Brusil, P.J, Johnson, L.A, Steeble, E.F. “Emerging Security Testing, Evaluation, and Validation"
Handbook of Emerging Communications Technologies: The Next Decade.
Ed. Saba Zamir
Boca Raton: CRC Press LLC, 2000

18 Emerging Security Testing, Evaluation, and Validation

The Key to Enhancing Consumer Trust in Security-Enhanced Products

Paul J. Brusil, L. Arnold Johnson, and Edwin F. Steeble

CONTENTS

18.1 OVERVIEW

Networked information technologies are changing the way the world interacts and the way industry, government, and other sectors do business. In the emerging electronic and global society, new electronic business (e-business) models are replacing traditional models propped up by trust built through personal interaction. With the proliferation of e-business powered by evolving network and information technology (IT) products, industry must earn consumer confidence by demonstrating that it has taken effective measures to protect the information being handled electronically. A key method of illustrating its commitment to safe transmission, processing, and storage of information is through validated, impartial, standards-based evaluations. Conducting such evaluations increases the confidence, or trust, that security features of network and information technology (IT) products are correctly and completely implemented and that these products behave as promised. Given the implications of vulnerabilities for the national economy and national security, the government has recognized the importance of safeguarding networks, particularly of critical national infrastructures. To promote an international marketplace for trusted, security-enhanced network and IT products, and in so doing protect its national interests, the U.S. Government formed the National Information Assurance Partnership (NIAP), a collaboration between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA). The NIAP program has seeded and is furthering the growth of a robust, state-of-the-art, commercial, security testing and evaluation industry. The NIAP is fielding a flexible national scheme to accredit private-sector security testing and evaluation laboratories and to oversee laboratory activities to ensure that security tests and evaluations are conducted in accordance with new, internationally recognized standards.

18.2 A NEW WAY OF DOING BUSINESS

Trade journals have documented that electronic businesses are transforming traditional business models in all market sectors. Business partners, suppliers, regulators, customers, and users worldwide are increasingly sharing critical information 7 days a week, 24 hours a day. Financial reports, business plans, inventory data, supply-chain management data, customer order data, health care claims and referrals, and other sensitive information are being communicated. Ready availability of such information is dramatically improving old business relationships and introducing new ones, to the detriment of competitors who do not make information easily accessible.

According to the trade press, new e-business models, based on ready and widespread availability of business data, are having profound effects. These new models are globalizing business operations by erasing traditional boundaries of time and space. They are improving business efficiency by more tightly integrating business processes and units, decreasing time to market, and reinventing and improving personalized customer services. They are attracting new business opportunities and stimulating new business relationships in ever more complex supply chains. They

are improving customer satisfaction, decreasing delays, and lowering the cost of doing business by orders of magnitude in diverse commercial market sectors. Businesses and service providers that fail to offer online e-business services to consumers and trading partners are losing out.

The following are just a few examples of emerging business changes and their impact:

- In the banking world, costs to process an electronic transaction are now under a penny compared to a dollar or more when customers deal directly with tellers.
- In retailing, online ordering and processing costs are being comparably reduced relative to telephone-based orders or in-store purchases, and online sales activities are being more highly targeted.
- In the transportation industry, the National Transportation Exchange (NTE) has introduced a new e-business model by providing an electronic trading floor to balance supply and demand by matching buyers and sellers of trucking space.
- In the automobile industry, the Automotive Exchange Network (ANX) provides unprecedented communication among competitors by effectively lowering the cost structure of the entire auto supply chain, thus allowing everyone in the chain to benefit.

18.3 ALONG WITH E-BUSINESS COMES A NEED TO PROTECT INFORMATION

The more business is conducted electronically, the greater the need to protect the information being handled. Security has become a necessary enabling technology for e-business. New business models depend on trust of the network and IT infrastructure used to conduct e-business among consumers and suppliers. Security has become a necessary revenue generation enabler, a necessary precursor to consummate new business ventures, and a significant cost-avoidance factor. One recent survey* showed that cyber attacks in the U.S. are rising and the direct costs attributed to such attacks are significant and growing. In 1998 such direct financial losses amounted to about $150 million. But direct costs may not be as significant as other indirect costs. If sensitive information, such as corporate strategies, customer profiles, and trade secrets, is not adequately protected, businesses can be destabilized, competitive advantage can be lost, and tenuous buyer/seller allegiances can be altered. In worst case scenarios, the consequences of compromised information can be dire and even fatal, such as in the medical sector where subversion of critical information concerning diagnoses, histories, or treatments during electronic referrals can lead to inappropriate and life-threatening medical decisions.

* "Issues and Trends: 1998 Computer Crime and Security Survey" by the Computer Security Institute and the Federal Bureau of Investigation, San Francisco, http://www.gocsi.com/prelea11.htm.

As the information age engulfs society, there is unprecedented demand in the commercial sector for security-enhanced network and interconnected IT products that can be trusted. Indeed, trust in the products they buy and use is what compels the telecommunications service providers to offer security service-level agreements that contractually guarantee the delivery of networking and IT security services. Trust evidenced through recognized security testing and evaluation is proving to be a powerful legal case builder to demonstrate "prudent business practice and due diligence" when seeking to reduce financial cost in liability suits associated with e-business.

In addition to the commercial world, society at large is beginning to depend on trusted network and IT products. In 1998, a Presidential Decision Directive[1] recognized that the viability of the U.S. (and accordingly the world's strongest military and largest national economy) relies upon critical national infrastructures. These infrastructures exist in both the public and private sectors: telecommunications, energy, banking and finance, transportation, water systems, and emergency services (including law enforcement, public health, and disaster recovery services). The directive recognizes that the network and IT systems that effectively link these infrastructures are key to ensuring minimal orderly functioning of the economy and government. The directive acknowledged that future enemies might seek to launch nontraditional offensives against the U.S. by attacking the critical infrastructures and the networking and IT upon which they rely. The directive requires "that the United States take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, including especially our cyber systems."

The U.S. is not alone in its resolve to protect itself from cyber attack. Other countries agree that determining the "… trustworthiness of [network and IT-based] products for national security systems has become a necessary objective of governments and businesses around the world."[2]

18.4 COMPETITION HEATS UP FOR TRUSTED PRODUCTS

System vulnerability concerns are yet one more problem being faced by modern enterprises already grappling with downsizing, market share, profits, and time-to-market questions. In today's e-business world, organizations have access to a growing number of security-enhanced network and IT products with various claimed security capabilities and with various less well-known limitations. Indeed, the size of the security product market is growing at a rate of over 75% per year and should reach $5 billion by the year 2000.* Customers must make important decisions about which of the products in such a large market provide an appropriate degree of protection for their assets. More and more, organizations

* 1997 Network Security Market Growth Analysis by The Computer Security Institute, as reported in Solutions Partner Presentation, RedCreek Communications, Inc., 3900 Newpark Mall Road, Newark, CA 94560, May 13, 1998.

find themselves needing to place increased trust in the security-enhanced products that they acquire.

In light of the several other business problems needing attention, organizations are looking for help to assist them in confirming, or validating, the level of trust they can place in products. Reliance on valid information about the degree of trust that can be placed in a particular product will become ever more critical as

- networking and IT continue to evolve rapidly,
- new networking and information technologies emerge,
- networking and IT products and systems become increasingly complex,
- business develops a more critical dependence on such products and systems, and
- businesses' technical support staffs get even less time to keep up with all such changes.

18.5 SECURITY TESTING AND EVALUATION IS KEY TO ENHANCING TRUST

But how can trust be developed in a security-enhanced network or IT product? Assessments of the security soundness of products can provide trust that the products are reliable and perform as expected. Such assessments are especially compelling when they are made according to well-known, well-engineered, and well-understood security testing and evaluation practices.*

Such testing and evaluation benefits all organizations within the chain of designing, building, marketing, procuring, and using products that are intended to be trusted. Designers and builders need effective product testing and test methods before shipping products. Vendors rely on testing to demonstrate compliance with consumer requirements regarding trust. Vendors also rely on testing and evaluation to increase the value and marketability of their products to would-be consumers. Consumers rely on testing and evaluation as a way of developing trust by ensuring product conformance to their security requirements. They also see testing and evaluation as providing a *mark of quality* and a way to differentiate between competing products. Users are beginning to rely on testing and evaluation to help establish due diligence in legal disputes.

Formal testing of network and IT products has traditionally been used to ensure product conformance to functional, performance, reliability, or interoperability standards. But testing the implementations of security is different. Implemented security services are intended to protect the functionality within, the performance achievable by, or the reliability expected of a component. When testing and evalu-

* To those readers familiar with security and the testing and evaluation of security-enhanced products, the term "evaluation" is typically used to mean both the testing of a product as well as the evaluation and analysis of its architecture, design, documentation, code, etc. In this chapter, the terms "testing" and "evaluation" are used in their traditional, colloquial senses. Herein the word testing implies the stimulation of an implementation and the observation of responses from the implementation; and, the word evaluation implies just the analysis of a product's architecture, design, code, etc.

ating a product that claims to provide security services, the confidence demands are greater than those associated with testing the functionality, performance, or reliability alone. Testing and evaluation requirements for security become more complex and difficult. For example, in addition to testing that certain behaviors exist in accordance with the specifications, security testing and evaluation must also help ensure that unwanted behaviors do not happen.

What further makes security assessment difficult is that the amount and type of analyses performed as part of security evaluation efforts will need to be increased as the degree of trust desired to be established is increased. Such analyses may include scrutiny of a product's architecture, design, and source code, depending on how much trust is desired. Furthermore, trust in a product can be enhanced when the testing and evaluations are performed and validated by competent, independent (ideally separate), third parties, i.e., one party for testing and evaluation, and another party for validating the testing and evaluation results.

18.6 NUMEROUS APPROACHES EXIST FOR SECURITY TESTING AND EVALUATION

Until recently, there have only been a few organizations able to perform competent, impartial security testing and evaluation — and even fewer effective methods for conducting such security assessments. Current and traditional approaches to security testing and evaluation include the following.

18.6.1 HACKING

De facto assurance of the underlying security in a product can arise from aggressive students as well as professional technicians and users who actively probe new products for security flaws. Hacking does not necessarily follow a consistent or comprehensive approach to evaluating the quality of the security functions and services that are implemented. Hence, the assurance achieved is to some uncertain, typically very modest, level of trust.

18.6.2 INITIAL COMMERCIAL APPROACHES

Initial commercial approaches arose typically to support trade press surveys or to provide surface-level testing results for vendor brochures. These approaches are often based on simple, one-size-fits-all (often-called *low-hanging-fruit*) testing that provides minimal, cursory checks of some of the implemented security functionality. No evaluation is made of the confidence (assurance) that can be associated with the soundness (or lack thereof) of the security implementation.

18.6.3 GOVERNMENT-INTERNAL APPROACHES

In order to introduce consistency in describing the security features and levels of trust of a limited set of security-enhanced products, and in order to facilitate comprehensive testing and evaluation of such products, the U.S. Department of Defense

(DOD) developed the Trusted Computer System Evaluation Criteria (TCSEC).[3] The TCSEC — or more colloquially, the "Orange Book" — defined a small set of six classes of increasing security functionality and increasing assurance (from a so-called C1 class to an A1 class) that applied to operating systems. The TCSEC was extended to networking devices[4] and database management systems.[5] Government in-house evaluations were offered first, followed by comparable, government-sponsored commercial evaluation services. Use of TCSEC concepts extended beyond the DOD to other U.S. government agencies and to foreign governments as well.

18.6.4 Vendor Self-Declarations

Another initial approach was based on vendor self-declarations that a specific product meets the needs of their customers in terms of the appropriate amount of confidence to be placed in its implemented security features. In part, such confidence was implicitly tied to the reputation of, or past experience in dealing with, a specific vendor to do a good and adequate job of implementing security.

18.6.5 Good Software Engineering Approach

Another approach is based on the notion of providing trust through use of sound engineering practices during product architecting, design, and implementation, rather than through post-implementation testing and evaluation. One way a software developer can demonstrate competence in building products is through recognized, so-called *capability maturity* assessments of the developer and the developer's software engineering processes. Security-enhanced products built by organizations with demonstrated expertise and maturity can be viewed to merit greater trust than products built by organizations that do not demonstrate mature, competent, software design and engineering capabilities.

18.6.6 Consumer Evaluations

Consumers can develop the requisite substantial technical expertise in-house to test and evaluate specific security-enhanced products directly. Alternatively, consumers can contract a private evaluator or evaluation organization to do such testing and evaluation.

18.7 SHORTCOMINGS OF OLD APPROACHES PROVIDE REQUIREMENTS FOR A NEW APPROACH

All the previous security testing and evaluation approaches added value to the commercial networking and IT marketplace. The degree to which different approaches helped tended to depend on the situation to which they were applied. The lessons learned from these early approaches have been analyzed, used, and integrated to fuel the development of a new, best-of-all-previous-breeds approach

(see "The National Information Assurance Partnership Embraces the New Approach to Security, Testing, and Evaluation," Section 18.11).

The types of shortcomings discovered in the old approaches had greater or lesser degrees of significance dependent on the approach and situation in which it was used. Not all shortcomings accompanied all approaches. Often, the old approaches were not as simple, effective, or inexpensive as they were thought to be. In any event, these shortcomings provided valuable insights, experience, and expertise that have benefited the development of the new, emerging approach.

The categories of the shortcomings that surfaced, and that have since been leveraged to develop the new approach, include a lack of

- a flexible common approach to specify security requirements,
- flexibility of the security testing and evaluation methodologies,
- a common security testing and evaluation methodology,
- security testing and evaluation expertise,
- an independent third party to conduct impartial testing and evaluations,
- an impartial third party to validate the quality of such independent testing and evaluations.

The ramifications of these shortcomings were many, as summarized in the following sections. But, in general, security testing tended to add cost to security-enhanced goods and services. It tended to be insensitive to vendors' time-to-market pressures, sometimes adding delays to product rollout schedules (in the worst cases to beyond the full lifecycle of the product undergoing testing). Sometimes delays arose because of the specific testing or evaluation methodology used. For example, some methodologies relied on a heavily iterated and sequential approach that cycled from testing, to patching and fixing, to retesting and regression testing, and then on to other new test scenarios. In the case of the TCSEC approach, delays sometimes seemed to arise because vendors were not prepared in terms of making detailed documentation and code available, or they sometimes seemed to lack the incentive to expedite testing and evaluation efforts that were subsidized by the government.

Specific ramifications of the shortcomings of early approaches surfaced.

18.7.1 The Lack of Security Requirements Specification Standards

There has been no common and flexible approach that could be used to specify, or to identify, just the right amount of security functionality and assurance for differing products or classes of products. The impact of a lack of a commonly understood, standard, specification language is particularly important in today's fast changing world of networking and IT. Accordingly, users have tended to be confused or unsure as to what security features are really being claimed for a product. Conversely, vendors have tended to find it difficult to articulate their security claims in ways that users can understand and in ways that distinguished one product from

another. Time and money were wasted in conveying knowledge about security features or security implementations.

18.7.2 The Lack of Flexibility of Security Testing and Evaluation Methodologies

Many testing and evaluation approaches were inflexible. They were not always able to provide desired trust in products because they could often not be tightly tied to products' security claims. Some approaches were only able to provide coarse, surface-level testing. The lesson of such approaches is that they did not always prove to be cost-effective or meaningful.

18.7.3 The Lack of Common Security Testing and Evaluation Standards

For users, it has been typically difficult, if not impossible, to compare security test and evaluation results associated with differing products. This is especially so if the tests and evaluations were performed by different testing and evaluation facilities or if the tests and evaluations were associated with different testing and evaluation methodologies. Accordingly, users could not readily compare various products to understand their relative security capabilities and limitations.

From the vendor's perspective, lack of a common, internationally accepted testing and evaluation methodology reduced international competitiveness for product sales. This resulted because tested products still often needed to undergo further user-specific, country-specific, or region-specific, retesting efforts. It was not uncommon for some vendors, especially those supporting large enterprise customers, to conduct a plethora of multiple, often redundant, tests and evaluations on a single product. The costs of retesting prevented vendors from being able to realize many economies of scale with respect to security testing and evaluation.

Accordingly, many leading-edge vendors developed a business case demand to institute a standard set of tests and evaluations that could cover the majority of their testing and evaluation needs across most customers (domestic or foreign). Such standards could be used to eliminate or minimize duplicate testing, could be used for cost avoidance associated with retesting, and could therefore positively impact product price and profit margins.

18.7.4 The Lack of Security Testing and Evaluation Expertise

Only a handful of organizations have had sufficient testing and evaluation expertise to be able to conduct a single, competent, independent security testing and evaluation campaign, let alone many concurrent security testing and evaluation campaigns. Fewer still were security testing and evaluation approaches that were both effective and efficient. In the highly competitive, fast-paced network and IT world, testing and evaluation approaches that added extensive costs or delays proved not to be relevant.

18.7.5 The Lack of Third Party Testing and Evaluation

There have been few third party testing laboratories available to conduct impartial security assessments to increase the perceived level of confidence in products; many vendors and consumers feel it necessary to use a competent, recognized, impartial, third party security testing and evaluation laboratory to conduct security assessments. From customers' perspectives, such third party testing and evaluation dramatically lowers any sense of impropriety.

18.7.6 Lack of Accreditation, Verification, and Validation of Independent Security Testing and Evaluation

There has been a lack of third parties to accredit the worthiness of independent testing and evaluation laboratories, to verify that tests and evaluations have been properly performed, and to verify that testing and evaluation results are appropriate and valid. This has lead to uncertainty and diminished consumer trust regarding the consistency and robustness of existing testing and evaluation approaches. It has also led to difficulty in comparing the results of testing and evaluation performed by different organizations. Vendors and consumers feel it valuable to have a third party to independently oversee, review, and/or otherwise validate the security testing and evaluation and to make sure the testing and evaluation approaches are used consistently across different product security assessments.

18.8 WHAT ELSE IS NEEDED

As networking and IT continue to change rapidly, as products become increasingly more complex, and as our dependence on them becomes more pronounced, effective and economic testing and evaluation of the security implemented in such products becomes even more critical. Security products and security-enhanced network and IT products must change to stay ahead of evolving threats. The tests and the test and evaluation methods and metrics used to evaluate such rapidly proliferating and changing product offerings must also be able to evolve quickly.

Users want to be able to create tailored specifications for the security-enhanced products they need to solve their specific problems. They do not want the completion of such specifications to depend on a lengthy standardization process. Instead, users now want to have control over their own specifications, rather than a long-term involvement in some standardization process. They want to be able to take full advantage of the COTS (commercial-off-the-shelf) marketplace and be able to stipulate their specific requirements in a language that both the user and vendor understand. They also do not want to be at risk that the language they use will become obsolete.

18.9 SETTING THE STAGE

Many other events and circumstances further set the stage for a new approach to security testing and evaluation of network and IT products. While the earlier

described initial approaches for security testing and evaluation filled early needs, a changing marketplace demanded a new approach based on international standards.

The marketplace for which the initial approaches were developed had been changing rapidly in the mid to late eighties both in terms of vendor production philosophies and erosion of U.S. centricity. Acquisition and development of unique, consumer-specific, network and IT products and systems were phased out in favor of an approach based on (a) acquisition of COTS network and IT products, coupled with (b) consumer integration of these COTS products into network and IT systems. Furthermore, the shift to networked computers and applications and use of new network and IT services brought forth a plethora of new security-enhanced network and IT products. These products began addressing security functional and assurance requirements far more diverse than could be handled by approaches such as those within DOD's "Orange Book."

Also, different countries and organizations began developing other security criteria divergent with U.S.-based approaches. In Europe, several countries jointly developed the Information Technology Security Evaluation Criteria (ITSEC) in 1991. The Canadian Trusted Computer Product Evaluation Criteria (CTCPEC) was developed in 1993 as a combination of ITSEC and DOD's "Orange Book" approaches. In the U.S., the Federal Criteria were also drafted in 1993 as another attempt to combine North American and European security evaluation criteria approaches.

These marketplace changes weakened the effectiveness of initial security testing and evaluation approaches. The shift of consumer reliance to COTS products with rapid vendor turnover cycles began rendering the slower reacting, government-internal, security testing and evaluation model less effective. Because of the various different security product evaluation criteria and because of concomitant marketplace confusion about the many criteria, many countries and organizations chose not to embrace government-oriented security testing and evaluation approaches.

18.10 STANDARDIZATION BEGINS

With the advent of such marketplace dynamics, a new approach for security testing and evaluation became even more evident. New international standards for specifying security requirements and features and for defining accompanying security testing and evaluation methods were needed. In 1993 the development of such standards began under the auspices of a multi-national Common Criteria (CC) project. One of the goals of the standardization efforts within the CC project was to develop new, state-of-the-art concepts by leveraging experiences gathered and lessons learned via all the earlier security specification, testing, and evaluation efforts.

The impacts of these new standards (see "Relying on Standards" under Section 18.14) eventually became significant. Their emerging ability to support specification and assessment of virtually unlimited, different combinations of security functionality and assurance for any security-enhanced network and IT product, or class of products, began reducing the utility of the more limited, initial approaches.

18.11 THE NATIONAL INFORMATION ASSURANCE PARTNERSHIP EMBRACES THE NEW APPROACH TO SECURITY, TESTING, AND EVALUATION

In light of the needs, problems, and factors presented above, the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) formed a collaborative venture to pursue the emerging new CC-based international approach to security assessment. This collaboration was dubbed the National Information Assurance Partnership or NIAP.*

The partnership combined the extensive IT security testing and evaluation experience in both agencies. The NIAP was initiated to help ensure the availability and quality of security-enhanced network and IT products and systems by means of new, commercial testing and evaluation services that are government-accredited, government-validated, and internationally recognized.

18.12 WHY THE U.S. GOVERNMENT GOT INVOLVED

The U.S. government got involved with this new approach in order to transfer its vast security assessment knowledge base and to represent the U.S. interests in the development of these international standards and agreements.

With the shift to new international standards, there were compelling reasons for the U.S. government to remain involved, but with a shifted focus, with the newly emerging CC-based security testing and evaluation paradigm. The U.S. government had significant security and security assessment knowledge and expertise it could contribute to the standardization efforts. The government also had a role in representing U.S. interests in developing the international CC standards and associated testing, evaluation, and implementation guides. The government was also needed to help develop and approve international agreements for recognizing the results of security tests and evaluations performed in other countries in accordance with these standards. In addition, the U.S. government could provide oversight to maintain quality and consistency of independent testing and evaluation facilities. It could foster research pertaining to new approaches for security testing and evaluation. Also, it had some ability to stimulate user-pull (demand) and vendor-push (investment) for the security-enhanced network and IT products that could arise from testing and evaluations done in accordance with the new CC-based security assessment approach.

NIST and NSA were the most appropriate elements of the U.S. government to bring together to form the NIAP. Each party was able to bring a distinct but complementary mission to this partnership. NIST is responsible for standards and guidance for the unclassified but sensitive systems within the U.S. government. Also, NIST has a statutory responsibility to assist the private sector when requested. NIST could leverage its traditional role in research, standards, accreditation of private laboratories, and metrology to address security testing, evaluation, and assurance needs. NSA is responsible for the security of classified

* The NIAP web site can be found at http://niap.nist.gov.

government systems. With an increasing shift to COTS products and a desire to shift evaluation of commercial products to the private sector, the NSA had a compelling need for its customers to use COTS products with a reasonable degree of assurance. The NSA brought many years of experience from working on the security of very sensitive, critical systems.

With the above factors as a backdrop, NIST and NSA signed a letter of partnership in August 1997 thus forming the NIAP.

18.13 NIAP'S GOALS

The strategic goals of NIAP are

- to improve the trust of citizens, private sector organizations, and government in the security and reliability of networking and IT that we rely on so heavily for conducting business,
- to help ensure the development, manufacture, and use of security-enhanced networking and IT products, with such trust, through the creation and maintenance of a standards-based, commercial, security testing and evaluation industry whose goal is to be cost effective, and
- to establish a program to ensure quality and validity of testing and evaluation and to foster an international marketplace for tested and evaluated products.

18.14 THE NIAP PROGRAM – ITS VISION AND APPROACH

To meet its strategic goals, the NIAP has initiated a program aimed at instigating both a new commercial security testing and evaluation industry with appropriate supports and a new security assessment paradigm. This new approach is unlike any of the other approaches summarized earlier. It capitalizes on the strengths, and overcomes the problems, of the earlier approaches.

The elements leveraged by NIAP for the new approach include

- newly emerging standards for specifying, testing, and evaluating security-enhanced products,
- many well-known and predefined security functional and assurance requirements profiles for specific areas of technology and specific vertical industries,
- commercial, competitive testing services that can be selected by customers based on their own, specific, business considerations,
- a scheme for accrediting testing laboratories, to foster testing quality and consistency, and for further increasing product trust by validating test and evaluation results from those laboratories,
- research and development to improve commercial security assessment quality,

- a framework for fostering international trade by recognizing validated test and evaluation results thereby fostering a "test once, buy/sell anywhere" marketplace,
- outreach to monitor the effectiveness of the approach, to tune the approach to evolving marketplace needs, and to promote development and enhancement of the quality of commercial, security-enhanced products.

The following subsections provide more details on each of these elements. Section 18.15 ("A New Common Criteria Scheme Ties Together the NIAP Elements") shows how these elements are related.

18.14.1 Relying on Standards

The NIAP approach relies on the use of international standards for specifying

- security requirements in products and systems,[6] and
- common security testing and evaluation methods.[7]

These standards are referred to as the CC (Common Criteria) and the CM (Common Methodology for Information Technology Security Evaluation), respectively. Use of the CC and CM standards is key to providing a common, internationally recognized understanding of IT security requirements and IT security assessment methods.

The CC provides a standard *language* for specifying security requirements. It also provides a flexible *method* for specifying security requirements of all sorts.

The standard language is contained in a pair of voluminous catalogs of elementary, re-usable, components of specific security functional and assurance requirements. Security functional requirements are organized into 11 major classes, such as auditing, cryptographic support, and security management. Similarly, security assurance requirements from several evaluation assurance classes form a set of seven defined levels of assurance. The elementary assurance requirements specify reasons to trust implemented security functionality to be effective and correct. These assurance levels articulate increasing rigor and formalism for ensuring increasing confidence in implementations of security functionality. The assurance levels range from a low assurance level, called Evaluation Assurance Level 1 (EAL1), to a high assurance level (EAL7).

The flexible method is based on the ability to use the CC to tailor-develop any of two different types of security requirements profiles.* A product-specific type of CC specification is called a security target (ST). It is typically developed by a vendor to describe the security-relevant portions of a single, specific product. The

* To those readers familiar with security testing and evaluation, the term *profile* is reserved for use only with the notion of a Protection Profile (defined later in the text above). In this chapter, the term is used in its traditional, less-constrained, colloquial sense of a selection of significant features from a larger set of features.

other type of CC specification profile is called a protection profile (PP). It is typically developed by

- a single user organization, or
- some broad user constituency with similar interests, or
- a consortium of vendors.

A PP is used to articulate the set of security requirements that define users' needs or that can define a class of desired products wherein any number of implementations may satisfy the stipulated requirements.

STs and PPs are constructed by selecting from the CC catalogs the set of elementary functional and assurance requirements that appropriately define the security aspects of a specific product or a generic class of products, respectively. The result is a tailored profile of standard security requirements. User needs and vendor product claims are profiled as specific subsets of standard security requirements from the CC catalogs. Some of the standard requirements may be refined from that which appears in the CC. Thus, solutions can be identified with exactly the degrees of security functionality and levels of assurance needed, no more and no less, for any particular situation. Being standard security requirements, they will generally be widely understood throughout the marketplace.

The CM defines assessment methodologies for CC-based testing and evaluations. It describes actions for conducting product tests and evaluations for a variety of assurance levels. Such common, well-recognized testing and evaluation approaches reduce the need for customer-unique and country-unique approaches.

Use of the CC and CM thus provides a common base for describing security-enhanced products and assessing whether they work as claimed. These standards form the foundation for international recognition of test results. They also form the basis for consumers of security-enhanced products to gain higher levels of confidence in the products they buy than has heretofore been generally available. The effect of these standards has been to raise the bar relative to trust in products.

The CC and CM are under various stages of public scrutiny and are thought to be technically fairly stable. Final standardization efforts for the CC are in progress in the joint International Organization for Standardization (ISO)/ International Electrotechnical Committee (IEC), Joint Technical Committee 1 (JTC 1) for Information Technology, Subcommittee 27 (SC27) for Security Techniques, Working Group 3 (WG3) for Security Criteria. Information about these standards and related activities is available on the World Wide Web.* The CM is under development in a multinational project and will likely be transitioned to the ISO/IEC community in the near future.**

* Public release versions of the CC and CM are available at http://csrc.nist.gov/cc/.

** The CC and CM are also available at http://ccse.cesg.gov.uk. This web site hosts the Common Criteria Support Environment (CCSE) which is expected to provide access to several CC-related and CM-related materials, such as Requests for Interpretations of the CC and CM Observation Reports, as well as access to newsgroups for discussing such materials.

18.14.2 Growing the Set of Security Requirements Profiles

As a way of jumpstarting the security-conscious community to begin using the new CC-based approach, NIAP, as well as its NIST and NSA parent organizations, have supported the development of a starter-set of PPs. Diverse user constituencies and vertical industry consortia are being encouraged to seed the marketplace with diverse, initial sets of PP requirements profiles. Vendors are also being encouraged to begin developing STs. Examples of the types of CC-based security requirements that existed, or were being completed, at the time of the writing of this chapter are indicated later.

Since early experience indicated that development of PPs and STs could be a daunting task for the uninitiated, NIAP has provided help in developing profiles and intends to continue providing help in a number of ways. The types of services that NIAP has provided to aid interested parties in specifying CC-based security requirements include

- profile development guidance,
- CC training,
- profile construction training,
- semi-automated profile analysis and construction tools,
- direct support to the initiation and construction of selected PPs,
- review (a.k.a. vetting) of selected draft PPs,
- validation services for formally evaluated PPs,
- a PP registry, and
- workshops, conferences, and forums to help produce, proliferate, and promote PPs.

For an understanding of the services that NIAP currently provides in this area, interested readers should visit the NIAP web site http://niap.nist.gov/.

18.14.3 Seeding and Using Commercial Laboratories

With the advent of the CC and CM and with growing proliferation of CC-based security requirements profiles, it became feasible to transition security assessment expertise and operations from current government facilities into approved, accredited, private sector laboratories that provide CC-based testing and evaluation.

In 1997, the NIAP began encouraging the initiation, growth, and development of a state-of-the-art, CC-based, commercial security testing and evaluation industry. Commercial laboratories operating under the auspices of NSA's Trust Technology Assessment Program (TTAP) provided initial CC-based testing and evaluation services.* The TTAP laboratories conduct CC-based testing using NSA's TTAP evaluation methodology. Commercial laboratories operating under the auspices of NIAP provide CC-based testing and evaluation using the CM.

The laboratories within this new industry have competitive flexibility to adjust their testing and evaluation services to accommodate different products and different security requirements. The laboratories operate by establishing private contracts

* Information on TTAP can be found at http://www.radium.ncsc.mil/tpep/ttap/index.htm.

with customers to provide such services as PP evaluations, ST development support, and assessments of the ST-specified features in security-enhanced network and IT products. As part of this initial effort, a number of market-dominating countries agreed[8] to recognize, multinationally, the results of this burgeoning U.S. testing and evaluation industry.

The types and degrees of testing and evaluation that need to be performed on products depend on the underlying security functional requirements and the degree of confidence desired in those products. Being based on the CC and CM, such tests and evaluation procedures are becoming well-known, repeatable, and credible.

18.14.4 Accrediting Commercial Laboratories

To increase trust in security assessments further, NIAP is instituting mechanisms for providing cost-conscious, government accreditation of commercial security testing laboratories. Such accreditation is in concert with international agreements regarding the multicountry mutual recognition[2] of security assessments. NIAP worked with NIST's internationally recognized National Voluntary Laboratory Accreditation Program (NVLAP) in 1998 to begin developing a laboratory accreditation process and procedures to accredit commercial testing laboratories. The process needed to be flexible so that laboratories could be accredited for exactly the types of security assessments they wanted to perform — no more or no less. The accreditation process and procedures are coming into place.

The accreditation mechanisms are being designed to assess a laboratory's ability to test products using test methods based on the CC and CM. More specifically, they are being used to ensure that commercial security assessment laboratories have the requisite capability to conduct quality security evaluations of network and IT products. They are ensuring consistency and quality among the different commercial testing laboratories both in terms of the quality of testing services they provide and the test results they produce.

According to the emerging accreditation mechanisms, laboratories are accredited, and periodically re-accredited, by NIST's National Voluntary Laboratory Accreditation Program (NVLAP). NVLAP ensures that laboratories meet specific international[9] and national[10] guidelines pertaining to laboratory competency. NVLAP ensures that laboratories meet additional, NIAP-specific requirements pertaining to security assessment procedures and requirements.[11] NVLAP also ensures that testing laboratories have all requisite, NIAP-specified proficiencies needed in order to facilitate subsequent government validation of test results.

Laboratories are accredited for a specific scope of security assessment activities and procedures. For example, a testing laboratory may limit its focus to products in only a specific range of claimed levels of assurance. Thus, a laboratory may choose to get accredited for a specific set of NIAP-approved test methods.

NIAP provides technical guidance, advice, support, and training standards to accredited testing laboratories. NIAP is working to ensure continuing quality within the private, security testing industry by monitoring the accredited laboratories. They are monitored for maintenance of competence and for their adherence to, application of, and interpretation of CC standards.

18.14.5 Validating Test and Evaluation Results

In accordance with the multinational arrangement,[2] NIAP looked to establish independent validation of testing and evaluation results by an impartial third party. The purpose of such validation efforts is to

- increase trust even further in network and IT products that have undergone testing by an accredited testing laboratory,
- promote consistency and comparability among independently conducted assessments, and thereby
- facilitate the international trade for validated, security-assessed products.

NIAP is developing a scheme,[12] the CC Evaluation and Validation Scheme (CCEVS), that stipulates the details of the organization, operations, and management of such a validation concept within the U.S.. According to the NIAP CC scheme, a validation body reviews and provides independent confirmation that security assessments have been conducted according to procedures and guidelines stipulated by NIAP. The amount and depth of private industry oversight to be provided by the validation body is tailorable to the assurance requirements, i.e., the EAL level, claimed of the product under test, the complexity of the IT product, and the experience of the testing laboratory.

The NIAP Validation Body provides confirmation that

- the product was assessed by a testing and evaluation laboratory that is NVLAP accredited and NIAP-approved,
- the laboratory correctly and completely applied the evaluation methodology to verify conformance of the security functional and assurance aspects of the product to a PP or ST,
- the appropriate criteria, test methods, and procedures were used,
- the conclusions of the testing laboratory, as documented in the laboratory's evaluation report, are accurate and consistent with the facts presented in the security assessment.

The scheme stipulates that after the Validation Body has completed the requisite confirmations, the Validation Body facilitates the granting of a CC certificate and accompanying validation report.

The CC certificate is issued by NIAP as designated certificate issuing authorities, namely the NIST Information Technology Laboratory and the NSA Information Systems Security Organization.

The validation report provides information on how well the assessed product conforms to the security functionality and assurance level that it claimed. It indicates the configuration for which the product was assessed, the environment for which the product is intended to be used, the coverage and depth of security analyses, details of the testing approach used, the testing suites used, the testing environment used, the test tools used, and so on.

The NIAP scheme recognizes that other third parties, such as a professional society or a vertical industry association, may choose to implement other validation schemes that may or may not complement the government's scheme.

At the time of the writing of this chapter, NIAP was planning to complete a number of materials related to the scheme in early 1999, including, e.g., NIAP Validation Body policies and procedures, technical oversight and validation procedures, guidance to sponsors of security evaluations, and guidance to testing laboratories.

18.14.6 Fostering International Trade

According to the multi-national arrangement,[2] the validation report and accompanying certificate issued by the government Validation Body are the only acceptable evidence that a product has undergone a security assessment that is recognized by the other country partners in the arrangement. Thus, a major benefit of the NIAP-advocated security testing, evaluation, and validation approach is that it opens global markets to vendors. All country partners recognize products that are tested, evaluated, and given certificates by any other country partner. This means that such products can be procured with a known degree of confidence and with no duplicative re-testing in foreign markets. The significant international competitiveness and market opportunities consequently afforded are powerful features that are working to increase the scope and availability of trusted products worldwide and to reduce their cost. The impact of the NIAP approach and the NIAP Validation Body is to help foster such improvements in international trade.

While validation is mandatory to obtaining an internationally-recognized certificate from the U.S. government, it is possible that obtaining such a certificate and its accompanying validation report may be an unnecessary final step for certain communities. For such communities, simply undergoing a security assessment by a government-accredited testing and evaluation laboratory may be sufficient.

18.14.7 Promoting R&D

During the first years of its existence, NIAP concentrated on fostering the establishment of the commercial security assessment industry, helping users articulate their security needs in Protection Profiles, and stimulating vendors to articulate their product's capabilities in Security Targets. NIAP is now focusing more attention on associated research and development (R&D).

NIAP is fostering public domain R&D. It intends to expand its support in key R&D areas. At a minimum, areas of interest include developing tools and techniques to help improve the efficiency, flexibility, quality, effectiveness, measurability of, and automation of commercial testing and evaluation methods and approaches. NIAP is especially interested in applied research that leads to quick, low-cost testing and evaluation solutions that can provide better assessment coverage and can be readily embraced within typical vendor product development cycles and product revision cycles.

In support of this, NIAP is investigating the feasibility of alternative assurance approaches, possibly to augment or to supplement its current focus on CC-based

testing and evaluation. One such alternative assurance approach is the Systems Security Engineering Capability Maturity Model (SSE-CMM). Development of the SSE-CMM is progressing through active participation and corporate investment of the security engineering community, coupled with sponsorship from the National Security Agency, the Office of the Secretary of Defense, and the Canadian Communications Security Establishment.

The objective of the SSE-CMM efforts has been to advance security engineering as a defined, mature, and measurable discipline, with the effect of improving the quality, cost and availability of, and trust in, IT products, systems, and services. A project has been established* to provide a framework for measuring and improving performance in the application of security engineering principles. The model is in trial use on some government procurements. Its purpose is to enable

- selection of appropriately qualified providers of security engineering by being able to differentiate bidders by their capability levels and by the associated programmatic risks each presents,
- focused investments in security engineering tools, training, process definition, management practices, and improvements by engineering groups,
- capability-based assurance, i.e., development of system or product trustworthiness based on confidence in the measured competency and maturity of an engineering group's security practices and processes.

It is this latter focus that may be of interest to NIAP as a potential alternative approach for assessing the assurance that can be placed in products developed by measurably competent vendors. Follow-on efforts in this area will be focused on investigating the feasibility of extending the NIAP CC scheme to accommodate security assessed by such alternate means.

Another area of endeavor is to investigate how CC standards can be employed for large, distributed, evolving systems composed of many products. It is not clear how, or how well, the CC language can be used to describe the security features of such systems. How to apply the CM for testing and evaluating such systems is also in question. NIAP is teaming with the Federal Aviation Administration to investigate the issues associated with applying CC concepts and conventions for just such a system in the early stages of system planning, development, and acquisition.

18.14.8 Conducting Outreach

NIAP supports outreach as an important function. It is continually conducting outreach and associated education for a number of reasons, including:

- maintaining an up-to-date understanding of the marketplace and its needs and demands for security testing, evaluation, and validation services,
- raising general awareness of, confidence in, demand for, and use of the commercial security assessment industry,

* See http://www.sse_cmm.org or, duplicatively, http://constitution.ncsc.mil/wws/sse_cmm.

- stimulating user demand for and use of security-enhanced products,
- stimulating vendor investment in developing security-enhanced products,
- bolstering trust in such products so that manufacturers and consumers can build and buy with confidence, approaching non-governmental bodies, such as vertical industry trade groups and consortia, to encourage them to embrace the new security assessment approach by
  - encouraging the use of evaluated security-enhanced IT products, or
  - issuing their own certificates that may be based on either more lenient or more restrictive validation requirements than those supported by the NIAP certificate,
- promoting expansion in the base number of mutual recognition partner countries, and
- evangelizing for the need to enhance academic interest in
  - conducting R&D to support and to advance security testing and evaluation concepts, and
  - developing degree programs focused on matriculation of experts to help populate positions within the new commercial security testing and evaluation industry and applicable government oversight and validation bodies.

18.15 A NEW COMMON CRITERIA SCHEME TIES TOGETHER THE NIAP ELEMENTS

The elements of the NIAP initiative interact, in aggregate, to provide the internationally recognized, CC scheme[12] for conducting high quality security assessments within the U.S. The details of this scheme were being developed at the time of the writing of this chapter and thus there may be changes from what is indicated herein.

A summary of the scheme is portrayed in Figure 18.1.

According to the CC scheme, there are four types of activities that can be undertaken in conjunction with the various NIAP elements. These activities are

- developing and using basic CCEVS supports: standards, specifications, test and evaluation methods, and R & D (see lines numbered 1.1 through 1.4 in the diagram),
- developing a set of accredited testing and evaluation laboratories (see lines numbered 2.1 through 2.6 in the diagram),
- developing a set of validated products that have been granted certificates based on successfully undergoing testing, evaluation, and validation (see lines numbered 3.1 through 3.6 in the diagram), and
- mutual recognition interactions (see line numbered 4.1 in the diagram).

18.15.1 Developing and Using the Basic Supports

The basis for all aspects of the scheme are the CC and CM standards. The CC provides the key input (line 1.1 in Figure 18.1) necessary for developing PPs. Validated PPs are entered into the PP registry. The PP registry identifies those PPs

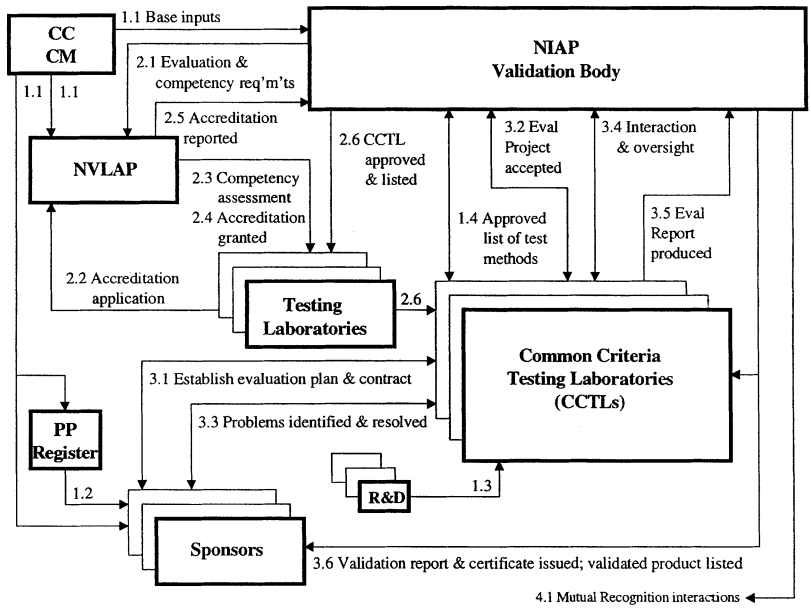

Figure 18.1 Summary of the CC Scheme.

that may serve as the basis for specifying products (line 1.2) that are submitted by product sponsors for testing, evaluation, and validation. Products that can be submitted may be PPs, or they may be hardware or software entities that implement STs. The CC and CM also provide the basic concepts (line 1.1) that drive the NIAP Validation Body and the laboratory accreditation efforts of the NVLAP. The CC and CM provides the basis for a list of approved test methods (line 1.4) that may be used during product testing and evaluation. NIAP-advocated R & D serves (line 1.3) to improve testing and evaluation concepts and methods approved by the Validation Body and used by accredited testing and evaluation laboratories.

18.15.2 Accrediting Testing and Evaluation Laboratories

Accrediting commercial test and evaluation laboratories so that they can be approved as official CC Testing Laboratories (CCTLs) sanctioned by the NIAP Validation Body is a multistep process. The NIAP Validation Body provides security testing, evaluation, and competency requirements (line 2.1) to the NVLAP. These requirements are used by the NVLAP to assess (line 2.3) the technical, methodological and security testing and evaluation competency of laboratories that have applied (line 2.2) for accreditation. Upon successful laboratory assessment, the NVLAP grants accreditation (line 2.4) to testing and evaluation laboratories for a specific scope of approved testing and evaluation activities (such as the specific set of test methods that can be used by the CCTL, line 1.4). NVLAP reports (line 2.5) such accreditation to the Validation Body. The Validation Body then approves (line 2.6) the accredited

laboratory to be recognized as an official CCTL. The Validation Body adds (line 2.6) the new CCTL to the list of approved laboratories maintained and publicized by NIAP. Through these processes the NIAP Validation Body expects to provide the marketplace with a set of competent and comparable private security testing and evaluation laboratories that can be used to assess the security-enhanced portions of any networking and IT product.

18.15.3 Testing, Evaluating, and Validating Products

The actual testing, evaluation, and validation of specific products is a multistep process involving a continuous partnering of activities among the sponsor of a product seeking a NIAP certificate, a CC Testing Laboratory, and the NIAP Validation Body. A sponsor and a specific CCTL negotiate (line 3.1) a contract in which both parties agree to a testing and evaluation workplan and schedule for a specific product; the sponsor agrees to provide the product and other materials required for testing and evaluation efforts. The CCTL and Validation Body interact (line 3.2) and, if the work plan, sponsor documents, and other materials are in good order, the Validation Body approves (line 3.2) the initiation of the specific testing and evaluation project. As the testing and evaluation proceed, any problems encountered by the CCTL are shared with the sponsor and the Validation Body (line 3.3). The sponsor and CCTL work to resolve (line 3.3) such problems, and, as necessary, the Validation Body (line 3.4) engages in technical interactions and provides technical guidance and oversight to help handle the problems. If the sponsor desires that later releases and versions of the product should undergo testing, evaluation, and validation, the sponsor, CCTL, and Validation Body could collaborate in developing a certificate maintenance process to expedite subsequent security assessments of the later releases and versions of the product. Upon completing its testing and evaluation efforts, the CCTL writes a testing and evaluation report that is provided (line 3.5) to the Validation Body and the sponsor. The Validation Body drafts an associated validation report. After review (line 3.6) by the sponsor and CCTL, the Validation Body issues (line 3.6) a CC certificate to the sponsor for the specific product model and version that was assessed. The Validation Body also provides a final validation report to the sponsor and lists the specific product on the validated-products list that NIAP maintains and publicizes.

18.15.4 Mutual Recognition Maintenance

The NIAP Validation Body interacts with comparable organizations (line 4.1) in the other countries abiding by mutual recognition arrangements. The purposes of this interaction are to

- maintain and update the mutual recognition arrangements,
- synchronize any interpretations that may need to be made relative to, for example the CC, CM, approved test methods, or certificate issuance procedures, and
- exchange lists of validated products that are mutually recognized.

18.16 NIAP'S EARLY SUCCESSES

The NIAP initiative has had numerous, early successes. They attest to the expected longevity of the flexible, new approach NIAP advocates for assessing the trustworthiness and quality of security-enhanced network and IT products. They also attest to the robustness of the emerging marketplace associated with such products. Early successes, described more fully in subsequent sections of this chapter, include

- the rapid adoption of mutual recognition arrangements among many of the countries representing the bulk of the world's economy associated with building and buying trusted security-enhanced products,
- the rapid uptake of the international standards to proliferate the number of security requirements profiles,
- the emergence of tools to help automate the development of security requirements profiles,
- the unprecedented number of security testing and evaluation laboratories that rapidly emerged,
- the growing number of vendors that have engaged the new approach and the growing number of different products that have already undergone assessments according to the new approach, and
- the growing number of key, large user, and vendor consortia who are exploring the desirability of embracing the new approach.

These successes are mitigating the initially perceived risks that were thought to be barriers to achieving the NIAP vision. These earlier-perceived risks included overcoming the momentum and tradition ensconced in extant approaches, the timing of the introduction of a new approach relative to other large IT needs such as Y2K preparation, and the ability for the marketplace to achieve a critical mass for a new approach.

18.16.1 MUTUAL RECOGNITION ARRANGEMENTS GUIDE GLOBAL COOPERATION

One of the most significant early successes to which the NIAP contributed was the consummation of a CC mutual recognition arrangement among several countries. An initial, interim version of such a mutual recognition arrangement[8] was signed in early 1998 by government bodies within Canada, the U.K., and the U.S. Later in 1998, several countries (Canada, France, Germany, the U.K. and the U.S.) signed a more comprehensive mutual recognition arrangement,[2] with The Netherlands being able to sign somewhat later as soon as its national scheme was put into place. There is serious interest in other countries, such as Australia, Japan, New Zealand, and Sweden, to be added to these multicountry arrangements as soon as admittance procedures are finalized. Other countries appear to be in the wings. In total, the signing countries represent a very large share of the marketplace that produces and consumes security-enhanced network and IT products.

The purposes of the full mutual recognition arrangement[2] are many-fold. The signing countries acknowledge a strong mutual understanding and respect for each other's knowledge, abilities, and experiences with respect to CC-based, security assessments. They agree to maintain a mutual understanding and trust in each others' technical judgment, reliability, and competence pertaining to security testing, evaluation, and validation. They agree to put into place and to maintain comparable, national, CC-based security testing, evaluation, validation, and oversight processes that are to be carried out in a duly professional manner and that will ensure consistent results worldwide. Responsibilities of security testing and evaluation laboratories and national oversight and validation bodies are spelled out, along with requirements on country-specific processes and validation certificates. The signing countries also agree to formally recognize the results of security assessments in each other's countries. (The recognition does not apply to assessments of products claiming the highest levels of assurance.) The countries agree to harmonize any interpretations of the CC and the CM that they feel might be necessary in the future. They agree that each country will list products that receive validation certificates in other countries and that each country will recognize these products as if they were validated in their own country. In effect, each country accepts any other country's validation certificate as equal to its own. Also, agreements were made on procedures for adding or terminating membership in the arrangement.

These processes are established either under a law or an official administrative procedure valid in each of the signing countries.

18.16.2 Profiles Are Proliferating

Another significant early success to which the NIAP contributed was the rapid uptake of the international CC standards by several networking-based and IT-based communities who have used these standards to develop and to proliferate the number of security requirements profiles. Examples of the types of security requirements profiles that were completed, or were being written, at the time of this chapter's writing, show a remarkable breadth of PP and ST development support, including the following:

Product-class-specific profiles

- Firewall (both router and packet filter) PPs
- Telecommunications switch PP
- Commercial DBMS PP
- Operating system PP equivalent to the TCSEC C2 class
- Operating system PP equivalent to the TCSEC B1 class
- Smart Card PP

General security profiles

- Role-Based Access Control (RBAC) PP
- CS2 PP for general computer security requirements at an EAL2 assurance level

Vertical-industry-specific or market-sector-specific profiles

- Federal Aviation Administration National Airspace System, Information Management System (FAA/NIMS) PP
- Telecommunications switch PP
- Department of Defense Warfighters' Intrusion Detection PP
- Health Open Systems and Trials (HOST) healthcare PPs (planned)
- Government Database Management System PP (G.DBMS PP, somewhat equivalent to a TCSEC C2 DBMS interpretation)
- Government Multi-Level Secure DBMS PP (G.MLS.DBMS PP, somewhat equivalent to a TCSEC B1 DBMS interpretation)

Vendor-specific security targets — A number of leading vendors in the database management system, firewall, and intrusion detection market sectors have written STs. (Readers should browse the validated products list available off the Product Testing page of the NIAP web site to get up-to-date information which indicates which vendors have written STs for which specific products.)

Additional information on many of the above security requirements profiles and profiling activities is available on the World Wide Web.*

18.16.3 R&D Makes Profile Development Faster, Better, Less Expensive

To maintain the momentum of the above early security requirements profiling efforts and to achieve maximum usage of the CC, the CC needed to be accessible to, and useable by, a wide swath of professionals throughout the various network and IT product communities. Since it is not practical to expect large numbers of potential PP and ST authors to acquire an in-depth knowledge and understanding of the CC, development of automated tools to help generate PPs and STs was needed.

Another early success to which NIAP contributed was the design, implementation, and delivery of a set of Java-based tools for profile development support that run under Windows95. The aggregate "CC Toolbox" is to assist both the PP author and the ST author in the basic tasks of generating the introductory documentation for PPs and STs. This is intended to simplify and to streamline the use of the CC for many profile writers. One of the main challenges for profile authors addressed by the CC Toolbox is to help find the appropriate components from within the CC requirements catalogs to apply to the profile being authored. Another major headache for profile authors that the CC Toolbox handles is the analysis of a draft profile for consistency and for resolution of dependencies that may exist among the various CC components tentatively selected to reflect the profiled security requirements.

The CC Toolbox consists of two basic tools. The PP tool is called PAA, Profile Authors Assistant, and the ST tool is CCDA, Common Criteria Developers Assistant. The PAA helps to define the security environment, security objectives, and security

* http://csrc.nist.gov/cc/pp/pplist.htm and
http://www.radium.ncsc.mil/tpep/library/protection_profiles/index.html.

requirements portion of a PP. The PAA will interview the PP developer regarding the security needs to be addressed. Based on the interview, the PAA is to produce a PP that specifies the appropriate functional and assurance requirements components from the CC catalogs.

The CCDA aids a product developer in creating an ST for an existing or new product. The CCDA interviews the developer about the security design features accompanying the product, or planned product, for which an ST is to be written. From the interview, the CCDA can produce an ST that specifies the applicable set of functional and assurance elements from the CC catalogs. These elements describe the security features, security environment, supporting documentation, and testing and evaluation activities of the product for which the ST is to be written. The CCDA also assists the ST author and evaluator (i.e., the product developer, the test and evaluation laboratory, or the evaluator) by performing some automated checking of functional security requirements.

Four release cycles are scheduled for the CC Toolbox, with the fourth scheduled for delivery in January 2000. Each release adds additional capabilities and is able to handle more complexities of the CC. Later releases are expected to incorporate artificial intelligence technologies so that a profile can be automatically generated in response to any specific threat scenario as input to the CC Toolbox.

18.16.4 Testing And Evaluation Laboratories Embrace The CC

Another early success indicator is that a significant number of private, security assessment laboratories have been rapidly entering the market under the interim auspices of the Trust Technology Assessment Program.* For them, there are clear, valid and profitable business cases for providing CC-based security testing and evaluation services in concert with NIAP's concepts. The TTAP was expanded in late 1997 to include CC-based evaluations. Recently, the TTAP has been operating in accordance with the Interim Mutual Recognition Agreement[8] using a TTAP Scheme** that could be thought of as an early, interim prototype of the NIAP scheme.[12] The procedures used by a commercial security assessment laboratory in order to become authorized to perform CC-based testing and evaluation within the TTAP are also spelled out in the TTAP Scheme. An up-to-date list of CC-based security testing and evaluation laboratories operating under the auspices of the TTAP can be found on the TTAP web site.

At the time of this chapter's writing, it was expected that in 1999 the NIAP CC scheme would be deployed and would operate in accordance with the final Mutual Recognition Arrangement,[2] and that TTAP would provide for a smooth transition to the CC-based testing program under NIAP. With the scheme fielded, the NIAP Validation Body would begin using NVLAP services to accredit laboratories. Laboratories would be approved as security assessment laboratories that could be used

* http://www.radium.ncsc.mil/tpep/ttap/

** The scheme can be viewed at http://www.radium.ncsc.mil/tpep/ttap/Scheme.html

by customers to obtain validated CC-based security testing and evaluation recognized worldwide under the final Common Criteria Mutual Recognition Arrangement.

It is expected that many of the above private laboratories that formerly operated under the auspices of TTAP and the Interim Mutual Recognition Arrangement would undertake NVLAP accreditation to become authorized under the NIAP CC scheme. These NVLAP-accredited laboratories will be electronically listed by NIAP on its web site as approved, accredited CCTLs (Common Criteria Testing Laboratories). Also listed on the web site will be the NIAP-approved test methods that can be used by the different CCTLs.

18.16.5 Products Emerging Amid More Efficient Testing and Evaluation Processes

Another early success indicator is that CC-based, tested, and evaluated products are beginning to populate the marketplace. Industry-leading vendors in numerous networking and IT market sectors have been early adopters of the NIAP-advocated security testing and evaluation made available via the TTAP. Vendors have written STs to describe the security features of their products. They have had the security portions of such products assessed by TTAP-approved testing and evaluation laboratories using CC-based testing and TTAP evaluation methodologies. Some vendors have used comparable foreign, CC-based laboratories, such as UK CLEFs (Commercial Licensed Evaluation Facilities), whose results are recognized in the U.S. by the Interim Mutual Recognition Arrangement.

Products so evaluated according to CC concepts and conventions are appearing in the intrusion detection, firewall, guard, operating system, and database management system market sectors. An up-to-date list of products that have undergone such testing and evaluation within the U.S. is available on the World Wide Web.* Products evaluated in other countries appear on the evaluated products lists electronically maintained by other such countries.**

There are early indications that the new, NIAP-advocated, testing and evaluation approach is overcoming shortcomings inherent in earlier approaches. The new commercial-based testing and evaluation industry is providing ways to shorten testing cycles. For example, testing and evaluation laboratories are able to provide mechanisms such as double shifts for evaluators, and they are able to provide evaluation services on a vendor's premises. Providing less government oversight for evaluations targeted for lower level assurances is speeding up evaluations for those products claiming lower levels of assurance.

The list of prominent vendors in their fields showing early and strong support of the NIAP vision continues to grow. It is reasonable to expect that a rich choice of timely and cost-competitive, validated products will exist, and that customers worldwide will select such products over ones that are not tested and evaluated.

---

* The list of such CC-based products using the CCEVS scheme is posted on the Product Testing page of the NIAP web site (http://niap.nist.gov). The list of products using the TTAP scheme is posted in the Common Criteria Evaluated Products List at http://www.radium.ncsc.mil/tpep/epl/cc_st.html.

** For example, products that have been successfully tested and evaluated according to the national scheme of the United Kingdom are listed at http://www.itsec.gov.uk/

18.16.6 NIAP Reaches Out To Work Directly With Several Market Sectors

Another early success indicator is the number of prominent user and vendor consortia examining the utility of the new security testing, evaluation, and validation approach for their needs. Since 1998, NIAP has been reaching out to various networking, IT middleware, and IT infrastructure communities. NIAP personnel have begun working with numerous user, vendor, and vertical industry consortia to identify and assess areas of mutual interest regarding PP development and testing, evaluation, and validation of security-enhanced products of interest to their communities. Such outreach is useful to provide senior corporate management, CIOs, and other network and IT decision-makers with exposure to security and security testing and evaluation matters. Such individuals are not normally cognizant of directions being pursued within the traditional, more-confined, close-knit, security community.

At the time of the writing of this chapter, it seemed likely that several cooperative initiatives would soon be in the works or bearing fruit. The following are examples of initiatives that were being examined or initiated at that time. Efforts on engaging in any specific collaborative projects within any of these communities were not yet fully explored or defined. Interested readers should browse the NIAP web site to ascertain the status of any joint activities that may have been initiated as a result of these early discussions.

18.16.6.1 OMG (The Object Management Group)

At the time of the writing of this chapter, NIAP had begun discussions with senior, executive leadership of the OMG, its testing and security special interest groups, and several of its vertical industry domain task forces (medical, electronic commerce, financial, DOD, and telecommunications). Areas of potential mutual and complementary interest included

- development of a PP or PPs to accompany the OMG's base security and security interfacing specifications for the Common Object Request Broker Architecture (CORBA) so as to facilitate corresponding CM-based security testing and evaluation of CORBA interfaces to vendor-specific security mechanisms and services,
- OMG use of the accredited, commercial, CC test laboratories and governments' certificate issuing authorities to augment the OMG's CORBA testing and branding program provided by The Open Group,
- development of vertical-industry-specific, CORBA security interfacing PPs that stipulate mandatory security requirements to be addressed by CORBA implementations supporting specific vertical markets in which NIAP is initially focused (healthcare, financial services, electronic commerce, telecommunications and transportation), and
- cross fertilization of outreach, promotion, and education efforts.

18.16.6.2 IETF (Internet Engineering Task Force)

At the time of the writing of this chapter, NIAP had begun exploratory discussions with leadership from several of the IETF initiatives that have developed draft security standards specific to supporting network management (namely, the SNMPv3 standard) and to supporting general Internet working (namely, the IPsec standard). The purpose of these discussions was to explore IETF leadership interest in getting emerging IETF security standards tested and evaluated, especially before many implementations might begin appearing in the marketplace. As the CC-based approach advocated by NIAP had not yet been used to evaluate an extant, base standard, the notion of evaluating a standard was intriguing, and developing an appropriate approach was of significant interest to NIAP.

18.16.6.3 Financial Community

At the time of the writing of this chapter, NIAP had begun planning discussions with leadership from the financial community's networking and IT standardization groups in the ANSI Accredited Standards Committee (ASC) X9 standards arena. Areas of potential collaborations appeared to be centered on developing PPs as ANSI standards for the most stable of the financial community's needs, such as PPs for Certificate Authorities and smart cards. Such PPs would apparently not be impacted by evolution and changes in underlying protocols, such as SET (Secure Electronic Transfer) and SSL (Secure Sockets Layer), that are under various degrees of acceptance and trial use in numerous financial community pockets. To be of maximal utility and acceptability, development of such PPs would need the involvement of key, senior information security officers and senior auditors from major financial institutions and accounting firms. Workshops and forums were being planned for 1999 to educate such potential PP developers in the financial community about the NIAP-advocated security testing, evaluation, and validation approach and how to translate financial terminology (risk, exposure, prudent controls, etc.) into comparable CC terms (threats, vulnerabilities, etc.). Efforts were being planned to determine what synergy, if any, might be feasible between possible new CC-based activities in the ANSI ASC X9 world and the OMG's financial domain task force.

18.16.6.4 HOST (Healthcare Open Systems & Trials)

HOST is a nonprofit consortium created in 1994 to promote the development of networked IT to improve healthcare. At the time of the writing of this chapter, NIAP had begun planning discussions with HOST to establish forums beginning in mid 1999 to investigate the options of articulating certain healthcare security objectives and requirements in the form of PPs. It was envisioned that these objectives and requirements would be gathered in a format that would assist healthcare IT professionals in comparing and validating the security features of IT products and systems. In addition, there is interest in using the CC concepts and methodology for developing security requirements in an internationally standard format.

18.17 SEVERAL BENEFITS AND POSITIVE TRENDS CONTINUE TO BRIGHTEN THE FUTURE WITH NIAP

No barriers are slowing the transition from old, physical-supply-chain, business models to new electronic business models in virtually all industries. This seemingly inevitable migration will continue to fuel unprecedented growth in market-driven demand for security for supporting and managing business-critical and society-critical network and IT infrastructures.

There are several stakeholders in the security marketplace: security testing and evaluation laboratories, vendors of security-enhanced products, consumers of these products, and researchers developing commercially applicable security assessment advancements. NIAP is working to balance the interests of all these marketplace factions, to improve the quality of security testing and evaluation, and to foster expansion of the number of countries that recognize NIAP validated product evaluations. Positive trends are emerging throughout the marketplace.

18.17.1 Security Testing and Evaluation Laboratories

NIAP is helping bring commercial, accredited security testing and evaluation laboratories online for assessment of products claiming medium and lower levels of assurance. It is moving security testing, and evaluation and validation expertise and operations from the public to the private sector for products claiming these levels of assurance, while maintaining a notion of government oversight via the NIAP Validation Body. (The National Security Agency is still offering security assessment services for products claiming high levels of assurance, such as Orange Book B2-A1 levels or CC EAL 5-7 levels, and, importantly, these NSA security assessment services are becoming based on the CC and CEM.)

The private sector testing and evaluation laboratories are benefiting from the recognition they have received as government-accredited, CC-based, security assessment laboratories. General perceptions about testing and evaluation laboratories have improved by benefiting from NIAP efforts to maintain quality across the pool of private testing and evaluation laboratories.

Vendors' use of standard, CC-based, requirements specifications allowed testing and evaluation laboratories to use customized combinations of standard test and evaluation methods specifically tailored to each product being tested and evaluated. Familiarity with and use of such standard methods tend to shorten the lengths of testing and evaluation efforts.

18.17.2 Vendors

NIAP is beginning to help vendors increase the value and competitiveness of their products through the use of formal, independent, validated, security assessment services recognized worldwide. NIAP is striving to ensure that such services are cost-effective. Vendor use of tailored, CC-based profiles of the security requirements addressed by their product is fostering rigorous and repeatable testing and evaluation.

Duplicate testing and evaluation for foreign markets is being minimized. It is also expected that duplicate, customer-specific testing is also being minimized.

By opening up a commercial security testing and evaluation industry and by qualifying security assessment laboratories, NIAP widened testing choices and alternatives. Vendors are now able to choose security assessment laboratories on business considerations as well as laboratory quality. Some vendors are looking to lower their overhead by reducing in-house security testing and evaluation resources. They also feel that the perception of increased trust arising from third party testing and evaluation will positively impact sales. NIAP's approach of tailoring the amount of validation oversight to the claimed assurance level of the product being tested is fostering sensitivity to time-to-market pressures for products undergoing security assessments.

The impacts of such NIAP efforts are facilitating the lowering of testing costs. Expectations are that vendors will continue to produce products that have undergone NIAP-advocated assessments as long as

- cost-avoidance continues due to minimal redundant testing,
- consumers demand security-assessed products, and
- security assessment processes stay reasonable (i.e., remain sensitive to cost and time-to-market pressures).

Expectations also continue to indicate that product retesting cost avoidance can facilitate more competitive product pricing and can lead to market share improvement.

From vendor marketing perspectives, it is expected that vendors who are among the early adopters of the NIAP-advocated security assessment approach will continue to be seen as leaders in their market sectors and that the validation certificates they receive will continue to provide a substantial sales tool.

It is also expected that acquisition authorities for large organizations of network and IT product users will begin using PPs and CC concepts in procurements of networking and IT products. Vendors will be able to quickly determine if their current products fulfill the needs of the procuring agency via PP to ST comparisons. By basing their responses on their products' STs, vendor responses will be more straightforward, less lengthy, and written in the common CC language and syntax that procurers will expect. Product procurement cycles might then be reduced in length, thereby potentially improving vendors' cash/profit flow. Even when a vendor's response is not based on COTS products, the vendor can still explain concepts using the language and syntax prescribed by the CC.

18.17.3 Consumers

NIAP has collaborated with key consumer groups to help them develop PPs specific to their individual needs. These profiles are helping users — in both the public and private sectors — by providing a sound and reliable basis for adequate, appropriate, credible security testing and evaluation. Likewise, with the emergence of vendor-developed STs, buyers and manufacturers now get clearer mutual understandings of

what security features were implemented, and what features are to be examined during accredited testing.

It is expected that consumer-specific PPs will be effective in ensuring that a consumer's security objectives are relevant to the policies and threats specific to the consumer's environment. It is also expected that PPs will be effective in demonstrating (potentially legally) that the consumer has taken steps to safeguard networking and information handling. PPs may prove to be effective in saving money since the consumer's focus can be narrowed to only those security requirements of essential need.

The availability of two independent and impartial third parties — one to conduct and another to validate security assessments — removed any sense of impropriety or partiality. It fostered comparability and consistency among testing efforts. It also seems to promote the expectation of additional product trust.

The evaluation reports from the security testing and evaluation laboratories are helping consumers by facilitating

- more meaningful understandings of what was evaluated, and
- comparison and selection of security-enhanced network and IT products.

Expectations continue to indicate that consumers will select COTS products that are assessed by the NIAP-advocated approach over products that are not assessed. Expectations also continue to indicate that consumers will buy with confidence, and with no duplicate testing, any product built in any one country and tested in another country.

Accordingly, it is expected that consumers will begin using PPs and CC concepts to help improve the cost, schedule, and performance of their processes to acquire network and IT products. It is expected that PPs will be used to state security requirements succinctly in a common language and syntax, and that acquisition authorities will expect vendor responses to use the same common language and syntax in the product STs they offer. Acquisitions will benefit from the lack of confusion that could have been caused by differences in terms and formats by consumers and the various responding vendors. Acquisition authorities will be able to verify quickly that bidders' STs match desired PPs, and they can expedite the selection of a winning vendor since all vendor responses can be easily compared because of their compliance with the CC.

18.17.4 Researchers

Academics and researchers are beginning to benefit from NIAP's interest in high priority R & D to advance the state of commercial security testing and evaluation practice. In time, NIAP-approved testing laboratories, vendors, and consumers may all benefit from research to make NIAP-advocated, commercial, security assessment quicker, less expensive, and better.

ACKNOWLEDGMENTS

The authors wish to acknowledge their appreciation to inputs provided by Ms. Daphne Willard, NSA and Ms. Mary Schanken, NSA, to reviews and assistance provided by NIAP staff and technical directors, and to assistance provided by Ms. Peggy Himes, NIST.

REFERENCES

1. William Clinton, Critical Infrastructure Protection, *Presidential Decision Directive*/NSC-63, PDD-63, The White House, Washington, D.C., May 22, 1998.
2. Arrangement on the Mutual Recognition of Common Criteria Certificates in the Field of Information Technology Security, The Sponsoring Organizations: Communications Security Establishment, Service Central de la Securite des Systems des Technologies de l'Information, Bundesamt fur Sicherheit in der Informationstechnik, Netherlands National Communications Security Agency, Communications-Electronics Security Group, National Institute of Standards and Technology, and National Security Agency, October 5, 1998.
3. Trusted Computer System Evaluation Criteria, DOD5200.28-STD, U.S. Department of Defense, December 1985.
4. Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria, National Computer Security Center, National Security Agency, Ft. Meade, MD, July 31, 1987.
5. Trusted Database Management System Interpretation of the Trusted Computer System Evaluation Criteria, NCSC-TG-021, National Computer Security Center, National Security Agency, Ft. Meade, MD, April 1991.
6. Common Criteria for Information Technology Security Evaluation, Version 2, CCIB-98-026 through CCIB-98-028, May 1998, Common Criteria Implementation Board (CCIB), ISO/IEC Final Committee Draft (FCD) 15408-1 through FCD 15408-3, ISO/IEC, JTC1, SC27, WG3, N-1951 through N-1953, May 27, 1998.
7. Common Methodology for Information Technology Security Evaluation, Version 0.45, Common Evaluation Methodology Editorial Board, October 31, 1998.
8. Letter of Intent to Support Interim Mutual Recognition, NIST Computer Security Division, Gaithersburg, MD, October 1997.
9. General Requirements for the Competence of Calibration and Testing Laboratories, ISO/IEC Guide 25, 1990.
10. National Voluntary Laboratory Accreditation Program — Procedures and General Requirements, J. L. Cigler and V. R. White, Editors, NIST Handbook 150, U.S. Department of Commerce, Technology Administration, National Institute of Standards and Technology, U.S. Government Printing Office, Washington, D.C., March 1994.
11. Common Criteria Testing, Draft NIST Handbook 150-xx, U.S. Department of Commerce, National Institute of Standards and Technology, Computer Security Division, Gaithersburg, MD.
12. Common Criteria Evaluation and Validation Scheme for Information Technology Security — Organization, Management and Concept of Operations (Draft), Version 1, NIAP (a joint NIST/NSA initiative), Department of Commerce, National Institute of Standards and Technology, Computer Security Division, Gaithersburg, MD, August 1998.