

PAPER

on

DESIGNING & OPERATING A MULTILEVEL SECURITY NETWORK USING STANDARD COMMERCIAL PRODUCTS

Abstract: In March 1996, the 2nd Bomb Wing, Barksdale AFB, LA declared initial operational capability on the first multilevel security system (a.k.a. multilevel network or MLN) using only low-cost commercially available products. The MLN integrates the many sources and sensitivities of information (secret and unclassified) necessary for a commander to effectively command and control global bombing operations. We developed and implemented the MLN for two reasons:

- First, to reduce the number of terminals each command and control center (C²) operator must use. Multiple non-integrated systems and the technical necessity of separating classified and unclassified systems have created enormous system overhead and operator training inefficiencies - base and Air Force wide. In many operational areas, real estate is at a premium and reducing required floor or table space would also improve the work environment. Reducing the number of garrison terminals needed could eventually affect deployed operations, where less combat support weight means more combat weight could be transported.
- Second, to reduce operational costs. Costs are reduced by buying commercial products. Savings are enhanced by the commonality of parts among various operational systems as they connect to the network. Training costs will decrease as new operational systems are added to the network because a common human-computer interface would exist between systems.

The MLN is working and the single most expensive item is the operating system at roughly \$3,000 each (\$1900 each with a site license). The MLN is already a model for other C² centers and continuous refinement will only improve its desirability.

Prepared by:

Richard A. Griffith & Mac E. McGregor
C4 Technology Validation Office
DSN 781-3777 Commercial (318) 456-3777
Fax: DSN 781-2638 Commercial (318) 456-2638
E-mail: mcgregor@c4tvo.barksdale.af.mil

Prepared for:

AIR FORCE C4 TECHNOLOGY VALIDATION OFFICE
245 Davis Ave. East, Suite 2
Barksdale AFB, Louisiana 71110

Contract Number: BA95218AFO Project Element Plan 04

U.S. Air Force Publication Release Authority

JILL N. ALTMAN, Lt Col., USAF
Director, C4 Technology Validation Office

DESIGNING & OPERATING A MULTILEVEL SECURITY NETWORK USING STANDARD COMMERCIAL PRODUCTS

ABSTRACT

In January 1996, the Air Force declared initial operational capability on its first multilevel security system (a.k.a. multilevel network or MLN) using only low-cost commercially available products. The MLN integrates the many sources and sensitivities of information (secret and unclassified) necessary for a commander to effectively command and control global bombing operations. We developed and implemented the MLN for two reasons:

- First, to reduce the number of terminals each command and control center (C²) operator must use. Multiple non-integrated systems and the technical necessity of separating classified and unclassified systems have created enormous system overhead and operator training inefficiencies - base and Air Force wide. In many operational areas, real estate is at a premium and reducing required floor or table space would also improve the work environment. Reducing the number of garrison terminals needed could eventually affect deployed operations, where less combat support weight means more combat weight could be transported.
- Second, to reduce operational costs. Costs are reduced by buying commercial products. Savings are enhanced by the commonality of parts among various operational systems as they connect to the network. Training costs will decrease as new operational systems were added to the network because a common human-computer interface would exist between systems.

The MLN is working and the single most expensive item is the operating system at roughly \$3,000 each (\$1900 each with a site license). The MLN is already a model for other C² centers and continuous refinement will only improve its desirability.

KEYWORDS

Air Force B1 B2 C² CMW Command and Control Compartmented Mode Workstation
MLN MLS Multilevel Network Multilevel Security System SCO SecureWare UNIX

PLAYERS

The Second Bomb Wing is the host organization at Barksdale AFB, LA. This fully combat operational B-52 wing can bomb any point on earth and return without landing at another base. This capability was proven when B-52's departing Barksdale, bombed Iraq during Desert Storm and returned to Barksdale. The nerve (C²) center for such an undertaking is the command post. All information necessary for force deployment feeds into the command post by telephone, radio, and a myriad of computer systems and networks. From the command post, the commander develops, organizes, and executes the battle plan.

The Command, Control, Communications, and Computers Technology Validation Office (C4TVO), operating location B of the Air Force Communications Agency (AFCA) at Scott AFB, IL, is also at Barksdale. The C4TVO's charge is validating the latest commercially available technologies and integrating them into the operational Air Force. The purpose of this mission is to enhance combat operations by applying technology:

- a.) Without the long research and development lead times required by designing systems from scratch,
- b.) Using commercial specifications instead of the more specialized military ones,
- c.) To act as a force multiplier through reduced combat support payloads, reduced personnel requirements, system simplification, or reduced operational cost.

This proximity to an operational unit permits the C4TVO to evaluate new concepts and technology at the tip of the spear instead of in laboratories separated by distance and occasionally the reality of operational needs. The location also permits rapid project changes or redirection, including cancellation, without losing huge investments in time or sunk development costs.

PROBLEM IDENTIFIED

The command post has sixteen major computer application systems that are or will be connected to it. These systems were all designed for their separate purposes before compatibility across major systems was a concern in system development. Inside the command post, there are mission planners, aircraft maintenance controllers, and others whose system access requirements are different. In addition to the numbers of systems to which each person needs access (anywhere from 1 to 16), each person may require access to only a certain classification level (secret or unclassified) of a given system. Without a course change, command post members would require unnecessary movement about the command post to access various systems as battle stations became heavily populated with incongruent terminals. Hence, the "fog" in the fog of war would thicken. The command post needed a better way of doing business.

PROPOSED SOLUTION

Beginning in November 1993, wing operations, AFCA, and C4TVO representatives developed a B1 assurance level MLN (having B2 operational features) with two main objectives:

- First, to reduce the number of terminals each C² operator must use. Multiple non-integrated systems and the technical necessity of separating classified and unclassified systems have created enormous system overhead and operator training inefficiencies - base and Air Force wide. In many operational areas, real estate is at a premium and reducing required floor or table space would also improve the work environment. Reducing the number of garrison terminals needed could eventually affect deployed operations, where less combat support weight means more combat weight could be transported.
- Second, to reduce operational costs. Costs are reduced by buying commercial products. Savings are enhanced by the commonality of parts among various operational systems as they connect to the network. Training costs will decrease as new operational systems were added to the network because a common human-computer interface would exist between systems.

As the system design progressed, it became apparent a successfully operating system would have applicability in all active and reserve Air Force command posts. Although not a major objective of the Second Bomb Wing host, portability to other command posts was always considered and design simplicity was the means to portability.

NETWORK DESCRIPTION

The MLN accesses unclassified and secret information from a single terminal type known as a compartmented mode workstation. Data confidentiality, integrity, and availability are maintained by combining a workstations' trusted computing base with technical and traditional procedural security measures. The network has unclassified and secret gateways and routers. Each workstation labels data unclassified or secret and transmits information to the proper gateway and router. Each gateway has an internal unlabeled and multilevel network interface card. The routers act as a firewall; hiding the network from the outside world. Network security is increased by prohibiting all common UNIX file transfer services since there are no operational requirements for them. All communication (e.g., electronic mail) beyond the firewall will be to mail hosts where aliasing will further protect the network by hiding MLN addresses from the outside. MLN users will have to pull their mail from the mail host rather than have it pushed to them. All MLN users are cleared for secret although they will not all have need-to-know access to all information within the network. Therefore, the security mode of operation is system high. Identification and authentication within the MLN is through user identification and passwording.

The security testing and evaluation team's methodology was to match the vendor-advertised security features against those of the MLN security policy. Where the advertised features met the security policy the team attempted to prove it or disprove the advertised feature. For those features not meeting the policy, we worked with the vendor to eliminate or mitigate the weakness. The penetration team assumed the positions of unauthorized users outside the MLN and authorized MLN users with bad intentions. They tried to penetrate the system configured in two ways - one as we intended the MLN to operate and the other with full customary UNIX file services available. This was to document, for potential follow-on MLN users, the disadvantages associated with full UNIX capabilities.

The MLN will be fully operational in the command post before any expansion beyond the command post's boundaries. The initial classified system connecting to the MLN is the Wing Command and Control System (WCCS). WCCS provides decision making information like weather, logistics, aircraft mission capability, etc. to the battlestaff for exercises, crises, and war. The initial unclassified system connecting to the MLN is the Core Automated Maintenance System (CAMS). CAMS provides the commander the maintenance status of all operational assets. There are no specially designed hardware or software items in the network. The most expensive item is the SecureWare, Inc. CMW+ 3.0 operating system - a secure version of SCO UNIX. The license price is about \$3,000 each for ten licenses. A new site licensing agreement with SecureWare will bring this cost to around \$1900 each.

DESIGN AND OPERATIONAL ISSUES AND LESSONS

An operational concern in designing the MLN was classified and unclassified data aggregation. If intruders were to compromise a fully operational (with all sixteen mission applications) MLN, they could presumably compose the full air order of battle. This knowledge, and knowing the unclassified networks beyond the firewalls had internet access, made the Designated Approving Official decide various MLN components would effectively meet the B1 and B2 assurance levels. Those components beginning at the MLN's secret gateway would have the mandatory access control feature of labeled security (B1). Those components between the MLN's secret gateway and the unclassified gateway would have the added assurance of a trusted path, least privilege, and proof the system can't be spoofed (B2).

The early challenges occurred when the OS vendor, switched from a previously tested and security certified OS version 2.3 to the current version 3.0. During our security testing and evaluation process, we discovered several security-related problems which required considerable coordination with SecureWare to resolve. Such problems are normal in any software design and development process. The vendor completed and delivered the patches. The patches passed the subsequent security and penetration testing and are now operational.

Other issues will arise as we add more and varied applications to the MLN. The main one with the first application suite, WCCS, were caused by differing system architectures. For example, the MLN was designed to use low-cost commercially available products like Wintel 486 systems. Initial MLN performance in such areas as screen refresh rate, etc., was slower than on WCCS terminals. This existed because MLN terminals are software driven and they were competing against WCCS diskless workstations where the X Window software was on a RISC chip. Upgrading MLN terminals to 90MHz Pentium processors seems to be the near term solution in our early trials. Faster processors, as they become readily available, will be the longer term solution.

An external incident directly affecting the MLN resulted from new WCCS OS versions being released with different software configurations which adversely affected the MLN interface. The new releases would not run, or would cause the MLN to crash. Our coordination with the WCCS program office (who is not specifically tasked with considering MLN requirements in their own system design) earlier in their design and release cycle would prevent this problem. These type problems will lessen as the MLN becomes a standard.

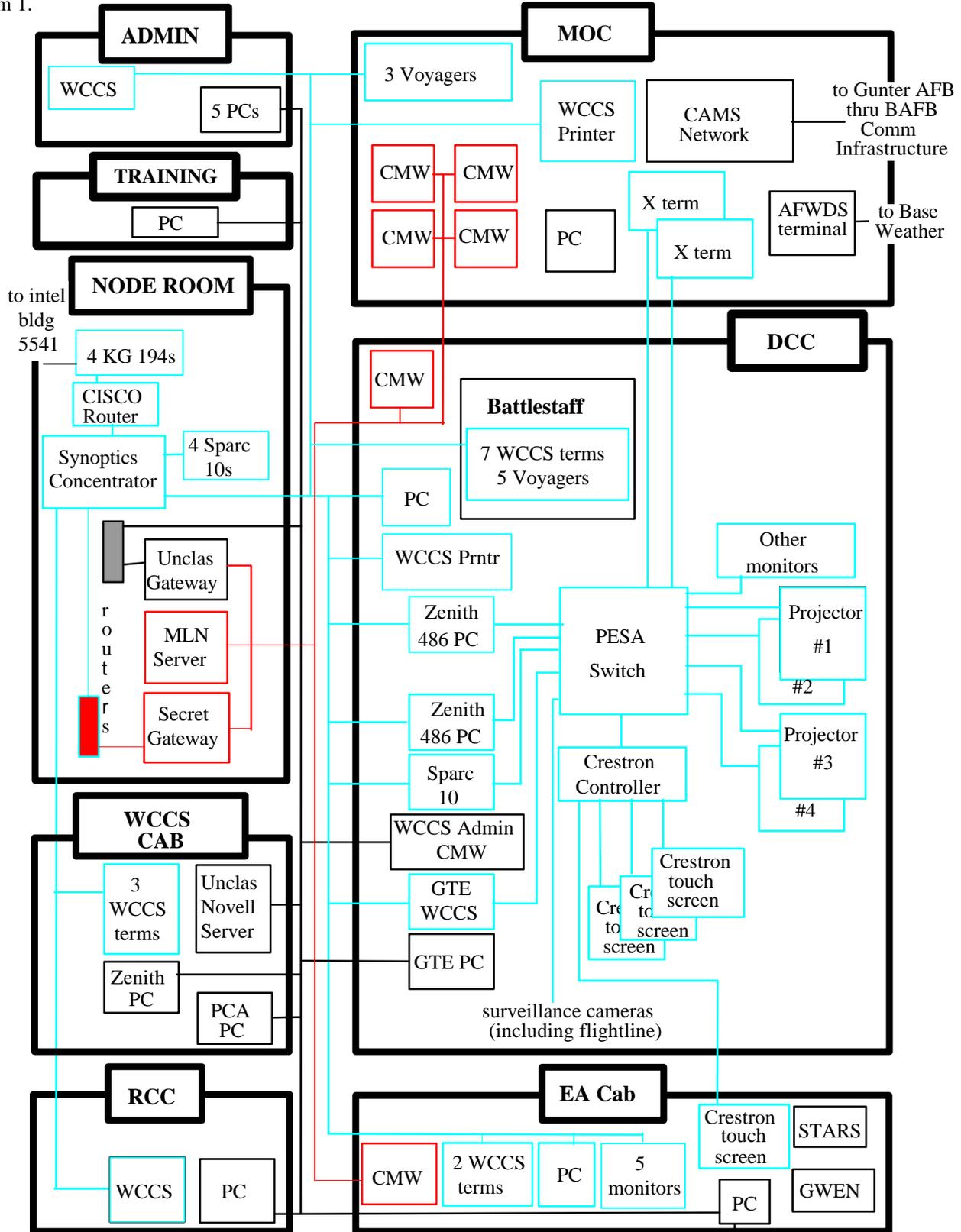
The final problem encountered to-date is a software licensing one, which SecureWare is changing. Our original SecureMail license permits seven users on the system, as we requested. We had only seven user terminals and that licensing arrangement appeared to meet our requirements. After receiving the software, we learned the software would only accept seven users in the system. What we truly needed was an unlimited number of users with a limit

of any seven simultaneous users. Better communication between ourselves and the vendor could have eliminated the delay in becoming fully operational until the newly licensed software package arrives.

SYSTEM OVERVIEW

Multilevel Network Logical Configuration

Diagram 1.



Colored lines are classified Red lines are MLN additions

to bldg 5546 concentrator

MULTILEVEL NETWORK CONFIGURATION KEY

AFWDS	Air Force Weather Data System
CAMS	Core Automated Maintenance System
CISCO	Private company name
CMW	Compartmented Mode Workstation
Crestron	Private company name
DCC	Display Control Center
EA Cab	Emergency Actions cab
GTE	Private company name (formerly Gray Telephone and Electric Company)
GWEN	Ground Wave Emergency Network
multi-level network	Multi-level Network (MLN)
MOC	Maintenance Operations Center
PCA	Private company name
PESA	Private company name
RCC	Reports Control Center
STARS	Strategic Arms Reduction System
Synoptics	Private company name
Voyagers	Sun corporation portable computers
WCCS	Wing Command and Control System terminal
X Term	NCD corporation dumb terminals running WCCS with an X Window user screen
Zenith	Private company name

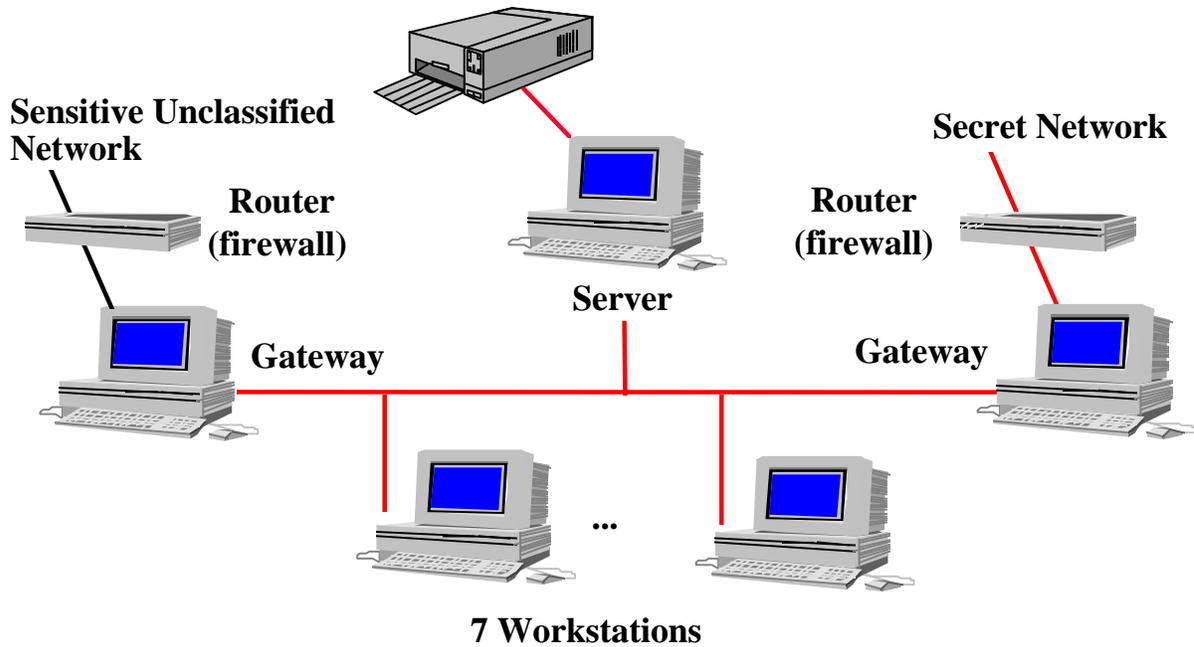
MULTILEVEL NETWORK COMPONENT CONFIGURATION

Hardware Identification. Table 1 shows the hardware on each workstation. Diagram 2 shows the hardware configuration.

Table 1. Hardware list.

Quantity	Item	Description
1	server	i80486 CPU, 2GB & 1GB hard drives, 3.5" floppy, 1 DAT 4mm tape drive
1	secret gateway	i80486 CPU, 1 hard drive
1	unclassified gateway	i80486 CPU, 1 hard drive
7	user terminal	i80486 CPU, 1 hard drive
1	laser printer	HP Laserjet 4 w/2MB memory

Diagram 2. Hardware Configuration



Red lines carry classified data

Table 2. Assurance Levels

Assurance Level	MLN Component	Boundaries
C2	Unclassified Segment	Begins at the unclassified gateway and includes the unclassified router
B1	Security Services	Begins at the secret gateway and includes the secret router
B2	MLN Segment	Includes the printer, user terminals, server, and all connecting lines

Hardware Notes.

All hosts are different Intel x486 platforms with 15" color monitors (to be upgraded to 17"). The disk drives range from 350 MB - 1 GB and the memory ranges from 28 - 32 MB.

Four compartmented mode workstations will be in the command post's Maintenance Operations Center (MOC), one in the Emergency Actions Cabinet (EA Cab), one in the Battlestaff area, and one in the Data Control Center

(DCC) for system administration. The server and gateways will be in the node room behind the EA Cab, each placed 1 meter apart.

Each gateway has two ethernet boards. They and the administration machine may only be accessed at the console. The gateways do no packet filtering. However, the operational user is considering using tcp_wrappers. Hot spares are planned for the gateways; two at the unclassified sensitive and two at the secret interface. The gateways will be statically routed.

The server will have at least two 2GB disk drives and at least 64MB memory.

There will be one multilevel printer (an HP 4) on the MOC floor. All output will be labeled at the appropriate classification level. Output for applications that reside outside the MLN (e.g., WCCS) will go to the normal application printers. For example, output for WCCS will print on the WCCS printer just as output from CAMS will print on a printer on the unclassified segment.

There are no modems. If dial-up service is required, then STU-IIIs will be used.

The floppy drive will not be accessible by the typical users. There may be a few users with floppy drive access. Drives df0 and df1 have been disabled and the drives cannot be accessed as a: and b: drives unless the user has the dosfloppy privilege.

Software Identification.

Table 3. Application Software

Product Name	Version	Vendor	Functionality
Office Professional		Microsoft	Spreadsheet, Slide Preparation, Word Processing, Database Management
SecureMail	2.0	SecureWare	Electronic Mail

Software Notes.

The compartmented mode workstation operating system is SecureWare 3.0 (CMW+ for SCO Open Desktop).

The compartmented mode workstation window system is an X-window environment.

The compartmented mode workstation includes MaxSix software, version 2.0, which provides additional network-related security capabilities. MaxSix provides the mechanism establishing authorized connections to high- and low-side systems from the appropriately labeled window through the correct network interface. It also labels the incoming data according to the assigned sensitivity label of the network interface.

Two Trusted Network (TNET) databases are used by MaxSix to implement security policy. They are the TNET Interface Database (TNETIDB) and the TNET Remote Host Database (TNETRHDB). The TNETIDB file specifies the default security attributes of datagrams associated with each network interface (each ethernet board). The TNETRHDB file specifies the security attributes associated with hosts residing on a network. For example, TNETRHDB specifies whether a host is another TNET host (e.g., another compartmented mode workstation) or a non-labeling host (e.g., a generic UNIX system). Also, TNETRHDB specifies the security accreditation range for the host. The host accreditation range is a set of minimum and maximum sensitivity labels representing those sensitivity levels that can be processed by the host as a whole. Table 2 shows the application packages installed on each workstation.

SUMMARY

The network is currently undergoing operational validation with a multilevel electronic mail system, one of the sixteen applications operating at the secret level (WCCS) and one operating at the unclassified level (CAMS). The MLN appears to be meeting the two design goals. However, until the MLN operational evaluation is complete, this should be considered an early, but reasonable conjecture.

Note: *Extra Drivel Not used in the above Paper*

One of the MLN's advantages is its ability to be a multifunctional user terminal. Besides tying in to several application specific networks, it also contains Microsoft's Official Professional Suite. The only application causing the MLN any problems was the Excel spreadsheet. We initially configured the MLN to allocate 4MB of RAM to Excel. The operational test showed it wouldn't work until the allocation was changed to 12MB.