DCI Director of Central Intelligence

FOR OFFICIAL USE ONLY

Computer Security Technology Assessment Report

An Executive Overview

Prepared for
The Deputy Director of Central Intelligence
by the
Computer Security Technology Panel

DCI/ICS 84-4036
December 1984

Computer Security Technology Assessment Report

An Executive Overview

PREFACE

In support of the Deputy Director of Central Intelligence, in June 1984, the Director of the COMPUSEC Program established a Computer Security Technology Panel to address what could be done, in the near term, with existing computer security technology to improve the security of critical systems currently operating within the Intelligence Community. Specific emphasis was given to three areas of security: authentication of users to an automated system, accountability of user actions in such systems, and labelling of information handled by them.

Over a six months period, members of the Technology Panel met on six different occasions to evaluate state-of-the-art technology against known vulnerabilities within Intelligence Community computer-based systems. This report presents the findings and conclusions of the Technology Panel and presents specific recommendations for future actions.

TABLE OF CONTENTS

MEMBERS OF THE DCI'S COMPUTER SECURITY TECHNOLOGY PANEL

STAT [redacted]
CHAIRMAN

STAT [redacted]
COMPUSEC PROJECT DIRECTOR

STAT [redacted]
EXECUTIVE SECRETARY

Organization	Principal	Alternate
Los Alamos National Laboratory	Dr. Lara Baker	
STAT NSA	[redacted]	
National Bureau of Standards	Dr. Dennis Branstad	Ms. Elaine Barker
STAT NSA	[redacted]	
FBI	Mr. William E. Kardash, Jr.	Mr. Franklin Standifer
Federal Emergency Management Agency	Dr. John LaBarre	Mr. Bruce J. Campbell
OUSDRE	Mr. John J. Lane	
STAT CIA	[redacted]	
Aerospace Corporation	Mr. Carroll Melkerson	
Naval Intelligence Command	Captain Phil McKnight	
Department of State	Mr. Lynn McNulty	Mr. Richard Condon
STAT DIA	[redacted]	
System Development Corporation	Mr. Howard E. Rosenblum	
DARPA	Dr. Steve Squires	
Chemical Abstracts Service	Dr. Ronald Wigington	

EXECUTIVE OVERVIEW

Report of the Technology Panel

INTRODUCTION

This is the executive overview of the report of the Technology Panel of the DCI's Compusec project. It offers the DCI a series of action-oriented recommendations that he can use to improve the security status of critical systems and to assist system managers of Community automated information systems. It addresses primarily the short term "quick fix" actions that can be promptly initiated. When these technology oriented recommendations are arrayed against the identified vulnerabilities of the critical systems and the threat against them, it can lead to a plan for significant security improvements. By extension, it also addresses key ingredients that should be included in the planning for and implementation of systems coming into the inventory.

The views expressed here are those of the individual Panel members who participated as skilled practitioners of the information system art. Specifically the views may not reflect the position of the organizations from which the Panel members were drawn.

CONTEXT

We address three issues which were selected for the specific attention of the Panel: authentication of users to an automated system, accountability of user actions in such systems, and labelling of information handled by them. Two of the three--accountability and labelling--are primarily software issues; the third, authentication, involves specialized hardware as well as accompanying terminal-level and host-level software.

Although we were told that the critical systems did use commercially available hardware and software, neither the technical details nor the operational names of the "critical systems" were made available to the Panel. This impeded our ability to relate our experience with various hardware/software combinations to system-specific suggestions for remedial actions to the critical systems. There is consequently a risk that our observations and intuitions will be incorrect, with the result that our recommendations may be slightly off-target.

Notwithstanding the arms-length arrangement and lack of specific details, our comments and recommendations below are based on the collective knowledge of the Panel and on its composite experience with many systems installed elsewhere. We believe that the DCI's critical systems, even though implemented to handle security sensitive information, are not likely to be very different from those of our experience.

TECHNOLOGY IN GENERAL

Since there is a temptation to believe that technology can readily be invoked to fix a wide class of computer-related problems, some general observations are in order.

Some aspects of security safeguards for automated infomation systems have long been understood; e.g., TEMPEST, physical protection, COMSEC. However, those safeguards which depend on software processes and/or a combination of software features plus supporting hardware features do not yet have a well-established foundation such as that found in the COMSEC area. Thus, there is not yet a wide variety of off-the-shelf products that can be simply "dropped in" to achieve some significant gain in security protection. Therefore, we conclude that

A. In the near term the DCI can not expect there to be a plethora of sophisticated technology that can be readily applied to the problems of his critical systems.

On the contrary, we conclude that

B. The DCI should expect to utilize low-level technology and management/administrative actions that can be promptly applied for important security improvement over the short term, i.e. 2 to 4 years.

The first order quick fix is not even technology, but rather upgrading installed systems to the level of guidance now regularly supplied to Community contractors; all systems should be brought into compliance with security safeguards that are well understood and readily employed, e.g., proper generation and management of passwords.

Such procedural, administrative, and in-hand technology approaches must be exploited prior to seeking elegant technical "magic solutions" to security shortfalls.

The explosive growth in technology indicates that ongoing attention must be given to security safeguards; it is not and will not be a static issue. Dramatically new operational circumstances will arise and require new approaches to security policy and corresponding safeguards. For example, computer terminals are being connected to broad-band local area networks, and the COMSEC protective mechanisms are being incorporated directly into each terminal. In contrast, key generators traditionally have been protected in locked physical spaces. Again, newer terminals--especially the so-called smart ones--have local storage which may include removable media such as floppy discs and permanent disc storage; thus, the protective mechanisms that are now required in the main computer will in the future have to be implemented in each terminal as well.

SOFTWARE

Since many desirable security safeguards must eventually be implemented in either the system's so-called "operating system software" or in other specially designed software packages, some specific observations and cautions in regard to software upgrades and modifications are essential.

Retrofitting an existing system with appropriate software to provide security safeguards is not only a potentially major task, but it also may have collateral consequences unrelated to the software task proper; e.g., restructuring all the computer files or the database. Moreover, only a few software products have been evaluated by the Computer Security Center, although a number of vendors (both hardware and independent software houses) do offer software products that might be useful in the critical systems.

Given the present state of art, however, with regard to software security, we conclude that

C. Comprehensive security safeguards as implied by the Guidelines of the Computer Security Center can not be retrofitted to existing installed hardware/software configurations.

Moreover, there may be substantial deterrents against doing major software upgrades especially on old hardware; e.g., existing maintenance contracts for vendor-supplied software, lack of an in-house programming group or one of sufficient expertise to do the job, operational restrictions against changing the software (such as interconnect arrangements), lack of a stand-alone machine separate from the operational one on which to do software development (the so-called Life-Cycle-Support facility), a too-small operational hardware configuration to accommodate new software.

Therefore, given the schedule and funding risks attached to major software modifications in the critical systems, plus the possibility that mission support might be disrupted, we recommend that

1. The DCI direct that an economic cost-benefit analysis be submitted to him for any proposal that seeks to retrofit extensive technical safeguards to an existing system by modifying its vendor-supplied software, as opposed to an expedited equipment upgrade bringing with it new safeguards in both hardware and vendor software.

This recommendation addresses proposals for specialized modifications to software whose operational life is limited, and to vendor software for which improved products can be made available but may require new hardware. [In this regard, SEE: Recommendations 27 and and 28.] Software changes may be needed to install some safeguards that we have suggested in other recommendations (e.g., machine-generated passwords) but even then, a careful cost analysis is warranted.

In this regard, it should be noted that both computing technology and computer science are both very dynamic with the result that the sophistication of the threat against computer systems, especially networked systems, tends to increase rapidly over time. Therefore, the "security lifetime" of an installed computer system is likely to be much shorter than the amortized economic lifetime. We conclude that

D. Equipment may have to be upgraded or replaced more frequently in order to maintain an adequate threshold of security protection against the developing threat.

<><><><><><><><><><><><><><><><><><><><><><><><><><><><>

Our recommendations are grouped by topic and presented below. For each topic there is a short background discussion; and a short commentary or explanation is interspersed between many of the recommendations.

SECURITY COMPLIANCE

Background

Technology cannot be a panacea for security vulnerabilities; every dimension of security must be attended as well, e.g., physical security COMSEC, personnel security. Such things are well understood in contrast to those safeguards that are implemented in hardware and/or software. Moreover, the latter safeguards tend to be technically intricate and their need tends not to be appreciated.

Since automated-information-system security safeguards of any kind are defensive in nature and do not directly contribute to mission performance, COMPUSEC generally has a low level of visibility and priority at management levels. Thus, decisions tend to favor operational and mission obligations, especially when it comes to funding decisions.

Recommendations

We recommend that

2. The DCI task his Compusec project to review the documented assessments of the critical systems, to report within 90 days where his critical system(s) is (are) deficient relative to the "best documentation" available for implementation of security safeguards, to report what actions can be taken to bring his system(s) into compliance, and the cost to do so.

Various guideline documents exist for specifying broad and comprehensive security practices in computer systems, e.g., CIA's Contractor Security Manual, DIA's DIAM 50-4. In general these all derive from DCID 1/16. For the initial examination, we mean by "best documentation" the most

comprehensive and current guidance that can be assembled, whether it be material that has been prepared for internal use, for contractor use, or is a combination of the above. However, recently updated documents that may be available from other (external to the agency) sources should also be examined.

Although the DCI might have tasked his system managers to make the reviews, it is expedient to task his Compusec project in view of the work that it has already accomplished.

3. **The DCI task each system manager to make similar compliance checks on an annual basis, and to take such actions as may be necessary to bring his system(s) into compliance with the then existing best guidance and documentation.**

4. **The DCI (concurrently with [2] above) cause to be prepared a Community standard security-guidelines document that will become the standard required of each present and new system within the Community, both at initial operational status and on periodic examinations thereafter.**

The DCI's "Safeguards document" is a start on such a comprehensive "Computer System Security Manual," but it must be supplemented with or reference sources of information about other dimensions of system security, e.g., generation and management of passwords, handling of audit trail information, assignment of management responsibilities. Much of this can come from extant documents if they are consistent, complete, contain all relevant terms, assignments of responsibility, etc. Documents to be examined for relevant other information include ones from CIA, DIA, NSA, probably CSC, perhaps DODCI, probably NBS.

5. **The DCI have DCID 1/16 updated and revised to remove any anomalies and limitations related to obsolescent technologies and their operational employment. To the maximum extent possible, the policies should be technology independent and permit interpretation in the environment of contemporary technology.**

New technology--and uses of it--have appeared that DCID 1/16 did not anticipate. For example, it overlooks communications networks between computers, and the data networking of personal computers. Moreover, technology has raised policy issues that are not addressed in the most recent edition of DCID 1/16.

However, we caution that

E. System managers must promptly institute security improvements that can be made now, and not await updated policy guidance.

AUTHENTICATION

Background

In the contemporary environment of information systems that are networked not only within themselves but also among one another, the word "user" must be understood to include: (1) an individual at a terminal, (2) an internal software process executing in behalf of a person at a terminal, and (3) an external computer or communication system. In this discussion, the emphasis is on (1) with some consideration for (3). The process aspect [item (2)] is largely a matter of trusted software for which the Computer Security Center is the national focal point; trusted solutions to the process authentication issue can not be expected to be operationally deployed in the near term, i.e. 2 to 4 years.

In the present state of development of the art, the DCI can not expect elaborate and technically complex schemes for authenticating system users to be available for presently installed computer and system architectures. In general, such schemes will be most needed when multilevel-secure systems become operationally widespread. However, he can expect the development of authentication devices that measure some biometric feature of a person (e.g., fingerprint, retinal pattern) and of devices that depend on something that the individual must possess (e.g., magnetic card, smart card). Each such device will have different operational appeal and shortcomings; but all have the same attribute that integration into the terminal and the automated system per se is required.

Recommendations

We recommend that

6. The DCI reiterate his requirement that DIA take the Community lead for the authentication issue; and

Specifically task DIA to promptly examine possibilities for utilizing "low-level" technology to install or to improve personal authentication procedures in the critical systems, and to make recommendations as appropriate to system managers.

The technology for installing devices at terminals to do personal authentication is not quite here, but significant improvements can be made promptly through administrative and procedural means. Examples of such "low-level" technology include: (1) the use of daily authentication codes which are made available to an individual upon reporting to duty, together with corresponding internal software changes to maintain such code tables in encrypted form; (2) the proper generation, management and periodic changing of passwords; (3) the automatic disconnection of an idle terminal after a prescribed period of time.

7. **The DCI task NSA to promptly issue guidance on the proper generation of and management controls for passwords; and task system managers to implement such guidance within 180 days.**

8. **The DCI task DIA to conduct a comprehensive comparative study to evaluate various approaches to authentication, taking into account the best information on each, the costs of each, and the operational environments of the systems for which the techniques will be used.**

Such a study should include such factors as:

- User convenience at the terminal. Does it force him to take some awkward or unusual action; does it require him to have or carry something; does it make a biometric measurement?

- Bottlenecks at the entry/exit to the facility if physical access to protected space is part of the scheme.

- Cost per terminal and per authentication object (e.g., individual, other system); device cost, integration cost and TEMPEST recertification costs all must be included.

- Perceived threat to the installation and/or system. Does an approach provide a cost/beneficial solution or will some techniques be an overkill for the anticipated threat?

- Sensitivity of the facility to be protected. How should the effectiveness of an authentication technique be related to system, facility, and information sensitivity?

- Availability of the technology to implement an approach. Is it here now, or is R&D or engineering development needed?

- The operational environment in which the device must function. For example, will the individual wear protective clothing during an authentication action, or will he have to function under extreme stress that would make some complicated approach unworkable, or might he be physically impaired or disabled? Is there risk of losing a physical object?

- Operational acceptance. Would it be acceptable to utilize an item to be left at the workplace, or invoked many times during an operational shift?

- The time to complete an authentication. Are some approaches so time consuming that individuals would be tempted to circumvent them, or would operational inefficiencies result?

- The technical consequences for system integration. In particular, what are the software consequences in the host system?

As appropriate, biometric techniques (e.g., retinal recognition) could be tasked to CIA.

Finally, the study should recommend the long-term executive agent to attend the authentication issue for the Community, and develop a requirements statement that can be incorporated into a system specification for Community procurements.

9. **The DCI task NSA to formulate and proceed with an aggressive program to examine new physical-object techniques; e.g., smart cards, magnetic cards, (so-called) ignition keys.**

10. **The DCI direct DIA to accelerate its program for investigating authentication devices (including the studies above) to assure that high-confidence personal-user authentication devices are available and fully integrated into commonly used Community systems by 1990.**

11. **The DCI provide funding wedges now for procurement of personal authentication devices that promise to be in the $500-$1000 range by the late 1980s or very early 1990s.**

Techniques such as retinal pattern recognition, smart cards, ignition keys, etc. could be available and fully integrated into operational systems in the late 1980s or early 1990s with proper programmatic emphasis. Based on background briefings to the Panel, we believe that present per-terminal costs will decline to $2000-$3000 by 1987-88 and into the $1000 or less range no later than the early 1990s.

LABELLING

Background

The technical issue is to associate the proper set of security labels with each database, file, or record in a computer system (or possibly with individual data element components in any one of them); and to assure that such labels accompany the information as it moves elsewhere, e.g., displayed, printed, handed-off to a communication system. As such, it is primarily a software issue and can have significant collateral consequences; e.g., installation of a comprehensive labelling system might require restructuring all the databases, files, or records.

With regard to the host computer software aspects, labelling is an especially troublesome software issue because retrofitting existing systems may require modification of not only the operating system software but also database management software. Either undertaking could be a major undertaking. In the short run (i.e., 2 to 4 years), there may be little that can be done, but such a conclusion is very

dependent on system hardware/software details. For some systems, it may be that there are newer database management systems that could be installed and would provide some capability for associating security labels with information. [In this regard, SEE: Recommendations 27 and 28.]

For some systems, there may fortuitously exist some software capability to accommodate labelling, but any actions to exploit such an opportunity will be system dependent. Given the minimal knowledge provided to the Panel about the systems, we can not offer specific suggestions.

In the long run, so-called trusted systems are expected to provide labelling capability, but they will have to be certified to B-1 (or better) by the Computer Security Center. One system (MULTICS) is a candidate for a B-2 rating but it is specific to a vendor's machines that are not widely used in the Community. However, products from other vendors have been submitted to the Center with the expectation that a rating of at least B-1 will be obtained. While evaluation of them is not yet complete, such systems clearly offer significantly better safeguards than software presently installed in the field, and should be considered for near-term installation. [In this regard, SEE: Recommendations 27 and 28.]

We, therefore, conclude that

F. *There may exist near-term (i.e., 2 to 4 years) opportunities for providing one or more of the critical systems with some labelling capability; but any decision to do so is system specific and must take account of possible collateral consequences; e.g., complete restructuring of the files, disruption of mission support, retraining of operators and/or users, the necessity to replace hardware or upgrade the configuration of presently installed equipment.*

There is a second nontechnical operational aspect of great importance; namely, does the information now in the critical systems carry the proper security labels? For example, a decision may have been made for a dedicated system not to associate labels with information, on the grounds that the entire facility and all users function at the same classification. It is unlikely, but possible, that a similar decision would have been made for a dedicated or compartmented system; but the Panel was not given such information.

If the critical systems have not captured labelling information and/or have not associated it with the substantive information in the database, then the near-term outlook (i.e., 2 to 4 years) is likely to be bleak because of the intellectual effort to assign classification labels for all items of information and because of the corresponding effort to enter such information into the databases, files, and records. The best that could be done--but it may represent an important security advance--is to build simple labelling conventions into the software that outputs information to terminals, communication systems, other software

processes, and printers. Even this may be a major software undertaking and we caution against undertaking it without a thorough examination of the consequences to the system, to user training, to operator training, to operational procedures, etc. The decision is very system dependent, especially with regard to possible side effects.

The only system for which a simple remedy appears possible is the dedicated one, all of whose users function with a uniform set of security labels. Paper could be preprinted with security labels; permanent physical security labels could be attached to each terminal; communication processors could be modified to attach security labels to all messages. Since the Panel did not have detailed information about the critical systems, this suggestion may already have been implemented.

When hardware/software configurations that can support full-scope labelling become operational, we conclude that

G. The Community is likely to find that it has not made the necessary investment in assigning labels to all computer-stored information; and

H. Will have to make a significant one-time investment to achieve such a state.

For classifying and labelling sensitive materials, the government uses a very complex schema to which there is no analog in business and industry; there, relatively simple classification and labelling schemes are satisfactory. Given such a business and industry view, computer vendors may not spontaneously develop systems that have the scope and flexibility to fully meet the DCI (and other government) labelling requirements. Thus, we conclude that

I. Labelling, in the complexity required by DCI systems, appears to be a security objective that will require government R&D support to achieve.

Furthermore, as systems internet with one another the necessity for a Community-wide standard set of security labels becomes more important, as does the need for having everything properly labelled. Technology is seen as offsetting a lack of standardization; but, in fact, the system designers need a more consistent schema than now exists.

Moreover, systems which internet must be mutually assured that security labels have not been perturbed in transit, nor has the association between the information and its rightful label been disturbed. This is the "label integrity" issue which has not yet been examined by the Computer Security Center. For some, perhaps all, of the critical systems, it may be possible to assure label integrity through the communication portions even though the internal (to the computer) aspect of labelling can not be accommodated.

Recommendations

We recommend that

12. The DCI task his Compusec project to review the documented assessments of the critical systems with regard to the technical opportunities that each has for incorporating some form of labelling; and to recommend within 180 days what near-term actions can be taken, at what cost, and on what schedule.

This examination must consider many software details of the various systems, include consideration of the difficulty and cost of taking such actions, and take account of new software products such as are referenced in recommendations [27] and [28]. It must also consider collateral effects, such as the need to restructure all databases, files and records. There should be some assessment of the improvement in security posture that can be achieved for the kind of labelling that might be done in each of the critical systems.

Although the DCI might have tasked his system managers to make the reviews, it is expedient to task his Compusec project in view of the work that it has already accomplished. The project may, however, require the cooperation of the system managers to provide technical details, especially of software, that may not exist in the documented assessments.

13. The DCI establish a requirement that no later than the end of FY 85 all information entered into general-user Community systems be accompanied by relevant security labels; and

Task system managers to implement this requirement in a way that will afford flexibility and adaptability in utilizing label information in the database when systems providing full-scope labelling become available.

The first part of this is to assure that all new information flowing into Community systems carries proper security labels. Otherwise, the situation outlined in conclusions [G] and [H] will continue unabated. Software, as well as operational or system, changes may be required; and therefore, implementation may depend on the outcome of recommendation [12] above. The phrase "general-user" is included in order that specialized or research systems that may not need security controls are not needlessly burdened.

The second part relates to future hardware/software replacements that will take place when B-1 systems become available. It is unlikely that the database, file and record structures in new equipment will be the same as in the old. Since label information acquired in the present systems may be represented differently in the new, and its association with the substantive information may be treated differently, it is important to take the steps now to facilitate conversion to new equipment at a later date.

It may not be possible to do a perfect job of planning for an equipment transition whose details are unknown, but the technical issue must be considered and a best-effort attempt made to assure transferability of label information and its relationship to database entries.

The Panel raised the question of security label standardization, but did not reach a satisfactory resolution to the issue. There may be some differences in meaning or usage of security labels that will have to be standardized. However, we know from our collective knowledge and experience that there is great consistency in meaning and usage of many security labels. Therefore, planning for and acquisition of security label information can proceed while resolution of any residual details is concurrently under way.

14. The DCI establish a requirement that all new Community systems designed or implemented after 1 January 1985 be able to (at least) capture and maintain security labels in association with the related information as it enters the system, and to do so in a way that will facilitate utilizing such security information for eventual full-scope labelling applications in B-1 or equivalent systems.

This is simply an extension of [13] to include new, as opposed to presently operational, systems. It must apply to R&D systems which are prototypes of operational systems. In this regard, note the "Background" discussion above [paragraph 3], and recommendation [30]. Jointly, they suggest that B-1 systems incorporating labelling should be available by 1988. Thus the collection of security labelling information in presently operating and soon-to-be-designed systems should begin as soon as possible.

If new systems are implemented in less than B-1 equipments, the same concerns for transferability will apply as in recommendation [13] above.

15. The DCI issue or cause to be issued a policy that requires security label integrity throughout communication networks.

Label integrity implies that security labels are guaranteed not to have been changed in transit through a communication network, and that the association between a message and its security labels has not been perturbed. It is a matter that needs to be examined, but has been dealt with in only one network (SACDIN).

In this regard, however, the Community should transition as soon as possible to communication processors (which handle plain-text material) that have been certified A-1 by the Computer Security Center.

16. The DCI task NSA to issue guidance on the vulnerability of security labels to traffic flow analysis.

There appears to be no doctrinal position on the matter. Traffic flow analysis of unencrypted security labels in transit through a communications network might prove to be an important vulnerability. Such a circumstance is likely to exist in packet-switched networks; for example, in the Defense Data Network, security labels will be in-the-clear at the node switches which are protected to only SECRET level. It is not apparent whether the issue is one of COMSEC or OPSEC; thus the matter might be appropriate to NSA or to system managers.

17. The DCI support R&D programs to develop automated schemes that can assist in determining classification of information as it is aggregated, disaggregated, or combined.

The so-called knowledge-based system is one technique to be examined. Such an approach might be able to mimic the activities of people in making security judgments about information.

=====

ACCOUNTABILITY

Background

The issue is to equip a computer-based information system with an array of internal record-keeping processes that collectively can be used to do such things as monitor the operational and ongoing security status of the system, conduct a damage assessment in case of a security breach, trace the sequence of events/actions taken by users (personal, process, other system) in case of a security breach, and detect/identify illegal actions by a user or an attempted penetration. The technique is commonly referred to as "audit trails."

Like labelling, it is largely a software matter with consequences primarily for the operating system software. Unlike labelling, there are business and industrial needs for systems of audit trails so that the DCI and his system managers can expect some commercial capabilities to be available.

Because of the software dominance, the near-term actions are limited to administrative/procedural ones plus exploitation of whatever audit trail capability that the installed critical systems might happen to have.

Recommendations

We recommend that

18. The DCI task system managers to identify and report within 90 days what audit data is now collected, how it is used, what tools for analyzing the data might make audit data more useful, and what audit capability may exist within their systems for potential use, but is not presently used.

Many vendor-supplied operating systems include audit trails for such things as accounting and resource charge-back. We believe that much more relevant activity data is, or could be, collected and exploited in present systems for security assurance purposes.

19. The DCI task system managers to institute procedures for maximally exploiting the audit data which is collected or could be collected; and that he take steps to have appropriate analytic tools and capability provided to the system managers.

20. The DCI task the CIA to take the Community lead for the accountability issue; to assemble working groups as may be necessary to identify technical, operational or policy aspects; to make recommendations to DCI for establishment of new policy; and to conduct a study of the accountability issue.

The study should examine such matters as:

- Types of information that can be collected.
- Security relevance of such information.
- Threats against which audit trails can protect.
- Operational requirements.
- Standards for what will be audited.
- Standards for representation of the audit trail.
- Processing standards for audit trails.
- Development of conventional audit trail techniques.
- Development of knowledge-based systems for auditing.
- Development of appropriate work stations for auditors.
- Development of an on-line auditing capability.
- Development of mechanisms for the security auditor to control the system when needed.
- Development of the appropriate operational concepts for the audit trail process (e.g., one- or two-man control).
- Development of analytic tools for the security officer to examine audit data.

The study should develop the required conceptual and technical foundation for a comprehensive set of audit trails, and a requirements statement that can be incorporated into a system specification for Community procurements.

Policy issues that will require attention include:

- The dependence of audit trail details on system aspects.
- One- or two-man control of access to audit trail information.
- The authority of the audit team to intrude on the system operational mission in case of trouble.
- The nature of actions to be taken in case of detected penetration attempts.
- The security audit positions required per system, and the manning profile for the audit team.
- A statement of responsibility and authority for the audit team.

Operational details include:

- The operational concept that will assure that audit trails will function as intended in an operational system and provide the security protection expected.
- An examination of the tradeoff between the necessity for ongoing operation of the system in its operational support vs. security actions to be taken in case of security compromise or detection of a penetration.

=====

GUARD TECHNOLOGY

Background

Several organizations have sponsored projects to develop a so-called Guard device. It sits astride a communication channel into or out of a computer, and allows only information with specified security labels to pass. It behaves, so to speak, as a security filter.

Although the devices were designed for specific applications, it appears that they could be exploited for some security aspects of the critical systems. At least one of them could be available as a commercial product.

Recommendations

We recommend that

21. The DCI have conducted a comprehensive state-of-art survey of the several Guard projects under way or completed.

The study should examine such details as:

- The availability of operational equipment.
- The flexibility for monitoring different combinations of security labels.
- Any special hardware/software details that such equipments might impose on cooperating computer and communication systems.

22. The DCI task system managers to prepare an implementation plan for the incorporation of Guard (or equivalent) technology into those systems which are serving "subscribers" of different levels of access.

A "subscriber" may be an individual, a terminal, or another system. When the level of access is not uniform, Guard technology should be considered a prominent option for security improvement.

=====

CERTIFICATION AND ACCREDITATION

Background

The process of certification is an examination by a technically qualified organization as to the security strength of an intended operational system. The process of accreditation is a statement by the system manager of the operational system that, having compared the mission requirement with the threat against the system and with the findings of the certification, he finds the system qualified to operate with information of specified levels of sensitivity.

Based on our collective experience within the Community, we believe that these two processes are quite variable from agency to agency, are applied with different degrees of rigor by different agencies, and lead to circumstances in which systems have never been accredited or are operating under a waiver.

Recommendations

We recommend that

23. The DCI have prepared policy guidelines to improve the quality of system certification and accreditation, plus an apppropriate manual that describes the steps that are necessary in (1) the certification process for a system, and (2) the ensuing accreditation action.

The process of examining a system for its security-worthiness, and then contrasting it with the threat and operational need should be a Community-wide standardized process.

An example of quality improvement would be the "licensing" of organizations that conduct certification so that each would follow the same process, consider the same technical factors, utilize the same procedures, etc. Such a step would be analogous to the situation with TEMPEST testing; many organizations conduct such tests but all do so according to procedures prescribed by NSA.

24. The DCI require recertification and reaccreditation of all systems on a periodic calendar-time interval, or when operational circumstances change substantially.

The periodicity of such actions should be related to the development of the threat and also take account of the progress of technology for affording new security safeguards. Moreover, the operational environment of systems will change from time to time. Some changes will have security implications; others will not. For example, adding a few new users or terminals at the same clearance level is not likely to raise a security concern, but adding a new group of users at a different security level or connecting to a new network will.

25. The DCI task each Designated Approving Authority to monitor on a regular basis the security status of systems for which he is cognizant, and to invoke appropriate parts of the certification and/or accreditation process when changes in the operational environment warrant reconsideration of the security posture and practices, or when other circumstances indicate.

Judgment will clearly be needed on the part of the DAA; he will have to determine whether changes in the operational environment raise security concerns. "Other circumstances" can include anomalous behavior of the system that might suggest a security vulnerability, the results of deliberate penetration testing, the detection of an attack against the system, or the appearance of a new threat.

INFORMATION SHARING

Background

User groups have proved very effective information transfer mechanisms in the commercial world. Such a group offers a forum in which users with common problems can discuss them and decide on appropriate remedial actions.

It should be possible to achieve the same information sharing among Community systems.

Recommendations

We recommend that

26. The DCI have created under his auspices a "user group" for each of the commonly occurring hardware/software configurations in the critical systems.

Such user groups would be able to:

- Compile a "catalog" of systems or places where users might turn for ideas, available software, preferred practices, etc.

- Provide a secure environment in which to exchange ideas/techniques/procedures/etc. that relate to security aspects of their operational systems.

In the short run, user groups organized by commonly occurring hardware/software configurations are administratively and jurisdictionally easier to establish; but in the long run, there should exist a Community-wide security forum in which all system managers and operational personnel can exchange information and work toward problem solutions.

SPECIFIC VENDOR SYSTEMS

Background

With regard to operating system software (also called executive system software), vendors phase out such systems from time to time and will no longer provide ongoing support to them. The DCI must be cautious not to invest in such dead-end software systems. It is likely that some of the operational critical systems already contain them.

Similarly, vendors are continuously upgrading both their hardware and system software. Presentations made to us indicate that newer software incorporates security features that could materially improve the situation in the critical systems.

Recommendations

We recommend that

27. The DCI direct that a review be made of all DEC PDP-11 systems running with RSX or IAS software for upward conversion to a VAX with VMS-4 software. If feasible, procurement of the new systems should be expedited on a priority basis. Alternatively, if cost and schedules permit, system managers need not be constrained to the same vendor.

This is an instance of software which is being abandoned by the vendor who, however, is offering newer systems with significant added security safeguards in the operating system. VMS-4 includes such improvements.

28. The DCI direct that a review be made of all IBM and all Burroughs systems to ascertain the feasibility of using security-enhancing software products available either from the equipment vendors or from independent software vendors.

Software products now on the Evaluated Products List of the Computer Security Center or those submitted for evaluation should be considered especially.

29. The DCI direct that the information about security aspects of Wang systems being regularly obtained by the Department of State be circulated on a periodic basis throughout the Community.

The Department of State has an established contractor to examine the security risks of Wang equipments and systems as they appear on the market.

====

GENERAL SECURITY UPGRADING

Background

The Community should point toward a general upgrade of equipment and software as rapidly as such products become available and are evaluated by the Computer Security Center. However, the Community should make known its interests in better security products. Meanwhile, the Center should be tasked to be reponsive to the special needs of the Community.

Recommendations

We recommend that

30. The DCI institute policy that, by 1988, the Community intends to acquire only systems that are certified B-1 or better by the Computer Security Center, and that he make known such policy to vendors.

31. The DCI task the Computer Security Center to review on a priority basis certain software products of especial concern to the Community for its critical systems, e.g., M-204, Inquire, Recon-Guard, KAIS-Guard.

====

RESEARCH

Background

Since computer security does not now have a fully developed theoretical foundation, R&D on various technical aspects must be pursued. For example, modelling of security policy is essential and must be supported for a high rate of achievement.

The Computer Security Center is the national focal point for coordinating and conducting computer security R&D. The Center sponsors generalized R&D with the understanding that sytem- or agency-specific R&D will be done by the military services or by other agencies, but with the cognizance of the Center.

Recommendations

We recommend that

32. **The DCI formally make known all of his needs for computer security R&D to the Computer Security Center, and that he evaluate the Center's program as it relates to his needs. To the extent that it does not meet his needs, he should conduct his own R&D efforts; but assure that they interface and are coordinated with the program of the Center.**

It is essential that the DCI exploit the achievements of the Center, with regard not only to technical advances but also with regard to policy implications. At the same time, the DCI must be free to conduct his own R&D when the Center can not meet his needs. Conversely, members of the Community may be qualified to carry out a part of the Center's program. Under any circumstances, it is essential that the knowledge and progress of R&D efforts be shared, that the total R&D effort of the Community and the Center be coordinated, and that all participants be mutually informed.

Approved For Release 2009/08/17 : CIA-RDP87M00539R000901160028-2

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu