USING EMBEDDED COMSEC: AN INTEGRATOR'S VIEWPOINT

THOMAS KIBALO, SENIOR DESIGN ENGINEER
W. E. BOEBERT, CHIEF SCIENTIST,
HONEYWELL SECURE COMPUTING TECHNOLOGY CENTER

1. INTRODUCTION

In order to expand COMSEC equipment availability, standardized usage, and lower COMSEC equipment cost, NSA established the Development Center for Embedded COMSEC Products (DCECP). The output of the DCECP, under a program entitled Project Overtake, is a standard set definition of COMSEC modules to be used in embedded applications to provide the encryption/decryption functional requirements in link, data, and voice COMSEC systems. These modules are called Forsee, Tepache and Winstor respectively.

This paper describes the use of the standard module set in a generic Command Control and Intelligence System and addresses the issues of embedding these modules from a system integrator's viewpoint at both the system and unit host levels.

2. PROJECT OVERTAKE AND THE HOST INTEGRATOR

2.1 Historical Background. Historically, endorsed cryptographic technology has been available only from NSA, generally in the form of limited-function, classified products with a strong functional bias toward the securing of passive communications links. This situation, combined with the ever closer integration of computers and communications, has caused many difficulties for groups attempting to incorporate cryptographic technology into host systems. Free-standing cryptographic units have been difficult to integrate, both physically and functionally, into modern computerized hosts. The classified nature of the products has often imposed physical security constraints which are incompatible with operational needs. The "communications-only" bias of the products has inhibited cryptographic solutions to computer security problems, such as the authentication of critical but forgeable user/-computer dialogues and the securing of classified information on removable media. Finally, the available methods of key management were often inconsistent with the volume, frequency, and nature of computerized communications.

2.2 Project OVERTAKE. The technical and managerial approaches used by Project OVERTAKE accommodate the near-total integration of computers and communications in contemporary systems by providing endorsed cryptographic technology in a radically different form: unclassified modules built to standardized interfaces by a broad supplier base and designed to be embedded within, as opposed to added onto, products and systems.

A radical change in a technology delivery mechanism inevitably involves a radical change in the relationships between the various organizations which must incorporate that technology into systems. In this paper we shall describe the new form of one such relationship: that between the provider of cryptographic technology and the host integrator. There are two significant areas of interest: what Project OVERTAKE delivers to the integrator, and what the responsibilities of the integrator are.

2.3 What the Integrator Receives. The integrator may obtain standardized, unclassified modules from any of a number of suppliers, along with support in the form of documentation and consultation. The documentation consists of an Interface Control Document (ICD) and an Embedding Manual, along with an informal list of "Do's and Dont's." The ICD defines standard external interfaces which will be enforced for all implementations of the modules; the integrator can therefore use it to define "sockets" in future systems with the assurance that technology changes in the modules will not force systems redesign. Consultation and technical assistance is available both from NSA and the supplier selected by the integrator. In addition, NSA will provide an evaluation of the host system which will, if successful, lead to an endorsement of that system as authorized to handle classified or sensitive information.

2.4 What the Integrator Must Provide. In the contractual domain, the integrator must negotiate Memoranda of Understanding and Agreement with NSA. These memoranda spell out various administrative responsibilities of the integrator; principal among these is the proper

handling of classified and Cryptographic Controlled information. The integrator must also provide technical and administrative support to the evaluation process.

In the technical domain, the integrator must satisfy the special physical and functional requirements of endorsed cryptographic technology. Functional requirements arise at two levels: system and host. System-level requirements and issues are those that deal with the selection of modules and their placement in a system architecture. Host-level requirements are those associated with the detailed placement of a module in a product, such as terminal or mainframe, and its relationship to that host.

3. EMBEDDING MODULES

3.1 Physical Module Requirements. The module is embedded within target host application equipments, and of itself, supplies only core cryptographic functions. The host equipment containing the module must supply all power sources and regulation, TEMPEST shielding and filtering, and tamper detection sensors to supplement module secure operation. This approach reduces duplication of hardware in both the host and module, and results in a more generic module design suitable for embeddment in a large variety of hosts. The host must also provide a CSESD-11 fill port to the module as a means of manually loading key. As an option, the host may also supply a crypto ignition interface to the module for more convenient operational startup.

Module integration is eased by the use of standardized interfaces. All defined interfaces must be LS-TTL compatible.

3.2 System-Level Functional Requirements. Figure 3.2a describes a hypothetical system-level architecture which incorporates a representative set of hosts and inter-host links. Hosts are assumed to reside in disjoint physical security areas connected by insecure media. The vulnerabilities in such an architecture are as follows (number in parentheses are keyed to the diagram):
The untrusted front-end processor to the Trusted Computer Base could be subverted, permitting a variety of spoofing attacks (1). Active and passive wiretap attacks could be mounted against the Local Area Network (LAN) (2), the high-speed link (3), and the low-speed link (4). Media removed from the workstation could be forged or compromised while in an insecure area (5).

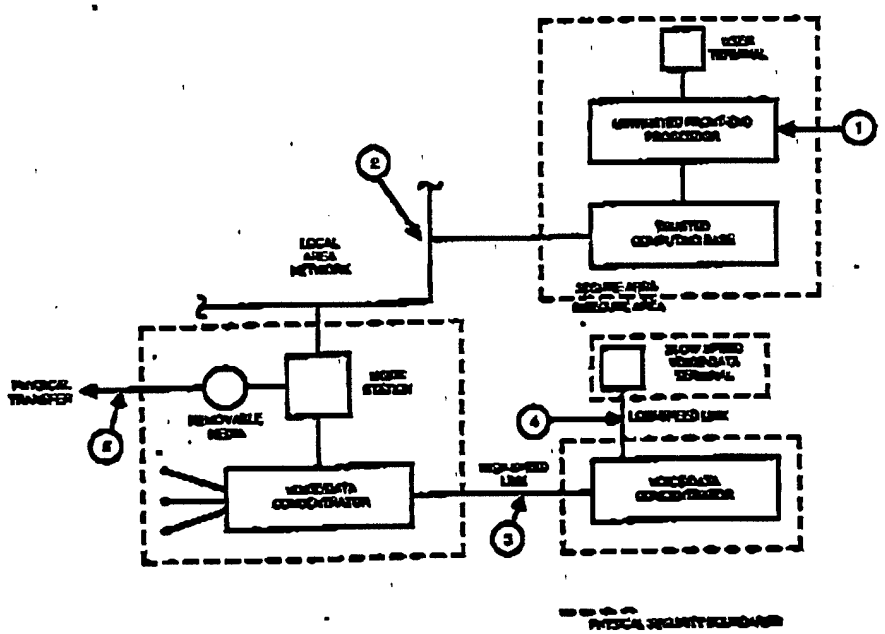


FIGURE 3.2a

When it is not practical to overcome such vulnerabilities by physical security means (e.g., by hardening communications lines or expanding the physical security perimeter), then the standard cryptographic modules may be used. The selection of a particular module is guided by considerations of speed and functionality (e.g., provision for bypass). A representative set of choices is given below (keyed to the numerals in Figure 3.2b):

Tepache modules are embedded in the TCB and the user terminal in order to authenticate critical TCB/user interchanges (1). A Tepache module in the workstation and the same module in the TCB are used to encrypt LAN traffic (2). Two Foresee modules are used to protect traffic on the high-speed link (3) and two Windstor modules are used to secure the low-speed link (4). A second Tepache module in the workstation is used to encrypt the removable media (5).

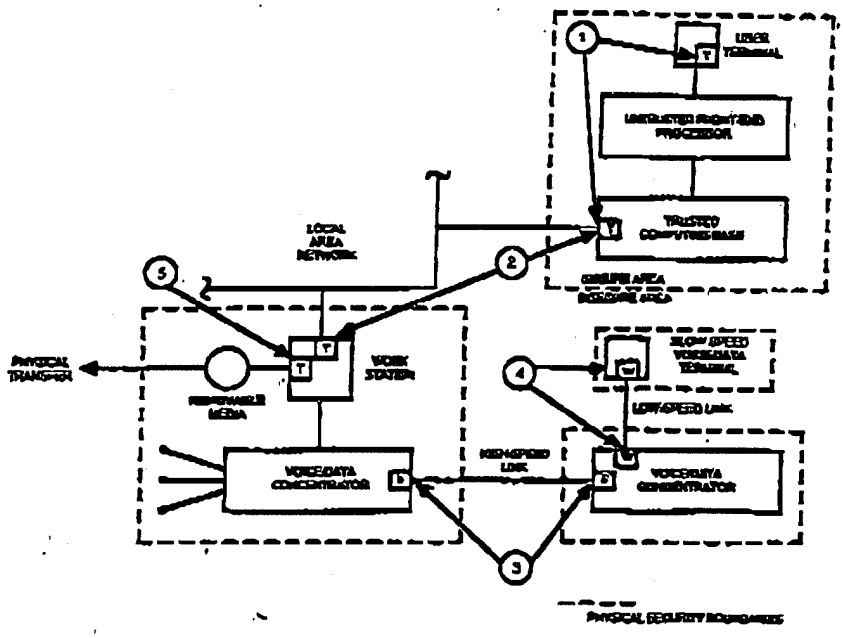


FIGURE 3.2b

Two Tepache modules are required in the workstation since there are two interfaces to insecure media. A single module suffices for the TCB because there is only one such interface, and the multifunction nature of the module permits its dual use as and encryptor/decryptor and an authenticator. Authentication is used instead of encryption in the user/TCB link because the transmission takes place entirely within the physical security perimeter; forging, not compromise, is the threat. Message contents must be in the clear to permit efficient processing.

The second major system-level issue is that of key management. The integrator must decide how keys are to be distributed (in-band or through fill devices) and how to integrate key management with the various communications and storage media protocols in the system. Project OVERTAKE will provide technical support to the integrator as well as key management modules; one such module is shown as part of the TCB in Figure 3.2. Encryption of information stored on fixed and removable media may raise applications-dependent issues, such as the impact of key changes upon archival storage. Integrators should anticipate that resolution of these and other key management issues will require access to classified information.

A final issue is that of interoperability. Different modules are inter-operable with different existing cryptographic products such as the KG-84, KY-57, and KGV-8/11; existing or forecasted interoperability requirements may dominate the selection criteria.

3.3 Host Level Functional Requirements. This section will discuss the requirements imposed upon the module integrator at the host domain level.

3.3.1 Red/Black Separation. The module interface is generic in structure and thus supports multiple inserts within a target host. For secure operation the module must be positioned on the logical boundary between red and black processing. The integrator can ensure this by placing the module directly "inline" with the red to black data flow from the host. The integration must enforce the module "ownership" of the path in such a way that no logical compromises can be made. For example, see the Tepache module (Figure 3.3.1a). A proper positioning for its placement is between the host and the outgoing communications circuits. This ensures that the traffic on the I/O side of the module is black and on the host side is red. If there are multiple outgoing data paths from the host, then it is the integrator's responsibility to identify those paths and to ensure that modules are used in all instances.

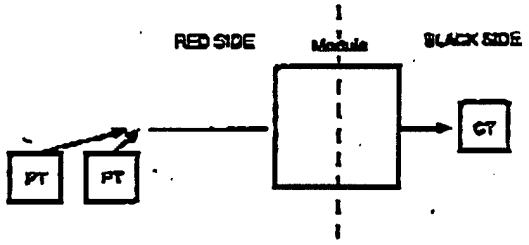


FIGURE 3.3.1a INLINE MODULE PLACEMENT

In contrast to this, consider the installation shown in Figure 3.3.1b. The integrator has chosen a module placement not inline with a terminal red to black boundary. Clearly an "open port" or sneak path exists where red data can be outputted.

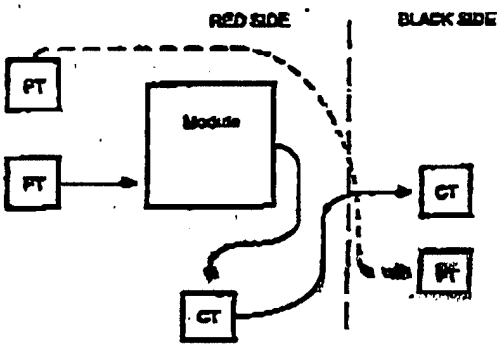
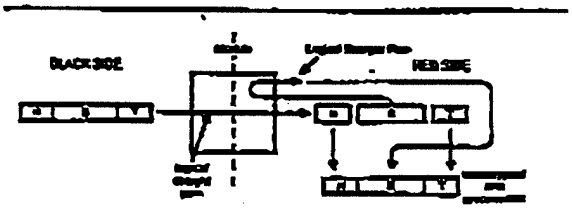
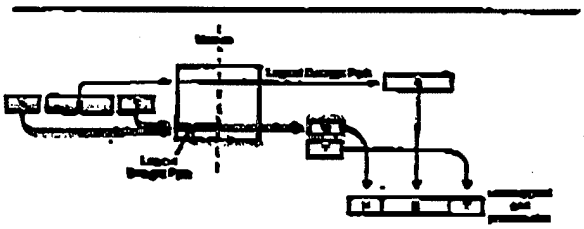


FIGURE 3.3.1b NOT INLINE MODULE PLACEMENT

3.3.2 Message Formatting and Reformatting. In the classic system environment of cryptology, most systems operating in a system high state (secure) do not gracefully degrade to a clear state without a break or total disruption of the communications. This burden may be acceptable for point to point communication systems but becomes intolerable for packet-switched systems or LANS where multipoint connections are common. The modules (in particular the Tepache) need to support multipoint networks. To support this a basic packet format for the module is proposed (see Figure 3.3.2a). The whole packet can be envisioned as encrypted but in the more general case only the body is encrypted, while the header and trailer remain unencrypted. There is good reason for this. In most modern day multipoint networks the trailer data supports error detection and correction. To allow encryption to work in these systems (in a transparent way at the data link level) an unencrypted trailer is a necessity. The same argument can be applied toward the use of an unencrypted header. The header is used by most systems to identify message type, source and destination. For a more rigorous application where traffic flow analysis can lead to some form of compromise then use of unencrypted headers is dangerous.





When unencrypted headers or trailers are used in an application, other considerations must be taken into account. The considerations are illustrated in two cases, both of which are presented from the aspect of decryption (the same rationale can be applied from the viewpoint of encryption as well).

For all cases the module is assumed to be placed along a terminal red/-black boundary in the host. For case one, on the black side it is assumed that there is no "smart" support for message disassembly (i.e., which part of the message should go through a decryption process and which should not). In this case (see Figure 3.3.2b) the entire message packet has to be passed through the module to the host without processing. Once received by the host, the message can then be disassembled into its encrypted and unencrypted parts. The encrypted parts are then fed back through the module from the host side for decryption and then assembled into a fully decrypted message.

An advantage to this approach is that the I/O used in such a host can be fairly unsophisticated (i.e., UART or parallel port). A distinct disadvantage with this process is additional time delay incurred through a second pass of data to the module.

In case two (see Figure 3.3.2c), the assumption is that the I/O is sophisticated enough so that additional functions of assembly and disassembly can be imposed upon it (thereby offloading the host). The I/O buffers the black message and disassembles it into encrypted and unencrypted parts. It then transfers the unencrypted part through the module to the host; the encrypted part is also passed through, but decrypted "on the fly." The end result on the host side is that only unencrypted messages are seen. This example is typical of the approach required for LAN's where a complicated I/O is the norm.

3.3.3 Bypass. Encryption is a symmetric process to the decryption, with the exception that unencrypted portions (i.e., header, trailer) must pass over the red/black boundary, thereby posing a potential security problem.

In the Tepache module, bypass is an internal function limited and audited to prevent abuse.

In the Foresee and Windstor, bypass is an external function (not serviced by the modules).

It is the responsibility of the integrator to control all bypass functions so as not to cause major insecurities to a system using Foresee or Windstor, and to prevent alarm lockup situation in the Tepache.

3.3.4 Cryprographic Modes. Each module type supports several cryptographic modes. These modes allow for use of cryptology under a number of different system situations and provide backward compatibility to a number of existing crypto equipments.

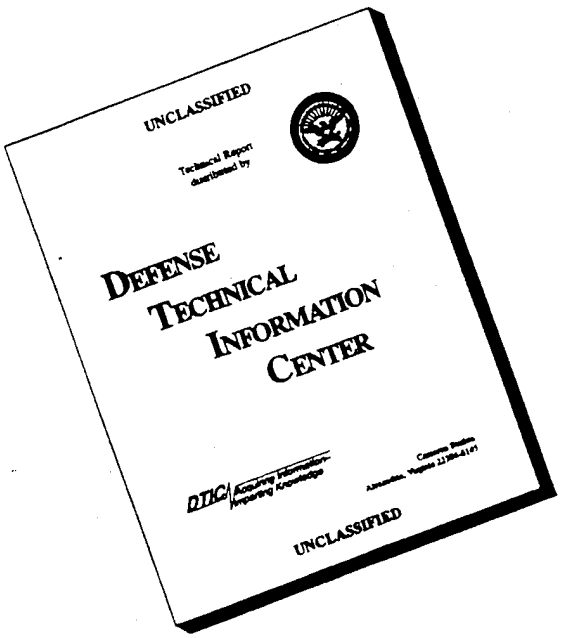
It is primarily a host responsibility to enforce proper use of module cryptographic modes. The system designer must identify that subset of modes applicable to the system and then pass this information on to the host integrators for proper mode use at host level.

The exact place where crypto sync is detected varies among the module types. In modules like Foresee and Windstor, the loss of sync is detected within the module. In the Tepache the loss of sync must be detected by the host. In all cases once a loss of sync has occurred, it is a host action to correct.

4. SUMMARY

Project OVERTAKE offers significant benefits to the host systems integrator. The multifunction, dynamically reconfigurable nature of the modules permits the incorporation of endorsed cryptography in a wide range of functional environments. The unclassified nature of the module permits the use of endorsed cryptography in previously forbidden physical environments, as well as reducing the integrator's costs and schedule. Module cost is further reduced and availability enhanced by the broad supplier base. Interoperability permits interconnection with, and the orderly upgrade of, systems which use current cryptographic products. Above all, the enforcement of standard interfaces to the modules will facilitate long-term technical planning, reduce technical risk, and permit systems to easily incorporate module-level improvements in technology.

DISCLAIMER NOTICE



THIS DOCUMENT IS BEST QUALITY AVAILABLE. THE COPY FURNISHED TO DTIC CONTAINED A SIGNIFICANT NUMBER OF PAGES WHICH DO NOT REPRODUCE LEGIBLY.