How a Variety of Information Assurance Methods Delivers Software Security in the United Kingdom

Kevin Sloan and Mike Ormerod
Echelon Consulting Ltd.[1]

Many in the software engineering world are already aware of the Common Criteria (CC) and the important role it plays providing confidence in the reliability of Information Technology (IT) product security claims through an independent evaluation and certification process. In the United Kingdom (UK), the CC philosophy has been adapted into a variety of pragmatic assurance techniques not just for single vendor solutions but for complete systems, sub-systems, network technologies, security architectures, and even managed service provision. How the general framework of CC can be adapted to provide assurance of security functions in software should be of interest to any person designing an assurance process for software security.

CC for IT security evaluation [1] and its forerunners have been successfully providing independent assurance of IT products since the 1980s. It has evolved as a framework for undertaking the formal independent evaluation of IT security products at either government or commercial evaluation facilities. The outcome of this process will be certification of an IT security product at a given Evaluation Assurance Level (EAL) as detailed in Table 1. The higher the EAL the more rigorous are the development and evaluation processes and the greater the confidence that the product can be trusted to perform the security functions the vendor claims, once successfully evaluated and certified.

By virtue of both the CC Recognition Agreement (CCRA) and the issue of CC as an International Standards Organization (ISO) standard (ISO 15408), CC certificates are recognized in many countries across the world.

A measure of global CC activity is demonstrated by the number of CC certificates issued. A quick check to date at <www.commoncriteriaportal.org> [2] reveals the certified product counts by category given in Table 2. *Protection Profiles* in this table refers to certificates issued to an abstract class of security functionality rather than an actual *Product Certificate*. Products are often themselves certified against a particular *Protection Profile*. One example of a class of security functionality would be role-based access control.

However, can CC be used as a framework for genesis of further assurance methods? From experiences in the UK, we believe this is the case; this is the main thesis of this article.

This article does not provide further detail on CC. For those unfamiliar with it and interested in further understanding, the full CC framework is published online at [2].

Why Is Independent Assurance So Important?

The need for IT product certification initially rose with a need for increased confidence and standardization in security products and operating systems deployed in the military domains. Safety and security requirements dictated that it was neither prudent to rely on manufacturer claims nor to allow a series of different proprietary approaches to develop functions that did not match the needs of the end user.

The natural response to this is to establish a framework of independent, functional specification and product verification. In this way those security functions can be validated as they are produced against a clear set of standardized requirements. Evaluators will verify and validate the design documents of the vendors, repeat tests using a defined sampling strategy (to ensure they produce the same results), attempt to expose flaws or vulnerabilities, and ensure the production process follows the prescribed practices and disciplines. This greatly increases the confidence in the finished product.

What Are Its Limitations?

The immediate fact to note from the

Table 1: *CC Evaluation Assurance Levels*

EAL 0	Inadequate assurance
EAL 1	Functionally tested
EAL 2	Structurally tested
EAL 3	Methodically tested and checked
EAL 4	Methodically designed, tested, and reviewed
EAL 5	Semi-formally designed and tested
EAL 6	Semi-formally verified, designed, and tested
EAL 7	Formally verified, designed, and tested

Table 2: *CC Certificates by Product Category*

Product Category	Product Certificates	Protection Profiles
Access control technology	15	1
Boundary protection technology	65	8
Data protection systems	23	0
Database systems	20	5
Digital signature technology	20	3
(Misuse) Detection technology	7	4
Integrated circuit and smartcard technology	136	22
(Cryptographic) Key management systems	18	1
Networking technology	37	5
Operating systems	49	5
Others	10	25
Total	400	79

count up of certified products given earlier (Table 2) is that most product categories are the direct components of security architectures (e.g. boundary protection), relatively few are generic IT products (e.g. operating systems and databases). This already signifies CC as a component and not a solution-focused method; a certified product is no use in isolation. Also, neither does CC meet the need for end to end assurance of network architectures and the overall assurance of business applications. Additional methods are needed to cover assurance of these solutions.

Another statistic to note is how the largest category by far (integrated circuits and smartcards, 34 percent of all certifications) are the most self-contained. These are ideal for testing from the comfort of a laboratory environment and are well defined for the rigor of CC. How do you assure a deployed solution comprising many products and which is infinitely more complex?

The main limitations of the classical CC approach can be summarized as the following:

- Practicality of evaluation reduces with complexity.
- Time, cost, and probability of an unsuccessful outcome increases with complexity and level of assurance required.
- It is impossible to define complex systems to the depth necessary to subject them to high assurance levels.
- It is difficult to apply to a collection of commercial off-the-shelf products due to the complexity introduced by combined permutation of configurations and competing proprietary interests (version 3.1 of CC now adds the concept of composition assurance profile to enable this form of evaluation).
- It is a product-focused credential; it cannot assure particular installations of that product outside of the laboratory environment or assure an overall service delivery that includes the product.
- The specialist nature of the products means it often is difficult for vendors to recover the cost of evaluation through volume; evaluated versions can have a high-cost premium.
- Government sectors know how to apply assured products by virtue of their security policies, but industry has no benchmark to apply them. In this environment, it is hard to build a business case for them.
- Complex evaluations take a long time; often, the certified version may be a product generation behind the latest version on the shelf once it becomes certified.
- Evaluated configurations are often limited in scope, not matching real-world implementations.
- Evaluation is not perfect; there will still be security patches.

Alternative Approaches

What other approaches are there to assure the security of delivered solutions? There are alternatives for providing confidence in software production processes, such as the Capability Maturity Model Integration (CMMI[®]) [4]. There are also holistic control-based approaches to information security that can be applied at the organization and business process level including ISO27001/ISO17799 [5,6] and Control Objectives for IT (COBIT) [7].

At the other extreme, there are both tools and experts available to provide vulnerability assessments and penetration tests of deployed solutions. The *tried and trusted* method is also still abundant in industry in which products are only incorporated after extensive proving within a customer environment.

Some product groups also have specialist watchdogs that provide constantly updated information on product quality. For instance, Virus Bulletin [8] provides a constantly updated profile of the performance of all anti-virus products on the market. ICSA labs [9] provides a subscription-based, broad ranging commercial product security list that was tested, and using their own proprietary method, West Coast Labs have established a proprietary independent product certification scheme (Check-Mark) [10].

However, none of the alternatives offers the depth and specificity of the CC process. The obvious approach is to customize the CC to the alternative needs to derive a range of information assurance (IA) techniques that are tailored to fit the specific assurance needs of each circumstance. CC especially lends itself to the production of derivative methods due to its modular nature and structured philosophy; it can be used as a toolbox to provide derivative assurance methods.

What's Happened in the UK

This is exactly what has happened in the UK: The Communications-Electronics Security Group (CESG) is the UK's national technical security authority. It has led initiatives to derive a selection of IA methodologies driven by customer demand (inevitably clients from the UK government sector). It is the main driving force behind all UK government technical security initiatives.

The remainder of this article is dedicated to this range of methods beyond the conventional CC evaluation process. These include the following:

- System level evaluations (SYS) [11].
- Fast-track assessments (FTA) [12].
- IT security health checks (CHECK) [13].
- CESG Assisted Products Scheme (CAPS) [14].
- Central Sponsor for Information Assurance (CSIA) Claims Tested Mark (CCTM) [15].

The SYS, FTA, and CHECK methods can augment laboratory based verification with assessment at the point of installation for a particular project. Also, the UK now has the CCTM scheme to test the manufacturer security claims of shrink wrapped products and services, using a single-pass, low-cost method; this proves suitable for assessing products and services which have so far eluded formal evaluation due to their polymorphic nature (including anti-virus software and content filters). It also moves away from open ended and unaffordable iterative approaches that risk never having a successful outcome to fixed assessment projects with known milestones, costs, and end products.

The Key Players

Apart from CESG, referred to above, the other UK organizations that play a key part in delivering IA requirements to the UK Government sector include the following:

- **Cabinet Office.** The Cabinet Office is the source of most political initiatives that drive UK public sector interest in information systems and IT. For instance, the UK has a requirement to provide all government services to the citizen online by the end of 2007. The Cabinet Office also owns UK government security policy.
- **CSIA.** CSIA is part of the Cabinet Office and takes a pan-civil government responsibility for accreditation of public sector information systems and IT. This remit extends from all central government departments through to local authorities and government agencies.
- **National Infrastructure Security Coordination Center (NISCC).** NISCC performs in the UK as part of the functions of homeland security. NISCC is part of the wider security services for ensuring the security and

[®] Capability Maturity Model and CMMI are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

availability of the critical national infrastructure. This extends beyond government to privatized utilities and critical services. NISCC also promulgates technical security advice and is also the central point for Unified Incident, Response and Alerting Scheme which is the UK government's Computer Emergency Response Team (CERT).
- **Ministry of Defense (MOD).** MOD is the largest UK consumer and investor in IA services and is, therefore, the key stakeholder. Naturally, they need to apply full rigor of formal processes to the assurance of systems and have helped to shape the methods in use today.
- **Department of Trade and Industry (DTI).** DTI has a role in advising industry on information security matters, especially for government contractors. It has been a key player in the past in promotion of adoption of standards in use by government to the commercial sector and in the standardization at both the national and international levels.
- **UK Accreditation Service (UKAS).** UKAS oversees all UK government sponsored certification services in the UK including the certificate or testing laboratories.

All of the above have had important roles in definition and practice of the standards and methods discussed in this article.

SYS

SYS is a clear CC derivative developed by CESG to meet MOD requirements for assurance of whole solutions. Typical MOD IT systems incorporate multiple products from multiple vendors and may extend from a system deployed in a single data center to an enterprise solution covering many sites.

Modeled along the assurance levels, the equivalent SYS2 to SYS4 levels provide a measure of equivalence to EAL2 to EAL4. It excludes those elements of CC that are specific to individual products and vendors and focuses on system level and end to end testing. It was formalized as a UK IT Security Evaluation Criteria (ITSEC) method in 2002.

It was the first method to reduce the iterative approach of CC and the pure *pass/fail* outcome to a more risk based approach in which the test report provides information on residual flaws and vulnerabilities; it is then for the system accreditor to accept the overall solution as is, to call for remedy in specific areas, or to build in compensating controls. This produces an approach that is more predictable in terms of project costs and timescales.

FTA

CESG, on realizing the benefits of the system-level approach and its broader applicability to all UK government projects then embarked on definition of a more generally usable *fast track* scheme that could be applied to specific products and for deployment of specific components. It was launched as a CESG IA service in 2001.

Here the emphasis is for an entirely predictable time to evaluate and for the cost to be known at the outset. Again the focus is on deployment of the product in a specific project environment, which can be a benefit over the more generalist approach of CC.

> "CC especially lends itself to the production of derivative methods due to its modular nature and structured philosophy; it can be used as a toolbox to provide derivative assurance methods."

It is designed to be at lower cost and therefore more within the budgets of the smaller government departments.

The output is an assessment report rather than a certified product; it is developed with the intention that it provides assurance that the product is fit for the purpose in the sponsor's desired deployment.

CHECK

The CHECK scheme is not strictly a derivative of CC. CHECK is another service from the CESG stable that has been operating since 1998. This scheme focuses on providing UK government trained *ethical* penetration testing personnel for undertaking penetration testing and vulnerability testing on deployed UK government networks and solutions. These test personnel undergo a stringent annual assault course examination at CESG to ensure their skills remain current. Companies that maintain the test personnel are given a green light status by CESG which allows them to tender for CHECK contracts.

The CHECK service is mandated for all UK government projects that involve the connection of sensitive UK government information systems to the Internet. An important recent development of this scheme (which originally focused on network testing) is a new application testing service that focuses on assessment of web enabled multi-tier applications and the vulnerabilities that can be exposed purely by the interaction of multiple software packages, how they are configured, and the presence of underlying bespoke application code.

CAPS

The CAPS scheme is the UK equivalent of the US Federal Information Processing Standard (FIPS)-140 encryption product evaluation standard. CAPS and FIPS-140 are formal means of evaluating cryptographic hardware and software products in a similar way to which CC evaluates IT products.

Cryptography is typically excluded from CC evaluations due to national sensitivities and import/export laws: cryptography is judged as having a *dual use* (military) application and therefore useful to rogue administrations.

UK government departments are required to protect UK classified information with CAPS approved products.

UK vendors of encryption technology enter into a partnership with CESG to engineer UK specific algorithms into their products. Once approved, these products become part of the UK catalogue of approved encryption products.

CSIA CCTM

CCTM is the latest scheme targeted with the widest possible applicability. This has been championed by the CSIA, with technical assistance of CESG. It is an entry-level assurance method; we have heard it described as *what EAL1 should have been*.

It is intended to be an affordable credential for all forms of security products and services. It is a single pass method that concentrates on validating vendor product functional security claims. The scheme was launched with pilot assessment in 2005 and is now fully in effect. Twelve security products and one service have so far been assessed under the scheme and awarded the mark. The single service assessed so far is the Messagelabs e-mail scanning service which exists between the UK government secure intranet and the Internet.

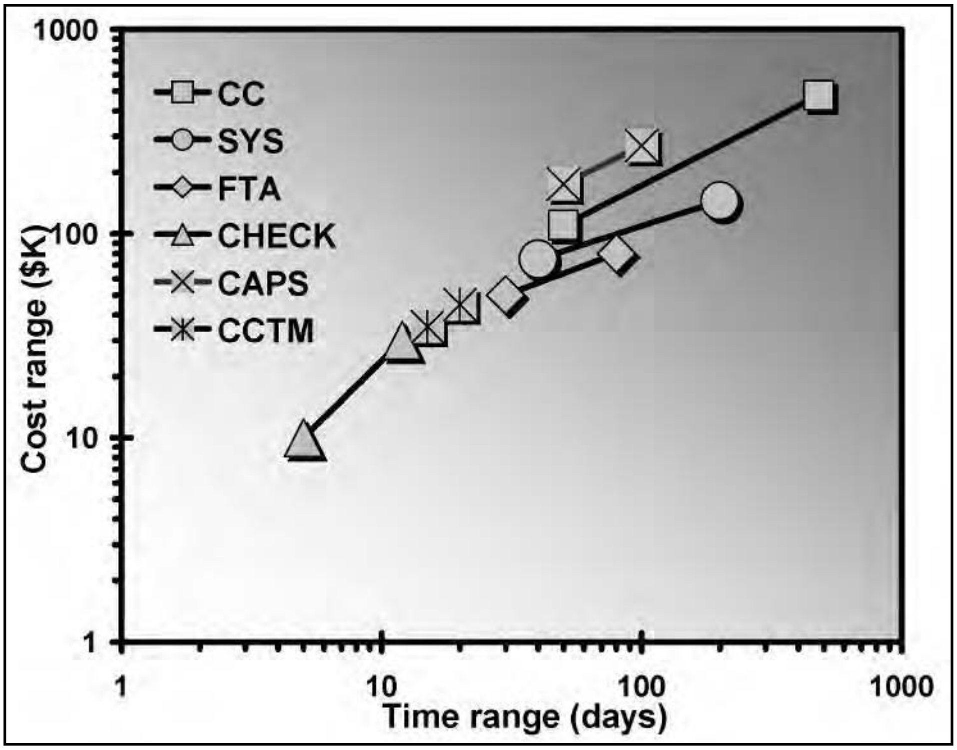

Figure 1: *Comparison of Assurance Method Ranges of Cost and Time*

The process is a simple single-pass process with limited functional testing that starts with a vendor provided IA Claims Document that specifies the security functionality of the product or service to be assessed.

Designed to be fast and at very low cost, it provides a baseline UK government approved badge. All new security products and services will need this as the minimum credential for inclusion in UK government procurement catalogues.

Table 3: *Information Assurance Method Requirements Fit*

Assurance Requirement	CC	SYS	FTA	CHECK	CAPS	CCTM
Certified product mark	✓				✓	✓
Mutual recognition	To EAL 4					
High assurance	✓				✓	
Medium assurance	✓	✓	✓		✓	
Low assurance				✓		✓
Pass/fail outcome	✓			✓	✓	✓
Risk enumeration		✓	✓	✓		
Flexible re-use	✓					✓
Project specific		✓	✓	✓		
Deployment specific		✓	✓	✓		
End to end		✓		✓		
Bespoke specific		✓	✓	✓		
Multi-product/vendor	In V 3.1	✓		✓		
Polymorphic products				✓		✓
Architecture/system		✓		✓		
Service delivery						✓
UK national requirements		✓	✓	✓	✓	
Deployment testing		✓		✓		
Open ended/iterative	✓				✓	
Time bounded		✓	✓	✓		✓
Low cost			✓			
Very low cost				✓		✓

Applicability of the Approaches

The coverage of the UK methodologies can be best illustrated by a comparison of the typical indicative minimum to maximum cost and time ranges for each of the derivative methods (SYS, FTA, CHECK, CAPS, and CCTM) displayed against the classical CC ranges. These are shown in Figure 1. Note that this diagram has logarithmic scales.

The cost ranges only relate to the evaluation and assurance processes themselves. The more rigorous methods impose necessary additional development costs on the vendor that are not shown and that also depend on the complexity of the component or system to be evaluated or assured.

So these practical considerations derived a set of IA approaches that are tailored to the demands of the UK consumers. This now provides a full spectrum of methods that can be applied to meet real-world assurance activities arising from information age projects in the UK.

Table 3 provides a summary of the characteristics and fit of these different methods according to the different project needs. This clearly demonstrates the need for a selection of methods to cover the full range of assurance requirements that are needed to address an increasingly diverse UK market.

How Can This Be Exploited Outside of the UK?

Alas, the methods outlined in this article are UK specific and are outside of the scope of CCRA. Plus, with the exception of CCTM, they are not focused on re-usable product certification but on assurance and accreditation requirements for specific UK projects (with there being some scope within the UK for re-use of accredited system designs and architectures). However, the methods of the CC derivatives are published in the public domain.

It is, of course, useful knowledge to international companies that wish to sell products and solutions to the UK government market.

However, the principal shown is that it is possible to derive efficient and successful assurance processes based on the CC model. CC can be used as a resource to build methodologies for enhancing the security in software engineering even if a product certificate is not the ultimate requirement. This can have universal application and can reap the same benefits experienced in the UK of timely deliveries, cost effective assurance regimes, and increased confidence in the security of the end product.

Looking Forward

It is possible to envisage further assurance methods that will be required, in the UK or elsewhere. The CHECK scheme extension into the testing of deployed applications demonstrates that there is a need to encompass all software in the overall assurance framework. Confidentiality, integrity and availability are increasingly protected not by isolated security products but by different aspects of the whole solution.

One emerging development is that CESG has commenced a project to rationalize the SYS and FTA methods into a *tailored assurance* framework that will allow specific programs of work to use CC derivative methods fitting to their exact need. This is a natural progression of the philosophy outlined in this article. Perhaps this is something that will be taken forward to future generations of CC and ISO 15408.

Conclusions

Is it right to compromise on the original design of CC? This article has demonstrated several derivative methods that reduce its complexity and that focus on risk management and acceleration of the development process. It is important to realize that CC is already a risk management method; evaluators do not repeat every vendor test, nor do they inspect every line of code. They adopt sampling approaches to assure the quality of the vendor product, just as in any risk based audit. It is also a benefit to be able to expand the use of elements the CC methodology from the limited boundaries of individual software, hardware, and firmware products to more open ended solutions and entire architectures.

We argue that the derivatives only extend the risk management concept to allow application of its principals in wider circumstances and to meet real-world business needs. We strongly believe in the founding concepts of CC and the importance of independent assurance of secure solutions. By recognizing the diversity of requirements and the flexibility of the framework to serve them, it will allow the CC method to meet its vision of universal recognition of this value in the years to come.◆

References

1. ISO/IEC 15408. “Evaluation Criteria for IT Security.” ISO 2005 <www.iso.org>
2. Common Criteria Portal <www.commoncriteriaportal.org>.
3. UK ITSEC. CESG/DTI 1990 <www.cesg.gov.uk>.
4. Carnegie Mellon University. Capability Maturity Model® Integration (CMMI®). CMU Software Engineering Institute <www.sei.cmu.edu/cmmi>.
5. ISO/IEC 27001:2005. Information Security Management Systems – Requirements <www. iso.org>.
6. ISO/IEC 17799:2005. Code of Practice for Information Security Management. 2005 <www.iso.org>.
7. IT Governance Institute/Information Systems Audit and Control Association. “The Control Objectives for Information and Related Technology.” (COBIT 4.0) 2006 <www. isaca.org>.
8. “Independent Malware Advice.” Virus Bulletin Ltd. 2006 <www.virusbtn.com>.
9. ICSA labs. Online portal <www.icsa.net>.
10. “Checkmark Certification and Product Testing.” West Coast Labs <www.westcoastlabs.org/checkmarkcertification.asp>.
11. UK ITSEC Scheme Certification Body. UK IT Security Evaluation and Certification Scheme – SYSn Assurance Packages Framework (Issue 1.0). 2002 <www.cesg.gov.uk>.
12. CESG. “Fast Track Assessment Service: Overview.” CESG. 2001 <www.cesg. gov.uk>.
13. CESG. “CHECK Service Provision Guidelines (Vers. 7.0).” 2002 <www.cesg.gov.uk/site/check/index.cfm>.
14. CESG. “Assisted Products Scheme.” <www.cesg.gov.uk>.
15. CSIA. “CSIA Claims Tested Mark Scheme - Description of the Scheme (Vers. 2.2.0).” CSIA <www.cabinetoffice.gov.uk/csia/documents/pdf/cctm/scheme_description.pdf>.

Note

[1] Echelon Consulting Ltd. (UK) is registered as a legal business entity in the UK and has no business connection with 2004-2006 Echelon Corporation of San Jose, CA.

About the Authors

Mike Ormerod is a qualified ISO15408 lead evaluator and consultant with 17 years evaluation experience and has been in the IT industry for 22 years. He has in depth knowledge in security evaluation and CCTM assessments. Ormerod has had a variety of customers in the UK government and private sectors, as well as overseas customers expanding to the far east. He is currently busy establishing the Echelon Test Facility, based in London, which is currently undergoing the UKAS certification process for Test Laboratory status.

Echelon Consulting Ltd.
Echelon House
93 Fleet RD
Fleet
Hampshire
GU51 3PJ
United Kingdom
Phone: +44(0)1252 627799
Fax: +44(0)1252 626509
E-mail: mike.ormerod@echelonltd.com

Kevin Sloan is a principal security consultant and the Echelon Consulting Ltd. (UK) Technical services manager. He has a background in electronics, microprocessor applications, firmware, software, and data communications, and specializes in information security. He has more than 26 years experience in the IT industry with information and communications security experience spanning over the last 18 years. Sloan is qualified by CESG to undertake IA activities for many UK government customers and has been a key player on several significant UK eGovernment projects. He has broad experience with commercial clients in the UK and overseas.

Echelon Consulting Ltd.
Echelon House
93 Fleet RD
Fleet
Hampshire
GU51 3PJ
United Kingdom
Phone: +44(0)1252 627799
Fax: +44(0)1252 626509
E-mail: kevin.sloan@echelonltd.com