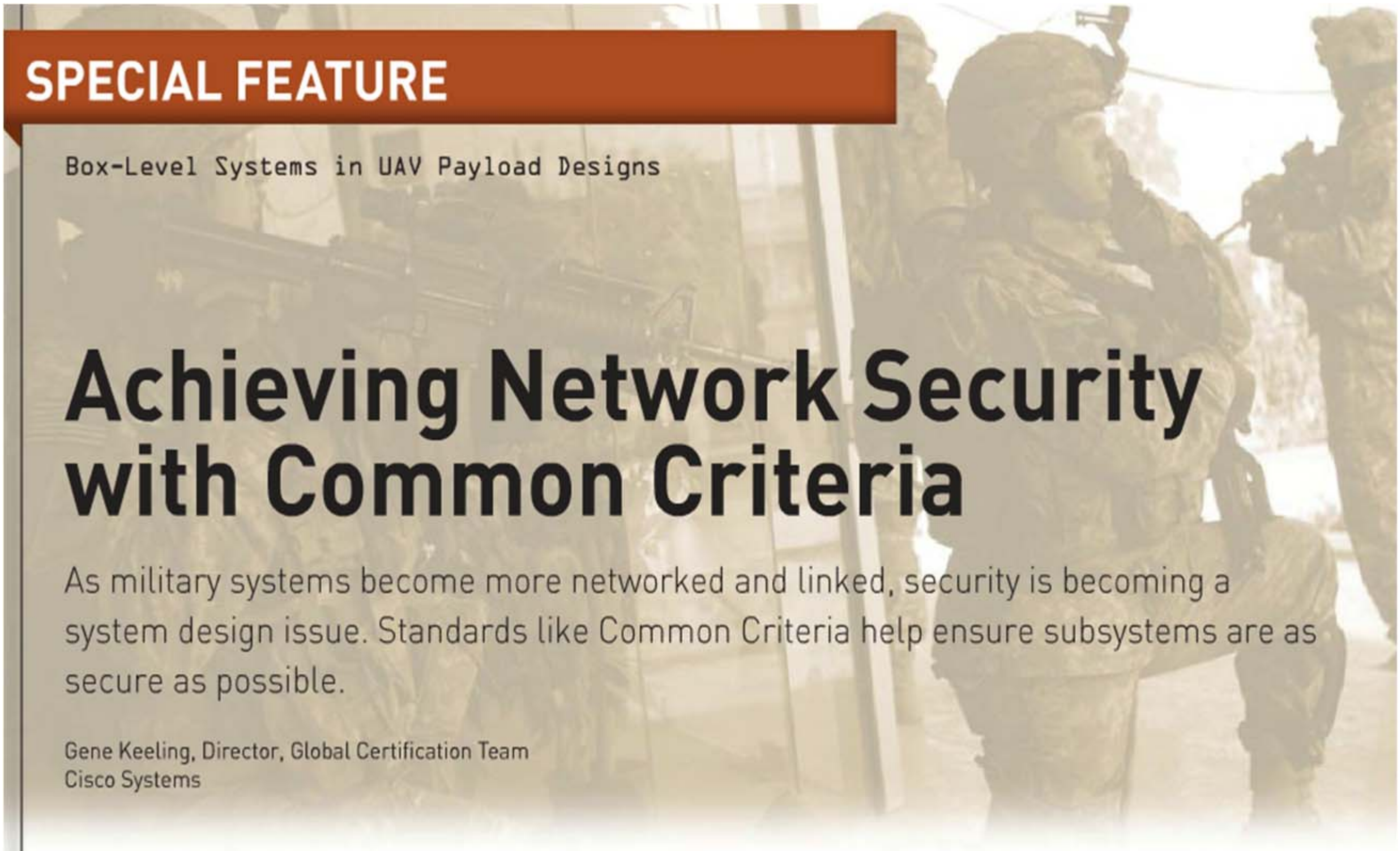

Achieving Network Security with Common Criteria

As military systems become more networked and linked, security is becoming a system design issue. Standards like Common Criteria help ensure subsystems are as secure as possible.

Gene Keeling, Director, Global Certification Team
Cisco Systems

Today's government and industry leaders overwhelmingly identify cyber security and information assurance as one of their top computing and networking concerns. Cyber threats are presented by both individuals and nation-sponsored groups with motivations spanning espionage, "hacktivism" (the disruption or invasion of systems for activist purposes), and the stealing of trade secrets. New issues are also arising around the security of the supply chain, with counterfeit and tampering incidents eroding user confidence. Organizations that suffer such attacks may lose control of confidential information, face millions of dollars in fines or business losses, and become a weak link in the national critical infrastructure.

What Common Criteria Standard Does	
√	Improves availability of evaluated, security-enhanced computing products
√	Contributes to higher levels of citizen confidence in network security
√	Improves the efficiency and cost-effectiveness of the evaluation and certification process
√	Allows vendors to focus their resources on a common set of requirements to improve the security of products overall
√	Increases the breadth of certified products and technologies available to IT administrators

Figure 1

Common Criteria is critical to ensuring that organizations get the equipment they need and that it is as secure as claimed. Endorsement of this uniform set of global IT security standards has several benefits as shown here.

Achieving a secure infrastructure is even more complex with today's mobility, collaboration and cloud services added to the mix. These new capabilities offer many operational efficiencies and reduce costs, but they also introduce additional risk to the network. In response, nations are increasingly cooperating to evolve a global standard to assure a base level of security for networking products. Known as the Common Criteria, this international program is critical to ensuring that organizations get the equipment they need, the equipment performs as advertised, and it is as secure as claimed. Endorsement of this uniform set of global IT security standards has several benefits as listed in Figure 1.

Defining the Standard

The Common Criteria for Information Technology Security Evaluation is an international standard (ISO/IEC 15408) that provides a framework within which participating organizations can specify functional and assurance requirements, vendors can implement and make claims about product attributes, and testing laboratories can evaluate products to determine whether they meet those claims. Common Criteria assures that the process of specification, implementation and evaluation of a product has been conducted in a rigorous and standardized manner.

Under the Common Criteria, classes of products are evaluated against the security functional and assurance requirements of Protection Profiles (PPs). All test labs must be in compliance with ISO 17025, the standard used to measure the competence of

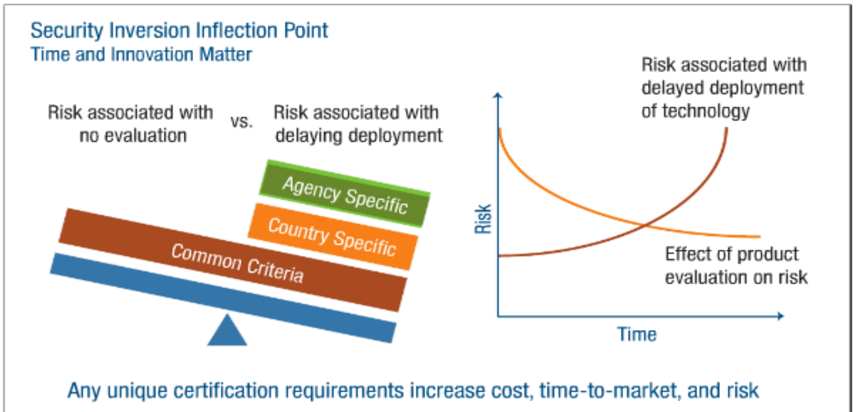
Security Inversion Inflection Point
Time and Innovation Matter
Risk associated with no evaluation
vs.
Risk associated with delaying deployment
Agency Specific
Country Specific
Common Criteria
Risk
Risk associated with delayed deployment of technology
Effect of product evaluation on risk
Time
Any unique certification requirements increase cost, time-to-market, and risk

Figure 2

Product security has to evolve to support new technologies. By relying on security standards, requirements can be rapidly developed to challenges as they occur.

testing and calibration laboratories. Such a process allows organizations to feel more confident in the security of critical information, and allows them to reduce risk within the network without increasing costs.

Currently, 26 nations participate in the Common Criteria program. Evaluation and testing is performed by independent third-party labs, with certificates of compliance issued by 15 certificate-issuing nations. So far, more than 2,000 certifications have been issued for IT products.

Worldwide Community

Through Common Criteria, participating nations gain access to a worldwide community of technical experts who can identify and address threats as a group, rather than each nation attempting to deal with each problem on its own. Solutions to threat vectors become scalable and repeatable, reducing the overall threat and cost at the same time. A few nations are still trying to pursue custom security standards, but this only limits the amount of technology available to them while diminishing the quality of goods. With finite resources for both vendors and consumers, it makes every kind of sense to use a mutually recognized standards-based approach to security certification.

Some governments are still learning how to manage the adoption process to keep costs down and timelines to meet the high-speed adaptations of cyber attackers. National agencies are also by nature wary of sharing too much information with otherwise trusted business and technology partners. However, overriding need has continued to drive the Common Criteria program forward, and indeed is leading to discussions on how to extend its effectiveness. By creating a faster, more effective, and more repeatable evaluation process, a new and broader set of evaluated products can be developed to address new and emerging threats.

Beyond the Public Sector

Note that the benefits of Common Criteria are not limited to government customers. The Common Criteria certification provides a level of quality assurance for any technology procurement team, giving those professionals a consistent, stringent and independently verified set of evaluation requirements for their IT investment. Although Common Criteria certification does not ensure that a product is absolutely free of security vulnerabilities, it does provide a higher level of objective assurance that the product performs as documented, and that the vendor will support the product to remediate flaws when and if they are discovered.

The Common Criteria program also provides purchasing organizations with a wealth of information that helps to enable higher security in their deployment of evaluated products. First, technology decision makers can compare their requirements against the Common Criteria's consistent standards to determine the level of security they require. They can also more easily determine whether particular products meet their security requirements. And finally, they can use Common Criteria certification reports about evaluated security features to judge the relative security of competing computer and networking products.

As a result, Common Criteria evaluations are increasingly used as a purchasing benchmark, providing a common set of requirements that can be used to assess products to meet both local and global security needs. Vendors can describe their products in terms of which evaluations their products have passed. Similarly, consumers can identify and communicate their security needs to vendors based on the Common Criteria.

For example, networking industry leader Cisco is finding that individual customers may not specifically mandate Common Criteria in their products, but they do require demonstrated secure development practices, with requests for reports, audits and showcases. Cisco, which operates the industry's most stringent compliance program, already meets a variety of government product certification requirements, offering an end-to-end, fully compliant network architecture. Increasingly, certifications such as Common Criteria offer a common framework within which network administrators can identify the security capabilities required to meet their needs.

The Future of Common Criteria

Until recently, Common Criteria has been focused on the evaluation of security products. However, the truth of the matter is that if organizations do not also secure the complete network, systems will still not be fully secure. Significant progress has been made over the last 12-18 months to expand evaluation criteria to address product security across a broader set of network components. In addition, Common Criteria has the potential to cover supply chain security and management procedures.

Clearly, product security must continue to evolve to support new technologies such as unified communications, video conferencing, mobility and cloud.

Each of these new technologies brings different challenges to the table. No single nation can identify the direction of the next security requirement—threats can change from nominal to critical in days or even hours. However, by relying on the broader public/private technical communities, security requirements can be more rapidly developed to meet evolving needs and respond to challenges as they occur (Figure 2).

Common Criteria in the Supply Chain

The other critical area of evolution for Common Criteria is in the supply chain. Global supply chains have opened the door to attacks at every stage, including fulfillment, distribution, sustainment and disposal. According to the U.S. Department of Commerce (2010), 39 percent of companies and organizations encountered counterfeit electronics just from 2005 to 2008, with the number of encounters increasing from year to year. The problem continues to recur: For example, a U.S. Department of Defense investigation in 2011 showed that no fewer than 93 separate suppliers to the DoD had provided suspect parts on at least one occasion, and some up to more than 10 times.

Along with meeting international standards, vendors need to ensure the security of the supply chain by combining traditional management practices with auditable, verifiable system security requirements. By combining a basic set of best practices into a single approach, nations participating in Common Criteria would be able to leverage consistent safeguards to greatly diminish the risks of the supply chain. This is not a new idea. It is already being implemented by the Smart Card community, where Common Criteria is being used as a basis to assure consistent development and manufacturing processes.

Buying Certified

Common Criteria is increasingly recognized for its relevance to every aspect of the network, especially in environments that can be identified as critical infrastructure. It's also key for environments in which governments impose strict regulatory requirements to assure security and mitigate risk. This includes everything from air traffic control and metro systems to electric utilities, which must comply with standards such as NERC CIP in the U.S. Meanwhile, service providers have found that Common Criteria compliance allows them to reduce risk without increasing costs.

The Common Criteria provides a baseline to greatly improve overall security of the network without additional cost to the customer. Vendors increasingly leverage this standard across their product portfolios, knowing that many customers now rely on this established security framework. With a choice of network security products available, there seems to be no reason why any organization, government or business, should not choose to buy products that are Common Criteria certified. ▮▮

Cisco Systems
San Jose, CA.
(408) 526-4000.
[www.cisco.com].