A METHODOLOGY FOR EVALUATING THE RELATIVE SECURITY OF COMMERCIAL COMSEC DEVICES

By: Albert L. Lang, Jr.*
AMERICAN SATELLITE COMPANY

and

Dr. Janet Vasak*
SCIENCE APPLICATION, INC.

May 20, 1982

*This work was performed by the co-authors when they were employed by Booz Allen & Hamilton, Inc.

A METHODOLOGY FOR EVALUATING THE RELATIVE SECURITY OF COMMERCIAL COMSEC DEVICES

The selection of a device to provide communications security (COMSEC) in a commercial environment is dependent on a number of criteria, one of which is security. From the several hundred commercially available equipments, it is straightforward to eliminate those which clearly do not meet current needs; e.g., a teletype encryption device when voice privacy equipment is needed. Once the candidate devices have been identified, in-house expertise is generally available to evaluate the engineering aspects like system integration, operation, reliability, etc., and the cost and delivery schedule constraints. In contrast, few companies are able to evaluate for themselves the security offered by a given device. There are few obvious sources of expertise. The open literature is very sparse in providing potential techniques. Manufacturers tend to present their products in the most favorable light. Among the ranks of unbiased analysts, possible sources are professors, researchers, and consultants. The selection of a knowledgeable and experienced analyst can be, in itself, a critical task.

The purpose of this paper is to describe a methodology for quantitatively ranking the security of commercially available COMSEC devices. The principal characteristics of this methodology are these:

- o the evaluation of comparable devices
- o the emphasis on security only
- o the relative ranking as a function of the time required to recover the message.

What makes this methodology worth considering is that it does not require a subjective assignment of weights to different security aspects. By focusing on the threat environment and on the opponents' constraints with respect to money, time, equipment, and analytic skills, a uniform application of the methodology to each candidate device is assured.

There are four steps in the process to quantitatively rank the security afforded by the candidate devices:

- o security description
- o assumptions and weakest element
- o attack algorithm
- o message recovery time

These steps enable the analyst to determine how the device works, the conditions under which the device will be compromised, what aspect of the device to attack, what kinds of attacks to formulate, and how to measure the success of the attack.

Of the four steps, the security description is the most important. The source of information on how a specific device operates will be the device's manufacturer, whose best interests are served by keeping this information secret. However, for a major sale, it is sometimes possible to obtain a great deal of information, provided the right kinds of questions are asked. The three main areas to which questions should be directed are the use of the code variables, the operation of the key generator, and the enciphering technique governed by the key stream.

The code variables are a sequence of symbols which make the output of the equipment readily intelligible only to those who possess both the same encryption device and the same code variables. The physical characteristics of the code variables are generally easy to obtain from the manufacturer's literature. The number, kind, format, and ease of changing are specifics to be determined. For example, if a code variable change is very difficult to effect, it becomes likely that a user will tend to keep the same variable operational for long periods of time, thus affording an opponent a greater opportunity to compromise the system. A second important piece of information about code variables is how they are used by the key generator. Are all bits used? Are any biases evident? How much will the change of one bit affect the key stream?

The key generator is critical to the security of any encryption equipment. Information about the key generator may be learned by asking about the initialization and synchronization. How does the key generator physically operate (e.g., the stepping of the registers, etc.)? What specific mathematical function is implemented by the key generator? This last question is almost never answered directly, but occasionally can be deduced from wiring diagrams or by disassembling the device.

The last area to investigate is the enciphering technique; i.e., how the device uses the key stream to encrypt the information. Digital encryption devices often use modulo two

addition of the key stream and the digitized data. Analog devices use the key stream to govern permutations or rearrangements of the signal.

Once a good security description has been developed, consideration must be directed to the threat assumptions against which the proposed device is to be used. These assumptions must be constant for the entire set of devices being evaluated. Typical assumptions are that any hard-wired elements in the device and short standard messages, sentences, or phrases in plaintext-ciphertext pairs are known by the opposition. In addition, assessments of the resources to be directed against the device should be made. The time, money, human resources, and equipment to be applied to compromise the device should be estimated.

Given these assumptions and the security description of the device, the selection of the weakest element (from the code variables, the key generator, and the enciphering technique) is next made. This choice will be partly subjective, depending on the strength of those doing the analysis. The reason for making the selection of the weakest element is to focus the effort to compromise the device on one area. Since a device is no more secure than its weakest element, a complete cryptographic assessment of the device is not necessary. Instead, the most vulnerable aspect of the device is exploited.

The third step, development of the weakest element attack algorithm, is dependent on the skills of the analysts. Typical attacks against code variables look for biases or dependencies

in the bits. In all cases, an exhaustive search is possible. To compromise the key generator, functional characteristics such as linearity, symmetry, or periodicity, are exploited. The enciphering technique is attacked by recovering the scrambling parameters or an adequate approximation of them.

The actual quantitative ranking is determined by using the time required to run the attack algorithm to compute the message recovery time. An assumption about a typical standard message length is made and all measurements are standardized to this norm.

The standard message is encrypted and a computer simulation of the attack algorithm is written. By estimating the number of computer operations required to execute the simulation, the standard message recovery time can be computed. This time becomes the ranking criterion, with the larger the recovery time, the larger the degree of security afforded.

* * *

The methodology just presented provides an approach to a quantitative ranking of security. Its limitations are a function of the analysts' skill, the available time, the accuracy of assumptions, and the completeness of information on the candidate devices. Despite these qualifications, it is a valuable tool to assist in the selection of a commercially available COMSEC device.