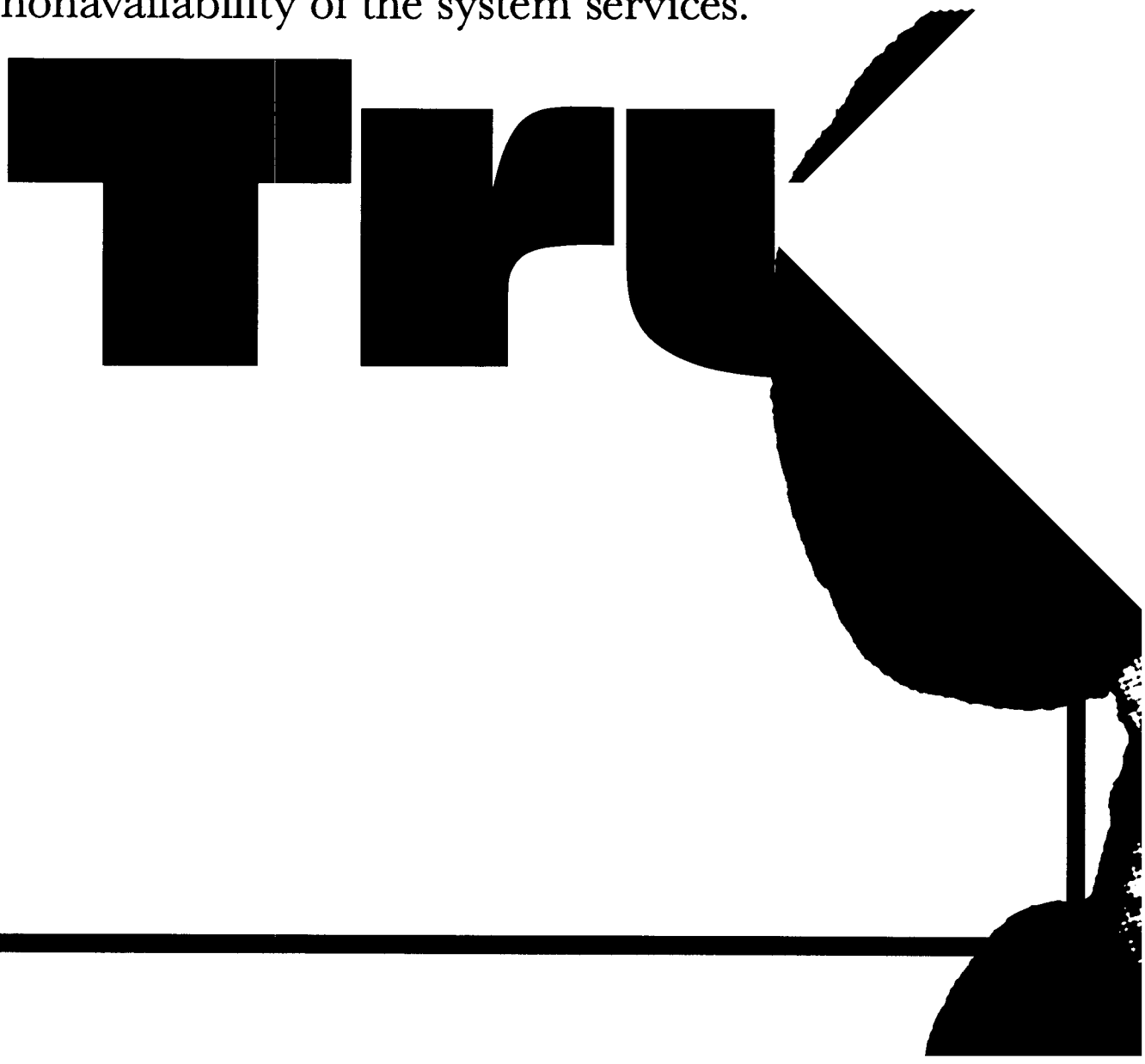
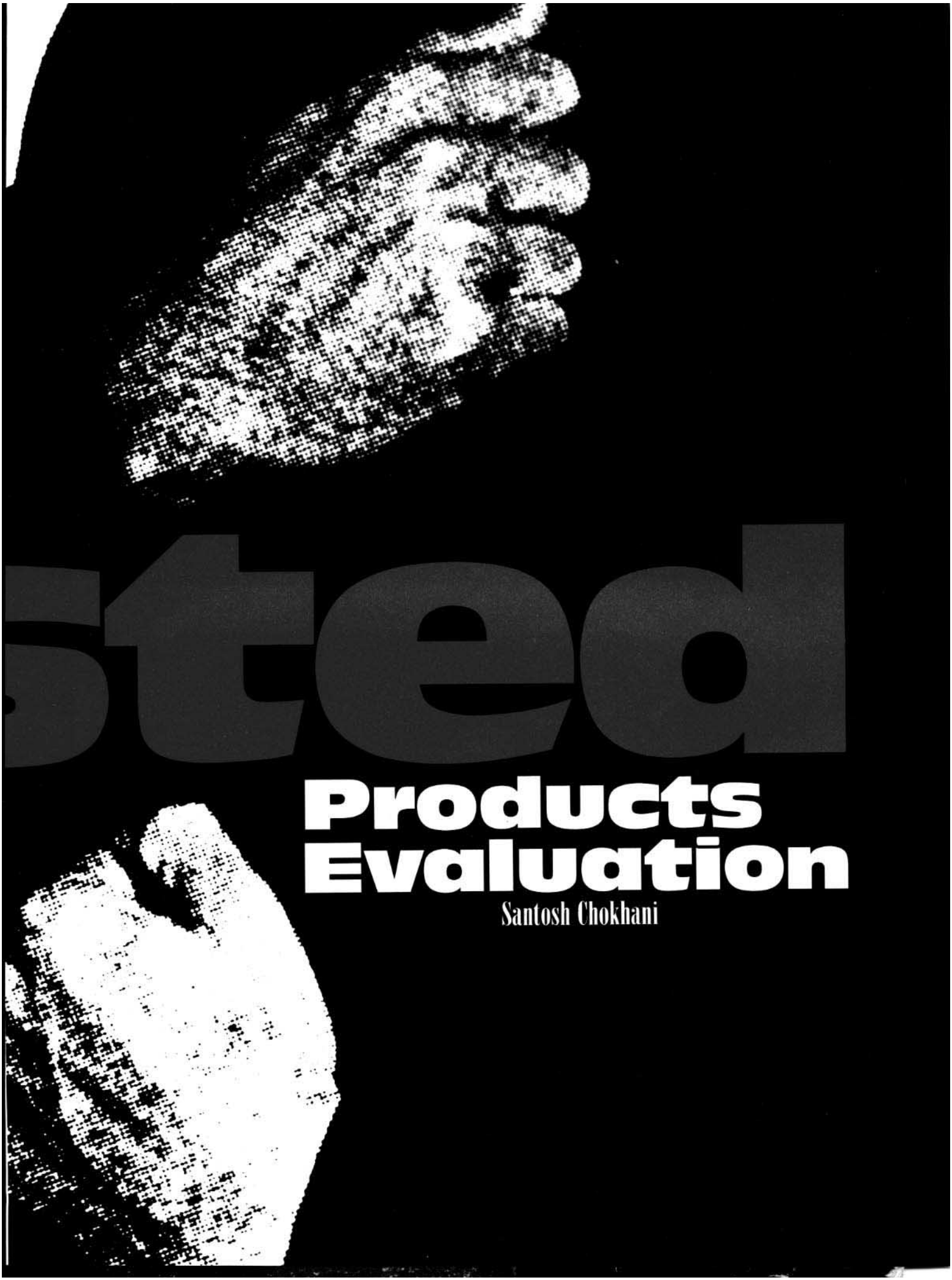
The advances in computer and communications technologies and trends toward standardization, interoperability, and connectivity pose a growing security threat to Automatic Data Processing (ADP) and telecommunications systems that process sensitive or classified information. The activation of a threat could result in: disclosure, modification, or destruction of sensitive or classified information; modification to hardware or software; and/or nonavailability of the system services.




sted
Products
Evaluation
Santosh Chokhani

The National Computer Security Center (NCSC) published the Trusted Computer System Evaluation Criteria (TCSEC) in 1983. In 1985, the TCSEC was published, with some revisions, as the Department of Defense Standard 5200.28-STD, also known as the "Orange Book" [7]. The focus of the TCSEC is disclosure protection of information and modification protection of system resources. Since 1982, the NCSC has been evaluating the products developed by computer and computer software manufacturers under the activity entitled "Trusted Products Evaluation Program." These products include standalone ADP systems (hardware, operating systems, and add-on software packages to incorporate security in the operating systems), networks and network components, and workstations. Future plans include evaluating database management systems. The evaluations are a joint government and industry effort; computer manufacturers spend their resources designing and developing trusted products, while the NCSC spends government resources evaluating the products. The objectives of the activity are the following:

1. Ensure widespread availability of commercial off-the-shelf trusted products for use by the government.

2. Advance the state of the art in information system security (specifically in the area of designing, building and evaluating trusted systems).

3. Transfer of computer security technology, specifically an understanding of techniques for constructing trusted computer systems, to government program managers and planners and to established computer manufacturers to assure an inventory of trusted computer product lines for application to government needs.

## Trusted Computer System Evaluation Criteria

The TCSEC provides a basis for evaluation of the effectiveness of technical security controls built into ADP systems. The evaluated system (hardware, firmware, and software) is called the Trusted Computing Base or TCB. As illustrated in Figure 1, the TCSEC levies requirements that can be broken down into the following categories: Security Policy, Accountability, Assurance, and Documentation. The TCSEC packages these requirements into hierarchically ordered divisions (C, B, A). Within each division there are one or more hierarchical classes.

### Security Policy

The requirements in this area are the fundamental needs of an organization to protect the information on an ADP system. An ADP system should support the following capabilities: Discretionary Access Control (DAC) [19], Mandatory Access Control (MAC), Labels, and Object Reuse.

***DAC.*** This capability allows the users to protect the information (e.g., files) they own. The owner may grant or deny access to information to individual users or groups of individuals. The owner may also define the access mode (e.g., read, write, delete, etc.) for each individual or each group.

Example: Staff salary information can be viewed only by the specified staff supervisors and department managers. The information can be modified only by the specified department managers.

***MAC.*** This capability allows the ADP system to enforce a label-based policy modeled after DOD Security Policy. A user can read only the information (e.g., file) for which he has a clearance. The clearance (sensitivity label) includes a hierarchical classification[1] level (e.g., secret, top secret, etc.) and a set of nonhierarchical categories

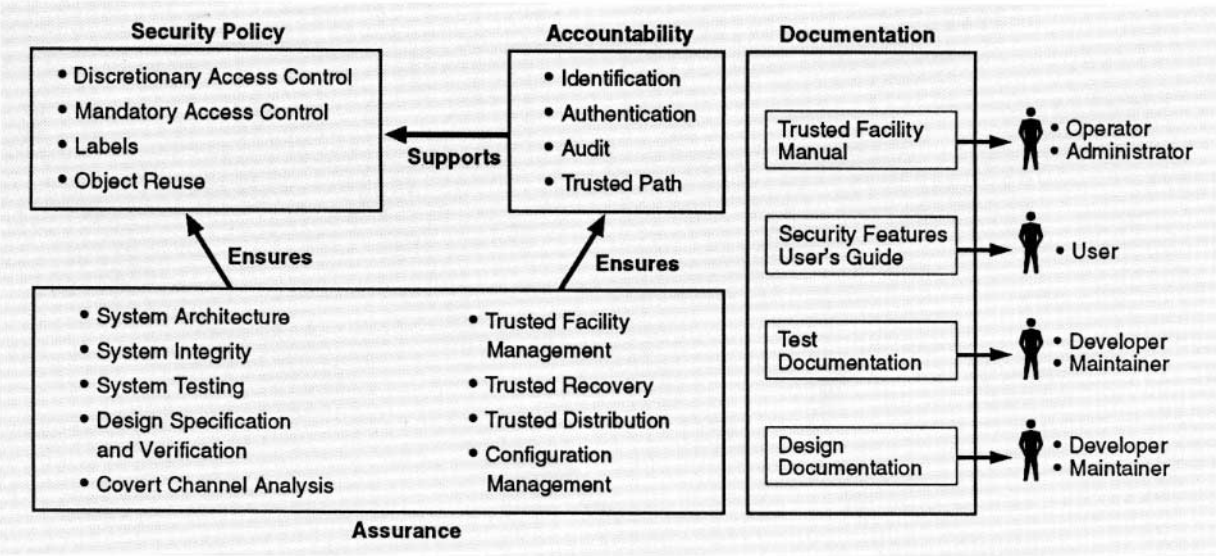



**Figure 1.** Trusted Computer System Evaluation Criteria—Overall View

(e.g., CRYPTO, NUCLEAR, privacy information, financial information, etc.). The ADP interpretation of the policy is that a program can read information only at or below the sensitivity label at which it is operating. In addition, in order to protect against downgrading[2] by trojan horses[3], a program can write information only at or above the sensitivity label at which it is operating.

***Labels.*** This capability associates the mandatory sensitivity label (classification level and categories) with users and with information being input/output to the ADP system, including printing the labels on hardcopy output.

***Object Reuse.*** This capability ensures that the basic storage elements (e.g., disk sectors, memory pages, etc.) are cleared prior to their assignment to a user so that no intentional or unintentional data scavenging takes place.

### Accountability

In order to support the DAC and MAC policy, an ADP system should provide the following features: Identification, Authentication, Audit, and Trusted Path.

***Identification.*** This feature allows the users to identify themselves to the TCB (e.g., by providing user name, user ID, etc.). It is the cornerstone for individual accountability.

***Authentication.*** This feature allows the TCB to authenticate the user's identity. Examples of authentication mechanism include passwords [6], biometrics, challenge-response devices [5], etc. In many breakins, we hear that the key weakness has been the ability to compromise the intent of the authentication mechanism by guessing passwords. It is very critical to have a protected authentication mechanism that cannot be easily compromised.

***Audit.*** This feature allows the TCB to record the security-relevant events (e.g., logins, logouts, file operations such as open, close, create, delete, etc.) in a protected file [21]. This information can be later analyzed for attempted breakins or other attempts to violate a system's security policy (successful or unsuccessful).

***Trusted Path.*** This feature allows the TCB and the user to be sure that no other user or program is masquerading as the system to obtain security-critical information (e.g., a trojan horse could emulate the login sequence to steal a user password). It can be implemented by assigning a type of interrupt (e.g., power on, break key) or character sequence from the terminal as a request for communications with the TCB. Occurrence of this event is typically detected by the terminal handler.

### Assurance

The variety of requirements in this area ensure that: 1) the TCB was built using acceptable systems engineering practices (in order to minimize errors), and 2) the TCB continues to operate correctly without circumvention of the security features and controls discussed in the previous subsections entitled "Security Policy" and "Accountability".

***System Architecture.*** The system architecture requirement addresses both the system development phase and the system operations phase [3]. Examples for the development phase include modular software design, layering, and data abstraction/information hiding. An example for the operations phase is isolation of the TCB from user processes. Further isolation of security critical (kernel) and nonsecurity critical portions of the TCB is also desirable.

## Glossary of Acronyms Used in This Article

| | |
|---|---|
| **ADP** | Automatic Data Processing |
| **CM** | Configuration Management |
| **COMPUSEC** | Computer Security |
| **COMSEC** | Communication Security |
| **DAC** | Discretionary Access Control |
| **DAP** | Design Analysis Phase |
| **DIA** | Defense Intelligence Agency |
| **ETL** | Endorsed Tools List |
| **FEP** | Formal Evaluation Phase |
| **FER** | Final Evaluation Report |
| **INFOSEC** | Information Security |
| **IPAR** | Initial Product Assessment Report |
| **LOCK** | Logical Coprocessing Kernel |
| **MAC** | Mandatory Access Control |
| **MMU** | Memory Management Unit |
| **PB** | Product Bulletin |
| **PTR** | Preliminary Technical Review |
| **RAMP** | Rating Maintenance Phase |
| **SFUG** | Security Features User's Guide |
| **TCB** | Trusted Computing Base |
| **TCSEC** | Trusted Computer System Evaluation Criteria |
| **TDI** | Trusted DBMS Interpretation (of the TCSEC) |
| **TFM** | Trusted Facility Manual |
| **TNI** | Trusted Network Interpretations (of the TCSEC) |
| **TRB** | Technical Review Board |
| **VAP** | Vendor Assistance Phase |
| **VWG** | Verification Working Group |

[1]The security community uses hierarchical to describe a total ordering; computer scientists generally use hierarchical to describe a partial ordering.

[2]Lowering the hierarchical classification level or reducing the set of nonhierarchical categories.

[3]A trojan horse is a computer program which, in addition to performing the desired function, performs functions that compromise the security of the system (e.g., copy sensitive data to public-readable files).

*System Integrity.* This requirement addresses the correct operation of the ADP system hardware and firmware and is typically satisfied by periodic use of diagnostics software.

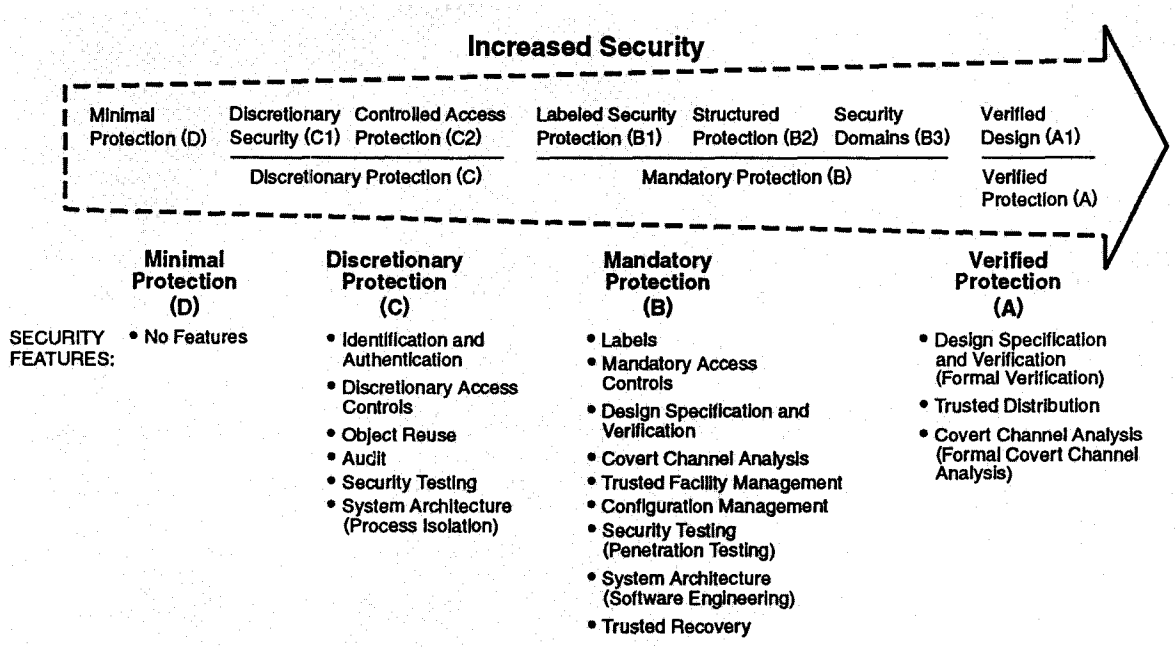
*System Testing.* This requirement ensures that the security features have been tested thoroughly.

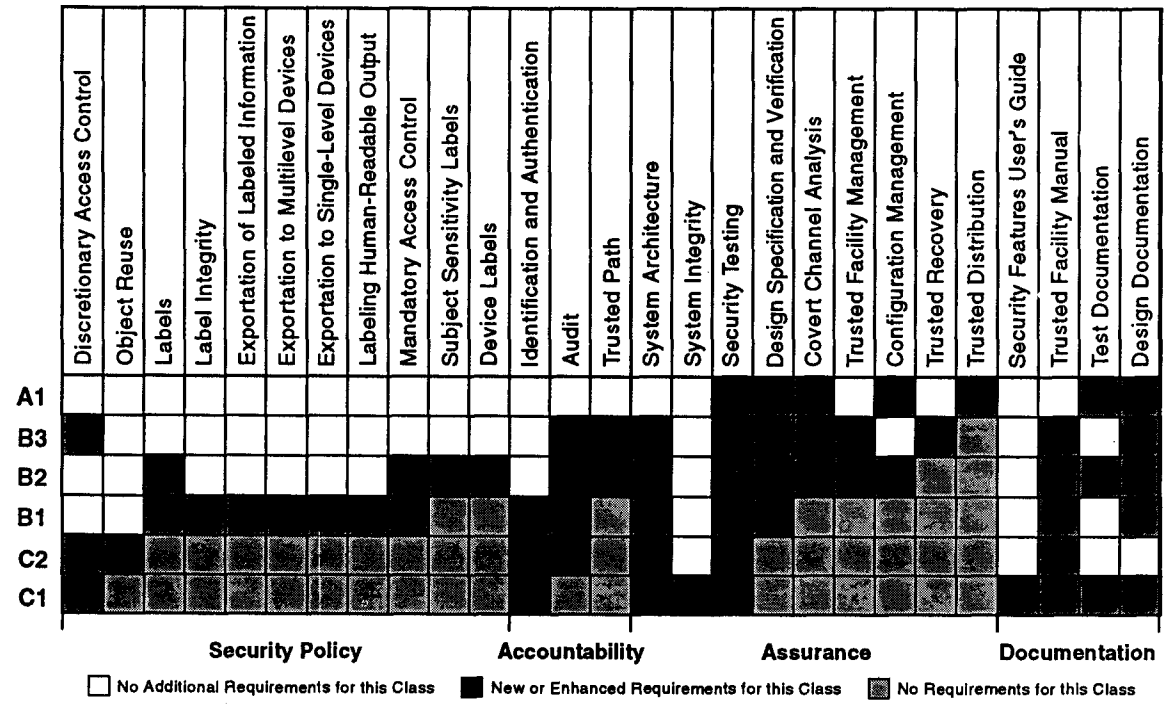
*Design Specification and Verification.* This requirement addresses the correctness of the system design and implementation with respect to the system security policy. The TCB Security policies must be stated and proven to be consistent with respect to security axioms [1]. The TCB Formal and Descriptive Top Level Specifications must be shown or proven to be consistent with the security policy model [1].

*Covert Channel Analysis.* In a multiuser environment, certain variables, attributes, or object informa-

**Figure 2.** Trusted Computer System Evaluation Criteria—Rating Scale

**Figure 3.** Trusted Computer System Evaluation Criteria—Detailed View



tion is invariably shared in violation of the MAC policy, forming a covert channel [10, 11]. For example: even if a secret user cannot read top-secret information, the user may be able to determine whether a top-secret file exists, which can be considered one bit of information (exists or does not exist). The TCSEC requires elimination, reduction of data rates, or auditing of these MAC violation information channels.

***Trusted Facility Management.*** This requirement provides for separation of the roles for the system operators and security administrators. Separation of roles helps security by reducing the scope and probability of exposure.

***Trusted Recovery.*** This requirement provides for correct operation of security features after the TCB recovers from failures or crashes.

***Trusted Distribution.*** This requirement ensures that the TCB hardware, firmware, and software do not go through unauthorized modification during transit from the vendor to the customer. Trusted courier, registered mail, physical seals, cryptographic checksum, etc., are some of the ways to meet this requirement.

***Configuration Management (CM).*** The benefits of CM are well-known. This requirement applies to hardware, firmware, and software, and to associated documentation.

### The Rating Scale

The TCSEC packages these requirements into hierarchically ordered divisions (C, B, A). Within each division there are one or more hierarchical classes. Figure 2 and the following subsections summarize the key aspects of each class. Figure 3, borrowed from the "Orange Book", is a detailed representation of this packaging.

### Discretionary Protection (Division C)

This division supports DAC and object reuse security policy. It also includes identification, authentication, and auditing features.

***Discretionary Security Protection (Class C1).*** Features in this class include: identification, authentication, and DAC. Some or all of these features can be implemented on the basis of an individual or groups of individuals. In other words there is no need to identify, authenticate, or provide access control on an individual basis; it can be done on a group basis. Individual identification and accountability are extremely important in order to discourage security violations and in order to investigate potential violations. Since they are not a requirement for C1 class system, this class is considered of little use and systems are generally not targeted for this class. Individual identification and accountability requirements come at Class C2, discussed next, and that is why C2 is considered the minimum to protect ADP systems that process sensitive information.

***Controlled Access Protection (Class C2).*** In this class identification, authentication, DAC, and auditing are required at the individual user level. Object reuse protection is introduced.

### Mandatory Protection (Division B)

In this division multilevel security is introduced through sensitivity labels and MAC. System architecture and other assurance requirements play a very significant role from Class B2 on, resulting in the popular and accurate notion: for C1–B1 systems, security can be added to an ADP system as an afterthought or enhancement, but in order to get to B2 or above, one must design the system with security in mind using sound system and software engineering practices. From B2 on, formal modeling and analysis also play increasingly important roles.

***Labeled Security Protection (Class B1).*** The best way to describe this class is C2 with labels and MAC. Sensitivity labels get introduced and MAC policies take effect in addition to C2 requirements. This is the highest class an existing operating system is likely to achieve where security has been added as an afterthought or enhancement.

***Structured Protection (Class B2).*** From B2 on, while there are additional requirements for Security Policy and Accountability features, the emphasis is on assurances. The software is expected to be modular. Security-critical portions of the TCB software should be separated and protected from the rest of the TCB software. A formal security policy model must be developed and proven to be consistent with respect to security axioms. Separation of roles of system administrators and operators is also required. Security Testing requirements are more thorough and white-box testing oriented, and include penetration testing. Covert channels must be identified, audited, and analyzed in terms of maximum bandwidth. Trusted path is provided for the users to securely communicate with the TCB.

***Security Domains (Class B3).*** Emphasis is toward minimizing and simplifying the TCB. Real-time monitoring and alerts based on security auditing are also introduced.

### Verified Protection (Division A)

In this division assurance is further enhanced by verification of the security control against the formal model of the security policy.

***Verification Design (Class A1).*** Assurance is enhanced by using formal and informal techniques to show consistency between the Formal Top Level Specification and the Formal Security Policy Model. Formal methods are required for the covert channel analysis.

***Beyond Class A1.*** Although not described in the TCSEC, in the future we may be able to formally verify the source code against the formal specifications and against the formal security model.

## Evaluation Process

In order to obtain a rating, a product goes through the following four evaluation phases described in this section:

- Preliminary Technical Review (PTR)

- Vendor Assistance Phase (VAP)
- Design Analysis Phase (DAP)
- Formal Evaluation Phase (FEP)

Figure 4 provides a summary of the evaluation process described in this section. In order to maintain a rating, a product goes through the RAMP described in the section entitle "Rating Maintenance Phase."

### Preliminary Technical Review (PTR)

When a vendor approaches the NCSC for a product evaluation, several business-related decisions are made in terms of the product market and the vendor's ability to develop the product. These issues are beyond the scope of this article. The technical aspects of the product evaluation begin with the PTR. For the PTR, the NCSC sends a team of two to three computer security evaluators to the vendor for briefings. Based on the technical exchange and documents supplied by the vendor, the NCSC team develops a Preliminary Technical Report. The emphasis is on assessing the high-level architecture's ability to meet the target rating. This assessment plays a key role in accepting the product for evaluation, rejecting or suggesting changes prior to acceptance for evaluation. While a PTR can be conducted at any time during a product's life cycle, depending on the vendor request and the availability of NCSC resources, the ideal time to perform a PTR is during the product planning phase or early in its development.

### Vendor Assistance Phase (VAP)

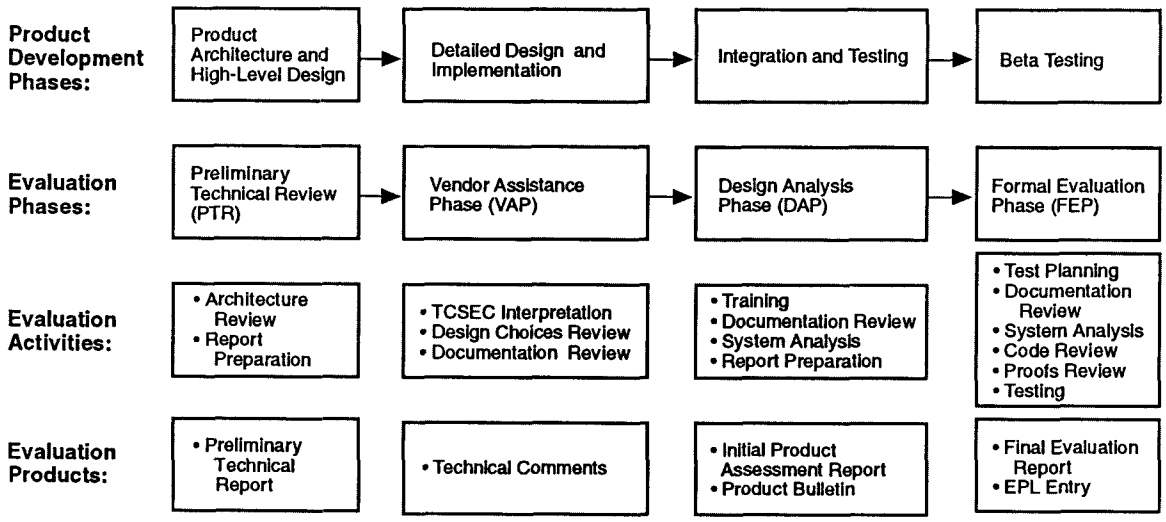
Once a product is accepted for evaluation, it enters the VAP. During VAP, the vendor is designing and implementing the product and a team of three to five NCSC evaluators is available to consult and assess how certain design decisions are likely to impact the target rating. During this phase, the evaluators are essentially offering their interpretation of specific TCSEC requirements in the context of the product under evaluation. The team also performs a high-level review of the vendor documentation required for the evaluation. This includes Security Features User's Guide (SFUG), Trusted Facility Manual (TFM), Design Documentation, and Test Plan.

It should be noted that at higher levels of ratings (B2 or beyond), a Configuration Management document [17][4], System Architecture document, Covert Channel Analysis Report, Formal Model, and Formal and Descriptive Top Level Specifications are also required. The test plan in this context encompasses all test preparation documentation in the traditional software engineering sense (i.e., the test plan, test specifications, test procedures, and test cases). Once the team feels that all the required documents appear to be in reasonable shape, the product transitions to the DAP. The ideal duration for the VAP is the product design and implementation phase.

### Design Analysis Phase

During the DAP, the team is augmented to the size of five to eight evaluators depending on the target rating and product complexity. The vendor provides the team formal training on the internal design and implementation of the product. The team carefully reviews all documentation to understand and analyze the system. During the DAP phase, the team also captures the understanding of the security relevant aspects of the system in a document entitled the Initial Product Assessment Report (IPAR). In addition, the IPAR includes the team's assessment of the product's ability to meet each of the requirements (see Figure 3) applicable for the target rating. The NCSC has established a mechanism to provide quality control, and consistency and uniformity across various evaluations[5]. The mechanism is a Techni-

**Figure 4.** Evaluation Process Summary



cal Review Board (TRB) consisting of several computer security experts. Upon completion, the IPAR is distributed to the TRB for their review and comment. After the TRB has a chance to review and provide its comments to the team, the team briefs the TRB on the product with emphasis on the issues raised by the TRB. At this time, the team and TRB make appropriate recommendations to the NCSC. These include: accept the product for formal evaluation, accept the product for formal evaluation after specified requirements are met, or request another TRB to clarify outstanding issues.

The ideal time to begin the design analysis phase is when the product design is frozen, implementation is complete and the vendor is going through the product testing. The ideal time to complete the DAP is when the product has been successfully alpha or beta tested.

### Formal Evaluation Phase (FEP)

The successful transition to the Formal Evaluation Phase (FEP) is marked by the formal announcement that the vendor has submitted a specified product for a specific target rating. This announcement, a Product Bulletin (PB), is made public. The NCSC evaluation team resolves all outstanding issues from the DAP and incorporates them into the Final Evaluation Report (FER). The IPAR is the basis for the FER. The team develops a set of its own tests. For B2 and higher level systems, the team reviews the code for compliance with the system architecture requirements, for correspondence with the Formal and/or Descriptive Top Level Specifications, and for developing penetration scenarios. For A1 level systems, the team reviews the proofs and arguments for consistency among the Formal Security Policy Model, Formal Top Level Specifications, and Descriptive Top Level Specifications. The team develops penetration test scenarios and incorporates them into the overall team test plan. An overall team test plan may consist of up to three components: vendor supplied test (they form the bulk of the tests), team tests, and team penetration test scenarios. At this time, the TRB is reconvened and briefed by the team on the test plan. It should be noted that based on the product complexity, maturity and evaluation status the DAP/IPAR TRB and the test TRB may be combined. The team test plan is revised based on the TRB recommendations. The team carries out all the tests and documents the test results. At this point, any security-relevant anomalies uncovered are fixed and appropriate regression testing is conducted. The test results are presented to the TRB. Based on the team and the TRB recommendations, the NCSC awards the rating to the product. A comprehensive summary of the technical features are published as an Evaluated Products List (EPL) entry. This is incorporated in the NCSC's catalog of INFOSEC products, published quarterly [29]. The FER incorporating the technical details is also published.

[4]For systems targeted for B1 and lower ratings, a Rating Maintenance Plan (including a Configuration Management Plan) is required.

[5]Applying the TCSEC to a given product is an intellectual exercise and is subject to differences in judgment and perspectives.

## Evaluation Products

This section provides further details on the documents produced by the evaluation team. Most of these documents have already been discussed in the Evaluation Process context. It should be noted that the vendor invests a greater amount of resources and produces many more documents than the NCSC does in evaluating the product. The requirements are summarized and described throughout the section "Trusted Computer System Evaluation Criteria." Further discussions of the vendor documents is beyond the scope of this article.

The purpose of the Preliminary Technical Report is to document and analyze the high level product architecture for its potential to meet the target rating. It is typically 20–40 pages long and contains descriptions of the hardware platform in terms of security relevant features such as the machine states, privileged instructions, rings, memory protection features, and domains [8, 12, 13, 15]. The software architecture is described at a high level (e.g., UNIX-like, multiprocessing, client-server, virtual machine/monitor, capability based [5, 8], etc.) The subjects and objects, their security-relevant attributes, MAC, DAC, Identification and Authentication, Audit, Object Reuse, and other security-relevant features are summarily described. Finally, the product engineering approach and product schedule are summarized.

The purpose of the IPAR is to document the preliminary analysis of the product's ability to meet the target rating. It is typically 100–200 pages long and provides the hardware architecture and details on the security-relevant hardware mechanisms. The IPAR provides the software architecture and summary description of software modules. It describes the subjects and objects in the system, their security-relevant attributes, how the subjects and objects are created and destroyed, and how their security-relevant attributes are acquired and manipulated. It provides a detailed description of security features (security policy and accountability features listed in Figure 1, [i.e., DAC, MAC, Labels, Object Reuse, Identification and Authentication, Audit and Trusted Path]). The IPAR also describes the assurance mechanisms illustrated in Figure 1. The items described so far complete the technical description of the system under evaluation. The IPAR also addresses each of the applicable TCSEC requirements (see Figure 3 for the list of all TCSEC requirements) and makes an informal analytical argument as to how and why the vendor system meets each of the requirements. The document also contains a list of

specific hardware and software components which form the TCB. Evaluators are encouraged to provide comments (positive, negative, or neutral, but of interest to system users). Finally, the IPAR provides a comprehensive list of references. The vendor product design and assurance related documents form the bulk of references.

The FER is essentially the IPAR with security testing results incorporated. It should be noted that before a FER is made available to the public, proprietary technical details may be removed upon vendor request.

## Evaluation Aids

The trusted products evaluation process is a labor-intensive analytical exercise. In the DAP and FEP, the evaluation progress is dependent on the ability and productivity of the evaluators. The NCSC has taken several steps to assist the evaluators in performing their tasks and to ensure consistency across evaluations, rightfully an area of importance to the highly competitive vendor community. The evaluation aids can be broken down in the following areas: Guidelines, information collection tools, automated or interactive tools, and process-oriented tools and mechanisms.

The TCSEC and associated guidelines are generally referred to as the "rainbow series" in the security community. The TCSEC was initially written for standalone general-purpose, multiprocessing ADP systems. The NCSC saw a need for developing interpretations of the TCSEC for network and database systems. The Trusted Network Interpretations (TNI), also termed the "red book" was published in 1987 [18]. Based on evaluation experience, it is being revised. The Trusted DBMS Interpretation (TDI) has recently been published as a formal guideline. In addition, the NCSC has a guideline published, drafted or under development for each of the features listed in Figure 3 [16, 20, 21, 23, 27]. These guidelines further explain the TCSEC requirements and provide detailed acceptance criteria with examples (where appropriate), to the system developers, NCSC evaluators and to the acquirers of trusted systems.

The NCSC has developed two questionnaires to assist the evaluators. One questionnaire is a tool to collect the observations and recommendations of the evaluators in terms of available and needed tools, mechanisms and the evaluation process. The information collected is used to refine the evaluation process and to prioritize the building of required evaluation aids. The other tool is a technical product questionnaire [28] that can be used by the developers, evaluators and acquirers to collect technical information on a product. It has about 200 specific questions in the areas of hardware architecture, software architecture, security policy, features, and assurances. The tool can be used by the evaluators throughout the product evaluation life cycle, beginning with the PTR and ending with the IPAR and FER. During the PTR phase, the vendors are required to cover the questions by answering them, by providing appropriate documentation, and/or by covering them during their briefings. During the IPAR and FER phase, evaluators are encouraged to use the questionnaire as a checklist to ensure all of them are duly addressed.

The NCSC provides a Multics-based system called DOCKMASTER for the evaluators and vendors to use for interaction using electronic mail, bulletin boards, and an electronic meeting facility. The forum facility on the system is used as an electronic meeting facility. Each product evaluation has two forum meetings associated with it. The members of an evaluation team can read and write to the "team forum" associated with the evaluation. The members of the evaluation team and the vendor team can read and write to the "vendor forum" associated with the evaluation. These forums are used to exchange ideas and comments, consolidate ideas and comments, and to schedule and coordinate face-to-face meetings.

In order to ensure consistency across all evaluations, the NCSC has established three fora which can be read and written to by all evaluators. The evaluators are required to discuss the topics in these three fora in general terms. The three fora are the following:

1. "Interpretations" (used by the evaluators to share their interpretations of the specific TCSEC requirements and associated rationale. This is a debate forum used for consensus building.)
2. "Decisions" (used to formalize a decision based on interpretation forum discussion or a team decision; this forum is used to formally announce decisions so that they can be consistently applied at a future date.)
3. "Evaluation issues" (while the first two fora are to discuss technical issues, this forum is used to debate the evaluation process-oriented issues.

The vendors and evaluators also have access to a public forum called "criteria discussions" to clarify and debate various TCSEC requirements.

The NCSC has also implemented the LaTeX [9] system on the DOCKMASTER to assist the evaluators in developing various products such as the PTR, IPAR and FER. Several LaTeX macros have been implemented to make report development faster and consistent from evaluation to evaluation.

In order to ensure completeness and consistency across the evaluations, the NCSC has developed annotated outlines for the PTR, IPAR and FER. The most important quality control and consistency mechanism is the Technical Review Board (TRB) consisting of experts in the area of computer security. These experts review evaluation team documents such as the IPAR, team test plan and FER. The team

also briefs them at the critical points in the evaluation (for further details see the previous section, entitled "Evaluation Process"). The TRB's comments and critique ensures consistency, thoroughness, and quality across the evaluations. The NCSC also has Senior Evaluators and a Chief Evaluator who ensure consistency across the evaluations by advising the team leaders. The Chief Evaluator also takes technical leadership in formalizing the consensus from the "interpretations" forum into official interpretations.

To provide guidance and assure consistency in the formal modeling (for B2 and higher level systems) and formal verification (for A1 level systems) areas, the NCSC has formed a Verification Working Group (VWG) consisting of formal methods experts. With the assistance of the VWG, NCSC has developed an Endorsed Tools List (ETL) [24], a list of tools that are acceptable to be used in formal modeling and verification.

Finally, the NCSC maintains detailed process oriented "how to" guides for the evaluators. These guides help maintain corporate memory, and are useful training tools for the evaluators in the area of the evaluation process.

## Rating Maintenance Phase (RAMP)

All products go through bug fixing, refinements, and enhancements. But a rating is for a specific software release executing on a specific hardware base. This means that if a system goes through even minor revisions (which may or may not be security-relevant), it has to be reevaluated to maintain its rating. Given the manual analysis aspects of the evaluation process, this may result in significant use of resources. In order to address the industry need for reevaluation, the NCSC has established a RAMP program for C1–B1 level systems [25]. Under RAMP, the emphasis is on Configuration Management (CM), security analysis by vendor staff, and on security testing.

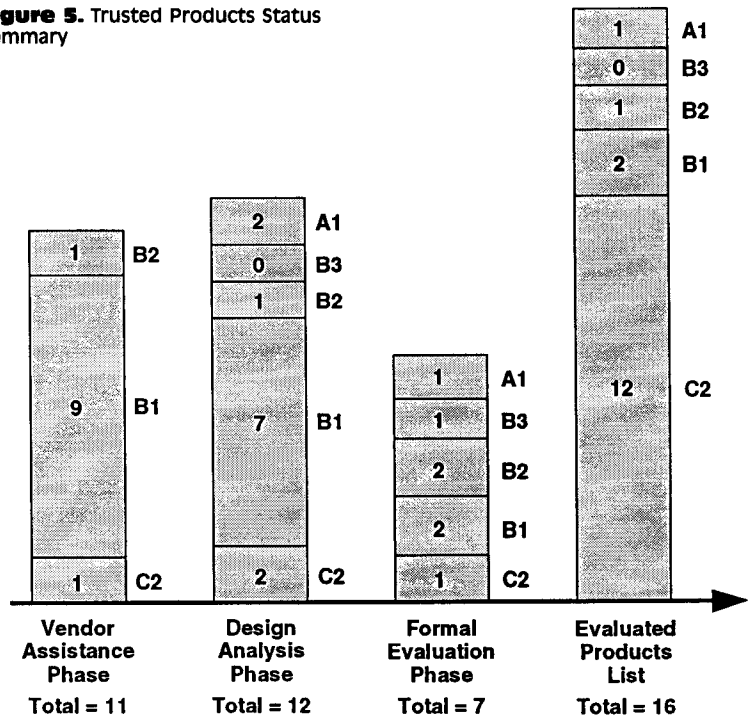
During the baseline evaluation, the vendor is required to submit a Rating Maintenance Plan which describes the vendor's CM philosophy and plan (for hardware, software, and associated documents), and responsible corporate and technical points of contact. The NCSC evaluates this plan for acceptability and can audit the CM process at any time. The vendor is expected to assign and train security analysts in the technical aspects of the product and in computer security. The NCSC offers a program consisting of lectures, reading assignments, and in-class and homework exercises to train the vendor security analysts in the area of computer security evaluations. The team of vendor security analysts reviews the changes in the product from one release to another and assesses them in terms of security relevance and the ability to maintain the rating. The security analysts are also required to augment the security test suite for comprehensiveness in light of the product modifications. The security analysts are required to run revised test suite to ensure successful test results. Finally, the vendor security analysts team is required to brief the TRB. The scope of briefing includes identification of changes, categorization of the changes in terms of security-relevance (with supporting rationale), analysis of security-relevant changes in light of the TCSEC requirements, enhancements to the test suite and results of testing. Based on successful TRB presentation and the TRB recommendations, the NCSC confers the rating on the revised product.

## State of the Trusted Systems Industry

Figure 5 provides a summary of trusted products status. The industry trend is toward B1- and B2-level systems.

There has been an increase in the number of vendors submitting UNIX-based systems for evaluation. The trend is also toward submitting single-user PCs and workstations for security evaluations. The NCSC is supporting a joint Government and industry effort to specify a POSIX-compliant Secure

**Figure 5.** Trusted Products Status Summary



Operating System interface called TRUSIX, which can meet B3 TCSEC requirements [26].

The interest in workstation security has been helped significantly by a joint National Security Agency (NSA) and Defense Intelligence Agency (DIA) effort called Compartmented Mode Workstation (CMW) [4] evaluation.

The trusted system developers need some financial incentives in developing A1-level systems, given the cost of formal verification and export control on high-level (B3 and above) systems. It is hoped that the Logical Coprocessing Kernel (LOCK) [14, 16] will provide the needed solution.

## Future Directions

The standalone ADP systems evaluated to date do not include any network interfaces. The reality of the operational world is that an ADP system, be it a PC or mainframe, has LAN or WAN connectivity. The NCSC must develop techniques and guidelines to evaluate network interfaces. Unfortunately, TNI [18] does not provide the necessary guidance. An Information Security (INFOSEC) approach to evaluation may be needed (see Figure 6). Computer Security (COMPUSEC) deals with controlling access to information using protected hardware and software mechanisms. Communication Security (COMSEC) deals with protection of information using encryption techniques, while the information is being stored or transmitted over an unprotected medium (e.g., a wide area network). The INFOSEC combines the two technologies in order to create, store, process, and transmit information in a secure fashion, even if some of the storage and transmission media are unprotected. This implies, in addition to the COMPUSEC controls discussed in this article, encryption techniques should be used to store and transmit information over unprotected media. Similarly, the systems that generate and store cryptographic keys must contain COMPUSEC controls discussed in this article.

The NCSC has faced debates from vendors (especially vendors of UNIX-based products) in the area of system architecture requirements [3] for B2 and higher level systems. The debate has been generally in the area of the modularity requirement. The evaluators and vendors should realize that some of the system architecture requirements are based on sound software engineering principles. The purpose of these requirements is to ensure understandability of software, which in turn aids maintenance, analysis, and testing. It is very difficult to come up with objective and quantifiable criteria to assess the modularity. Furthermore, it seems impossible to develop a justifiable threshold for acceptance of modularity, even if it could be quantified. Nonetheless, the NCSC has recognized the need to further elaborate on the modularity requirement and has established a working group to develop more detailed guidance.

The NCSC is also facing the issue of covert channel bandwidths. The TCSEC has some specific guidance in terms of limiting the bandwidths of covert channels. Certain classes of timing channels (caused due to sharing high-speed hardware resources) can operate at very high rates. Their prevention, detection, or auditing may be very difficult. In order to deal with the issues related to acceptable covert channels and their bandwidths, the NCSC has formed a working group of experts to formulate the recommendations. It is understood that the covert channels are always going to be present in a multiprocessing, resource-sharing system which has been designed for a certain degree of performance and user-friendliness. The current guidance in terms of specific maximum bandwidth, can be changed to that of requiring to justifying covert channels as sound design decisions to support performance, functionality, user friendliness, and TCB simplicity requirements. The vendors should also be required to provide tools and techniques to reduce their bandwidths. Usage of these tools should not be mandatory to main-

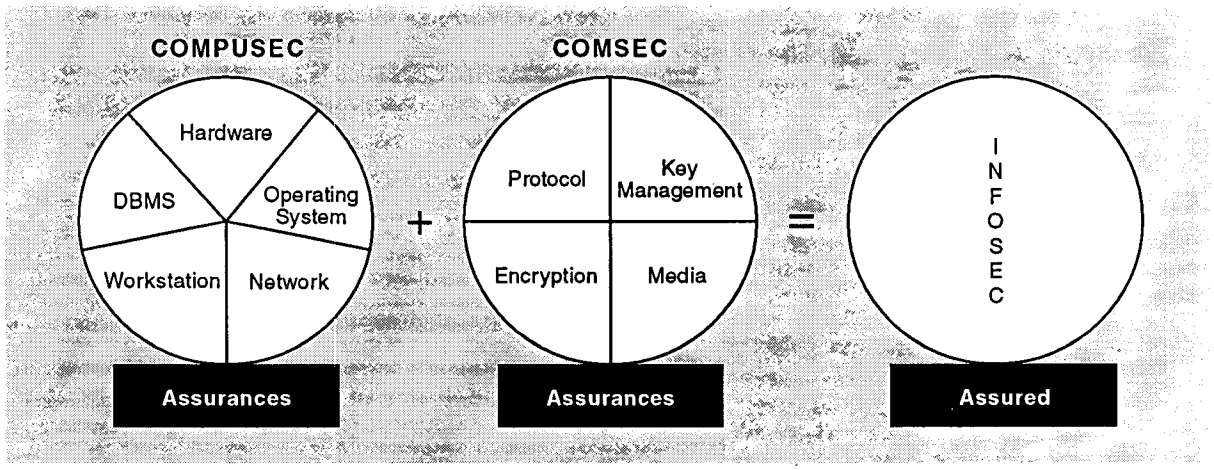



**Figure 6.** INFOSEC

tain a rating. It should be up to the users of the system to decide, based on the threats and risks. For instance, one can envision very stringent covert channel requirements for a system that stores cryptographic keys. Yet the same requirements are inappropriate for each and every system that handles multilevel data.

It is envisioned that as we gain experience with networks and DBMS evaluations, the NCSC will extend the guidelines, questionnaires and RAMP concepts to those types of evaluations. As we gain experience with RAMP (RAMP is a relatively new concept, introduced in 1987), the NCSC will be in a position to evaluate its suitability for B2 and higher level system. The practical experience will also help define metrics and threshold when refinements and enhancements go beyond the point of being RAMP-able to requiring a full NCSC evaluation. The RAMP process may also be useful in evaluating porting of an operating system (e.g., UNIX) to various hardware platforms.

For the long term, the NCSC should explore the ways evaluators could be provided knowledge tools that can help enhance the quality, consistency and efficiency. It should be noted that this article has focused on the evaluation aspects of the product—the amount of time and resources required to develop a trusted product are order(s) of magnitude greater than those required for evaluations. Thus, from the cost and schedule perspectives, real savings will come from speeding up the development process. Nonetheless, the manual task of security analysis requires significant investment in reconciling documents and researching specific issues. If evaluation documents were developed electronically, with appropriate hypertext-type linkages among them, an evaluator will be able to search and reconcile the documents very quickly. This recommendation needs support from the industry, since the electronic document preparation needs to be an integral part of the software development process.

Expert Systems technology (Case-Based Reasoning to be more specific) may help provide an automated tool to educate evaluators in security-relevant design aspects of systems. The approach also offers a sanity-check and assistance to expert evaluators. Such tools should provide more focus on security-relevant aspects and issues of a system, based on design choices made about the system.

The TCSEC does not address the issue of "integrity." Integrity deals with preventing unauthorized modification of data or programs. Mandatory integrity can be very important in combating viruses and trojan horses. For B2 and higher level systems, the TCSEC should be augmented to require mandatory integrity [2].

The major issue in the development of the TDI, and hence the forthcoming evaluations of DBMSs, is the topic of "TCB subsets." The NCSC is attempting to develop the TDI as the guideline for building and evaluating trusted applications (called "TCB subsets") running on an evaluated TCB. The current draft of the TDI attempts to develop a theoretical framework for the TCB subsets and to identify TCB subset architectures that are amenable to incremental evaluations, (i.e., evaluating the application only without evaluating the underlying TCB subset [typically the operating system], which has already been successfully evaluated). The approach has led to conservative and cautious conclusions about the reevaluation of the underlying operating system. The conclusions have significant implications in terms of required resources. The problems can be further exacerbated in multivendor situations, where the DBMS vendor may not have access to the operating system internal details needed for an evaluation.

The NCSC needs to explore alternate approaches for the TDI. For instance, the NCSC could limit the TDI to DBMSs and not address trusted applications. For the DBMSs, the NCSC could evaluate the architectures of widespread off-the-shelf DBMSs and assess whether reevaluation of the underlying operating systems is warranted. These experimental evaluations should help prove or disprove the following theory we propose. An operating system need not be reevaluated except for the Covert Channel Analysis and Penetration Testing, if:

1. The DBMS target rating is at or below the operating system rating.
2. The DBMS uses a clear, well-defined interface with the operating system. This may include using some of the operating system privileges.
3. The operating system has not been modified in order to host the DBMS.

## Summary

This article has presented an evaluator's perspective of the Trusted Products Evaluation Program. The activity has been growing since 1982 and represents a bonafide success of a joint industry and government venture. (The industry spends its resources in developing the products and the NCSC spends government resources in evaluating them.) In addition to a large population of PC add-on security packages (called subsystems) [22], the EPL has 16 products: twelve C2, two B1, and one B2, and one A1 (see Figure 5). Currently, the NCSC is evaluating 30 products. Of these, seven are in the formal phase: one C2, two B1, two B2, one B3 and one A1 (see Figure 5). While the target rating of the products in VAP and DAP is proprietary and details cannot be disclosed, the trend is unmistakably toward higher-level systems.

The NCSC has been able to define a process, and develop tools and techniques that capture the project memory and ensures evolution and consistency over a period of time in an endeavor that involves a large number of evaluators.

**Acknowledgments**

I would like to thank all my fellow evaluators (too numerous to mention each individual's name), and the NCSC management for their help. I would like to thank MITRE management (Peter Bergstrom and Peter Tasker) for providing me with the opportunity to be involved in this effort. I would like to thank Ravi Sandhu, Frank Belvin, and Steve LaFountain for their review and suggestions. I would like to thank Helen Long and Lucy Bhatia for preparing the manuscript to this article. ◻

**References**

1. Bell, D.E. and LaPadula, L.J. *Secure Computer Systems: Unified Exposition and Multics Interpretation.* MITRE Corporation, MTR-2997, 1976.
2. Biba, K.J. *Integrity Considerations for Secure Computer Systems.* MITRE Corporation, MTR-3153, June 1975.
3. Chokhani, S. and Wagner, G. *System Architecture Requirements in Trusted Computing Bases.* MITRE Working Paper 89W262, August 1989.
4. Cummings, P.T., Fullman, D.A., Goldstein, M.J., Gosselin, M.J., Picciotto, J., Woodward, J.P.L. and Wynn, J. Compartmented mode workstation: Results through prototyping. In *Proceedings of 1987 IEEE Symposium on Security and Privacy,* (April 1987).
5. Denning, D.E. *Cryptography and Data Security.* Addison-Wesley, Reading, Mass., 1983.
6. Department of Defense. *Password Management Guidelines.* CSC-STD-002-85, April 1985.
7. Department of Defense. *Trusted Computer System Evaluation Criteria.* DOD 5200.28-STD, December 1985.
8. Fabry, R.S. Capability-based addressing. *Commun. ACM 17,* 7 (July 1974).
9. Lamport, L. *LaTex: A Document Preparation System.* Addison-Wesley, Reading, Mass., April 1986.
10. Lampson, B.W. A comment on the confinement problem. *Commun. ACM 16,* 10 (Oct. 1973), 613–615.
11. Millen, J.K. An example of a formal flow violation. In *Proceedings of the IEEE Computer Society 2d International Computer Software and Applications Conference.* (November, 1978).
12. Saltzer, J.H. Protection and control of information in multics. *Commun. ACM 17,* 7 (July 1974).
13. Saltzer, J.H. and Schroeder, M.D. The protection of and control of information sharing in computer systems. In *Proceedings of the IEEE 63,* 9 (September 1975).
14. Saydjari, O.S., Beckman, J.M. and Leaman, J.R. LOCK Trak: Navigating Uncharted Space. In *Proceedings of 1989 IEEE Computer Society Symposium on Security and Privacy,* May 1989.
15. Schroeder, M.D. and Saltzer, J.H. A Hardware Architecture for Implementing Protection Rings. *Commun. ACM 15,* 3 (Mar. 1972).
16. Saydjari, O.S., Beckman, J.M. and Leaman, J.R. LOCKing Computers Securely. In *Proceedings of the 10th National Computer Security Conference,* (October 1987).
17. Thompson, R. Reflections on trusting trust. *Commun. ACM 27,* 8 (Aug. 1984).
18. National Computer Security Center. *Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria.* NCSCV-TG-005 Version 1, July 1987.
19. National Computer Security Center. *A Guide to Understanding Discretionary Access Control in Trusted Systems.* NCSC-TG-003 Version 1, September 1987.
20. National Computer Security Center. *A Guide to Understanding Configuration Management in Trusted Systems.* NCSC-TG-006 Version 1, March 1988.
21. National Computer Security Center. *A Guide to Understanding Audit in Trusted Systems.* NCSC-TG-001 Version 2, June 1988.
22. National Computer Security Center. *Computer Security Subsystem Interpretation.* NCSC-TG-009 Version 1, September 1988.
23. National Computer Security Center. *A Guide to Understanding Design Documentation in Trusted Systems.* NCSC-TG-007 Version 1, October 1988.
24. National Computer Security Center. *Guidelines for Formal Verification Systems.* NCSC-TG-014 Version 1, April 1989.
25. National Computer Security Center. *Rating Maintenance Phase—Program Document.* NCSC-TG-013 Version 1, June 1989.
26. National Computer Security Center. *Trusted UNIX Working Group (TRUSIX) Rationale for Selecting Access Control List Features for the UNIX System.* NCSC-TG-020-A Version 1, August 1989.
27. National Computer Security Center. *A Guide to Understanding Trusted Facility Management.* NCSC-TG-015 Version 1, October 1989.
28. National Computer Security Center. *Trusted Product Evaluation Questionnaire.* NCSC-TG-019 Version 1, October 1989.
29. National Security Agency. *Information Systems Security Products and Services Catalog.* Issued Quarterly, April 1990 and successors.

**CR Categories and Subject Descriptors:** D.2.0 [**Software Engineering**]: General—*Protection mechanisms;* D.2.9 [**Software Engineering**]: Management—*Software Quality Assurance (SQA);* D.4.6 [**Operating Systems**]: Security and Protection; H.2.0 [**Database Management**]: General—*Security, integrity, and protection;* K.6.m [**Management of Computing and Information Systems**]: Miscellaneous—*Security*

**General Terms:** Security

**Additional Keywords and Phrases:** Covert channel analysis, integrity, security, TCSEC, trust

**About the Author:**

**SANTOSH CHOKHANI** is the Department Head of the Information Systems Engineering Department at the MITRE Corporation. He is also the Associate Director of the company's Information Security Technology Center. His current research interests include information security, software engineering, and computer systems architecture. **Author's Present Address:** MITRE Corporation, 7525 Colshire Drive, McLean, VA 22102; email: santosh@mwunix.mitre.org