A major purpose of the Technical Information Center is to provide the broadest dissemination possible of information contained in DOE's Research and Development Reports to business, industry, the academic community, and federal, state and local governments.

Although portions of this report are not reproducible, it is being made available in microfiche to facilitate the availability of those parts of the document which are legible.
TITLE: SECURE TRANSMISSION OF SHIPPER/RECEIVER CONFIRMATORY MEASUREMENTS

AUTHOR(S): R. M. Tisinger and T. Brumfield

SUBMITTED TO: 29th Annual Meeting of the Institute of Nuclear Materials Management, Las Vegas, June 26-29, 1988

DISCLAIMER

The report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. The United States Government reserves the right to use, reproduce, or disclose this information or any derivative works thereof, or to authorize others to do so for United States Government purposes.

The authors and individuals expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

By acceptance of this article, the publisher recognizes that the U.S. Government retains a nonexclusive, royalty-free license to publish or reproduce the published form of this contribution or to allow others to do so, for U.S. Government purposes.

The Los Alamos National Laboratory requests that the publisher identify this article as work performed under the auspices of the U.S. Department of Energy.
SECURE TRANSMISSION OF SHIPPER/RECEIVER CONFIRMATORY MEASUREMENTS

R. Tisinger
Los Alamos National Laboratory
Los Alamos, NM 87545

T. Brumfield
Y-12 Plant, Martin Marietta Energy Systems, Inc.
Oak Ridge, TN 37831

ABSTRACT

Shipper/receiver confirmatory measurements will be performed at Y-12 using equipment designed by Y-12 and the Safeguards Assay Group at Los Alamos. Equipment consists of three stationary NaI(Tl) gamma-ray counter arrays and a Digital Equipment Corporation Micro-11 processor for processing data. In the case of outgoing shipments, the counter data will be incorporated in a shipping file with other necessary documentation and transmitted to the intended recipient. In the case of incoming shipments, this station will receive a similar file from the sending organization. Protection of all data at the S/R/O level is required.

Transmission of the data files can be made point-to-point over telephone lines with proper encryption. Two commercial devices used in conjunction with a personal computer are being evaluated to provide secure communication endorsed by the National Security Agency (NSA). One device is the Gillaroo from P. E. Systems, Inc., and the other is the STU-III, which is available from several vendors. The Gillaroo is available as a PC board or a standalone unit, whereas the STU-III is a Secure Telephone Unit with an RS-232 port for connection to a computer. In both cases, file encryption is performed in hardware using keys supplied by NSA.

The prime advantage of this approach is simplicity. Aside from key management, the whole operation can be automatically controlled by command files on the computer without involving additional interfaces with secure networks or mail systems. Additional benefits are rapid response, immediate confirmation of receipt of message, a communication channel independent of the shipment itself, and low cost.

INTRODUCTION

Shipments of special nuclear material (SNM) are frequently sent between the Y-12 plant and various other sites within the nuclear weapons complex. It is of great concern to know that the amount of SNM received in any given shipment was actually the same amount that was initially shipped. Among the ways to be fairly certain are to make mass determinations and isotopic analyses or to make high-accuracy, direct measurements by nondestructive assay (NDA), but these take appreciable time. It is imperative that a scheme be devised to make rapid, though less accurate measurements that give timely assurance that no diversion of material has occurred. Timeliness is the driving imperative. It is this problem that was attacked by Y-12 and Los Alamos with the following solution.

Shipper/receiver confirmatory measurement apparatus was designed to provide rapid measurement of SNM as it is received in the shipping containers and to provide immediate results. Incoming shipping containers will be received at the loading dock and placed on a conveyor. They will be carried through the counting station, counted, and then sent to the vault. NDA measurements will be made on three stationary counter arrays and the data processed on a Digital Equipment Corporation Micro-11 computer. The results of these measurements will be immediately compared with the corresponding measurements made by the sender on equipment of identical design. Outgoing shipments will be handled in a similar manner.

Details of the counting apparatus and procedure are given in Ref. 1. The question being addressed in this paper is how to transmit the measurement results to the intended recipient (or receive incoming measurement results) with an appropriate level of security.

TRANSMISSION OPTIONS

Various means have been devised to transmit classified information from one location to another. As technology advances, new methods are added to the toolbox. Old methods usually decline in use but continue to be used where appropriate. With electronic communication advancing so rapidly, it is time to reexamine the issues and reevaluate the options now available for this new application.
Inclusion with Shipment
A floppy disk could be sent with the SMN shipment, but this would lose the advantage of advance notice and the security of separate transmission, would be vulnerable to magnetic fields, and would admit to possible tampering of the data if it is in plaintext.

Classified Mail
The classified mail channel would allow the sending of a floppy disk with plaintext information between two points. The advantages are ease of implementation and low cost. The disadvantages are primarily operational inefficiency and loss of timeliness.

Secure Network
Existing secure networks such as SABNET and WBON have the advantage of providing accurate and secure transmission between nodes with minimal security responsibility on the part of the user. The chief problem is getting information from the instrument area to the node and from the node at the receiving end to the recipient. This could possibly be achieved using secure local networks, but the number of interfaces increases with an accompanying increased complexity.

High-Speed Cryptographic Link
Dedicated point-to-point equipment has the big advantage of independence. The total system can be automated with external dependence on only the commercial telephone system, which is highly reliable. An example of such a system is one that connects the Report Library at the Los Alamos National Laboratory with the corresponding library at Oak Ridge. The traffic rate is moderately high and the price is also moderately high at $7200 per node.

Secure Telephone Unit
The Secure Telephone Unit (STU-III) is now replacing the STU-II as a secure telephone link. This new standard product, now available from a number of vendors, is beginning to proliferate at Los Alamos. It provides a voice link with secure encryption that meets NSA requirements. It also has a modular jack to accommodate computer input directly without using an acoustic coupler. In this application a PC could prepare the file and send it through an RS-449 link to the STU-III, which would then encrypt the file and transmit it over the commercial telephone lines. The GSA cost of the STU-III is about $2700.

Gillaroo
P. E. Systems, Inc. makes a plug-in card for the IBM-PC called the Gillaroo that does hardware encryption to NSA standards at the S/RO level. This would allow one to complete the process under program control of DOE on the IBM-PC. The complete package includes software as well as the PC add-in board, which provides for integrated secure communication. The GSA cost of this package is $1195 with 45-day delivery.

SYSTEM CONFIGURATION
The prime considerations in designing the communications for the system are completeness, accuracy, security, and ease of operation. The files transmitted should contain all the information currently carried in a shipper's manifest, with expansibility. Accuracy of the data is mandatory. This requires a minimum of manually entered data and proper error checking throughout. Because the data are classified S/RO, the communication must comply with DOE Orders, which require proper encryption of the data if transmission is by common carrier. Ease of operation requires minimal human involvement in the actual transmission and a minimal number of interfaces between components for reliability.

Each record in the data file will be a complete description for one item counted, which is a single item in the shipment. The maximum size of the file to be transmitted will be about 30 KB, including header information. This header information will include all the other information normally found on a shipping document.

Assuming that operational simplicity and rapid response have a high priority, the latter two options outlined above seem to offer the best solutions. The STU-III costs more than twice as much as the Gillaroo and may require a bit more operator action, but it would also offer the advantage of a secure voice channel as well as a data channel if that is desirable. The Gillaroo is less costly and would be completely under program control of the PC. There may also be slight operational differences in key management procedures. In light of this finding it was decided to proceed with a test of the Gillaroo.

The Technical Engineering Support Group at Los Alamos is also interested in the Gillaroo for a different project and purchased several sets for evaluation. Preliminary results have been obtained and specifications seem to be met. They have been used on two PCs in the same room connected with a null modem and seem to transfer files satisfactorily. The next step is to actually operate them over commercial telephone lines using modems.

SECURITY
Both the Gillaroo and the KOI-18/TSEC tape reader are controlled cryptographic items, though the Gillaroo is not classified unless a key is installed. This means that tight security is not necessary when unkeyed and unattended. Key management is the primary maintenance procedure. It involves setting up a standard procurement procedure for periodically ordering the keying materials from the NSA. Upon receipt, these materials must be kept in a secure repository. Each day of operation a tape must be removed from the repository and entered into the Gillaroo through the
KOI-18/TSEC tape reader. At this point the computer becomes classified, subject to all pertinent DOE security orders.

FUTURE PLANS

The first test of the system will be the simple test described above involving only two PCs with Gillaroo connected by modems. The next test will involve the installation of a Gillaroo on a PC at Y-12 connected by modem over common carrier to Los Alamos, where the information will be received on a second PC with a Gillaroo. The information transmitted will be actual data produced on the measurement system with proper formatting and inclusion of all header information necessary for a shipment.

REFERENCE