

Security Certifications: When Is Faster Better?

What's worse than a known security vulnerability in government? Answer: A new security product that introduces an unknown vulnerability.

That's why government is committed to evaluating security products before authorizing their use. The Common Criteria, for example, provide a cost-effective and consistent approach to evaluating security products, answering questions such as:

- Are the software features designed in a secure manner?
- Does the software contain vulnerabilities that can be exploited?
- Do the software features behave as expected when tested?
- Is the solution susceptible to secret messages instructing it to perform an undesired function?
- Does the software contain trap doors that the developer can later exploit?

An international standard for evaluation, Common Criteria is administered in the United States by the National Information Assurance Program (NIAP) within the National Security Agency (NSA) and internationally recognized by members of the Common Criteria Recognition Agreement (CCRA). Federal government agencies that handle sensitive information must purchase products certified against the Common Criteria.

The Great Irony

Although the Common Criteria provide a high level of assurance that a security product works as advertised, there is some concern about the time required for certification, according to Gene Keeling, director of Cisco's global certification team. "Cybercriminals devise a new type of attack or exploit every week," he says. Security vendors respond quickly with new solutions to detect the attack or patch the hole. In extreme cases, they develop a new product to protect against the attack type. In addition to the development cycle for a new product, Common Criteria evaluation requires another two years, and intelligence agencies perform additional evaluations that take up to another year or more.

"By the time an agency can implement a security solution, it's already three years old," Keeling says. Ironically, delaying introduction of a security product to increase confidence actually undermines an agency's security posture.

Therefore, industry and governments around the world continue to look for ways to make the certification process better and faster.

Shortening the Cycle

NIAP has announced proposed changes for reduced requirements to accelerate the evaluation process (www.niap-ccevs.org). "We are excited about NIAP's proposed changes," Keeling says. "The challenge is making sure that the changes also satisfy our international customers."

An idea that complements the proposed change is to add an accelerated technology adoption process that operates in parallel with Common Criteria testing. The parallel process, currently under consideration by NIAP and the Office of the Secretary of Defense, combines those parts of the Common Criteria, FIPS 140-2, and Department of Defense IA Accreditation processes that can be automated. "The goal of the approach is to achieve 80 percent assurance in 20 percent of the time, ideally just two or three months," Keeling says.

Under the proposal, early adopters would receive an Interim Authority to Operate (IATO) while the product undergoes the full Common Criteria and other certification processes. Depending on the results, the agency would either receive Authority to Operate (ATO) or be told to decommission the product. "Supplementing the Common Criteria with the accelerated track will provide earlier validation of new technology and give early adopters a head start once an ATO is granted," Keeling says.

Cisco is a global leader in completing and pursuing Common Criteria evaluations as well as other global government certifications. To see completed Global Government Certifications, as well as those in progress, visit: www.cisco.com/go/securitycert.




Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

 CCDE, CCVP, Cisco Eos, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0801R)