THE MITRE CORPOR
BEDFORD, MASSACHUSETTS

WORKING PAPER

WP- 3697 __ __ __ __ __
No. Vol. Series Rev. Supp. Corr.

Subject: MACIMS Security Configurations

To: Distribution List

Contract No.: F19(628)-71-C-0002

Sponsor: ESD

From: S. B. Lipner

Project No.: 5150

Issued at: Bedford, Massachusetts

Dept.: D73 /18865

Page 1 of 14 Pages

Date: 6 January 1971

Approved for MITRE Distribution: Jonathan Mitchell
J. Mitchell

ABSTRACT:

This paper presents four configurations that can be used to allow MACIMS to support its mixture of secured and unsecured terminals. The configurations avoid creating a requirement for general-purpose multi-level security software, relying instead on separation of classified and unclassified information. Further MACIMS security studies will be directed toward evaluation and selection of the alternatives presented and of other alternatives which may be suggested.

THIS WORKING PAPER IS PREPARED FOR CORPORATION INTERNAL USE. IT HAS NOT BEEN REVIEWED BY THE DIRECTORATE OF SECURITY REVIEW, DEPARTMENT OF DEFENSE, AND IS NOT FOR PUBLIC RELEASE.

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

SECTION I

INTRODUCTION

This paper presents four alternative configurations that can be used to protect classified data in MACIMS. Further MACIMS security studies will define the cost, feasibility, and impact on MACIMS operations of each configuration.

Section II below outlines the assumptions under which the alternatives were developed. Section III describes the four alternative configurations and presents a few comments on the advantages and disadvantages of each.

SECTION II

ASSUMPTIONS

The alternative configurations presented below were developed to conform with the following assumptions:

(1) MAC will initially receive a WWMCCS Force Control dual processor to be installed at Hq MAC.

(2) Some time after the Force Control processor has been installed, each of the MAC Air Forces will receive a WWMCCS General Staff Support-Large (GSS/L) dual processor.

(3) Although the WWMCCS specification requires that the operating system include security features, these features will not be adequate for use with the MACIMS mixture of secured and unsecured terminals. Should this assumption prove incorrect, the operating system itself will provide all the security required, and the software-secured configuration of the Development Plan can be implemented.

(4) Attempts will certainly be made to provide a high level of security by modifying the WWMCCS operating system. However, these attempts will necessarily be controlled by the details of the WWMCCS hardware and software and will not be discussed below. If and when they suceed, the software-secured configuration of the Development Plan will be feasible.

(5) The security features of the WWMCCS operating system will be adequate to provide need-to-know control over Secret and Confidential information in a MACIMS processor with no unsecured terminals.

SECTION III

ALTERNATIVE CONFIGURATIONS

INTRODUCTION

This section describes four approaches to configuring the MACIMS data processors so that classified data receives adequate protection while unsecured terminals receive adequate service. Each configuration provides less flexibility than would a full resource-sharing, software-secured configuration but involves less technical risk.

The first approach involves allocation of classified and unclassified functions to the three MACIMS processing centers. The remaining three approaches attempt to provide for the processing of classified and unclassified data by a single processing center.

APPROACH 1 - GEOGRAPHICAL DIVISION OF FUNCTIONS

R. C. Davis has suggested[1] that the problem of providing security for the MACIMS processors may best be addressed by operating each processor as either an all-classified or an all-unclassified system. The regional (MAC Air Force) processors would be devoted primarily to MACTRAC but might also handle some other unclassified tasks. The Hq MAC computer would perform all MACIMS classified processing. Communications processors (CIU) would allow unsecured terminals to interact only with the MAC Air Force processors and secured terminals to interact only with the Hq MAC processor. Summary reports could flow from the regional processors to the one at Hq MAC. The proposed configuration is shown in Figure 1.

The main advantage of the geographical division approach is that it avoids entirely the problem of mixing classified and unclassified data in a single processor. A direct solution to this problem is generally considered beyond the limits of current technology.[2] The three approaches outlined in the following subsections represent partial solutions to the problem with associated costs in extra hardware and reduced operating efficiency. Other advantages of the geographical division approach include:

[1] R. C. Davis to S. B. Lipner, D73-M-1568, MACIMS Security, 8 December 1970.

[2] W. H. Ware, editor, Security Controls for Computer Systems (Report of DSB Task Force on Computer Security), Rand Report R-609, February 1970 (C).

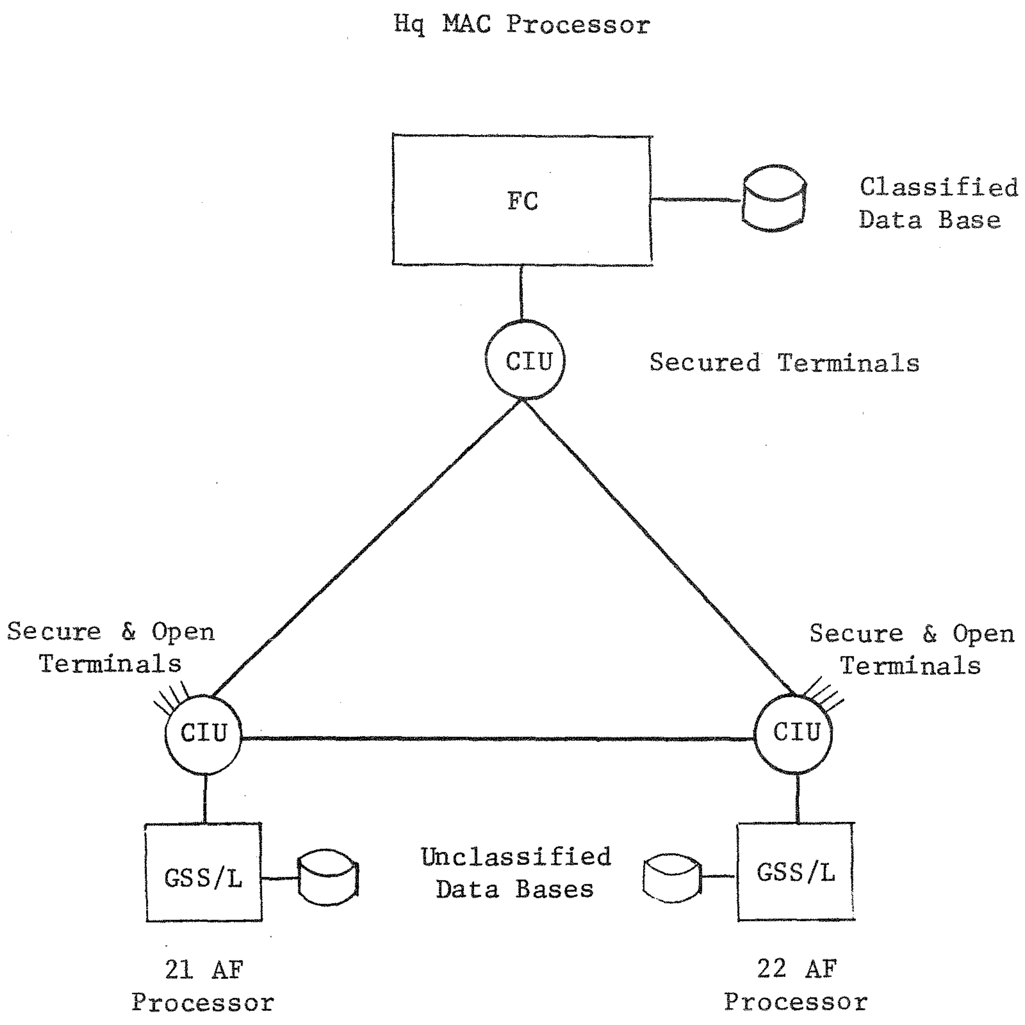

Figure 1. Geographical Division of Functions Configuration

(a) Most of the MACIMS terminals in unsecured areas will require interaction only with MACTRAC.

(b) MACTRAC will tend to be more manageable if developed on dedicated computers. Civil airline experience has shown significant difficulty in integrating reservation systems with other management applications.

(c) The configuration will tend to centralize the remaining MACIMS functions at Hq MAC and enhance their coordination.

Geographical division of functions does have its disadvantages. Among them are:

(a) The requirement that only secured terminals interact with applications implemented at Hq MAC may result in some terminals being secured even though they only operate on unclassified data.

(b) The separation of MACTRAC from other MACIMS functions is contrary to the philosophy of integration of functional areas and the establishment of one common data base.

(c) If a MAC Air Force computer is to back up the Hq MAC processor in the event of an outage, procedures must be established to redistribute workloads, secure the Air Force processor, and transfer the data base.

(d) The scheduled acquisition of MAC's WWMCCS processors will preclude the operation of unsecured terminals under this approach with the initial MACIMS (Hq MAC processor only). Thus, either

    (1) one of the approaches outlined below must be implemented as an interim measure, or

    (2) the unsecured terminals must be served outside of MACIMS.

The geographical division approach can be implemented alone or in combination with the approaches outlined below. For example, both regional processors might be used in an unclassified mode while the Hq MAC processor served both secured and unsecured users. In this case, only the Hq MAC processor would require one of the security approaches described below. The regional processors could still avoid the hardware and efficiency costs of these approaches.

APPROACH 2 - SPLIT THE DUAL PROCESSOR

The first method of handling both classified and unclassified data in one of the MACIMS dual processors involves splitting it into two uniprocessors: one classified and one unclassified. A communications processor connects the two uniprocessors to each other and to MACIMS user terminals (Figure 2). The communications processor may hold incoming messages for either processor if it is inoperative and forward the messages when the processor returns to service. Alternatively, it may redirect such messages to one of the other MACIMS sites.

The configuration can include limited data base sharing by allowing the unclassified processor to transmit selected data to the classified one or by giving the classified processor read-only access to unclassified storage. In the former case, security restrictions will prevent the classified processor from asking the unclassified one for data by message since there is no way to guarantee that classified data are not concealed in a request. In the latter case, the unclassified processor will not know when the classified one is accessing unclassified files and may inadvertently interfere with the classified processor by ill-timed updates. Either problem can probably be solved during detailed configuration design.

The major advantage of the approach outlined above is its low risk. There is little about the method that is new or untried. Communications processors have been certified to handle both classified and unclassified traffic, while the data processors are effectively isolated and should not require certification. Most available dual processors are equipped with configuration controls and can be divided into two independent uniprocessors.

The disadvantage of this approach is that it represents a poor use of modern hardware. The costs of the configuration should be higher than those for operation as a dual processor, since the two independent uniprocessors must operate without sharing main memory, operating system code, secondary storage or control units. Indeed, one available dual processor (the CDC 6500) cannot be divided in the manner described. There is only an inflexible method of sharing data--that is, of giving the classified processor access to the unclassified data base. Finally, the method sacrifices the load sharing and immediate backup inherent in a dual processor. If one uniprocessor becomes overloaded or malfunctions, the second can only assume its workload after a manual switchover has been performed. Automated switchover is possible but would approximate the mechanism of Approach 3, as described below.

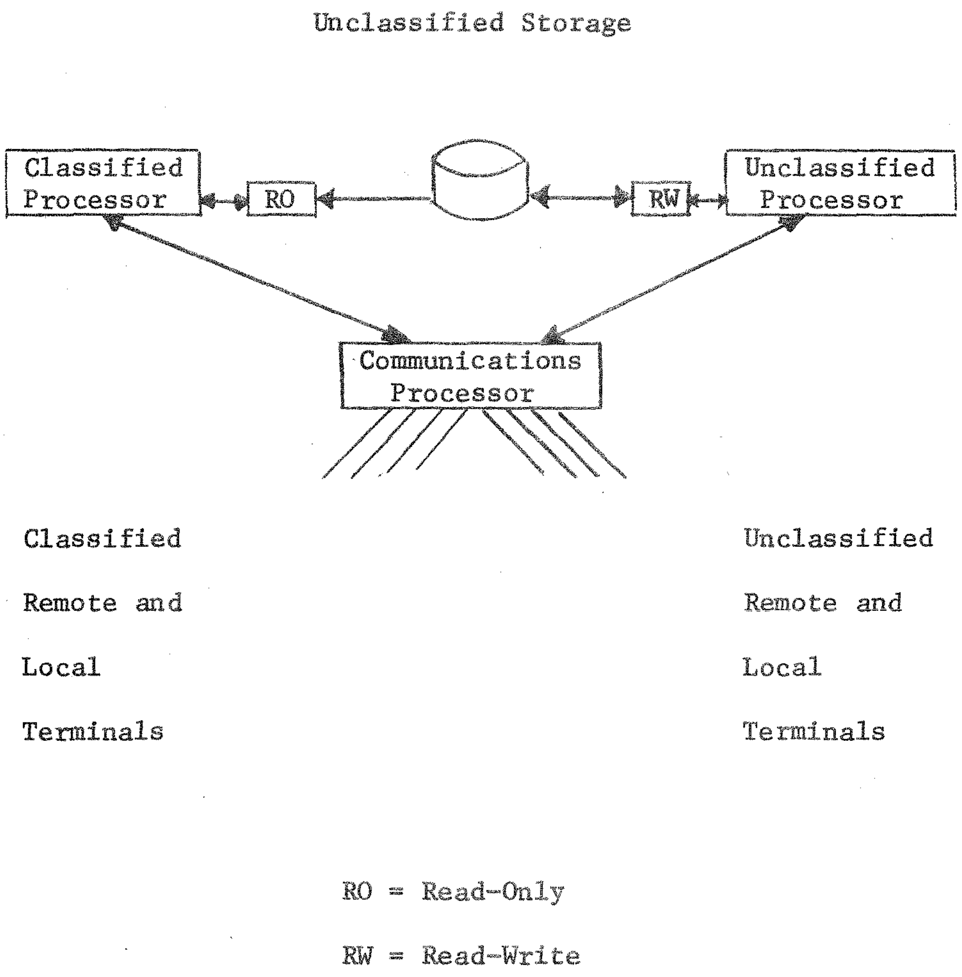

Figure 2. Split Processor Configuration

APPROACH 3 - EXTERNALLY CONTROLLED TIME-SLICING

The second approach to securing a dual processor involves using a communications processor to switch the dual processor from a classified to an unclassified state. The communications processor controls the data processor's access to secondary storage through electronic switches. In switching the dual processor between classified and unclassified states, the communications processor directs the data processor to terminate input-output operations and save a core image on disk or drum. The communications processor then clears the data processor's core memory and directs it to initialize itself and begin executing the alternate (classified or unclassified) saved core image. Electronic switches under control of the communications processor assure that the data processor, when in its unclassified state, never accesses classified data. Messages that arrive addressed to one state (classified or unclassified) are held in the communications processor until that state is active (see Figure 3).

Approach 3 can provide a somewhat better file-sharing mechanism than Approach 2. The communications processor and storage switches can be configured and programmed so that the data processor has read-write access to unclassified secondary storage when it is in the unclassified state and read-only access when in the classified state. Thus, classified programs can make use of data in the unclassified data base but cannot write classified data into it by mistake. Since the dual processor is only in one state at a time, the problem of file access coordination is reduced compared to Approach 2.

The major advantage of Approach 3 is that it uses the dual processor as a dual processor. Thus, it preserves much of that configuration's reliability and flexibility. The communications processor can consider the data processor's classified and unclassified workloads in scheduling its state-switching operations. The configuration for Approach 3, thus, does not create the inflexible division of resources characteristic of Approach 2.

There are three major disadvantages to the configuration of Approach 3. The first is its responsiveness. If a classified message arrives while the dual processor is doing unclassified processing, the message must wait until the processor's state is switched. State-switching may be a fairly long operation. If so, it cannot be done too frequently, or the dual processor will spend all its time state-switching and none processing MACIMS applications. Thus, messages that arrive when the processor is in the "wrong" state will have a long wait for response. The second disadvantage to Approach 3 is its cost. Special switching equipment may be required, and some secondary

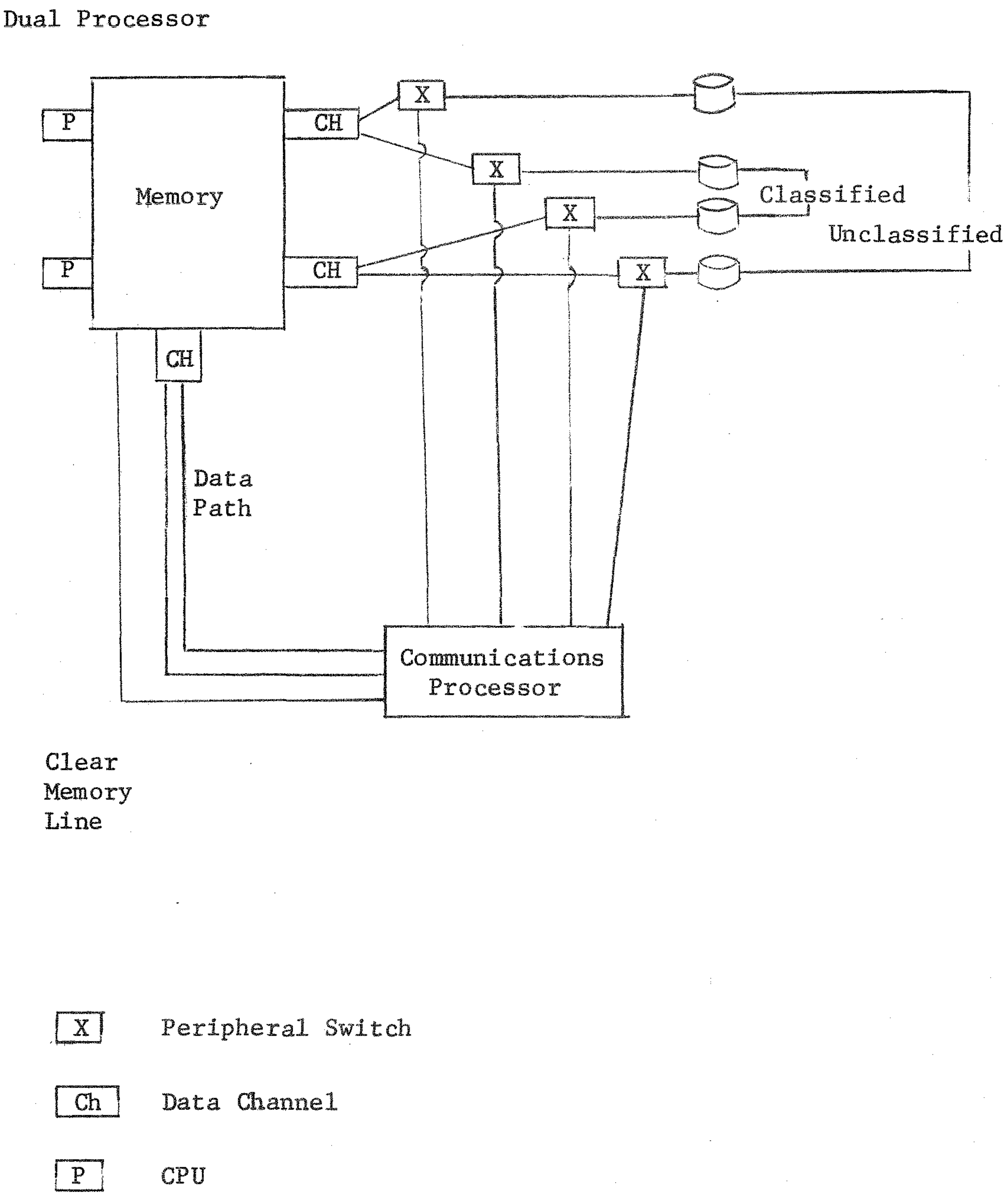

Figure 3. Externally Controlled Time-Slicing Configuration

storage will have to be duplicated. Thus, the resulting configuration will be more costly than a software-secured one. The final disadvantage to Approach 3 is its newness. While the approach seems straightforward, it does not appear anywhere in the literature. Thus, it will have to be certified as an entirely new approach. Some difficulty and delay for certification should be expected.

APPROACH 4 - VIRTUAL MACHINES

The final method for providing security in the MACIMS data processor involves writing a control program to split the processor into two "virtual" machines--one classified and one unclassified, each with its own operating system. The control program interprets the primary and secondary memory address references of each virtual machine and translates them so that they address the correct physical locations. Invalid address references are caught during interpretation. The partition of secondary storage between virtual machines is typically static and fixed by physical address; that of primary memory is typically dynamic and hardware-aided. As long as the control program is correct and its translation tables protected, neither virtual machine can access any part of the other's storage since all physical access paths are established by the control program. Since both virtual machines share the processor's physical storage, the control program can switch the processor from classified to unclassified operation very quickly. This approach is implemented by the CP-67 system.[1]

File-sharing in the virtual machine environment can be similar to that with externally controlled time-slicing. The classified virtual machine can be provided read-only access to the unclassified data base by appropriate definition of translation tables. Problems of file lockout for updating will, however, arise in such a configuration.

The communications processor (or CIU) in the virtual machine configuration assembles messages and passes them on demand to the data processor. The control program interprets requests for data by the virtual machines to assure that neither asks for messages of the wrong classification.

The virtual machine approach shares most of the advantages of the external time-slicing approach. In addition, it can offer a high degree of responsiveness since there is, for example, no need to clear main memory of classified data before unclassified processing begins.

[1] IBM Data Processing Division, An Introduction to CP-67/CMS, Doc. 320-2032, May 1969.

The virtual machine approach has two major disadvantages. The first concerns its hardware requirements; virtual address translation in main memory is almost always hardware-assisted, and not all processors include the required hardware. Furthermore, the WWMCCS specifications do not require such hardware. Thus, there is a good chance that the WWMCCS Force Control dual processor will simply not be suitable for the implementation of a control program. The second disadvantage concerns the fact that the approach is very close to a software solution. As such, it will require an extensive certification--perhaps aided only slightly by the small size of the control program.

DISTRIBUTION LIST

INTERNAL

D-73
N. W. Anschuetz
S. A. Bauer
E. H. Bensley
S. Berkovits
J. A. Clapp
J. T. Connolly
C. G. Crothers
Z. W. Esper
R. H. Fayman
R. J. Fortin
R. A. J. Gildea
I. D. Holtzman
O. R. Kinney
A. J. Kleinman
E. L. Lafferty (2)
S. B. Lipner (10)
J. L. Mack
T. A. Mackey
J. Mitchell (5)
R. W. Piernot
M. N. Sherman
L. Stites
N. B. Sutherland
L. M. Thomas
A. M. Thompson
D. M. Townley
J. S. Vitalis
E. W. Williamson

D-93
R. C. Anderson
H. T. Cervantes
J. M. Vene

PROJECT

ESD, L. G. Hanscom Field
Bedford, Massachusetts
Lt/Col. D. Kennedy (MCL)
Maj. R. Karabela (MCL)
D. Eriksen (MCL)
W. Morton (MCL)

ESD, Hq MAC (MACAM/ESD)
Stop 111B
Scott AFB, Illinois
Lt/Col. R. Bullington (MCDM)
Lt/Col. J. Dellaripa (MCDM)
Lt/Col. R. Hook (MCDM)
Lt/Col. G. Pickett (MCDM)
Maj. E. Hansen (MCDM)
Maj. D. Salisbury (MCDM)
Maj. E. True (MCDM)
Capt. J. Hawkins (MCDM)
Capt. L. Thompson (MCDM)
R. LeClair (MCDM)

Approved for Project Distribution

Jonathan Mitchell

Jonathan Mitchell
Project Leader