WORKING PAPERS

EAST-WEST CENTER WORKING PAPERS

Economics Series

No. 108, January 2010

The Common Criteria for Information Technology Security Evaluation — Implications for China's Policy on Information Security Standards

Dieter Ernst and Sheri Martin

EAST-WEST CENTER
COLLABORATION • EXPERTISE • LEADERSHIP
SINCE 1960

The East-West Center promotes better relations and understanding among the people and nations of the United States, Asia, and the Pacific through cooperative study, research, and dialogue. Established by the U.S. Congress in 1960, the Center serves as a resource for information and analysis on critical issues of common concern, bringing people together to exchange views, build expertise, and develop policy options.

The Center's 21-acre Honolulu campus, adjacent to the University of Hawai'i at Mānoa, is located midway between Asia and the U.S. mainland and features research, residential, and international conference facilities. The Center's Washington, D.C., office focuses on preparing the United States for an era of growing Asia Pacific prominence.

The Center is an independent, public, nonprofit organization with funding from the U.S. government, and additional support provided by private agencies, individuals, foundations, corporations, and governments in the region.

East-West Center Working Papers are circulated for comment and to inform interested colleagues about work in progress at the Center.

For more information about the Center or to order publications, contact:

Publication Sales Office
East-West Center
1601 East-West Road
Honolulu, Hawai'i 96848-1601

Telephone: 808.944.7145
Facsimile: 808.944.7376
Email: EWCBooks@EastWestCenter.org
Website: EastWestCenter.org

EAST-WEST CENTER
COLLABORATION • EXPERTISE • LEADERSHIP
SINCE 1960

Economics Series

No. 108, January 2010

The Common Criteria for Information Technology Security Evaluation — Implications for China's Policy on Information Security Standards

Dieter Ernst and Sheri Martin

Dr. Dieter Ernst, senior fellow at the East-West Center, is an authority on global production networks and R&D internationalization in high-tech industries and on Asia's industrial and innovation policies, with a focus on standards and intellectual property rights. He was a senior advisor to the OECD, Paris; research director of the Berkeley Roundtable on the International Economy (BRIE) at the University of California at Berkeley; and professor of international business at the Copenhagen Business School. Recent books include *A New Geography of Knowledge in the Electronics Industry? Asia's Role in Global Innovation Networks* (2009), *Innovation Offshoring—Asia's Emerging Role in Global Innovation Networks* (2006), *International Production Networks in Asia. Rivalry or Riches?* (2000), *and Technological Capabilities and Export Success—Lessons from East Asia* (1998).

Sheri Martin was a 2008–2009 Next Generation Fellow at the National Bureau of Asian Research. Ms. Martin holds an MA in political science from the Johns Hopkins University, Nanjing University program. Prior to the Hopkins-Nanjing program, Ms. Martin studied Chinese language at Inter-University Program in Beijing. Her main research interests include media and public opinion in China.

This paper has been prepared as part of the East-West Center/ National Bureau of Asian Research project Standards and Innovation Policy in the Global Knowledge Economy—Core Issues for China and the US. A revised version will appear in Ernst, D, ed., forthcoming, *Governing Complexity—Standards and Innovation Policy in the Global Knowledge Economy*.

The Common Criteria for Information Technology Security Evaluation – Implications for China's Policy on Information Security Standards

by

Dieter Ernst and Sheri Martin

ErnstD@eastwestcenter.org

This paper has been prepared as part of the East-West Center/National Bureau of Asian Research project **Standards and Innovation Policy in the Global Knowledge Economy – Core Issues for China and the US.** A revised version will appear in Ernst, D, ed., forthcoming, *Governing Complexity –Standards and Innovation Policy in the Global Knowledge Economy*.

Information security – a highly contested field of China-US relations

As the recent dispute between Google and the Chinese government demonstrates, information security-related policy issues are rapidly becoming 'hot button' challenges for China-US relations. In the US media, much of the debate has focused on internet censorship. Equally important are economic impacts and implications for national security of a perceived increase in cyber attacks. In fact, both Chinese and US policy makers are searching for ways to improve the protection of information systems that are of strategic importance for economic growth and competitiveness, as well as national security. And the arsenal of cyber warfare keeps growing by the day.[1] In fact, there is reason to argue that cyber warfare has the potential to morph into a new form of technical trade barriers (TTBs) and hence should be appropriately discussed within the WTO (Ernst, 2009b).

A better understanding of the policy implications of information security-related conflicts requires research on the evolving policies and institutions that shape information security standards. This paper looks at an international cooperative attempt to develop a set of "Common Criteria for Information Technology Security Evaluation," explores its strengths and weaknesses, and examines implications for China's policy on information security standards.

The global landscape of the technology industry[2]

An information security ("infosec") standardization system seeks to provide assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and standard manner.[3] As China develops its national infosec standardization framework, it faces the task of finding the optimal balance between trade-offs of cost and assurance. China also faces the task of creating a framework within a global economy in which there is already a pre-existing hierarchy and international framework for standardization. Hence, it is useful to consider the global landscape of the technology industry and to study and learn from the strengths and weaknesses of existing international infosec policy models.

As globalization has extended beyond markets for finance and goods into markets for technology and knowledge workers, the organization and geographical mobility of knowledge has increased. Global corporations are at the forefront of these developments. Innovation

---

[1] Cyber espionage is one rapidly growing activity, not just in China but in all major economic powers. Many programs have backdoors placed by the programmer to allow them to gain access to troubleshoot or change the program. Some backdoors are placed by hackers once they gain access to allow themselves an easier way in next time or in case their original entrance is discovered. A *loophole* is a weakness or exception that allows a system, such as a HlawH or security, to be circumvented or otherwise avoided. Loopholes are searched for and used HstrategicallyH in a variety of circumstances, including HtaxesH, HelectionsH, HpoliticsH, the Hcriminal justiceH system, or in breaches of security. The *Trojan horse*, in the context of Hcomputing and softwareH, describes a class of computer threats (HmalwareH) that appears to perform a desirable function but in fact performs undisclosed malicious functions that allow unauthorized access to the host machine, giving them the ability to save their files on the user's computer or even watch the user's screen and control the computer. Trojan viruses can be easily and unwillingly downloaded.

[2] The following draws on Ernst, 2009a, and the author's studies cited in this report.

[3] Hhttp://en.wikipedia.org/wiki/Common_Criteria

management is undergoing profound changes, leading to increasingly vertical specialization or "fragmentation" of knowledge production. The fragmentation - dispersed engineering, product development, and research activities – are integrated across firm boundaries and geographic borders in Global Innovation Networks (GINs).

Although knowledge production has become collaborative across geographic borders, the new geography of knowledge is not a flatter world. There is clear evidence that the United States, Europe, and Japan retain their dominance in science and in high-impact IP, controlling the emerging new geography of knowledge. However, there is also substantial increase in the mobility of knowledge which gives rise to a dispersion of innovation hubs, including locations in China.

Ernst (2009a) demonstrates that integration of Asian emerging economies into diverse global corporate networks of production and innovation has provided these countries with new opportunities for industrial upgrading through innovation. That research also suggests that technology diversification, which combines incremental and architectural innovations, is within the reach of Asian emerging economies, such as China, and can serve as a complementary option to strategies aimed at achieving technology leadership.

The difficulty with solely pursuing technology leadership strategies is that attempts to compete head-on with global technology leaders necessitate a massive upgrading of absorptive capacity as well as innovative capabilities. In addition to requiring time, these strategies necessitate large financial investments, and are risky with uncertain market prospects. For these reasons, an exclusive focus on technology leadership strategies is unlikely to support a broad-based upgrading through innovation strategy.

A viable complementary strategy is *technology diversification* that focuses on the expansion of a company or product's technology base into a broader range of technology areas. The advantages to such an approach include lower cost and risk, and the generation of technology-related economies of scope by recombining component and process technologies. Diversification strategies capitalize on Asia's existing strengths in process development, prototyping, and electronic design, integrated solutions capabilities, and can build on Asia's accumulated capabilities to implement, assimilate, and improve foreign technologies. Focusing on these architectural innovations, Asian firms can extract greater benefits from deeper forms of integration into global innovation networks.

Pursuing technological diversification as a complementary option to technological leadership strategies has important implications for China's national standardization framework. A framework that allows for China's technology industry to pursue technology diversification would encourage network integration, avoid disrupting GINs, and be compatible with existing international standards, such as Common Criteria.

Common Criteria

A widely used approach is the **Common Criteria for Information Technology Security Evaluation** (abbreviated as **Common Criteria** or **CC**), an international standard (ISO/IEC 15408) for computer security certification. Its defining characteristics are a focused, flexible, and consensual approach to standardization. This note provides an assessment of important strengths and weaknesses of this approach, and highlights possible implications for China.

The Common Criteria originated out of collaboration between the governments of Canada, France, Germany, the Netherlands, UK, and the US. These six governments unified three previous standards, the European (ITSEC)[4], Canadian (CTCPEC)[5] and US (TCSEC)[6], in order to facilitate buying and selling computer products internationally for government markets using a single evaluation system.

Currently in version 3.1, the Common Criteria is a framework in which computer system users can *specify* their security requirements, vendors can then *implement* and/or make claims about the security attributes of their products, and testing laboratories can *evaluate* the products to determine if they actually meet the claims. In other words, the Common Criteria seek to provide assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and standard manner.

The Common Criteria address an important governance challenge of the emerging global knowledge economy – how to protect global information flows and knowledge exchange against unauthorized access and security threats. National policies, however well-intentioned, were unable to provide cost-effective solutions. In fact, before CC came into existence, vendors had to evaluate the exact same product in multiple countries, which was costly and time-consuming.

---

[4] The **Information Technology Security Evaluation Criteria** (**ITSEC**) is a structured set of criteria for evaluating computer security within products and systems. The ITSEC was first published in May 1990 in HFranceH, HGermanyH, the HNetherlandsH, and the HUnited KingdomH based on existing work in their respective countries. Following extensive international review, Version 1.2 was subsequently published in June 1991 by the HCommission of the European CommunitiesH for operational use within evaluation and certification schemes. Since the launch of the ITSEC in 1990, a number of other European countries have agreed to recognize the validity of ITSEC evaluations. The ITSEC has been largely replaced by HCommon CriteriaH, which provides similarly defined evaluation levels and implements the target of evaluation concept and the Security Target document.

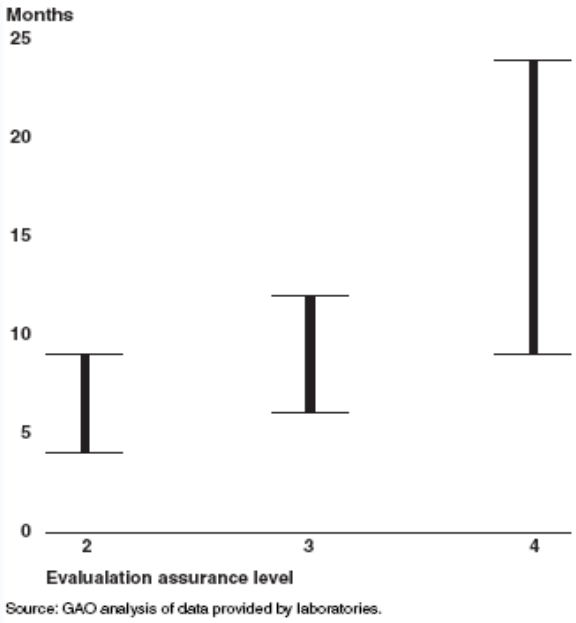
[5] **CTCPEC** is the **Canadian Trusted Computer Product Evaluation Criteria**. It is a Hcomputer securityH standard published in 1993 by the HCommunications Security EstablishmentH to provide an evaluation criteria on IT products. It is a combination of the HTCSECH (also called *Orange Book*) and the European HITSECH approaches. CTCPEC, ITSEC and TCSEC have been large superseded by the HCommon CriteriaH standard.

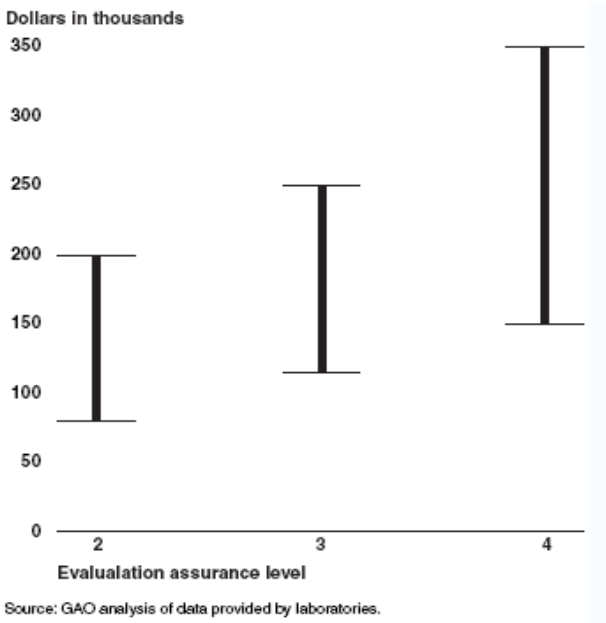
[6] **Trusted Computer System Evaluation Criteria** (**TCSEC**) is a HUnited StatesH HGovernmentH HDepartment of DefenseH (DoD) standard that sets basic requirements for assessing the effectiveness of Hcomputer securityH controls built into a Hcomputer systemH. The TCSEC was used to evaluate, classify and select computer systems being considered for the processing, storage and retrieval of sensitive or Hclassified informationH.The TCSEC, frequently referred to as the **Orange Book**, is the centerpiece of the DoD H*Rainbow SeriesH* publications. Initially issued by the HNational Computer Security CenterH (NCSC) an arm of the HNational Security AgencyH in 1983 and then updated in 1985, TCSEC was replaced with the development of the HCommon CriteriaH international standard originally published in 2005.

With CC in place, a single evaluation is now recognized by 26 member countries, which amounts to improved cost and time efficiency for vendors.

Multiple trade-offs

While the CC plays an important role in creating an international standard for information security evaluation, there are many valid criticisms of the scheme such as problems of validity and efficacy. For instance, the validity of assurance that the CC can provide is constrained by financial and temporal considerations. According to available information, vendors in the mid to late nineties reported spending US$1 million and even US$2.5 million on evaluations comparable to EAL4.[7] As we can see from the following chart, time and financial costs both positively correlate to evaluation level:





Clearly, there are trade-offs between assurance level and costs. To further convolute the topic, there are multiple trade-offs as well between attempts to promote the development of national industries, attempts to promote harmonization if not uniformity in standards, and attempts to reconcile cost of implementation and validity.

The challenge for policy-makers is that these trade-offs are systemic - an improvement in one dimension may well lead to a worsening in another dimension. Hence, attempts to solve these trade-offs in information security regulation will not be easy. This implies that for

[7] Wikipedia: EAL (Evaluation Assurance Level). Accessed Mar. 13, 2009: Hhttp://en.wikipedia.org/wiki/Evaluation_Assurance_Level

latecomers to infosec standards and certification policies, it may well be advisable to start with incremental changes in the administration of existing international standards and regulations, in order to find out what works and what doesn't. This trial-and error approach may be a necessary prerequisite for developing robust alternative national policy frameworks.[8]

There is, after all, no such thing as a perfect, fool-proof model for information security standards and certification policies. The key in future standards development in the People's Republic of China will be to strike a healthy balance between an acceptable level of validity in infosec evaluation and its costs - financial, temporal, as well as more indirect costs associated with possible unintended negative side effects, especially on innovation.

A focused approach

The Common Criteria evaluation and validation scheme is more focused than its TSCEC, ITSEC, and CTCPEC predecessors for the simple fact that the international Common Criteria Recognition Agreement (CCRA) eliminates duplicate evaluations of IT products and protection profiles. This saves vendors and users time and resources. The Common Criteria scheme also streamlines the evaluation process by reducing the government's role and shifting the onus of infosec onto the private sector. By doing so, the CC scheme capitalizes on vendors' collective interest in creating a successful certification scheme.

Although there are criticisms that the CC is cumbersome, and time and cost intensive, it is considerably less cumbersome and time intensive than China's MLPS framework. In terms of scope, the regulatory framework for China's MLPS (Multi-Level Protection Scheme) extends well beyond sensitive military and government agencies to cover all non-government end users. Strategic information systems include those that handle

"state affairs (party and government), finance, banking, tax administration, customs, audit administration, industry and commerce, social services, energy, transportation, national defense industry, and other information systems that are related to the national economy and people's livelihood including education, state science and technology institutions, public telecommunications, television broadcasting and other basic information networks."[9]

Added scope and participating agencies create a more bureaucratic and thus slower process. That means new products have a much longer process to go through so new innovations needing certification will be slower to enter the market. A national infosec system, with its own evaluation and certification process means that companies that have potential markets in China and CC member countries must double-up on evaluation. This leads to added cost for two processes, and an added difficulty of designing products that incorporate the demands of both standard systems. This is a financial disincentive for Chinese companies to market to CC member countries as well as vice-versa.

[8] This is in line with the suggestion by Peter Drahos (2007: 410) who argues that it is more realistic to focus on incremental changes in the administration of regulations rather than on attempts to revamp governance architectures.
[9] Ernst, 2009b, quoting MLPS (Multi-Level Protection Scheme)

Although China may be able to successfully monopolize China's domestic market through micromanagement of corporate information security networks, the strict multi-level security requirements and dictation of the organization and implementation of the infosec management structure will have a disruptive effect on management and coordination of global networks of production and innovation.

Flexibility

The Common Criteria is flexible because of its generic nature; it does not directly provide a list of product security requirements or features for specific classes of products. This follows the approach taken by Europe, but has been a source of debate to those accustomed to the more prescriptive approach of other earlier standards such as those proscribed by the US Department of Defense. Less specificity lowers costs and lowers the vendor's burden, but the trade-off is lower validity in the assurance process.

CC is also flexible in the sense that it certifies seven levels of security assurance. This convention avoids an all-or-nothing benchmark allowing vendors to improve their assurance gradually over time.[10]

One criticism of the 7-tiered system is that in the lower levels (EAL 1 through 4), CC only evaluates paperwork, and it fails to evaluate the actual computer system. A recent listing of 186 products validated under CC showed a spread between assurance levels with a majority of products falling within EAL levels 1 through 4.[11]

If this is representative, the vast majority of products undergo only a paper-based evaluation, which does not account for environmental factors. However, once again this is a case of trade-offs; critics of CC already have noted the exorbitant cost of the evaluation process. The process would certainly be more expensive if all evaluations required verifying code.

China's MLPS (Multi-Level Protection Scheme), in contrast, has much more rigorous classification levels MLPS distinguishes five levels of information systems (Ernst, 2009b). Most industries are classified as level 3 and above systems. They must meet the very demanding security requirements of the US Department of defense TSEC or "Orange Book" standard. CASS S&T backbone networks are also recommended to be classified as level 3. However, China's infosec product market is still at an early stage of development, and product performance levels

[10] According to Mary Ann Davidson Chief Security Officer at Oracle and co-chair of the Technical Standards and Common Criteria Task Force. Her personal email is unpublished, but Oracle's media relations contact email is: HOracle-Press_ww@oracle.comH. Davidson often gives interviews and has some publications. More information can be found on her on Wikipedia: Hhttp://en.wikipedia.org/wiki/Mary_Ann_Davidson

[11] Jackson, William. "Under Attack: Common Criteria has Loads of Critics, But is it Getting a Bum Rap?" *Government Computer News* Aug. 10, 2007. Accessed Mar. 12, 2009. Hhttp://gcn.com/articles/2007/08/10/under-attack.aspx

do not match that of leading global competitors. According to Chinese experts, the majority of China's infosec products can only meet level 2 classification requirements.

In addition to the more demanding security requirements, China's MLPS stipulates (Ernst, 2009b):

- The infosec products must be developed and manufactured by companies that are "invested or owned by Chinese citizens or legal persons, or the state."
- The core technology and key components of those infosec products must have "independent Chinese" or "indigenous" intellectual property rights. For all practical reasons, this prevents the usage of foreign infosec products for systems classified at level 3 and above. In other words, incumbent global market leaders in the infosec market will face significant entry barriers to the China market for critical information infrastructure.
- To add yet another level of complexity, systems operators must follow detailed guidelines for product procurement.
- Without a mandatory "CCC Mark" certification, a wide range of IT products will not be allowed to be shipped out of the factory, sold, or imported
- Encryption testing requires the sharing of source code encryption keys
- All products must comply to Chinese national standards
- Chinese labs must carry out complicated encryption testing and equally complicated post-market factory inspections.
- Adding even further to complexity, a level 3 system is required to procure a level 3 infosec product, etc. Chinas-based exporters thus would need to meet extreme and stringent product requirements that are unnecessary for commercial success.

These stipulations would require significant financial resources to implement the policy correctly. By adding further to an increase in the China price, this will have negative consequences for the competitiveness of all China-based exporting companies, irrespective of whether these are global or local companies (Ernst, 2009b)

Consensus through dialogue

The Common Criteria scheme intends to engage many communities, including IT product developers, product vendors, value-added resellers, systems integrators, IT security researchers, acquisition/procurement authorities, consumers of IT products, auditors, and accreditors.[12] The Common Criteria scheme differs from its predecessors in that it is based on the idea that dialogue and cooperation between government and industry is paramount to the success of the scheme and the realization of its objectives.

The Common Criteria scheme seeks to engage these communities via three forums and organizations. Common Criteria Users' Forum (CCUF), which includes customers, vendors, Common Criteria evaluators, in principle, provides an opportunity for stakeholders to express

[12] According to the United States Department of Defense 's Common Criteria Evaluation and Validation Scheme website. Retrieved 3-24-09 from: Hhttp://www.niap-ccevs.org/cc-scheme/ccevs-objectives.cfm

their perspectives and reconcile problems. Its impact however seems be limited, as CCUF apparently has met only once on October 6-7, 2004. The National Information Assurance Partnership (NIAP) program,[13] jointly established by the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA), is designed as a partnership between the public and private sectors.

A third way in which the Common Criteria scheme seeks to engage industry is through the Vendors' Forum (CCVF). Oracle's Davidson describes the importance of the CC and vendors' mutual support: "The value of assurance is the extent to which a vendor embraces it across its development processes. That said, since every vendor of [information technology] products claims, 'Our product is secure: trust us!' having a third party validate the product against the Common Criteria is tremendously valuable to customers, who otherwise would have to rely on unproven security claims. Also, many vendors, including Oracle, view the Common Criteria as the starting point for assurance, not the ending point."[14]

Although a successful evaluation process necessitates engaging industry, a by-product of opacity in the process arising from an attempt to appease industry, is undermined validity. To be more specific, the CC doesn't require proprietary software companies to divulge code for the evaluation process. This acts to protect the industry's intellectual property, but reduces the validity of the evaluation process since the evaluation cannot be verified.

According to Johns Hopkins researcher Jonathan Shapiro, opacity in the evaluation process also gives rise to the incidence of vendors negotiating with evaluators and moving to a second evaluator when the first doesn't give them what they want.[15] Shapiro believes that the Common Criteria labs are not as independent and accountable as they could be. He says that companies are playing the labs off each other for favorable treatment.[16]

---

[13] According to Hhttp://www.niap-ccevs.org/cc-scheme/aboutus.cfmH:
An important objective of NIAP is to help consumers select commercial off-the-shelf information technology (IT) products that meet their security requirements and to help manufacturers of those products gain acceptance in the global marketplace. The NIAP program's main objectives are:

- To meet the needs of government and industry for cost-effective evaluation of IT products;
- To encourage the formation of commercial security testing laboratories and the development of a private sector security testing industry;
- To ensure that security evaluations of IT products are performed to consistent standards;
- To improve the availability of evaluated IT products

[14] Jackson, William "Mary Ann Davidson: in Defense of Common Criteria," *Government Computer News*, Oct. 7, 2007. Accessed Mar. 10, 2009: Hhttp://gcn.com/Articles/2007/10/07/Mary-Ann-Davidson--In-defense-of-common-criteria.aspx?Page=1

[15] Johns Hopkins researcher Jonathan Shapiro as cited in "Under Attack: Common Criteria has Loads of Critics, but is it Getting a Bum Rap?"

[16] Criteria for a Lab to Certify Software" Public Wiki, retrieved 3-24-09 from:
Hhttp://abstract.cs.washington.edu/wiki/index.php/Criteria_for_a_Lab_to_Certify_Software

Oracle Corporation Chief Security Officer and Common Criteria proponent, Mary Ann Davidson acknowledges that vendors "shop" for labs. However, she counters that vendors shop based on expertise and cost. "A lab doing substandard work would face scrutiny by the national scheme."[17] However, if vendors are playing labs in different countries off one another, it seems that scrutiny by a national scheme would be insufficient to keep the practice of shopping in check.

Although imperfect and up for debate, the degree of opacity that vendor's retain with CC is important for industry well-being. In contrast to the CC's consensual approach, MLPS is much less collaborative; the government retains absolute authority through direct management and broad definitions of its domain (Ernst, 2009b):

- All systems above level 3 are directly managed by government regulatory authorities.
- "National security" is broadly defined to include "national competitiveness and the strength of the economy, science and technology".
- "Social order" includes the "stability of any type of economic activity" as well as "the research, development and production of any industry".

The enforcement of encryption requirements in MLPS is another area in which government involvement trumps industry (Ernst, 2009b). The agency in charge of enforcing encryption standards:

- uses manuals that are not publicly available
- can carry out unannounced cryptographic inspections on any system level
- has the full right to exercise complete control over any cryptographic technology used in MLPS systems
- can access key management and other cryptographic protocols
- has complete authority to subject violators of cryptographic regulations to administrative punishment
- requires, through OSCCA (SEMC's commercial encryption office) that a significant portion of cryptographic source code must be handed over[18]

Increased government involvement and control potentially has two negative consequences for China. One, it suppresses the collaborative role of domestic vendors in the infosec evaluation process, Two, it may be disruptive to global innovation networks, making it more difficult for China to collaborate with foreign companies, hurting China's "absorptive capacity."[19]

---

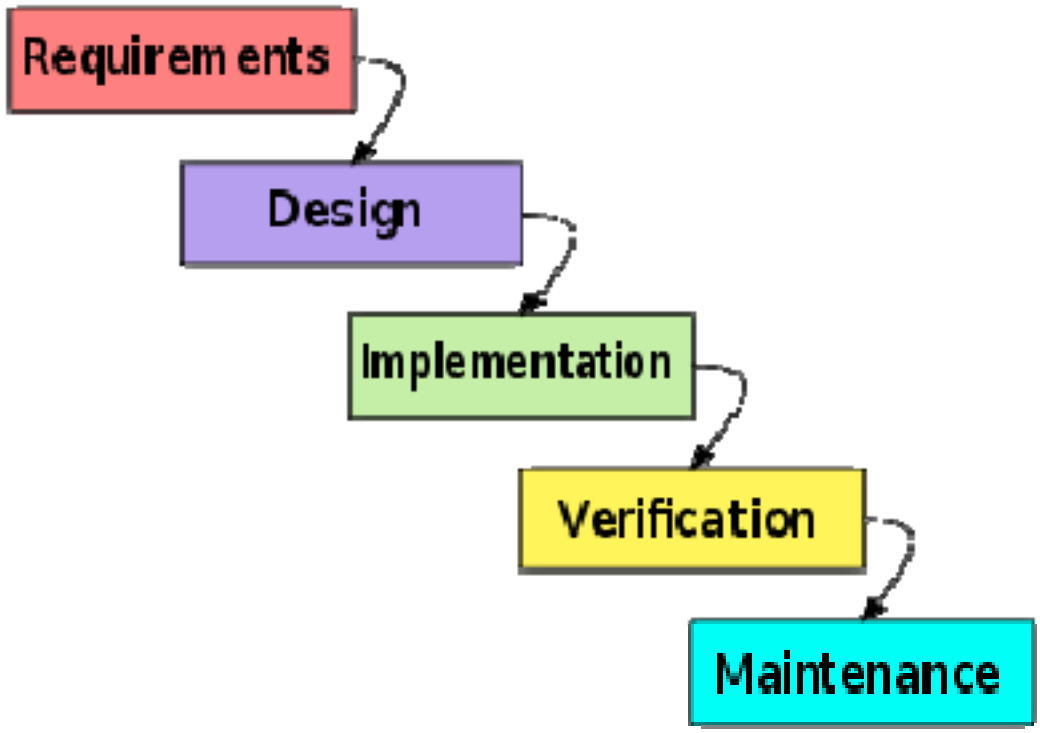
[17] Jackson, William "Mary Ann Davidson: In defense of common criteria," *Government Computer News*, Oct. 7, 2007. Accessed Mar. 24, 2009: Hhttp://gcn.com/Articles/2007/10/07/Mary-Ann-Davidson--In-defense-of-common-criteria.aspx?Page=1

[18] Dieter Ernst, MLPS paper, p 4.

[19] Accessed on Oct. 3, 2009 from Wikipedia: a firm's ability to value, assimilate, and apply new HknowledgeH.

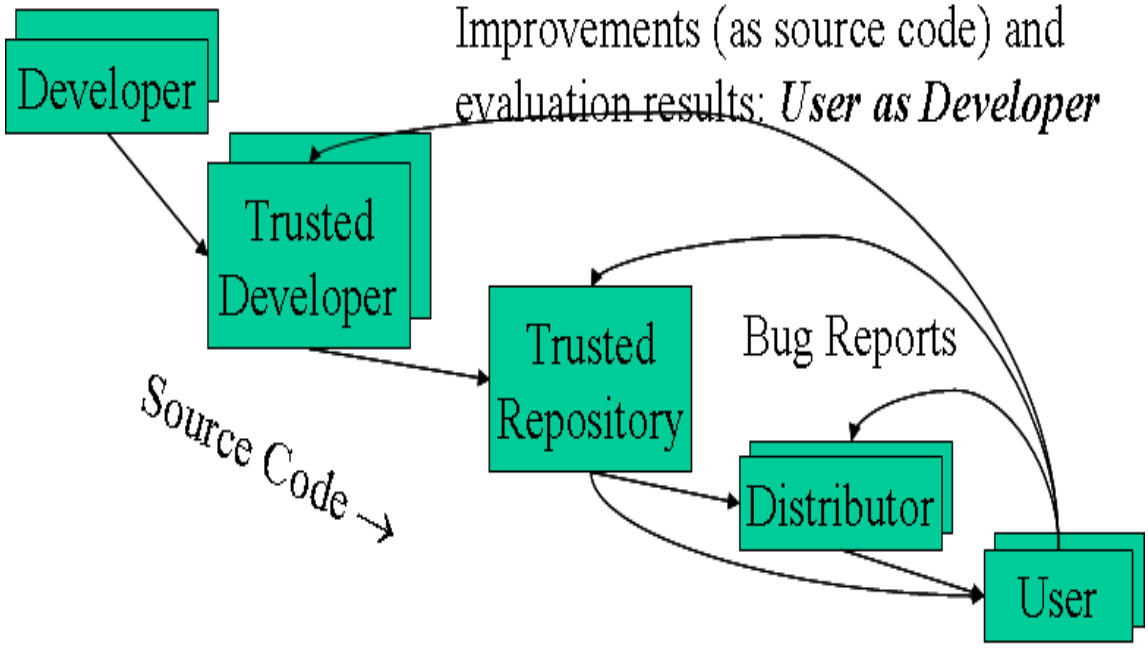
One by-product of industry's large role in shaping the process is that the CC evaluation scheme favors proprietary industry over FLOSS (free-libre open source software). According to Saltzer & Schroeder's (1974-5) *open design principle* regarding security, the protection mechanism must not depend on attacker ignorance. FLOSS better fulfills this principle than proprietary software, and so, as many security experts believe, FLOSS has a security advantage over proprietary software.[20] Despite scholarly consensus that FLOSS has a security advantage, Common Criteria assurance requirements reflect the traditional waterfall software development model (see Diagram A). Because FLOSS is usually produced using modern agile paradigms (see Diagram B), it is incompatible with the Common Criteria evaluation process.

Diagram A:



[20] Wheeler, David. "Free-Libre / Open Source Software (FLOSS) and Software Assurance," PPT presentation. *Towards a Transparent Acquisition Marketplace for Increased Mission Agility with Open Technology Development Conference, December 12, 2006 at the National Science Foundation (NSF) in Rosslyn, VA.* Hhttp://www.dwheeler.com/essays/oss_software_assurance.pdfH, p 12.

Diagram B:


Developer
Improvements (as source code) and
evaluation results: *User as Developer*
Trusted
Developer
Trusted
Repository
Bug Reports
Source Code
Distributor
User

At this point, it is difficult for Common Criteria to accommodate FLOSS because the scheme has a certain level of ossification. As a relative newcomer to infosec security, it should be easier for China to create a system that can better accommodate agile paradigms. As China develops its infosec evaluation process, it would make sense to take into account whether or not China wants to promote Open Source Software development in China. If the decision is reached that China wants to promote or allow for the potential development and proliferation of OSS, it would want to take into account the differences in the waterfall and agile paradigms when developing the evaluating system.

Conclusions

In conclusion, the focused, flexible, consensual approach that CC aims for are some of the evaluation processes' greatest strengths. The relatively narrow focus (or scope) increases manageability and efficiency. CC's flexible, tiered-system that allows companies to not divulge code at the lower EAL encourages industry innovation and lowers costs (in comparison to completing evaluations for each market country or in comparison to China's national infosec evaluation framework), which reflects a consensual approach to the evaluation process. One of CC greatest weaknesses is its incompatibility with FLOSS. The other major weaknesses are inversely related issues of time, cost, and validity, so an improvement in validity will likely lead to increases in time and/or cost.

As China develops a national framework for infosec standardization, it is important to examine how China's infosec framework will cohabitate with the international standardization framework, Common Criteria. There is no doubt that China will seek to use this framework to foster the development of its domestic industry. But in light of China's deep integration into global networks of production and innovation, it would make sense if China's infosec framework would be synchronized with a policy to shape the development of the international Common Criteria framework.

There are some encouraging developments. Leading multinational corporations from the US, the EU and Japan are now promoting China's participation in the Common Criteria Recognition Agreement (CCRA). They suggest helping China to establish the necessary high-quality infrastructure that Chinese certificates will be accepted worldwide[21].

This has led the Chinese government to announce in early 2009 that it has initiated a study of the CCRA. No draft of this study is yet available in the public domain. But informed observers are cautiously optimistic that, once the dust is settled that was stirred up by the current Google conflict, there are strong economic reasons for a more cooperative approach to the development of common and widely shared infosec evaluation criteria and standards.

[21] This is a positive development, as it signals that global industry leaders have accepted that their initial policy of passive obstruction has led the Chinese side to be even more convinced of the necessity of establishing a strong national infosec framework.

References

CCEVS website (Common Criteria Evaluation and Validation Scheme): http://www.niap-ccevs.org/cc-scheme/

Drahos, Peter. "Patent Reform for Innovation and Risk Management: A Separation of Powers Approach." *Knowledge Economy Studies*, vol. 1 (2007)

Ernst, Dieter (2009a). *A New Geography of Knowledge in the Electronics Industry? Asia's Role in Global Innovation Networks*, East West Center, Policy Studies, No 54: http://www.EastWestCenter.org/pubs/3242

Ernst, Dieter (2009b). *China's National Information Assurance Policy Framework – Objectives, Players, Impacts, and Solutions.* Mansucript, East West Center.

Farr, J. Aaron. "Open Source in China," PPT presentation. *2008 OSCON (Open Source Convention) Conference* held in Portland, OR: http://assets.en.oreilly.com/1/event/12/Open%20Source%20in%20China%20Presentation%201.pdf

Jackson, William "Mary Ann Davidson: in Defense of Common Criteria," *Government Computer News*, Oct. 7, 2007. Accessed Mar. 24, 2009: http://gcn.com/Articles/2007/10/07/Mary-Ann-Davidson--In-defense-of-common-criteria.aspx?Page=1

Jackson, William. "Under Attack: Common Criteria has Loads of Critics, But is it Getting a Bum Rap?" *Government Computer News*, Aug. 10, 2007. Accessed Mar. 12, 2009: http://gcn.com/articles/2007/08/10/under-attack.aspx

Wikipedia: "Common Criteria." Accessed Mar. 10, 2009: http://en.wikipedia.org/wiki/Common_Criteria

Wikipedia: EAL (Evaluation Assurance Level). Accessed Mar. 13, 2009: http://en.wikipedia.org/wiki/Evaluation_Assurance_Level

Wheeler, David. "Free-Libre / Open Source Software (FLOSS) and Software Assurance," PPT presentation. *Towards a Transparent Acquisition Marketplace for Increased Mission Agility with Open Technology Development Conference, December 12, 2006 at the National Science Foundation (NSF) in Rosslyn, VA.* http://www.dwheeler.com/essays/oss_software_assurance.pdf