

CENTER FOR COMPUTER SECURITY NEWS

Volume 9, Number 1

April 1990

**CIC-14 REPORT COLLECTION
REPRODUCTION
COPY****An Overview of
Kerberos: A Network
Authentication System**Cheryl Steverson
DOE Center for Computer Security

This paper provides an overview of the Kerberos Model, a network authentication system designed to "[verify] the claimed identity of a client or service"¹ as presented by D. E. Geer Jr., J. A. Rochlis, and J. I. Schiller at the USENIX Summer 1989 Conference in Baltimore, Maryland.

The Kerberos system, designed and implemented as a part of Project Athena* at the Massachusetts Institute of Technology (MIT), is a network authentication system "... based on the Needham and Schroeder third-party model and using private-key encryption."² Kerberos provides a trusted third-party authentication service between a client and a server or service that ensures the identity of the client or service to the other network entity.

The physical environment in which Kerberos operates at MIT "... currently consists of 850 hosts" of which 450 are public workstations located throughout the campus and available to any member of the MIT community; another 100 are dedicated servers; and the remaining machines are private workstations owned by individuals or staff. The workstations are primarily DEC Vaxstation IIs, Vax 2000s and IBM RT/PCs. In addition, there are "a variety of peripheral devices, notably laser printers, at the ratio of one

per eight workstations."² In this environment "the primary security threats result from the potential of a workstation user to forge the identity of another user in order to gain unauthorized access to data and/or resources." Because of the insecure nature of a workstation, "including operating system and network interface ... an authentication service is required to counter such attempts."¹

Encryption

The Kerberos implementation at MIT uses the Data Encryption Standard (DES) algorithm because it provides a cost-effective encryption solution for the MIT environment. Most nodes in a Kerberos environment will have software DES; a few nodes—namely, the Kerberos Key Distribution Center—will have hardware DES.

***Kerberos provides a
trusted third-party
authentication service
between a client and a
server or service that
ensures the identity of the
client or service to the
other network entity.***

The encryption mechanism is designed in a modular fashion so that it can easily be replaced. Because it is illegal to export DES, it must be replaced in Kerberos versions intended for export, and other encryption mechanisms should be considered for Kerberos versions intended for use in environments with higher security requirements.

The Kerberos Model

The goals of the Kerberos Model are detection of unauthorized user activities such as masquerading and other "fraudulent connection attempts," prevention of the release of message contents to other than the intended recipient, and detection of message stream modification.¹ To detect masquerading, "... each association [of client and server] must be established in a manner which allows secure identification of the principals at each end." For both the user (client) and the service, "knowledge of [the] encryption key proves identity." However, the key production and distribution system must be trustworthy and protected. The Kerberos Model uses a Key Distribution Center (KDC) to perform this function; it "knows primary keys for all principals" and "distributes session keys encrypted in appropriate primary keys to principals wanting to communicate." This "requires a secure communications channel to establish each principal's primary key," as well as physical security for the machine hosting the KDC. A "compromise of [the] KDC is a disaster!"³

To prevent a "playback of a previous legitimate [connection]," the Kerberos system uses a "challenge-response" approach; "one party sends [an] encrypted challenge [and the] other party replies with some function of the challenge, also encrypted." To verify that the connection request is current, the challenge and response include encrypted time stamps. Synchronization of clocks is accomplished using the Network Time Protocol (RFC1059).³

*"Project Athena is a joint effort between MIT and a number of external sponsors, principally Digital Equipment Corporation and International Business Machines" to develop and implement a network services model for an educational environment. "... An experiment in computer-aided education, its charter is to create a computing environment that fosters educational innovation." Athena has developed several network service systems that perform functions including a service management system, a name service system and Kerberos—a network authentication system.²

To prevent the release of message contents, Kerberos encrypts message packets—protocol data units, or PDUs—using keys that are administered by the KDC. The security of these packets is ensured by using a key granularity appropriate for the security level required by the implementation, by using cipher block chaining (CBC) to prevent the exposure of block-aligned data, and by using initial vectors that are pseudo-randomly chosen for each association.

Detection of message stream modification is frequently provided through the mechanisms controlling the prevention of message contents release. "A PDU decrypted using the wrong key will be detected with high probability; changes made to an encrypted PDU as it traverses the network will [also] be detected with high probability when the PDU is decrypted." However, CBC techniques are "subject to exchange of cipher text blocks or [to] insertion of pairs of cipher text blocks." To prevent this, a CRC [cyclic redundancy check] or other code with good burst properties may be added to the PDU before encryption.³

Kerberos provides authentication—not authorization . . .

Message authenticity is established by determining "to which [client-server] association and to which direction a PDU belongs." Both the "insertion of a new PDU into an association stream" by an intruder and a playback attempt from another session are detected with high probability in the Kerberos system by "using a unique key per association." Because a unique key exists for each association—the key issued by the KDC—Kerberos uses it to protect the integrity of the PDU. Detection of "playback from [the] same association, but [in the] opposite direction" is addressed by the inclusion of a direction bit in each PDU.³

To ensure the correct ordering of messages, Kerberos must detect deletion of a PDU, a change in order of a PDU, and the duplication or playback of a previously valid PDU. To protect against PDU deletion and a change in order, Kerberos

includes a sequence number encrypted along with the other contents of the PDU. Kerberos protects against playback by assigning unique sequence numbers to each association.

Kerberos does not address the prevention of traffic analysis, nor does Kerberos detect denial of message service or Trojan Horse software. Kerberos provides authentication—not authorization, "e.g., a[n] NFS [Network File System] server can be sure that it is [a specific user] asking to read a file."³ Applications software may, however, use this authentication information to make discretionary access control or authorization decisions.

Kerberos's Design Goals

In designing the Kerberos system, the developers' primary goals were to provide reliable authentication services while requiring "minimal modification to existing network applications . . ." and to remain "transparent [to the users] during normal [system] use . . ." To avoid any burden to system users, Kerberos requires only one password that the user enters at login in order to gain access to authorized network services. "No clear text passwords [are transmitted] over the network."³ A further goal for Kerberos

was to limit the window of damage if a compromise is successful.

The Kerberos Implementation

Tickets and Authenticators

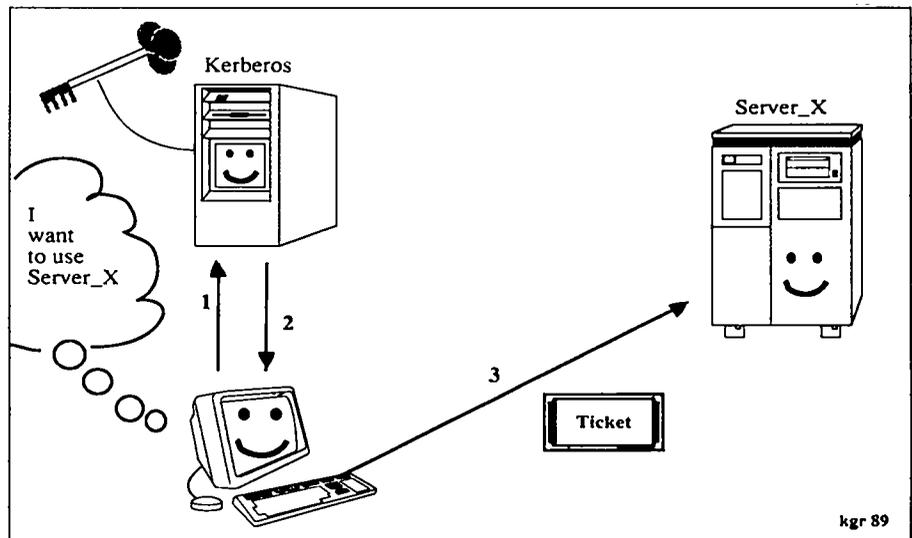
$$T_{c,s} = \{s, c, \text{address, current time, ticket lifetime, } K_{c,s}\} K_s$$

$$A_{c,s} = \{c, \text{address, current time}\} K_{c,s}$$

Notation

- c = client (workstation)
- s = server
- K_c = private key of "Client"
- $K_{c,s}$ = session key for "c" and "s" {info}
- K_x = "info" encrypted in given key
- $T_{c,s}$ = ticket for "c" to use "s"
- $A_{c,s}$ = authenticator for "c" to use "s"

The Kerberos system provides authentication services between client and service based upon an encrypted "ticket" that Kerberos issues to the client to allow access to the requested service. For example, when a user is issued a username and password by his system administrator, the password is "one-way encrypted [and] . . . serves as the user's private key. . . . The Kerberos Authentication Server stores the user's private key encrypted under its own master key . . ." All clear text keys are destroyed immediately after encryption.



1. Client sends {c, s} to Kerberos
2. Kerberos sends { $K_{c,s}, T_{c,s}$ } encrypted in K_c to Client
3. Client sends { $T_{c,s}, A_{c,s}$ } to Server_x

Figure 1. The Kerberos Server

When a client requests the service of server_x, he or she does so by sending a login request to the Kerberos Server from the client machine (Figure 1).

The Kerberos Server returns a "ticket" for the user to access server_x, together with a unique session key, both encrypted in the user's private key (the user's encrypted password). The ticket contains the server name, client name, client address, current time, ticket lifetime and the session key for client and server. The client creates an "authenticator" by encrypting client name, client address and the current time in the session key (previously issued by Kerberos). The client's "ticket" (allowing use of service_x) and the "authenticator" are then sent to service_x. If the user is an authorized user of service_x, the server can, using the user's private key, decrypt the information and allow access. Should decryption of the "ticket" and the "authenticator" yield garbage (s!=s), "you.lose." In addition, the ticket contains a ticket lifetime value; if ticket issue time plus ticket lifetime is greater than current time, the ticket life has expired and "you.lose!"⁹

To ensure the validity of the time fields passed between network entities, clock synchronization is necessary in the Kerberos environment and is achieved using a master time server. To accommodate minor deviations from the global clock, a clock skew factor is typically introduced into the lifetime equation. A note about clock synchronization: backwards discontinuities will open a security hole in Kerberos. Therefore, it is necessary to use an algorithm to slow the clock to achieve synchronization with the time server instead of "jumping" back in time. Forward clock synchronization is no problem. The ticket lifetime achieves one Kerberos design goal by limiting the window of damage to a fixed period if a compromise should occur. Ticket lifetime values are arbitrary and controlled by the Kerberos system administrator for each user; a common ticket lifetime in the MIT environment is 8 hours.⁹

The Kerberos Ticket-granting Service

To avoid having the user type in a password each time a service is requested,

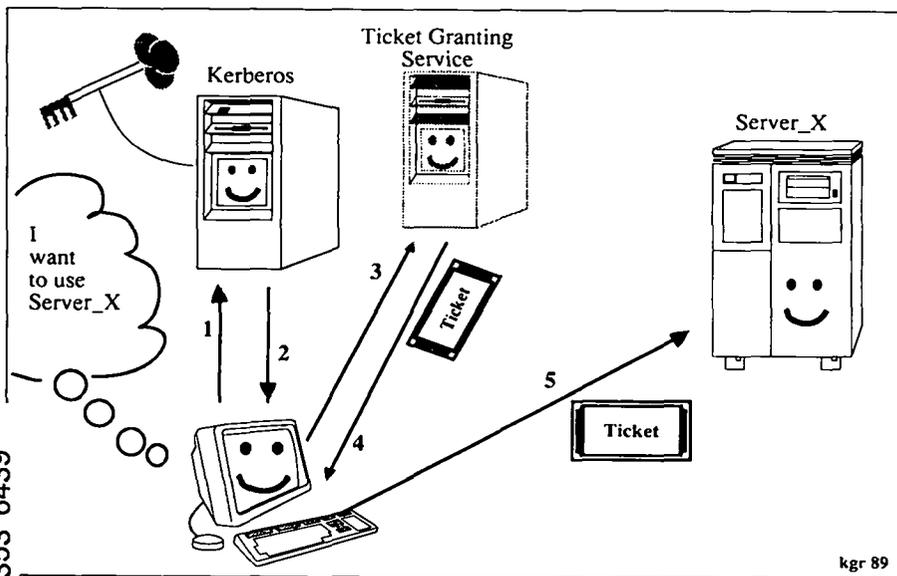
the Kerberos system includes a ticket-granting service that runs on the same host as the Kerberos authentication server (Figure 2). With the ticket-granting service, the first time a user logs in and requests access to a service, the client name and a request to access the ticket-granting service are sent to the Kerberos server.

Kerberos returns a session key for use by the client and the ticket-granting service, and a ticket allowing the client to use the ticket-granting service. The client encrypts an authenticator as previously described and sends this, along with the ticket to use the ticket-granting service and the service name (service_x), to the ticket-granting service. The ticket-granting service sends a session key for service_x and a ticket to use service_x back to the client, all encrypted in the session key issued by Kerberos for use between client and ticket-granting service. Finally, the client sends the ticket to use the specific service and the authenticator to the desired service (service_x).

Using this scheme, a client need repeat only step 5 to initiate re-use of service_x, and the client needs to repeat only steps 3-5 to request a new service, thus reducing the overhead involved in multiple service requests.

Kerberos Configuration

The main components of the Kerberos authentication service consist of the Administration Server, the Time Server, the Authentication Server, the Kerberos database, and the Kerberos libraries.² The Administration Server adds new accounts and administers password changes; the Time Server provides global clock information. The Authentication Server hosts the Key Distribution Center and runs continuously to "... service authentication requests sent over the network by creating server tickets and session keys." The Kerberos database can be implemented using a simple database management system; the Kerberos libraries consist of a Kerberos library, a DES library, and a Kerberos database library.



1. Client sends $\{c, tgs\}$ to Kerberos
2. Kerberos sends $\{K_{c,lg}, T_{c,lg}\}$ encrypted in K_c to Client
3. Client sends $\{T_{c,s}, A_{c,lg}, s\}$ to TGS
4. TGS sends $\{K_{c,s}, T_{c,s}\}$ encrypted in $K_{c,lg}$ to Client
5. Client sends $\{T_{c,s}, A_{c,s}\}$ to Server_x

Figure 2. The Kerberos Ticket-granting Service



Kerberos can reside on one or more servers, with a typical configuration consisting of a master Kerberos server and one or more slave servers. The master server is a physically secure machine running only trusted software. The Kerberos database, the authentication server, the time server (optional), the administration server, and the libraries reside on the master server, with similar data residing on the slave server (also secure and trusted) in case the master is down or busy. Other servers on the network are typically located in only moderately secure areas and run potentially untrusted software, including user's software.

It is imperative that the Kerberos authentication server be highly available. An uninterruptable power source and the ex-

istence of a Kerberos slave server containing a replica of the master database will increase the availability and reliability of the Kerberos system. The slave server updates its database by performing read-only operations from the master. All updates to the database must go directly to the master, thus avoiding most of the problems associated with distributed databases.

Kerberos Administration

The Kerberos system software includes system administration programs that initialize and maintain the Kerberos master server, additional servers, and the Kerberos database. Kerberos system source code and documentation are in the public domain.

References

- ¹ S. P. Miller, B. C. Neuman, J. I. Schiller, and J. H. Saltzer. *Kerberos Authentication and Authorization System*. Project Athena Technical Plan (Cambridge: Massachusetts Institute of Technology, 1988), pp. 1-9.
- ² J. G. Steiner and D. E. Geer, Jr. "Network Services in the Athena Environment" (Cambridge: Massachusetts Institute of Technology, 1988), pp. 1-3.
- ³ D. E. Geer, J. A. Rochlis, and J. I. Schiller. *Security Issues in a Distributed UNIX Environment: the Kerberos Approach*. Tutorial from the USENIX Technical Conference and Exhibition. 12-16 June 1989, Baltimore, Maryland.

Gordian Key: Access Management System

Kenneth Grady
Administrative Data Processing
Los Alamos National Laboratory

The Center for Computer Security neither evaluates nor recommends commercial products; we do, however, try to provide information that we feel may be useful to those in the field. This article is based on another group's experience with the Gordian Key and its Access Management System.

The Access Management System can serve as a user authentication mechanism on a wide range of host architectures. The Gordian Key is a "challenge/response" device that reads and deciphers an encrypted flashing pattern from the terminal screen; the key returns a password that allows the user to gain access to the host computer system.

The key, together with host-resident software, is a password-generating device that provides a means to control access to a specific computer system, network, data unit, or program. One-time passwords are generated with each use of the Gordian Key. The Access Management

System consists of the host-resident protection program, hand-held Access Key devices, and the "Key Cutter."

The Key device is self-contained, battery-powered, and relatively small (Figure 1); its four optical sensors read a flashing stimulus from the terminal screen.

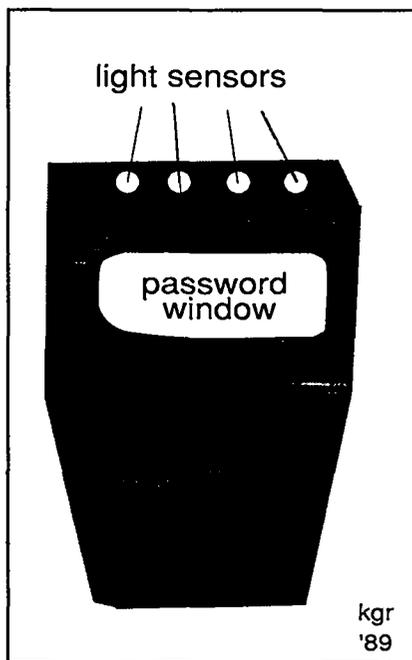


Figure 1. Gordian Key Access Device.

The key uses encryption routines to convert the host-generated stimulus to a six-character password which it displays on the LCD screen.

In our implementation, the keycutter hardware and software are installed on an IBM-PC; additional database software is installed on a VAX. The database on the PC supplies information to add keys to the database on the VAX where access checking is performed. The PC database also provides disaster recovery for the VAX database.

The first database is maintained by a "CUT" program and contains information about the Gordian Key such as key number, date the key was cut, and other miscellaneous information. Correct dates are essential to the success of this system. The CUT program requires a special customer key to allow access to the database. After gaining access to the database, the system administrator enters each new key's identification number and (if the use of the key is to be limited) the restrictions and number of days and/or number of uses.

The Key Cutter device programs each Access Key with seed information specific to the customer. This is the information used during the key's encryption of the password. The key's limits can be

permanent or resettable. Resettable limits (one to control the length of time and a second to control the number of uses for which the Gordian Key device will remain valid) are updated by a special "LIMIT" program accessed through the CUT program. The key cutting is accomplished through the flashing of a pattern of lights into the four light sensors located on one end of the Gordian Key. In about thirty seconds, the display window on the key locks onto a pattern of six eights and remains there for four to five minutes. This pattern indicates that the key is being cut.

A file is created and transferred to the VAX where it is used to add new keys to the second database. The new entries are updated with a "USER ID" or, in our case, a nonclassified password from OS-4. Once this password is entered in the VAX database, the Gordian Key can be used to unlock the system and gain access to the micom switch.

After a user enters his/her password, the Access Key protection program is invoked and flashes a graphic pattern on the terminal screen (Figure 2). The user holds the Gordian Key's light sensors against the screen so it can "read" the data represented by the flashing pattern. The Access Key device encrypts this

data with seed information stored within its own memory cells. This encrypted six-character code is then presented on the key's LCD. The user enters this response to the host-resident protection program which, after verifying the correctness of the response, grants the user access to the micom selection menu.

When the user presses the carriage return at a terminal, the micom connects the terminal to the Gordian VAX and the process which requests the password begins. When the user enters a password, a program runs to set the username; then the authentication program checks for a valid username. If the username is not in the database, the session is terminated. If the username is found, a flashing pattern is displayed on the terminal. The user must aim the Gordian Key's light sensors at the flashing pattern and place them against the screen; within a few seconds a six-digit code will appear and lock in the window for ten to twenty seconds. This code must be entered at the terminal keyboard so the program can validate the response. If the program cannot validate the response, another flashing pattern is displayed. If the response is accepted, another program is run to send the micom switch a security redirect request.

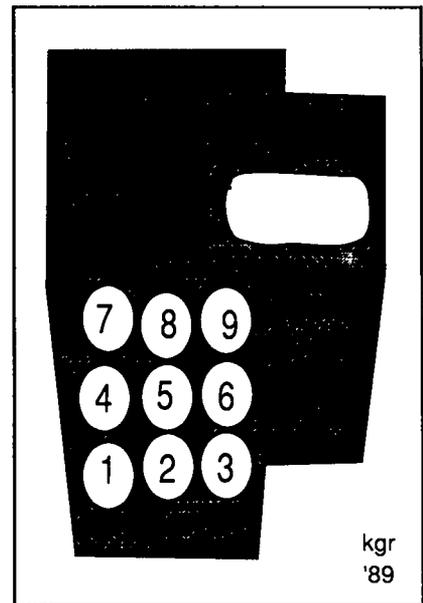


Figure 3. Gordian Key Keypad.

The micom processes the security redirect and displays a menu of machines for selecting. After a selection is made, the familiar "Username:" prompt appears. When the user ends a session on the selected machine, the micom again displays the menu of machines for selection. If the user does not select an additional machine within sixty seconds, the Gordian Key is required to access the micom.

In normal use, if the user log-on is completed before invocation of the Access Management System, the protection program can use the user's log-on ID to generate the password. The system manager for the host machine must develop and place on the host system the database that contains users' IDs and the necessary seed information for all Keys. The system manager also has to tailor a number of subroutines to the host machine's operating system and security design.

Whenever the Gordian Key is used, an internal counter in the key is updated to keep track of the number of uses. Successful, as well as failed, attempts are stored on the database on the VAX. For each key the database has a switch that allows automatic denial of access after three consecutive failures with the key. If access evasion is in effect, the database manager must reset the key's entry in the database before access can once again

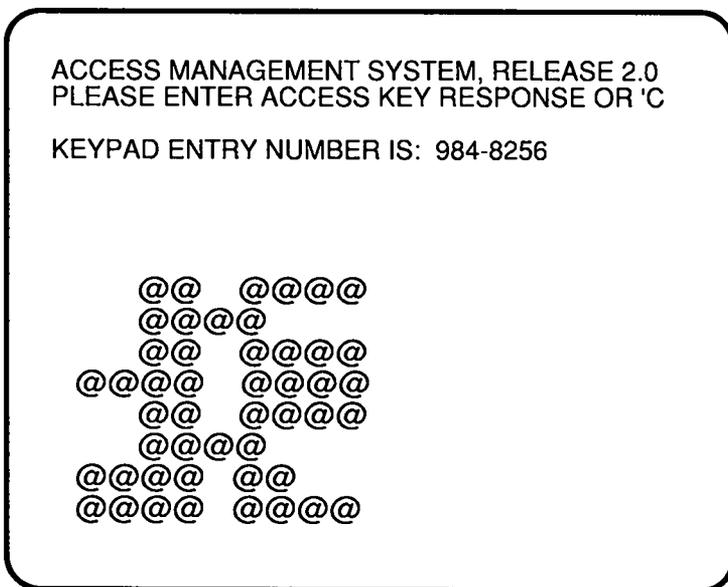


Figure 2. The Access Management System Screen.

be granted. When a limit has been reached (the number of days or number of uses a key is allowed), the key must be returned to the keycutter for the expired limit to be reset; otherwise, the key is useless. If the key was cut with permanent limits or if the battery runs down, the key is good only as a status symbol. If anyone attempts to open a Gordian Key, the program within the key self-destructs without smoke, noise, or other sensory evidence.

This system cannot guarantee that someone did not give his/her key and keycode to another person; it does, however, ensure that someone monitoring the telephone line cannot infiltrate the system. We tried using two terminals to log on, running the program at the same time, and entering the keycode and response at both terminals, but only the session using the key was granted access.

The keys are rugged and dependable; one that went through the washing machine and soaked in water overnight (they float, by the way) and others that went through airport metal detectors still worked. Users with color monitors find that some color combinations work better than others; green and yellow seem to be difficult for the light sensors to pick up while magenta on red worked fine.

Ken Grady is a system administrator in ADP-1.

Removing the Mystery from the OSE I&E Program

Kenneth A. Rogowski
McDonnell Douglas Electronics Systems Company

Since its inception in 1983, the Office of Security Evaluations (OSE) Inspection & Evaluation (I&E) Program has evolved in response to ever-changing mission requirements, budget constraints, and new technologies. The one thing that has remained constant over the years is the need to ensure that DOE security interests are protected effectively. The restructured Inspection Process aims to do just that—to ensure the effectiveness of the security safeguards throughout DOE.

The purpose of this article is to explain the inspection process clearly and in terms of the recent restructuring of that process. In order to do this, we will couple some general remarks with a walk through the process from the initial trauma upon arrival of the I&E notice to the relief of receiving the final report. Along the way we will examine the mission and organization, the functions of the program, and the concept of operations so that sites will know what to expect.

Overview: OSE I&E Program

The responsibility for ensuring the protection of the security interests of DOE lies with the Secretary of Energy. To

assess the effectiveness of the current safeguards and security programs, the Secretary relies on the OSE I&E Program to connect DOE Headquarters with the Operations Offices and their contractor sites in the common goal of ensuring that effective safeguards and security are implemented.

For the purpose of managing inspection resources, the DOE Operations Offices and their contractor sites are divided between the two branches of the OSE Inspection Division. The Applications Branch is responsible for inspecting Albuquerque, Nevada, Oak Ridge, and the San Francisco Operations Offices and associated facilities. The Production and Research Branch is responsible for inspecting Chicago, Idaho, Richland, and Savannah River Operations Offices and Pittsburgh and Schenectady Naval Reactors Offices and associated facilities.

The program accomplishes its mission using three basic functions: inspections, performance tests, and evaluations (also referred to as assessments).

Inspections are reviews of the effectiveness of the implementation of DOE protection programs in selected topical areas such as Information Security, Personnel Security, Protection Program Operations, and Computer Security at a specific Operations Office or associated facility. The inspection process is based on DOE Orders and is conducted using the Safeguards and Security Orders, Standards and Criteria, DOE-approved handbooks,

and procedural guides to develop site-specific inspection plans and guides. The inspection focuses on how an Operations Office manages the safeguards and security programs of its subordinate contractor sites.

A performance test is an on-site exercise of the personnel, equipment, and procedures of selected parts of the protection program to determine compliance with DOE policy. Each performance test is designed to exercise both technical and procedural protections required by the DOE Order and is fully defined in a Performance Test Plan that must be coordinated with OSE and site personnel before it is approved by the Inspection Chief for implementation. The performance test results are incorporated with other data gathered during the inspection process.

An evaluation is an assessment of the overall effectiveness of the DOE-wide protection program within a topical area. Evaluations are based on data obtained in the field during inspections and on other pertinent input regarding the overall state of the safeguards and security programs. This process results in an Annual Assessment Report for each topical area. These reports are not specific to any particular Operations Office, but cut across DOE organizational and functional boundaries in an attempt to provide an overall assessment of program effectiveness.

The Restructured Inspection Process

The remainder of this article will focus on a coordination initiative with the Office of Safeguards and Security (OSS) and the component parts of the restructured inspection process.

Coordination

Enhancement of the coordination between OSS and OSE is accomplished under the terms of a memorandum of understanding between these two elements. This coordination incorporates a more comprehensive involvement throughout the entire inspection process and provides for one or more OSS observers to accompany the inspection team during the data-gathering and report-writing phase. The observer's responsibility is to address policy issues and, whenever possible, to resolve those issues before completion of the inspection. This capability enables the inspection process to be more responsive to the site with regard to the interpretation of policy issues.

The Schedule

Inspection schedules are developed on an annual fiscal year basis by the Director of the OSE. The schedule is coordinated with the appropriate DOE Operations Office to ensure that the inspection timeframes selected can be accommodated and do not conflict with other known significant events. Once the schedule is established, every effort is made to minimize changes to provide the sites and the inspection staff with stability for planning purposes and to preclude confusion.

The Inspection Components

The restructured inspection process consists of a topic and team selection phase, a planning phase, and a data-gathering and reporting phase. While these are the same basic elements as those that constituted the previous inspection process, the activities that occur within each phase have been restructured to reduce the burden placed upon key personnel in the safeguards and security organizations of both the field

and Headquarters and to enhance the coordination between OSE and the Office of Safeguards and Security (OSS) regarding inspection activities. Reduction of the burden on key personnel will be accomplished by expanding the advanced inspection planning phase and reducing the number of on-site visits from three (totaling four weeks) to one (over a two-week period), while retaining the basic characteristics required of the inspection process.

Topic and Team Selection

This part of the inspection process begins with the selection of the Inspection Chief (IC) from the OSE staff and the assignment of the senior coordinator from the contractor support staff that provides

There are eight topics that are potentially inspectable.

direct support to the OSE I&E Program. The identification of the topics that will be inspected is accomplished at the direction of the Director of the OSE by the IC and a small cadre of OSE inspectors. There are eight topics that are potentially inspectable. These include the Safeguards and Security Survey Program, Information Security, Personnel Security, Physical Security Systems, Material Control and Accountability, Operational Security, Computer Security, and Protection Program Operations. The actual number of topics selected for any one inspection may vary during the selection process. Topic selection is made only after review and consideration of the following parameters:

- Management-directed topics tasked from The Office of the Secretary, Assistant Secretary for Defense Program, or other authorized DOE Headquarters element;
- Security protection specified in documentation on file at DOE Headquarters (e.g., Master Safeguards and Security Agreement, Security Survey Reports, Security Plans, previous Inspection Reports, etc.);

- Assigned ratings based upon previous inspections, Annual Security Surveys;
- Current threat data, both generic and site specific;
- Available inspecting resources; and
- GAO Reports, IG Report, etc.

Once the inspection topics have been established, the team-selection process begins with the assignment of an OSE oversight person for each topic. These oversight responsibilities are normally assigned to members of the OSE inspection staff. Subsequent activities include selection of the proper technical expertise from among the contractor and sub-contractor resources available to support the OSE I&E process, as well as active participation in the conduct of planning and execution of inspection activities. All participants are officially notified of their assignments and of the final arrangements for the planning meeting.

Planning Phase

The Planning Phase is conducted at DOE Headquarters in Germantown, Maryland. During the Planning Phase, the IC begins preliminary coordination with the applicable Operations Office regarding details of the inspection. Featured among the issues addressed is a request to the Operations Office for documentation (plans, policies, procedures, etc.) that can be used by the inspectors during the planning phase to (1) determine the scope of the inspection within their topics, (2) become familiar with site operations, and (3) develop appropriate performance tests.

The formal planning phase for the entire team spans one week. Along with the read-ahead documentation, each inspected site normally provides at least one knowledgeable individual for each topic to travel to Germantown and assist the inspection team with its preparation for the inspection. These site personnel provide considerable assistance in clarifying issues not readily apparent from the documentation. If, however, there is not sufficient documentation or participation by the Operations Office at the planning

meeting, OSE may still need to plan a site visit. A visit may also be required to support tailoring of a performance test that will be used during the inspection.

At the conclusion of the Planning Phase, each topic lead inspector briefs the Director of the OSE, Director of the Inspection Division, the Inspection Chief, and the OSS representative, as well as the rest of the inspection team, on the course of the action that has been prepared for the inspection of their respective topics. A final Inspection Plan is prepared to guide the course of the inspection.

Data Gathering and Reporting Phase

The Data Gathering and Reporting Phase takes place at the inspected site and extends over a period of approximately two weeks. The activities during this phase include data gathering, daily validation of the data gathered on each topic, report writing, validation of the draft report by

the Operations Office, and exit briefings. Data gathering is accomplished through interviews with site personnel, document reviews, performance tests, and observation of site operations. A summary of how the activities of this phase are allocated during the two-week period is shown in Figure 1. Particular attention is given to the validation and report-writing processes. Every effort is made to ensure that the data gathered is correct so that the report accurately reflects the security environment observed at the site.

A draft report is prepared and submitted for an initial twenty-four hour review to the Operations Office being inspected. Information contained in that draft is a compilation of the individual facts that were validated daily during the data-gathering phase, along with an analysis of those facts and the impact they have on the site's security program. This rapid review by the Operations Office offers the first opportunity for site representatives to see

how these facts will be presented in the report. Obvious factual errors commented on by the Operations Office will be corrected; areas which involve an interpretation of DOE policy will be taken under consideration and, where appropriate, will be incorporated into the final draft.

Post-Site Activities

Before the inspection team leaves the site, a draft of the final report is submitted to the Operations Office for formal comments. Fifteen days are allowed for this review in order to ensure that all issues can be appropriately addressed. Issues regarding policy gaps, clarity, or interpretation of the DOE Order are referred to OSS.

At the completion of the review process, the report is prepared in its final form. That inspection report provides the mechanism for advising DOE Headquarters and the appropriate Operations Offices of the ability of safeguards and security policies, programs, procedures, systems, personnel, and/or operations to meet the spectrum of threats to the inspected sites. These reports also provide major input to analytical assessments prepared to assess risks to the national security, the environment, or the health and safety of the public. Every effort is made to ensure that reports are clear and concise and do not contain unnecessary levels of detail. The present format will easily adapt to the future direction of the restructured inspection process.

Trends for FY 1990

FY 1990 will be marked by reorganization of selected functions within the DOE. As part of this realignment, DOE Headquarters has announced that the OSE will leave Defense Programs and become part of the organization that falls within the purview of the Assistant Secretary for Environment, Safety, and Health. The effective date for this realignment is pending. Any changes in the inspection process that may occur as a result of this reorganization will be announced as quickly as possible.

	Travel to Facility	Team Meetings	Data Gathering	Daily Validation	Summary Validation	Report Writing	ID Directors' Briefing	Internal Reviews	Report Modification	Briefing Materials Preparation	Written Field Validation	Outbrief	Travel Home
Sunday	X												
Monday		X	X	X									
Tuesday		X	X	X									
Wednesday		X	X	X									
Thursday		X	X	X									
Friday			X	X	X								
Saturday		X	.		.	X							
Sunday													
Monday			.		.	X	X	X					
Tuesday								X	X		X		
Wednesday									X	X	X		
Thursday									X	X	X		
Friday												X	X

Figure 1. Field Inspection—Generic Schedule.

In the meantime, every effort will continue to be made to enhance the technical level of the Computer Security inspection and to ensure closer coordination of the inspection process with the Operations Offices, site personnel, and OSS. The technical aspects will be enhanced by the use of structured, limited-scope performance tests to assess the extent to which security features are in compliance with DOE 5637.1. Early use of these performance tests has revealed that they not only benefit the inspection process, but may also have applicability for use by the sites as part of the system test and certification process.

Initiatives are underway to enhance the availability of computer security expertise within the OSE inspection staff and to provide more efficient coordination with OSS. These initiatives reflect the importance of ensuring that the inspection staff



understands the intent of the Order against which the sites are being evaluated and that program management and OSS are provided with immediate infor-

mation regarding how the sites are interpreting and implementing the DOE policy. The spirit and intent of this closer working relationship is reflected in the memorandum of understanding between OSE and OSS.

Points of contact for additional information regarding the computer security topic for inspection are Don Agnew (FTS 233-5360) and Ken Rogowski (FTS 233-4541).

Kenneth A. Rogowski is Manager of Information Security Programs, McDonnell Douglas Electronics Systems Corporation in McLean, Virginia. Mr. Rogowski has been participating in the OSE computer security inspection process since 1986. In September 1989, he began a one-year period on the OSE staff where he provides direct computer security support to the Inspection Division and Assessments Division.



The CSSO Training Seminar held February 26th through March 2nd at the Central Training Academy, Albuquerque, NM, was fully subscribed. The next course is scheduled for October. For further information, contact Harry Rosenblum at the Center or Carla Baker at CTA:

DOE Center for Computer Security
(FTS) 843-0444 or 843-0100
(505) 667-0444 or 667-0100

OR

Central Training Academy
(FTS) 845-5170 5170
(FTS) 845-4539 or (505) 845-4539

Center for Computer Security News

ATTENTION!

This issue features articles on authentication tools and systems and access control; some of you probably have information on additional authentication or access control measures. How about submitting an article for a future issue?

If your interest lies in another area, don't hesitate to submit an article. Any topic related to computer security is appropriate. See page 20 for guidelines on submitting articles. Those of you in the field undoubtedly have ideas and information that can be useful to individuals in similar positions.

The Keys to Security— SAVE-ME

This article is reprinted from *News to Use: A Newsletter for VAX Systems Managers*, Vol. 1 (Summer, 1989), 6-7, by permission of DEMAX Software, 999 Baker Way #500, San Mateo, CA 94404.

A comprehensive security assessment of a small VMS system with thirty accounts and eight to ten thousand files will require a minimum effort of at least one day, using just the tools provided with VMS. Performing a similar assessment of a larger system having two thousand accounts and half a million files is a week-long task for a team of experienced people.

After much discussion with various experts in the field of VMS security, DEMAX Software has developed a series of steps to ensure the desired level of security can be developed and maintained. We have coined the phrase **SAVE-ME** to help remember each step. In this article we will outline those phases:

- System Setup
- Account Setup
- Volume Setup
- Evaluation/Verification
- Monitoring/Auditing
- Education

The necessity of the **SAVE-ME** steps is growing each day as the number of nodes and accounts grows. In fact, with many facilities facing the need to secure access to millions of files, the task is nearly becoming unmanageable without specific security tools. Let us now turn and look at each of the **SAVE-ME** phases.

System Setup

This phase is designed to ensure that the system can be trusted. Any viruses and most holes, whereby viruses can infect the system, will be eliminated. The major access paths to the system will be carefully guarded and alarms will be enabled to ensure any changes are detected. During this stage the system manager must

- Reinstall VMS and all applications images.

[Assuming the distribution is not infected,] reinstalling VMS and application images FROM THE ORIGINAL TAPES will ensure that no viruses are attached to executables. Note that reinstalling from a backup tape gives you no protection—you have no way of knowing whether the backup was made on a secure system or not.

- Check ownership and protection of all system files.

This step involves checking that all system files are properly owned and protected according to DEC recommendations. Create a report on these files and use it to compare to current settings on a timely basis.

- Install any images requiring privileges.

This step is a precursor to step five. It is frequently preferable to install an image with privileges rather than give privileges to all the potential users of the image.

- Set up security-related SYSGEN parameters.

The security and integrity of the system is affected by a number of SYSGEN parameters. For example the LGI_* parameters let you determine the number of times someone attempts to login unsuccessfully before he is considered an intruder; what to do when an intruder is found; "hide" time; etc. Other helpful parameters include TTY_DEF_CHARS, which can prevent someone setting up a "world-readable" terminal.

- Set up select terminals for

SYSPASSWORD and
SECURE_SERVER.

In some organizations there are terminals in public locations that can access confidential information. These terminals are frequently protected by having an additional password called the SYSTEM PASSWORD. [Dialup ports should also be protected.]

- Set up and enable the alarms.

The next step is setting (and using!!) alarms. A useful set of alarms might include

- remote logins
- dialup logins
- failed login attempts
- failed file access attempts
- security-related events

Be sure to regularly monitor the OPERATOR.LOG to catch such alarms as soon as they occur. Some sites find it useful to dedicate a printer terminal to output the OPERATOR.LOG.

Account Setup

This phase will ensure that unnecessary account-related "windows" are closed. All accounts and their related privileges and access rights will be rationalized, and initial password parameters will be standardized. Here the system manager must

- Correct duplicate UICs.

Each user should have his own account. This is necessary in order to restrict access as well as provide an audit trail for overall system security. Make this a priority in your account setup.

- Correct login directory problems.

Each account on the system has a defined login directory. This directory should be owned by the account. If the directory is not properly owned the account will experience problems with various functions, including the creation of files and the submission of batch jobs.

- Remove unneeded accounts and disable unused accounts.

Many organizations consider an account a candidate for disabling when it has been unused for thirty days; one unused for six months may [should?] be removed. The time periods, of course, depend on the site, but all unused accounts should be carefully monitored since they are windows into the system.

- Reduce privileges where possible.



Indexes

Included in this issue are several indexes that have been requested from the Center. They have been placed here in the center of the newsletter so you can remove them easily and keep them for reference. You will find an index of articles that have appeared in past issues of the **Center for Computer Security News**, an index of videotapes that can be used for training and security awareness, and an index of currently available Toolkit items.



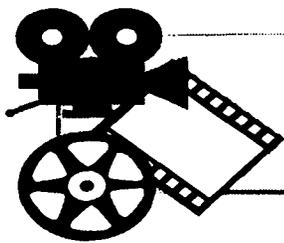
New Video!

Now available is a Center-sponsored film that lasts about 20 minutes: *The Outsider: Training for Escorting Uncleared Personnel into a Classified DOE ADP Facility*. All CSSMs have received a copy of this video. There is no restriction about making copies; CSSMs are encouraged to make copies for their CSSOs.

Other helpful videos are *Computer Security: Make the Commitment*, Office of Personnel Management, about 14 minutes; *Computer Data Security*, 20 minutes; and *Data Security: Be Aware or Beware; Locking the Door*. For more information on these, contact Harry Rosenblum:

(FTS) 843-0444 or 843-0100
(505) 667-0444 or 667-0100.





Available Videos

DOE-ID Security Education/Awareness Videotapes

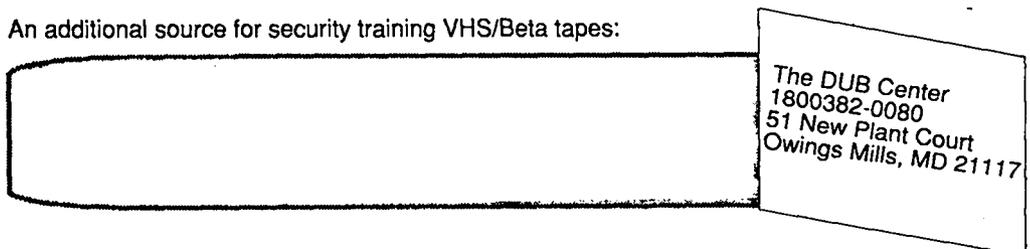
The Idaho Operations Office has the following films in its Security Education/Awareness Videotape Library. Brief descriptions are included when available. Patty Graves, Security Assistant, DOE-ID Technical Security, has indicated willingness to exchange information and thoughts on the use of videotapes as an aid in effecting ongoing, positive Security Education/Awareness. She can be reached at (208) 526-2301 or FTS 583-2301.

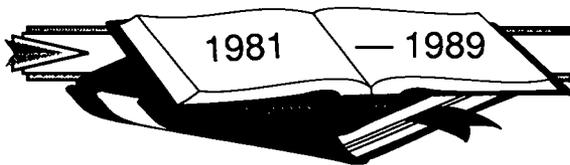
<i>DOE-D FY-89 Annual Security Briefing</i>	48 mins	12/88
<i>The SF 312</i>	13 mins	
<i>Spies Among Us</i>	48 mins	
<i>Recording Inked Fingerprints</i>	16 mins	2/84
<i>NOVA: Computers, Spies & Private Lives</i>	55 mins	5/82
This NOVA presentation dealing with misuse of computers is much too long; very minimal mention of security-related computer precautions, but might be of interest to computer operations personnel.		
* <i>M. E. Sphere</i>	12 mins	
Discusses document security, badges, physical security, and procedures to follow in case of marriage, arrest, or travel to Soviet-bloc countries.		
* <i>In the Dark About Security</i>	12-14 mins	
Specific to Bendix, but contains good information; references AEC, ERDA, DOE, and ALO.		
<i>INEL Security</i>	18 mins	2/85
<i>Travel to Communist Controlled Countries</i>	18 mins	3/82
Contains a number of tips for DOE employees; a "must" for personnel about to visit such a country.		
<i>The Ultimate Terror</i>	50 mins	2/84
<i>Information Security Briefing (3 segments)</i>	46 mins	
<i>Secrets & Security: For Your Information</i>		
<i>FY-88 Security Education/Awareness Orientation</i>	41 mins	12/87
<i>The Innocent Abroad</i>	18 mins	8/87
<i>Need to Know</i>	13 mins	
<i>Travel Safety & Security: A Survival Guide to Traveling Abroad (Foreign Travel Briefing)</i>	23 mins	
Fast-moving, entertaining, informative training video; addresses concerns expressed by international travelers on safety and security issues.		
<i>Hostage Survival</i>	25 mins	1977
Video quality poor, discussion rather drab, but covers some good points.		
<i>When in Doubt</i>	16 mins	
<i>CBS Reports: Terrorism</i>	49 mins	

<i>Something of Value</i>	10 mins	
<i>Terror: To Confront or Concede</i>	60 mins	
More suitable for semester-length college class in international terrorism than a security refresher; an in-depth philosophical discussion of the consequences of repressive government actions.		
<i>The Dark Side of Espionage</i>	18 mins	
Convicted spy Christopher Boyce debunks "popular myths" about espionage; objective of the tape is to increase awareness of the hostile intelligence threat and its personal consequences.		
<i>Tom Brokaw—Achille Lauro—NBC</i>		6/86
<i>Drug Identification</i>		
<i>Foreign National Congressional Hearings</i>	60 mins	
<i>Persons, Places & Things: Security at INEL</i>	9 mins	
<i>Classification: Your Role at the INEL</i>		
<i>Oak Ridge Swat Team</i>	4 mins	
<i>The INEL Guard Force</i>	5 mins	
<i>Understanding Classification</i>	10 mins	4/85
<i>INEL Security</i>	18 mins	
<i>Advanced Tactical Training: Savannah River</i>	15 mins	
<i>Personal & Family Security (Overseas Assignment)</i>	25 mins	
Tips for persons assigned overseas, including common sense measures and communications procedures.		
<i>INEL Central Alarm Monitoring & Access System</i>		
<i>The Invisible War (20/20)</i>	20 mins	12/79
<i>NBC Magazine—"Silicon Chips"</i>	12 mins	
<i>Espionage: It Does Happen</i>	18 mins	
<i>Confidentially Speaking</i>	14 mins	1980
Illustrates the vulnerability of voice and other communications sent by telephone.		
<i>Something of Value (NATO & DOE/OSS)</i>	10 mins	
Ideal for security awareness meeting; subtle animated allegory illustrating how a great symbolic "structure" of prosperity and freedom was built, and through unwitting disclosure of seemingly harmless information regarding its inner workings to outsiders, was destroyed.		
<i>Addition to "Necessary Choices"</i>	23 mins	
<i>John Lewis, LANL-8/18/87 "Chinese Nuclear"</i>	2 tapes	
<i>The Threat of Hostile Intelligence</i>	27 mins	1979
Discusses various aspects of the "threat profile;" emphasizing the most damaging leakage of vital information is via the telephone because of transmission "spills." Discusses problems of technology transfer and briefly covers cultivation and recruitment of DOE or other government agency personnel for obtaining classified information.		

<i>Operation Red Fox</i>	30 mins	
Shows some of the methods used by Soviet-bloc intelligence to obtain technical information.		
<i>Anti-nuclear Demonstration</i>	56 mins	9/80
<i>Anti-nuclear Rally at EBR-II (INEL)</i>	53 mins	9/80
<i>Anti-nuclear Demonstration; Arco, ID (INEL)</i>	49 mins	11/79
* <i>What You Know Could Make a Difference</i>	12 mins	
Very good for security meetings; cartoon character releases classified information to KGB (take-off of actual espionage incidents).		
<i>Time of the Jackal (20/20)</i>	55 mins	
May be too long for a security meeting but very well done and entertaining; relates terrorist activities conducted by an infamous international terrorist, "Carlos"; features attack on OPEC ministers in December, 1976.		
<i>The Classification Picture</i>		1979
<i>Dixie Lee Ray, WTTG—Channel 5: "Nuclear Power—How Safe"</i>		1973
<i>Postmark: Terror</i>	15 mins	1977
Designed to help security and law enforcement personnel cope with package and letter bombs.		
<i>George Weisz (20/20)</i>		5/84
<i>Deadly Force</i>		
<i>National Security & Freedom of the Press</i>	60 mins	
<i>CBS Reports: Terrorism</i>	49 mins	6/85
Multiple Video (includes 7 films)		
Includes the films marked with an asterisk above, plus the four below:		
<i>Technical Security</i>	4 mins	
Discusses foreign radio intercept, alarms for security areas, and CCTV pan scan tilt capabilities.		
<i>ADP Security</i>	2 mins	
Discusses computer, physical, personnel, hardware, and software security.		
<i>It All Fits Together</i>	2 mins	
Discusses the Bendix security puzzle (physical, personnel, equipment, and information security).		
<i>Security Education—Proper Use of Computers</i>	11 mins	
Includes IG guidelines and DOE orders 1360.2 and 5636; includes <i>Computer Security Is Your Business</i> .		

An additional source for security training VHS/Beta tapes:





Index of Articles—DOE Center for Computer Security News

Andrews, William H. Jr.	<i>Vulnerability Assessment: PC—Network Connectivity.</i>	Vol. 6, No. 3 (December 1987), 18.
Anonymous.	<i>Acquiring a Commercial Turnkey Local Area Network.</i>	Vol. 3, No. 3 (March 1984), 40.
	<i>Admiral Foley to Give Keynote at Ninth DOE Computer Security Group Annual Conference.</i>	Vol. 5, No. 1 (February 1986), 6.
	<i>ADP Security Education at Bendix Kansas City.</i>	Vol. 3, No. 3 (March 1984), 63.
	<i>Air Force Summer Study.</i>	Vol. 2, No. 1 (August 1982), 3.
	<i>Are You a Candidate for Personal Computer Security Problems?</i>	Vol. 8, No. 2 (August 1989), 7.
	<i>Article/Topic Submission Form.</i>	Vol. 8, No. 1 (April 1989), 23.
	<i>Ask the Expert.</i>	Vol. 6, No. 2 (July 1987), 8.
	<i>Ask the Expert.</i>	Vol. 7, No. 1 (July 1988), 34.
	<i>Assistance with DOE Order 1360.2 Implementation.</i>	Vol. 2, No. 3 (May 1983), 46.
	<i>Authentication, Discretionary and Nondiscretionary Access Control in Computer Networks.</i>	Vol. 3, No. 3 (March 1984), 59.
	<i>Availability of Awareness and Training Package.</i>	Vol. 7, No. 2 (December 1988), 7.
	<i>Backup and Contingency Planning.</i>	Vol. 1, No. 4 (June 1982), 33.
	<i>Baker Moves to Germantown.</i>	Vol. 5, No. 3 (September 1986), 7.
	<i>Bob Abbott Presents Keynote Address.</i>	Vol. 1, No. 4 (June 1982), 2
	<i>Calendar of Coming Events.</i>	Vol. 2, No. 2 (November 1982), 3.
	<i>Calendar of Coming Events.</i>	Vol. 3, No. 1 (July 1983), 4.
	<i>Center for Computer Security Activities.</i>	Vol. 6, No. 1 (March 1987), 1.
	<i>Center for Computer Security Survey #1.</i>	Vol. 5, No. 2 (May 1986), 9.
	<i>Center for Computer Security Survey #2.</i>	Vol. 5, No. 2 (May 1986), 9.
	<i>Center Makes Significant Progress.</i>	Vol. 1, No. 2 (Autumn 1981), 2.
	<i>Center Moves to New Location.</i>	Vol. 4, No. 2 (January 1985), 1.
	<i>Center Objectives Outlined.</i>	Vol. 1, No. 1 (Summer 1981), 2.
	<i>Center Services:</i>	Vol. 5, No. 1 (February 1986), 7.
	<i>Certification and Accreditation.</i>	Vol. 1, No. 4 (June 1982), 14.
	<i>Changes in Center Mission and Operation.</i>	Vol. 5, No. 1 (February 1986), 7.
	<i>Chief of Operations Security Branch.</i>	Vol. 2, No. 2 (November 1982), 1.
	<i>Classified Computer Security Policy Being Revised.</i>	Vol. 5, No. 1 (February 1986), 6.
	<i>Clearing Terminal Screens.</i>	Vol. 3, No. 1 (July 1983), 3.

Anonymous.	<i>Color-Coded Floppy Disks.</i>	Vol. 4, No. 2 (January 1985), 3.
	<i>Colorado Computer Crime Law—Potential Applications.</i>	Vol. 3, No. 3 (March 1984), 67.
	<i>Computer Assisted Instruction and Its Role in the DOE Headquarters Computer Protection Program.</i>	Vol. 3, No. 3 (March 1984), 64.
	<i>Computer Security Advisory Group Participates in Update of Computer Security Order</i>	Vol. 5, No. 3 (September 1986), 7.
	<i>Computer Security Awareness Management Guide.</i>	Vol. 6, No. 3 (December 1987), 1.
	<i>Computer Security Branch Chief Named.</i>	Vol. 6, No. 1 (March 1987), 1.
	<i>Computer Security Bulletin Board.</i>	Vol. 5, No. 3 (September 1986), 9.
	<i>Computer Security Education Plans and Activities.</i>	Vol. 6, No. 1 (March 1987), 8.
	<i>Computer Security Effort Centralized.</i>	Vol. 1, No. 1 (Summer 1981), 1.
	<i>Computer Security Group Annual Conference.</i>	Vol. 6, No. 1 (March 1987), 1.
	<i>Computer Security Group Meeting June 18-19, 1981 Idaho Falls, Idaho.</i>	Insert—Vol. 1, No. 2 (Autumn 1981).
	<i>Computer Security Group Steering Committee.</i>	Vol. 8, No. 2 (August 1989), 2.
	<i>Computer Security in the International Environment.</i>	Vol. 2, No. 3 (May 1983), 24.
	<i>Computer Security Management.</i>	Vol. 1, No. 4 (June 1982), 11.
	<i>Computer/Terminal Processing Warning Signs.</i>	Vol. 8, No. 1 (April 1989), 1.
	<i>Conference Attendees.</i>	Vol. 1, No. 4 (June 1982), 37.
	<i>Cook Becomes Deputy Assistant Secretary for Security Affairs.</i>	Vol. 4, No. 3 (April 1985), 1.
	<i>Correction.</i>	Vol. 1, No. 4 (June 1982), 34.
	<i>Danger—Virus on the Loose.</i>	Vol. 6, No. 3 (December 1987), 14.
	<i>Data Base Security.</i>	Vol. 1, No. 4 (June 1982), 24.
	<i>Decision Analytic Methods for Security & Safeguards Risk Assessment.</i>	Vol. 3, No. 3 (March 1984), 46.
	<i>Department-Wide Unclassified Computer Security Assessment.</i>	Vol. 6, No. 1 (March 1987), 3.
	<i>Detection and Prevention of Computer Misuse.</i>	Vol. 1, No. 4 (June 1982), 12.
	<i>Director of OSS Visits the DOE Center for Computer Security.</i>	Vol. 5, No. 3 (September 1986), 1.
	<i>DoD Computer Security Center.</i>	Vol. 1, No. 4 (June 1982), 29.
	<i>DOE Applications of the Trusted Computer System Evaluation Criteria.</i>	Vol. 3, No. 3 (March 1984), 54.
	<i>DOE Center for Computer Security Report.</i>	Vol. 2, No. 3 (May 1983), 20.
	<i>DOE Headquarters Report.</i>	Vol. 6, No. 2 (July 1987), 2.
	<i>DOE Hosts DOE/NCSC Computer Security Council.</i>	Vol. 5, No. 1 (February 1986), 7.
	<i>DOE Order 1360.2 Implementation Verification Guidelines.</i>	Vol. 3, No. 3 (March 1984), 12.
	<i>Editorial.</i>	Vol. 4, No. 3 (April 1985), 1.

Anonymous.	<i>Edward V. Badolato Sworn in as Deputy Assistant Secretary for Security Affairs.</i>	Vol. 5, No. 1 (February 1986), 1.
	<i>Eighth Conference Schedule Changed.</i>	Vol. 4, No. 2 (January 1985), 1.
	<i>Future Events.</i>	Vol. 4, No. 3 (April 1985), 1.
	<i>GAO and NBS Achievements in Contingency Planning and Computer Security.</i>	Vol. 2, No. 3 (May 1983), 50.
	<i>General Accounting Office Views on Management of Micro-computers.</i>	Vol. 3, No. 3 (March 1984), 68.
	<i>Graphical Network Representation Model and Generic Network Model.</i>	Vol. 8, No. 1 (April 1989), 21.
	<i>Guide on Selecting ADP Back-Up Processing Alternatives.</i>	Vol. 5, No. 3 (September 1986), 8.
	<i>Guidelines for the Center for Computer Security Newsletter.</i>	Vol. 4, No. 2 (January 1985), 2.
	<i>Harder Serving as Executive Secretary to DOE Computer Security Group.</i>	Vol. 5, No. 1 (February 1986), 7.
	<i>Headquarters Personnel Changes.</i>	Vol. 6, No. 1 (March 1987), 6.
	<i>Headquarters Reports.</i>	Vol. 1, No. 4 (June 1982), 2.
	<i>Headquarters Reports.</i>	Vol. 2, No. 3 (May 1983), 7.
	<i>Headquarters Reports.</i>	Vol. 3, No. 3 (March 1984), 6.
	<i>Headquarters Task Force Assisting the Computer Security Program Manager.</i>	Vol. 5, No. 1 (February 1986), 7.
	<i>Hoover Takes Over as Assistant Secretary for Defense Programs.</i>	Vol. 4, No. 2 (January 1985), 2.
	<i>The Impact of Security Controls on Computing Productivity.</i>	Vol. 3, No. 3 (March 1984), 65.
	<i>Implementing R&D.</i>	Vol. 1, No. 4 (June 1982), 27.
	<i>In Memoriam [William S. Heffelfinger].</i>	Vol. 5, No. 1 (February 1986), 8.
	<i>Inspector General Report.</i>	Vol. 1, No. 4 (June 1982), 31.
	<i>Inspector General's Recent Findings.</i>	Vol. 2, No. 3 (May 1983), 52.
	<i>Interested in Attending the Next CSSO Training Class?</i>	Vol. 6, No. 3 (December 1987), 1.
	<i>Interview with a CSOM [Bob Caldwell—Oak Ridge Operations Office].</i>	Vol. 6, No. 3 (December 1987), 8.
	<i>Interview with a CSOM [Ray Surface—Albuquerque Operations Office].</i>	Vol. 7, No. 2 (December 1988), 2.
	<i>Introductory Remarks.</i>	Vol. 2, No. 3 (May 1983), 4.
	<i>Introductory Remarks.</i>	Vol. 3, No. 3 (March 1984), 4.
	<i>Key Notarization System.</i>	Vol. 1, No. 4 (June 1982), 28.
	<i>Keynote Address.</i>	Vol. 2, No. 3 (May 1983), 5.
	<i>Keynote Address.</i>	Vol. 3, No. 3 (March 1984), 5.
	<i>LAVA for Computer Security—Distribution Update.</i>	Vol. 6, No. 2 (July 1987), 16.

Anonymous.	<i>Lawrence G. Martin Appointed Classified Computer Security Program Manager.</i>	Vol. 5, No. 1 (February 1986), 2.
	<i>Leon Breault is Classified Network Security Projects Manager.</i>	Vol. 5, No. 1 (February 1986), 4.
	<i>Let's Not Re-Invent the Wheel.</i>	Vol. 7, No. 1 (July 1988), 26.
	<i>Link ACE—A Data Link Access Control & Encryption System.</i>	Vol. 3, No. 3 (March 1984), 61.
	<i>Link ACE Used for DOE CPCI.</i>	Vol. 3, No. 1 (July 1983), 1.
	<i>Local Hard Disk Secured by Safe.</i>	Vol. 6, No. 1 (March 1987), 6.
	<i>Los Alamos Gives Congressional Testimony about "414" Hackers.</i>	Vol. 3, No. 2 (November 1983), 2.
	<i>Martin Manages Order 1360.2 and Circular A-71 for DOE.</i>	Vol. 2, No. 1 (August 1982), 1.
	<i>Meeting Scheduled.</i>	Vol. 1, No. 2 (Autumn 1981), 1.
	<i>Meet the DOE Center for Computer Security Staff.</i>	Vol. 6, No. 2 (July 1987), 15.
	<i>Michael B. Seaton Appointed Acting Director of the Office of Safeguards and Security.</i>	Vol. 5, No. 1 (February 1986), 1.
	<i>Model Security Guidelines for Microprocessors and Word Processors Issued by OSS.</i>	Vol. 5, No. 1 (February 1986), 8.
	<i>Model Threat Statement to Be Issued.</i>	Vol. 5, No. 1 (February 1986), 8.
	<i>NBS Special Publication on the Way.</i>	Vol. 5, No. 3 (September 1986), 10.
	<i>Network Security.</i>	Vol. 1, No. 4 (June 1982), 6.
	<i>Networking at Lawrence Livermore National Laboratory: Past, Present, and Future.</i>	Vol. 3, No. 3 (March 1984), 44.
	<i>Newly Formed Computer Security Advisory Group Meets in Kansas City.</i>	Vol. 5, No. 1 (February 1986), 4.
	<i>News from Headquarters.</i>	Vol. 7, No. 1 (July 1988), 1.
	<i>Nominations Are Being Accepted for Upcoming Vacancies on the DOE Computer Security Group Steering Committee.</i>	Vol. 5, No. 1 (February 1986), 7.
	<i>O'Brien Replaces Caudle.</i>	Vol. 4, No. 2 (January 1985), 1.
	<i>Office of Safeguards and Security Reorganization Announced.</i>	Vol. 5, No. 1 (February 1986), 6.
	<i>OPMODEL Contract Awarded.</i>	Vol. 2, No. 2 (November 1982), 3.
	<i>OPMODEL—The Security Aspects of Phase II.</i>	Vol. 3, No. 3 (March 1984), 28.
	<i>Orosz Coordinates 1360.2 for "Mini-operations Office."</i>	Vol. 2, No. 2 (November 1982), 2.
	<i>Password Policy, User Responsibilities, and DOE Computer Systems.</i>	Vol. 6, No. 3 (December 1987), 14.
	<i>Personnel & Projects.</i>	Vol. 8, No. 1 (April 1989), 1.
	<i>Personnel Changes and the Center.</i>	Vol. 5, No. 1 (February 1986), 7.
	<i>Personnel Changes at DOE Headquarters.</i>	Vol. 1, No. 3 (Winter 1982), 1.
	<i>Personnel Screening, Procedural & Administrative Safeguards.</i>	Vol. 2, No. 3 (May 1983), 27.
	<i>Possible Illegal Attempt to Access DOE Computer System.</i>	Vol. 5, No. 1 (February 1986), 7.

Anonymous	<i>Product Announcement—CSSO Tool-Kit Item—Inventory Control Software.</i>	Vol. 7, No. 1 (July 1988), 3.
	<i>Program Generates Passwords.</i>	Vol. 2, No. 1 (August 1982), 4.
	<i>Programmatic Controls for Classified and Unclassified Software Applications.</i>	Vol. 2, No. 3 (May 1983), 13.
	<i>Protection of Computer Security, Perspective from a Program Office.</i>	Vol. 1, No. 4 (June 1982), 15.
	<i>Publication & Presentation Highlights.</i>	Vol. 8, No. 1 (April 1989), 3.
	<i>Questionnaire Results.</i>	Vol. 6, No. 3 (December 1987), 7.
	<i>Recent Center Activities.</i>	Vol. 4, No. 2 (January 1985), 2.
	<i>Richard W. Carr Appointed Sensitive Unclassified Computer Security Program Manager.</i>	Vol. 5, No. 1 (February 1986), 3.
	<i>Risk Analysis—A Realistic, Automated Tool.</i>	Vol. 3, No. 3 (March 1984), 45.
	<i>Risk Analysis Program.</i>	Vol. 2, No. 3 (May 1983), 37.
	<i>Risk Analysis—Three Approaches.</i>	Vol. 1, No. 4 (June 1982), 18.
	<i>The Sandia Experience.</i>	Vol. 1, No. 4 (June 1982), 30.
	<i>Sandia National Laboratories Albuquerque Security Testing—A Case History.</i>	Vol. 3, No. 3 (March 1984), 49.
	<i>SCOMP Is Rated A1.</i>	Vol. 4, No. 3 (April 1985), 2.
	<i>Secure Accreditation Systems.</i>	Vol. 1, No. 4 (June 1982), 21.
	<i>Security Considerations of the OPMODEL.</i>	Vol. 2, No. 3 (May 1983), 41.
	<i>Security Group to Meet June 18-19.</i>	Vol. 1, No. 1 (Summer 1981), 4.
	<i>Security Guidelines for Microcomputers and Word Processors Issued by DOE Office of ADP Management.</i>	Vol. 5, No. 2 (May 1986), 2.
	<i>Security in the Office Automation and Word Processing Environment.</i>	Vol. 2, No. 3 (May 1983), 33.
	<i>Security of Distributed ADP Systems: Problems & Some Solutions.</i>	Vol. 3, No. 3 (March 1984), 37.
	<i>"Sensitive Unclassified Computer Security Program Compliance Review Guideline" Issued.</i>	Vol. 5, No. 2 (May 1986), 4.
	<i>Staff Changes at DOE Headquarters.</i>	Vol. 6, No. 2 (July 1987), 2.
	<i>Status Report on OPMODEL.</i>	Vol. 3, No. 1 (July 1983), 3.
	<i>Steering Committee for the 11th DOE Computer Security Group Conference.</i>	Vol. 6, No. 2 (July 1987), 8.
	<i>Steering Committee for the 12th DOE Computer Security Group Conference.</i>	Vol. 7, No. 1 (July 1988), 34.
	<i>Steering Committee Needs Two New Members.</i>	Vol. 5, No. 3 (September 1986), 3.
	<i>Subscription Renewal Form.</i>	Vol. 8, No. 1 (April 1989), 23.
	<i>Summary of Center's Annual Report.</i>	Vol. 1, No. 3 (Winter 1982), 3.

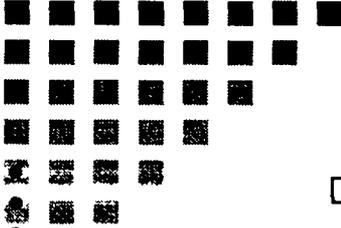
- Anonymous. *TEMPEST Standards for ADP and Word Processing.* Vol. 2, No. 3 (May 1983), 21.
Tempest-Approved Portable Microcomputer. Vol. 5, No. 2 (May 1986), 2.
Testbed System Incorporates KNF. Vol. 1, No. 2 (Autumn 1981), 1.
Time to Renew Your Subscription. Vol. 8, No. 1 (April 1989), 1.
Trusted Computer Systems Evaluation Criteria. Vol. 2, No. 3 (May 1983), 54.
Up Close and Personal—Alice Baker. Vol. 8, No. 1 (April 1989), 2.
Up Close and Personal—David Martinez. Vol. 8, No. 1 (April 1989), 10.
Upcoming CSSO Training Seminar. Vol. 8, No. 2 (August 1989), 19.
Update on NBS Electronic Bulletin Board. Vol. 6, No. 1 (March 1987), 6.
Using the Trusted Computer System Evaluation Criteria. Vol. 3, No. 3 (March 1984), 50.
Wanted: Articles & Article Ideas. Vol. 1, No. 4 (June 1982), 40.
WBCN Security Committee Meets in Kansas City. Vol. 5, No. 1 (February 1986), 6.
Who Are We? Vol. 8, No. 1 (April 1989), 1.
Will We See You in TX? Vol. 8, No. 1 (April 1989), 1.
Word Processor Security Policy. Vol. 2, No. 1 (August 1982), 1.
Workshop—Implementing DOE Order 1360.2 Management Control Process. Vol. 3, No. 3 (March 1984), 18.
10th DOE Computer Security Group Conference Keynote Speech. Vol. 6, No. 2 (July 1987), 3.
- Austin, Gene. *Pinellas Tests SCOMP.* Vol. 2, No. 2 (November 1982), 2.
- Augustson, Sharon. *An ADP Computer Security Classification Program.* Vol. 4, No. 1 (July 1984), 45.
- Bailey, Dave. *Attacks on Computers: Congressional Hearings & Pending Legislation.* Vol. 4, No. 1 (July 1984), 54.
Conference Wrapup. Vol. 4, No. 1 (July 1984), 63.
Quarterly to Be Forum. Vol. 1, No. 1 (Summer 1981), 1.
- Baker, Dan. *Hanford, Washington, Site of the 1985 CSG Conference.* Vol. 4, No. 3 (April 1985), 2.
Mode Switch Improves Hanford Supercomputer Security and Protection Efficiency. Vol. 7, No. 1 (July 1988), 21.
- Baker, Lara. *Partitioned Computer Networks.* Vol. 4, No. 3 (April 1985), 4.
Partitioned Computer Networks (reprint). Vol. 7, No. 2 (December 1988), 7.
- Baker, Shirley J. *ADP Security at Bendix Kansas City Division.* Vol. 5, No. 2 (May 1986), 3.
Ninth AESOP Operations Managers' Conference. Vol. 4, No. 2 (January 1985), 3.
- Bartich, Gail. *Writing Secure Application Code.* Vol. 7, No. 2 (December 1988), 11.
- Biles, Leon. *Microcomputers: Security's Problem Children.* Vol. 4, No. 1 (July 1984), 15.
- Black, Dave. *Tailoring System Logging for Security Needs in AOS/VS.* Vol. 7, No. 1 (July 1988), 32.
- Bogenholm, Sandra. *Memo: Computer Viruses and Personal Computers.* Vol. 8, No. 2 (August 1989), 8.

- Brand, Steve and Gerald Chichester. *New Ways of Thinking about PC and LAN Security.* Vol. 7, No. 2 (December 1988), 1.
- Brooks, Steve. *Security Compromises—What You Can Do.* Vol. 6, No. 2 (July 1987), 5.
- Brown, David C. *Computer Abuse and the Hacker* Vol. 4, No. 1 (July 1984), 6.
- Burnham, Blaine. W. *Highlights of the Ninth DOE/CSG Conference.* Vol. 5, No. 3 (September 1986), 3.
The Ninth DOE Computer Security Group Conference Convenes May 6-8, 1986. Vol. 5, No. 2 (May 1986), 1.
Results of DES Encryption Hardware Beta Test. Vol. 4, No. 1 (July 1984), 46.
- Burr, Elaine. *Computer Security—A People Problem.* Vol. 6, No. 2 (July 1987), 9.
- Camillo, Dottye. *Automated Office Support Systems (AOSS): Los Alamos Security.* Vol. 4, No. 1 (July 1984), 18.
A Case Study—Using an Incident Reporting System Approach. Vol. 4, No. 1 (July 1984), 20.
- Carr, Rick. *ADP Standards.* Vol. 6, No. 1 (March 1987), 8.
Sensitive Unclassified Computer Security Program Policy Revision. Vol. 5, No. 3 (September 1986), 6.
- Clark, Clara. *Risk Analysis for the Morgantown Energy Technology Center.* Vol. 4, No. 1 (July 1984), 37.
- Cohan, Lloyd. *Hard Disk Assembly (HDA) Degausser.* Vol. 7, No. 1 (July 1988), 8.
- Cole, Charles E. *Highlights of the 1988 Conference.* Vol. 7, No. 1 (July 1988), 1.
It's After Hours . . . Do You Know Where Your Modems Are? Vol. 4, No. 2 (January 1985), 3.
LLNL Octopus Network Provides Computer Security. Vol. 3, No. 2 (November 1983), 4.
Tenth Computer Security Group Conference Highlights. Vol. 6, No. 2 (July 1987), 1.
- Computing and Telecommunications Security Organization. *Computer Operations and Security at Martin Marietta Energy Systems in Oak Ridge.* Vol. 5, No. 2 (May 1986), 7.
- Condon, Richard. *ADP Security Education Program at the U. S. Department of State.* Vol. 4, No. 1 (July 1984), 59.
- Corynen, Guy C. *Questionnaire Aids Risk Assessment.* Vol. 1, No. 3 (Winter 1982), 1.
- Courtney, Robert H. *Protection for Sensitive and Other Valuable Data.* Vol. 7, No. 1 (July 1988), 14.
- Crass, Harold. *EDP Auditor's Role: DOE Order 1360.2.* Vol. 4, No. 1 (July 1984), 25.
- Cross, Darwin. *Installing a Secure and an Open Local Area Network System on a Single Cable Plant.* Vol. 7, No. 1 (July 1988), 16
- Crutcher, Richard and Ewing, Paul. *Broadband Network Sharing by Different Sensitivity Levels.* Vol. 6, No. 3 (December 1987), 10.
- Davidson, Barbara. *Digital PBX as a LAN.* Vol. 4, No. 1 (July 1984), 10.
- Dolven, Lyle. *A Management Information System for Computer Security Programs.* Vol. 6, No. 1 (March 1987), 8.
- Douglass, Charlene. *Computer Security Violations [Speakers].* Vol. 4, No. 1 (July 1984), 24.
- Duerre, Ken. *Automating Transaction Analysis for the WBCN.* Vol. 8, No. 1 (April 1989), 19.
- Duffy, Jim. *Computer Systems Contingency Planning.* Vol. 4, No. 1 (July 1984), 27.

- Egdorf, Harry W. *Center Will Evaluate SCOMP.* Vol. 2, No. 1 (August 1982), 2.
DES-based Software Is Available. Vol. 1, No. 3 (Winter 1982), 2.
- Favaron, Paul. *Baseband Local Area Networks.* Vol. 4, No. 1 (July 1984), 8.
- Fluckiger, J. D. *Notes From J. D. Fluckiger, Chairman of the Steering Committee for the Computer Security Group.* Vol. 5, No. 3 (September 1986), 7.
- Ford, Wendell. *Personal Identity Verification.* Vol. 5, No. 3 (September 1986), 4.
- Fraser, Gary. *Computer-Assisted Instruction in Computer Security at Rockwell—Rocky Flats.* Vol. 5, No. 3 (September 1986), 6.
- Garrett, Gary. *Software Piracy: Have You Broken the Law?* Vol. 7, No. 1 (July 1988), 17.
- Grosman, Lou. *Desktop Computer Security.* Vol. 8, No. 2 (August 1989), 7.
- Gurth, Bob. *In on a Virus Workshop, Out on a Tornado Warning.* Vol. 8, No. 2 (August 1989), 1.
- Harder, Duane. *What Is Your Center Doing for You?* Vol. 4, No. 1 (July 1984), 48.
- Harris, Lynn Massagli. *ANSI Data Management Security and Privacy Task Group.* Vol. 8, No. 1 (April 1989), 6.
Los Alamos Vulnerability Assessment (LAVA). Vol. 5, No. 3 (September 1986), 3.
Product Announcement—CSSO Tool Kit Item—Contingency Planning Guide. Vol. 7, No. 2 (December 1988), 6.
Tool Kit Items. Vol. 8, No. 1 (April 1989), 6.
- Heffelfinger, William S. *Security Milestone Lauded.* Vol. 4, No. 1 (July 1984), 1.
- Hofferth, Lyle. *I&E Standards and Criteria for Computer Security.* Vol. 5, No. 3 (September 1986), 9.
- Hogan, Carole B. *Protection Imperfect: The Security of Some Computing Environments.* Vol. 7, No. 1 (July 1988), 5.
- Huntzman, William *Computer Security Enhancement Review Program.* Vol. 8, No. 1 (April 1989), 13.
Computer Security Program Review Assistant. Vol. 8, No. 1 (April 1989), 14.
Knowledge-Based System in Computer Security. Vol. 8, No. 1 (April 1989), 16.
- Irion, Dennis L. *The Nature and Control of Compromising Emanation.* Vol. 6, No. 1 (March 1987), 7.
- Isaac, Irene. *Contingency Planning: Selecting Alternate Processing Support.* Vol. 5, No. 2 (May 1986), 5.
- Jacobson, Robert V. *Organizing and Conducting an Automated Risk Analysis.* Vol. 4, No. 1 (July 1984), 39.
- Jaehne, Edwin M. *Security and Productivity.* Vol. 4, No. 1 (July 1984), 32.
- Kidd, Duane and Grosman, Lou. *Word Processing Security at NRC.* Vol. 4, No. 1 (July 1984), 13.
- Killip, Scott. *TOKAY/BBS Serving the DOE Community.* Vol. 6, No. 3 (December 1987), 11.
- Kusserow, Richard P. *Computer Related Fraud and Abuse in Government Agencies.* Vol. 4, No. 1 (July 1984), 60.
- Lewis, Richard E. *NWCnet and WBCN Security Review Project.* Vol. 8, No. 1 (April 1989), 20.
Security in the OPMODEL Network. Vol. 4, No. 1 (July 1984), 49.
- Lewis, Richard E. and Smith, Marshall. *Wideband Communications Systems.* Vol. 4, No. 2 (January 1985), 1.
- Lindberg, Richard C. *SCOMP—A Class A1 Secure Operating System.* Vol. 4, No. 3 (April 1985), 6.

- Lloyd, Naomi, Morton, Don, and McClary, Jim. *Product Announcement: CRISK—Computer Risk Analysis Program.* Vol. 7, No. 2 (December 1988), 18.
- McClain, Bill. *Automated Badge System Implemented.* Vol. 2, No. 2 (November 1982), 1.
- McClary, Jim. *Book Review.* Vol. 4, No. 3 (April 1985), 1.
- McDonald, Chris. *Defending Against the Wily Hacker.* Vol. 7, No. 2 (December 1988), 1.
Reflections on an Internet Worm. Vol. 8, No. 2 (August 1989), 2.
- Mansur, Doug L. *The NCSC/DOE Computer Security Council: Opening Lines of Communication.* Vol. 6, No. 1 (March 1987), 2.
Update: DOE Computer Security Advisory Group. Vol. 6, No. 1 (March 1987), 9.
- Martin, Larry. *DOE Order No. 1360.2: Beyond Implementation.* Vol. 4, No. 1 (July 1984), 19.
Security of Office Automation. Vol. 4, No. 1 (July 1984), 12.
War Games—A Movie Review. Vol. 3, No. 1 (July 1983), 1.
- Martinez, David P. and Cheryl Steverson. *Overview of the Audit Log Analysis Package (ALAP).* Vol. 8, No. 1 (April 1989), 7.
- Massagli, Lynn. See Harris, Lynn Massagli.
- Mayerfeld, Harold N. and Troy, Gene. *An "Expert System" to Perform Knowledge-Based Risk Management.* Vol. 7, No. 1 (July 1988), 19.
- Mick, Steve. *Security Profile Inspector (SPI).* Vol. 8, No. 2 (August 1989), 4.
- Myers, Eugene D. *Network Security System Access Control in Network Partitioning.* Vol. 4, No. 1 (July 1984), 51.
- Nessett, Dan M. *Adding Central Authentication to DECNET/VMS.* Vol. 6, No. 2 (July 1987), 13.
Encryption Unit Used to Protect Resource Access. Vol. 3, No. 2 (November 1983), 1.
- Nizio, Eugene. *Personal Computer Security: "Are We Reinventing the Wheel?"* Vol. 5, No. 3 (September 1986), 4.
- Nolan, Michael J. *Contingency Planning for a Classified System.* Vol. 6, No. 3 (December 1987), 12.
- Poirier, Leo. *Computer Security Violations [Speakers].* Vol. 4, No. 1 (July 1984), 24.
- Price, Doug. *Computer Security and Risk Management.* Vol. 7, No. 1 (July 1988), 25.
- Redle, Karleen. *Articles of Interest [reviews].* Vol. 8, No. 2 (August 1989), 15.
The Editor Wants You. Vol. 8, No. 1 (April 1989), 23.
- Reid, Brian. *Lessons Learned from a Recent Rash of UNIX Computer Break-Ins.* Vol. 6, No. 2 (July 1987), 6.
- Revo, Lance E. and Figelski, Gary. *The Apocalypse of Western Technology: Transforming American Ingenuity into a Resource of the Soviet State.* Vol. 7, No. 1 (July 1988), 26.
- Robson, William M. *The Technologies of Communications: How They Are Changing Computer Security.* Vol. 6, No. 1 (March 1987), 4.
- Robson, William M. and Lewis, Richard E. *DOE Albuquerque Operations Office's SALSA Communications System: Can Red and Green Coexist on the Same Cable?* Vol. 6, No. 1 (March 1987), 5.
- Rosenblum, Harry. *Computer Security Training.* Vol. 7, No. 2 (December 1988), 13.

- Rosenblum, Harry. *Computer Security Training.* Vol. 8, No. 1 (April 1989), 4.
Introduction to CSSO Seminar Modules. Vol. 6, No. 3 (December 1987), 22.
Training Aids Available. Vol. 8, No. 1 (April 1989), 4.
Upgrading the Center Bulletin Board. Vol. 8, No. 1 (April 1989), 3.
- Santilli, Joseph V. *Sample Qualitative Risk Analysis for Small Systems.* Vol. 6, No. 3 (December 1987), 15.
- Sauer, Hank *Computer Security Conference Scheduled.* Vol. 2, No. 1 (August 1982), 1.
- Schultz, E. Eugene, Jr. *The Computer Incident Advisory Capability (CIAC).* Vol. 8, No. 2 (August 1989), 13.
- Shake, Tina and Vernon, D. L. *Savannah River Computer Security Conference.* Vol. 6, No. 3 (December 1987), 1.
- Smith, Col. Lloyd. *Disaster Recovery of a \$138-Million Fire.* Vol. 6, No. 2 (July 1987), 11.
- Smith, Suzanne T. *Book Review: Foiling the System Breakers by Jerome Lobel.* Vol. 5, No. 3 (September 1986), 8.
- Smith, Suzanne T. and Lim, Judy J. *Computer Security Evaluation Tools.* Vol. 4, No. 1 (July 1984), 36.
- Springer, Edward A. *Computer Security Initiative.* Vol. 2, No. 1 (August 1982), 2.
Current Status of the Link ACE Project. Vol. 4, No. 1 (July 1984), 49.
OMB Circular A-71: Comments and Update. Vol. 4, No. 1 (July 1984), 4.
- Springer, Ed and Dauelsberg, Lois. *Nevada Upgrades Badge and Clearance System.* Vol. 5, No. 2 (May 1986), 6.
- Stark, William W. *Broadband Local Area Networks.* Vol. 4, No. 1 (July 1984), 9.
- Steuerwalt, Michael. *We All Have Problems.* Vol. 7, No. 1 (July 1988), 4.
- Steverson, Cheryl. *Assurance of Software Security: From Design to Delivery.* Vol. 8, No. 1 (April 1989), 11.
- Stoll, Cliff. *What Do You Feed a Trojan Horse? Techniques for Solving Hacking Problems.* Vol. 6, No. 3 (December 1987), 2.
- Tipton, Hal. *New Security Need: Dial-Up Access Control in an Era of Connectivity.* Vol. 7, No. 1 (July 1988), 10.
- Weynand, Joseph A. *Software Controls Access.* Vol. 3, No. 1 (July 1983), 2.
- Williams, L. K. *Degaussing Disc Assemblies.* Vol. 3, No. 1 (July 1983), 2.
- Wood, Bernard E. *File Auditing on VAX/VMS.* Vol. 6, No. 2 (July 1987), 10.
- Working Group D—
Computer Security
Risk Management Model
Builders Workshop *A Framework for Measuring Computer Security Risk.*
Compiled by Peter Browne. Vol. 7, No. 2 (December 1988), 14.
- Wrenn, Charles M. *Computer Security Violations [Chair].* Vol. 4, No. 1 (July 1984), 21.
- Zawadzki, Andrew J. *Security, Hardware Maintenance Contracts, and You.* Vol. 7, No. 1 (July 1988), 10.
- Zetlin, Bryan A. *Security for Personal Computers (PCs).* Vol. 4, No. 2 (January 1985), 4.



DOE Center for Computer Security Toolkit Items

N-4/89-144 *CSSO Tool Kit Guide on Contingency Planning for Multiuser Computer Systems*
Author: Lynn Massagli Harris

This guide was developed to meet DOE regulatory requirements for contingency planning and to aid DOE Computer Systems Security Officers (CSSOs) in creating, maintaining, and testing a contingency plan for their ADP facilities.

CCS-TK/90-001 *CSSO Tool Kit Item: Guide to Monitoring Resources*
Author: Michael Steuerwalt

This guide is intended to help Computer Systems Security Officers (CSSOs) monitor classified ADP system resources. It discusses how to use several other Tool Kit products (*monfile*, *view*, *forms*, and *fairsmpl*) in an effective program for monitoring files for waste, fraud, and abuse. In addition, it offers general suggestions about resource monitoring.

CCS-TK/90-002 *CSSO Tool Kit Item: monfile version 2.5, view version 2.2*
Author: Michael Steuerwalt

This product contains programs to help select files on DOS systems to monitor for waste, fraud, and abuse and to view the contents of files (as required by DOE Order 5637.1).

CCS-TK/90-003 *CSSO Tool Kit Item: fairsmpl*
Author: Michael Steuerwalt

This product contains a program to help make fair random selections of items from a given set of items. Such selections are useful in monitoring computer resources.

CCS-TK/90-004 *CSSO Tool Kit Item: forms*
Author: Michael Steuerwalt

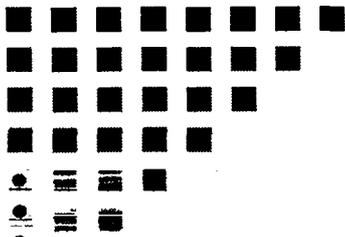
This product contains a program to generate multiple copies of a master document (like a form letter), inserting lines of text into the copies at places specified in the master.

LA-UR-88-3011 *Generic ADP Security Plan Guide for Multiple Computer Systems with Identical Security Properties*
Authors: William J. Huntman and Sandra J. Bogenholm

This guide is intended to aid Computer Systems Security Officers (CSSOs) in considering site-specific security issues as well as all of the requirements of DOE orders, other relevant orders, the draft *Standards and Criteria*, and good security practices, and to assist Computer Systems Security Officers (CSSOs) in writing an acceptable security plan for multiple ADP systems with identical security properties.

LA-CC-88-10 *Inventory Control Software*
Author: Lynn Massagli Harris

This software provides Computer Systems Security Officers (CSSOs) with an automated means of creating and maintaining an inventory of the hardware and software components for their classified computer systems and is intended to comply with inventory control requirements specified by DOE Order 5637.1, *Standards and Criteria*, and good computer security practice.



Toolkit Items (continued)

Password Generator

The password generator consists of user documentation and a floppy disk with the executable program and supporting data files. Because the program contains an implementation of the DES encryption algorithm, the software may not be provided to foreign nationals nor exported outside the U.S.

LA-UR-88-3012 *Shared System ADP Security Plan Guide*
Authors: William J. Huntzman and Sandra J. Bogenholm

This guide is intended to aid Computer Systems Security Officers (CSSOs) in considering site-specific security issues as well as all of the requirements of DOE orders, other relevant orders, the draft *Standards and Criteria*, and good security practices, and to assist the CSSO in writing an acceptable security plan for a shared system.

LA-UR-88-3013 *Stand-alone Personal Computer and Word Processor ADP Security Plan Guide*
Authors: William J. Huntzman and Sandra J. Bogenholm

This guide is intended to aid Computer Systems Security Officers (CSSOs) in considering site-specific security issues as well as all of the requirements of DOE orders, other relevant orders, the draft *Standards and Criteria*, and good security practices, and to assist the CSSO in writing an acceptable security plan for a stand-alone, single user personal computer or word processor system.

LA-CC-8913 *uuencode, uudecode, bcdecode for DOS*
Author: Michael Steuerwalt

The programs *uuencode* and *uudecode* are Pascal implementations for DOS of Mark Horton's Unix algorithms. They are used to ship binary files across ASCII transmission links. The program *bcdecode* is a Basic implementation for DOS of a simple version of the *uudecode* algorithm, intended for bootstrapping the *uudecode* executable to a machine that has no Pascal compiler.

Evaluate the privileges of all remaining accounts. Most users only need [the standard VMS] TMPMBX and NETMBX privileges. Excessive privileges can override the best security you have. Remember that you can set up a privileged account for someone to use on a limited basis (e.g., 9-12 a.m. Mondays) while reverting to few or no privileges the rest of the time.

- Reduce access rights where possible.

Be especially careful with Network, Remote and Dialup access. Consider restricting by hours of the day or days of the week (e.g., 7 a.m. to 10 p.m. M-F) and then relaxing access restrictions for the minority who need more access.

- Review passwords.

Monitoring passwords is difficult to do without a software tool, since VMS has no decryption mechanism. Make sure the length is AT LEAST six characters—a three-character password can be broken in six minutes, and a four-character one would take approximately forty-five minutes. A six-character password would require about fifty-two [sic] days to crack. Also set the LIFETIME parameter on passwords.

Volume Setup

This phase will ensure that the data stored on the disk volumes is appropriately protected. The system manager must

- Set up volume initialization, ownership, and protection.

Many sites have system ownership of all volumes and mount volumes with system ownership. This allows all users access to data they may not have a need to access. The first gate to set up is volume ownership—make sure all public volumes are set up as other than system owned. The second gate comes when the volume is mounted; by mounting it just for group, or yourself, you can restrict access to the data.

- Set up directory ownership and protection.

Very few directories should have world write access . . .

Very few directories should have world write access—only a few users should be able to add and delete data.

- Locate files owned by deleted accounts.

Removing files owned by deleted accounts reduces the risk of a new account with the same UIC as a previously deleted one inheriting data for which it should not have access.

- Locate files with ACLs.

Directories and files that are important enough to require an ACL are important enough to have their ACLs reviewed at regular intervals.

- Locate files and directories with world access.

Files and directories with world access are an invitation to browse; at their worst they are an invitation to disaster since they are easy to corrupt or destroy. Carefully evaluate any file or directory with world read/write access.

- Reduce ownership and protection anomalies.

Files should have the same owner as their parent directory and most files in a directory should have similar protection settings. Investigate any apparent anomalies and make sure a mistake hasn't been made.

Evaluation

Perhaps one of the best ways to evaluate your security settings, after having performed the previous three setup steps and reducing access and privileges, is to run with the new settings and see who complains. Then you can systematically increase or alter access rights and privileges in order to reach the optimum for your environment.

Monitoring

This phase ensures that any changes are caught quickly, and any required corrective action is taken. Monitoring must take place at three levels of frequency:

- Daily
- Weekly
- Monthly

"Daily" monitoring requires the checking of a number of items frequently. For instance, you should do a quick review of the accounts to determine what, if any, changes have occurred in the last period. You can also check the pertinent SYSGEN parameters. You can check the ownership and protection setting for all files on the system disk. And review the OPERATOR.LOG file to detect security-related events. These are just a few of the elements that require frequent checking.

"Weekly" monitoring requires the less frequent checking of additional items. You can check the file, directory, and volume ownership and protection of volumes containing shared data. You should also analyze SYS\$ERROR:ERRLOG.SYS for security-related events.

"Monthly" monitoring refers to the much less frequent checking of ownership and protection of files, directories, and the volume containing private or non-shared files.

Education

This phase ensures that all staff are aware of the corporate concern for system and data security. The greatest impediment to increased security is the lack of awareness by system users and management of the potential pitfalls of having a poorly secured system. This can be partially addressed by ensuring everyone receives copies of pertinent articles and publications, that the staff responsible for security have the opportunity to attend related symposiums and that all users are aware of the importance upper management places on security. No matter how perfectly your system is designed, if the users of that system are not aware and [do not] take seriously the need for security, your system will be at risk.

Electronic Authorization System (EAS)

Gary Rich
 Administrative Data Processing
 Los Alamos National Laboratory

During the first forty years, Los Alamos National Laboratory developed manual and automated information systems to serve the needs of individual organizations. As time went by, manual systems gave way to automated systems. Because there was very little integration among the various manual systems, very little integration existed in the automated systems. Common data were entered separately into different information systems causing duplication of effort, time delays, and diminished accuracy. Laboratory managers had almost no access to these information systems while the various service organizations had limited access. All information and reports were the by-products of information systems designed to perform routine processing and paperwork.

After a review of the information systems in the Laboratory, it was decided that the fundamental cause of the Laboratory's data problems had been a long-term lack of adequate information policy. Coupled with conflicting interpretations of directives and regulations, this resulted in few standards of accuracy, a lack of timeliness, few procedures to assure validity, and a lack of methods and designation of responsibility for assessing the effectiveness of those information systems. Data sources, input formats, definitions, and input schedules lacked management control. Finally, there was limited oversight of parochial information systems scattered throughout the Laboratory.

In 1980, top management saw a need for a Laboratory-wide Management Information System. To satisfy this need, the Laboratory formed the Information Systems Steering Committee (ISSC). The ISSC's primary function was to set a common direction for all administrative data processing in the Laboratory. Understanding the need for a staff which could carry out the committee's wishes on a day-to-day basis, the ISSC formed

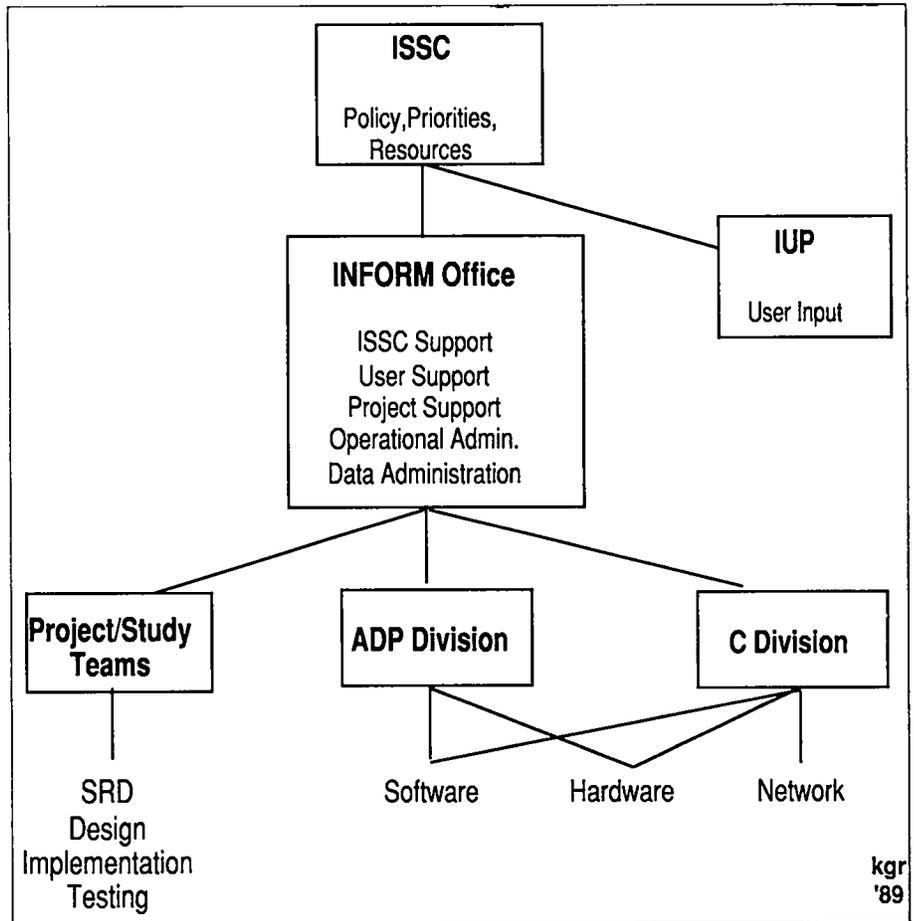


Figure 1. Current Functional Responsibilities.

the INFORM (INformation FOR Managers) Office. The participating organizations and their responsibilities are shown in Figure 1. One of the first administrative systems commissioned through the INFORM office was the Electronic Authorization System (EAS).

The Administrative Data Processing (ADP) Division developed EAS to ensure that access to sensitive administrative information is allowed only for those users with prior authorization. EAS restricts user access to the VAX/VMS operating system and provides application systems with information to control the release of sensitive information. EAS meets its objective by providing a structure to those users who need to access information in order to perform their jobs (e.g., payroll). EAS also provides an inherent access authority based on user attributes such as job code (e.g., Division Leader). In addition, default authorities can be set up for large groups of users (e.g., Labora-

tory employees can look at their own Employee Information System data). EAS consists of six major modules. (See Figure 2.) The modules and their major functions are as follows:

Authority Control Services—Data Flow Diagram (DFD 1.0)

The primary objective of this group of processes is the update (and review) of the attribute and authority data stores. This data is used by the Menu Controller to dynamically control user access to menu options and the application systems. The major sub-modules in the Authority Control Services are as follows:

- **The Authority Editor** allows the user to add, change, delete, or modify assigned authority records. This is the major tool for building individual authority structures. EAS allows a user to assign only authorities that he/she already possesses. Additionally, the

acceptance, the user is passed to the menus. If access is denied, the user is removed from the system.

- **Build Menu Structure** accepts a request from various sources and responds with the appropriate menu. This process is used to allow easy, dynamic navigation through the menu system. After the user selects a request from the system through the menu, control is passed to the Transfer Control Process.
- **Transfer Control** accepts a menu option from an application program and verifies that the user selected an appropriate option. The process ensures both that 1) the option exists and 2) the user is eligible to use the option. This is achieved with the authority and attribute structures to determine which privileges the user has been granted. If the user has the authority to execute that request, then the request is granted.

Data Administrator Services (DFD 3.0)

The major objective of this group of processes is to allow the data administrator (located in the INFORM office) to keep various EAS information current including menu definition and Laboratory line management structure. It allows the data administrator to add, change, delete, or modify a wide range of EAS tables. Development of these processes allows the flexibility necessary to meet the changing needs of each application system. Each of the major table updates (not previously presented) is included below for use in describing the major file structure of EAS.

- **Update Menu Description File** is used by EAS to define the menu which each user will see. Included in this file are the menu options, authority required to execute the option, and the action that will be taken if a user selects the option. The action can be an application executable, a linked subroutine, a menu, or a command procedure.
- **Update System Name File**—The System Name file contains each valid application system, as well as a short

code for each. This information is used by EAS to display proper headings on menus and system utilities.

- **Update Authority Codes**—The Authority Codes file is used by EAS to define all valid authority codes. Included in this file are the short codes as well as the code definitions. Although some codes have universal meanings in all application systems, most are defined by a specific application system.
- **Update Management Levels**—The Management Levels file is used by EAS to define the line management structure used by EAS. This file is based on valid job codes and can be modified to meet the needs of each application system.
- **Update Job Code Default Authorities**—The Job Code Default Authorities file is used by EAS to ensure that users at different levels receive enough authorization to do their jobs without having to be granted authorization on a one-by-one basis.

Text Display Services (DFD 4.0)

The major objective of this group of processes is to provide for the use and maintenance of help screens, bulletin boards, and other text applications. Help screens and bulletin boards are so similar in function and construction that the same modules will serve both purposes.

Utility Services (DFD 5.0)

The major objective of this group of processes is to provide either utility programs (invoked by application programs) or other functions which are needed by the system. Only the major functions in this category are included below.

- **Assume Alias**—This process allows the user to assume the "look" of another user without providing update privilege. This process is essential for system testing as well as problem definition for the INFORM office consultants.

- **Organizational Domain**—This function provides the application system with information about the organizational domain the user currently has. The domain describes each organization for which the user is considered a line manager. This information is essential for the application programs when deciding what information can be released.

Notification Services (DFD 6.0)

The major objective of this group of processes is the addition, deletion, and approval of notifications. A *notification* is defined as "the process by which an application program can notify a valid user of some action." That action might be the request for signature on a Travel Request or acceptance of an employee to attend a training class. The major processes in the Notification Services are

- **Maintain Notifications**—This process is the brain of the notification process. It receives a notification request from the application process, logs it into its central files, and processes it through a wide variety of media. Planned output formats include hardcopies delivered by mail, electronic mail, and telephone dial-out.
- **Approve Notifications**—This process allows the user the opportunity to approve an outstanding notification. The user can approve/disapprove a notification request in either summary or detailed form. If the user requests that a detailed review be made before approving/disapproving, EAS will make the application present this review.

Report Services (DFD 7.0)

The major objective of this group of processes is to provide report services to itself, as well as to other application systems. These reports are aimed at three major user communities: application developers, INFORM office personnel, and Laboratory-wide users.

- **Application Development Reports** are used by application developers to determine who is using the system, what parts they are using, and how often they are using it. This allows the

application development team to expend its effort in those areas with the greatest payback.

- **INFORM Office users**—These reports are used by the INFORM Office to determine who is using the system, what parts they are using, and how often

they are using it. In addition, these reports provide the INFORM Office the ability to look at any problems, potential problems, or security problems that the system may be having.

- **Laboratory-wide user**—The major reports for the Laboratory-wide user show the authority/attribute assignments which have been made.

Gary Rich is the Group Leader of ADP-3 and has been a developer of INFORM systems for eight years.

VAX Security 1

The Center for Computer Security neither evaluates nor recommends commercial products; we do, however, try to provide information that we feel may be useful to those in the field. The following two articles are based on individuals' experience with SECUREPAK, a set of utilities useful in the setup, verification, and monitoring of an optimally secure VMS system.

David Tenorio
Sandia National Laboratories
Albuquerque, NM

As system manager for the COMPUSEC Database at Sandia, I am required to create and maintain all data pertinent to computer security. This includes an active record of all memos, DOE correspondence, and information involving computer security. A separate list is kept of all computer systems at Sandia and the responsible parties associated with these systems. In the process of identifying key personnel, a verification is done to identify the clearance level and identity of personnel.

In examining SECUREPAK, I intended to evaluate and critique the software to see if it would be a good utility tool to add to the VAX world to help in locating security trouble spots and ensuring data integrity within my system. The COMPUSEC Database consists of 15 disks and an estimated 80,000+ files. With this amount of data, it is imperative to have a means of continuous file monitoring with the flexibility to generate comprehensive reports. SECUREPAK permitted me to locate potential vulnerabilities to my system and readily rectify these "problem" areas.

The "Account/UAF" report generated simple reports that identified old and unused accounts, a rights-list summary, privileged users, misowned home directories, and login failures. Other reports generated by this feature dealt with "File Structure" which reported tree directories, shared directories, abnormal files, misowned files, files with ACLs [Access Control Lists], and mismatched directory/file protections.

The one report of particular interest to me during the evaluation was the "Password Management" report, consisting of expired passwords, aged passwords, minimum length accounts, generated password accounts, lifetime accounts, locked passwords, disabling of forced password changes, and guessable password accounts.

In my opinion, this software package is a very useful product and promotes a more secure system for system managers. System managers should not be overburdened with timely monitoring procedures and security concerns. This software package reduces the time spent on these responsibilities and allows more time for the basic purpose of processing data.

SECUREPAK is an integrated set of reporting, query, and modelling functions allowing a more secure VAX/VMS system. It enhances and maintains an existing security setup and provides a more comprehensive audit (in a timely, efficient manner) for my computer system. This software allowed me to effectively meet the specific needs of the Computer Security Division at Sandia.



VAX Security 2

David P. Martinez
Los Alamos National Laboratory

I am a network manager for a predominately research and development organization at Los Alamos National Laboratory. Our local area network (LAN) consists of a diverse assortment of workstation and PC hardware platforms interfaced (*i.e.*, networked) through a host cluster of VAX computers. We operate in an unclassified environment, processing unclassified information. Our LAN network is in turn interfaced to the Los Alamos National Laboratory Integrated Computing Network through the open/unclassified partition.

As network manager, a role which I have just recently assumed, I am responsible for various aspects of our network, one being security. Well, as one might imagine, this task can be quite demanding in direct proportion to the complexity of those systems integrated into the network. Needless to say, there are some trade-offs between security and the flexibility and accessibility of networked systems and their data. Having to make trade-offs amplifies the system administrator's task. I will not address those issues at this point except to suggest that those considering security versus functionality tradeoffs should perform vulnerability and risk assessments to determine what level of risk is acceptable at their sites.

As we are emphatically reminded through media coverage of viruses, worms, computer break-ins, and other malicious actions, computer systems—in particular networked systems—are vulnerable to

many forms of attack. Ideally, we would like operating systems that, through-and-from-within-themselves, ensure security against such attacks. However, given current technology and the computer security problems we face today, as security administrators, we must develop a security program consisting of

- documented policies and procedures,
- training and awareness programs, and
- software and hardware tools and utilities to enhance protection of our computing resources.

As network manager of our LAN, one of my first experiences with computing system attacks was the WANK (Worms Against Nuclear Killers) worm. My awareness of such computer system attacks led me to search, early on, for tools that would permit me to evaluate, identify, and correct security vulnerabilities in our network. Coincidentally, as I was testing a demo package of a product called SECUREPAK, developed by DEMAX, VMS systems at Los Alamos National Lab, accessible over the Internet, were being attacked by the WANK worm. My immediate responsibility became to determine the state of security on our VMS systems and to determine if they had been attacked and if so, the consequences. Getting a quick profile of overall VMS system security using conventional VMS security tools can be difficult and time consuming.

However, using DEMAX's SECUREPAK I was able to get a good profile of our VMS systems to identify potential security vulnerabilities (Figure 1). The first SECUREPAK report that I generated was the "General Security Summary" which evaluated our VMS accounts, access to our data files and directories, and ACLs, among other things, and generated a summary of these items along with a User Authorization File (UAF) rating on our VMS account and a disk security rating. The report was generated within seconds, and provided me with valuable general information about our VMS environment, such as

- the number of privileged accounts,
- the number of old and unused accounts, and
- world access to files.

The type of report generated by the General Security Summary utility is shown in Figure 2.

Other summaries provided me with more detailed information on

- accounts with expired passwords,
- privileged accounts,
- accounts with guessable passwords, and
- system security parameter defaults in SYSGEN.

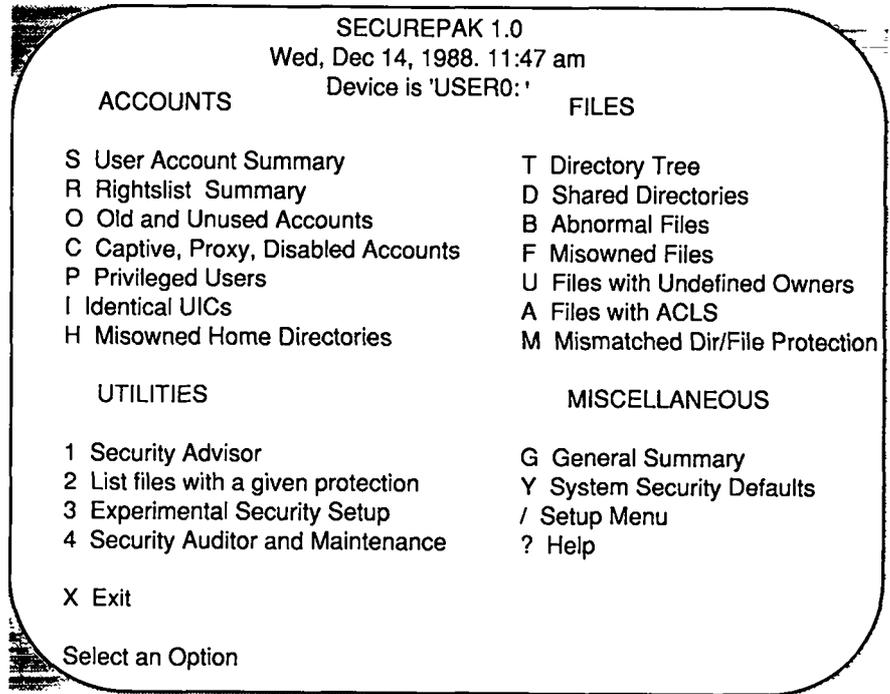


Figure 1. Main Menu

GENERAL SECURITY SUMMARY			
Fri, July 22, 1988. 2:39 pm			
Device is 'DISK\$VAXSAMPLE:'			
Total Accounts	:	32	Total Files : 2877
Privileged Accounts	:	16	Total Directories: 177
Old & Unused Accounts:	:	10	Files with Acls : 38
Duplicate UICs	:	1	Dirs with Acls : 1
Identifiers	:	7	Misowned Files : 189
World DELETE Files	:	21 (0.73%)	
World WRITE Files	:	23 (0.80%)	
World READ Files	:	888 (30.87%)	
Group DELETE Files	:	484 (16.82%)	
Group WRITE Files	:	1103 (38.34%)	
Group READ Files	:	2362 (82.10%)	
World READ Directories:	:	109 (61.58%)	
Uaf Security Rating	:	53%	
Disk Security Rating	:	80%	

Figure 2. General Security Summary

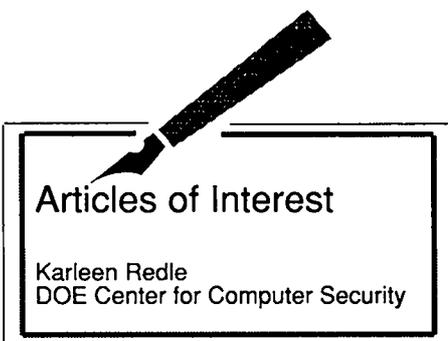
In general, within a few minutes I was able to acquire a quick profile of the state of system security relative to our accounts, data files, and system security defaults and thereby to eliminate unjustified risk factors in the system. Because we are a research and development group, where some projects are short lived or tasks are subject to periodic change, we also need to systematically review the following:

- 1) our accounts to assure that the account attributes (e.g., privileges, network access, etc.) are appropriately

set for the task(s) the owner of the account is working on, or more importantly, whether accounts should be expired or not;

- 2) ACLs to assure that they permit appropriate access to the appropriate owner; and
- 3) overall system and data security to ensure overall system security coherence.

While my experience with SECUREPAK has been limited to the demo package, it has proved to be a valuable tool in our environment. Using SECUREPAK, I was able to get a quick snapshot of our VMS systems' security. I was able to identify and correct potential vulnerabilities. In general, I acquired a much improved perspective of the state of our system resources and how they were protected. I expect to find that other features, particularly the feature that allows system security profiling, will enhance our overall security.



Most individuals who responded to our questionnaire felt reviews of articles on computer security are useful. Therefore, we will continue to review such articles. Some of you requested information on *Computers & Security*. It is published eight times a year by Elsevier Science Publishers. Additional information may be obtained by writing Elsevier Advanced Technology, Journal Information Center, 655 Avenue of the Americas, New York, NY 10010. *Computer Fraud & Security* is also published by Elsevier.

General security issues

Booty, Frank. "Local Area Networks" *Computer Fraud & Security*, 11 (1989), 11-14.

Booty considers local area network (LAN) security still in its infancy. The greater sophistication of PC LAN product users, the greater difficulty of protecting PC data from theft or destruction, and the flood of utilities available for DOS all pose security problems. Not only does one have to worry about access to the PCs on a

network; there is the potential for unapproved nodes to be added or network data traffic to be monitored. With physical access security assured, one must still be concerned about logical access to the data. Of the two basic logical architectures supported on PC LANs today, peer-to-peer is less secure because of the lack of centralized data storage across the network. Client-server architectures have more sophisticated security. "Centralized disk storage architecture provides a more straightforward platform for control of user access and of back up operation than a peer-to-peer architecture." Because "workstations constitute the highest security risk in a LAN" one should consider using keyboard lock devices. Access monitoring can help considerably; "administrative procedures and responsibilities remain critical to [security support's] total success."

Feuerlicht, J. and Grattan, P. "The Role of Classification of Information in Controlling Data Proliferation in End-User Personal Computer Environment." *Computers & Security*, 8 (February, 1989), 59-66.

Feuerlicht and Grattan propose classification of business information combined with relevant control measures as a means of managing data proliferation. They discuss a number of methods for classification of information. "The proliferation of PCs throughout organizations has resulted in end-user computing with a

number of unresolved planning and control issues. Among the most pressing problems is the impact on computer security." The authors feel external threats have been overstated while insufficient resources are devoted to addressing internal threats; "lack of awareness of the value of data processed in the end-user environment [is] an area of major concern."

PC software seldom has safeguards against unauthorized access and generally accords too little attention to control and auditability of business applications. Although classification of information by the data originator together with supplying information on a "need-to-know" basis can constitute a practical and cost-effective way to improve data security in the end-user environment, there are limitations to this approach. "For example, individual fragments of corporate data released on different requests may not pose a security risk but information derived from combining the data may be of strategic importance to the organization."

Feuerlicht and Grattan review some methods for classification of information and conclude that "Protection measures which correspond to the level of classification of information will minimize the risks of unauthorized disclosure, modification or misuse of data. An important indirect benefit is the increased awareness of information security issues."

Rees, Frank. "Australian Roundup: Research into Secure Transaction Services." *Computer Fraud & Security*, 11 (1989), 5-6.

"Telecom Australia's Research laboratories (TLR) have demonstrated a secure mailing system as part of research into secure transaction services. It consists of a standard Unix mailer and additional programs to implement the security features." One program uses the sender's secret key information to sign mail messages, and a second program uses the publicly available key to check that the signature is valid. "Combined, these programs provide a message integrity and a data origin authentication service."

Sidrow, Christina L. "Freeze, System Manager! Part 1: Developing a Case for Computer Crime," *DEC Professional* (September, 1989), 60-66.

Sidrow suggests that system managers should prepare themselves for the possibility of a break-in by reading company policy regarding crisis management and then by implementing procedures for those on the crisis management team. The system manager also needs to know how to use the tools available on the VAX (and from vendors) to monitor users and terminals. Sidrow says you must be able to prove that a crime has been committed when there is a break-in. It is important to be familiar with state laws so you can show what violations took place and who was probably responsible.

She goes on to suggest how to build a case and what legal savvy is essential (knowledge about hearsay evidence, the best evidence rule, etc), and the article concludes with a reminder of some commands that enable system managers to monitor activity easily and regularly.

Sidrow, Christina L. "Freeze, System Manager! Part 2: Apprehending a Computer-Crime Suspect" *DEC Professional* (October, 1989), 62-65.

Sidrow stresses the need for a system manager to know what usual computer activity is and to be able to produce documentation to substantiate a definition of normal activity if required for a court hearing. Some VAX/VMS capabilities are

briefly mentioned, together with steps to follow if there is a break-in. Being able to provide evidence of a break-in is extremely important.

Spencer, Cheryl England. "Data Safety." *MacWorld*. (January, 1990), 142-149.

Spencer indicates that "Any good security scheme works by providing a hierarchy of increasingly restrictive levels of access. An example of how levels of access can be restricted is the interaction between a network and a relational database where records can be locked so only specified users can access information and applications are also protected by the network software's security features.

Spencer discusses encryption and points out some potential problems in relying on it though she feels it is "an ideal solution" for those who send data out-of-house over modems or dedicated data lines, or on floppy disks. Hardware devices and software programs can prevent anyone else from having access to your Mac. In addition, there are programs that password-protect the Mac and others that lock individual hard disk partitions. For multi-user environments, there are a couple of new products that allow you to "set various levels of file, folder, and disk access for individual users, and both let you protect applications from being copied or deleted . . . [one program] even lets you restrict access to desk accessories, printers, and modems and prevent unauthorized applications from being installed."

Viruses and Virus Protection

Highland, Dr. Harold Joseph. "Random Bits & Bytes: The Italian or Ping-Pong Virus," *Computers & Security*, 8 (April, 1989), 91-94.

The Ping-Pong virus infects a system upon booting; any unprotected floppy disk you copy to will be infected. The virus takes over three sectors, the first of which contains virus code; the second "contains a copy of the original boot sector." Examination of the virus revealed two abnormalities: the "reinfection of the virus and a peculiar wiping out of data on the screen." Highland suggests more than one way to cure an infected disk.

Highland, Dr. Harold Joseph. "Random Bits & Bytes: The Marijuana Virus Revisited," *Computers & Security*, 8 (April, 1989), 97.

Analysis of a disk infected with the marijuana virus shows it to be dangerous, "Not only will it infect the standard floppy disk but it will also take over the master boot record of a hard disk. . . . It infects a disk during a read or write operation."

Menkus, Belden. "The Computer Virus Situation is not Encouraging." *Computers & Security*, 8 (April, 1989), 115-119.

Menkus disagrees with those he considers "misinformed experts" who do not consider viruses a serious threat. To those who feel the problem would disappear if media coverage ceased, he responds that like the hacker problem which did not go away when publicity ended, the virus problem will not disappear. He feels there are no quick fixes because the problem is complex. Freeware and shareware products "are of questionable value and integrity" and are themselves open to virus infestation. Commercial products often do not work "or [they] perform unreliably."

When reporters who do not understand computing or information security processes interview self-designated experts on computer viruses, misinformation proliferates.

Menkus doesn't agree with those who feel those responsible for viruses are relatively innocent pranksters with limited capability to do anything malicious or sophisticated. He feels hackers are increasingly more sophisticated and in some cases intentionally destructive. At best, virus developers are unconcerned "about the consequences of their actions; there is no reason to believe that they will end their activities in the near future. There is, instead, every reason to believe that the computer virus problem will continue to grow, create a variety of information integrity and control problems, and eventually force major changes in the ways in which both operating system and application software are structured."

Menkus did not feel any of three proposed protective approaches [isolating viruses by partitioning a single micro-computer into numerous virtual machines, issuing program code in nonmodifiable CD-ROM form, and issuing programs in the form of conventional ROM microchips] would be feasible on a broad scale before the 1990s. In the meantime, it would be wise to design trap interfaces to prevent unmediated direct access from outside sources to disk content and to segment "the interconnection of data-center-resident DASD—and the program that manages the use of this space—to reduce the possible impact of virus infection of mainframe-supporting memory."

There are two tests Menkus suggests should be met by quality virus-combating programs: they should be suitable for those in a conventional business environment and they should enable users to establish and maintain a virus-free computer environment. Currently available products do not prevent infection; they simply detect and report it. They are difficult to use, which means many users won't bother. Nor do the products allow for possible advances in virus design, especially the possibility of increasing complexity in viruses.

Menkus feels current anti-virus products fail because they do not seem to be designed for individuals who

- use computing only as a means to an end,
- are interested in the uses of the data rather than in the intricacies of the software used;
- want simple-to-install, easy-to-use software that does not add overhead or otherwise interfere with getting their jobs done; and
- want protection that ensures a more trustworthy environment but are indifferent to the multiple levels of protection offered by some products.

Menkus gives details of weaknesses in currently available products; the article concludes with a concern that the end of an open computing environment is imminent.

Reports from the Victims:

Radai, Yisrael. "The Israeli PC Virus." *Computers & Security*, 8 (April, 1989), 111-113.

People first became aware of the virus when programs they had run successfully in the past were suddenly too big to fit into memory; once the problem surfaced, someone soon discovered that each time an EXE file was executed, "its size grew by 1808 bytes (later it became evident this continual increase in size was the result of a bug in the virus). Infected COM files also grew, but only one time. Radai defines a virus as

program code, usually attached to the beginning or end of a program file, which contains the following:

(1) A part which is responsible for self-replication, i.e., which causes propagation of the virus by copying the entire virus code (or a modified version thereof) to other program files (or to some other region of a disk) at certain opportunities (usually upon execution of the already infected program or execution of the to-be-infected program).

(2) A part which performs some action (often a destructive action on files or on entire disks) when a certain event takes place (e.g., upon execution of an infected program on a certain date or after the virus has replicated itself a certain number of times).

He explains how viruses propagate, mentions several other viruses that hit Israel, and comments on the spread of misleading information by inaccurate and sensationalized reporting by the press. Like Menkus, he believes we will see new viruses that can circumvent current antiviral programs. "The best countermeasures seem to be hardware protection devices to prevent infection, and checksum programs to detect infections before any destructive action is committed."

van Wyk, Kenneth R. "The Lehigh Virus." *Computers & Security*, 8 (April, 1989), 107-110.

An especially destructive virus infected several hundred floppy disks at Lehigh University shortly before Thanksgiving vacation in 1987. It copies itself "from disk to disk at least four times," then destroys the contents of the original disk. The rapid spread of the virus was attributed to floppy disk sharing. Because of what appears to be a bug in the virus code, multiple copies of the virus were loaded into memory when programs that invoke COMMAND.COM were run.

The Computing Center now uses notchless floppy disks where possible and encourages users to write protect their floppies. Commercial anti-virus software has been evaluated; implementing some form of virus protection is being considered.

Webster, Anne E. "University of Delaware and the Pakistani Computer Virus." *Computers & Security*, 8 (April, 1989), 103-105.

The University of Delaware has about 500 microcomputers in general access microcomputing facilities; the need for an open computing environment "makes many of the security recommendations suggested for business use inappropriate" in this university environment. Webster indicates that only a couple of dozen users had files corrupted by the Brain virus. She suggests that "the site-operating procedures already in place . . . helped account for the generally low infection rate.

- 1) All DOS boot disks have write protect tabs or are 'notchless' disks.
- 2) Site applications software (e.g., WordPerfect, Lotus 1-2-3) generally is not bootable.
- 3) Systems are booted with their own DOS disk (e.g., site system #1 uses DOS disk #1, system #2 uses DOS disk #2 etc.).

An Overview of Kerberos: A Network Authentication System	4
Gordian Key: Access Management System	4
Removing the Mystery from the OSE I&E Program	6
CSSO Training Seminar	9
Attention	9
The Keys to Security—SAVE-ME	10
New Video	Insert 1
Index of Available Videos	Insert 2
Index of Articles—DOE Center for Computer Security News	Insert 5
DOE Center for Computer Security Toolkit Items	Insert 15
Electronic Authorization System	12
VAX Security 1	15
VAX Security 2	15
Articles of Interest	17

LALP-90-21

Address Correspondence to

Newsletter, MS E541
DOE Center for Computer Security
Los Alamos National Laboratory
Los Alamos, NM 87545
(FTS) 843-0444
(505) 667 0444

This newsletter is published as an account of work sponsored by the United States Government. Neither the United States Government, nor the University of California, nor any of their employees, nor any of their contractors, subcontractors, or their employees, make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe on privately owned rights. Reference herein to any specific commercial products, 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 the University of California. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government nor the University of California, and shall not be used for advertising or product endorsement purposes.

Los Alamos National Laboratory, an equal opportunity/affirmative action employer, is operated by the University of California for the United States Department of Energy under contract W-7405 ENG-36



Submit articles or ideas for articles to

Newsletter Editor
DOE Center for Computer Security
Los Alamos National Laboratory
Los Alamos, NM 87545
(505) 667-0444 (FTS) 843-0444
FAX No. (FTS) 843-7626
Confirmation No. (FTS) 843-7777

or submit electronically to

kgr@LANL.gov

Submissions should conform to these guidelines:

- Articles should be 1200 words or less (If you write an article of greater length that you feel is timely and of significance to computer security personnel, it may be possible to print it in installments. Please phone the editor to discuss such submissions: 505-667-0444 or FTS-843-0444).
- Articles should be written for the technically literate layman. Preference will be given to articles of a technical nature.
- Include photos or drawings for illustration or elucidation. Please indicate what software was used to produce graphics.
- Include a brief biographical sketch.
- Articles should not promote commercial products
- Submit articles in both hard-copy and digital format (ASCII files on Macintosh diskettes are preferable).

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