Common Criteria Users' Forum

Summary Report
October 6-7, 2004
Washington, DC

Executive Summary

The Common Criteria Users' Forum (CCUF) took place on October 6-7, 2004 as a follow-on activity to the Cyber Security Summit meeting and National Cyber Security Partnership (NCSP) Technical Standards and Common Criteria Task Force. The NCSP Task Force Report contained over 30 recommendations related to improving the Common Criteria evaluation process. The CCUF was formed to make progress on some of the key recommendations.

The CCUF opened with presentations by representatives from NIAP, Common Criteria Testing Labs (CCTL), the vendor community and customers. These presentations helped improve communications among the stakeholders. In direct response to a Task Force recommendation, a panel of experienced vendor and CCTL representatives shared tips on how to successfully complete a Common Criteria evaluation. Another panel was assembled to discuss the critical issue of broadening the application of Common Criteria versus addressing the problems of Common Criteria.

The main activities of the CCUF were the 4 workshops:
Workshop A: Incentives for Security and Common Criteria Evaluations
Workshop B: Reducing the Time and Costs of Common Criteria Evaluations
Workshop C: Security Metrics Relevant to Common Criteria
Workshop D: Setting Requirements for Commercial Users

These workshop discussions developed the following results:

1) NIAP has committed to develop more vendor, evaluator and validator training. This training will help vendors understand Common Criteria and the evaluation process better and improve the consistency between evaluators and validators. Education was identified as a key issue in the NCSP Task Force Report.
2) "Reducing the Time and Cost of Common Criteria Evaluations Tips" white paper was developed from the results of Workshop B (Reducing Time and Cost) and the Secrets for Successful Evaluations Panel. This paper provides valuable information and best practices on how to complete a successful evaluation and minimize costs. Time and cost of evaluations were called out as a major issue in the NCSP Task Force Report.
3) The output of Workshop D (Commercial Requirements) and Workshop A (Incentives) identified the need to investigate the value of independent, third party, internationally-recognized security evaluations to the commercial marketplace. The concept of developing a set of baseline security requirements for the commercial marketplace is worth exploring further along with the topic of metrics (Workshop C).

4) Once we've identified the security requirements that are applicable and valuable to commercial users in 3), we need to market them by creating awareness and advertising programs around them. The output of Workshop A provides some areas for further discussion.

A follow on workshop is planned to continue to address the commercial requirements and improve the relevance and value of Common Criteria to the commercial customers. This workshop is tentatively planned for the first quarter of 2005.

Background

Governments from around the world have invested millions of dollars in the development of the Common Criteria. Common Criteria product certifications are recognized in 20 countries and required by the US Department of Defense. However, while some perceive the Common Criteria as inefficient and costly, others believe that Common Criteria is the best bet for helping the IT industry improve the security of products and provide customers world-wide assurance that these products are secure.

The NIAP Review and the National Cyber Security Partnership Technical Standards Task Force Report on Common Criteria are two specific efforts to address the issues raised by Common Criteria and the U.S. NIAP process that implements Common Criteria. One of the key recommendations from the Task Force report on Common Criteria is to assemble a forum to foster open discussion about the issues and potential resolutions.

Without proactive action, the recommendations collected in the NIAP Review and the Task Force report will not be implemented. We are planning a Common Criteria Users' Forum composed of Common Criteria related stakeholders including customers, vendors, Common Criteria evaluators and NIAP (NSA and NIST). The users' forum will have the following goals:

1. Recommend practical means to improve the Common Criteria processes and standards to make them a truly viable mechanism for improving COTS product security for all customers, as well as Governments.
2. Present the opportunity for all parties to express their perspectives on the issues raised and to identify realistic means to resolve them.
3. Provide an open forum to discuss and resolve the apparent differences between the views of commercial entities and NIAP.
4. Develop a specific plan of action for the recommendations from the NIAP Review and the Task Force Report as well as any additional recommendations developed by the attendees.
5. Begin to share Common Criteria experiences as a means of educating all stakeholders.

Agenda

Wednesday, October 6, 2004

Introductory Remarks
Andy Purdy, Department of Homeland Security

NCSP Task Force Overview
Ed Roback, National Institute of Standards and Technology

NSA Presentation
Pamela Yocum, National Information Assurance Partnership

NIST Presentation
Stu Katzke, National Institute of Standards and Technology

CCTL Presentation
Cynthia Reese, Science Applications International Corporation

Commercial Customer Presentation
David Cullinane, Washington Mutual, Inc.

Vendor Presentation
Mary Ann Davidson, Oracle Corporation

Security Vendor Presentation
Heath Thompson, Internet Security Systems, Inc.

IDA Status Report on National Information Assurance Partnership Review
Rick Harvey, IDA

Panel: Secrets of Successful Common Criteria Evaluations: Tips and Best Practices from Vendors and Labs
Leslie Saul-Garvin, TechNet - Moderator
Shaun Lee, Oracle Corporation
Jim Hughes, TippingPoint Technologies, Inc.
Ray Potter, Cisco Systems, Inc.
Regina Hammond, Symantec Corporation
Cynthia Reese, Science Applications International Corporation

Thursday, October 7, 2004

Panel: Broadening CC Application vs. Addressing CC Issues
Stu Katzke, National Institute of Standards and Technology - Moderator
Robin Pizer, CESG
Steve Lipner, Microsoft Corporation

Eustace King, OSD
Catherine Webb, IBM

Workshop A: Incentives for Security and Common Criteria Evaluations
Janine Pedersen, NIAP - Moderator
Workshop B: Reducing the Time and Costs of Common Criteria Evaluations
Wes Higaki, Symantec - Moderator
Workshop C: Security Metrics Relevant to Common Criteria
Steve Lipner, Microsoft - Moderator
Workshop D: Setting Requirements for Commercial Users
Glenn Brunette Sun Microsystems - Moderator

Panel Summary: Secrets of Successful Common Criteria Evaluations: Tips and Best Practices from Vendors and Labs

Experienced vendors and evaluation lab representatives have some valuable information about how to prepare for the Common Criteria process. They will discuss "best practices" to help ensure a successful and timely evaluation.

Cynthia Reese - SAIC

Common Problems:

- The product or Target of Evaluation (TOE) is a moving target and has changing requirements
- Targeting more than one Protection Profile is problematic. In theory, this is a good idea, but Protection Profiles are not written to be done simultaneously.
- Product not thoroughly tested by the development team. Development should work to resolve problems before evaluation.

Tips:

- Start with a reasonable schedule
- Keep abreast of current interpretations and standards
- Build up knowledge about Common Criteria or use consultants

Ray Potter - Cisco

Three needs to be more user involvement in Common Criteria. Cisco's development process maps to the Common Criteria requirements. Cisco became tired of being in reactive mode and decided to be more proactive with Common Criteria evaluations. All products are being affected so they are interested in doing it better, faster and cheaper. Cisco wants to bring the role of the consultant in-house to integrate evaluation into the normal development process.

Tips:

- Go to multiple schemes to support Common Criteria internationally to improve it and share experiences
- Set expectations with customers, labs.
- Development staff must be involved. Becoming more organized in training and evaluators and validators.
- Cisco has had mixed experiences with consultants. It is important to do due diligence in selecting consultants and evaluators.

Issues:

- Common Criteria is not ready to be taken to the private sector.
- Multiple customers with multiple requirements may lead to proliferation of Protection Profiles (not a good thing)
- Need to educate end users on the benefits of Common Criteria

Regina Hammond - Symantec

Symantec's first evaluation complicated by a company acquisition, staff turnover and little applicable documentation and no plans or experience. Moreover, they had a requirement to meet EAL 4. It was a challenge to get developers write necessary evidence (design docs, CM, etc.)

Tips:

- Have a dedicated technical writer to create evidence documents
- Have a QA lead liaison to address test questions
- Used the same evaluators for the last 4 years, so they know the product well.
- Common Criteria is now part of the product requirements and so everyone knows that they must set aside resources/time to address certification issues.
- Program manager holds weekly status meetings with evaluators to track progress.
- Reused configuration management (CM) and delivery documents and have leveraged these across the company.
- Have reduced time from customer ship–to-certification from 18 months to 6 months with experience.
- Educating developers and all employees gets everyone thinking about security and evaluation especially during evaluator site visits.
- Preparation before evaluation and site visit avoids problems.

Shaun Lee - Oracle

Oracle has been participating in certifications for 14 years, mostly through the UK Scheme. They do evaluations to improve their products and processes and not just to satisfy a checkbox for procurement. At Oracle, consultants are part of the evaluation team and are knowledgeable about the products. Common Criteria has helped in the drive to make corporate culture become more aware of security issues. Improved testing has been a benefit. Formal third-party evaluation has value because of the labs' independence. Common Criteria has helped in fostering a climate of security awareness.

Tips:

- Choose an evaluation lab and validators that have expertise with your product technology. Check CV's to learn about the evaluators.
- Use consultants to provide expertise on Common Criteria. Consultants filter through existing Oracle documents for evaluation use.
- Choose evaluators that meet your needs.
- Start small.
- Treat evaluation as just one component of improving product and process security.

Jim Hughes - TippingPoint

TippingPoint certified their UnityOne product against 4 IDS Protection Profiles at once. TippingPoint's experience was that they naively entered the process to gain access to the Government business. They learned that there are benefits to technical support, bug fixing and development through the structure of the Common Criteria process.

Tips:

- “Learn the Common Criteria lingo” to communicate with evaluators and understand what they need.
- “Tallest tree gets cut down first.” Don’t do things too different that causes confusion for evaluators. Stick to standard or normal ways of doing things.
- “Common Criteria is the ante, not the bet.” Obtaining Common Criteria certification means you only get to bid on Government contracts. Don’t expect too much.
- Get a strong internal champion to get resources and commitment.
- “Beware of consultants bearing gifts.” Consultants do not know the product, so they need to be educated.
- Do not delegate project management.
- Understand the document architecture. Understand the scope and relationships between Common Criteria evidence documents.
- “Choose your battles” with the Scheme.
- Engage all of the players early and often. Start with a strong kickoff meeting with all of the stakeholders.
- Learn the Common Criteria landscape.

Other Tips:

- Evaluators should have direct access to developers to reduce delays. Consultants can help address Common Criteria detail issues with evaluators.
- Schedule for potential problems. Plan with realistic estimates.
- Sometimes, design and test documents are still being developed when a product starts an evaluation, so evaluators can use this time to evaluate CM or delivery documents first and learn more about the product.
- It is better to deliver draft documents to evaluators early so that they can catch major problems early rather than spending a lot of time developing "final" documents only to find out that they are seriously flawed. Oracle however generally delivers final documents to their evaluators (perhaps because the evaluators know the products).

Panel Summary: Broadening CC Application vs. Addressing CC Issues

There is not much use or demand for Common Criteria evaluated products outside of the Government. We may need to push evaluated products to the commercial market to do more cost amortization, but there are issues with Common Criteria. There is a lack of a business case to justify the need for Common Criteria evaluations in the commercial marketplace.

Eustace King – OSD

Security is key to the DoD IT organizations. DoD is responsible for providing warfighters the best and most secure products. The DoD fully supports NSTISSP #11.

GOTS used to be prevalent in DoD and security was easy because the agency developed to their specific needs. Today, COTS are more prevalent. The DoD wants assurance that the product components they deploy on their networks are secure when they are plugged into their systems.

NIAP's role is to provide cost effective, timely information assurance (IA) products. Some question that CCRA labs have the same capability as NIAP to meet DoD needs. Each program within DoD must have a Mission Assurance Category (MAC); one of three levels. These three levels align with the NSA robustness levels for products and Protection Profiles.

Eustace believes that NIAP does not address software security. Perhaps the entire "cradle-to-grave" life cycle of software must be evaluated for software. Common Criteria is not suited to do this. DoD is looking at changing the paradigm for addressing software security.

Steve Lipner – Microsoft

Customers say 3 things regarding security:

1. I need some security features
2. I need to meet Common Criteria requirements. – usually for policy compliance
3. I want security assurance/quality – I don't want to have to keep installing security patches.

In order to meet these requirements, Microsoft will:

1. Do the necessary engineering and development of the requested security features.
2. Respond to the customer mandate to meet the Common Criteria requirements.
3. Employ the Security Development Lifecycle (SDL). This is an internal mandate.

The SDL is a dynamic process that can evolve to mitigate new classes of attacks. The SDL is built into the normal development process at Microsoft. There are various checks, procedures and test throughout the development process to provide better security and higher assurance.

Since the introduction of the SDL both the number and criticality of the vulnerabilities and patches have decreased. Microsoft has noted that incremental application of the SDL results in incremental improvement. Today, Microsoft spends 1 to 2 orders of magnitude more on SDL than on Common Criteria.

Robin Pizer – CESG

Robin was invited to speak about the Smart Card experiences in Europe. Stu felt this is an example of a success story with commercial customers.

Many things have changed since the 1990's when Common Criteria was developed. It may be time to refresh it with modern developments. There is a clash between commercial use and Government use.

Smart card work began in 1997 prompted by the European Commission (EC) and took 3 years to complete with collaboration between government, evaluators, academia and industry. In 2001 there were several issues with the Smart Card Common Criteria.

- There was no use for protection against low attack profile (unrealistic)
- Could not accredit enough labs because they would not share test procedures
- The Protection Profiles was monolithic – over 300 pages. There was no common agreement.
- The Common Criteria was not written with smart cards in mind. Customers want to know where the eminent threats are.

In spite of the problems, they felt Common Criteria was the way to go. The EC created Trailblazer3 with 3 subgroups to address these issues to improve Common Criteria. Some things are still being worked on:

- The list of tests and attacks used by evaluation labs are confidential and more work needs to be done in order to share information.
- There is a need for languages for specific technologies
- There is a need to new evaluation packages
- Need higher assurance for commercial users

Catherine Webb – IBM

Value to the customer is key to making Common Criteria relevant to the commercial markets. AIX and DB2 Common Criteria evaluations were completed soon after general availability (GA) of the product.

IBM uses the NIAP and BSI (Germany) schemes. IBM chooses the based on the lab's experience with the technology being evaluated.

Common Criteria provides a better product. Security is well defined using the Common Criteria language. Development documentation has been adjusted for Common Criteria. There is more focus on security because of Common Criteria. The Common Criteria/third-party evaluation gives customers assurance that security claims are true. Mutual recognition is beneficial where one evaluation is leveraged across many markets/regions.

Documentation has improved and the process for handling vulnerabilities has improved. IBM has implemented a continuous improvement program so each release must be better than the one before. They are providing training on secure programming.

- Protection Profiles must be achievable by COTS products. Protection Profiles should not be wish lists.
- More labs would mean more competition and lower evaluation costs.
- NIAP needs more funding for tool development.
- Helmut Kurth of @sec has written a paper on secure system composition. System-level evaluations are not appropriate for vendors.
- Need to make adjustments to Common Criteria. Catherine agrees with the BITS approach to use extensions of Common Criteria.
- Certifying against multiple Protection Profiles is expensive. Need to limit Protection Profiles proliferation.

Workshop A Summary: Incentives for Security and Common Criteria Evaluations

Workshop goal: formulate incentives to motivate vendors and customers regarding the use of the Common Criteria for Information Technology Security (CC) evaluation. The workshop members recognized that both vendors and customers needed incentives to pursuer Common Criteria evaluations.

Incentives for Customers

There is a need to educate customers on CC, starting at upper management and working down to the users. This education should include descriptions of general CC concepts to provide simplified and comprehensible terminology, dispelling Evaluation Assurance Level (EAL) “myths” and “Frequently Asked Questions.” This education package should also address questions of why customers should ask for CC, evaluated products. This should highlight the value of an evaluated product.

Part of the value statement is an explanation of how customers can use CC evaluated products. This will require descriptions of how to apply/use the results of the CC evaluation and how CC fits in with other processes, such as Certification & Accreditation (C&A), and overall security measures. Sharing success stories and testimonials from other users can help improve the recognition of value.

To help customers understand what they are getting, we need to improve the usefulness of Common Criteria. This will mean addressing problems associated with Protection Profile development and maintenance. Providing Executive Summaries will help make Protection Profiles and ST’s more understandable. Customer-driven surveys should be used to determine other outputs that are necessary and to tailor support to specific users (e.g., integrators, C&A personnel, procurement, etc.) Improving CC mechanics will help customers understand the value of Common Criteria. We need to revisit EAL assurance packages and determine what packages exist and Mutual Recognition CEM beyond EAL Level 4 for non-Department of Defense customers.

Incentives for Vendors

Vendors need more education and increased communication. They need to understand the roles and responsibilities of vendors and consultants. Pre-evaluation support is important. Vendors need more guidance and insight on Common Criteria results and evidence. Common Criteria should allow for re-use of other standards and compliance results to increase consistency.

Common Criteria can be used more in vendor marketing collateral. It can be used to illustrate “truth in advertising”. More open dialogue among vendors, to process lessons learned and other issues can help promote Common Criteria.

There are of course, several issues that need to be addressed regarding the standards and Protection Profiles. National Information Assurance Program (NIAP) should constantly review policies involving CC and PP compliance and engage the vendor consortium in the process. Vendors need to drive PP development for commercial products as the lowest common denominator and discourage custom PPs (focusing on specialized requirements) and clarify and encourage the proper application of PPs. An actual “users” conference is essential to obtain the user’s perspective on Common Criteria. There are some Product Life Cycle Issues that need to be addressed. CC should be more responsive to vendor life cycle issues (keep up with version releases, etc.). We should re-evaluate how assurance management must fit with the end-users requirement.

Workshop B Summary: Reducing the Time and Costs of Common Criteria Evaluations

The Cyber Security Summit's Technical Standards and Common Criteria (CC) Task Force recommended the workshop on reducing time and cost of evaluations. The Common Criteria Users' Forum was held to follow up on the Task Force recommendations. The issue of the time and cost associated with CC is a hot topic with vendors.

What costs are we concerned with?

Costs include evaluation costs, consultants and contractors and developers' time. Vendors are particularly sensitive to these items because they bear most of these costs.

How do I start?

Enlist the help of consultants. Apply due diligence in the selection of consultants and the evaluation lab. Investigate the technical expertise of the consultants and evaluators. It is important to identify consultants and evaluators who are familiar with your product's technology to reduce the learning curve time and effort. Note, most US evaluation labs offer consulting services. It is helpful to engage evaluators early in the process so that they can begin to learn your product's characteristics. The best time for evaluation is during pre-release stage. The vendor has an opportunity to incorporate the Common Criteria evidence creation and security features into the product as it is being built rather than after the fact.

Set reasonable requirements

Start small. Don't evaluate against multiple Protection Profiles – they are not designed to be hierarchical. Conduct a pre-evaluation assessment to determine how much effort will be required to meet EAL requirements. Schedule for potential problems. Plan with realistic estimates.

How to reduce evidence creation time and costs?

Seek out sample evidence. Security Targets are available on the NIAP website. Open source Linux Common Criteria evidence is available through IBM. Use consultants to help determine the depth and detail required for evidence documentation.

Make Common Criteria evidence development become part of the normal development process. Cost depends on whether or not you already have best practices in place. Treat evaluation as just one component of improving product and process security.

How to reduce time and cost related to testing?

Consider automating your test suites. Minimizing the number of manual tests that have to be reproduced will save time during the product-testing phase of the evaluation.

Involve QA from the beginning so that they have an opportunity to provide input to the ST as the test suites may need to be augmented to include tests for the specific ST claims.

How effective are consultants?

Hire consultants to help get through the process. Hire them for their expertise with the Common Criteria process. The advantage consultants have over evaluators is that evaluators cannot influence product designs so use consultants up front then involve evaluators. "Beware of consultants bearing gifts." Consultants do no know the product, so they need to be educated.

Tips on project management

Do not delegate project management. Vendors know the product; they know the limits of their organization and they are paying the bills. The vendor needs to manage the scope and progress of the evaluation. Use project management to manage communications and reduce delays. Bring the evaluation team in early in the process. Keep in close contact throughout the process. Facilitate informal communication; product training for evaluators can foster more informal communication due to product familiarity. The greatest delays occur when a developer is not responsive enough to answer even simple questions for evaluators.

Product training for evaluators

The back and forth conversations between developers and evaluators about technical questions about the product takes time. Evaluation labs need to know the product and technology. Consider providing product training to the evaluation lab. There is a learning curve for consultants, evaluators and validators.

Common Criteria training for vendors

"Learn the Common Criteria lingo" to communicate with evaluators and understand what they need. Developers and evaluators have different mindsets. The more the developer understands the Common Criteria lingo and the way evaluators think the quicker evaluation issues can be resolved. Understanding the Common Criteria document architecture will help provide guidance to the developer. Understanding the scope and relationships between Common Criteria evidence documents will help ensure the evidence is developed properly.

Vendors need to set expectations

Vendors who have successfully completed Common Criteria evaluations have made Common Criteria a priority through the organization. It is important to get developer commitment for the time and costs involved.

Vendors need to understand that they will spend potentially hundreds of thousands of dollars on evaluation lab fees plus consulting costs and development and QA time. These evaluations will take months to complete. Vendors need to set customer expectations appropriately that evaluations take significant time.

Workshop C Summary: Security Metrics Relevant to the Common Criteria

Observations

Measuring security (and/or security improvement) is in general is a hard problem. There is too little data available to defend effectiveness of Common Criteria and too little data available to evaluate impact of individual components of Common Criteria. Schemes and vendors would benefit from additional feedback based on this data.

What is it we're trying to measure? There are two key things: (1) Measuring effectiveness of Common Criteria evaluated products at different EAL levels – what does that mean about the security of the product? (2) Process metrics – how am I doing with building a secure product? If you look at EALs and ask what each is supposed to get you (level of security) then perhaps you can get a sense of how close applying those measures get you to the goal of the EAL level?

Objectives

- Measure effectiveness of Common Criteria process as a whole
- Measure effectiveness of individual activities
  - Within Common Criteria process
  - Within product development process
- Improve evaluation process
- Improve Common Criteria
- Measure return on investment in Common Criteria evaluaiton

Measure and improve effectiveness of individual activities within product development process

Internally we do track bugs and know what pieces of the evaluation process found them, but threat modeling has a different effect because it ought to prevent the creation of bugs. How are the internal development processes of individual companies comparable (at EAL levels)? "Credit" should be given to those companies with better internal processes.

Evaluating organizations using process criteria will reduce overhead on product evaluations to focus on testing.

The things you can always see are the externally reported vulnerabilities, but mapping these to development and process metrics is really hard. For each externally reported vulnerability, what are the internal process assurance components that affect it? Is there a need for process change to make that area stronger? Is a new innovation necessary to deal with a new type of attack? Also need a measure of how much it costs to fix the flaw as an indicator of relative severity

Measure and improve effectiveness of individual activities within Common Criteria process

We need to know where in the evaluation process we are finding the ideas that lead to the discovery of vulnerabilities (i.e., how many hours of evaluation per discovery of

vulnerability). Can we correlate vulnerability discovery with Common Criteria level?
What type of metrics can help you make the case that Common Criteria leads to improved security?
How do you measure the incremental security you get by meeting Common Criteria?
Why does complying with more assurance measures result in greater security?

The main benefit is that the Common Criteria process has forced some vendors to change their development process to create a higher quality product in the end. At the very least Common Criteria makes people think about security during development.

Recommendations

Vendors and schemes should measure impact of Common Criteria processes on security as recognized by commercial customers. Measurement should focus on commercial 'security issues' such as actual vulnerabilities (found internally or in field) and other issues that indicated potential vulnerabilities (inconsistencies, incomplete designs) rather than documentation issues or technical flaws (i.e., the semi-colon issues that plague some Common Criteria evaluations today).

Measurements should focus both on overall and per-area benefits. Identify security issues in product as a whole and security issues found and not found by each area of Common Criteria (e.g., configuration management, vulnerability analysis, design analysis). Consider extending the Common Criteria to reflect measured development process quality as a key component of assurance.

Metrics regarding security issues found can and should be applied to elements of processes that purport to improve security independent of Common Criteria. These metrics can help us define and refine potential improvements. Vendors, labs, and schemes can track 'security issue' metrics for products under evaluation and evaluated products. Vendors may wish to aggregate data or report metrics as percentages to indicate what aspects of Common Criteria are paying off. Ideally, information should be made public to drive process improvements across the industry

Workshop D Summary: Setting Requirements for Commercial Users

Workshop Goal:

Determine the appropriateness and relevance of the Common Criteria to users in the commercial sector. Identify gaps and issues related to Common Criteria evaluations and commercial user needs. Discuss ways in which the overall value of Common Criteria evaluations can be improved to better take into account commercial user security requirements. Determine if commercial organizations would be willing base procurement decisions on or pay additional money for evaluated products where the evaluation better reflects their requirements and needs.

Workshop Summary:

Many commercial users, both large and small, do not see the value associated with Common Criteria evaluations. This is in part due to their lack of knowledge of the program and its goals as well as the applicability of evaluation materials to commercial audiences. Another problem is simply that today's Common Criteria evaluations do not target areas about which many commercial users care. Implementing Common Criteria evaluated products, even in evaluated configurations, does not necessarily mean that the resulting system will be secure.

Further, there is no conclusive proof that Common Criteria evaluations actually improve the security of a product as would be typically deployed in a commercial setting. Anecdotal evidence seems to suggest that the evaluation process is good for identifying and addressing security weaknesses in products, but more work must be done in this area. There is a concern however that other forms of security evaluation including penetration testing may yield results that are more relevant to commercial audiences and less costly to accomplish.

Another issue is that the Government and commercial industry do not appear to effectively working together on these issues. NIAP was founded as a partnership between NSA and NIST. NSA was tasked with representing the DoD and intelligence community interests while NIST was supposed to represent the interests of the commercial industry. Unfortunately, NIST has not had sufficient staffing or budget to actively participate as a peer in NIAP which is why commercial interests are not well represented. Simply put, NIST does not have the money to contribute significantly to NIAP and cannot match NSA’s capability in this area.

The problem here is that the needs of commercial customers tend to differ from those in Government. While there are certainly some commonalities, commercial industry also has greater interest in purchasing products that are evaluated to be “secure by default” or have gone through some standard form of assessment and penetration testing. Further, proven secure software development practices could also factor in the overall opinion of a commercial customer. Fundamentally, the commercial user wants a secure product not necessarily one evaluated by the Common Criteria. The two are simply not the same today. The Common Criteria does not give commercial users that kind of assurance.

Commercial users are looking for the security equivalent of a “Good Housekeeping” seal for software and hardware products. They want to purchase products that are secure and can be securely deployed, integrated and managed within their environments. To accomplish this, commercial users must be convinced that a product evaluated in this manner has been closely examined in a structured, reproducible way and that any vulnerabilities in the product were very likely found and corrected by the vendor prior to the release of the product.
This evaluation may also take into account design practices such as “secure by default” where all services or functions not necessary for initial product installation and configuration are disabled out of the box.

Today, these types of requirements are not met by the traditional assurance packages such as EAL-4. It is likely that a new assurance package would need to be defined in order to better meet the needs and requirements of commercial users. That said, NIAP may not be the best organization to set these requirements. It is likely that a working group comprised of members of the commercial industry and government would be best able to develop a set of baseline requirements for this assurnace package. NIST could participate actively however as an advisor for these groups as well as a clearinghouse for the work products developed by this team.

The Common Criteria needs to be relevant to commercial users. Today, it is clearly not meeting their needs. Commercial customers are more focused on direct and perceived value. Customers want to know the product has been sufficiently tested under real-world conditions, is safe and can be securely deployed and managed within their environment. Security benchmarks, checklists, assessments and independent testing can help answer many of the needs of the commercial industry. Even with this however, there still is a need to better educate commercial users regarding the place and value of evaluations and certifications both in general and with respect to the Common Criteria in particular.

The Common Criteria can also be improved by being more proactive to changes in technology and security recommended practices. Using the development and design process as the main source of assurance can help address the cost and time issues associated with evaluations. There is also a need to make the Common Criteria protection profiles, assurance packages, and related documentation and artifacts more accessible to commercial users. Most of the documentation as it exists today is written either for a product developer or an evaluator. Often this language and format is not useful to commercial users who are trying to compare evaluated products finding it nearly impossible to perform an “apples to apples” comparison. This gap detracts from the usefulness of Common Criteria evaluations for commercial users. This problem is compounded by the lack of assurance packages that address commercial user requirements, as noted above.

Actionable Initiatives:

1. Establish a public/private user's group that includes the U.S. Federal Government to help develop standards and requirements that are specific to the commercial sector. The commercial sector does not have the same needs as the government. Therefore, they should not be forced to use the same standards. It is imperative that these requirements be understood and documented so that a baseline set of requirements can be developed.

   It is likely that many of these requirements will also be of use to the Government. Ideally, these commercial user requirements could form a solid foundation upon which Government users could apply their specific requirements and needs. In this way, the Government would benefit from these commercial requirements while still being able to evaluate products using its own set of requirements. This will ease product development and testing procedures and costs by limiting the amount of duplicate work that must be completed for vendors selling to both commercial and Government users while raising the overall quality and security of vendors' products.

2. Clearly describe the place and benefits of security evaluation and certification for commercial users. More specifically, discuss Common Criteria evaluations for commercial users making a strong case for why Common Criteria should be relevant to the commercial sector. This should be part of an education campaign to raise commercial awareness of the Common Criteria, what it is, what it is not, and what value comes from using products evaluated under the Common Criteria.

3. Refine the Common Criteria documentation and artifacts to make them more relevant and accessible to commercial users. This could take the form of an executive summary or appendix. Ideally, these updates should make it easier for commercial users to understand how a product was evaluated, under what conditions, limitations or constraints, etc. The documentation should also make it simpler for commercial users to compare similar products from different vendors on the basis of how they were evaluated and the results of the evaluation so that commercial users can make more informed decisions about they products they purchase.

4. Develop a Common Criteria assurance package (e.g. “EAL-Commercial”) that reflects commercial grade assurance requirements. It will be against this assurance package that commercial requirements will be evaluated. This will ensure that the requirements of commercial users are addressed.

5. Fund NIST efforts allowing them to be a more active member of NIAP in representing the needs and requirements of commercial users. This funding could be used to conduct cooperative research and development with private industry to better understand these issues and solve these problems.

Next Steps

The CC Users' Forum came about because industry (NCSP, CSIA) took on a leadership role in engaging Government and industry to push forward on some of the Recommendations made in the Cyber Security Summit Task Force Report. DHS started the ball rolling and industry is working to keep the momentum going because improving the protection of our information infrastructure is important and we believe CC is a tool that can help us achieve that improvement.

1) NIAP has committed to develop more vendor, evaluator and validator training. Since education and awareness was identified as a key issue in the Task Force Report and reinforced during the Users' Forum, this training will be quite useful. This training will help vendors understand Common Criteria and the evaluation process better and improve the consistency between evaluators and validators. NIAP welcomed industry inputs especially examples of evidence that can be cited. Industry associations and vendors should monitor the progress of this training and take advantage of it once it is available. This training is planned to be made available through the CCTLs and at appropriate workshops and conferences.

2) Complementing the NIAP training for vendors are the Workshop B and Secrets for Successful Evaluations Panel results. Tips and best practices from vendors and evaluators provide valuable information on how to complete a successful evaluation and minimize costs. Time and cost of evaluations were called out as a major issue in the Task Force Report. "Best Practices" paper that will be vetted by vendors, evaluators and validators will be useful tool for vendors to use to address the cost issue.

3) The output of Workshop D (Commercial Requirements) and Workshop A (Incentives) identified the need to investigate the value of independent, third party, internationally-recognized security evaluations to the commercial marketplace. The concept of the "EAL-Commercial" (set of baseline security requirements) for the commercial marketplace is worth exploring. The key will be to identify security requirements that commercial customers will readily attach value to (e.g. stopping viruses and worms or ensuring confidentiality of private information and reducing vulnerabilities). This touches on the topic of metrics (Workshop C). Vendors and customers with the help of Common Criteria consultants can work to develop these requirements. An investigation and report on alternatives such as ICSA and BITS may lend a useful perspective.

4) Complementary to 3) above, educating (and perhaps selling) customers on the relevance and value of independent, third party evaluations will help capture the attention of commercial customers. Once we've identified the security requirements that are applicable and valuable to commercial users in 3), we need to market them by creating awareness and advertising programs around them. As a follow-on activity by the group that develops the requirements in 3), the group should address the awareness and marketing issues.

5) One unintended result from the CCUF was that vendors, evaluators and validators learned more about each other's worlds. There were certainly some eye-opening tales told by folks like Jim Hughes from TippingPoint. Vendors, evaluators and validators should continue to get together to swap war stories and success stories. To share best practices and identify areas where myths need to be debunked and where problems exist.

The CCUF was intended to address only a small fraction of the 30 recommendations coming from the Task Force Report, but it was attempting to move forward on some key issues. There are certainly many more recommendations to try to advance and certainly more work that needs to be done to complete the issues we discussed at the CCUF. The message is that we can expect many more forums and other activities to resolve the issues and improve the security of products in the nation's (and the world's) information infrastructure.