INFORMATION TECHNOLOGY SECURITY WORKSHOP PROCEEDINGS

FEDERAL CRITERIA FOR INFORMATION TECHNOLOGY SECURITY WORKSHOP PROCEEDINGS

NIST NSA United States Department of Commerce Department of Defense National Institute of Standards and Technology National Security Agency
Turf Valley Hotel and Country Club Ellicott City, Maryland June 2-3. 1993
Issue 1.0
July 30 1993

CHAPTER 1 Introduction

The first draft of the Federal Criteria was made public in January 1993. Several thou-sand copies of the Federal Criteria were distributed and comments on this first draft were received between January and April of 1993. Over 20,000 comments were obtained from approximately 120 organizations. These organizations represented defense and civil government, producer and procurer, and North American and Euro-pean concerns. The purpose of the Federal Criteria Workshop that was sponsored by the National Security Agency (NSA) and the National Institute of Standards and Technology (NIST) on June 2nd and 3rd of 1993 was to address these comments. All those who commented on the first draft were invited to attend. The workshop consisted of approximately 128 participants.

In the opening remarks by Stuart Katzke of NIST and Robert Scalzi of the NSA, the participants were informed of NIST's and NSA's decision to work with the Canadians and Europeans in creating a Common Criteria (see Chapter 12). The members of the Common Criteria Editorial Board (CCEB) are Gene Troy (NIST), Mario Tinto (NSA) Yvon Klein (France), Chris Ketley (United Kingdom), Hartwig Kreutz (Germany), and Paul Cormier (Canada). The plans for the CCEB call for aligning the various criteria (Trusted Product Evaluation Criteria (TCSEC), draft Federal Criteria, the Information Technology Security Evaluation Criteria (ITSEC), and the Canadian Trusted Computer Product Evaluation Criteria (CTCPEC)) from the participating countries. All the CCEB members attended the workshop and were available for any questions that the other participants may have had.

The workshop focused on specific problems that were identified in the comments but did not focus on a line-by-line review of the text. First, global issues that transcended the various areas were identified in a plenary session. Then, the global issues, as well as issues from each of the separate areas (functional requirements, protection profiles, protection profile creation, development assurance, evaluation assurance, CS protection profiles, LP protection profiles, and issues on international harmonization), were discussed in separate breakout sessions.

The purpose of this proceeding is to inform the Federal Criteria commentators and the workshop attendees of the outcome of the workshop. Also, this proceeding will be used as a blueprint for updating the Federal Criteria. This proceeding, and the revised portions of the draft Federal Criteria contents, will be the two principal NIST/NSA inputs to the CCEB. Priliminary plans for dealing with the Federal Criteria comments are included in this document, and all revisions will be performed under the direction of NIST and the NSA.

The plans for revising portions of the draft Federal Criteria are still being determined. Note, however, that all the topics listed in the Executive Summary in the next section are considered to be important and will be input to the CCEB. After specific plans for the revision are finalized, these plans will be made available to all those who commented on and attended the workshop for the draft Federal Criteria.

The next section of this proceeding gives the Executive Summary. This is followed by the moderator reports for each of the individual breakout sessions. Then the plan for future work on the Federal Criteria, which is a direct outcome of the comments and the workshop, is described. The appendix gives the text of the public announcement on the Common Criteria effort.

CHAPTER 2 Executive Summary

The one issue that dominated the vast majority of the comments and workshop partici-pants was the need for the next criteria to address distributed systems, networks, encryp-tion, and PC security. These areas were discussed extensively in the workshop but were not specifically addressed since there was no text in the present draft of the Federal Criteria to discuss, and since a working group had already been established to look at these issues. However, there was clearly a mandate from the commentators and from the participants that the document is severely deficient without these requirements and that any future criteria would not be fully useful unless these issues were addressed.

Also, the majority of the participants felt that there were several elements of the Federal Criteria that should be retained in the progression to the Common Criteria, especially the notion of a protection profile. The participants liked the idea of creating protection profiles by assembling them from pre-defined components. However, the participants also felt that the make-up of the components themselves should be revisited. They felt that the ordering and the grouping of component requirements should be re-examined, and that the interdependencies among the various components and of particular require-ments in a single component should be made more clear.

The participants also felt that there was a problem with TCSEC compatibility. One of the main goals of the Federal Criteria work was the incorporation of the TCSEC requirements. This was not only in recognition of TCSEC technology but also for back-wards compatibility for those products that were created against the TCSEC. The measure of this incorporation was the creation of protection profiles that reflected the TCSEC classes (with CS1 addressing the TCSEC's C2 class, and LP1, 2, 3, and 4 addressing B1, B2, B3, and A1, respectively). However, the participants felt that this goal was not met. They felt that neither the draft Federal Criteria nor the LP protection profiles that were created properly represent the TCSEC classes. They felt that the LP protection profiles and the components used to create them should be rewritten.

The commentators and participants also felt that there was a need for the Federal Criteria to go beyond the scope of stand-alone products. They also felt that the relation-ship of protection profiles to security targets was not made clear. Although not specifi-cally addressed in the Federal Criteria, many commentators and participants also took the opportunity to express their concerns about the present evaluation process and the issue of mutual recognition of international evaluations and certificates, especially in light of the Common Criteria effort. There were also concerns expressed on how protec-tion profiles should be standardized, registered, and vetted, and on the international vetting of protection profiles.

CHAPTER 3 Global Issues

Overview

As reflected in the comments, there were several global issues that transcended discus-sion in a single area. The global issues session was created to reflect these comments. Four global issues were identified: Federal Criteria benefits, the concept of Protection Profile, the concept of components, and products vs. systems. All of these topics were introduced in a plenary session, and then discussed individually in break out sessions for the rest of the morning. Then, these (and other topics) were discussed in a global issue session that continued through the afternoon. It should be noted that different concerns were expressed in the morning and afternoon groups, and that for one of the global issues there was a divergence of opinion. Where this divergence occurred will be indi-cated in the following text.

Each of these areas are discussed below. Note that no differentiation is made between what the morning and afternoon groups discussed except in the area where there was a divergence of views.

It should also be noted that there were several global issues in the comments that were not addressed in this session even though most reviewers expressed concern about these areas. These are: networks, distributed systems, low end PC security, and encryption. There was an agreement that these issues not be discussed during the workshop since there was no intent to address these areas in this particular draft and since there was no text in the Federal Criteria on which to base this discussion. However, these issues were brought up in the plenary question and answer session and many in the audience expressed the opinion that these areas should be addressed.

Federal Criteria Benefits

This session focused on a variety of subjects and these topics will be important as we move to the Common Criteria. It also focused on several flaws of the Federal Criteria, and these will also be reflected in this report.

In general, the group agreed that the following were Federal Criteria benefits:

- The unbundling of functional requirements from each other and from assurances.
- The creation of protection profiles by assembling pre-defined components and elabo-rating them to specific product targets.
- The explicit separation of documentation, process, and evaluation assurance.
- Recognition of Ease of Use, Physical Protection, and Flaw Remediation (this was thought to be especially important to retain) as requirements.

Protection Profiles

There was a lot of discussion on the notion of a protection profile. The consensus among both groups was that we need the notion of a protection profile, and that protection profiles describe what a consumer wants and what a vendor should build towards. Protection profiles go hand in hand with risk analysis. They were felt to be a useful consumer's tool to spell out requirements. Protection profiles provide the basis for market driven requirements, ease flexibility in presenting requirements, and improve the credibility of the ITSEC's notion of "effectiveness." [The ITSEC defines "effective-ness" in security evaluations as being an aspect of assurance that assesses how well the applied security functions and mechanisms working together to actually satisfy the security requirements.] Documenting the environmental assumptions in protection profiles were felt to be a beneficial feature.

However, several concerns were expressed about protection profiles. One of the ques-tions asked was, What is the value of a protection profile as an evaluation entity? It was felt that consumer needs do not have to be evaluated, but that the notion of how the product satisfies those needs do. It was felt that the definition/purpose of what is a protection profile is not clear in the Federal Criteria. The group came to the conclusion that protection profiles are a "what" definition, i.e., that protection profiles state what the functional and assurance requirements are, and a security target is a "what" and "how" definition, i.e., that security targets state what the requirements are and how they are being met for a particular product. The group also felt that in some cases products should be able to be developed without a protection profile when, for example, a unique product is being built, or when a generalized statement of requirements is not needed.

The group also expressed the opinion that protection profiles facilitate governments and other agencies in getting their security requirements in front of vendors. To be useful, protection profile creation needs to be market driven. The user groups that will have an interest in creating profiles include not only end-user groups, but integration contractors and value-added resellers as well. Vendor market-research groups may also be in a good position to know both what is needed and what is feasible. Thus, even though profiles are designed to express user needs, vendors may also become actively involved. If similar security targets continue to be produced and used, someone will realize the value of extracting a common protection profile from them. It was felt that in the long run, security targets will be a source of protection profiles.

The global issues group felt that the creation of protection profiles may be too hard for consumers to vet even though consumers have needs that don't map to the TCSEC. The group felt that protection profiles are really application profiles for various commercial industries, e.g., financial, telecommunications, etc., but did not feel that the market will create these protection profiles without some government intervention. The group felt that it was unrealistic to assume that consumers will "get together" to create protection profiles, and they felt that the government (e.g., NIST, Information System Security Association (ISSA)) should take a leading role in sponsoring the creation of protection profiles, and should assemble people from these various industries for the purpose of putting these profiles together.

There were also many concerns with how many protection profiles there was going to be and what mechanisms or controls would be in place to limit the number of protection profiles. The global issues group felt that the proliferation of protection profiles may be self constraining because of the number of resources that are needed to create the protection profile. Several participants expressed concern that too many profiles will produce market fragmentation, thereby undermining a primary motivation for distin-guishing between profiles and security targets in the first place. The protection profile group expressed much pessimism on actually accomplishing control. The

problem of controlling the proliferation is related to the question of who will produce profiles: if their creation is privately funded, they may be registered only with their funding organi-zation. It was felt that vendors will probably aggregate profiles to cover more than one market and that products may be designed to simultaneously satisfy several different profiles. This already happens for products that are simultaneously evaluated against the C2 and B1 TCSEC classes. Because of this, it may be appropriate to consider profile composability so that vendors, evaluators, and consumers can better appreciate the implications of such products.

The protection profile group also felt that acceptance vetting could be performed in a decentralized or local mode. That is, there could be local registries of protection profiles, and also a centralized registry of profiles that can be used to coordinate consis-tency or to allow a vendor to gain information on the "largest common intersection of protection profiles."

The International Standards Organization (ISO) was discussed as a possible answer to the registration of protection profiles. Unfortunately, ISO has a reputation for being slow and unoriginal. This implies that for profile registration to be effective, other stan-dards bodies must be involved. The NIST FIPS publications could provide a more timely U.S. mechanism for registering profiles, at the expense of not being international. Registration issues differ for government and nongovernment profiles: national profiles presenting government security needs make more sense than national profiles presenting the security needs of a multinational industry or consumer group. The primary purpose of protection profile registries should be to create a sensible market-place for security ideas and products, as opposed to enforcing control over this market. Also, as past evaluations against the TCSEC classes have shown, the TCSEC require-ments change continuously under interpretation by evaluators. Consequently, a regis-tered profile needs to include points of contact that can explain the needs of the user group that produced the profile, in order to facilitate useful profile interpretation. Simi-larly, the profile registry needs to include, for each profile, a legislative history of how its (unintended) ambiguities have been resolved.

As to the registration of functional and assurance packages, one participant noted that functional requirements are more marketable than assurance requirements, and consumers tend to buy assurance only under duress. This suggests that there might be many functionality packages but relatively few assurance packages, with most assur-ance packages emphasizing straightforward third-party validation of vendor claims.

It was felt that the vetting process will help to establish the ITSEC's notion of "correct-ness." [The ITSEC defines "correctness" in security evaluations as being the preserva-tion of relevant properties between successive levels of representations. Examples of representations could be top-level functional specifications, detailed design specifica-tions, or an actual implementation.] It was also felt that vetters need to have enough authority to constrain originators, and that international vetting will indirectly alleviate concerns about export licenses. However, the Federal Criteria was not clear about the vetting process and who will pay for the vetting. It was also thought that a well-designed centralized registration process could provide cost-effective, high standards for the evaluation of protection profiles. Without protection profiles, this evaluation activity, much of which is needed for the evaluation of any conforming product, would be performed by many independent laboratories in multiple countries. This multiplicity could result in both a lack of uniform quality and duplication of effort from one evalua-tion to the next.

It was also felt that the vetting of profiles is inherently difficult. During the creation of the TCSEC, vetting of the evaluation classes involved lots of arguing. The challenge is to provide procedures which will make vetting routine, predictable, and well-under-stood.

As to the issue of whether there will be too many protection profiles, the group felt that this will not happen since it will take too much time and money to produce one. Market driven is an important concept - the government should only dictate what the security requirements should be for government agencies, not dictate to vendors what the secu-rity requirements should be for those outside of the government. The protection profile subgroup felt strongly that the market should do that. They also felt that profiles that were responded to frequently (as evidenced by having products created against them and by having them referenced in end-user procurements) would be the ones that would last. Thus, having a large number of profiles was deemed not too important. This concept reduces the need for government participation except as a local registry and as a provider of coordination services.

As to the question of whether the ITSEC notion of a security target is necessary or suffi-cient, it was felt that both profiles and security targets are needed because they serve different, complementary purposes. According to the participants, the most significant difference between protection profiles and security targets, by far, is the fact that consumer groups produce profiles whereas vendors produce security targets. As noted in the session on evaluation assurance, a security target includes not only protection profile information but additional design information and

justification that the design is correct. Security targets allow flexibility by providing a vehicle for a producer to specify security objectives, services, and/or mechanisms that exceed those found an existing profile. For example, many C2 systems meet the B3 Discretionary Access Control (DAC) mechanism requirements. Both groups felt that having a security target without having a protection profile may be sufficient in cases where there is no need to have a general set of requirements that several vendors can built to, or when specifying the security aspects of a "one shot" system or product prototype. If a single unique product is being built, a security target is all that is needed and can be evaluated against. The Federal Criteria needs to be designed in such a way as to not shut out good security solutions. Allowing products to be evaluated solely against security targets provides a means of addressing this concern. Such an evaluation can encourage a vendor to find a solution to a user's problem, even if it doesn't meet an existing profile.

The participants felt that the existence of a security target is always necessary in that it shows how a vendor meets a protection profile (when one exists), shows claims of what a vendor provides in absence of a profile, and shows claims of what a vendor provides beyond a profile. It was also felt that the relationship of a security target and an imple-mented product with respect to the evaluation process needs further clarification, and that the structural differences between protection profiles and security targets also needs further clarification. The participants concluded that when a security target can meet a variety of protection profiles, we may have the best marketing value.

The Federal Criteria allows but does not require the creation of linear profile hierarchies (as in the LP1 - LP4 series). One participant observed that since different environments have different risks, a linear profile hierarchy suggests that all risks in one environment at a lower profile hierarchy are included in some uniformly more risky environment in a higher profile hierarchy. In general, it was felt that there should be no requirement that protection profiles be hierarchical since this would be too rigid, but a number of protec-tion profiles could be considered as a family or hierarchy to give the industry some lati-tude for improvement. It was also felt that vendors will probably aggregate profiles to cover more than one market.

Components

There were a lot of issues regarding how the components were created that transcended what type of components (functional, development assurance, or evaluation assurance) they are, and the component group (morning) and global issues session (afternoon) were asked if the components ("building blocks") as created were a useful notion. There was a slight divergence in opinion between the two groups. The component group was unhappy with the existing components even though they liked the concept of a common language for building protection profiles. They felt that the Federal Criteria components as they are now stated do not help protection profile writers since few were happy with the Federal Criteria profiles and two-thirds of the existing components were not used in these profiles. However, the global session group liked the component approach. However, the divergence of opinion here is not that large since the global issues group also agreed that all the components should be re-examined.

The component subgroup was not sure a "common" component language was possible since there is no "algebra of building blocks", that is, it was unclear how one specifies component requirements at a uniform low level as the Federal Criteria attempts and how one should put these levels back together as a coherent set of requirements. Most (but not all) in that group felt that many functional requirements could be stated by utilizing an algebra, but that this would be more difficult for assurance requirements. The group generally felt that we as a community do not understand the ways in which components can be merged and therefore were very concerned that meaningless (and even harmful) requirements could be derived from what seem like valid components. The group was not convinced that just listing the dependencies would suffice to address this concern.

The component group also felt that the authors should state the basic principles behind the components that were built. They felt that if these criteria were not based on accepted scientific or engineering principles, they would not be valid. There was a strong consensus in the component group on this point. The most conservative members in the component group felt that the only basic principle that was stated in the Federal Criteria was that of the reference monitor, and that this was not satisfactory. The global issues group could not identify any basic principle beyond the reference monitor that could be a justification for why the components were built and therefore thought the "basic principle" notion would not help in building the components.

Both groups agreed that the ordering and grouping of requirements in the components themselves should be re-examined, however, the component group was more critical about the component content and felt that the

components should be recast. The compo-nent group felt that value added "features" should not be ordered (the global issues group could not see an alternative to this), but that other requirements should be strongly ordered and grouped (mostly the assurance components). The component group also felt that some components should have been further unbundled (these being mostly the functionality components). Also, both groups thought that components need not be of like ordering or granularity. The afternoon group thought that the present hier-archy with increasing levels may not necessarily create a product that is more secure, and agreed with the morning group that the separation of requirements into different functional levels were arbitrary (e.g., the auditing component). The global issues group stated that component requirements should not restrain implementations. The global session group also pointed out that there is a problem with the meaning of the word "level" in and of itself. For example, it was pointed out that if level 3 were chosen across the board for a protection profile, you would not come out with something reasonable. However, as opposed to the component group, the global issues group thought that the ordering and grouping should be re-examined and not done away with.

One suggestion was made in the component group for re-doing the component organi-zation. First, the basic principles should be documented. Then, the currently accepted industry "bundles", that is, all the criteria that is know as accepted (e.g., the TCSEC, ITSEC, CTCPEC, Minimum Security Functionality Requirements (MSFR), Trusted Database Interpretation (TDI)) should be used as a starting point and then value added features should be added unbundled and unordered. Then, the authors should carefully examined the "new" components that were created. However, the global issues session strongly disagreed with this suggestion. They felt that the components should not be re-done, and were unsure as to what basic principles can be identified. They felt very strongly that the TCSEC "bundles" should not be used as a starting point because the TCSEC "bundles" did not address commercial concerns. They also felt that the TCSEC did not represent all basic principles.

Both groups thought that the inter-dependency analysis between and among the various requirements in the components should be better spelled out since it will be difficult for profile writers to figure them out for themselves. It was felt that for each "shall" in the Federal Criteria the dependencies should be identified and listed with each component. It was also felt that the Canadians did this in a more straightforward fashion in that all their dependencies were highlighted in boxes with each component, and that we may not be able to map out all the dependencies.

The component group felt that new or modified requirements were introduced in too great a volume, but the global issues group thought that this could be only a document organization problems. The component group also felt that the document organization should be re-examined and the Federal Criteria should be minimized. They also would have liked to have seen the functional packages. The component group also felt that the Federal Criteria should limit the requirement statements to accepted engineering prac-tices rather than research ideas (but not exclude adding new accepted ideas), but the global issues group didn't see how this statement applied to the Federal Criteria - the only research idea that they could remember was real time audit alarms. The component group identified several items that they felt were not well accepted. These included the requirements for both functional and penetration testing as defined in the Federal Criteria since they are significantly different from the ITSEC and TCSEC, the require-ment for using "high-level synchronization," the allowance for layering violation, and the use of multi-threaded tasks for Trusted Computing Base (TCB) structuring.

Products vs. Systems

The first discussion focused on the different approaches to "products" and "systems" in the ITSEC and FC. Someone from the audience stated that the Federal Criteria is only applicable to a "product," while the ITSEC was applicable to both "products" and "systems." [The ITSEC defines a "product" as being a package of IT software and/or hardware that provides functionality designed for use or incorporation within a multi- plicity of systems. It defines an IT "system" as being a specific IT installation with a particular purpose and operational environment.]

Part of the problem is semantic. The definitions appear to be overloaded. "Systems" appears to refer to both actual environments of use as well as assemblies of products. The definitions also seem to be dependent on the observers viewpoint. A supplier may be a "system integrator" who employs "products" to produce a "system." But to the integrator's customers, the resultant integration may be a "product" offered for sale.

Some people thought that additional concepts existed between "products" and "systems." Others thought that the problems were all in the semantics.

Next, the group addressed the re-use of "product" evaluations when the "products" are integrated into "systems" or larger products. The consensus was that the "product" eval-uation produced by the existing Trusted Product Evaluation Process (TPEP) are not re-usable. The published evaluation reports appear to be designed as final reports, not as intermediary vehicles for conveying information for subsequent re-use. For example, detail and proprietary information are excluded. Limited re-use might be possible with respect to correctiveness, but only with many caveats. A need was expressed for a rigorous methodology, referred to as an algebra, for combining various evaluation results.

On a positive note, they felt that the knowledge gained from looking at previous evalua-tion results were useful from a social point of view in that it gave the reader some knowledge as to who performed the evaluation and how much they could be relied upon.

The combination of several products was referred to as composition. It was the group consensus that composition depends on architecture, design, and interface specifica-tions. Without specifications for interfacing security-relevant parameters between prod-ucts, composability will be difficult and re-use of evaluation results next to impossible. Security interface specifications are probably the key to evaluation re-use.

The majority of this group thought that it is practical to specify generic criteria that could be used for either products or systems.

Miscellaneous Issues

Several other points were brought up in the global issues session. These are listed below.

Other Federal Criteria Benefits

- The flexibility found in both the functionality and assurance requirements should be preserved.
- Ease of "Secure" Use (it was felt that the component title "Ease of Use" was not descriptive enough) is an important security concern and should not be deleted.
- The System Entry component was also felt to be an important security concern that should not be deleted.
- The commercial protection profiles were thought to be a good start.
- The notion of safe defaults should be preserved.

Other Federal Criteria Concerns

Objective measures: There was a great deal of discussion by the commercial vendors that objective measures may not be necessarily useful to the customer and that the Federal Criteria has to strike a balance between sticking to measurable requirements vs. making value judgements (which can be product differentiators).

Flaw Remediation: In general, the global issues group liked the Flaw Remediation component, but some commercial vendors where concerned that how flaw remediation was addressed may depend on the severity of the flaw and that the issue may be "who do you tell what to when." They also felt that they wanted the freedom to tell a customer to apply the fix without revealing what the particular problem is (for security reasons) and that this was not spelled out in the Federal Criteria. Also, how one prevents the intro-duction of flaws during flaw remediation should be addressed.

Development and Evaluation Assurance: The group felt that the separation of evalua-tion and development assurance requirements as now found in the Federal Criteria may not be useful.

Evaluation process: The group was not happy with the evaluation process as it now exists and felt that the evaluation process is a ten year experiment that has failed. It was pointed out that in Europe the evaluations of products only occur when the customer demands it, and the Federal Criteria in and of itself has value even if no evaluations are ever done against it. Some commercial vendors stated that "designed to meet" has some relevance to the consumer, although others stated that this phrase could just as easily be used to mislead the consumer. However, the protection profile group also felt that there needs to be some way of encouraging truth in advertising; vendors too often have prod-ucts evaluated in unusable configurations, thereby defeating the whole purpose of the evaluation process. This might be done via constraints on the vetting of profiles and the evaluation of security targets. One light hearted suggestion was for the government to copyright profile names, requiring that they not be misused, just as the Ada Joint Program Office copyrighted the use of "Ada."

Rating Maintenance Phase (RAMP): There was a concern that the RAMP process was not addressed in the Federal Criteria.

CHAPTER 4 Functional Requirements

Initial Topic Issues

Based on analysis of the comments to the Functional Requirements the following set of issues were presented for discussion. Whenever possible, people who made insightful comments were invited to present their positions.

- Precision in Terminology
- Identification and Authentication
- Access Control
- Availability & Fault Tolerance
- Policy Neutral Criteria
- TCB & Reference Monitor Focus
- Integrity
- Open-Ended Criteria
- Issues from the attendees

The ground rules for discussion were to focus on philosophy & high-level issues. Word-smithing was to be handled by the written comments. The objective of the workshop was to seek guidance and direction. Multiple options were considered useful, especially if statistical indicators such as distribution of opinions and variance were captured.

Precision In Terminology

Martha Branstad of Trusted Information Systems presented issues concerning precision in terminology. She emphasized that the Federal Criteria must be meaningful and under-standable. Her focus was on arriving at a definition of security. She quoted Dan Sterne's definition of a security policy objective as "A statement of intent to protect an identified resource from unauthorized use" and emphasized that security is not synonymous with correctness.

The ensuing discussion surfaced several incompatible positions concerning definitions of information security. The pragmatic position was that information security encom-passes whatever activities are conducted by people whose function is to support infor-mation security. The theoretical position was that information security consisted of those objectives and controls that could be supported by a single technological mecha-nism, namely the reference monitor. It was also observed that just because a concern is important, or even critical, doesn't make it part of security. It was suggested that combining too many concerns under the rubric of information security dilutes the focus.

Identification and Authentication

Presentations on Identification and Authentication were made by Russell Davis of PRC and Robert Bosen of Enigma Logic. Both their presentations and the discussion focused on passwords. Overall, they felt that the FC should not specify implementation mecha-nisms. "The Federal Criteria should lead but not mandate the way."

Although networking issues had been declared out of bounds during the opening plenary session, there was general consensus that plain text transmission of passwords was too important a vulnerability to ignore. Network monitoring hardware and software makes it very easy for passwords to be compromised. Users without private offices were identified as being vulnerable to password compromise.

In light of these well-known vulnerabilities of passwords, there was considerable senti-ment that too much emphasis was placed on password selection and generalization. Lack of human engineering was also cited as a problem, especially when more than one password must be memorized by a user with multiple computer systems and accounts. Removal of password guidance to a separate document was strongly advocated.

The absence of any material addressing authentication by means other than memorized passwords was considered a gross oversight. Various technologies were mentioned, including smart cards, trusted path, and encryption. Biometrics were not mentioned during the session.

Access Control

Joe Sirrianni of the Air Force Cryptologic Support Center and Ravi Sandhu of George Mason University presented their views on Access Control. They felt that Access Control is the single most important issue, perhaps after Identification and Authentica-tion. They admonished the working group to start afresh and write clearly. In particular, they pointed out that Access Control is a mechanism and that it was unwise to force a policy legacy from the TCSEC onto the new criteria, suggesting that the TCSEC should be preserved as a protection profile and not as Access Control Functional components. See the discussion on policy neutrality for more on this point. They suggested that the granularity of the Access Control component is too coarse; it should be subdivided. Questions were raised about the validity of comparing Access Control ratings between two products or profiles. For example, CS2 and CS3 contain dissimilar extensions to the AC-2 component. Separate rating of Access Control components according to the policy enforced was suggested.

Availability & Fault Tolerance

Presentations on Availability & Fault Tolerance were made by Vic Marshall of Booz, Allen & Hamilton and Holly Hosmer of Data Security. They pointed out the need for worked general-purpose examples to aid in assessing these attributes. There is no agree-ment on what any of this means. It is an application-dependent issue; for example, prevention of denial of service in one application inappropriately denies service in another.

Availability covers much more than security; availability is not a security service, according to GOSIP. Denial of service is only one type of threat. Resource allocation is a duty of the system administrator. Fault management is not security management. The TCB should be expanded to provide these services. The components of availability are containment, fault tolerance, robustness, and recovery. Customers take a holistic view; so should the FC.

Policy Neutral Criteria

There were several comments that the FC failed to meet the stated goal of policy neutrality. Policy is implied in many places. There is no technical rationale and justifica-tions for the statements about policy neutrality. We know how to build things that enforce some confidentiality policies; we do not know how to build things to enforce availability and integrity policies. The fundamental mechanisms that work for one policy do not work for the others. When one starts requiring policy, one restricts innova-tion in design of policy. The requirement to define a policy was not stated clearly or obviously.

The components are replete with policy. For example, System Entry is a policy issue. “The TCB shall appear to perform the entire user authentication procedure even if the user identification entered is invalid” is an I&A policy issue. Policy is ANYTHING which restricts the methods by which the vendor can meet the requirements stipulated in a given functionality or assurance component.

Discretionary Access Control (DAC) assumes that the individual user is the funda-mental policy attribute on which the controls are based. This does not have to be so; for many commercial uses, it should not be so. A requirement for fail-safe default parame-ters is logically impossible because definition of “safe” is policy dependent in a very complex way. The FC appears to prevent a policy which preserves the anonymity of users.

TCB & Reference Monitor Focus

A presentation concerning focus on the TCB and Reference Monitor was made by Sven Larsson of the Swedish Defense. Considerable polarization focused on TCB & Refer-ence Monitor concepts. (At one extreme was the position that the FC exhibits a lack of underlying principles from “basic science.” This was understood to refer to the Refer-ence Monitor concept as the principle basis for secrecy and integrity. Rigorous mathe-matics has been applied to the Reference Monitor.) The FC omits the partitioned TCB, balanced assurance, and TCB subsets. From this viewpoint, the FC fails to protect against deliberate acts of a hostile opponent; rather it relies on “penetrate and patch.”

The contrasting position holds that the TCB and Reference Monitor are merely a design concept. They represent one way to design an operating system and that design concepts should be covered under assurance, NOT functionality. A question was raised as to whether the Reference Monitor concept is still suitable when information flows from one computer system to another in a network. In this instance there is no single state or single domain and security

information needed by the Reference Monitor is not strictly under its own control. Software that implements any functional security requirement is part of the TCB.

Somewhat between the extremes are observations that a TCB should really protect against malicious software. The TCB sometimes is not distinct software within a product. The TCB may not be identifiable or minimal; it is often the entire product. Appendix B in the Federal Criteria, "The Reference Monitor Concept," does not accu-rately reflect the notion of the Reference Monitor.

Integrity

Gary Grossman of Cordant made a presentation on integrity, introducing the concept of integrity problems which do not involve a subject or access control. Examples include hardware noise and component failure, software bugs and viruses, and errors by privi-leged users.

Considerable discussion focused on the question as to whether the TCB concept applies to integrity. The FC does not provide for the notion of an integrity TCB. One position is that an integrity TCB is significantly different from a traditional confidentiality TCB. It necessarily includes application- specific components and well-formed transactions. Access control solves a very small (albeit important) aspect of the integrity problem.

There is no mention in the FC of how security management affects integrity.

Open-ended Criteria

The FC and all the components are stated to be extensible, but most of the comments appear to assume that the components presented in the FC constitute the entire set. Why is the message not getting across?

Structure of Requirements

Sentiment was expressed that many of the components in Chapter 4 of the Federal Criteria have been randomly put into a hierarchy. The structure may be related to the policy that a particular system implements and/or the type of threat addressed. Since the relative importance of threats will vary among environments, a hierarchy is not appro-priate.

Summary of Functional Requirements Discussions

The discussions concerning functional requirements are summarized in this section, grouped into the following areas.

- Defining the scope of security
- Integrity
- Policy Independence
- Identification and Authentication
- TCSEC Compatibility
- Access Control

Defining the Scope of Security

Definition of the scope of "security" is a management decision. Two alternatives are:

- Accept the current usage of the term. All work done by people who are called secu-rity professionals should be accepted as "security work." This includes support for availability, recovery, and fault tolerance.
- Taxonomize according to a fundamental technology basis. Security should be those activities that can be supported by a Reference Monitor. Availability, recovery, and fault tolerance are excluded.

Keeping disciplines separate does not diminish their importance. Just because a problem is important or even crucial doesn't make it security. Specialists in various disciplines can work together.

Integrity

Even after many years of work, there is no agreement on definition. Perhaps the FC should focus on specific protection policies, such as protection against unauthorized or undesirable modification, without trying to achieve a comprehensive definition of "integrity." That is, get on with the work and stop arguing on what name to call it. There appears to be insufficient recognition that protection against unauthorized or undesirable modification is considerably different in malicious and non-malicious environments.

The implications of applying the TCB and Reference Monitor concepts to "integrity" need to be studied. It is unclear whether an integrity TCB is a valid concept compatible with the concept of a confidentiality TCB. In many cases the integrity policy is in the application. Extending the TCB and Reference Monitor to encompass applications needs further study. In many cases the application is specific to a system; in these cases, integrity cannot be addressed in a product, only in a system.

Further understanding of the interaction of multiple policies in operating systems and applications is needed. New models may help. The terms "mandatory" and "discre-tionary" do not appear to be rich enough to characterize the integrity concerns.

Policy Independence

Protection profiles should include polices, but components should not have a policy bias. In many cases there may be a one-to-one relationship between a policy and a component. This relationship should be explained. Alternative components should be provided for other policies. In some cases the policies, and the corresponding compo-nents, may be diametrically opposed. The set of available components should be as inclusive as possible.

There are many policy assumptions and biases throughout the FC. For example, Identi-fication and Authentication, System Entry, and Accountability are all policies. Many people appear to find it difficult to acknowledge an unfamiliar policy; they tend to think that the policy they are familiar with is "right" and the unfamiliar is "wrong."

Identification and Authentication

Identification and authentication must be strengthened. There is too much emphasis on passwords, especially when privacy is not assured by physical means. Passwords alone are insufficient in many cases; provision should be explicit for alternative technology.

A common authentication approach is needed. The FC should not specify mechanisms.

The FC should lead, not mandate, the way.

TCSEC Compatibility

The TCSEC should be preserved as protection profiles, not as functional components. An open question remains concerning incorporation of knowledge gained, and require-ments changes made, since publication of the TCSEC.

Access Control

Access control is a mechanism that can enforce many different policies. The tendency to embed policy in access control should be resisted. Role-based access control is not well understood. The interaction between role policy and mechanisms is hard to unravel.

CHAPTER 5 Evaluation Assurance

Introduction

This session addresses those comments pertaining to evaluation assurance and evalua-tion processes. In general, this pertains to Chapter 6 of the Federal Criteria (FC) but some issues will overlap with those of other chapters, and with general issues to be considered by the drafters of the FC.

Session Preparation

To stimulate discussions during the session, an initial list of key discussion topics was constructed from the written comments provided by the FC reviewers. These are outlined below:

- Role of Evaluation-Assurance Requirements. From the comments, the proper role of evaluation assurance requirements in the FC does not seem be fully understood or agreed upon. This prompted such basic questions as the following: Do we need Evaluation Assurance Requirements? Should they be a separate set of requirements? Should they be included in protection profiles?
- Evaluation Processes and Organizations. Some reviewers thought that Chapter 6 should have said more about evaluation processes and organizations and should have given more explicit advice on how to handle subjective aspects of evaluations. How should the evolving FC incorporate these thoughts?
- Need for Additional Material. Some reviewers felt that Chapter 6 was insufficient with respect to current technologies and assurance techniques. Others thought it went too far in presenting options that have not been tested in existing evaluations. What should be the form and content of evaluation requirements? What should constrain the evaluation requirements?
- Inter-chapter dependencies. These comments were particularly troubling with respect to Chapter 6. Some reviewers recommended explicitly mentioning all depen-dencies on previous chapters. Others recommended that the requirements be recast in more general form in order to eliminate unnecessary dependencies. How should dependency linkages be addressed? Again, what should be the form of evaluation requirements?
- Miscellaneous Evaluation-Specific Issues. Some reviewers also thought that the evaluation methods presented in Chapter 6:
- assume an evaluation process that is not appropriately tied to product develop-ment cycles.
- do not provide evaluators with enough (subjective) latitude with respect to au-thority for evaluation progress.
- lack clarity, objectivity, and simplicity.
- fail to provide explicit objective measures of what counts for success.
- do not properly meld evaluations for Protection Profiles, Security Targets, and Products.

Session Overview and General Observations

The session began with an introductory briefing on the purpose and scope of the session tasking. The moderators provided background on how the current evaluation chapter evolved. This included working group discussions on whether the draft FC should include:

1. evaluation authorities and organizational structures (e.g., Trust Technology Assess-ment Program (TTAP)),
2. specific forms of an evaluation process (e.g., Trusted Product Evaluation Program (TPEP) Process Improvement Team),
3. qualifications of evaluators,
4. specific evaluation techniques and methods, and/or
5. evaluation metrics.

It was explained that it had been decided that the first three items in this list were deemed to be out-of-scope because they are essentially business decisions and could change. Therefore only the last two items were addressed in the FC. It was also explained that this caused many reviewers to see this chapter as being incomplete.

Finally, the moderator introduction included the presentation of the above “key” ques-tions prompted by a review of all the public commentary on evaluation assurance in the draft FC.

This initial context set a constructive tone and allowed the participants to respond with positive direction and comments. The essentials of the session discussions are captured below.

While the session was lightly attended, the session had a good cross-section of interests and opinions. The participants consisted of approximately 9 individuals representing vendors, accreditors, integrators, European CCEB, National Computer Security Center (NCSC), National Security Agency (NSA), and evaluators. Their participation was generally lively and discussion extended well beyond the allowed session timeframe.

With respect to workshop consensus, the size of this group precludes any results of this session “speaking for the workshop.” However, the items (key questions) used to stimu-late the discussions were developed from the

"consensus" of the written comments produced by the FC reviewers on assurances in general and Chapter 6 specifically. Although directly impacting Chapter 6, the "guidance" themes that resulted from these discussions became more global in nature than specifically addressing Chapter 6. Perhaps this is because of the "back to basics" approach taken by the group. The single major conclusion of the discussions was that evaluation assurance should take a different form. This is discussed in more detail below. There was simply little else to say to directly improve any material currently written in Chapter 6 until the basics were covered.

Specific Observations

Role of Evaluation Assurance Requirements

In response to the question, "Do we need evaluation assurance requirements?," the general opinion of the participants was "globalized" to state that evaluation criteria should be the central aspect of the FC. That is, the document should be product and/or system infosec evaluation criteria. It does not quite achieve that now. It should provide appropriate product and/or system evaluation perspectives. The essential themes of such an evaluation criteria not only should be telling the vendors what to build into their products (the FC does this), but telling them what counts for success. This means detailing what evaluators must do to assure that the product actually meets the success criterion and telling vendors and evaluators both what and how they should document and report the achievement of a successful evaluation in a meaningful way. If the Protec-tion Profile concept is to prove adequate, it must provide such criteria. The components in Chapter 6 do not now support this "global" set of evaluation requirements.

In arriving at guidance, the discussion evolved around three audiences for evaluation criteria: accreditors & certifiers, who must use the output of product evaluations; evalu-ators, who must assess both the product and the processes that produced it; and vendors, who must be responsive both in terms of their product and their (development assur-ance) processes to the criteria requirements. It was proposed that the FC should start with the requirements of the system accreditors & certifiers to derive what is necessary with respect to reporting product information and conveying the assurance gained by product evaluation and vendor product development. The FC authors should then back into what must be done to produce that information and assurance. Additionally, to avoid non-useful products, the criteria must take a system's view with respect to product use and secure extensibility. Finally, to ensure that appropriate products can be acquired for systems, there needs to be an explicit tie-in with government acquisition regulations. Evaluation requirements should be written in such a way that they can be used in procurements, so that a statement of work (SOW) can make use of them (i.e., the Data Item Descriptions (DID) should be visible in, or capable of being assembled from, the product criteria). Current criteria cannot be so used because it is too vague-thus, many of the requirements are not contractually enforceable.

Perhaps most importantly, the discussion of the issue of who are the intended recipients of product evaluation information raised the issue of the proper specification of product evaluation output (e.g., the Final Evaluation Report) which in turn could lead to changes in the evaluation process or to changes in trusted product criteria. Here the discussion indicated that expression of a trusted product must contain some system implications (e.g., the proper way to securely interface the product to communications products which are also trusted; the way to extend the product's TCB). The FC must ensure that interface and extension issues are properly dealt with in evaluations.

For example, accreditors are typically asked to accept modifications of evaluated prod-ucts, and are often faced with unevaluated products built on evaluated platforms. They need help with questions such as the following: Was a given DBMS built on a B1 plat-form in such a way as to destroy its B1-ness? What is the impact of adding Ethernet cards and/or X-windows? Can I&A be done with smart cards or biometric devices instead of with passwords?

>From an accreditor's point of view, the issue of composition of secure products is a real concern. TCSEC evaluations typically have not dealt with this issue. The Trusted Network Interpretation (TNI) and TDI interpretations take some initial strides by articu-lating partitioned and subsetted TCB architectures. However, what is to be provided in evaluation reports with respect to allowable "trusted composition" alternatives (e.g., the methods for interfacing an application on the product when one or both have been eval-uated, or when the evaluated product is connected to another with a different trust rating) should be included in the criteria. Further, if one is connecting products together for performance reasons, what are the limitations with respect to preserving the TCB-ness of the evaluated products?

Another issue that was discussed was missing material that was needed by the accredi-tors. For example, the FC contains no specific support for downgraders and other filters. Accreditors routinely use this kind of functionality and would greatly appreciate evalua-tion support for it.

Almost as an aside, but still very important, a comment was made regarding main-taining a history and rationale for key decisions regarding the system architecture and design. Such information, if made available to accreditors, certifiers, and integrators could be very instructive. It would also be extremely useful for any product evaluation.

The need for evaluation assurance requirements was recognized by everyone present. It was strongly felt that evaluations must be useful to those who would make use of them. This general point came across much more forcefully in the working session than in the various written comments. It was felt that one of the major shortcomings of the TCSEC was that it failed to appropriately articulate and constrain what evaluators do. The rationale expressed for needing evaluation assurance requirements included: (1) ensuring that vendors and evaluators know "what they are getting into,"(2) ensuring uniformity of evaluation, "what counts for success," across organizations and nations, and especially (3) improving the utility of the evaluation output.

Other primary points of this discussion were the following:

- Evaluations should be geared to ensuring that those who use the results of evalua-tions get what they need to know.
- Evaluation must be done in such a way that it doesn't break easily under product deployment.

Inter-Chapter Dependencies

The discussion included global perspectives on the expression of requirements. Since we don't want to be too general or too prescriptive, the requirement for expressing what to build and what counts for success remains an issue. From the discussion, we still seem to have bi-polar views endorsing on the one hand, increased generalization to allow vendor flexibility, and on the other hand, increased detailed specifications to constrain evaluator interpretations. Since the criteria written to date, including the FC, provide mostly generalized expression of requirements, the criteria themselves mandate both vendor and evaluator interpretation. This is a natural process, but it has led to adversarial relationships and some "religious" conflicts between vendors and evalua-tors.

It was noted that dependency linkages between and among functional, developmental, and evaluation requirements should be explicitly noted at appropriate points in conjunc-tion with a requirement statement.

One thing that did seem important to the discussion was the need to express the func-tional and development requirements in measurable (qualitative and/or quantitative) terms and directly link both vendor and evaluator actions to these requirements. This action linkage is important whenever the requirements are qualitative, and subjective judgement must be applied.

Additionally, the issue of proprietary information contained in evaluator criteria inter-pretations was discussed. Since many, if not most, of these evaluator interpretations involve assessments of one or more vendor's solutions (expressed in proprietary terms) against a particular TCSEC requirement, these interpretations are not available to the vendors at large. Since the evaluators' interpretations provide a measure (in some cases an extremely significant measure) of what counts for success, a means to publicly express this measure, without compromising proprietary information, must be devised.

Evaluation Organizations and Processes

The discussion also included the issue of the evaluation process. The only security product evaluation organization with extensive experience is NSA. The European Commercially Licensed Evaluation Facilities (CLEFs) and the use of the ITSEC/ ITSEM (Information Technology Security Evaluation Manual) is only just beginning. The NIST TTAP proposal remains on the "drawing board" in a conceptual form awaiting additional details, approval, and resources. Thus, the discussion of process was only discussed at a very general level. However, some important issues did arise.

For example, since evaluation processes are not publicly articulated in detail, the "up front" understanding by both vendors and evaluators of what is involved in reaching an evaluation rating remains open-ended. It was

acknowledged that the U.S. TPEP Management Handbook has important process details that need to be made more public in a fashion similar to the ITSEM.

Taking a different tack, a suggestion was to examine new models of evaluations. For example, many software vendors do internal evaluations to better their products. The FAA does assurance by requiring an airplane vendor to get senior employees to certify the plane according to FAA standards. Thus, the vendor does the evaluation at the vendor's expense, using senior staff. The FC could provide a model for doing evalua-tions. Standards for the evaluation process need not only apply to outside evaluations.

Still another tack was the concept of standardized conformance testing suites. The subjectivity behind testing requirements could be greatly reduced by supplementing a protection profile with a conformance test suite. POSIX conformance tests were given as an example.

Significant in the discussion was the recognition that process information, being more dynamic, should be published separately from the evaluation criteria. This would allow for independent process evolution. The content of the Evaluation Criteria itself should be (from the point of view of business management) largely "process-free." It should be results oriented to achieve "objective" repeatability. An exception to this is subjective requirements which clearly require evaluation guidance (e.g., in the form of amount of testing per 1000 lines of code).

It was suggested that to make the criteria process-free requires that evaluator activities be "normalized" and linked to the functional and developmental requirements. Then, separate evaluation process and organizational documents for each type of evaluation agency can be produced, based on these normalized activities. These documents would be companion documents to the FC. These separate documents would contain the more dynamic business processes associated with evaluations (e.g., types of products to be evaluated, length of an evaluation, specific procedural interactions between the vendor and the evaluation team, use of a vendor security analyst, how many resources, qualifi-cation levels). They would not be a "standard" per se, but rather a set of acceptable eval-uation business practices that in actual use would be conditioned by organizational evolution, organizational goals, budget, available skilled evaluator resources, vendor readiness, etc.

Another point raised in the discussions was repeatability of results. This does not mean that multiple evaluation agencies must all be run in the same way, but rather that the quality of the output remains equivalent across evaluations (i.e., a product evaluated by one agency would get the same rating from another agency). If it is perceived that a vendor can get an "easier" evaluation from one or more evaluation agencies, then "shopping around" will occur and the entire process will lose credibility. Thus, proce-dures for maintaining quality control across evaluation agencies must be devised.

In summarizing this portion of the discussion, it was a primary requirement (strongly held opinion) of the group that the FC (or the ensuing Common Criteria) have such companion process documents produced concurrently with the actual evaluation criteria. Having the evaluation processes articulated and resources in place is especially important if the resulting criteria are to undergo a trial use period in a timely fashion.

Need for Additional Material

Evaluator Output: As stated above, requirements are needed as to how evaluators report on their work. The ITSEM contains specific requirements that aim to provide useful information about products in an Evaluation Technical Report. The importance of such requirements is underscored by widespread criticisms of Final Evaluation Reports as being neither timely nor meaningful to potential users of products. Accreditors need to be asked what they need, and evaluators need to receive feedback as to whether their reports are serving a useful purpose.

Closely-Held Source Code: A software assurance technique that is in neither the TCSEC nor the FC is to develop software using cleared users and then to only distribute the object code. An example was given where ITSEC E3 assurance would be needed if source code was distributed and ITSEC E2 assurance if not.

Other Significant, Relevant Issues

A few ideas provided during the working session on protection profiles seem to be more relevant to Chapter 6 than to protection profiles and are thus presented here instead in order to improve readability of the summary reports.

Need for Clarity. Requirements must be clear and unambiguous. Unclear requirements inspire an adversarial relationship between vendors and evaluators and slow down the evaluation process.

Assurance Objectives. How does one market assurance? How does one arrive at a concrete figure as to the value of a given kind of assurance? Other industries face similar questions. How does the phone company decide on a level of protection for a cable vault? How does an airbag manufacturer decide on the thickness of airbags?

Relevant NCSC Literature. There seem to be many relevant documents that are in review or have just come out that are relevant to evaluation assurance. One document that could contribute to evaluation aspects is "A Guide to Procurement of Trusted Systems," Volumes 1-4, NCSC-TG-024, December 1992. Other relevant draft docu-ments are being developed on improving Final Evaluation Reports, on the form and content of vendor test documentation, and on the form and content of vendor design documentation.

Security Targets and Protection Profiles. How should evaluators note that a security target or product is "better" than a profile? If a particular security target realizes some protection profile but also provides some additional features, then profile-vetting requirements may apply to these additional features, so that evaluation teams become involved in the same kinds of activities as profile vetters.

CHAPTER 6 Development Assurance

Working Group Objectives

The Development Assurance Working Group (DAWG) moderator presented the objec-tives and scope for the working group. The objectives for the working group were two-fold:

- Focus on philosophical and major technical issues, questions, or concerns with those portions of the FC that relate to development assurance requirements.
- For each issue/question discussed, attempt to identify possible solutions or alterna-tive directions that address the issue/question.

Several issues were specifically deemed to be in or out of scope for the working group. Specifically in scope were all aspects of technical "assurance" (excluding those issues based solely on evaluation activities which was the topic for a separate working group), and all related parts of the FC (which was principally chapter 5). Specifically out of scope for the DAWG were issues/questions that did not impact on the question of tech-nical assurance, or were solely related to evaluation activities; and technologies not currently within the scope of the draft FC (e.g., distributed systems, cryptography).

Summary of Written Comments

Prior to the workshop, the moderators reviewed the written comments on the draft FC. NSA/NIST received 111 sets of written comments. Fifty-seven of these contained comments specifically related to development assurance. To initiate technical discus-sions, the moderator presented a summary of these comments. The salient points from this summary presentation are captured in this section.

The moderator distilled the written comments into three general questions, and offered these questions as starting points for discussions. The questions were:

1. Is the FC's assurance paradigm satisfactory? If not, why and what are some alterna-tive approaches?
2. Does the expression of development assurance requirements as "components" have utility? Can assurance be defined as "components" that are composed into profile requirements? Can technical assurance requirements be defined generically in a way that would satisfy most needs?
3. What are the major technical problems with the FC's development assurance "components?" Are there any assurance technologies missing, misrepresented, or incorrectly stated?

For each of these questions, summaries or paraphrases of selected written comments were presented. These comments summaries are listed below. The items listed below are the moderator's paraphrase and/or summary of written comments as presented to the DAWG. They are not exact quotes from the written comments. The items are listed in no particular order.

QUESTION 1: Is the FC's Assurance Paradigm Satisfactory?

- The FC confuses the concepts of TCB and a reference monitor, and often ignores the foundational importance of these concepts. This can lead to developers spending endless effort addressing trivial issues and ignoring the more important concerns.
- The argument that some of the TCSEC's security architecture requirements are func-tionality, and not assurance, is inaccurate and must be re-thought.
- Despite repeated, detailed suggestions, the FC still fails to include Beta-testing as an assurance requirement. Beta-testing is a primary assurance method for commercial vendors.
- All of the assurance requirements apply to the TCB and not to the entire product.

This restriction is too strong. Some requirements, for example configuration management, should include the entire product.

- Operational assurance needs to be decoupled from the functionality requirements and treated separately from functionality and development assurance (much like the ITSEC's effectiveness requirements).
- We expected the FC would be able to handle conceptually complex systems.
- The FC suggests that the existence of a defined TCB is a mandatory requirement for any product to be evaluated. The ITSEC view is that while a defined TCB is a valid method, it is not the only method for achieving assurance.
- The chief concern is that the basis in science on which the TCSEC is based (i.e., the reference monitor concept) is clearly not the basis upon which the FC is founded. Certain aspects of some security policies (e.g., confidentiality and integrity) can be implemented with high-assurance using the reference monitor concept. Others cannot (e.g., availability). The FC should embrace the reference monitor concept for high-assurance while recognizing the utility (and limitations) of low-assurance mechanisms.
- The FC lacks a single, consistent assurance paradigm, and in some respects destroys the TCSEC's operational assurance requirements.
- Much of the FC constrains the implementation of a TCB in order to ensure that secu-rity is upheld. The ITSEC is much less constraining, and instead emphasizes ensuring that the security enforcing functions are implemented correctly and effec-tively.
- There is no direct equivalent to the ITSEC's effectiveness criteria, although many aspects of effectiveness are covered in the functionality and assurance components. Effectiveness should be treated separately.

QUESTION 2: Does the expression of development assurance requirements as "components" have utility?

- Many of the QUESTION 1 comments apply here.
- The "Construction of Profiles" chapter, which discusses how component are composed together, is difficult to understand, and the process it defines for compo-nent constructions seems overly complex.
- The assurance requirements are unnecessarily complex.
- The assurance requirements are easy to meet; breaking them into five separate divi-sions with impressive sounding names provide very little actual assurance but a major increase in the perception of assurance.
- The FC structure spends considerable effort emphasizing trivial issues (e.g., the specification of numerous security functions) and spends little effort on the issues of foundational importance (e.g., the reference monitor concept, assurance).

QUESTION 3: What are the Major Technical Problems with the FC's Development Assurance Components?

- Concepts are introduced which are neither commonly accepted nor adequately described. These include:

oo Design principles such as mandated use of "high-level synchronization constructs," multi-threaded tasks for TCB processes, and allowed layering viola-tions.

oo A variety of modelling concepts: "penetration models," "TCB isolation models," a "model of reference mediation," and a "model of access control."

oo Re-definitions of functional and penetration testing.

- Terminology is used in a confusing and historically inconsistent manner. Some examples are:

oo TCB, Reference Monitor concept, and Reference Validation Mechanism are misused and confused.

oo needless new terms like Descriptive Interface Specification (DIS) and Formal Interface Specification (FIS) are introduced in place of the understood and accepted Descriptive Top-Level Specification (DTLS) and Formal Top-Level Specification (FTLS).

oo the term "formal" is overloaded (i.e., using formal to mean something other than mathematical rigor).

oo the principal of least privilege is trivialized and mechanized.

oo the Bell-La Padula model is incorrectly defined.

- Evidence requirements have been separated, resulting in two different statements (with potentially differing interpretations) for the same requirement.

Summary of Working Group Discussions

Most of the working group deliberations consisted of "open, moderated debate." At the outset, the discussions were directed towards the three questions briefed by the moder-ator, plus any additional questions the working group thought were pertinent and that were within the DAWG's scope. One additional philosophical question was added to the moderator's list before debate begun:

QUESTION 4: Why does not the FC allow profiles to include the concept of "balanced assurance?"

As defined in the draft FC, a profile's assurance requirements are monolithic, i.e., they apply equally to all security policy features. The notion of balanced assurance would allow some security mechanisms (e.g., discretionary access control, virus detection techniques) to be implemented with less assurance than other security mechanisms (e.g., label-based protection, certain integrity constraints).

The DAWG did not have the opportunity to discuss this new question. No one objected to this question when it was first offered, and several participants noted their agreement. After further discussion, another question kept arising and merits recognition as an addi-tional philosophical concern:

QUESTION 5: What are the assurance objectives of the draft FC? What should they be?

As described below, several definitions for assurance were debated. A (rare) group consensus was that the FC should specifically motivate its assurance requirements with definitions and objective statements. It is possible for the FC to have multiple (different) assurance objectives.

The working group started by discussing the questions raised by the moderator, but the group dynamics quickly led to other related topics.

The remainder of this section captures the key points raised during the DAWG's discus-sion.

Definitions of Assurance

At the repeated prompting of one participant, the working group listed possible mean-ings for "assurance." This discussion is probably best characterized as an exercise in answering the question "What does assurance mean to me?" The following brief defini-tions were put forth.

- Techniques that provide "confidence" in the implementation of security mechanisms
- Risk/threat mitigation techniques (i.e., threats are important in the definition of assurance)
- Assurance = verification and correctness with respect to some specified objective
- Techniques that increase one's ability to analyze and understand the security mecha-nisms.
- Trustworthiness (as opposed to Trustedness-a reference for these terms was given to the paper by Peter Neumann titled "On the Design of Dependable Computer Systems for Critical Applications, SRI-CSL-90-10, SRI International, October 1990).
- Effectiveness, as defined in the European Information technology Security Evalua-tion Criteria (ITSEC)
- Reliability

- Vendor warranties and guarantees

In an attempt to bring the discussion back to the FC, the DAWG addressed the question of what did the FC mean by "assurance." To provide a basis for comparison, the group first addressed the question of what assurance meant to the TCSEC, the ITSEC, and the CTCPEC, all of which were sited as key source documents for the FC. Fortunately, there were individuals participating in the DAWG that were principal participants in the development of each of these standards and were able to offer their view of this ques-tion.

TCSEC: Evidence that a particular security policy is correctly implemented using the reference monitor concept

ITSEC: Effectiveness, correctness, and ease-of-use.

CTCPEC: Exactly the same as the TCSEC but for a potentially larger set of policies, i.e., evidence that some specified security policy is correctly implemented using the reference monitor concept. The CTCPEC also meant to "open the door" for vendor self-assurance.

Draft FC: Correctness and understandability, and maintenance of these traits over time (effectiveness was specifically excluded from this definition and is intended to be addressed by the protection profile development and acceptance ("vetting") process).

Process versus Product Assurances

The DAWG had a long discussion on types of assurances; specifically "product assur-ance" and "process assurance." Roughly speaking product assurance is gained through the design, implementation, and analysis of a product, and process assurance is gained through the controls and procedures used to ensure the quality, safety, and security of the development process and development environment.

Though the DAWG discussed this topic at some length, no general consensus was reached. The way in which this view of assurance is addressed by the FC was also not significantly discussed. Some felt the FC (and other security standards) focused too much on product assurances. Others felt the FC focused too much on process assurance, and that these were of lesser importance. Others still thought both were important, but had to be balanced with the expected threats and expected level of assurance.

QUESTION 2: Does the expression of development assurance requirements as "components" have utility?

The DAWG discussed this question at length. The general consensus was that compo-nents give the profile developer flexibility, but they also carry some significant liabili-ties. Much of the debate centered around these liabilities, and whether they justified the flexibility gained.

Liabilities Associated with Components

The liabilities discussed fell into two major areas:

- Complexity
- Problems with Reconstruction

Complexity: There was a consensus that the FC's current concept of requirement components and profile construction was too complex and may be impractical as defined. One person noted that the CTCPEC at one time had a component concept for assurance requirements, but removed it in favor of complete sets of assurance require-ments due to its complexity. It was noted, however, that the CTCPEC's components were targeted at vendors, evaluators, and system procurers whereas the FC's compo-nents are targeted at profile writers and approvers (with the presumption that this latter audience was smaller and more sophisticated). Most felt that the FC's current concept must be simpler to be successful. There was a great deal of concern about the possibility of technically inaccurate, invalid, or inappropriate profiles being developed. This last point led to the next liability: problems with reconstruction.

Reconstruction: The problems with reconstruction of coherent whole sets of require-ments from requirement components was discussed at length by the DAWG. The prin-ciple concern, which was labelled "bundled versus bungled" by one participant, is whether the breaking of coherent whole sets of assurance requirements into very small components and then reconstructing the whole requirement again introduces opportuni-ties for technically

flawed (and potentially harmful) protection profiles. Most of this discussion centered around the profile development and acceptance ("vetting") process, since the problems with reconstruction places a strong emphasis the profile "vetting" process.

Several participants noted that it will be difficult to maintain a "corporate memory" during the years in which the FC would be in effect. The prime example of this problem was an analogy of the TCSEC and its writers. For over a decade the vendor and evalu-ator communities have debated and interpreted the meanings of the TCSEC require-ments (the general consensus was that the TCSEC is a simpler problem than the FC since the TCSEC is itself simpler and more narrowly focused). Even though it was first published only ten years ago, and all of the authors are alive and active within the community, the rationale for the way in which the TCSEC requirements were constructed are not captured in any single place. Many experienced engineers misinter-pret its meanings and attempt to combine requirements in less than meaningful ways (examples of this latter case included rigorous design specifications for B1-like assur-ance, formal verification without formal policy models). No one believes what the TCSEC authors now say was their intent (this is the problem of the "authors being dead" once standards are published). Many working group members suspected that the same problems will occur with the FC, but will be amplified due to the codification of requirement components and the apparent encouragement of the development of many profiles.

Another concern with reconstruction focused on the possibility of combining two sets of requirements, and losing the meaning of one or both of them. One example discussed was combining information flow controls (i.e., covert channel handling) with some fault tolerance techniques. Fault tolerance often requires a lot of data to flow via many different paths whereas information flow control tries to restrict the flow of data to a few well-defined paths. It is unclear whether we understand what a combined fault-tolerant/ information flow control criteria would be, yet if both types of components existed (and each were technically sound as separate components), it is likely that a profile will be constructed the combines both of these requirements. The group felt that many other such examples exist, and were unsure that the "vetting" process could control these potentially harmful combinations.

The last concern with reconstruction was with the evolution of de facto standards. The issue is that, even assuming that the "vetting" process can control the quality of profiles, it is likely that vendors or some third-party organization will develop profiles that are not "vetted" and that these profiles will become de facto standards. Much of the discus-sion on this issue focused on the current NSA Trusted Product Evaluation Process (TPEP), and the ways in which some B1 and B1-like Compartmented Mode Worksta- tion (CMW) vendors imply that their products are B2, B3, or even A1-like since they were "designed to meet" certain higher-level requirements (which are never the really important and most-difficult-to-satisfy higher-level requirements). Many DAWG members felt that this problem will be even greater with the FC since requirement components are officially recognized and separately labelled. Vendors who, for example, may want to imply that their product is almost LP-2 or higher, can pick certain components that were part of LP-2 (but not the most important and most difficult ones), and claim that they meet them. Some felt that this was a significant flaw with the notion that the profile "vetting" process can control the quality of profiles. [FOOTNOTE: One person half-seriously suggested that the labels for components and profiles should be copyright protected as was done with Ada to prevent "unvetted" combination of requirements. Most felt this could not hurt-if practical-but would not address all the concerns.]

Liabilities versus Benefits

After discussing the potential liabilities with requirements components, the working group discussed whether the benefits of components out-weighed their liabilities. Most of the DAWG were reluctant to drop the notion of components from the FC and thought that, at least in theory, it was a good idea. However, there was also a great deal of concern whether components and subsequent reconstruction into profiles was practical. Some DAWG members felt we do not have sufficient understanding of requirement components (the understanding we lack has been called the "algebra of components"), and the FC should not depend on what is essentially a research issue (i.e., the FC should address whole protection profiles or large sets of requirements like assurance "pack-ages" rather than requirement components). One person gave the analogy that "two arms, two legs, a torso, and a head does not necessarily make a person."

This discussion led to the issue of quality control over components. Repeatedly, the group heard that the "vetting" process will control the quality of profiles, but there seemed to be no similar control over components. When a participant asked how new components are included, the answer was that they are introduced via "vetted" profiles. The discussion then focused on whether any component should be included in the FC unless it has first been "vetted" in a profile, and then the requirement should be taken as a whole from the profile. The group observed that

more than two-thirds of the compo-nents listed in the FC were not included in the FC's example profiles. Some felt that "unvetted" components should be strictly banned, since there will be the impression that if a component is listed in the FC, it must be technically sound. Others felt that the out-right ban of "unvetted" components may be too strong, but that there should be some control over their quality.

QUESTION 3: What are the Major Technical Problems with the FC's Development Assurance Components?

The DAWG briefly discussed the third question raised by the moderator. A couple of participants asked whether these were "nits" that were not important enough to discuss at this time. However, most of the DAWG felt that these comments were indeed funda-mental technical issues that should be addressed before the Common Criteria effort begins. Indeed, some felt the issues raised in the written comments and summarized by the moderator (see the QUESTION 3 summary in Section 4) are fundamental concerns that must be address prior to the Common Criteria effort. There was a general sense that the FC was introducing concepts that are not well-accepted, and sometimes introduced these concepts under names which had different meanings in the TCSEC, ITSEC, or CTCPEC.

Miscellaneous Topics

In this section, various related topics that were discussed by the DAWG are listed. These topics are listed in no particular order.

Some felt that the concept of effectiveness as defined in the ITSEC was inadequately addressed by the draft FC. This concern was still present even after it was explained that the FC intended to address effectiveness via the profile "vetting" process.

Many DAWG participants voiced strong concern about the manner in which the FC distributed the TCSEC and CTCPEC's notion of operational assurance, especially the system architecture requirements, throughout the development assurance and function-ality components. This structure resulted in reduced or even harmful redefinitions of the system architecture requirements. The principle example of this problem was the way in which the FC defined the least privilege requirements as solely a set of mechanisms (some felt that these mechanisms themselves encouraged poor least privilege designs) rather than defining least privilege as a global design concern, which may partially be satisfied in some cases by the mechanisms listed.

Some DAWG participants felt that evaluation requirements should be listed with the functional or development assurance requirements.

There was a general consensus that "reliability" does not necessarily imply "assurance" in a security sense. The example given was the phone system, which is exceptionally reliable (i.e., phones calls go through at rates of success) but has been widely and deeply penetrated over the years.

The DAWG generally agreed that the FC poorly uses the terms "trusted subject" and "privileged subject". In particular, the FC uses the term "privileged subject" where "trusted subject" should be used. A subject need not have privileges in order to be part of the TCB (e.g., an unprivileged audit collection utility). Likewise, possession of a privilege need not mean that a subject is part of the TCB (e.g., a privilege to increase or decrease a process' priority may be allocated to non-TCB subjects). Others noted that the FC should not discuss "trusted subjects" at all, since it is an implementation detail. In most cases, it should suffice to simply distinguish between TCB and non-TCB (and possibly Reference Monitor and the non-RM TCB).

Summary and Conclusions

The DAWG did not achieve consensus on a lot of the issues discussed. This was due in part to the small amount of time available for discussion. Nonetheless, many excellent points were raised, the most significant of which are hopefully contained in the material presented above. In the moderator's opinion, there was general agreement on a number of important issues:

- Few were happy with the current contents of Chapter 5. There was not a consensus on what Chapter 5 should look like, but many opinions were given (as discussed above).
- Most participants liked the idea of components in principle. However, nearly everyone had serious concerns about the concept in practice, and in particular, about the FC's components as currently defined. The principle concerns focused on the possibility of reconstructing meaningless (and possibly harmful) assurance require-

ments from components, the lack of control over the quality of individual compo-nents, and the loss of meaning by breaking assurance requirements into components and then reconstructing new assurance requirements. This issue consumed most of the DAWG's time.

- Nearly all participants had serious concerns about some of the technical assurance concepts introduced in the FC. Many felt that some of the concepts were not well-accepted, and that some of the "new" concepts were not well described. Others were concerned that some well-accepted concepts were replaced by less-accepted or poorly described "new" concepts. The group consensus was that the FC should stick to accepted concepts and ideas (but not close the door on new ideas being introduced in the future).

CHAPTER 7 Protection Profiles

This report represents a summary of the discussion held during the Protection Profile session. Most of the discussion points scheduled for this topic were included in the "global issues" sessions held during the first day of the workshop. Consequently, a new set of questions were posed by the moderators for consideration by the participants. This set is presented below.

Questions Posed by Moderators

The following questions were posed by the moderators. These questions are listed in the order in which they were addressed by the participants.

1. Is the notion of a Protection Profile useful? If Yes, to whom (e.g., users, certifiers, accreditors, evaluators)? If No, why not?
2. What is (should be) the relationship between Protection Profiles and Security Targets?
3. How should a Protection Profile be synthesized? Should a formalism be developed (e.g., an "algebra" of component synthesis be developed)? Or should a series of informal steps illustrating the use of criteria components be provided?
4. Should the description of the process of developing, vetting, registering, changing a Protection Profile be included in the Federal Criteria, or should a separate document (i.e., guideline) be developed?

Discussion and Recommendations Made by the Participants

1. In addressing the first question, most of the participants had already agreed (in a prior session) that the notion of a Protection Profile is useful and sound. Of some interest was the fact that, unlike TCSEC classes and other types of bundled require-ments, the Protection Profiles must include the type of threats countered, vulnerabil-ities eliminated, standards supported, and regulations addressed. These items, without which a protection profile cannot be vetted, were considered of particular interest to accreditors and certifiers, if not to evaluators. (The moderator underlined the fact that it is precisely this set of items that is necessary to establish whether a profile is security effective; i.e., whether its functional requirements counter a speci-fied set of threats, eliminated a specified set of vulnerabilities, supports a specified set of standards, addresses a specified set of regulations.)

   Much of the discussion focussed on the process of changing a protection profile (e.g., when, by whom?). It was suggested that "minor" deviations from the anticipated use of a profile should be allowed during profile use because, in practice, the environment of profile use is likely to differ, to some extent, from that assumed by the profile developer. The notion of how extensive a change can be (i.e., what is meant by a "minor" change of environment assumption) was answered, somewhat facetiously, by noting that a major change would always require a significant expenditure of resources whereas a minor change would only require a small amount of resources.

   It was also suggested that minor changes in the Protection Profile definition and use should be at the accreditors' latitude. However, if it is discovered that a lot of common changes occur in practice, these common changes should trigger a profile change, which would be vetted under the normal procedures (to be defined). It was also suggested that changes to a protection profile should also be made when

security technology changes (i.e., a technology insertion program should be established akin to some of the programs established by NASA).

A final set of remarks by the participants addressed the need for:

- involving accreditors in the process of vetting a Protection Profile;
- educating end-users, accreditors, and certifiers in assessing and using Protection Profiles in specific environments;
- resisting the pressures from the user community to introduce extraneous details in the definition of a profile.

2. In addressing the second question, the participants noted that neither the notion of the "security target" nor the relationship between a "security target" and a Protection Profile is defined in the Federal Criteria. However, it was also noted that the product evaluation process always involves both Protection Profiles and Security Targets. It was agreed that, for the purposes of the discussion, the notion of the Security Target was that of the ITSEC.

   In addressing this question, the participants made the following three observations:

   - the relationship between a Security Target and a Protection Profile is "many-to-one." That is, a Security Target may satisfy several Protection Profiles. The typical example would be that of a Security Target which satisfies a CMW Profile and, at the same time, satisfies a B1 Protection Profile. Other examples of the "many-to-one" relationship involving widely independent Protection Profiles are anticipated.
   - the relationship between a Security Target and a Protection profile may be affected by the product configurations. For example, two configurations of the same product may satisfy two different Security Targets. Also, it was noted that, although a certain product configuration change may satisfy some Security Target that differs from the intended one, the configuration may disable desirable features, which would cause the product not to satisfy any Protection Profile. These configurations were called the "conflicting configurations," and were distinguished from those that could lead to secure, but "less-than-useful" products.
   - the role of the Protection Profiles and Security Targets in the certification and accreditation process should be defined in the Federal Criteria (or other ancillary documents).

3. The third question was addressed by several participants, each providing different views on what was important in synthesizing Protection Profiles. A common point of agreement was that, although formalisms for composing requirement components are generally desirable, it is premature to consider such formalisms given the fact that the requirement components themselves are informally defined. The following three observations were also generally accepted by the participants:

   - the steps provided by the Federal Criteria, Chapter 7, seem to form an adequate basis for profile synthesis. However, the synthesis process is not documented for the Protection Profiles examples included in Volume II. Without such documentation it is somewhat difficult to determine with certainty whether the steps provided in Chapter 7 are sufficient for profile synthesis in practice.
   - the profile synthesis should include some "mandated" components for both func-tional and assurance requirements. It was noted by the moderators that the Federal Criteria already mandates three functional components; Logical TCB Protection, Reference Mediation, and Security Policy. The participants suggested that a similar mandated inclusion should be made for assurance components, and the component suggested for initial inclusion was Penetration Analysis. During this discussion, it was also noted that a distinction must be made between the penetration analysis carried out at product development and evaluation and the penetration analysis performed during product accreditation in the environment of use. Both types of penetration analyses were strongly recommended with emphasis on analysis during accreditation.
   - the introduction of new components in the Federal Criteria may affect existing profiles not only future ones. The questions of when, why, who, and how these new components are introduced should be addressed.

4. The fourth question was only tangentially addressed as part of the overall discussion on the synthesis of Protection Profiles. The sense of the moderators is that, given the level of detail required in illustrating the synthesis of a Protection Profile, the general recommendation would be to provide a (set of) guidelines on Protection Profile development, vetting, changing, etc.

CHAPTER 8 Commercial Security Requirements

Overview

The Commercial Security Requirements (CSRs) Technical Working Session included presentations from Michael Ressler from Bellcore, Kenneth Cutler from MIS Training Institute, and Ellen O'Conner from the Internal Revenue Service. Both Mr. Ressler and Mr. Cutler participated in the NIST/NSA working group that developed the Minimum Security Functionality Requirements (MSFR), from which the Commercial Security Protection Profiles (PPs) were derived. As a person responsible for ensuring that extremely sensitive but unclassified information is adequately protected while it is managed by an information system, Ms. O'Conner is representative of a potential typical user of the CSRs Protection Profiles.

In addition to the presentations, the session also provided an opportunity for participants to discuss issues related to CSRs with the intention being that these comments would provide input into the Common Criteria efforts. Participants were requested to focus on general comments (rather than detailed line-by-line comments) and also to focus on areas that were felt to represent "successes".

During the discussion portion of the session, two major themes developed. The first theme centered around concerns with certain information included in the CSRs, while the second theme related to requirements that participants felt should be included in one or more of the CSRs.

The remainder of this report describes the major concerns discussed by participants and their suggestions for additional requirements, and also summarizes the presentations presented by the three invited speakers.

Concerns

Participants expressed four main concerns with the CSRs:

1. There was concern that the specification of some of the requirements was too specific. Participants cautioned that the CSRs should focus on "what" security feature is required, not "how" the security feature is implemented. They also pointed out that focusing on the "how" rather than the "what" severely limits innovation.
2. There was general concern with the use of TCSEC terminology within the CSRs.
   The Department of Defense and the commercial/civil sector use different termi-nology. Participants felt that the use of TCSEC terminology to describe requirements causes the commercial/civil sector to assume that the related requirements are not applicable for their environment. The following two examples were given:

   - Commercial/civilian users have a need for mandatory access controls. However, when the term "label" is used, there is a DoD connotation, and the implication is that requirements related to labels are not relevant to the commercial/civil sec-tor.
   - Commercial users state that they do not require "trusted distribution" (TCSEC terminology), which connotes couriers and armored cars. However, commercial users are very concerned with the introduction of viruses and may require soft-ware to be shrink-wrapped. Shrink-wrap is a form of "trusted distribution."

The consensus among the participants was that the CSR profiles must be commer-cialized. Terms that are not used in the commercial/civil sectors must be removed and replaced with the appropriate terms.

3. There was concern that there may be a proliferation of Protection Profiles. This was expressed by the question asked several times of "How many PPs will there be?" It was also pointed out that vendors only want to build to one (or maybe 2) set(s) of requirements.

   Consequently, there should be only a very limited number of profiles. It was suggest-ed that a profile can support options so that different sets of requirements can be sat-isfied.

4. There was concern that "commercial" was not a descriptive name for the CSRs since there are other environments for which these profiles are useful.

Suggestions

The consensus of the session attendees appeared to be that while the CSR profiles do not yet adequately address the needs of commercial and government users, they are a good first approximation (with the possible exception of CS1, which does not reflect the needs of the users and should not be used).

There were several recommendations for features that participants felt needed to be included in the CSRs. There seemed to be consensus that the major missing features related to networking and distributed systems, low-assurance PCs, and encryption. Other features were also mentioned. The discussion related to each of these features is described below.

Networks and Distributed Systems: Participants mentioned that excluding network connections resulted in an "unrealistic environment" since most environments have network connections. Consequently, networks and distributed systems should be addressed by the Federal Criteria. In a related comment, it was pointed out that other requirements should take the networking environment into consideration. For example, in developing authentication (e.g., passwords) requirements, there should be a recogni-tion of the fact that users log onto multiple systems via networks.

Low-Assurance PC Requirements: Attendees stressed that profiles with lower assur-ance and functionality are needed and that the CS profiles must address other environ-ments beyond multi-user operating systems. Profiles that provide for lower functionality and assurance would be very useful for both commercial and government users. A low functionality/basic assurance profile for PC's or workstations may be appropriate for some users.

Encryption: Another missing feature that was widely commented on was the lack of requirements related to encryption. However, someone mentioned that encryption cannot be mandated in a Protection Profile because of export restrictions. Someone else countered that although encryption algorithms are not exportable, the interfaces to the algorithms are exportable. There was some additional discussion as to whether this comment was correct.

Labels: The issue of the need for labels in the commercial environment generated a great deal of discussion with first one participant stating that they were definitely required, and another responding that they were not needed. It was also noted that mandatory access controls are needed, but that the term "label" (with its DOD connota-tion) is the problem. A suggestion was that the term "security tag" be used rather then the term "label". Other attendees pointed out that labels can be used to protect against viruses and may be useful in protecting against corporate espionage. The consensus among attendees seemed to be that there is a need within the CSRs to include require-ments related to mandatory access controls.

Role-Based Access Controls (RBAC): The concept of RBACs was another topic that generated a great deal of discussion. Several attendees felt that RBACs were needed in the commercial/civil section, and consequently, that requirements related to RBACs should be included in the CSRs. However, there were cautionary comments that "roles" are a new concept and not yet well-understood, and that perhaps for this reason they should not be included as requirements. In spite of these cautionary comments, the consensus of the group seemed to be that, because RBACs are needed they should be studied for possible inclusion as requirements in one or more of the CSRs. There were also suggestions that the Federal Criteria include the "primitives" from which RBAC requirements could be built.

MSFR: The attendees felt that "the MSFR was a more useful protection profile." The participants preferred the approaches used in the MSFR to those in the CS profiles. Terminology, level of granularity and clarity of requirements were all mentioned as superior in the MSFR.

The consensus of the participants was that the MSFR work should be preserved and included in the Federal Criteria as a Protection Profile.

Ratings Maintenance Phase (RAMP) and Official TCSEC Interpretations:

Someone commented that the CSRs appear to include neither RAMP nor the interpreta-tions. Another attendee stated that commercial users do not care about RAMP. Another attendee stated that some RAMP requirements, such as configuration management and trusted distribution, are needed by the commercial/civil sector.

Application Programming Interfaces (APIs): CSR's need to include requirements for APIs that can be used by application programs to access security-relevant information.

Malicious Users: The CSRs should include requirements that protect against malicious users.

User Education: There was some discussion as to whether the CSRs should include requirements related to user security awareness education since this acts as a threat reducer. However, the consensus of the participants seemed to be that it should be not included as a requirement in any of the CSRs.

Presentation One - Michael Ressler - Bellcore

Mr. Ressler presented an overview of Bellcore and its security requirements. He stated that Bellcore security requirements do not align with the TCSEC because the 'C' level does not provide enough security functionality nor assurance and the hierarchical access control model of the 'B' level is inappropriate for their environment.

He also provided an overview of general commercial security requirements, including the need for inclusion of confidentiality, integrity, and availability policies and the need for confidence, quality and robustness of security features. Mr Ressler also gave an overview of the Minimum Security Requirements and his critique of the Federal Criteria.

Finally, he provided his recommendation for a new Commercial Security Profile based on the CS3 Protection Profile which reflects the original Minimum Security Functional Requirements (MSFR) and Minimum Security Assurance Requirements (MSAR).

Presentation Two - Kenneth Cutler - Vice President, MIS Training Institute

Mr. Cutler provided general comments on the Commercial Requirements contained in the Federal Criteria. He also recommended the creation of additional profiles and the deletion of superfluous profiles.

He suggesting adding requirements for expert systems to be used for audit analysis purposes and real-time checks. He also suggested that the concept of "approval authori-ties" should be considered.

He felt that supporting availability is important.

Presentation Three - Ellen O'Conner of the Internal Revenue Service

Ms. O'Conner works for the Criminal Investigation Division (CID) of the IRS. Ms. O'Conner described CID applications that manage extremely sensitive (but unclassi-fied) information such as case- related information, informant, undercover, and agent information.

Ms. O'Conner explained that because of the sensitivity of the information that is being managed, both RBAC and row/record access controls are required. She would like the CS3 Protection Profile to include both RBAC and row/record access controls.

CHAPTER 9 Label-Based Protection Profiles

Introduction

The Federal Criteria Workshop session on Label Based Protection (LP) Profile Comments was attended by thirteen organizations ranging from government, such as DOE, Air Force, and DIA, to industrial, such as Grumman, Boeing, TIS, Sparta, CTA, and individual consultants.

Discussion

LP Profiles versus TCSEC Classes

The general discussion of the equivalence of the LP Profiles and the corresponding Trusted Computer System Evaluation Criteria (TCSEC) classes revealed that there are many areas that prevented the two from being equivalent. Several issues would prevent equivalency between the LP Profiles and the TCSEC classes:

- Inclusion of terms not fully defined
- Use of products previously evaluated that would not meet a requirement without significant change

- Addition of words that would make a requirement weaker than that stated in the TCSEC
- Addition of requirements such as System Management and Integrity
- Inclusion of minor modifications (inclusion of an “s” at the end of a word) that would change the entire meaning of a requirement
- Inclusion of ill-defined models (i.e., penetration model or privilege model).

In several places, words have been changed and thus the meaning changes. Examples of this include the use of “privileged” and “unprivileged” in place of the words “trusted” and “untrusted.” Additionally, it was pointed out that the separation and repackaging of assurance added to the change in requirements.

Other examples of changes to the requirements are in the Least Privilege and Label requirements. Least Privilege expounds on the requirement and changes its meaning. Label requirements in AC-3+ are changed by requiring labels on subjects and storage objects rather than all resources. This change does not support the basis for covert channel analysis. It was noted by one vendor of an A1 network component that his product would not meet the requirements of LP-4, and a vendor of a B2 product indi-cated his product would meet the functional requirements but that the assurance require-ments could not be met.

Conclusion: The current profiles do not represent the same requirements as defined in the equivalent TCSEC classes. Backward compatibility should be based on the TCSEC with valid clarifications that have been tested over the last 10 years. Evaluators and vendors should have the opportunity for extensive reviews. The TCSEC was mostly correct in this respect, while the Federal Criteria was not. The TCSEC should be used as a basis for clarifying the requirements. Due to time constraints, it may be necessary to explain the vetting process that will be applied to ensure compliance with TCSEC classes.

Relationship of Components and Profiles

There was considerable discussion on the relationship of components and profiles. It was felt that the separation of requirements into components with arbitrary relationships added to the differences with the TCSEC. The dividing of Operational Assurance may not have been necessary if a large component had been defined to maintain the relation-ship that exists in the TCSEC. The requirements in the LP Profiles are based on require-ments that have been inaccurately divided into components which when put back together do not equal the TCSEC classes.

It is not well understood whether components or profiles should be defined first. Since the vetting involves profiles, it was felt that components should be pulled from approved profiles to be used as building blocks. Artificial creation of components was viewed as a cause of the LP Profiles being different from the TCSEC classes.

Conclusion: The TCSEC requirements should not be divided into arbitrary components. After the profiles have been vetted to be equivalent to the TCSEC classes, the compo-nents could be identified for use in building other profiles. If other components are still required, then new profiles should be made based on those new components, as written and without extra verbiage or refinements. Words used in components should match the words in profiles and they must be correct. Note: There may need to be a vetting of new components from new profiles.

Reference for Including a Requirement

It was discussed that there needs to be a set of guidelines to define worked examples that qualify for inclusion as a new component or a new requirement in the criteria. The TCSEC claim was that there were three worked examples of each requirement; however, some of these examples were not readily available to industry. The inclusion of a worked example must have wide acceptance over multiple communities and in industry. Multiple examples of implementations by vendors must be provided to vali-date that the concept is reasonable and implementable. Research should not serve as the basis for inclusion; however, there may need to be an acceptance of a few basic research concepts.

Conclusion: For inclusion in the criteria, the requirement must exist in industry (not just academia), multiple examples must be provided, the requirement must reflect a reason-able view of the technology community wide, and there must be a balance of technical advancement and example implementations.

Need for Rationale in LP Profiles

This discussion focused on the different levels of detail in the rationale sections of the LP and CS Profiles. There is a great deal of rationale that should not be missed to support the requirements of the TCSEC. It was noted that due to time limits this ratio-nale could not be included, but that in the future there needs to be consistency in the rationale sections of the profiles.

Conclusion: Rationale is totally missing from the LP Profiles. Well-written rationale could provide effective input for procurement specifications. The rationale should iden-tify threats and Yellow Book English rationale types of things.

Naming Conventions

The current naming conventions imply a relationship between components and between profiles. The hierarchical nature of the TCSEC classes should be maintained, but that does not mean that there is a relationship among all components or profiles.

Conclusion: The naming convention should be changed such that there is not an implied relationship for profiles or components. One way to do this is to use the names of the TCSEC classes, such as Controlled Access Protection, which could be called "LP-CAP." The profile description should define any relationship or inclusion of other profile requirements.

Summary

The existing LP Profiles do not represent the same set of requirements that exist in the TCSEC classes B1 through A1. Because of time constraints, it may be necessary to use the exact TCSEC language in the profiles to allow for a vetting of the profile to update them with evaluation case law that has evolved over the past decade of experience. A multidiscipline group of vendors, evaluators, and users should update the profiles over time to enhance the requirements to the level of practice. This process would then produce new profiles that relate to the TCSEC as well as provide an exact copy of the TCSEC requirements.

The language and description of profiles need to be further refined to ensure that the relationship between components and profiles is precise and well understood. The process of profile development and vetting must be defined so that it is well understood by the vendor community. Until the vetting process is well defined, the language of the TCSEC should be maintained in the equivalent LP Profiles.

CHAPTER 10 International Harmonization

Introduction

This workshop session covered the steps for moving forward from the draft Federal Criteria (FC) to international harmonization. It was held in the context of the announce-ment that the governments of North America (NIST, NSA, and the Canadian CSE) have entered into an agreement with the European Community (United Kingdom, France, and Germany) to work over the next year towards a Common IT Security Criteria. A Common Criteria Editorial Board (CCEB) has been established, though at the time of the workshop it had not yet met. In this session, all six members of the Editorial Board were present as participants in the discussions. They are:

Paul Cormier, Canada (Communication Security Establishment)

Chris Ketley, UK (Communications Electronics Security Group)

Yvon Klein, France (Central Security Service for Information Systems)

Hartwig Kreutz, Germany (German Information Security Agency)

Mario Tinto, US (National Security Agency)

Eugene Troy, US (National Institute of Standards and Technology)

Approximately 25 other individuals were present, including representatives from various US government agencies, other European organizations, and several representa-tives of multinational computer product suppliers.

Initial Topic Issues

The FC states that international harmonization of criteria and mutual recognition of evaluations are objectives. The basic question that must be asked is whether the FC work has advanced or hindered international harmonization. A second and related ques-tion is what is the path to achieving harmonization from this point. It is generally agreed that we all want to be pointed toward international convergence in this area, yet how do we achieve that while saving those things in the individual criteria (e.g., TCSEC, ITSEC, FC) that the nations believe are important? Numerous comments were received that generally discussed issues related to harmonization. The topics below were derived from an analysis of those comments in the light of the impending Common Criteria project.

1. What are Potential Roadblocks to Harmonization?

The key issues about harmonization identified in the FC comments deal with:

a. Assurance Approaches

What are the elements of assurance, the process of gaining confidence about the security functions in the product? The Europeans have advanced the twin notions of effective-ness and correctness in the ITSEC, while the US has divided the assurance process into development and evaluation assurance. Is there a way of converging these two approaches, and do they even cover the same thing? It may be that the differences between them are more perceived than real. The issues may be more of form and style, rather than substance.

b. Protection Profiles in the FC versus Security Targets and Functionality Classes in the ITSEC

Some convergence in the area of security targets has already been seen in the workshop. There is no indication of this prospect for convergence in the comments because in the draft FC protection profiles were not clearly enough related to security targets and func-tionality classes. It seems to be becoming much clearer that in general, protection profiles can usefully be viewed as user requirements while security targets are to be seen as engineering specifications. It is also clearer that protection profiles may not always be needed for product evaluations.

c. International Profiles

A number of FC comments focused concern on the prospect of further fragmenting the international IT product market via free creation of a spate of protection profiles. There was also a significant amount of concern in the comments over the implication of export laws with respect to products built to protection profiles. The reviewers generally seemed to accept that it must be left to the national government agencies to decide the IT security requirements for their governments and state them to the suppliers. Several reviewers advanced the notion of going beyond national standardization (or vetting) of profiles to do so on the international level, although it was noted that it is difficult to see how that could work. There is clearly an expressed need to converge with other interna-tional standardization work, such as ISO SC27. Questions that arose in this connection are the following: How do you handle international development and vetting of protec-tion profiles? Who is a legitimate developer of profiles under such a system? Who will be entrusted with the duty of deciding whether profiles are proper? How can profiles evolve over time to keep pace with requirements and technology?

2. Phase-in to Harmonization

The key concerns about the process of achieving harmonization identified in the FC comments and in later informal comments received on the Common Criteria project deal with:

a. What Should be the Steps to Harmonization?

Some comments expressed concern about the inherent feasibility of achieving harmoni-zation. It was noted that there are four IT security criteria now in existence, in varying degrees of completion. The concern was how we can move from that posture to a single criteria that can be agreed upon by a large number of nations. A proposal has been made that the CCEB should focus its work on the common core, the toolset, and not on devel-oping or agreeing on profiles.

b. How Should Users & Suppliers Proceed during Convergence?

This is a concern that was expressed in the comments with respect to the phase-in of the FC which has even more applicability to the Common Criteria work. There is a concern whether there are some specific things that we can do to help users and suppliers in the interim. It was noted that the UK and Germany have experienced this problem of having their own criteria and then phasing into use of the ITSEC. There is a need to plan care-fully for the transition. One supplier noted that suppliers will tend to respond to these influx requirements by building their products more generally to encompass multiple sets of requirements.

c. How Should Backward Compatibility with National Criteria be Handled?

This question is closely related to the previous question. Comments in this area were expressed mostly as generalized concerns, not so much with protecting the criteria themselves but with the supplier and user investments in prior standards. In the interna-tional arena, it was noted that national laws or regulations, such as those of Germany, have an impact because they specify adherence to particular criteria.

d. How Does this Work on Common Criteria Relate to ISO SC27?

In the same context, other reviewers were concerned about how to handle the issue of achieving an ISO standard that incorporates the FC work. This question is now extended to the Common Criteria work. The question boils down to: How can ISO SC27 relate to the Common Criteria development process? How will the Editorial Board and its spon-soring nations make their work applicable and acceptable in ISO?

Presentation by Julian Straw, SISL (UK)

Mr. Straw, a senior evaluator for one of the UK commercially licensed evaluation facili-ties, made a cautiously optimistic presentation on the FC versus the ITSEC, which has specific application to the Common Criteria work. He viewed the FC work as providing many new ideas and material that are supportive of harmonization.

Mr. Straw identified the following main issues that need to be dealt with in achieving international harmonization. Several of these were also covered in his written comments. Accordingly they will not be gone into in detail here.

1. Common Criteria

The FC has helped sort out the differences among the current criteria by moving in the direction of rapport. He cited the separation of functionality and assurance, the use of the security target as a basis for the notion of a protection profile, and the acceptance of the notions of correctness and effectiveness as expressed in high-level requirements. He noted that there are indeed commonalities between the ITSEC's correctness/effective-ness and the FC's development/evaluation assurance approaches, but pointed out several specific differences in application of these requirements at various levels on each side. He was very concerned with the FC notion of dependencies, and felt they would become a big issue because there is no common agreement on what they are or how they are identified and expressed.

2. Evaluation Method

Mr. Straw noted there is some experience with using a multi-national criteria in Europe. However, he said there have already been instances where evaluators and certification bodies in Germany and the UK have interpreted parts of the ITSEC differently. This makes it clear that a single set of criteria among nations is not enough in itself. There is also a need for a common evaluation method as a basis for harmonization, to ensure that developers and evaluators do the same things.

3. Product Certification Process

Mr. Straw pointed out the central importance of evaluation results acceptable in one country also being acceptable in another country. He identified two levels of mutual acceptance: acceptance of the results of evaluation, and acceptance of certificates issued. These can be considered somewhat independently. For example, it is possible for a product evaluation report to be passed from one country to another, with the certifying body in the second independently deciding whether it wants to award the product a certificate based on acceptance of the evaluation report. However, he said that the second level of mutual acceptance, that of a second national certifying body accepting a certificate issued by the first, should be the objective. If we can trust one another in both the evaluation and certification processes, it will minimize the amount of duplicated effort.

4. Why Do We Want to Achieve Harmonization?

Mr. Straw stated that there are four main reasons for seeking harmonization of criteria and evaluation methods:

- It is easier for those who are buying products. When products are evaluated under different criteria it is hard for the buyers to determine the differences and how they should respond.
- It is much cheaper and quicker for suppliers to comply. Who would voluntarily want to undergo two evaluations in two countries? It is far more economical to do just one evaluation.
- The criteria can be improved by taking the best things from each. None are perfect, yet each nation has the same problems to solve via security criteria.
- There will be an improved basis for comparing security requirements between coun-tries and between products.

5. What We Need to Move Forward.

Mr. Straw felt that the following things are needed to move forward towards harmoniza-tion.

- We need some product to evaluate as part of the process of trying out the criteria concepts. The trial evaluation should be done in a common way, against a product with any useful set of security functionality.
- We need a body to decide whether evaluation of a particular product or product type is worthwhile. Under the FC, this is accomplished via the vetting of a protection profile. Under the ITSEC, this is usually achieved by a certification body deciding whether a particular security target is suitable for evaluation, as well as by evaluators looking at it for consistency.
- Criteria must overtly cover both correctness and effectiveness. Does the product work as specified? Does it do what it is supposed to do by satisfying the objectives as stated in the protection profile and/or security target?
- Criteria must cover both commercial and military requirements. He is not totally convinced whether there is a commercial requirement for evaluation. Evaluation of commercially-oriented products has not caught on well due to the costs involved.
- Criteria must be comprehensible. Complaints have been received that the ITSEC has too many levels (6) of assurance. The FC has 28 separate assurance components that must be built into protection profiles, with no fixed levels that must be used. He is not looking forward to the task of explaining this variety to people submitting their products for evaluation. Therefore the area of building a straightforward and useful set of profiles is quite important. Try to keep it simple.

Presentation by David Chizmadia, NSA

Mr. Chizmadia, a former evaluator, presented ideas on how to reconcile the ITSEC's effectiveness/correctness with the FC's development/evaluation assurance.

He provided two working definitions for discussion. Correctness asks, "Does the product do the thing (security function) right?" Effectiveness is oriented towards an assurance objective by asking, "Does the product do the right thing (security function)?" Effectiveness then becomes a judgment about the environment and the product.

Part of his work has been oriented towards finding some policy oriented motivation for assurance. In his view, policy is just about how the system makes information available. Security objective is a better term than security policy, because it helps avoid confusion. He states that effectiveness and correctness should be defined at the same level of abstraction as other kinds of "security policy-based objectives," including integrity, accountability, confidentiality, and availability. By doing so, you now have a way of tracing from high-level policy objectives to what specifically is being asking for. You may now identify assurance objectives based on policy, in the same way as you identify the objectives for the security policy-based requirements. These two can then be possibly independent. In this way, all of the requirements for a product must be reflected in the objectives and therefore must be soundly based on policy.

Following this proposed approach, the user has a much better ability to decide what is needed and can then map it down to specific requirements. Independent of security objectives, assurance objectives may also be stated. In this way, you can do assurance independent of security objectives.

General Discussion

A general discussion followed the two presentations, generally based on the set of topics given originally under "potential roadblocks" and "phase-in to harmonization."

1. What are Potential Roadblocks to Harmonization?

The key discussion points centered on the potential roadblock topic issues raised at the start of the session:

a. Assurance Approaches

Discussion continued about some of the incompatibilities between ITSEC and FC assur-ance approaches, particularly effectiveness/correctness vs. development/evaluation. As discussion proceeded, it appeared that incompatibilities remain to be worked out, but these are probably less a problem than initially thought. One of the key differences is that some of the effectiveness work, such as suitability of functionality, is done during profile construction and analysis. A European security expert noted that ease of use is actually handled better in the FC than in the ITSEC, that it is more well rounded. It is treated as part of functionality instead of assurance. He also noted that strength of mech-anism is becoming less important in the ITSEC as European evaluators gradually try to refine what they are trying to test the strength of. In his view, other effectiveness factors may be in the FC, but they are generally found only at the higher levels, while in the ITSEC they are applicable to some degree to all levels. He gave as one example penetra-tion analysis, where it is not used until LP2 while under the ITSEC it is done at the lowest levels.

The general argument about how and why assurance is gained about a product's security functions was raised. This was coupled with discussion about why overt assurance via evaluations should be sought. This issue is important to the harmonization work, because the European Community seems to be strongly vested in the notion of product and system security evaluations for both government and private enterprise. It was noted that assurance that a product works as advertised is commonly expected, but in the non-military world the notion of third-party evaluation as its source is seldom volun-tarily considered. One individual raised the notion that the intelligence community has national risk assessment documents that link risks/objectives of the organizations into TCSEC assurance levels. He noted that they tend not to publicize these documents-they are internal for accreditors use. The end result is that assurance tends to be a distress purchase-because users are told to, not because they want to.

It was agreed there is a range of ways by which people gain assurance about what they buy or use, whether it is cars, seatbelts or computers. The formalized evaluation process is one of these ways that the military and intelligence communities have found impor-tant to them. It is clear that as of this time, commercial users do not see the same kind of value in that process, and tend to do the assurance work themselves in various ways. It may be that work needs to go forward on finding suitable and possibly standardized ways for the private world to achieve assurance about security products short of lengthy and costly third-party formal evaluations. This whole area seems to be tractable as long as we continue to understand more and more on what each side is intending.

b. Protection Profiles in the FC versus Security Targets and Functionality Classes in the ITSEC

The discussion indicated that most people did not find inherent conflict between the notions of protection profile and security target, when each is properly understood. There was growing acceptance of the notion that the concepts tend to be mutually supportive. The discussion pointed up the need for a far better explanation of the joint roles of the protection profile and security target and how the two should be used together in connection with product development and evaluation.

One big remaining area of disconnection centered around the FC notion of dependen-cies. Interaction between product elements is treated in the ITSEC under binding of functionality. As such, it is left up to those preparing security targets and to the evalua-tors. This was noted by some participants as a possible weakness in the ITSEC. It remained clear that the treatment of dependencies in the FC was well below what many viewed as needed. The process of identifying dependencies still seemed overly complex to the participants, and it was unclear how this issue should be treated in the Common Criteria.

c. International Protection Profiles

Perhaps the largest single area of discussion in the session had to do with the notion of international protection profiles. The issues raised covered all the points initially identified.

There was deep concern over the potential proliferation of protection profiles interna-tionally. One speaker from the supplier community even suggested, with support from other speakers, that the success of the Common Criteria venture, from the point of view of actually getting products out in the marketplace, is going to be inversely proportional to the number of profiles available. He stated the reason for that is the market for secu-rity products is actually very weak. There are no security vendors that will claim there is anyone beating down their door. He expressed hope that with internationalization the world will become one marketplace. A number of different profiles will fragment the market again, and then there will be a bunch of little weak markets instead of one strong one.

Another supplier expressed support for the effort because there would be fewer basic requirements, and all of them generated from a Common Criteria which would be used as the basis. He was concerned about one possible scenario with multiple profiles. Say his company decided to build a product to a given profile and have it evaluated (based on a business decision) and then later perceived the incremental market going for another similar profile. He wanted to know whether an incremental evaluation could be done against the differences or would they have to do the whole evaluation all over again and double their costs.

The issue of international protection profiles, from the viewpoint of how to standardize them, who develops them, etc., was discussed. It was noted that this problem has begun to be looked at in the ISO SC27 context. An initiative was also started in the European Community to develop predefined functionality classes for vertical industry segments. A European Community (EC) research task was funded to identify a dozen functionality classes for the commercial sector. No results have yet been published from the study. There was no resolution as to the mechanics of the processes needed to arrive at interna-tional protection profiles. In general, suppliers want to see the advent of these profiles to make their life easier. One point that was brought up is that such profiles should not be highly specific in their requirements.

Another point that was raised is if we gently phase it in (taking into account what everyone wants) we never will achieve the goal-it will take too long. The process is so large and important that some groups/agencies/governments will have to step up and dictate what they want to see. One speaker noted that it will be up to governments to come up with the first set of international protection profiles for it to happen in our lifetime. Who

standardizes/vets/registers profiles may be a consortium of interested government bodies. This is the only way to do it in a short time.

One evaluator pointed out the great degree of difficulty that has already begun over gaining consensus that LP-1 represents the same thing as B1. He felt that based on that experience it is not likely that international profiles will gain easy acceptance in the community-there are too many disparate viewpoints and vested interests for consensus. He stated that a set of international profiles is desirable but not likely.

Several participants noted that national laws may also have an effect on the develop-ment of international profiles and on the prospects for international harmonization. Two areas were pointed up, export restrictions and encryption mechanisms. It was noted that export licenses are possible for B3 and higher products, but that this restriction was still burdensome. Until these issues are clearly resolved among national governments, and especially the cryptologic authorities, there is little prospect for international trade in high-security computing devices.

The issue of including encryption technology in evaluatable products arose. It was observed by several that there is little prospect for network or distributed security without encryption. There was a discussion whether the criteria were to be expanded to include evaluation of encryption devices. One evaluator said that what one does to eval-uate encryption devices and algorithms is much different than what is described in any public criteria. It was pointed out that evaluation of products which contain an imple-mentation of encryption mechanisms was different from evaluating the mechanisms themselves, which must be considered separately by cryptologic authorities. The quality of the implementation or the need for it are properly subject to IT security evaluation, while the encryption techniques themselves are not. It was clear that this is still a fuzzy issue which needed to be tackled by the national authorities.

2. Phase-in to Harmonization

The key discussion points about the process of achieving harmonization were:

a. What Should be the Steps to Harmonization?

The Editorial Board members and others pointed out that the North American and Euro-pean governments' planned steps are already becoming somewhat clear, even though detailed planning work has not yet been done. (At the time of the workshop, the Edito-rial Board had not yet met.) The role of the Editorial Board to come into agreement on the structure of the aligned criteria and to orchestrate its creation was discussed.

Internationally representative technical groups of security experts will be used to support the work, although their specific roles in the project have not yet been estab-lished. Technical support groups will work alongside the Editorial Board and will be tasked to do specific things. This covers whatever needs to be done-writing, research, etc. This brings in an opportunity for broader representation. The technical support groups do not have to be exclusively composed of government employees or contractors of the various countries, some could be from the user community or supplier commu-nity. There are no ground rules yet.

One question arose as to whether technical groups could be used to capture and refine commonly seen protection profiles, security targets, or functionality classes that have been created under the ITSEC or FC. It was agreed this would be a valid use of tech-nical groups and an especially productive place for suppliers and users. However, some of the Editorial Board members pointed out that the Board has a very short time in which to operate, and that it would be better to concentrate on developing the tools for building the profiles rather than on developing the profiles themselves. There could be some parallel effort, but there is a work factor.

In discussing the role of the Editorial Board, the notion of a common core of tools arose. One observer stated that this workshop has already had an impact on the underlying assumptions and semantic differences-it is becoming ever more clear that the issues are semantic more than differences in what we are trying to do. We have six agencies from five countries represented on the Editorial Board, all who have the same problem to solve. They have all tried individually to solve the problem. It appears that we can draw the circle quite large around the requirements of the various IT security constitu-encies to include them all.

b. How Should Users & Suppliers Proceed during Convergence?

One supplier representative suggested that research on market segments found that most users needed essentially the same things. Therefore there should not be that many different protection profiles, regardless of harmonization. The governments want to buy Commercial Off-the-Shelf (COTS) products. He felt that no supplier is going to produce four different multi-level products for government use. Perhaps there will be a high one and a low one-two at the most. Therefore, suppliers will tend to proceed along paths they already know, to build to known requirements that have already come from govern-ments and user communities. They will, however, seek to generalize their products as much as possible, to include a wide range of security features.

Another participant stated that there still will be differences at the national level as to what is required. The coming to a set of international profiles will be a long and difficult one. Perhaps the suppliers will have to combine the more stringent requirements from the different countries to arrive at an international profile. The supplier will have to take the least upper bound. The criteria would then be in excess of requirements for each country in order to meet all requirements for each country. There would also be a problem if the requirements are in conflict with one another. He felt the cost for building to an envelope such as that would not be as great as that for going through several evaluations.

c. How Should Backward Compatibility with National Criteria be Handled?

One point in this area that was brought up was the RAMP process. There was consensus that this process has fully demonstrated the value of the notion of development assur-ance and should be retained in future criteria. It does not yet exist in the ITSEC, although there have been discussions about including it.

d. How Does this Work on Common Criteria Relate to ISO SC27?

Several speakers noted that the long term objective of the Common Criteria project must be to fit its work into ISO and achieve an international criteria standard. In addi-tion, people noted that standardized requirements profiles for various products already are coming out of the ISO environment, witness ISO 7498-2 for security of open system interconnection. But a transition plan needs to be worked out, which may be a common criteria agreed to internationally. It was noted that ISO tends not to do original work, but to work on existing documents that have been tabled.

Other speakers identified several other related international standards activities in the IT security area in addition to ISO SC27. These include the European Computer Manufac-turers Association (ECMA) TC-36, Portable Operating System Interface for Computer Environments (POSIX), Open Software Foundation (OSF) and X/Open. There will be a difficulty converging all these with the Common Criteria effort, as the only common forum is ISO, which tends to operate slowly.

X/Open activities were described as especially germane to the Common Criteria project. X/Open is intending to define a common set of security functionality, and they intend to provide a branding scheme so that a vendor that claims compliance will be able to execute against a test suite and get a brand. There is the prospect that a large number of users may be happy with the X/Open brand as demonstration of needed security features and assurance, which will further reduce the market for evaluation. X/Open's publica-tion of security standards is temporarily on hold while they look at the implications of security services, APIs and distributed security.

Moderator Conclusions

This session has demonstrated that the gap between criteria is not so great as some may believe.

- In the area of assurance, there has developed a basis for discussion to resolve the apparent differences between effectiveness/correctness and development/evaluation assurance. The question about how to resolve the ITSEC's fixed assurance levels versus the FC's more flexible approach of protection profile specification not depen-dent on T-levels remains open.
- Regarding protection profiles versus security targets, the earlier perceived differ-ences were mainly due to a lack of doctrine in the FC about how the two relate. Further discussions have demonstrated that the two are not

in conflict, but rather can work together nicely. However, the protection profile development and approval process does have implications for assurance harmonization, because it subsumes some of the processes related to effectiveness. This issue needs substantial clarifica-tion. Also, the notion of dependencies, introduced in the FC, needs to be developed in significantly greater detail regarding the method of identification and the manner of expressing them.

- Internationally-accepted protection profiles appear feasible on a limited basis for very common sets of requirements. The MSFR work has had strong impact on both ECMA and Japan, and could become the nucleus of work on the first international profile. There is great concern over the process of forming the profiles and gaining approval for them. There is also concern about the prospect for proliferation of many profiles, which may have negative market effects.
- The Common Criteria Editorial Board's early activities in charting a course to align-ment will be scrutinized closely, especially from the viewpoint of external (user and IT product supplier) participation in the process. The Board should focus on devel-oping the tools for the criteria, not on developing profiles.
- The Common Criteria project must take into consideration the other international standardization activities which are going on in IT security. In particular, the project must interact closely with ISO SC27, which is the logical point of convergence of all other interests beyond North American and European governmental agencies. Ulti-mately, an ISO standard criteria is needed, and ISO is also the likely candidate for vetting and registry of international protection profiles.

CHAPTER 11 Future Work with the Federal Criteria for Input into the Common Criteria Editorial Board

Overview

As a result of the comments received on the first draft of the Federal Criteria, and the input of those at the Invitational Federal Criteria Workshop, it is clear that additional work needs to be done on this new criteria for information technology security. The Common Criteria Editorial Board (CCEB) has been formed to develop a common criteria based on the input from the TCSEC, ITSEC, CTCPEC, draft Federal Criteria, and the draft ISO standard on IT Security Criteria. The U.S. representatives need a complete technical proposal that represents the security needs of government agencies and industry. The purpose of the Federal Criteria project is to provide this proposal. The proposal initially will consist of the first draft of the Federal Criteria and the contents of these proceedings from the Federal Criteria Workshop. As time passes, drafts of the U.S. contribution to the Common Criteria incorporating the comments will be provided. The Common Criteria will undergo extensive external review allowing those involved in the original Federal Criteria project (both originators and reviewers) to continually provide valuable data to this process.

Major Areas of Work

The first draft Federal Criteria motivated over 20,000 comments. There were some central themes in these comments as to the needed direction to any new criteria, whether it be a U.S. Federal Criteria or an international Common Criteria. These general themes were confirmed at the invitational workshop. The result is the following list of concepts that should be addressed by NIST and NSA as they contribute to the CCEB effort to develop the Common Criteria, progressing rapidly toward a truly international informa-tion technology criteria standard.

1. Fundamental Security Principles

A section needs to be written which clarifies the security principles on which the docu-ment is based. The objectives and scope of the document need to be clarified as well.

2. Clarification of Security Components

The components presented must be recast in language that is easy to understand for the information technology expert assembling protection profiles and/or security targets. In addition, the dependencies must be clearly stated. Further, the components must be rewritten to be evaluatable and usable under procurement laws.

3. Completion of Underlying Vetting, Registration and Evaluation Concepts

The process by which a protection profile is reviewed, accepted and registered needs to be completed. Similarly, an evaluation process which uses the protection profiles must also be established, complementing the development of the Common Criteria. These two processes are essential so that both criteria and product developers know what requirements to build to and how the resulting product will be assessed in relation to those requirements.

4. Preservation of Information Technology Security Investment

Attendees clearly and strongly emphasized the importance of preserving industry investment in security based on the TCSEC, not necessarily the words of the TCSEC. This means adequately capturing the experience of the past ten years in the Trusted Product Evaluation Program (TPEP). The components, as well as the protection profiles, must allow for all current implementations of the trust principles contained in the TCSEC, its formal (and informal) interpretations, and its evolution through the TPEP process. This includes concepts such as Rating Maintenance, subsystems, appli-cations (TDI) and network components (TNI).

5. Distributed Security Issues

Information technology products of the 1990's are commonly designed to work in larger system architectures with distributed and networking services. The impact of security on these products is still under research. This research will provide both clarification of known concepts in light of distributed issues as well as new security concepts specific to distributed environments.

Specific Work Area Plans in Support of the CCEB

The immediate plans must focus on support for the Common Criteria Editorial Board. This means focusing resources on those portions of the Federal Criteria which can provide the most valuable initial contribution to the work of the CCEB along with the associated comments and recommendations on those portions. Although the preferred method would be to complete a version of the Federal Criteria based on the received comments and recommendations from the invitational workshop, it is understood that the CCEB cannot wait while that version is generated. Therefore, the Federal Criteria project plans to provide updates on appropriate sections when they are needed at the CCEB.

Application of and Response to Received Comments

The comments received on the first draft of the Federal Criteria will be an important source of information for the NIST/NSA contributions to the Common Criteria. Comments received will be used to make the necessary changes to the document. This includes both the general comments discussed here and the specific comments on the different chapters and sections of the Federal Criteria. It is planned to provide commen-tators with responses to comments provided once the resolution to them is known. In addition, commentators will be placed on the mailing list to receive the draft Common Criteria for public review and comment when it becomes available.

Resources to Complete the Work

The bulk of the work defined here will be completed by NSA and NIST personnel, with input from contracted information technology experts. However, review and input from the information technology industry as a whole will be necessary as the Common Criteria development process proceeds. It is understood that the user and vendor community will remain an important source of technical information as this project continues.

Summary

The draft Federal Criteria made a significant contribution to the field of information technology security. However, it was a first draft and substantial work would be required to complete the Federal Criteria. Instead of expending resources directly on this effort, NSA and NIST will focus on contributing the central material from the Federal Criteria, augmented by the incorporation of the many comments and recom-mendations made on it by the

commentators of the draft,to the Common Criteria effort. The result will be an information technology security criteria with an international scope that will meet the needs of both U.S. government and industrial users.

APPENDIX North America and Europe Agree to Develop Common Criteria

Summary

The governments of North American and European nations have agreed to develop a "Common Information Technology Security Criteria" (CC). Participants include the European Community, Canada, and the United States.

Security criteria are needed to develop trusted information technology (IT) products that can be used to help protect important information of the government and private sectors. IT security criteria common to Europe and North America will help broaden the market for these products and further lead to economies of scale. In addition, common criteria will help achieve the goal of mutual recognition by North American and European nations of IT product security evaluations.

The effort, which is expected to begin in early Fall of 1993 and be completed in the Spring of 1994, will use the ISO Subcommittee 27, Working Group 3 draft criteria documents (Parts 1-3) as an initial framework. Specific inputs will include the Informa-tion Technology Security Evaluation Criteria (ITSEC), the Canadian Trusted Computer Product Evaluation Criteria (CTCPEC), the draft Federal Criteria for Information Tech-nology Security (FC), the experience gained to date with the ITSEC in the form of suggested improvements, the comments now being received on the draft FC document, and the results of the FC invitational workshop planned for 2-3 June 1993.

The resulting common criteria are expected to undergo extensive international review and testing by performing evaluations of "real" products against the criteria prior to being fully accepted for use within Europe and North America. When mature enough, the CC will be provided as a contribution towards an international standard to ISO Subcommittee 27, Working Group 3.

Background

The agreement grew out of a 4 February CEC-sponsored workshop in Brussels on the Federal Criteria that was attended by many European security professionals. The general European response to the workshop was that alignment of criteria between Europe and North America is now both feasible and opportune.

This idea was taken up and endorsed by the EC Senior Officials Group for the Security of Information Systems (SOG-IS) in their meeting on 11 February, clearing the way for EC participation in the work required to achieve common IT security criteria.

As a result of informal meetings held thereafter, a proposal was made to proceed with a joint project to develop common criteria. This proposal was then given preliminary approval by EC member nations and North American government senior officials.

Planned Development Procedure - The Editorial Board

Current plans call for the establishment of a six member Editorial Board (EB) consisting of three members from North America and three from Europe. The EB will be composed of senior IT security experts who have had experience designing IT security criteria and have the authority and autonomy to make decisions with regard to the contents of the CC. The EB will be requested to complete their work within a six month timeframe. The main tasks of the EB are to obtain a clear understanding of the similari-ties and differences between current criteria and to develop a first-draft CC for presenta-tion to the participating government bodies. The EB will be instructed to use the material identified above as the primary material from which to develop the CC. The CC is to represent a synthesis of the best concepts and components contained in the original material. The EB is to avoid inventing new criteria.

Technical Groups to Provide Support

The EB may establish and utilize special Technical Groups (TGs), as needed, to help develop specific technical areas of the CC. These TGs will operate under the direction of the EB for the time needed to perform their assigned tasks. They will be staffed in a representative way, in a pattern like that of the EB.

Public Review and Trial Use

Following completion of the first draft criteria, the governments involved will jointly review the CC. When they mutually determine that the CC is ready for further review by the IT security community at large, they will initiate an extensive review cycle to obtain comments from all interested parties. This cycle is expected to result in additional versions until convergence is achieved. The CC will then enter a trial period to allow the specification and evaluation of vendor offerings against the CC. Upon completion of the trial period, the CC will be revised if necessary to gain final adoption by the partici-pating governments.

Relationship to ISO International Standardization

During the process of CC development and trial use, the associated governments will work through their respective national standards bodies to help keep the ISO draft stan- dard in relative synchronization with the CC. An issue requiring further study and consultation is how to maintain the necessary level of momentum in ISO, yet avoid finalization of an International Standard prior to achieving generally acceptable common criteria for Europe and North America