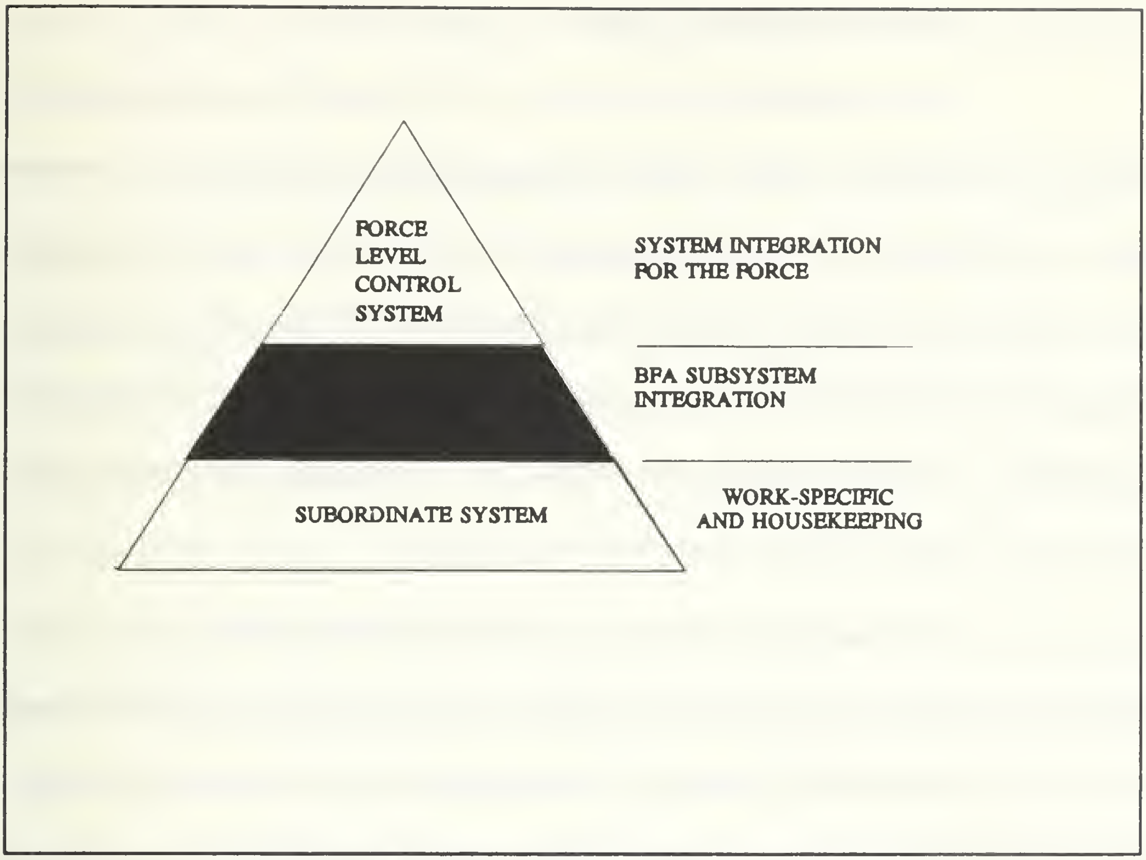

FORCE LEVEL CONTROL SYSTEM
SYSTEM INTEGRATION FOR THE FORCE
BFA SUBSYSTEM INTEGRATION
SUBORDINATE SYSTEM
WORK-SPECIFIC AND HOUSEKEEPING

Figure 4 CCS2 Vertical Architecture

a. Force Level Control System

The force level control system (FLCS) provides automation to support the horizontal synchronization of the force at an echelon. It allows the commander to use all C2 resources available in order to make sound, timely decisions and direct the actions of the force. It provides for information exchange both horizontally and vertically and thus ties all the BFAs together. The FLCS is a software capability resident on each BFA control systems hardware which provides the means to interconnect the functional control systems into an integrated system for C2.

b. Functional Control System

The functional control system (FCS) is each BFA commander's C2 system. Each BFA has its own unique data base subsystem and integrates information from the subordinate systems to permit the functional commander to perform his internal C2. It supports the FLCS by collecting data from the five BFAs and then structuring it into meaningful information for the force commander and his staff, by disseminating the commander's and staff's guidance and direction, and by coordinating across BFA lines. The specific functions related to each BFA are as follows:

(1) Maneuver. Develop an integrated combined arms and services concept of operation for the Airland Battle force; develop C3 Countermeasures concept to assure the effectiveness of the C2 capability of the force. The maneuver functional area includes infantry, armor, aviation, military police, chemical, engineers and the signal corps. The BOS that implements maneuver is the Maneuver Control System (MCS).

The MCS is the force level commander's information system. It enables the commander to execute integrated arms operations, make decisions concerning the employment and sustainment of combat power and synchronize all five BFAs in executing tasks directed by higher headquarters or perceived by the echelon commander.[Ref. 8:p. 2] The MCS is the commander's primary tool for correlating, filtering and processing information for his force. It provides automated assistance in the coordination of plans, dissemination of orders and guidance, and the monitoring and supervision of operations. MCS makes this information available by displaying the current situation on battlefield maps and decision graphics. It automates command and control for maneuver forces.

(2) Intelligence/Electronic Warfare (IEW). Develop the intelligence preparation of the battlefield; direct intelligence resources to provide timely, useful information to the force level commander concerning the enemy, terrain and weather; direct electronic warfare resources in consonance with the force level commander's concept of C3 Countermeasures. The BOS that implements the IEW is the All Source Analysis System (ASAS).

The ASAS provides for the creation and coordination of intelligence products that accurately portray the enemy's current course of action (COA) and predict the enemy's probable COA, provide data on enemy vulnerabilities, orders of battle, and installations. ASAS is the only BFA that requires a Top Secret classification (including compartments). The other four BFAs require Secret.

(3) Fire Support. Develop and direct the fire support concept of operation to influence and defeat surface targets by active, indirect means in support of the AirLand Battle force concept of operation. The BOS that implements Fire Support is the Advance Field Artillery Tactical Data System (AFATDS).

The AFATDS provides automated support for planning, coordinating, controlling and executing close support, counterfire, interdiction, deep operations and enemy air defense artillery suppressions. It automates the collection, prioritization and display of data supporting fire planning and execution, maneuver control, mission support and field artillery fire direction operations.

(4) Air Defense. Develop and direct the air defense concept of operations to influence and protect airspace of the AirLand Battle force and defeat aerial targets in support of the AirLand Battle force concept of operation. The BOS that implements Air Defense is the Forward Area Air Defense Command Control Communication and Intelligence System (FAADC^{3}I).

The FAADC^{3}I system provides automated support to the air defense commander in order to detect, identify, engage and destroy hostile airborne platforms. It provides for interoperability with adjacent, allied, combined and joint forces by exchanging and disseminating airtrack and surveillance information.

(5) Combat Service Support. Develop and direct the CSS concept of operation to sustain and reconstitute the AirLand Battle force in support of the AirLand Battle force concept of operation. The BOS that implements Combat Service Support is the Combat Service Support Control System (CSSCS).

The CSSCS system provides automation support to plan, coordinate, control and execute personnel and logistic services in support of friendly operations. The CSS command and control mission is to provide critical CSS information to theater and force level commanders as well as to provide C2 for its own CSS commanders to best employ CSS units to sustain and reconstitute the force.

(6) Subordinate Systems. Subordinate systems are manual or automated systems which perform unique C2 functions within the BFA.[Ref. 7:pp. 4-5] The functions include work-specific duties of the BFA and housekeeping. Housekeeping includes intra-BFA communications, security and protection of the BFA resources, and self-sustainment of BFA resources. The housekeeping functions for all five BFAs are similar. Personnel, procedures and material comprise the subordinate systems that accomplish these functions.

2. Communications

The ATCCS interfaces to three communications systems: Combat Net Radio (CNR), Area Common User System (ACUS), and the Army Data Distribution System (ADDS). Because this is the objective architecture, many of the systems mentioned have not been fielded and evaluated. Communications provide the means to interconnect the functional control systems and implement the CCS2 architecture. Figure 5 shows the horizontal representation of the CCS2 requirements, commonly called the Sigma Star. Superimposed upon the Sigma Star are the three communications means. Figure 6 depicts the vertical synchronization through CCS2 from corps through battalion.[Ref. 7:pp. 4-6]

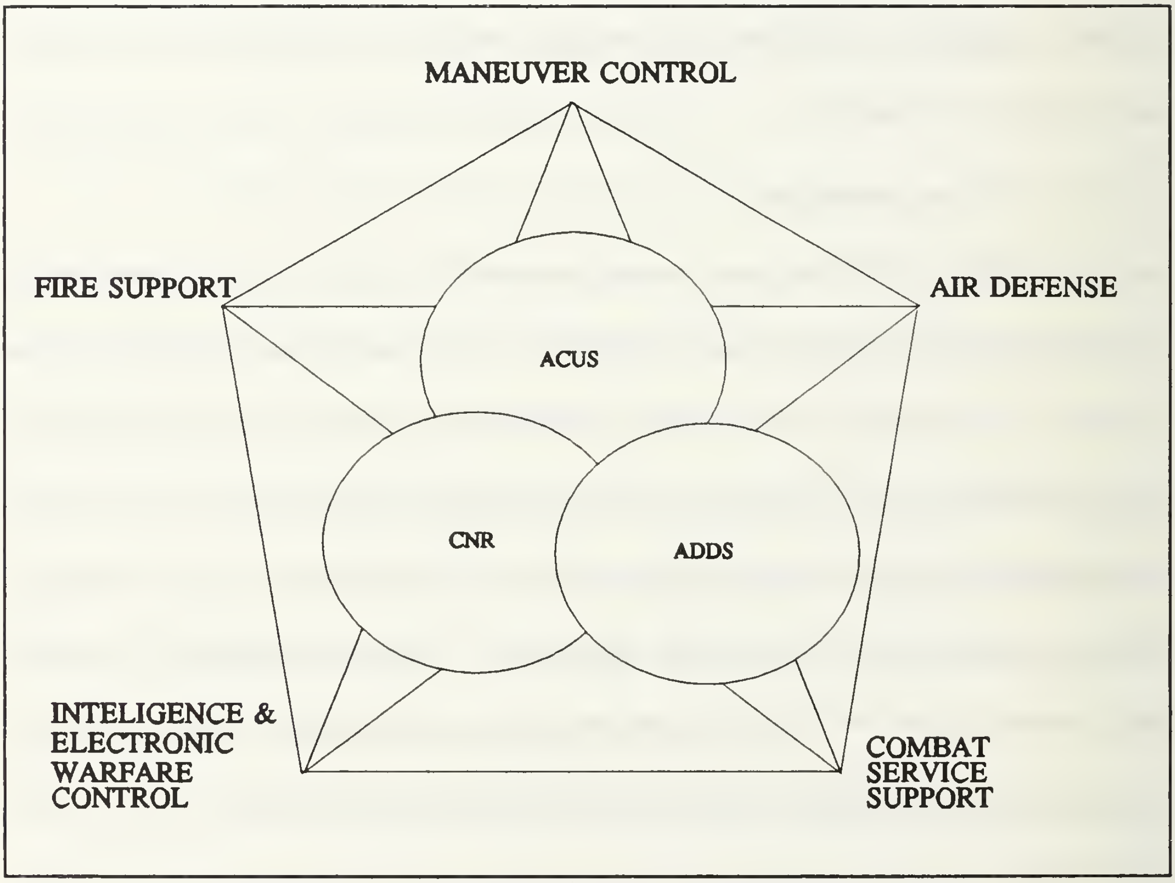
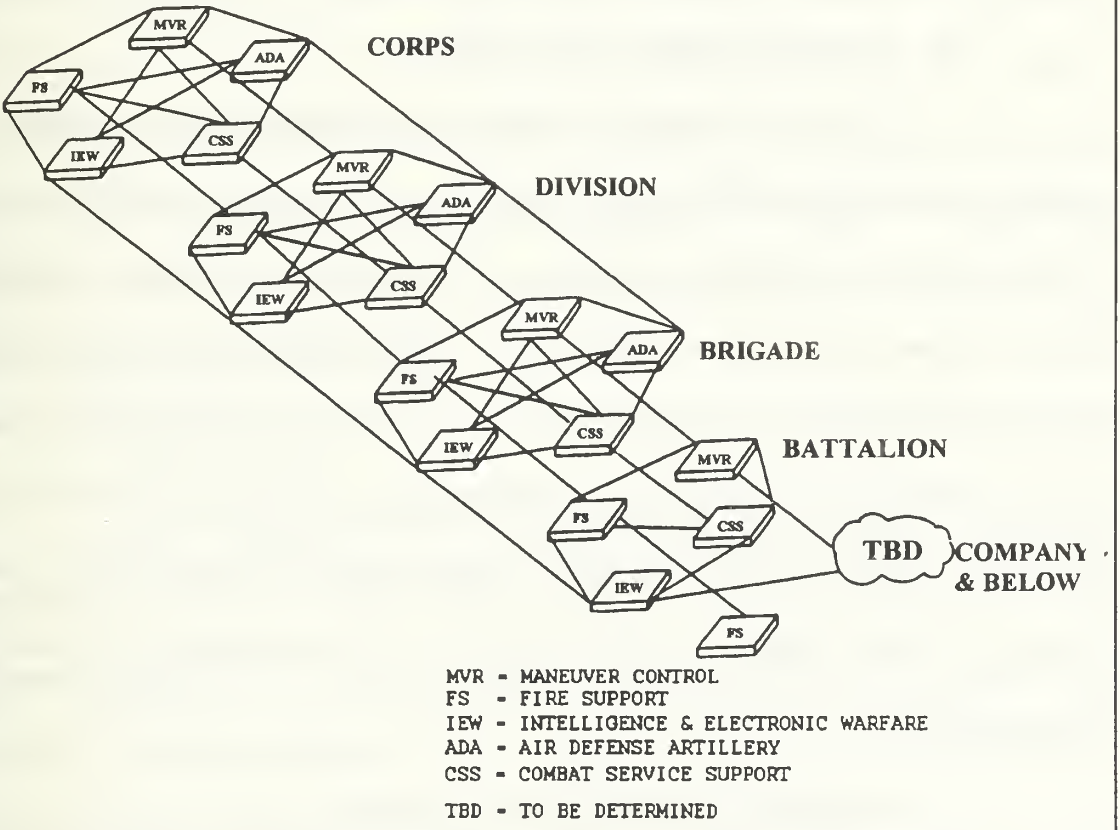


Figure 5 CCS2 Needlines Representation



MVR - MANEUVER CONTROL
FS - FIRE SUPPORT
IEW - INTELLIGENCE & ELECTRONIC WARFARE
ADA - AIR DEFENSE ARTILLERY
CSS - COMBAT SERVICE SUPPORT
TBD - TO BE DETERMINED

Figure 6 Vertical synchronization through CCS2

a. *Area Common User System (ACUS)*

The area common user system supports two networks, the packet switched network and the circuit switched network. The Mobile Subscriber Equipment (MSE) system which provides both packet switching and circuit switching is used at corps level and below. It is capable of handling voice and data communications for a five division corps in an area of operations of up to 37,000 square kilometers.

b. *Combat Net Radio System (CNR)*

This is a new family of combat net radios that provides for command and control from the squad level through the corps. It is primarily voice although there is a limited data communications capability. The CNR family consists of the Single Channel Ground and Airborne Radio System (SINCGARS) and the Improved High Frequency Radio (IHFR). SINCGARS is a secure, frequency-hopping or single channel VHF-FM radio that is used in combat, combat support, and combat service support units from squad through corps level. IHFR is a single channel HF radio which is used for non-line of sight situations which allows for rapid deployment and immediate communications.

c. *Army Data Distribution System (ADDS)*

The ADDS is an integrated command control and communications system providing real-time data communications and position, location, navigation, identification and reporting information for the battlefield. ADDS includes two systems, the primary is the Enhanced Position Location Reporting System (EPLRS), and the other is the Joint

Tactical Information Distribution System (JTIDS) which supports only the Army Air Defense roll and its interface with the Air Force Tactical Air Control System. These systems are a family of secure, jam-resistant, near real-time communications systems.

D. REQUIREMENT FOR MLS[3]

The ATCCS system requires MLS because tactical units have a requirement to exchange information with adjacent units, unified command elements, senior components of the armed services and with national and allied agency information systems. Information to be transmitted is often classified information with compartmented caveats, hence the need for proper protection between networks and computers. There are three functional areas which need MLS; on the host computer, on local area networks (LANs), and on wide area networks (WANs).

1. Host Computers

A host computer should be able to determine the identity of the person attempting to operate it and, based on that identity, allow or deny access to its files and application programs on an individual basis. A host computer may be a stand alone terminal or a central processing unit with multiple peripherals. MLS can be implemented through the application of software. MLS will permit authorized users at different levels (Top Secret, Secret, Confidential, Unclassified to include compartmented and SCI information) to use the same host. Users will be able to retrieve and manipulate

[3] Paraphrased from the Multilevel Security Operational Concept,US Army Signal School Ft. Gordon, Ga.

information up to their authorized level of classification and will be denied access to those files and programs above their level of authorization.

2. Local Area Networks

A LAN should be able to determine whether or not a specific terminal is allowed to receive data of a given security level. It should also be able to determine whether or not the current operator of that terminal is authorized access to that data. Once physical access to each terminal is fully controlled, then the LAN needs only to determine authorization of the terminal. Since a LAN can also function as a real-time operating system, the controller device must also be able to apply the same set of rules to the LAN's application programs. A LAN must have a file server which has the same characteristics of a host computer in order to implement MLS. MLS devices will permit the exchange of classified information within and across local area networks without increasing the probability of compromise.

3. Wide Area Networks

Wide area networks will very likely go through some sort of switched communications system. This will require that the address of the recipient be readable to the switch while the content of the subject data remains unreadable until arrival at its destination. In the case of packet switched systems, this is very critical since the devices communicating are in a near-real-time mode. With that in mind, the WAN must be able to do all that a LAN does. For either a LAN or WAN to implement MLS across switched communications systems, it requires a specialized method of cryptography.

This cryptography could be a plug-in printed circuit card with a combination of firmware and software and additional memory capability for its own functions. The memory required for this cryptographic software could force the implementation into a separate piece of hardware (a Multilevel Security User Device (MLSUD)) rather than on the host computer.

E. SECURITY POLICIES AND REQUIREMENTS FOR THE ATCCS

The security policy for (the objective) ATCCS dictates that it be at least B2 in accordance with the Orange Book and the Trusted Network Interpretation (Red Book). Specifically, FM 24-7 has outlined the following requirements for ATCCS system security:

1. Logon attempts on an individual ATCCS workstation shall be limited to a number, configurable by the Information Systems Security Officer (ISSO).
2. Local and remote users who fail to properly enter their login within the authorized number of logon attempts shall be denied access to the workstation. The ISSO shall restore the system to normal operations.
3. The highest level of data processed and stored by ATCCS (except ASAS) shall be SECRET with multiple special handling instructions, e.g., NATO, U.S. ONLY, NOFORN, WININTEL, and RELEASABLE TO.
4. ATCCS shall be protected against unauthorized modification to either hardware or software, and stored data.
5. ATCCS shall provide labeling or hard copy information outputs from the system to the system high water mark. In the objective time frame, ATCCS shall provide automated trusted labeling of hard copy information outputs form the system with the highest classification of data contained therein and special handling caveats in human readable form.

6. Data displayed by ATCCS workstations shall be labeled with a human readable security label depicting the system high water mark.

7. Data displayed by ATCCS workstations shall be labeled with a human readable security label depicting the highest level of classification associated with the displayed data.

8. Data transmitted by ATCCS workstations shall be labeled with a computer readable security label depicting the system high water mark.Data transmitted by ATCCS workstations shall be labeled with a computer readable security label depicting the highest level of classification associated with the transmitted data.

9. Common Hardware/Software (CHS) shall be capable of purging classified information IAW AR 380-19, paragraph 2-21, in field and garrison locations.

10. CHS shall be capable of the degaussing or overwriting of sensitive information on magnetic or other storage media to support the downgrading of classified information.

11. ATCCS shall provide sufficient detail to reconstruct events in determining the cause and magnitude of compromise should a security violation or malfunction occur.

12. Passwords shall be generated randomly and shall be a minimum of five character strings using the 36 alphanumeric characters, or six-character strings using only the alphabetic characters.

13. Passwords shall be changed on the system at least semi-annually.

14. Password changes shall be made incrementally (e.g.,20 percent per month) and aperiodically (different days of the month).

15. CHS shall provide the capability for ISSO (or his designee) to generate a new password during the creation of a new user account and in those instances where a new password is required for an existing account.

16. BFACS shall provide Compromising Emanations protection (TEMPEST) IAW AR 380-19-1 and NSA Compromising Emanations Laboratory Test Requirements. Electromagnetics, 21 March 1991 (C). BFACS will utilize physical security and Standing Operating Procedures (SOPs) to provide the most cost effective protection as specified in AR 380-19-1.

17. ATCCS shall prevent unauthorized access to ATCCS databases, and permit users' access only to database elements to which they are authorized. In the short range, the ATCCS database management capability shall provide C2 level security IAW DoD 5200.28-STD. The objective ATCCS database management capability shall provide B2 level security IAW DoD 5200.28-STD.

The ATCCS database management capability shall provide the functionality:

1. To protect data security at the record level.
2. To protect data security at the field level.
3. To protect data security at the data element level.

The Operational Requirements Document (ORD) submitted by the US Army Signal School lists the system performance /capabilities /characteristics required of the objective MLS as the following:

1. Allow users at different security classifications (unclass through TS/SCI) to use a single DCN through the use of releasable FIREFLY or equivalent technology. MLS will permit the exchange of all classifications of information within the DCN without increasing the probability of compromise.
2. Allow users without MLS system components to exchange information at their authorized level with users who have MLS, i.e., provide a secure release capability.
3. Allow remote over-the-air rekeying through the use of the Army Key Management System (AKMS) as implemented in ACMES.
4. Be capable of assigning minimum and maximum security classifications to all files, programs and terminals.

5. Be capable of operating on tactical and strategic local area and packet switched networks, including MSE and DISNET 1, 2 and 3, with no difference in the software and hardware being used:

    a. Interface with and operate on all networks in accordance with International Telegraph and Telephone Consultative Committee (CCITT) X.25 standards.

    b. Interface with and operate on all networks in accordance with Institute of Electrical and Electronic Engineers (IEEE) 802.3 standards.

    c. Provide a trusted gateway between strategic and tactical networks which utilizes Internet Protocol Security Option [IPSO] labelling to route datagrams to the proper network as part of the interim solution.

6. Be capable of operating on both theater/tactical and strategic/sustaining base DCNs, this includes:

    a. Provision for using logical addressing methodology on all DCNs.

    b. Supporting the current DoD protocol stack transmission control protocol/internet protocol(TCP/IP) with the capability of migrating to the Government Open Systems Interface Profile (GOSIP) protocols and the Defense Message System (DMS) when necessary.

7. Provide for multiple virtual circuits.

8. Support separate operator, supervisory, administrator and security functions.

9. Provide for a workstation in a to-be-designated management facility, with the capability of performing planning, initialization and management of the MLS system. Redundant supervisory and administrator capabilities will be provided to allow continuity of operations during all phases of tactical operations.

10. Record events of system malfunction or procedure violation. The user, operator, supervisor and system administrator will be notified (monitor, printer, light, alarm) to the extent required that a problem exists. If required, a user log will also record the event.

11. Retain internal security relevant information at loss of primary power.

IV. MLS Product Technology Assessment

A. BACKGROUND

In response to the validated Requirements Submission documenting the MLS requirement within DoD AISs, the Joint Staff established the Joint MLS Technology Insertion Program effective 4 January 1990. The program organization is as follows: the Deputy Assistant Secretary of Defense for C3I (DSAD(C3I)) has oversight; the Defense Information Systems Agency (DISA) is the program manager; the Joint Staff (J6K) is the program sponsor; the National Security Agency (NSA) is the security coordinator; the Defense Intelligence Agency (DIA) is the intelligence coordinator; and two groups consist of the DoD MLS Working Group and the DoD MLS Testbed Steering Group. In July 1990, the DASD(C3I) designated this program as part of the Defense-Wide Information Systems Security Program (DISSP). In February the Joint Staff validated the Multicommand Required Operational Capability (MROC) for this program. The program developed a Target Architecture and Implementation Strategy (TAIS) that presents the technical approach and strategy for the program. The TAIS has four basic activities:

1. Planning and coordination of DOD MLS projects and initiatives.Development and evaluation of generic MLS technology, including architectures and standards, methodology and guidance, and components and systems.

2. Provision of security engineering assistance for MLS implementations at specific operational sites.

3. Exchange of information on MLS-related technologies and activities.

This program supplements the larger NSA INFOSEC program and has no involvement in officially evaluating and rating products (a NSA responsibility). The purpose of the program is to expedite the fielding of MLS capabilities within a specific community.

The architectural concepts in the TAIS complement the architectural efforts of other programs such as the Integrated Communications Architecture (ICA), Defense Information System Network (DISN) and the Defense Message System (DMS). The TAIS however is narrower in scope, focusing on MLS in AISs rather than on INFOSEC as a whole in both AISs and WANs, and emphasizing the fielding of capabilities.

This chapter presents an overview of the MLS target architecture and implementation strategy for DoD AISs with a focus on fielding capabilities. The goal is to provide an understanding of the MLS technologies available now and in the near future, and then evaluate their applicability to the ATCCS requirements for the purpose of developing an ATCCS-specific implementation strategy. Comparisons between systems presented in the MLS target architecture and the ATCCS system are made to facilitate the readers' understanding of the rationale used for the implementation strategy to be proposed in the next chapter. The focus will be on the MLS methods as developed by the TAIS in both its target and near-term architectures. The target architecture (see Figure 7) is dependent on the findings of the near-term operational capabilities within the near-term architectures. The term *trusted* in this chapter indicates that a product has the capability to enforce security internally. Thus the term *trusted* will be used in connection with products and components. The term *capability* means a collection of one or more products or components that can be integrated into a system to provide operational abilities. The term MLS will be used in connection with capabilities and systems. The distinction between *trusted* and *MLS* is important because not all trusted products or components are adequate to provide an MLS capability.

B. TARGET ARCHITECTURE--2000

Progress in MLS technology has resulted in many trusted products and subsystems making their way onto the Evaluated Products List (EPL). These products will finally bring the much needed MLS capability to the field. The pitfalls are that these products may not be properly integrated or securely used. One of the purposes of the TAIS program is to exploit the potentials and avoid the pitfalls by providing a target architecture to guide the program efforts.

The target architecture is a general framework showing which components are most likely to be trusted. Trusted components as shown in the target architecture support MLS or partitioned (compartmented) mode capability. Untrusted components support dedicated or system high mode capability and are untrusted from an MLS or partitioned mode perspective. Not all components are shown as being trusted because a typical system needing MLS capabilities may have only a few trusted components in order to achieve an optimal balance between security and functionality.[Ref. 10:p. 9] Additionally, the uncertainty in MLS technology makes it impossible to predict which trusted components will be operationally successful. Figure 7 depicts the Target architecture--2000 in terms of Trusted LANs, Untrusted LANs and WANs.

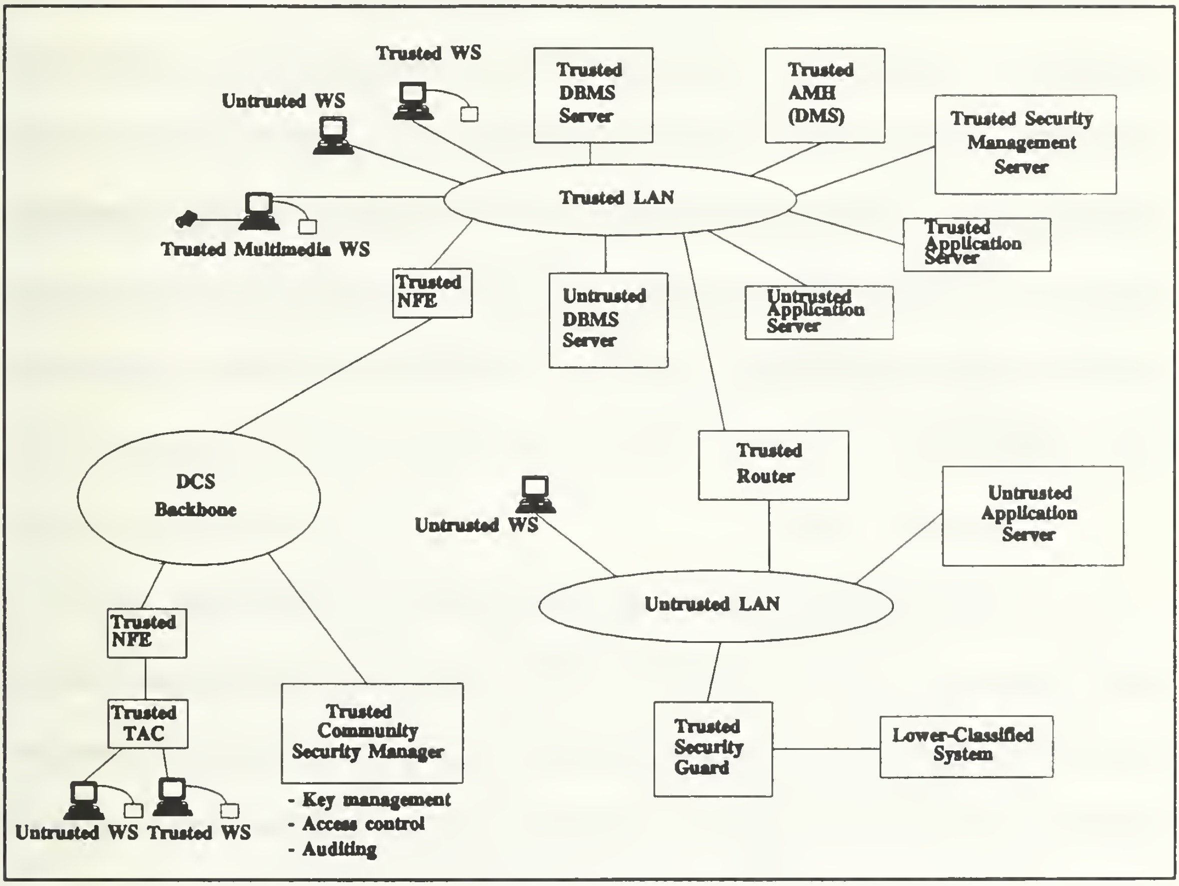


Figure 7 Target Architecture--2000

1. Trusted Local Area Network (LAN)

The trusted LAN supports two types of workstations: trusted and untrusted. Trusted workstations will incorporate trusted Defense Message System (DMS) functions, trusted DMS Automated Message Handler (AMH) and trusted Secure Data Network System (SDNS) functions, such as the use of Message Security Protocol (MSP) to authenticate messages. The trusted Security Management Server provides central security management for the LAN. It enables central management of authentication and permissions, supports central audit data collection, and provides a central intrusion detection service. Untrusted workstations such as the untrusted DBMS and application servers shown demonstrate the possibility that some trusted servers will not be able to provide the functionality needed, hence the inclusion of both trusted and untrusted servers in the architecture.

2. Untrusted LAN

The untrusted LAN is connected to the trusted LAN by a trusted router. The Verdix Secure Internet Protocol Router (VSIP) is a trusted implementation of the DoD standard routing protocols. It provides a means of transferring security-labeled data from one local area network to another. This allows network designers to connect MLS networks together in a secure manner without requiring a separate router for each level and category of information.[Ref. 11:p. 1] It is designed to provide a B2 level of security although it is not accredited. It is designed to operate with the Verdix Secure LAN (VSLAN), a B2 accredited product.

The untrusted LAN may include both trusted and untrusted components as Figure 8 depicts. A security guard is shown that provides connectivity to a lower-classified system.

3. Wide Area Network (WAN)

The WAN portion is based on the Defense Communications System (DCS) backbone. It is connected to the Trusted LAN by a Network Front End (NFE) such as a BLACKER Front End (BFE) or a CANEWARE Front End (CFE). Untrusted and trusted workstations can dial in via a trusted Terminal Access Controller (TAC). As depicted in Figure 7, several trusted community security managers are needed to provide key management, access control and auditing. These security managers are needed for BLACKER, CANEWARE, SDNS, DOD Intelligence Information System (DODIIS) Network Security for Information Exchange (DNSIX), and Electronic Key Management System (EKMS)-related systems.

BLACKER is an NSA developed A1 certified system in operation today for meeting strategic/sustaining base requirements. It is a host to host encryption system that will let the three classified segments of the DDN share a common backbone. It meets some of the tactical Army requirements but is considered unsuited for tactical operations because it must be repaired at Depot level and cannot be repaired in the field (Intermediate level).[Ref. 12:p. 2]

CANEWARE is an NSA developmental system incorporating new technology which is backward compatible with BLACKER. It meets most of the tactical Army requirements.[Ref. 12:p. 2] It is targeted for a B2 level of MLS. CANEWARE is field repairable and has full GOSIP compliance. It uses FIREFLY technology which is not releasable to allies. FIREFLY evolved from public key technology and is used to establish pair-wise traffic encryption keys for the subsequent encryption of data.[Ref. 13:p. 172]

The target architecture guides the program efforts and does not try to attempt simultaneous development of all of the components and capabilities. The diverse nature of the trusted components lends itself to inherent development risks. Thus, the near-term focus is on limited MLS capabilities. Success will depend upon an effective blend of MLS and operational functionality. The target architecture will be continually refined based upon near-term findings.

C. NEAR-TERM ARCHITECTURES

The near-term architectures presented in this section describe how they can be used in operational environments. They provide immediate and near-term operational capabilities that lay the foundation for the target architecture. They include the five component architectures: Guard, Workstation, LAN, Database Management System and Host. The technologies involved are sufficiently mature, promising, and meet DoD needs. The architectures provide an initial set of MLS capabilities and are not intended to provide full MLS capabilities since that objective is not achievable in the near term.

The operational environment for the near-term architectures includes nationally deployed systems for data communications. Almost all of these systems operate in the system high or dedicated mode. As is the case with the ATCCS system, the ASAS BFA also operates in the system high mode. The WWMCCS system represents one such nationally deployed system. It operates at TOP SECRET system high. The military planners who use this system normally access information classified SECRET or lower. ASAS operates at the TOP SECRET system high mode while its users in the ATCCS operate in the SECRET mode. Data is currently transferred between WWMCCS and the SECRET systems through cumbersome review and downgrade mechanisms. Often other sites are forced to operate their local unique system at the TOP SECRET system high level solely to facilitate communication with WWMCCS, despite a desire to run these systems at the SECRET level.[Ref. 10:p. 15.] Unlike WWMCCS, ASAS is a subordinate system to the ATCCS and cannot impose its TOP SECRET classification level upon its ATCCS users. Like the "other sites" in the WWMCCS system, however, ASAS must operate at the SECRET level to communicate with the ATCCS. ASAS does this through what is called a collateral enclave which is a human review filter (discussed shortly) in order to sanitize its information to the SECRET level for its ATCCS users. While the WWMCCS guard (discussed shortly) is application specific, the capability to provide a similar ASAS guard becomes more apparent. The near-term architectures would allow sites to process data on a SECRET system when appropriate, while providing users a means to access data from both TOP SECRET and SECRET system high systems.

The Target Architecture and Implementation Strategy investigates and uses its near-term architectures operationally at the program testbeds and other sites to encourage the fielding of similar capabilities at other sites. The near term strategy is to address the most common security ranges: TOP SECRET and SECRET, SECRET and unclassified, and TOP SECRET/SCI and SECRET (applicable for the ASAS to ATCCS implementation). The following is a discussion of the five component architectures presented by the TAIS as near-term MLS architectures. Some of the current technologies that support these architectures are described. Each of these architectures has the potential to provide MLS capability within the ATCCS.

1. Guard Architecture

The emphasis of the guard architecture is to provide limited near-term operational capabilities whereas the emphasis in the other architectures is to establish a foundation for mid-term and long-term MLS improvements. A guard is defined as a process or set of controls that helps to control trusted transfers across security boundaries. Thus a guard can include components that downgrade data (change the classification of the data or its container without changing the data) as well as components that sanitize data (reduce the actual classification of data by changing the data). Guards help to transfer information between systems operating at different classification levels.

Security guards have been in use for years in lieu of MLS systems. Many guards have been developed because of their functional simplicity and because they allow limited MLS interoperation between dedicated or system high mode systems. Guards also have a relatively low current development risk and high payoff, which makes them an attractive capability in providing the intersystem interoperability required for an MLS system. A fully-MLS system lessens the need for guards although guards remain an obvious step in achieving MLS.

The Department of Defense Multilevel Security Program's National Security Agency testbed has surveyed many guards in its Survey and Analysis of Security Guards. Table V represents the guard overview. While the list of guards is numerous and some represent redundant efforts, the number of efforts reflects a growing number of competing commercial products, research into different guard-related topics, adaptation of common approaches for different environments, and development to the needs of different applications. [Ref. 14:p. 3] The DOD MLS Program sponsors a number of guards in whole or in part. Guards have been the focus of much attention since they are suitable for near-term fielding and because the objective of the MLS Program is to expedite the fielding of MLS capabilities. Some of the guards funded include the WWMCCS guards, because they satisfy a requirement that is of significant interest to the Commanders-in-Chief (CINCS); the Modern Aids to Planning System/ Command Automation System (MAPS/CAS) and MLS-100, both low to high guards; and the Secret to Unclassified Network Guard (SUNG) which will provide an important e-mail guard capability.

There are two types of guards: low-to-high (LTH) and high-to-low (HTL). LTH guards support data flow between systems where the sending system operates at a lower classification level than the receiving system. The general security requirements guards must meet are to prevent leakage of data from the high to the low side and to defend against penetration and data integrity or denial of service attacks from the low side. Some transfers are achieved by pure simplex links, which allow no acknowledgement to be returned from the high to the low system. These one-way links use no explicitly defined guard. A shortcoming of LTH guards produced to date is that there has been almost no attention placed on protection against denial of service attacks from the low side.

High-to-low guards can be classified into three categories: cyclic redundancy check (CRC) based guards, automatic sanitization guards, and human review guards. Human review guards are terminals placed between communicating systems with the terminal operators serving as security reviewers. Human review guards have been selected for the program for two reasons:

1. A well-designed human review guard should be useable in a wide variety of DOD systems.
2. Human review guards should be within the state of the art using new trusted products.[Ref. 10:p. 54]

Cyclic Redundancy Check based guards still involve a human reviewer and are sometimes considered to be a type of human review based approach. The improvement from earlier human review based approaches is that with CRC based guards, the human reviewers remain at their normal workstations and there is no need for a person to man a terminal dedicated solely to the guard function. CRC guards are being developed for several intelligence systems and might see widespread use within the intelligence community. Some examples include the United States Air Force, Europe (USAFE) Guard and the Joint Services Imagery Processing (JSIPS) Guard. CRC based guards work as follows: human review is done in the system high high-side host. After the review is completed, the data and label are automatically supplemented with a CRC. The data is then released to the guard which checks the CRC to ensure that the data has not been changed, verifies that the label is at the low level, possibly performs additional checks, and releases the data. This concept relies on two assumptions: the users will not act maliciously; and there is no malicious software in the high-side system. The problem is that these assumptions are valid for Defense Intelligence Agency accredited systems but not for many non-intelligence systems. Encryption that supplements the CRC is needed to defend against malicious modification of the data. This encryption is referred to as an Encryption-Based Integrity Lock (EBIL).

Automatic sanitization guards automatically change the data to lower its classification and then release the data to the low-side system. This guard avoids involving humans in the data flow. It is not possible in most cases, however, because data is normally not well enough structured and the sanitization rules are not defined well enough to permit this automatic sanitization. It has been successful in sanitizing sensor data because sensor data is automatically generated in a rigid format. The automatic sanitization of sensor data is application-specific and has no widespread applicability. Products have not been successful to date in providing a generic base for automatic sanitization. Radiant Mercury and the WWMCCS guard are recent attempts to improve on the percentage of data that can be handled without human involvement.

2. Workstation Architecture

This architecture is based on a two-level trusted workstation. It supports full-capability usage of both high (e.g., TOP SECRET) and low (e.g., SECRET) systems from one workstation and is thus an improved capability over a guard. Workstations are important to the near-term MLS for the following reasons:

1. Many trusted workstations now are coming available.Trusted workstations offer a relatively simple platform (compared with hosts, discussed later) to begin experimentation with MLS capabilities.
2. Workstations house the user interface, which can support an MLS operational view even though most of the hosts and servers accessed operate in the system high mode.
3. Many of the new trusted workstations (e.g., Compartmented Mode Workstations (CMWs)) provide selected features and assurances beyond B1, and thus might enable using the workstations (supplemented with certain operational restrictions) in environments where a B1 base normally would not be sufficient. [Ref. 10:p. 18]

Figure 8 shows the workstation architecture. The example is a two-level workstation connected to LANs operating at the SECRET and TOP SECRET levels. The workstation is supplemented with several security guards for improved functionality. The low-to-high guard shown in the figure supports data transfers from a SECRET LAN to both local TOP SECRET systems and a TOP SECRET WAN (the Defense Secure Network 2 (DSNET2)). Included in the workstation but not shown is a software-supported human review-based guard function. This guard function supports downgrades from TOP SECRET to SECRET systems. Integration of these components may require some development. [Ref. 10:p. 18] This example of a trusted workstation could be changed to indicate ASAS for the WWMCCS Host, and the Secret LAN could be the area common user system (MSE) that supports ATCCS.

This architecture uses trusted multiwindow workstations and guards to support interaction with multiple system high systems. The trusted workstation allows the user to access systems at different classification levels simultaneously and transfer data between security levels (assuming the user has the appropriate privilege). The user can alternate working with both systems through the multiple windows. It is not necessary for all workstations to have MLS in this configuration; only those workstations needing access to both the SECRET and TOP SECRET systems. The TAIS program plans to use this architecture, or a similar one to support interaction between the TOP SECRET WWMCCS and a SECRET command-unique system (e.g., the SECRET CAS planned for CENTCOM).[Ref. 10:p. 19]

3. LAN Architecture

This architecture (Figure 9) is based on a two-level LAN. A two-level LAN allows sharing of the LAN by MLS systems or by system high systems operating at different security levels. One approach is to provide Commercial COMSEC Endorsement Program (CCEP) encryption-based products to provide separate communities of interest on a single network. Another approach is to provide separation on a per-connection basis (e.g., trusted LANs).[Ref. 10:p. 19] A trusted LAN architecture requires trusted communication protocol capabilities to integrate individual trusted products into networks. Currently a B2 rated trusted LAN product, Verdix

VSLAN, exists and has been demonstrated in prototype configurations with many of the trusted workstation products.[Ref. 10:p. 20] The two-level LAN is a logical next step once one or more two-level workstations are installed and operational. One of the DOD program testbeds will use a two-level LAN while other sites plan to use it as well.[Ref. 10:p. 20]

4. Database Management System Architecture

This architecture (Figure 10) involves a trusted DBMS. A trusted DBMS can be relied upon to enforce a mandatory security policy on database objects labeled at different sensitivity levels. The trusted DBMS supports the sharing of data between two separate system high communities. Two-level LANs and workstations can be included if needed. From the figure, the SECRET and TOP SECRET communities are supported by SECRET and TOP SECRET LANs. The DBMS server is accessible to both of these communities. Users operating at a high security level have a view of the entire database; users operating at a low security level have a restricted view of only the portion of the database at or below the user's security level. For example, TOP SECRET cleared users can have read access to the entire database while SECRET cleared users are restricted to read and write functions within the SECRET portions of the database. TOP SECRET system high workstations cannot write to SECRET portions of the database, which would result in the SECRET data being upgraded to TOP SECRET.

This architecture eliminates duplication of information on separate systems. There are no cumbersome procedures that allow SECRET information to be available to TOP SECRET users, and as a result the database is more timely and accurate. This architecture could be substantially improved by adding a two-level trusted workstation, which would allow TOP SECRET cleared users to write to SECRET portions of the database.

Three different architectural approaches are being pursued for secure DBMS products: a trusted filter approach, a subsetting approach (constrained), and a monolithic approach (unconstrained). In the trusted filter approach, a trusted function encircles an untrusted, or lower assurance, DBMS. Integrity locks in the form of checksums or CRCs ensure the integrity of labeling. TRUDATA is Atlantic Research Corporation's (ARC) implementation of this approach. The trusted filter approach is considered a near-term solution since it takes advantage of the capabilities of current commercial DBMS products. The drawback is that assurance is limited to B1 because an untrusted DBMS is used.

In the subsetting approach, the host operating system is relied upon to ensure separation and enforcement of mandatory access control. Here, the trusted database is restructured into separate single-level fragments that can be stored in separate operating system objects. Separate instances of the DBMS running at different security levels have access to these database fragments based on the security level of the DBMS process. The commercial product ORACLE Relational DBMS (RDBMS) is following this approach. This approach allows the trust level of the DBMS to increase as the trust level of the underlying operating system increases. Because of the requirement to run a separate DBMS at each active security level, this subsetting approach has negative performance impact as the number of security levels increases.

Finally, in the monolithic approach, the DBMS itself enforces separation and enforcement of MAC. The INGRES RDBMS and SYBASE Secure Query Language (SQL) Server are using this approach.[Ref. 10:pp. 62-63] The ability to validate the assurance of the system is decreased because of the separation of the DBMS from direct hardware mediation and because of the large amount of trusted code that needs to be examined.

The DBMS architecture is at a higher developmental risk than the workstation architecture despite six or more trusted DBMSs under development. These DBMSs are not as far along in their development as are trusted workstations or LANs. One of the reasons is that the underlying guidance from the National Computer Security Center has not yet been finalized.[Ref. 10:p. 21] Many issues in DBMS security have not been resolved among policy makers, standards organizations and vendors. Because most trusted DBMSs use the relational model, many AIS databases may have to be restructured. Finally, the technology is immature as with the workstation architecture and may be required to integrate the components.

5. Host Architecture

The MLS Host is the fundamental building block for MLS systems. The near-term architecture uses a B3 or A1 trusted host based on a B3 or A1 trusted operating system. The trusted operating system provides the platform for MLS applications such as guard software and DBMS systems. It can serve as the security front-end to multiple single-level applications. The operational value of this architecture is derived from the high-assurance products which enable support of greater risk ranges.

The TAIS program is not examining the host architecture in a program testbed because several current efforts are ongoing to develop and field similar architectures. A near-term technical issue of the trusted host architecture is the evolution to the trusted workstations that can support simultaneous sessions at different security levels. Trusted workstation capabilities are preferable but because they require trusted protocol software, they significantly complicate the requirement for a high-assurance (B3 or A1) host. The current network protocol software is untrusted and presumes system high workstation operation. This issue (the requirement for a trusted network protocol) limits the capability of high-assurance host architectures.

TABLE VI SELECTED GUARD OVERVIEW

Guard	High-to-Low	Low-to-High	Target of Platform	Status
AFMSS Guard	limited	✓	B2	Research prototype
AIG	✓	✓	TBD	Research
ASAS MSF	✓	✓	none	Operational
ASCC	ack only	✓	none	Operational
Boeing MLS LAN	ack only	✓	A1	Available
Collateral Filter	✓	none	none	Operational
EISI Guard	ack only	✓	B1	Operational soon
EPIC Guard	ack only	✓	B2	Operational
Firewall Guard	✓	✓	B1	Operational soon
FSM	✓	✓	B3	Research prototype
GAAP	✓	✓	TBD	Beginning
GateGuard	✓	✓	none	Operational
GTNP	✓	✓	B3	Operational
JSIPS Guard	✓	✓	C2	Operational soon
KBMLS	✓	NA	TBD	Research prototype
LOCE/IINCOMNET	ack only	✓	B2	Research prototype
LOCKGuard	✓	✓	A1+	Available for beta sites
MAPS/CAS Guard	✓	✓	B2	Operational mid 1993
MFM	✓	✓	A1	Research prototype
MLS-100	ack only	✓	B2+	Operational
NASA RAP	✓	✓	B3+	Operational
NAVMACS-2	✓	✓	none	Operational soon
OBU Sanitization	✓	✓	B1-	Operational
OWG	nack only	✓	B2	Operational
PSIDS	✓	TBD	TBD	Beginning
Radiant Mercury	✓	✓	B1	Operational soon
RAPIDE Guard	✓	✓	B1	Operational mid 1993
SCOPE	✓	✓	B1	Operational soon
Simplex Links	none	✓	none	Operational
STATS-3	ack only	✓	B1	Operational
SUNG	✓	✓	B1	Operational mid 1993
UNIGUARD	✓	✓	none	Available
USAFE Guard	✓	✓	B1	Operational
VSLAN	none	✓	B2	Available
WWMCCS Guard	✓	✓	B3	Operational soon

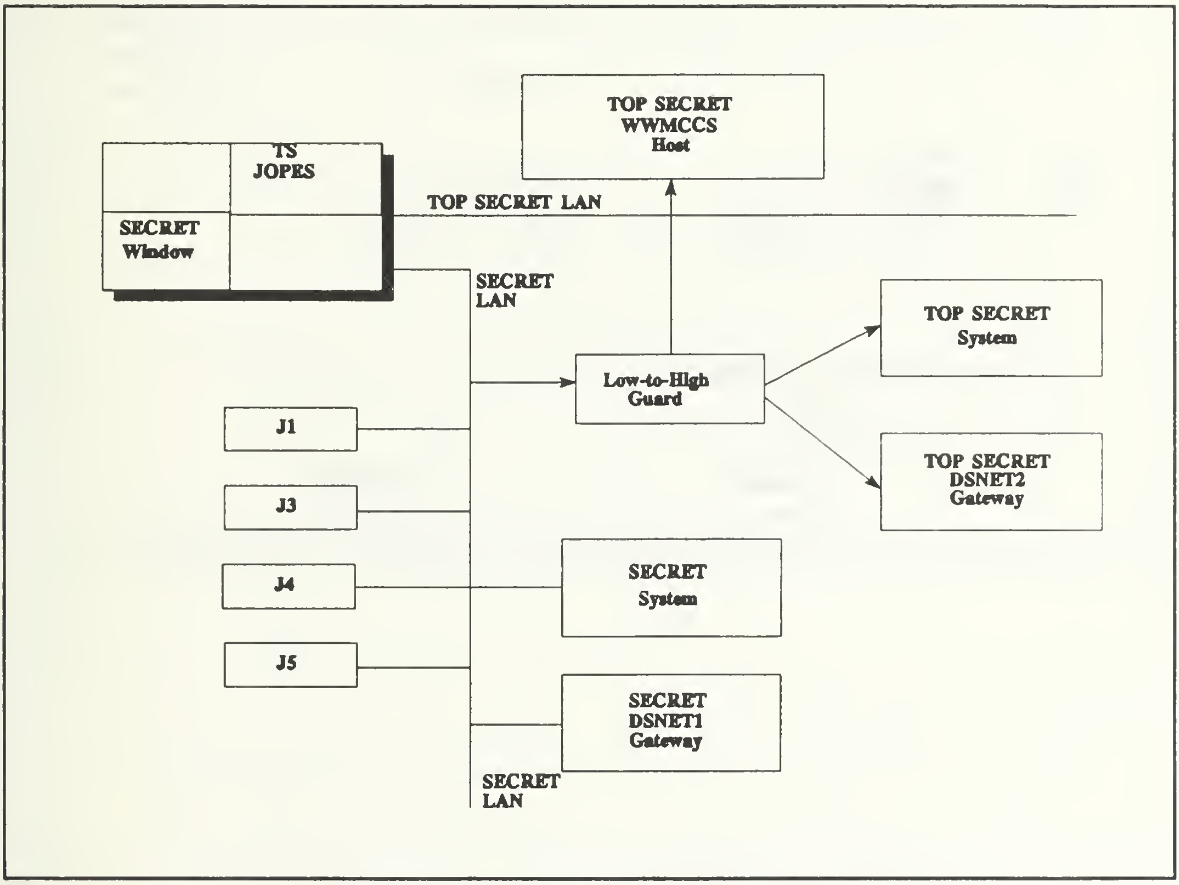


Figure 8 Workstation Architecture

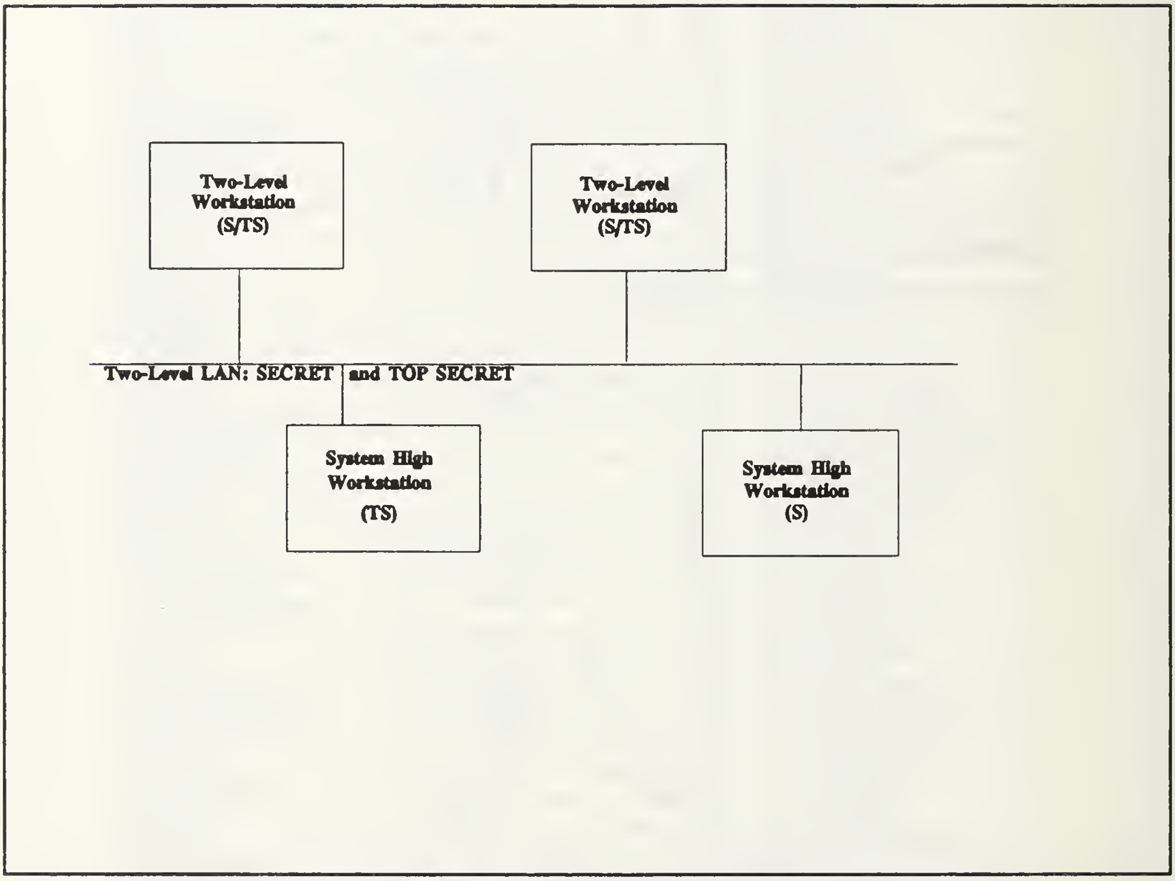

Two-Level Workstation (S/TS)
Two-Level Workstation (S/TS)
Two-Level LAN: SECRET and TOP SECRET
System High Workstation (TS)
System High Workstation (S)

Figure 9 LAN Architecture

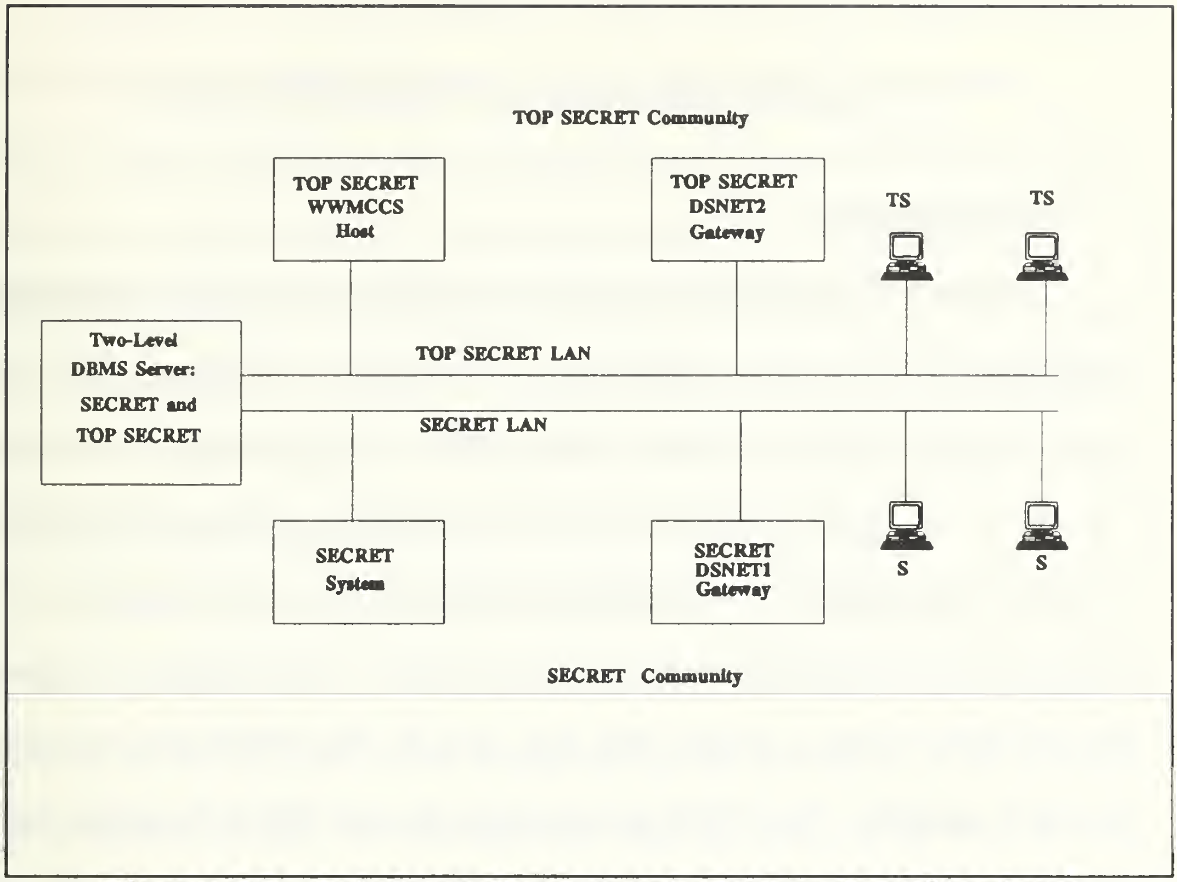


Figure 10 Database Management System Architecture

V. MLS IMPLEMENTATION WITHIN THE ATCCS

A. BACKGROUND

The Defense Planning Guidance specifies the requirement for MLS in its Battlefield Development Plan Command, Control and Communications Architecture (BDP C3A) priority number 34, dated 24 August 1988. It says, "Timely exchange of intelligence information and nuclear control orders will be a particular problem, complicated by accreditation requirements for multiple levels of security." It is further delineated in the Force Level Control System Concept (FLCS) in the Army Command and Control Master Plan (AC2MP) Volume 1, 14 May 1990. [Ref. 12:p. 1] The ATCCS does not currently have MLS capability. The ATCCS Implementation Strategy (FM 24-7) requires that the ATCCS be secure to the B2 level. Further, the US Army Signal School has outlined the requirements for MLS in its Mission Need Statement (MNS) and Operational Requirements Document (ORD).

MLS is needed both for external interface to the ATCCS (DCS connectivity) as well as for ATCCS internal operation (primarily for the ASAS BFA). The five component architectures (guard, LAN, trusted workstation, database management system and host) of the Target Architecture and Implementation Strategy for the Joint MLS Technology Insertion Program (referred to as TAIS) presented in Chapter III are the vehicles used to structure how MLS can be implemented within the ATCCS.

Although each of the five component architectures presents workable near-term versus target MLS capabilities, only portions of the five will be incorporated to best provide an MLS capability so that MLS capabilities can be implemented with either technologies currently available or technologies approved for use and awaiting NCSC accreditation. While the target architecture in Figure 7 would provide the MLS solution, a near term architecture is necessary as a practically feasible implementation strategy. The target architecture suggests an ideal approach that is not currently feasible since the technology required to support the architecture has yet to be developed.

The MLS implementation strategy proposed for the ATCCS includes both a target and near term architecture. Each proposed architecture includes an MLS capability internal to the ATCCS LAN (ASAS interoperability) and external (DCS and untrusted LAN) to the ATCCS LAN. For this thesis and within the context of the TAIS, ATCCS will be considered to be a LAN although is actually a WAN.

B. AN MLS ATCCS TARGET ARCHITECTURE

1. MLS Internal to ATCCS

The trusted multiwindow workstation concept described in the Workstation architecture offers a tremendous capability to ATCCS users. Coupled with a two-level LAN, the TOP SECRET (ASAS) users and the remaining SECRET ATCCS users will be fully MLS. For access to shared databases, a trusted DBMS using the monolithic approach such as the SYBASE Secure Query Language (provided it is accredited) will provide ATCCS users with the required MLS assurance.

2. MLS External to ATCCS

Specific MLS solutions will not be needed for external interfaces to the ATCCS. The trusted workstation in conjunction with the two-level LAN described above offers the user a transparent ability to interface with any network. As such, networks other than the ATCCS are not "external" in the normal connotation of this word. The MLS proposal outlined for the internal operation of ATCCS reflects a fully MLS system that can interface with external LANs and WANs.

C. AN MLS ATCCS NEAR TERM ARCHITECTURE

1. MLS Internal to ATCCS

The ATCCS currently operates at the SECRET system high mode. Of its five BFAs, the IEW's subfunction, ASAS, is the only subfunction that operates above the SECRET level, at TOP SECRET/SCI system high mode. Within the IEW BFA, ASAS could be made multilevel secure in its own right through a compartmented workstation such as TIS Trusted Xenix, a B2 certified trusted workstation to automate the sanitizing of information before release throughout the ATCCS.

2. MLS External to ATCCS

a. WAN connectivity

The CANEWARE Front End (CFE) provides an MLS capability (intended for certification at the B2 level) for potential use between the ATCCS LAN and the Defense Communication System (DCS). Although BLACKER is currently certified at the Al level, it is better suited for the strategic community because of its inability to be repaired at the tactical field level.

b. Untrusted LAN connectivity

The Verdix Secure Internet Protocol Router (VSIP) trusted router has the potential to provide the interface to untrusted LANs.

VI. CONCLUSION

The objective of this thesis was to look at MLS implementation within the ATCCS. The requirement for MLS is necessary in order to exchange information within our own military forces as well as with allied forces. The ATCCS currently does not have a seamless MLS capability that allows for user transparent data handling and communications capabilities.

The scope of this thesis was the target ATCCs architecture. No attempt was made to justify or replace the five Battlefield Functional Areas that constitute the ATCCS. The operating systems that support the BFA's were examined only in terms of the security measures they provide for the ATCCS. The ATCCS architecture operates in the SECRET system high mode. The ASAS operating system that supports the IEW BFA is the only system that operates above SECRET, at the TS/SCI classification level. Currently the ASAS system interfaces to the ATCCS via a human review filter, called a collateral enclave.

The methodology of this thesis was to first examine the basic computer security principles found in DoD 5200.28, Trusted Computer System Evaluation Criteria. Next the ATCCS architecture was studied to better understand its place in the context of the strategic (sustaining base), theater (operational), and corps & below (tactical) environment. How information flows within the ATCCS was also examined. Armed with this basis of knowledge, the MLS products and technology were next introduced.

The vehicle used for assessing MLS product technology was the Joint MLS Technology Insertion Program Target Architecture and Implementation Strategy. The TAIS categorized its assessment into two categories: target and near term. The near term was further delineated into five component architectures. This TAIS categorization was the tool used for applying the MLS products into the ATCCS architecture.

As a result of applying the MLS product technology assessment to the ATCCS architecture, two different implementation strategies became apparent. In the target architecture, a trusted multiwindow workstation operating on a two-level LAN, with a trusted DBMS product such as SYBASE would provide the ATCCS with a fully MLS capability. While all of the products to support the target architecture are not yet developed, a near term strategy is a more realistic alternative that provides an interim solution to the target architecture. The near term strategy includes operating the ASAS operating system with a compartmented workstation to allow for an automated sanitizing of information before release throughout the ATCCS. To interface with external WANs and untrusted LANs a network front end such as the CANEWARE front end will provide an MLS capability between the ATCCS LAN and the DCS WAN.

LIST OF REFERENCES

1. Chokani, Santosh,"Trusted products evaluation," *Communications of the ACM*, v.35, n7, July 1992.

2. Department of Defense National Computer Security Center, *Department Of Defense Trusted Computer System Evaluation Criteria,* DOD 5200.28-STD, Government Printing Office, Washington, DC, December 1985.

3. Russell, Deborah, and Gangemi G.T. Sr., *Computer Security Basics*, 1st ed., O'Reilly & Associates, Inc., 1991.

4. Department Of Defense National Computer Security Center, *Computer Security Requirements--Guidance For Applying The Department Of Defense Trusted Computer System Evaluation Criteria In Specific Environments,* CSC-STD-003-85, Government Printing Office, Washington, DC, 25 June 1985.

5. Department Of Defense National Computer Security Center, *Technical Rationale Behind CSC-STD-003-85: Computer Security Requirements--Guidance For Applying The Department Of Defense Trusted Computer System Evaluation Criteria In Specific Environments,* CSC-STD-004-85, Government Printing Office, Washington, DC, 25 June 1985.

6. Department Of Defense National Computer Security Center, *Trusted Network Interpretation Environments Guideline-- Guidance For Applying The Trusted Network Interpretation,* NCSC-TG-011 Version 1, Government Printing Office, Washington, DC, 1 August 1990.

7. Department Of Defense *Army Command and Control Master Plan--Executive Summary*, Government Printing Office, Washington, DC, August 1990.

8. Department Of The Army *Field Manual 24-7 (Expanded Outline) Army Tactical Command and Control System (ATCCS) Systems Management Techniques*, 4 December 1992.

9. Rogers, Bill, "Evolving ATCCS integrates the battlefield: refined by war, $17 billion system aims for near-real-time response," *Government Computer News*, v. 10, 23 December 1991.

10. Defense Information Systems Agency, *Target Architecture and Implementation Strategy for the Joint MLS Technology Insertion Program*, September 1991.

11. Verdix Corporation, *VSLAN Verdix Secure Local Area Network*, Verdix corporation, Chantilly, Virginia, 1992.

12. Department of the Army, U.S. Army Signal School, *MISSION NEED STATEMENT for Multi-Level Security (MLS) for Data Communications Networks (DCN)*, September 1992.

13. Rogers, Herbert L., *"An Overview Of The Caneware Program,"* paper presented at the National Computer Security Conference, 10th, 21-24 September 1987.

14. Mitre Corporation, *TAMPS Security Guard Survey and Analysis Working Paper,* 1992.

INITIAL DISTRIBUTION LIST

No. Copies

1. Defense Technical Information Center 2
Cameron Station
Alexandria VA 22304-6145

2. Library, Code 052 2
Naval Postgraduate School
Monterey CA 93943-5002

3. C3 Academic Group, Code CC 1
Naval Postgraduate School
Monterey, CA 93943-5000

4. Myung Suh, Code AS/Su 1
Naval Postgraduate School
Monterey, CA 93943-5002

5. Carl R. Jones, Code AS/Js 1
Naval Postgraduate School
Monterey, CA 93943-5002

6. Kathleen S. Loper 2
28 Kristin Dr.
Portland, Ct 06480

7. Jeanne D. Schmidt 1
1311 Old East Main St. Unit A
Meriden, Ct 06450