Chapter 4

SSEM in the Secure LAN/WAN Environment

Introduction

A network is a system that interconnects a multitude of computers and workstations for the purpose of communications and information/resource sharing. To keep the various interconnected parts of the system interoperable, rules and procedures must be established. In a secure processing environment, networks have additional "layers" of rules and procedures imposed each addressing unique security requirements, with no one set of requirements (software or hardware) applicable to all security issues for any specific situation.

Problems could occur because there are layers of security, each very narrowly focused for specific conditions. For ever emerging systems and new equipment with greater capabilities and a multitude of abbreviations and operating names, the potential exists to overlook or forget "old" rules in favor of ever more simplistic ways of dealing with security, regardless of the layers involved. This tendency has created both the need for increased understanding of the various security layers when using shared resources in multi-secure network environments, and also the need for continuing industry awareness of network security problems[1].

This chapter is intended to address two principal facets of a very large and complex issue, information security in the network environment. First, it is intended to educate the reader on the many macro and micro aspects of network security. With such a large base to draw from, some issues will obviously receive more attention than other equally as important issues. The second aspect dealt with in this report is an attempt to apply the principles of systems engineering to network security problems. This will be addressed by providing examples of suggested approaches for overall control of network security using a recognized systems security engineering approach. Only networks with computers that process classified information will be addressed herein.

System Security Engineering Management (SSEM)

As user requirements mandate the need for ever more complex technology to fulfill operational requirements, at least one method is available which ensures the designed system has satisfied its many user security needs. In the disciplines of quality assurance, security and accessibility, SSEM[2] is an attempt to apply systems engineering to the host of possible problems that could affect overall security requirements particularly throughout the acquisition process, from concept exploration through deployment. In addition, SSEM sets the stage for long term security control over the life cycle of the system.

[1] **NCSA NEWS, The National Computer Security Association, Washington D.C., Vol.2 No. 2, January, 1991.**

[2] **SSEM is defined in MIL-STD 1785, Systems Security Engineering Program Requirements.**

The Multitude of Security Standards

To control the proliferation of classified information over networks, numerous standards exist[3] that define user restrictions, equipment capabilities, network management controls, audit trails, etc. These standards are not only applicable just for the system as it will first be configured, but they are also applicable to the system as it might exist in the future. The ultimate goal of an overall system security standard is to insure that a level of security, consistent with security priorities, is applied to all resources throughout their procurement and deployed life cycle process.

Not only are network applicable security standards far reaching, but there are also numerous security certification requirements imposed on the equipment used in networks[4]. Because of the fast pace of emerging equipment capabilities, many of these requirements are under constant pressure to be streamlined and simplified by those who often don't understand the technology issues behind communication security. When those who don't understand are faced with making a decision, often the potential threat issue, regardless of technical concern, is regulated to a position of less importance.

The concept of information security (INFOSEC) encompasses physical security, system/network administration and operating procedures, countermeasures (OPSEC), communications security (COMSEC), hardware emanations (TEMPEST), computer security (COMPUSEC) (including the National Computer Security Center's (NCSC's) rainbow series documents), and data integrity (including sensitive unclassified data and virus protection).

Understanding just how each discipline contributes to overall security for ever evolving specific system is a complex issue. Security control for complex and secure environments is really a management issue. SSEM is an element of systems engineering that applies scientific and engineering principles to identify and reduce overall security vulnerabilities[5] from all INFOSEC disciplines. These security disciplines are tied together or

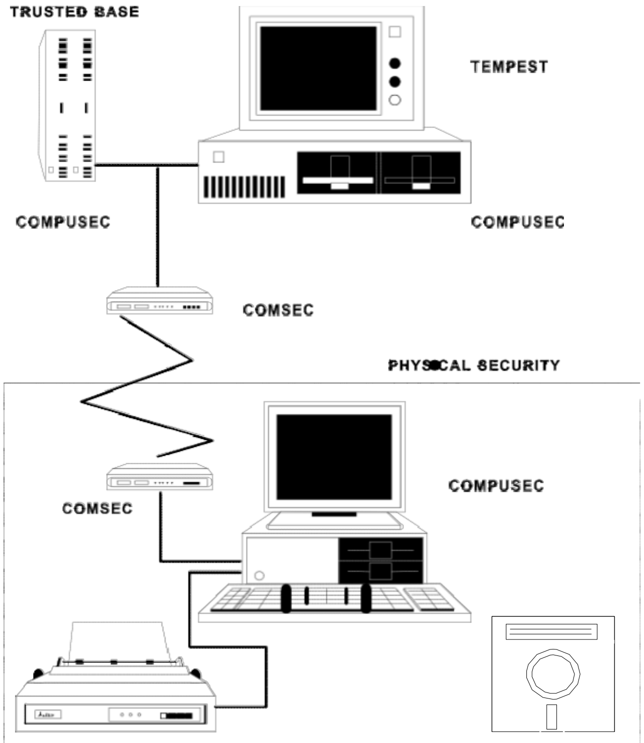


Figure 1 – Interrelated Computing Security Elements

[3] NACSEM and NTISSAM series documents; NCSC documents such as TDI and Rainbow series books; DIAM 50-3 and -4; MIL- STD 1757; MIL-HDBK 232; DOD, AF, AR, MC, JS, and Navy Instructions such as DC

[4] King, Julia, Secure Communications Stuck in Certification Mire, Fe

[5] MIL-STD 1785, Systems Security Engineering Program Requirements, as implemented by AFR 207-1, 3 October 1988.

inter-related as shown in Figures 1 and 2, with SSEM addressing each in turn.

The inter-related security requirements of a trusted computer and network are an ideal platform for the application of SSEM. When dictated by system vulnerability, a SSEM program insures all security disciplines such as COMSEC, INFOSEC, TEMPEST, operations security (OPSEC), counter-intelligence, etc. are integrated into the total system security engineering effort spread throughout the acquisition process, regardless of the operational requirements of any specific system. This paper explores the SSEM function in the acquisition of typical secure networks.

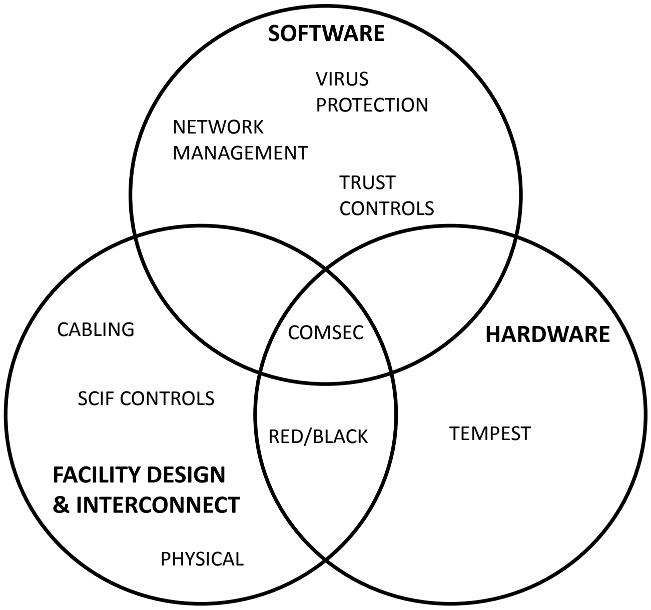


Figure 2 – Interrelated Disciplines

Generic Classified LANs

A LAN containing classified information can operate in one of several security modes that will be discussed later. A wide area network (WAN) is a data network typically extending a LAN outside the building, over telephone or other common carrier lines or dedicated communications links to connect to other LANs in remote buildings, possibly in distant cities. A WAN, in contrast to a LAN, often uses common-carrier lines, and is typically run over leased phone lines ranging from one analog phone line up to T1 (1.544 Mbps).

Multiple Local Area Networks (called Ribs) are connected together with shared data resources such as WAN gateways, optical disk farms, etc. by way of a high speed LAN known as a Backbone. The configuration is shown in Figure 3 with the Backbone shown as an overall high speed LAN.

The principal connection between the Ribs and the external WAN is made through a gateway device, a bridge, or a bridging router, depending on the topography and operating system of the user community. Bridges and bridging routers operate independently of the protocol employed.

Rib and Backbone architecture is best employed when packet order arrival and real time is important. The maintenance of this delivery system is especially important in Department of Defense (DoD) secure network implementations which use SIPRNET such as the Naval Supply Systems Command Logistics Network (NLN), and also when large amounts of high resolution graphics data must be retrieved from diverse locations across the US (CONUS- wide).

For secure networks, the primary area of importance is the protection of classified LAN information from unauthorized access through an unprotected gateway. There is also the secondary serious concern of protecting both sensitive unclassified and privacy information. Privacy information, although required by law to be protected, will not be addressed herein.

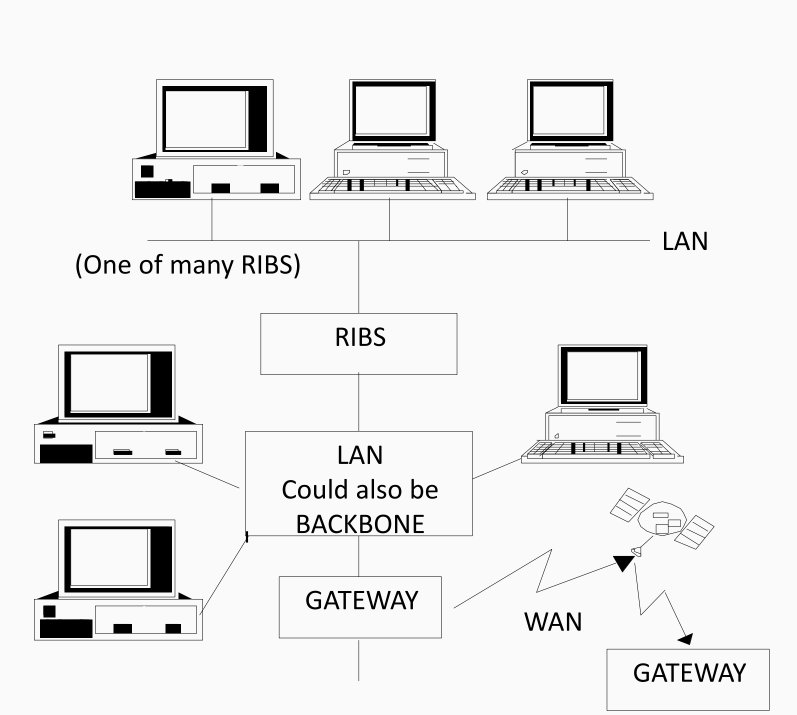


Figure 3 – Shared Interconnecting Resources

The gateway between an Ethernet LAN (Rib) and a FDDI (Federal Distributed Data Interface) backbone is the ideal place to put a secure gateway. Encryption and decryption of data can take place at the workstation LAN interface with a Stu-III (encrypting telephone), Serial Encryption Unit (SEU), a GILLERO[6] type pc board, or any similar type device.

A typical local message encrypted network is shown in Figure 4[7]. Each workstation represents either one or one of many. The router functions as the interface in this network to other outside networks. For this particular example, the SEU would perform simultaneous encryption and decryption utilizing either a RS-232 or RS-423 type interface.

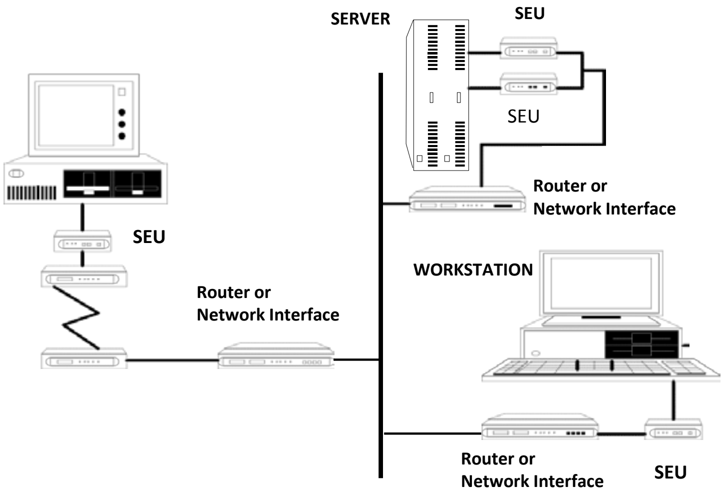


Figure 4 - Typical Encrypting Network

Two SEU's are necessary at the host here since communication between two users with and through

[6] ***GILLERO is a National Security Agency approved COMSEC encryption board intended for installation inside a TEMPEST approved personal computer.***

[7] ***IMS Serial Encryption Unit (SEU), Integrated Microcomputer Systems, Inc., Rockville, MD.***

the host might involve setting up two different secure channels. The SEU is a Controlled Cryptographic Item (CCI), as is a GILLERO board, a STU-III, and other similar items. CCI devices are unclassified when un-keyed, but are required to meet TEMPEST emission security limits when installed and operational as is any other DoD COMSEC device.

Classified Networks and Multiple Accesses

Multiple accesses imply the support of multiple simultaneous virtual connections. The quantity and type of these connections is governed by the traffic handling requirements levied on the specific server. These items can be fine tunable by the network administrator (or possibly the Security Officer) as part of network management functions.

Open System Interconnection (OSI) standards are intended to allow network hardware and software from a multitude of vendors the ability to interconnect into a network. According to OSI standards, five distinct areas have been identified for network management systems: fault and problem management, performance management, configuration management, accounting, and security management. The integration of these functions, on a single platform, constitutes integrated network management. One of the problems with using this projected future approach is the incorporation of security on an equal level with other major areas of management. Obviously, the network management function most important to SSEM is security management. However, when OSI is fully implemented into existing architectures, the tendency towards narrowly focusing on only interconnection security issues will be greatly increased.

Operational Modes

Various organizations have defined restricted modes of operation depending on the level or levels of classified information involved, the percent of time each level is used, each users need-to-know, and access to the network itself. The restrictions sometimes address various other security concerns in addition to COMPUSEC.

While not all requirements are under the control of the system or network administrator, most require some type of interaction. A typical example of the various modes of operation used during classified processing are indicated below:

- Multi-level: An ADP system that uses an operating system and associated system software to provide separation of personnel and material on the basis of security clearance and need-to-know.
- Compartmented: An ADP system that provides separation of materials by establishing separate physical devices and areas of memory for the exclusive use of the assigned user.
- Controlled: An ADP system that does not provide separation of users within the system. Separation and control is maintained by means of procedural or physical safeguards.
- Dedicated: An ADP system, that at any given time, is used exclusively for a particular category of data, and all users have clearance and need-to-know for all of the data in the

system. (note: unclassified is not permitted on this system when classified work is in process)

- System High: An ADP system operated in accordance with the requirements for the highest category and type of material then contained in the system. All personnel having ADP system access shall have a security clearance, but not necessarily a need-to-know for all material contained in the system. In this mode, the design and operation of the ADP system must provide the control of concurrent available classified material in the system on the basis of need-to-know. (note: unclassified is permitted in this mode when classified work is in process)
- Limited Access: An ADP system processing UNCLASSIFIED data that requires implementation of special controls to restrict access to individuals who, by their job function, have a need-to-know. Types of data processed in the limited access mode include FOUO, proprietary and Privacy Act data.

Trusted Systems

Computers that meet the National Computer Security Center's (NCSC's) trusting criteria have integrated safeguards into their operation such that only the users "trusted" to have access to the restricted data can actually gain access. According to an October 1991 Federal Computer Week article, at that time only eight companies offer secure database products approved through the NCSC[8]. However, a new requirements document, NCSC's Trusted Database Interpretation (TDI) was under development which would allow new systems to be evaluated and approved much quicker.

Software and data operational security as a functional part of open systems standard protocol is in its formative stage. Currently there are six levels of Trusted Computer classifications as shown on Figure 5 from the Orange Book[9]. As shown in the figure, requirements for software/hardware security policy, accountability, assurance, and documentation vary depending on the level of security to be achieved. The Orange Book only indirectly addresses emission security and/or Red/Black isolation requirements.

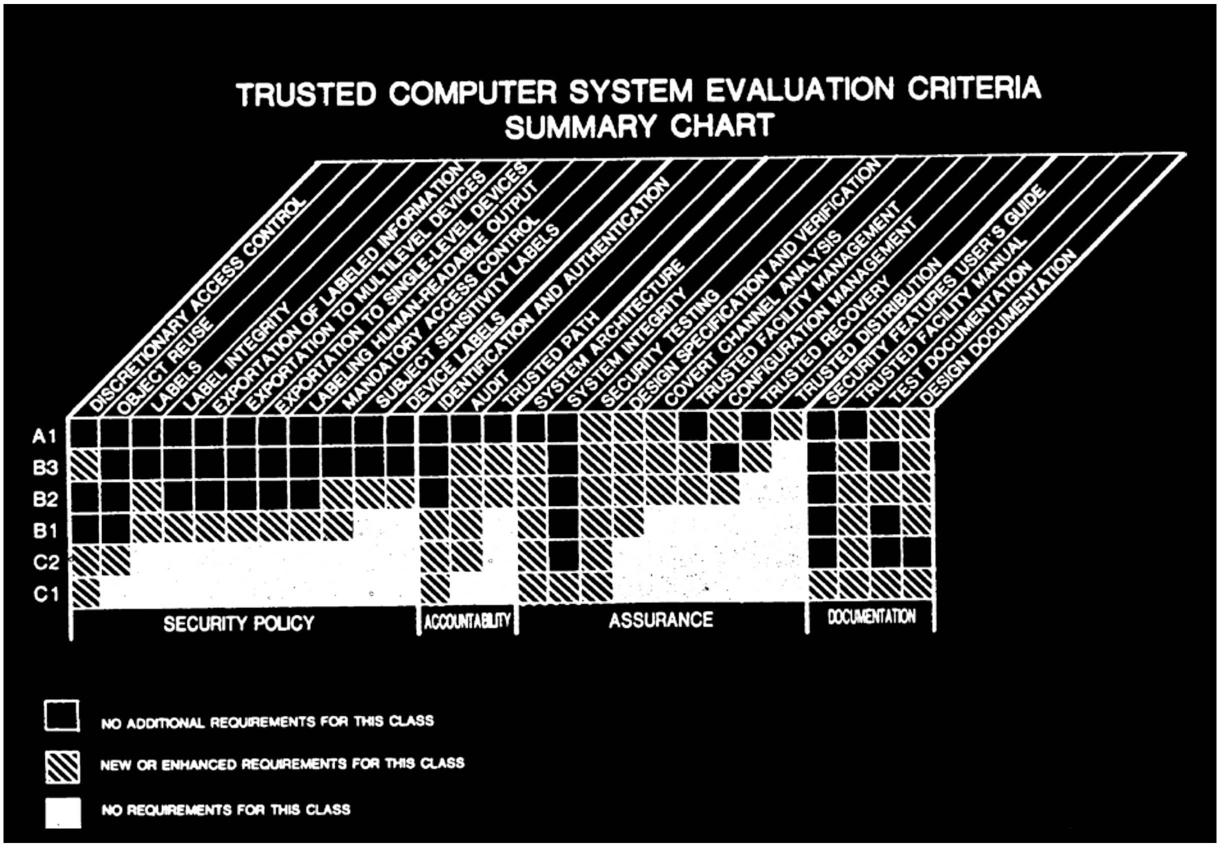
The required controls or "rules" of operation for the trusted computer and network are specified based on the level of trust placed on the system to protect and maintain security levels specified. Each higher level incorporates lower level rules plus additional new or enhanced rules for added security.

As an example of additional trusted requirements, when using B3 Gateway systems within a secure LAN and/or WAN, additional support must be provided for discretionary access control over and above the requirement for B2. The B2 requirement calls for mandatory access control with configuration management. The Gateway access capability required "need-to-know" rules

[8] *Danca, R., TDI Marks Banner Year for Trusted Databases, Federal Computer Week, October 7, 1991.*

[9] **Trusted Computer System Evaluation Criteria, DoD "Orange Book", CSC-STD-001-83, August 1983.**

over the distributed processing environment, with complete information security management and an upgraded access control, auditing, verification testing, and covert channel analysis in place.



TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA
SUMMARY CHART

	DISCRETIONARY ACCESS CONTROL	OBJECT REUSE	LABELS	LABEL INTEGRITY	EXPORTATION OF LABELED INFORMATION	EXPORTATION TO MULTILEVEL DEVICES	EXPORTATION TO SINGLE-LEVEL DEVICES	LABELING HUMAN-READABLE OUTPUT	MANDATORY ACCESS CONTROL	SUBJECT SENSITIVITY LABELS	DEVICE LABELS	IDENTIFICATION AND AUTHENTICATION	AUDIT	TRUSTED PATH	SYSTEM ARCHITECTURE	SYSTEM INTEGRITY	SECURITY TESTING	DESIGN SPECIFICATION AND VERIFICATION	COVERT CHANNEL ANALYSIS	TRUSTED FACILITY MANAGEMENT	CONFIGURATION MANAGEMENT	TRUSTED RECOVERY	TRUSTED DISTRIBUTION	SECURITY FEATURES USER'S GUIDE	TRUSTED FACILITY MANUAL	TEST DOCUMENTATION	DESIGN DOCUMENTATION
A1	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	▨	▨	▨	□	▨	□	▨	□	□	▨	▨
B3	▨	□	□	□	□	□	□	□	□	□	□	□	▨	▨	▨	□	▨	▨	▨	▨	□	▨	■	□	▨	□	▨
B2	□	□	▨	□	□	□	□	□	▨	▨	▨	□	▨	▨	▨	□	▨	▨	▨	▨	▨	■	■	□	▨	▨	▨
B1	□	□	▨	▨	▨	▨	▨	▨	▨	■	■	▨	▨	■	▨	□	▨	▨	■	■	■	■	■	□	▨	□	▨
C2	▨	▨	■	■	■	■	■	■	■	■	■	▨	▨	■	▨	□	▨	■	■	■	■	■	■	□	▨	□	□
C1	▨	■	■	■	■	■	■	■	■	■	■	▨	■	■	▨	▨	▨	■	■	■	■	■	■	▨	▨	▨	▨
	SECURITY POLICY											ACCOUNTABILITY			ASSURANCE									DOCUMENTATION			

□ NO ADDITIONAL REQUIREMENTS FOR THIS CLASS

▨ NEW OR ENHANCED REQUIREMENTS FOR THIS CLASS

■ NO REQUIREMENTS FOR THIS CLASS

Figure 5 – Trusted Computer Criteria (Orange Book)

One rainbow document maps Orange Book requirements to system requirements. The Yellow Book[10] establishes trusted computer security requirements for specific applications by identifying the minimum class of system required for a given risk index. The system's risk index is defined as the disparity between the minimum clearance or authorization of system users and the maximum sensitivity of data processed by the system. Therefore, both the Orange Book and the Yellow Book measures must be applied together for any one system.

Concerning trusted computer rules, quoting from the Yellow Book, "They are to be used by system managers in applying the Criteria and thereby in selecting and specifying systems that have sufficient security protection for specific operational environments." However, the Yellow

[10] **Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments, DoD "Yellow Book", CSC-STD-003-85, June 1985.**

Book also recognizes that "While communications and emanations security are important elements of system security, they are outside the scope of the two documents." Therefore, especially in the LAN/WAN environment, two other major security aspects are not covered directly by Rainbow Series documents.

Constantly Evolving Requirements

Even currently specified computer security rules are evolving. Research and development is underway in the industry for providing B3 OTS/COTS (off-the-shelf/commercial off-the-shelf) products that support information transfer between separate networks running at different security levels. Additionally, as newer network products are implemented, it will be necessary to provide automatic, rule-based, information downgrade functions to control access to information over networks at different security levels.

Emission and COMSEC controls have also evolved recently. The National Security Agency released new requirements in 1991 directed at allowing some tailoring of levels depending on equipment location and level of threat. Regarding COMSEC equipment, many varieties of Type 1 and Type 2 equipment are emerging at a fast pace to address a variety of network applications.

Concerning trusted systems, multi-level secure (MLS) Gateway systems have been designed to meet or exceed Class B3 requirements and are currently preparing for or in formal evaluation by the National Computer Security Center (NCSC). What all this means is that as new systems and enhancements become available, users want to immediately incorporate them into new or existing secure networks, hence producing a continuous need to re-think what current and future security rules and requirements might necessitate.

Open Systems Design and the Need for Security

Open systems are often governed by specific applications programming interface standards (APIs). APIs address such topics as Operating Systems commands and utilities, Data Base Access (Structured Query Language or SQL), programming languages, Graphic User Interfaces (X Window System). A significant effort has been made by the industry to define and standardize many of these system aspects, especially when applied to protected systems.

X/Open is an independent open systems organization that is concerned with standards and their adoption. X/Open defines a family of X/Open products that conform to de jure standards, where they exist, and to adopt widely supported de facto standards in other cases. X/Open has a trademark licensing program which identifies products that meet X/Open specification requirements.

A specific example of an X/Open application occurs when it builds on the IEEE Standard Portable Operating System Interface for Computer Environments, Portable Operating System Interface (POSIX) (mandated for use by the Federal Government as Federal Information

Processing Standards FIPS 151-1 in 1988, but with only four systems compliant at this time[11]) which pertains to hardware platforms such as SUN and MacIntosh. POSIX, in simple terms, can be defined as a functional interface between applications and the operating system environment. POSIX is a standard, not an operating system itself. The Sun/OS 4.1 is a standard product that makes available security features patterned after the C2 (Controlled Access Protection) classification. With this product, support is provided for the specific C2 requirements of:

Security Policy	Discretionary access control and object reuse control
	Accountability, Identification, Authentication, and Audit Assurance
System	Architecture, integrity, and security testing
Documentation	Administrator/Users Guide

With trusted requirements such as those listed above available for the system and often easily implemented, there is a growing tendency to overlook many of the other security requirements imposed on the system. A security officer faced with commercial advertising for turn-key operations might at first think that the protection battle was won. However, even the system questions still exist concerning when each requirement should be implemented, how each can be controlled throughout acquisition, and where each should be integrated with other security related requirements over the life cycle of the system.

General SSEM Requirements

The previous discussions provided an overview of the many security related topics that must be dealt with in the network environment. The sheer magnitude of the problem lends itself to a systems engineering approach.

Following good SSEM engineering practice requires an appropriate and timely response in the following key areas; conformance to engineering standards, proper understanding of unique vulnerabilities at each stage of procurement, furnishing of the personnel and materials necessary to perform the security tasks, and finally insuring life cycle security measures are implemented. The following phases of the system procurement are examined during the SSEM effort. A comparison of these phases with the acquisition process for a typical network is shown in Figure 6.

- Planning
- Acquire/Implement
- Evaluation
- Deployment

[11] Cashin, J.,POSIX Points Way Towards Open Systems, Federal Computer Week, 7 October, 1991.

These disciplines and operational areas provide support for the representative scope of SSEM activities as detailed below.

PLANNING		EVALUATION	DEPLOYMENT	INTEGRATION
Concept Exploration		Demonstration & Validation	Full Scale Development	Production
Processing Needs	Feasibility Studies	Preliminary System Design	Installation, ILS, & Mgt	Inter-Network Mgt & Life Cycle Support

Planning

This area involves operational requirements analysis, risk analysis[12], facility design support evaluation, and related access control/intrusion detection requirements for the acquisition and deployment of secure communications services and systems. Since a crucial step in security engineering is the clear and unambiguous definition of specific security needs, this area must receive the appropriate emphasis and attention. The product of these efforts should result in specific acquisition and deployment plans for equipment and facilities.

One item specific to the planning stage is the initial risk assessment of COMPUSEC applications as required by Orange Book/Yellow Book analysis. This is difficult at the system level since these documents are not applicable to many classified systems, only to trusted computers. Using the single function approach is preferable at this stage.

Another area of planning, not even considered in many security documents, is facility design. For the facility, insuring high quality RED/BLACK isolation for a system to be installed within the Limited Exclusion Areas is a major thrust of the initial planning effort. Standards governing the construction and protection of facilities for storing and processing sensitive compartmented information and material are contained in DIAM 50-3[13].

The most cost-effective approach to implementing an emission secure LAN/WAN is to increase the isolation of the overall facility through zoning or attenuation enhancement rather than through the use of fully protected TEMPEST equipment. Since non-developmental (commercial off-the-shelf) items are normally used in within the Sensitive Compartmented Information Facility (SCIF), the best approach is to also follow design guidelines such as those contained in MIL-HDBK 232A[14] and NACSEM 5203[15] for equipment layout and facility design.

The SSEM plans produced during this phase should delineate the criteria and operational environments for specific solutions to defined security needs. These needs may span the range

[12] *Risk analysis includes for some agencies the derivation of security policy requirements for specific applications. This is particularly the case for organizations not currently employing SSEM as a formal requirement.*

[13] *DIAM 50-3, Physical Security Standard for Sensitive Compartmented Information Facilities, Defense Intelligence Agency.*

[14] *MIL-STD 232A, Military Standardization Handbook, RED/BLACK Engineering-Installation Guidelines, DoD, 14 November 1972.*

[15] *(U) NACSEM 5203, Guidelines for Facility Design and RED/BLACK Installation, National Security Agency, 30 June 1982 (C)*

from providing additional network connectivity to existing systems to the provision of new network and/or computing environments. The plans should identify specific security evaluation, implementation, and deployment requirements as needed to complete the delivery order. Planning at this time should also include virus protection.

Acquisition/Implementation

The SSEM activities during this phase tend to focus primarily on the control and acquisition of leading edge/state of the art OTS/COTS solutions for specified needs. In many instances, particular equipment is specified for purchase based on functional capabilities rather than on security concerns, with the intention by the purchaser to "make it work when it gets here or we'll use it anyway". Unfortunately, the use it anyway attitude often creates far reaching problems that must be resolved as part of the SSEM function.

Evaluation

The evaluation of secure communications capabilities and systems is seen as performing robust Quality Assurance exercises based on the defined requirements and evaluation criteria. SSEM is, after all, a quality assurance function. Of particular importance in the implementation and integration of a LAN is the exercise and demonstration of interoperability between components (hardware and software) of the system. The component level operational interoperability evaluated in this area should at a minimum honor identified security constraints.

This area includes the evaluation of TEMPEST equipment as required to conform to the security requirements of the system. Wherever appropriate and justifiable, the acquisition and provision of commercial off-the-shelf TEMPEST equipment can be accomplished. However, only by the prior identification of a TEMPEST problem through a definite vulnerability assessment should TEMPEST equipment be authorized.

Specific Trusted computer security requirements such as the applicable audit requirements and network management for the particular application are tailored at this stage. While it is usually hoped that when the system is actually installed it will immediately work with very little tailoring, this is seldom the case in the real world.

For trusted end-systems which require formal C2[16] and higher ratings, emphasis shall be first made on the acquisition and/or use of those systems which have received formal evaluations from the National Computer Security Center (NCSC), followed by consideration of systems undergoing formal evaluation by the NCSC.

Deployment

The deployment of secure communications and systems solutions includes the aspects of initial (alpha) site installation, field exercising, and eventually full distribution to multiple sites

[16] *Formal C2 ratings are based on meeting full Orange Book requirements. However, many DoD organizations have defined a level called C2 functionality which may be similar to full C2 but requires a less ridged certification process.*

with field support. Of great importance with secure communications and systems at a site is the individual site installation checks and audits. The deployment requirements specified in the Secure Engineering Planning efforts, including specific DIAM 50-3 requirements for cable and plant installations, will guide these audit efforts.

Cable Installation

During the deployment phase, many security requirements may be applicable which relate to minute details. Often, proper cable/plant installation is often the primary security concern. Installation practices must be in accordance with local utility practices and agreements, client agency standards, the National Electric Code and all other applicable Federal, state, city, and county ordinances, statutes, and regulations, including the security specifications. Tables 1 and 2, from MIL-STD 232A provide guidance for proper RED/BLACK cable separation. The following sections delineate other cable installation guidelines.

LAN cable construction is such that relatively minor damage, such as dents and kinks, can have a major impact on not only system performance, but also shield leaks can create security hazards related to reduce shielding effectiveness. Therefore, installers must take every precaution to prevent cable damage, including improper connector termination, during cable installation. In particular, the cable should be left uncut, and fastened securely to its shipping reel until immediately prior to its installation. The use of techniques such as sag, pay-off, reel braking, and clamping prevents kinking or bending the cable beyond its limits.

For broadband LANs, all amplifiers and distribution taps must be installed in accordance with security restrictions and at protected or controlled locations where they are accessible for future connection or maintenance. All equipment and taps should be permanently mounted to building structures or attached to a supporting messenger strand to allow access to unused tap ports or normal maintenance operations with amplifiers without damaging the distribution or trunk cables.

For twisted pair LANs, wiring closets are sometimes used. In these instances, wiring must be installed neatly, in an isolated and secure structure, with proper labels attached. All active components and patch panels (RED or BLACK) will be rack-mounted. All backboards, punch blocks, and cross-connects will adhere to both security standards[17] and to telecommunication standards for color coding, layout, and numbering.

Fiber optic cabling does not provide an emission or ground loop problem in secure installations. However, care must be taken to insure regular physical inspections to safeguard against taps. In addition, the cable should be attached to a connector and spliced by certified technicians using the tools and materials recommended by the cable vendor. Both fusion and mechanical splicing are acceptable. Both secure and non-secure fiber optic networks should be built to American National Standards Institute (ANSI) Physical Media Description (PMD).

[17] *such as DIAM 50-3, NACSEM 5203, and MIL-STD 232.*

LAN/WAN Integration Engineering

Typical integration engineering for secure networks involves tying all the pieces into a cohesive operational system and then performing a multitude of functional checks. Therefore, integration is very specific for system and equipment type. The best way to describe specific integration efforts is by example. The following examples indicate the scope of typical secure network integration efforts:

- Integration of Sun and SunSPARC workstations into a single secure network with recommendations for hardware configurations and file server performance. This should include the description of the equipment used and its performance rating (including TEMPEST rating if applicable depending on physical location).
- Integration of Novell networks with recommendations for further integration into networks containing higher classification of information.
- Integration of 3COM networks with recommendations for possible further integration of networks containing higher classification of information using FDDI, SEGNET (proprietary), or Ultra-Net Interfaces. If the connection requires access to a remote LAN using a WAN circuit, interconnection designs that use ISDN or SONET with COMSEC interfaces may be necessary.
- Apply security requirements as they relate to physical access, file access, log-in IDs, passwords, and virus protection. For all file storage areas determine the level of access each user will have (none, read only, read/write) and grant file access accordingly; if appropriate options have been installed, limit user access by time and location; restrict or grant user access to all network features. Establish password length and duration requirements.
- Establish server log. Based on routine maintenance activities and other reporting requirements of the client agency, establish server maintenance log.
- After user accounts are established, connectivity and functionality tests will be performed. For each workstation location, connectivity will be checked by establishing that log-in to the network can be achieved from that workstation location. Functionality testing will be done by logging in as the user from the workstation location and testing each menu option.

Typical C2 Network Program

As an example of an often encountered requirement, the following description is typical of a secure tactical system operating as a C2 network. In this particular C2 network, a system was required on which one operator could not gain access to the work of another operator without specific permission of the system administrator.

As an overall protective measure, due to common requirements for connectivity to multiple classified systems, and other unique security considerations (such as emission security) which could be imposed at a particular site, only fiber optic cable is recommended for the design, including running fiber to each workstation or personal computer.

The first step in the LAN design phase is the Preliminary Site Survey, during which engineers (including SSEM engineers) perform an on-site physical inspection of the facility to obtain Government Furnished Information (GFI) (e.g., site maps depicting existing cable plant(s), floor plans, utilities, etc.), inspect buildings, existing conduit systems, manholes or other possible access points, determine power availability, conduct building radiated attenuation testing, and obtain other data which will impact on the LAN design or security.

It is important to also conduct interviews with critical facility personnel to clarify their data requirements. This preliminary survey generally takes about five days with 20 or more in-depth interviews conducted. Based on the information obtained, the system designer, in consultation with SSEM personnel, prepares an information flow analysis to determine the LAN functional and operational requirements for the facility. In some instances, extensive suites of both PC and Host based application software, ranging from only a handful to multiple applications per workstation, might be required.

Following completion of the preliminary survey and the resulting analysis, usually between 90 and 120 days, engineers will return to the site to conduct a Final Design Review. The purpose of this review is to assure that the information on which the requirements analysis and the designs are based is both accurate and current.

Detailed design drawings, including site plans with proposed cable paths; floor plans depicting proposed equipment locations, and logical connectivity diagrams are generated and submitted. These plans and drawings are often classified when the extent of secure processing capabilities or their potential weaknesses are indicated.

Typical C2 LAN Installation Activities

Installation technicians, under the guidance of design and SSEM engineers, perform the turn-key installation of all LAN hardware, software, and cabling. All installed fiber is tested for attenuation and distortion products according to a formal Test Plan. Fiber optic repeaters, hubs, and transceivers are connected to the fiber and tested using network analyzers to generate and monitor sample traffic.

Ethernet adapters are next installed in their TEMPEST certified workstations and tested for compliance with security regulations as well as interrupt, direct access memory (DMA), and I/O addressing conflicts with other boards.   File servers, communication servers, bridges, routers, and Network Control Server (NCS) are also installed and tested using manufacturers' diagnostic software utilities at this time.

All network operating systems, management utilities and application software are next loaded, initialized and tested. Workstation-to-host communications as well as workstation-to-file server links are established and exercised to test functionality and interoperability. Shared network printers are next connected and tested with a variety of application software to ensure compatibility. Network security services, including controlled access, traffic segmentation, and data encryption, are next implemented and extensively tested.

Software installation often requires expertise with several operating systems, primarily: 1) DOS for workstations; 2) OS/2 (new IBM operating system) for file servers; and 3) UNIX for the Network Control System (NCS). Initializing the protected software configuration parameters includes building IP addressing tables and defining customized filtering algorithms for the bridges and routers in order to implement traffic segmentation for security purposes. For file servers, setup includes establishing user accounts, log-in scripts, naming conventions, directory structures, and access privileges as well as initializing network services and loading and testing application software.

In accordance with plans developed during the initial evaluation phase, initializing a NCS requires establishing bootstrap services for network components, building port configuration files for communication servers to enable host access, defining a logical name service, configuring network management utilities for monitoring network traffic and generating statistics, defining network utilization alarm thresholds, establishing a real-time time and date service, and starting an audit trail service for reporting such information as connections/disconnections and bootstrap initiations.

Normally communications equipment is rack-mounted with critical components protected from power fluctuations by Uninterruptible Power Supplies (UPS). Network adapters are normally installed in TEMPEST certified workstations for compliance with security regulations. Extensive acceptance testing is necessary on the final system to ensure that all requirements are met.

Training courses which address the specific requirements of the LAN installation and operation are normally required[18] for most secure networks. Courses may consist of several hours of intensive instruction, and are designed for network administrators, security managers, and LAN technicians, with a heavy emphasis on security management. Topics of instruction include system installation and setup in a live environment, basic networking concepts, planning the network, establishing standards, adding users, managing resources, installing application software, installing menus for users, groups and/or organizations, monitoring network activity, routine maintenance, diagnostic activities, and network security management. Specialized training is also required to ensure proper certified management and segmentation of multi-level secure traffic across these networks, plus training in the maintenance of TEMPEST type equipment is sometimes provided.

[18] ***Most agency and organization implementation instructions, such as SECNAVINST 5239.2, require annual security and awareness training for computer users. In addition, the Computer Security Act of 1987 contains program requirements for training.***

SSEM is also concerned with life cycle and integrated logistics support. A major problem in secure installations over time is the breakdown in shielding isolation for secure node protection. Secure nodes are racks of non-TEMPEST equipment that obtain their radiated emission protection using an overall shielded chassis. After repeated maintenance and internal re-work, the back doors on these racks are often removed, violating the TEMPEST integrity of the system. Therefore, continuing work on a typical secure network includes systems software support, data communications design and integration, knowledge based systems support, network security evaluation and testing, TEMPEST field testing, systems administration, computer room reconfiguration, and regular visual inspections to insure the secure node is maintained.

The OTS/COTS B3 Example

The OTS/COTS B3 level designed Trusted Computing Base (TCB) gateway systems/subsystems have been advertised as available with "turn-key" security that provides the following features:

- Most agency and organization implementation instructions, such as SECNAVINST 5239.2, require annual security and awareness training for computer users. In addition, the Computer Security Act of 1987 contains program requirements for training.
- Commodity UNIX System V.3-like interfaces for applications support; Complete mediation of accesses between programs and data; Isolation of security-relevant components of the system; Secure communications support for Transmission Control Protocol/INTERNET Protocol (TCP/IP) and OSI (TP4/IP and X.400); Validation that security mechanisms are operational and enforced.

These features are commendable as far as they go. With such features available, an acquisition manager might purchase the system thinking very few additional security measures are necessary. Without regard to the other security related issues that could be applicable, or even without a proper risk assessment, the potential exists for tremendous additional implementation costs before network users can operate securely. However, an active SSEM program in place would insure these other needs and requirements would not be overlooked in planning for and implementing this system. Additional requirements that could be applied to this example might include:

- Network control security training;
- Virus protection;
- Facility/Equipment emission security;
- Facility access security;
- Protected facility power;
- COMSEC interface requirements to the outside world;
- Secure installation (including separation) provisions;
  Upgrade provisions;

- Long term emission protection;
- Maintenance provisions.

Conclusion

The advancement of network design and the increased sensitivity of classified processing within a network has brought with it "layers" of ever more complicated security requirements. To effectively manage this multi-faceted problem has imposed ever more demanding requirements onto the shoulders of the SSEM engineer. It has also facilitated his integration into other related areas of engineering, including network management.

This chapter has discussed a few examples of the many possible configurations associated with networks processing data in a secure environment. As was shown, security issues involve virtually all aspects of operation from the software operating in the system to the details on how interconnect wiring is performed. Clearly, "turn-key" type basic network acquisitions will not fully address security issues at all potential application levels. Therefore, to implement a control measure covering all security issues as they evolve in the network environment, SSEM offers a workable solution. SSEM has proven itself on many programs to be an effective systems approach to dealing with integrated security.