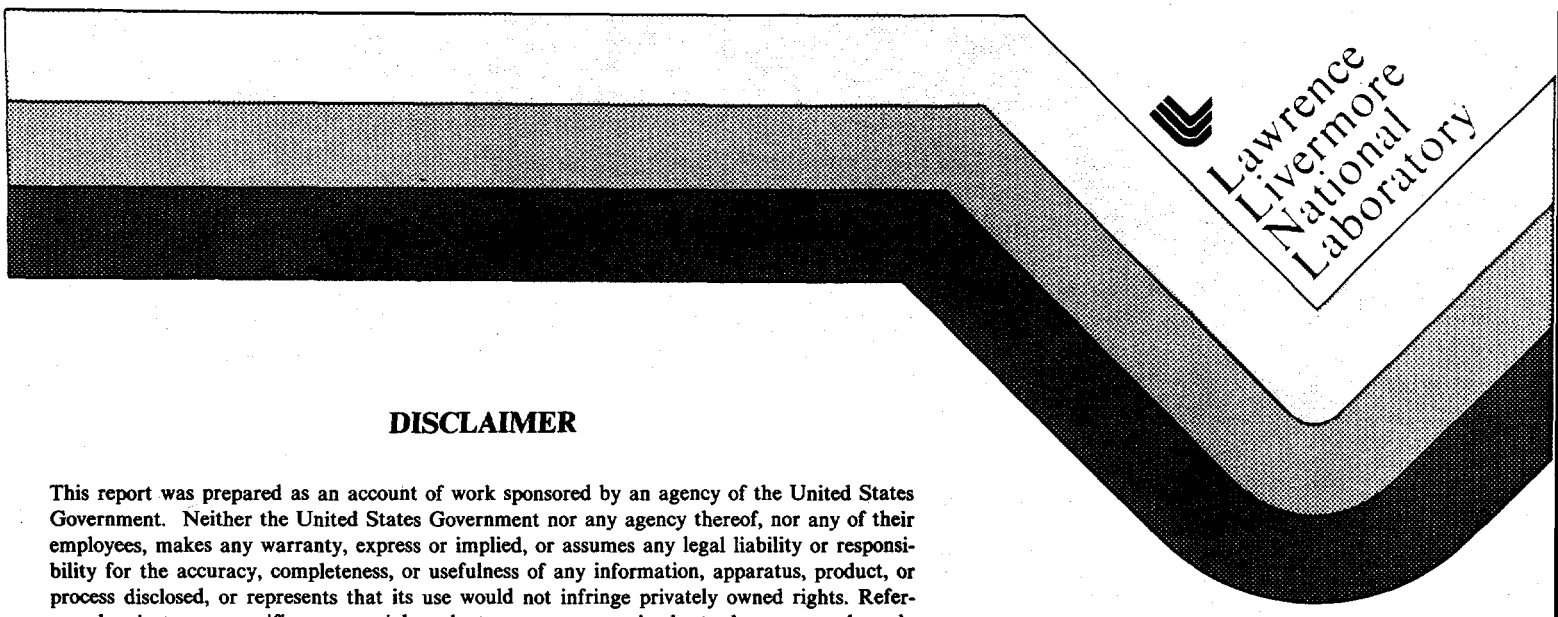
UCRL-CR-114243

DOE Integrated Security System (DISS) Preliminary Communication Security Analysis

Douglas J. Sweeney

October, 1993



DISCLAIMER

Purpose

The purpose of this analysis is to document a technical approach to improve DOE Integrated Security System (DISS) dial-up communications security and the requirements to address them. This document is not intended as a comprehensive analysis of the security aspects of the DISS computer system but rather as an analysis of the dial-up communications security as it pertains to the use of the DISS database in the new DOE Automated Visitors Access Control System (DAVACS) procedures.

Current access controls into the DISS will be discussed with emphasis on the DAVACS procedures. Recommendations will be provided for increasing the dial-up communications security into DISS as it relates to the automated visit procedures. Finally a design for an encrypted dial-up communication link to DISS will be given.

System Description

The DOE Administrative Computer Center at DOE Headquarters in Germantown Maryland houses a variety of classified and unclassified computers. The unclassified system provides IBM/SNA and Internet network services in addition to dial-up communication to the host. This document focuses on the unclassified system which contains the DOE Integrated Security System. Access to the system can be obtained either through network services or dial-up link. The system is attached to a DOE network that has connections to internal and external DOE facilities (see Fig. 1). The system is used as a network gateway to other computer systems on the DOE network. It should be noted that DISS is one of many applications on the system that can be accessed by users. Any security measures considered must take into account the effect on the rest of the system and user population.

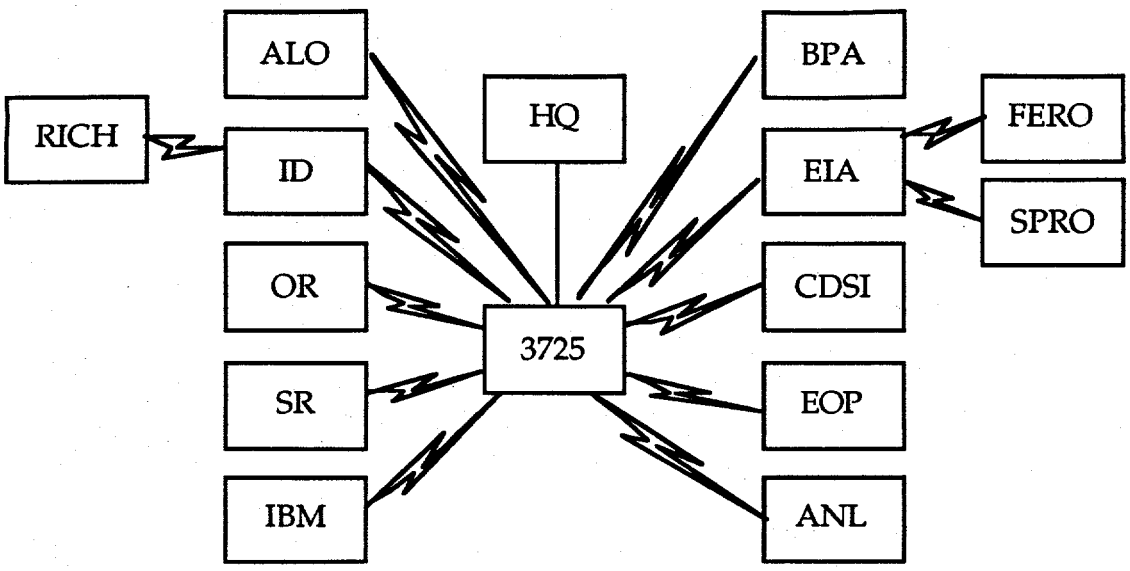


Figure 1. Diagram of DOE Computer Network.

Hardware

DISS resides on a Amdahl 5890/200E mainframe, which is a similar to an IBM 370 mainframe computer.

A front end processor, FEP (IBM 3725), allows access to other remote systems on the SNA network in addition to the Amdahl system. Remote host would use this connection to gain access to the DOE network.

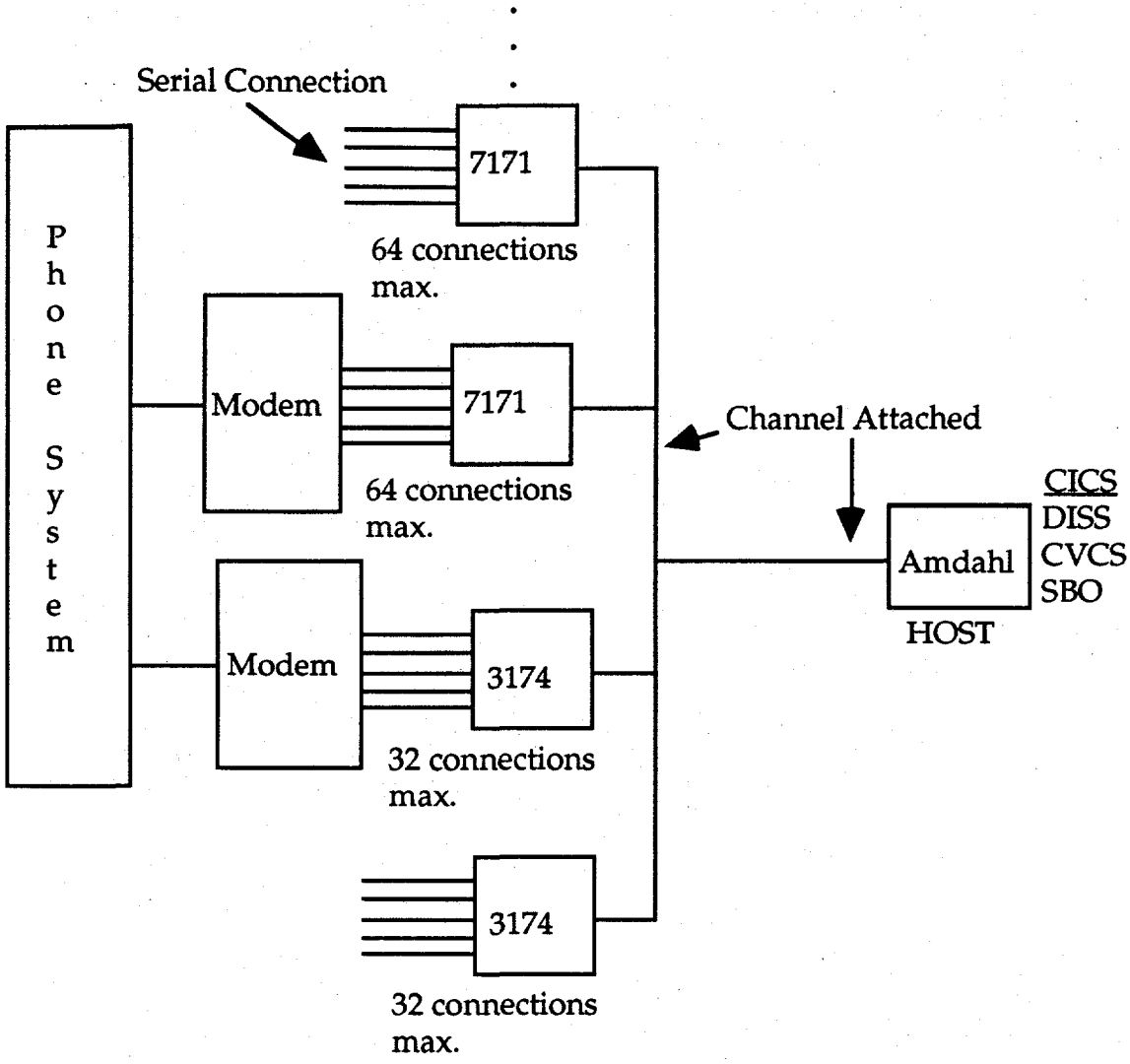


Figure 2. Simplified System Diagram.

Figure 2 shows a simplified view of the system where DISS resides. Other host and communications devices are also channel attached on the network.[1] The complete network configuration can be obtained from the DOE/HQ computer center.

The IBM 7171 ASCII Device Attachment Control Unit allows a maximum of 64 remote ASCII devices access to the system.[2] The IBM 7171 provides the ability to

[1]Channel attached is a IBM specific parallel connection of devices, while serial connection is a direct connect of devices (i.e. through a modem).

[2]The 7171 is no longer supported by the IBM Corporation. Third party vendors are available to supply services and used equipment.

attach a variety of ASCII devices to a IBM host processors. ASCII devices, via the RS-323-C interface, can be connected through modems, leased lines, or directly attached to the IBM 7171. The IBM 7171 also provides ASCII to IBM 3270 protocol conversion.

The IBM 3174 Control Unit is a communications controller for the 3270 terminals and a replacement for the IBM 7171. The 3174 supports a maximum of 32 serial links to 3270 type terminals. In order to support ASCII terminals each 3174 is capable of supporting 3 ASCII Emulation Adapter Cards (AEC, also referred to as the Asynchronous Emulation Adapter ,AEA). An AEC provides 3 major operating modes :

3270 Terminal Emulation	Allows ASCII terminals to emulate an IBM terminal.
ASCII Terminal Emulation	Allows an IBM 3270 Display to emulate an ASCII terminal.
ASCII Pass-Through	Allows ASCII terminals to connect through the 3174 control unit to ASCII hosts.

Each AEC can support 8 ASCII terminals for an additional total of 24 ASCII terminals for each 3174.

This particular DOE/HQ network is made up of seven 7171 ASCII Device Attachment Control Units, this would give a maximum of 448 ASCII terminals. Out of the 448 connections 28 are dedicated to a modem pool of Motorola UDS modems. These modems can be accessed through the 903-2201 modem number. More than 300 lines are connected to the internal digital PBX phone system. The remaining lines are direct connect to the IBM 7171. Currently there are less than 10 terminal connections available on the IBM 7171 units.[3]

The system has a total of two 3174 Control Units. In the DOE configuration only two AEC's per 3174 are used and each AEC has 6 ASCII connections for a total of 24 ASCII terminals.[4] All 24 ASCII terminal connections are connected the 903-8222 modem pool. This modem pool is made up of General Data Communications rack mounted modems. The remaining IBM 3174 connections are used on site within DOE/HQ.

---

[3] As of June 16, 1993

[4] Speed problems have been noticed when more than 16 terminals are connected per 3174. This could be due to the current software on the 3174. A software upgrade may allow additional terminals to be added without the transmission speed problems.

Software

Computer systems on the DOE network can run the IBM VM and/or MVS operating system (OS). The DOE/HQ computer is running the MVS version OS. The choice of the operating systems does not affect the channel attached communications on the IBM network.

There are a variety of applications that reside on the DOE computer network system . Applications can be run from the DOE main screen (see Fig. 3). Applications may reside on different host systems.

```
DOE MVS VTAM SA-11    DDDDD        00000000     EEEEEEEE
Terminal Name:        DD   DD      00    00     EE
   H11LD68            DD    DD     00    00     EE
                      DD    DD     00    00     EEEEE
                      DD    DD     00    00     EE
                      DD   DD      00    00     EE
                      DDDDD        00000000     EEEEEEEE

                HEADQUARTERS ADMINISTRATIVE COMPUTER CENTER
                             GERMANTOWN, MD.
WARNING:  Unauthorized access to this computer system is prohibited,
          and is subject to criminal and civil penalties.
Select an application from this list:
 TSO       - TSO           TEKTRAIN - TRAINING     UCC7      - JOB SCHEDULR
 VM        - PROFS, CMS    VTVM1    - VA TECH      NETVIEW   - NETVIEW
 CICS      - CICS          CICSTEST - CICS TEST    CICSDEVL  - CICS DEVL
 CXTSO     - CDSI TSO2     CXTSO1   - CDSI TSO1    CXCICS    - CDSI CICS
 EIATSO    - EIA TSO       EIAWYL   - EIA WYLBUR   EIAARB    - EIA ARBITER
 SPRTSO    - SPRO TSO      FERCTSO  - FERC TSO     FERCCICS  - FERC CICS
 INEL      - IDAHO FALLS   ALTSO    - ALO TSO      ALCICSP   - ALO CICS
 BPATSO    - BONNEVILLE    BPACICS  - BONNEVILLE   CICSXA    - ON MVSTEST
 IBMINFO   - IBM NETWORK   RICHTSO  - RICHLAND HAN TSOPROD   - PRODUCTION
 DISCICS   - BALTIMORE
 Enter Application Desired ->                                              <-
```

Figure 3. DOE Main Logon Screen.

One of those applications is the Customer Information Control System (CICS). This software allows on line data entry, update, delete, and query capabilities on the DOE Integrated Security System (DISS). DISS is a Headquarters-resident computer application made up of three individual systems: the Central Personnel Clearance Index (CPCI), the Classified Visitor Control System (CVCS), and the Security Badge Control System (SBCS). The three systems provide a method of tracking the major areas of personnel security. The CPCI tracks all of the DOE

security clearances. The CVCS tracks visit information for all DOE facilities. The SBCS assist DOE Headquarters with security badge accountability.[5]

System Access

The DOE main menu can be accessed via a network connection. A number of remote DOE facilities access the DISS through a personnel computer with modem capabilities. An emulation program is needed to emulate a compatible interface with the host computer and interpret correct keyboard functions. The connection to the host system is made through a pool of timesharing modems. There is no measure to deny access to the modem pool. This allows anyone access to the main DOE/HQ computer center screen, which lists all the applications that can be run (see Fig. 3). User ID's and passwords are not required until a an attempt is made to run one of these applications.

The CICS application is accessed with the proper account authorization, login ID, and password. Users must acquire access to DISS by applying for a User ID and Password. The forms (DOE-F-1450.5, DOE-F-1450.5A) are sent to the System Owner at DOE/HQ. For access to any of the other applications an extra form may be required (i.e. DISS Access Request form). When system access is granted the user is allowed to logon to the specific application requested. Accounts are then authorized access to only those applications given permission For access to other networked systems authorization must be given via their system administrator.

Access to DISS is controlled by the Access Control Facility (ACF2) and a DISS User Profile (see Fig. 4). ACF2 is a standard IBM community product that controls and monitors logon procedures. It prevents repeated attempts to logon to the host. Violation of ACF2 rules results in a suspended logon ID. System administrator authorization is needed to reverse the suspension. ACF2 also enforces a scheduled password change. Users must change passwords on a regular basis or faces suspension of their logon ID.

[5] *Department Of Energy Integrated Security System (DISS), System Reference Manual, Operational System Documentation,* Document Number 02-70-R, August 1990

```
      SYSTEM: DBDCCICS U.S. DOE CICS PRODUCTION ENVIRONMENT
                       UNAUTHORIZED ACCESS PROHIBITED BY FEDERAL LAW
    TERMINAL: L611
        NODE: H13L611

         DAY: TUESDAY

 SYSTEM DATE: SEPTEMBER 28, 1993
 SYSTEM TIME: 07:08 PM

     LOGONID: ===> 
    PASSWORD: ===>

NEW PASSWORD: ===>
(enter twice) ===>




CICS/VS - ACF2  (SYSTEM SIGNON/SIGNOFF FACILITY)
```

Figure 4. CICS Logon Screen.

The user profile holds the record of each user's level of access approval. Different levels determine what functions the user is allowed to perform. The profile is maintained by the DOE System Owner.[6]

ACF2, user profiles, user ID's, and passwords control access to the DOE applications. This security procedure has been adopted by DOE/HQ administrators as an adequate security for the level of information contained in the DISS database. To determine the actual vulnerability of the system a vulnerability analysis (VA) would need to be done on the system , that task is beyond the scope of this document.

DAVACS

With the new DAVACS procedures implemented at Lawrence Livermore National Laboratory and other DOE facilities the reliance on the accuracy of the DISS information is of utmost importance. The new CVCS query screens will be of primary interest in the verification of clearances portion of the DAVACS procedure.[7] The CVCS query screen record contains information regarding an

---

[6] *Department Of Energy Integrated Security System (DISS), System Reference Manual, Operational System Documentation*, Document Number 02-70-R, August 1990

[7] Refer to the *DOE Automated Visitor Access Control System Implementation Guide*, UCRL-MI-113646

employee's DOE clearance. The data required for DAVACS procedures is not classified, but can be considered sensitive (clearance level, social security number, etc.). Figure 5 shows the information contained in the CVCS query screen.

```
DBB8 N5548B8          U. S. DEPARTMENT OF ENERGY  (CVCS)          HD68
U8970DS                  CVCS - ACTIVE CLEARANCE QUERY      09/27/1993 15:55

Enter One of the Following:

1.  Social Security Number:
2.  Name                  :
                           (LAST)          (FIRST)      (MIDDLE)

================================================================================
                                CLEARANCE DATA
PSF Location           :
Employer               :
Highest Clearance Level:
This Clearance Granted :
Security Badge Number  :




CLEAR=Exit  PF3=End  PF4=Return  PF12=Cancel
```

Figure 5. CVCS Query Screen.

As more facilities use the new visit procedures the usage of the DOE modem pool and DISS database will increase. This will increase the use of modems and phone lines to transmit clearance data from the host to remote sites.

Recommendations

Remote sites following the DAVACS procedures will only require read authorization. Write capability to the DISS database will not be addressed. Although DISS is an unclassified system, the information being transmitted to DOE sites is sensitive enough to warrant an investigation into secure dial-up communications. Measures should be in place to insure that the possibility of unauthorized access or misuse of data in DISS is minimized. The approach and cost of trying to secure the entire system would be beyond the scope of this document.

The following are several possible recommendations that could be adopted to improve the dial-up communications security of the computer system. None of these measures prevent access through the other available network connections. The ability to selectively secure portions of the computer applications is only a measure that will temporarily inhibit an intruder.

VTAM

Virtual Telecommunications Application Messaging (VTAM) allows logical communication ports to be established via tables which dictate logon sessions. VTAM tables can be set up in a variety of ways. It is possible to identify specific host to run from known ports. This means that access to a host application can be restricted depending on the port a user is attached. This would have the effect of limiting the number of ports that can access a host computer and the applications that reside there. Using VTAM to control access to the DISS database is possible by restricting the number of ports having access to the CICS application.

Password Protected Modems

Making the access to the modem pool password protected is one method of securing access to the computer system. Currently the dial-up modems can grant access to the DOE main screen to anyone with a modem. A modem pool can be configured to request a password before establishing a modem link. This would protect access to the modem link, but would offer no extensive security protection since the password would have to be known by all the users of the dial-up modems. This would also require development of applications to allow this feature. Hardware implementation of this scheme are available but would require a possible upgrade of the modem pool.

Call back Modems

Another variation of modem access control is the use of callback scheme. This would control access by calling a pre-defined remote modem after a communications link is requested. A remote site would dial into the host modem, after some initializing and identification the modem connection is released by the host. The host proceeds to reestablish the communication link to remote user at an authorized telephone number stored in memory. This provides access security of the modem network and only allows those who are authorized to access a modem connection.

The host modem pool would need to be configured with modems that have the ability to call a remote system. This approach requires that the remote sites have a fixed phone number for their DISS connections and that their modems are capable of remote access.

Callback applications can be implemented by the host. An application would constantly monitor the modem lines and initiate a callback when a request to connect is received.

Leased Lines

A brief questioning of some LLNL users indicated that connections into the DOE modem pool are established at the beginning of the business day and maintained until the end of business. This would indicate an average of 7 hours of connect time every business day. Fear of losing modem connection and not being able to re-establish dial-up communications was the reason for this practice. The CICS application has a time-out feature that sets a session inactive if no command keys are entered within 10 minutes (see Fig. 6). To resume the session the user is allowed 10 attempts to enter their correct password, this procedure is monitored by ACF2. Users typically quit the application and return to the main DOE application selection screen where there is no time-out feature. This allows the user to maintain their modem connection throughout the day. This practice not only ties up a modem link it also establishes a fixed link to the DOE network.

```
                    ACF2/CICS PASSWORD VERIFICATION PROMPT
                    --------------------------------------

O/S NAME: CICS
  SYSTEM: DBDCCICS   U.S. DOE CICS PRODUCTION ENVIRONMENT
   SYSID: PROD       UNAUTHORIZED ACCESS PROHIBITED BY FEDERAL LAW
TERMINAL: L611

  REASON: TERMINAL INACTIVE

 ACFAE908 ACF2/CICS: PLEASE... ENTER YOUR PASSWORD  >>>=======> _
```

Figure 6. ACF2 Timeout Screen.

Leased phone lines connecting each of the facilities to the DISS system would not provide much more protection than the open phone lines currently used. Although this would improve the reliability of the communications to DISS. The DISS connection is tied to a known permanent link which would eliminate the

need for a modem dial-up link. Digital links could be used which would improve transmission speed (up to 56K baud) and reliability.

Encryption

The above communication link options address access to the DOE computer system and do little to protect the data being transmitted. Data encryption has long been a method of securing information during transmission between two sites. This method of securing dial-up communications is to encrypt the data between the host computer and remote sites. Encrypting of the data lines would secure the data across the physical phone lines without hampering the operation of the system.

There are a variety of encryption methods available, the following is a brief description of one possible method.

Encryption schemes usually require a set of encryption keys, a randomly generated key and a public key. The random key is generated independently and is kept secret, it is not accessible to the user. This random key is used to create a set of public keys. The public key is exchanged at the time a communication link is established. The exchanged public key is loaded into each encryption device prior to any data communications. Algorithms, such as the Data Encryption Standard (DES), use these keys to encrypt and de-encrypt the data. If no key is present or the keys are not valid the ability to de-encrypt the data is not possible.

Encrypting devices do not maintain a data communications link if there is an unsuccessful key exchange. This would have the affect of restricting access to the dial-up network. This technique to some extent provides access control to the dial-up network.

There is the required process of key management as with most encryption methods. The creation of valid keys and their use in an encryption system require a management procedure to insure protection of generated keys and secure communications. This would be considered a draw back in the encryption solution. In the past this has meant that a key administrator would have to be assigned, insuring that the encryption keys are generated and changed periodically in the encrypting devices. The latest models of encrypting devices have a the capability of automatic key management. This is where the management of the encryption keys are handled by computer and are transparent to the user. Keys would be generated and distributed electronically. An administrator is not needed to manually generate or exchange keys, but only to monitor the encryption network. This does not eliminate the need for personnel to manage the network.

Hardware changes would have to be made since the data encryptors are placed in-line with the existing configuration of modems, remote terminals, and host

computers. Each end of the communication link would be required to have an encrypting device (see Fig. 7).

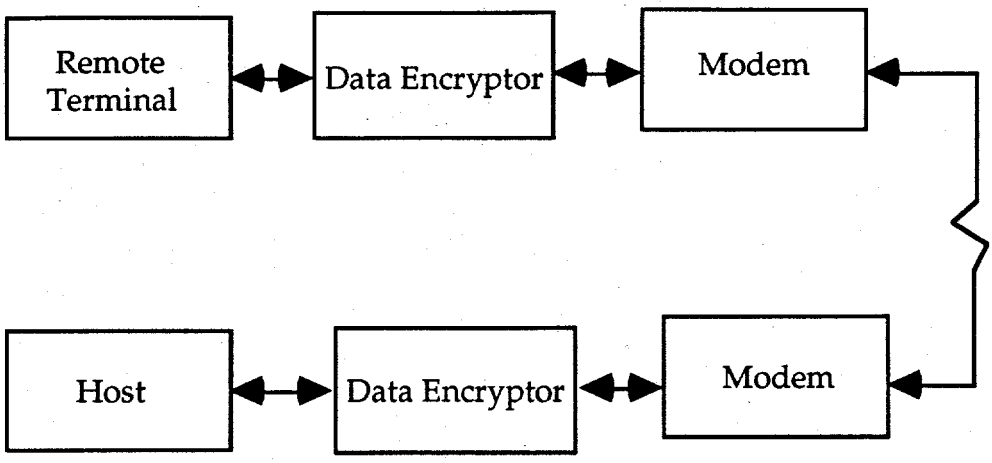


Figure 7. Diagram of a Encrypted Dial-up Communications Link.

Encryption of DOE/HQ Dial-Up Communications

This design is presented with a few assumptions :

1) The current network connections, including dial-up, into the DOE network would be unchanged. The design is presented as an addition to the existing network system.

2) Modeled after LLNL, each site will have a minimum of 1 DAVACS terminal. A maximum of 50 DOE sites to implement the DAVACS procedures will be considered a worst case estimate. A maximum of 64 modem connections would be sufficient to adequately handle all sites connected simultaneously.

3) Access to DISS would be administratively controlled. All sites accessing the DISS database must be authorized and use the proper encryption methods.

4) A majority of users will communicate via ASCII terminal devices.

5) The design will not deviate drastically from the network system already installed at DOE/HQ

Communication Control Units

The addition of two IBM 3174 channel attached into the DOE network would provide an additional 64 (max.) 3270 terminal connections. The installation of 3

AEC cards in each 3174 would add another 48 (max.) ASCII terminal devices. Currently IBM 3174 model controllers are approximately $10K and each AEC is approximately $2K. A possible third 3174 could be added if significant communications speed reduction is noticed on the ASCII terminals.

COST : $32K

Encryption Devices

Companies such as CYLINK Corporation and Information Resource Engineering, Inc. (IRE) produce encryption equipment for small and large networks. The host encryption system would consist of rack mount devices. Each device would have the capability of housing 16 encryption cards, one communication link per card. With a total of 16 encrypted lines per rack a total of 4 encryption racks would be needed for 64 communications lines. Four racks would be used at a cost of approximately $3K each for a total of $12K. Each encryption link needs a host encryptor card for 64 connections at $1K each this cost would reach an estimated cost of $64K.

COST : $76K

Modems

Two additional modem pools (3270 and ASCII terminals) would be added to enable remote sites to dial into the encrypted link. A modem rack will hold 8-16 modems at a cost of approximately $1K. A total of four modem racks would be required, in keeping with the encryption links, at $4K. Each modem would control one communications link. A reliable high speed modem in such a system would cost approximately $.7K. A full modem pool would require a total of 64 modems would be needed at a cost of $44.8K.

COST : $49K

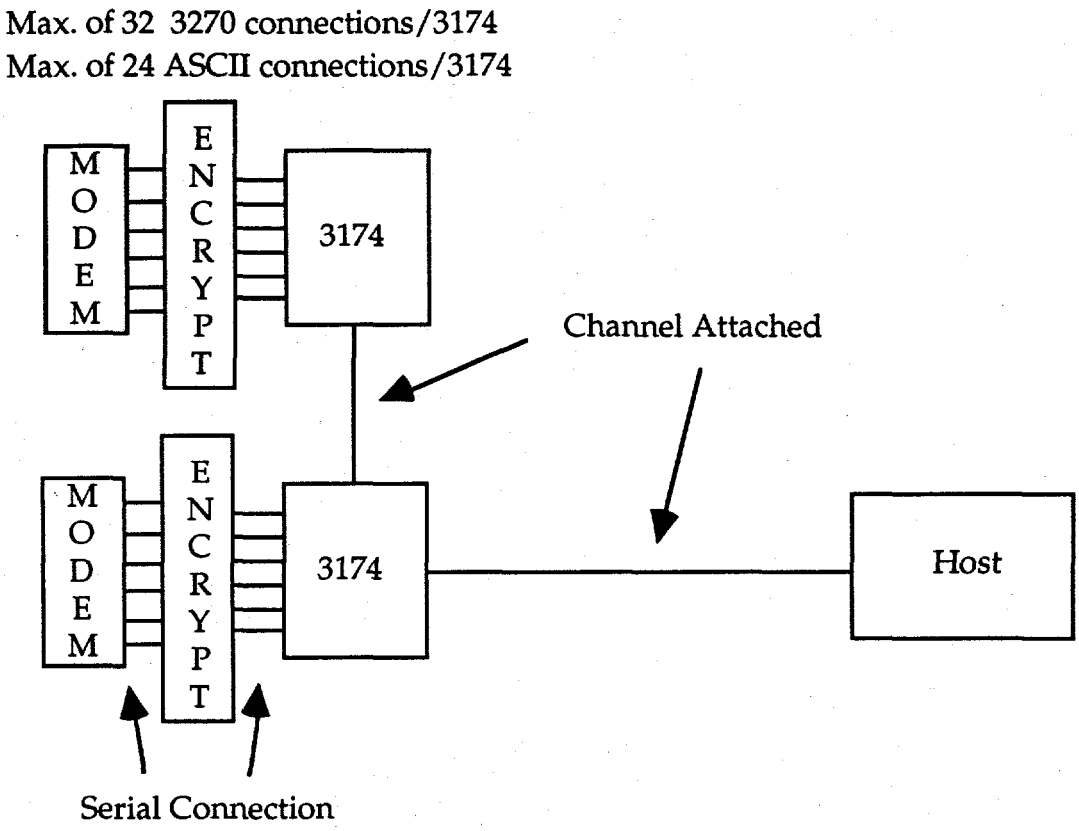


Figure 8. Encrypted Dial-up Communications Enhancement

By taking advantage of VTAM, it is possible to restrict certain ports to a particular application or system. Therefore it is possible to restrict access into DISS by allowing only those ports connected to the encrypted modem lines to run the CICS application. It should be a small issue using software controls to restrict users to only those applications that they are authorized access. With VTAM and ACF2 it is possible to restrict application access to certain ports.

Remote sites would have to install a remote encryption device, by the same manufacturer of the host encryptor, into their dial-up DAVACS terminal setup. Assuming the terminal is already setup, with a CPU, modem, and terminal emulation package, the encryptor would add a cost of approximately $1K.

A more in depth design would have to be done to take into account features of the latest hardware and software.

Summary

There are many issues that must be resolved before encryption of the DOE dial-up communications can be achieved.

Close ties with the communications group at the DOE/HQ computer facility is needed to insure support for the encrypted network. Cost of reconfiguration and installation of equipment needs to be addressed. Responsibility and ownership of the equipment will be an issue.

With such an encryption system, the need arises for personnel to monitor the encryption network. Not necessarily for key management purposes, but to monitor network failures and insure the operation of the system. With the possible addition of new hardware and procedures, personnel would have to be trained to operate such a network. Staff and procedures to monitor the encryption system for faults, errors and alarms are needed to maintain a reliable encryption system.

DOE requirements on encryption devices installed on the DOE network must be adhered to. There are standards such as the DES (Data Encryption Standard) ANSI X3.92 and FIPS 46 (Federal Information Processing Standard) that are a requirement for encrypted DOE systems. There are many commercially available encrypting devices that follow these standards and many more.

Encryption related Standards:

FIPS PUB 46-1 Data Encryption Standard
FIPS PUB 74 Guidelines for Implementing and Using the NBS (NIST) Data Encryption Standard
FIPS PUB 81 DES modes of operation
FIPS 140-1 Tamper proof case
FIPS 170-1
ANSI X3.106 Modes of DES
ANSI X3.92-1981 (ISO DIS 10126) Data Encryption Algorithm
Federal Standard 1027 Key protection and tamper-proofing requirements
ANSI X9.17-1985 (ISO DIS 8732) American National Standard for Financial Institution Key Management/Key Exchange Protocol

The question of electronic key management needs to be addressed. If electronic key exchange is not approved for use in DOE/HQ, then a manual key exchange must be implemented. This would considerably increase the overhead of maintaining an encryption network.

The effect on the users and non-users of the DOE computer facility require attention. The ability to be transparent to users is important. Administrative controls would be necessary in any case since there would be other avenues into the DISS database.

Other possible options are available for communications to the DISS that need to be investigated. One imaginable alternative is the ability to connect to the DOE/HQ computer system through an Ethernet connection. Currently there is a

TCP/IP link on the VM system (vm1.hqadmin.doe.gov). Expansion of this capability may be a option in obtaining more reliable communications and improved security. Remote sites would need to get a TN3270 emulation to run full screen editing from the service. Encryption devices are available that interface with Ethernet networks. This subject is beyond the scope of this document and needs more in depth study.

There are many options available in designing an expanded dial-up network with encryption. Engineers from IBM and encryption manufacturer are needed to assist in the most efficient design possible for the DOE computer facility.

Conclusion

As more DOE facilities implement the DAVACS procedures, access to the DISS database will be performed on a larger scale. DOE/HQ dial-up communications security can be improved with the addition of a encryption network. Determination of the need for such an enhancement should be made based on the DISS database classification level and the amount of protection needed. Technically the addition of a dial-up encryption system is possible.