

Los Alamos National Laboratory is operated by the University of California for the United States Department of Energy under contract W-7405-ENG-36.

TITLE: CURRENT STATUS OF LINK ACCESS CONTROL AND ENCRYPTION SYSTEM

LA-UR--84-465

DE84 009604

AUTHOR(S): Ed Springer

SUBMITTED TO: 7th DOE Computer Security Conference, New Orleans, LA, April 10-12, 1984.

DISCLAIMER

This 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. References herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

MASTER

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.

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

MP

Los Alamos Los Alamos National Laboratory Los Alamos, New Mexico 87545



CURRENT STATUS OF
LINK ACCESS CONTROL AND ENCRYPTION SYSTEM

by

Ed Springer, Los Alamos

The purpose of this project is to develop necessary technologies for the secure protection of data communication networks. Data encryption equipment, using the Federal Government's Data Encryption Standard (DES) algorithm, was designed and developed. This equipment is the Link Access Control and Encryption (Link ACE) system. It protects unclassified sensitive data transmissions over unprotected lines between central computers and remote terminals. Link ACE units have been installed and are operational in the Department of Energy's Central Personnel Clearance Index (CPCI) system.

The ACE system project was begun as an informal survey of DES devices available through the commercial market. The DES algorithm, a mathematical operation for encrypting data, was developed by IBM researchers and approved in 1977 as the standard of the Federal Government by the National Bureau of Standards (NBS). At the time of the study, although there appeared to be an assortment of commercial companies competing for a position in the data link encryptor market, no commercial effort was directed

at computer file encryption devices. As a result, the effort at the DOE Center for Computer Security (CCS) at Los Alamos was initially directed at developing data file encryption devices to fill the void in the commercial area. The CCS has been successful in developing a personnel access and data file encryption system known as the Transportable ACE system. This development came at a time when the commercial market had failed to develop the devices needed for the DOE applications. It was hoped that commercial organizations would perfect data link encryptor designs and lower the cost of such units through market expansion, but this did not happen. Many commercial organizations dropped their link encryptor design efforts, enabling those remaining to increase the prices of their units because of weak market penetration. As a result, the CCS developed a link encryptor, using the technology and hardware from the Transportable ACE system. The use of standard hardware has improved functionality and lowered cost to meet DOE requirements for unclassified sensitive data link encryption.

The Link ACE system is part of a continuing effort to produce a full range of computer and communication data-protection tools for the DOE. The Link ACE system has been installed in an operational test bed on the DOE CPCI

system. The CPCI system is a clearance information data base network in Germantown, Maryland, with remote terminal points at 10 DOE area offices. Link ACE makes it possible to send unclassified sensitive data in a secure manner between the area offices and DOE Headquarters using dial-up telephone communications. Remote Link ACE units are installed between terminals and dial-up modems at the area offices, and Master Link ACE units are installed between the central computer and auto-answer modems at the DOE Headquarters Computer Facility. The Link ACE devices are used in physically protected areas, and personnel with access to these areas have a DOE "Q" clearance.

The Center for Computer Security has now developed a new and better link encryptor, the Link ACE II. It will be used in the Headquarters CPCI system along with the previously developed Link ACE. It will also be used in other sensitive unclassified applications. This new link encryptor provides the same functionality and characteristics as the previously developed Link ACE. Tamper detection has been added for use in controlled areas with various access levels. This unit is smaller, faster, and more cost effective than the previous Link ACE.

The purpose of this Link ACE II project has been to develop a pair of

encryption units (one Master, one Remote) to be used to protect unclassified sensitive data transmissions over data links specifically between central computers and remote terminals. The Link ACE II units could be easily adapted to operate in other types of data links: between personal computers, in networks, between computers, and between networks. The Link ACE II is designed to fit on one printed circuit board. The design logic is primarily CMOS except for the encryption chips. The DES chips used in the Link ACE II were approved by the NBS.

The DOE Center for Computer Security at Los Alamos National Laboratory has developed the Link ACE II for the DOE to be used in secure as well as unsecure areas. This equipment has been designed with flexibility and at a reasonable cost in comparison to commercially available units. The Link ACE II allows for frequent and simple Key Encrypting Key (KEK) selection while at the same time preventing exposure of the KEK to the user or operator. KEK selection is allowable only at the Master Link ACE II. The Data Encryption Keys (DEKs) are generated internally and randomly by the equipment using DES.

The Link ACE II provides a cost-effective means to securely protect sensitive unclassified data during transmission over unprotected communications links.