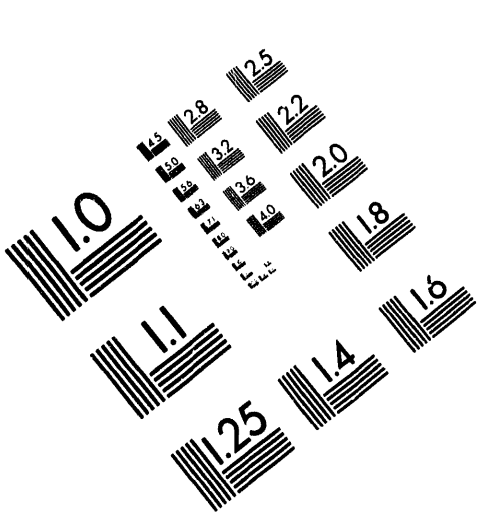
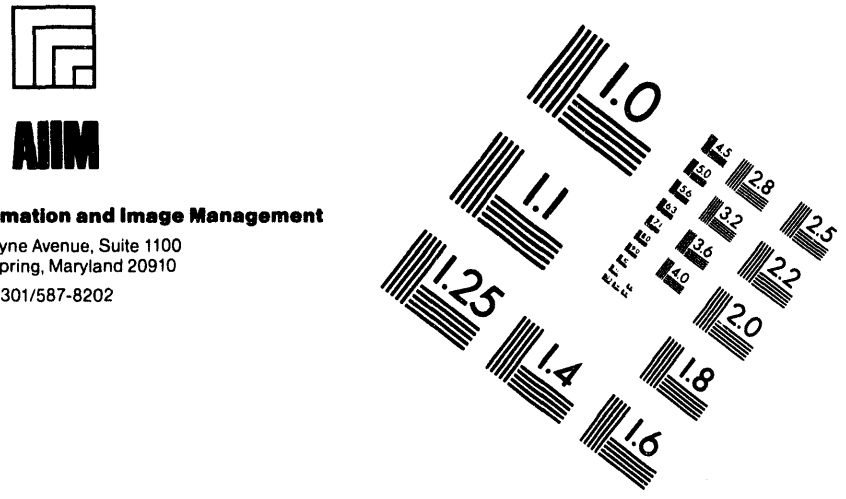
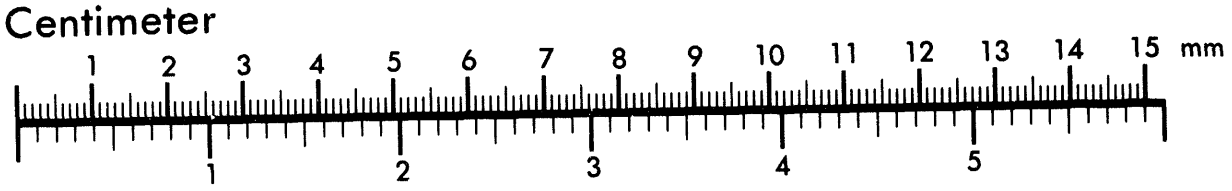


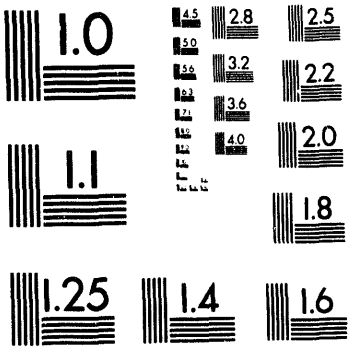


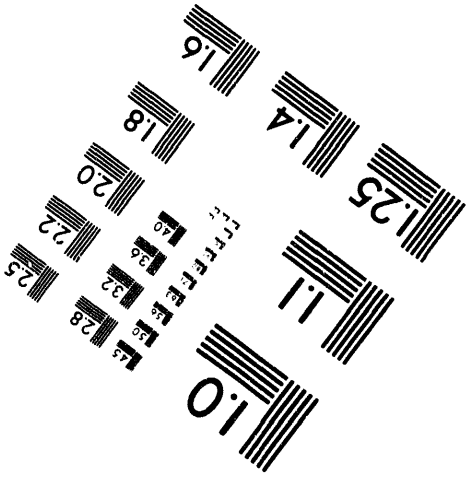
Association for Information and Image Management

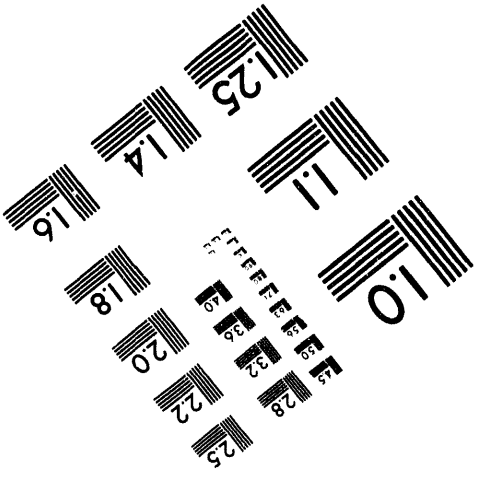
1100 Wayne Avenue, Suite 1100
Silver Spring, Maryland 20910

301/587-8202









MANUFACTURED TO AIIM STANDARDS
BY APPLIED IMAGE, INC.

1 of 1

Conf-9410140--1

LA-UR-94-2128

Title: INDEPENDENT VALIDATION AND VERIFICATION OF AUTOMATED INFORMATION SYSTEMS IN THE DEPARTMENT OF ENERGY

Author(s): William J. Hunteman and Robert Caldwell

Submitted to: 17th National Computer Security Conference
Baltimore, Maryland
October 11-14, 1994

Los Alamos
NATIONAL LABORATORY

INDEPENDENT VALIDATION AND VERIFICATION OF AUTOMATED INFORMATION SYSTEMS IN THE DEPARTMENT OF ENERGY*

William J. Hunteman
Los Alamos National Laboratory
Safeguards Systems Group
Phone: 505-667-0096
Fax: 505-667-7626
(wjh@lanl.gov)

Robert Caldwell
Department of Energy
Office of Safeguards and Security
Phone: 301-903-3019
Fax: 301-903-8414

Introduction

The Department of Energy (DOE) has established an Independent Validation and Verification (IV&V) program for all classified automated information systems (AIS) operating in compartmented or multi-level modes. The IV&V program was established in DOE Order 5639.6A [1] and described in the manual [2] associated with the Order.

This paper describes the DOE IV&V program, the IV&V process and activities, the expected benefits from an IV&V, and the criteria and methodologies used during an IV&V. The first IV&V under this program was conducted on the Integrated Computing Network (ICN) at Los Alamos National Laboratory and several lessons learned are presented.

The DOE IV&V program is based on the following definitions. An IV&V is defined as the use of expertise from outside an AIS organization to conduct validation and verification studies on a classified AIS. Validation is defined as the process of applying the specialized security test and evaluation procedures, tools, and equipment needed to establish acceptance for joint usage of an AIS by one or more departments or agencies and their contractors. Verification is the process of comparing two levels of an AIS specification for proper correspondence (e.g., security policy model with top-level specifications, top-level specifications with source code, or source code with object code).

DOE IV&V Program

The DOE IV&V program is designed to provide an additional level of assurance for automated information systems (AIS) that have a higher level of risk due to the sensitivity of information being processed or due to differences in user clearances. This section will discuss the goals of the IV&V program, when an IV&V is required, the outputs expected from an IV&V, and the administrative issues, such as funding, organization, and management.

The DOE protection requirements are arranged in a hierarchical manner based on the classification level of the information and the clearance level of the AIS users. This hierarchy ranges from zero to five and is called a protection index. A protection index of zero corresponds to a dedicated mode of operation. A protection index of one corresponds to the system-high mode of operation. A protection index of two

*This work supported by the US Department of Energy, Office of Safeguards and Security.

corresponds to a compartmented mode of operation where information is separated into one or compartments and formal access approvals are required for access to the information.

A protection index of three is loosely defined as "secure multi-level" because all AIS users are cleared, but there is at least one level of difference between one or more user clearance levels. For example, an AIS in which some users have a DOE Q clearance (equivalent to a Top Secret clearance) and one or more users have a DOE L clearance (equivalent to a Secret clearance) would have a protection index of three.

A protection index of five is a multilevel AIS where at least one access point, used by an uncleared person, is located outside the security area and is authorized to process only unclassified information. An additional requirement is that all of the access points outside the security area must be located within the boundary of the facility. No access is allowed from off site.

IV&V Program Goals

The primary goals of the IV&V program are to

- support the objective analysis of security risks in an AIS operating with a protection index greater than or equal to two and
- to facilitate the accreditation of AISs by providing assistance to the designated accrediting authority (DAA).

These goals ensure that all AISs with an increased level of risk receive an independent review that is integrated into the accreditation decision. Secondary goals of the IV&V program include

- providing technical input to the AIS certification,
- maintaining a technical library of the results of IV&V activities to reduce redundant activities and to aid AIS developers,
- identifying any policy areas that should be considered for modification or addition to the DOE policy for classified computer security, and
- identifying areas where research and development is needed to enable DOE AISs to meet the policy requirements.

A library of IV&V results should reduce the overall resources needed to conduct future IV&Vs by eliminating the need to repeat previous analyses and reviews. This library is also expected to improve the security of new AISs by allowing the AIS developer or integrator to apply the results of previous IV&V work.

When an IV&V is Required

An IV&V is required for all AISs that have or will operate with a protection index of two or higher. The IV&V process will begin when the tentative or actual protection index for the AIS is determined. The IV&V process is initiated by the AIS security officer who documents the need for an IV&V and forwards the request through the accreditation hierarchy. The security officer is also expected to simultaneously submit a funding request for IV&V support through the appropriate channels.

The actual IV&V activities are expected to start with the preliminary design of the AIS. The maximum benefit will be gained by involving the IV&V team during the AIS design when changes can be made with a minimum impact.

IV&V Outputs

The outputs expected from an IV&V are divided according to the phases of an IV&V. Phase one occurs during the AIS preliminary design phase. Phase two occurs after the AIS has been implemented and during the security certification testing of the AIS.

The outputs required for phase one of an IV&V are

- a report documenting the results of the analysis of the AIS preliminary design including any recommendations for changes and
- a description of the expected IV&V phase two activities including a plan for managing the activities and the estimated costs for the activities.

The report required as output from phase two of an IV&V contains

- documentation of the analysis of the AIS Security Test Plan and the analysis of the security test results,
- any recommendations for changes in the AIS design or implementation or both,
- if necessary, recommendations for additional security testing, and
- the IV&V team recommendations for AIS accreditation.

Depending on the results of the IV&V analyses of the AIS, recommendations may be made to modify or clarify current DOE computer security regulations. The analyses may also identify areas where new or redirected research and development is needed to provide cost-effective solutions to meeting DOE requirements.

Funding, Organization, and Management of an IV&V

All funding for an IV&V is provided by the organization responsible for the management and operation of the AIS. Typically, the initial funding is provided only for the phase one activities. The additional funding necessary for phase two is supplied after the IV&V team has completed the phase one activities. All estimated funding requirements must be reviewed and approved by the accreditation hierarchy before committing any funds. This review will ensure that IV&V resources, such as personnel and money, are appropriate to the required level of effort. Funding for an IV&V for a very complex AIS should not exceed $30,000 for phase one and $60,000 for phase two. The values are the maximum expected for an AIS and will be required only when the network involves a number of different computer systems and other network components that all require extensive analysis and review. An IV&V on a typical local area network is expected to cost $15,000 to $25,000.

An IV&V is performed by a team. The minimum composition of the team is a coordinator and at least one other individual. Most teams are expected to contain a coordinator and two individuals. The team members are contractors from outside the DOE and DOE contractor organizations to ensure the proper independence in the process. The official team coordinator is the DOE Computer Security Program Manager (CSPM) or a person designated by the CSPM. The CSPM is the DOE person responsible for establishing the computer security policies for classified computing in the DOE. Other individuals may be added to the team either as members or as observers to represent organizations that may have an interest in the AIS. The AIS organization will contribute at least one person who acts as the liaison between the IV&V team and the AIS organization. All personnel who participate in the team activities are expected to contribute to the analyses, reviews, and report preparation.

The team activities are directed by the chairperson. The chairperson is responsible for coordinating the team activities with the representatives of the AIS organization and representatives of the accrediting authority.

IV&V Process and Activities

An IV&V is performed in two phases. Phase one is performed during the initial design and implementation of the AIS. Phase two is conducted after the AIS has been implemented and is ready for security certification.

Phase One Activities

Phase one activities include reviews of documents and interviews with AIS developers, AIS management, and computer security people responsible for the AIS. Critical documents reviewed during this phase include the AIS design specifications and descriptions, the AIS Security Plan, and the AIS Security Test Plan (if it exists). During phase one, the team is guided by the criteria established for the validation phase. These criteria, described in the following section, define the minimum requirements the AIS must meet to comply with DOE regulations.

Phase one is concluded with reports prepared by the team and reviewed with the AIS personnel prior to release to the DAA. The contents of the phase one report document the team's understanding of the AIS, a description of the AIS Security Support Structure (SSS), the results of the team analysis, and the team's initial assessment of the risks or vulnerabilities in the AIS.

The DAA, in coordination with the CSPM, reviews and accepts the phase one reports. The DAA may accept the risks resulting from vulnerabilities or concerns identified by the team. The decision to accept risks will be coordinated with the CSPM and documented by the DAA. Once the DAA accepts the phase one report and documents the acceptance of any remaining risks identified by the team, phase two of the IV&V can be scheduled.

Phase Two Activities

Phase two activities are not scheduled until the developers have implemented the AIS and prepared the Security Test Plan. The first phase two activity is to review and comment on the AIS Security Test Plan. This review is performed by the team members before it returns to the facility. After the team has reviewed the Security Test Plan, the AIS developers and security people will perform the security tests. After the security testing is completed, the team returns to the facility and reviews the results of the tests. This review is focused on ensuring that the security tests are complete and that the results clearly indicate that the tested function is implemented correctly. Depending on the results of the security tests, the team may request additional security tests to address any anomalies in the testing or to address functions missed in the original test activity.

During the review of the Security Test plan and test results, the team is guided by the verification criteria, described in the following section, to ensure that all necessary tests are included in the test plan and that each test adequately addresses the required security features.

After all testing is completed, the team will prepare the phase two report, which will document the team's analysis of the AIS testing, the team's assessment of the AIS risks and vulnerabilities, and the team's recommendations to the DAA. The phase two report is reviewed with the AIS personnel to ensure accuracy prior to release to the DAA. After the DAA has received the phase two report, the AIS organization, the computer security personnel at the site, and the DAA are expected to address any security issues identified by the team. The DAA may choose to accept the risk for any or all of the concerns identified by the team.

During either phase of an IV&V, the team may identify policy issues that may need clarification or modification. The team may also identify areas for new or re-directed research and development. The team will prepare a report describing the issue or need and a recommended solution and forward the report to the CSPM for consideration.

IV&V Criteria

As mentioned earlier, the IV&V team is guided by criteria for validating the AIS design and verifying the AIS implementation. These criteria have been developed to establish a baseline set of requirements for satisfying DOE policy and to guide the reviews and analyses performed by the team. This section will describe the general approach to development of the criteria, how the DOE criteria are consistent with initiatives by the US Government, the DOE profiles defined by the criteria, and the structure of the criteria.

General Approach to Development of the Criteria

The criteria were developed to define the minimum requirements necessary to meet DOE policies for classified computer security. The primary base for the criteria is DOE Order and Manual 5639.6A. Additional criteria that exceeded the DOE Order requirements were identified as desirable or recommended practices. If a protection was identified as desirable but was not reflected in the DOE order, during its development, either the order was updated or the protection was dropped from the criteria. Another concern during the criteria development was to ensure consistency between the DOE requirements, as expressed in the criteria, and other US Government initiatives in information security.

Consistency Between DOE Criteria and US Government Initiatives

A desired goal during development of the criteria was, where possible, to maintain consistency with the draft Federal Criteria (FC) for Information Technology [3] then being developed by the National Institute for Standards and Technology. The consistency was desirable to permit DOE to easily update its criteria when the FC were officially released.

Because the DOE requirements take precedence over the draft FC, we used DOE Order 5639.6A as the baseline. For each DOE protection index defined in the Order, the FC components were mapped into the DOE protection requirements. If necessary, the FC components were modified to meet the DOE requirements and environments. This mapping process resulted in a clear understanding of the differences between DOE requirements and the draft FC. This mapping process created a combined set of requirements that met the DOE Order and incorporated the FC. A by-product of the incorporation of the FC was a structure similar to the profile concept defined in the FC.

This "profile" development process is somewhat different from the process described in the draft FC but has achieved the same results. The FC security environment and policy-requirement mapping descriptions are expressed in the DOE Orders through the protection index structure. The DOE Order and Manual defined the minimum security features that must be present for each protection index. The requirements are defined in very general terms and allow an AIS developer to select and implement the algorithm that is most appropriate for the AIS mission. Incorporating the requirements from the draft FC allowed a refinement of the DOE Order without specifying a particular implementation approach. Once the general requirements were defined, detailed criteria for each requirement were developed and the criteria were then composed into DOE "profiles" for each protection index.

DOE Profiles

The DOE "profiles" have been developed for protection index two (compartmented mode), protection index three ("secure" multi-level mode), and protection index five (multi-level mode). The profiles are hierarchical beginning with protection index two. Most of the differences between the profiles are in the expected strength of the mechanisms. The DOE profiles contain elements that describe the information protection problem addressed by the profile; a rationale discussion that provides the fundamental justification for a profile, including the threat, environment, and usage assumptions; functional requirements that establish the protections that must be provided by an AIS; and development assurance requirements for all phases of an AIS development from initial design through implementation. Evaluation assurance requirements from the draft FC were not included in the DOE profiles.

The functional requirement components in a DOE "profile" include

- Identification and Authentication
- System Entry
- Trusted Path
- Audit
- Access Control
- Resource Allocation (object reuse)
- Security Management (security officer interface to the system)
- Reference Mediation (the involvement of the SSS in all accesses to objects)
- SSS Logical Protection (separate execution of the SSS functions)
- SSS Self Checking (checks for consistency and integrity of SSS components at startup and during execution)
- SSS Startup and Recovery (checks to ensure that the proper SSS is executed at start up and that the SSS always recovers to a secure state)
- SSS Privileged Operations (executions of SSS security functions are restricted to privileged components)
- Ease of Use (requirements for programming interface to SSS security functions)

The DOE "profiles" do not contain any requirement for covert channel analysis because the threats to DOE information do not justify the expenditure of resources necessary to identify and eliminate all covert channels. Some covert channels are identified indirectly as part of the development assurance component, such as penetration analysis and functional testing.

The development assurance components in a DOE "profile" include

- Property Definition (description of the protection properties implemented by the SSS)
- Interface Definition (description of the interface to the SSS, including informal models of the SSS)
- Modular Decomposition (description of the disciplines used during design and implementation of the SSS)
- Implementation Support (description of the configuration control procedures followed during implementation of the SSS)
- Functional Testing (description of the SSS testing and the procedures used to manage the test activities)

- Penetration Analysis (description of the process used to perform penetration analysis of the SSS)
- User Security Guidance (description of the AIS security functions for the users)
- Administrative Security Guidance (description of the AIS security functions for the security officer and system administrators)
- Flaw Remediation (description of procedures for reporting, tracking, and correcting flaws in the SSS)
- Trusted Generation (description of procedures for generating a known version of the SSS)
- Life Cycle Definition (description of the procedures and methods used to manage the SSS through its entire life cycle)
- Trusted Distribution (description of procedures used to ensure no unauthorized modifications are made to the SSS during shipment)
- Configuration Management (description of the procedures to manage the SSS)

The criteria for each protection are organized into two documents. The validation document defines the requirements and criteria that must be met for the AIS to conform to DOE requirements. The verification document contains all of the validation information and adds a generic test description for each criterion.

Structure of the IV&V Criteria Documents

Each IV&V criteria document is organized into three sections. Section 1 describes the required security features and assurances and the environment addressed by the criteria. Section 2 describes the expected target audience of the criteria and the contents of the document. Section 3 contains the components that must be satisfied for the AIS to successfully meet the DOE requirements. Each component description contains

- a general description of the component,
- the specific DOE requirement(s) directly related to the component,
- one or more criteria that must be met to satisfy the component, and
- for each criterion, a generic verification test description.

Criteria

Each functional requirement or development assurance component, such as audit or trusted generation, is decomposed into one or more criteria that must be satisfied to ensure that all of the requirements for the component are met. Each criterion represents a single concept or requirement. The general rule followed during the development of the criteria was that the criteria must be required or clearly implied by the component and the criteria must be easily tested.

During the development of the generic test description, we required that each test must unambiguously indicate success or failure. If we were unable to define a clear test description, we modified or split the criterion until the test description was unambiguous. This guideline also required that, while individual tests may be based on the results of previous tests, the test could not attempt to evaluate more than one criterion at a time.

Another requirement for the criteria was that the statement of the criteria must be independent of specific computer systems or architectures. This approach requires the IV&V team to interpret and apply the criteria to a specific AIS. However, this interpretation is not difficult because DOE requires the specific

security mechanisms in an AIS to be described in a document called the AIS Security Plan. This document provides the details that allow the IV&V team to apply the criteria. An example criterion from the criteria for protection index two is

> The SSS shall end the attempted login session after the user performs the authentication procedure incorrectly for a number of successive times. Termination of the session, such as lockout, shall be recorded on the audit trail, the system console, and the system administrator's terminal.

An AIS implementation of this criterion would be described in the AIS Security Plan for the system, using language similar to the following:

> The security software in this system will terminate an attempted login session after the user incorrectly enters a password five consecutive times. Each incorrect attempt is recorded in the system audit trail. After the fifth unsuccessful attempt, the session is terminated by locking out the terminal device. After the session is terminated, a message is written to the system audit trail and a message is sent to the operator console.

Generic Test Description

The IV&V criteria documents are intended to provide a complete set of requirements and criteria for each of the protection indices. A generic test description, independent of any specific computer system or architecture, is supplied as part of each criterion. The descriptions are designed to be templates that can be used by a test developer to guide the generation of system-specific tests and to aid the IV&V team in evaluating the test plans and test results. Each test description contains

- Test Purpose (purpose of the test)
- Expected Result (results that should be produced by the test)
- Controlled Configuration (components of the AIS that should be controlled to ensure repeatability of the tests and to minimize impact on AIS users)
- Test Equipment, Material, and Personnel Required (resources required to perform the test)
- Input Used for Test (any special input needed during the test; for example, during a test for SSS self-checking, one of the SSS tables must be modified to introduce an error)
- Test Description (detailed sequence of events: describes the who, what, when, where, and how for the test)
- Pass/Fail Criterion (criteria for successfully passing the test, depends on the AIS and the SSS component being tested; for example, the pass/fail criteria for testing an authentication process that is based on passwords would include a description of the range of acceptable password lengths and the range of unacceptable password lengths)

Lessons Learned from First IV&V

We have completed the first phase of the first IV&V conducted under the DOE IV&V program. This IV&V phase one review was performed on the Los Alamos National Laboratory Integrated Computing Network (ICN). This network is being redesigned and upgraded to support operation at the protection index three ("secure multilevel"). Phase one of the IV&V was performed on the ICN design during February 1994. Phase two of the IV&V will be conducted during the fall of 1994 depending on the progress toward implementing the design.

ICN Description

The ICN consists of several segments and separately accredited networks. The ICN backbone contains an Fiber Distributed Data Interface (FDDI) ring and several routers. Users operate from one of several separately accredited networks that operate in the system-high mode. These user networks are connected to the backbone through the routers. The routers provide a primary control of messages and allowed communication paths.

Network servers, such as file storage, output services, and a CRAY YMP (running UNICOS 8.0), provide services to the users. All of the servers are designed to support multi-level operation. Other management and security services, such as collection and analysis of audit trails and user identification and authentication are provided by a separate network connected to the backbone. These additional services operate in the system-high mode because they do not allow user access or the execution of user processes. These services are provided to all components of the ICN, including the user networks.

Lessons Learned

Early lessons learned from the IV&V phase one include several unanticipated or underestimated benefits. In addition to the objective analysis and review of the ICN design, we identified several areas where the then draft DOE policy needed clarification and one area where the policy need some interpretation to address state-of-the-art networking technologies. During our review of the ICN backbone and the servers, especially the identification and authentication server, we learned that the traditional view of security requirements for a complex network was difficult to apply to individual segments of the network.

When we attempted to review the ICN backbone, the traditional model of users as subjects acting on objects did not apply. Within the ICN backbone, the routers and network control nodes make security and routing decisions on message addresses. While the messages were being sent on behalf of users, there are no "users" in the backbone. We were forced to adapt the normal definitions of subject and object to fit the backbone. The definition we used was that a subject is a computer identified by a unique address and objects are the physical or logical communications paths connecting the computers. This definition of subjects and objects then allowed the team to adapt the IV&V criteria to allow analysis of the backbone. The backbone analysis required interpretation of components, such as access control and audit, using the new definitions of subject and object. For example, access control decisions in the backbone were based on mediation of connection requests between the source and destination addresses. Discretionary access was determined by administrative criteria expressed in the router tables. Mandatory access was determined based on a priori knowledge of data sensitivity through the hard-wired ports on each router and the contents of router tables.

Another segment of the ICN where the team experienced difficulty in applying the traditional view of security was the multilevel servers. For example, the ICN identification and authentication service is provided by the KERBEROS software operating on a platform isolated from the ICN backbone by a router. This approach allows the service to be available to all users and nodes anywhere in the ICN while ensuring that users are not allowed to directly access or execute processes on the server. The traditional model of security requirements is built on the assumption that users have (or may gain) the ability to execute their processes on the system. By creating a distributed system with multiple layers of protection, the identification and authentication server should not be required to meet the requirements necessary for a normal multi-user computer system. During phase one of the IV&V, we decided to analyze these servers from two perspectives. The first view was at the platform level. These platforms are located in an exclusion area, and access is restricted to system administrators, operators, and development personnel. A platform in this environment can operate in the system-high mode if there is adequate assurance that the interface between

the operating system and the application is sufficiently strong to prevent the application activity from affecting the security of the platform.

The second view of the servers was at the application level. Many of the servers in the ICN must operate the application in the "secure" multi-level mode. Analysis of the application from this perspective focuses on the security features of the protocol used to access the service and the interface between the application and the platform. We are currently developing additional criteria for this view of network servers.

Another underestimated benefit of the IV&V was the interaction between the ICN designers and the IV&V team. During the numerous discussions and interviews, the team members were able to offer suggestions to the designers to improve the security and information flow in the ICN. Most of the suggestions have been adopted in the ICN, and the designers obtained a better understanding of the security needs and requirements for the ICN.

Applicability to Other Environments

The IV&V criteria and process appear to be a viable approach to obtaining an objective analysis of an AIS that would work for any other organization. The overall methodology is similar to the accreditation process used in the Department of Defense with the addition of criteria to guide the team's analysis.

Although the IV&V criteria are specific to the DOE, the process used to develop the criteria could be easily applied to other environments and organizations. The DOE criteria could be easily adapted to other situations because the criteria are generic and independent of AIS architectures.

Conclusions and Future Work

The IV&V program and criteria have been demonstrated to be an effective technique for objective analysis of complex computer systems and networks in the DOE. The process provides detailed objective technical support to an accrediting authority and will reduce the residual risk in DOE AISs.

The initial IV&V activities have indicated that new criteria and approaches are needed for network components, client-server architectures, and distributed systems. We are currently working on developing new criteria for these areas.

References

[1] "Classified Automatic Information System Security Program," DOE 5639.6A, Department of Energy, Office of Safeguards and Security, April 4, 1994.

[2] "Manual of Security Requirements for the Classified Automatic Information System Security Program," DOE M 5639.6A-1, Department of Energy, Office of Safeguards and Security, April 4, 1994.

[3] "Federal Criteria for Information Technology Security," Volumes I (Draft) and II (Draft), National Institute of Standards and Technology and National Security Agency, December 1992.

DATE
FILMED
9/8/94

END