Risk Reducer: Security Certifications and Evaluations

A big step in managing security risk on government networks is minimizing the number of unknowns in the way products behave. That becomes easier when agencies deploy products that have earned the Federal Information Processing Standards (FIPS) 140 or Common Criteria certifications.

FIPS 140 is a certification specification specifically for encryption products, such as those used in virtual private network (VPN) systems that enable teleworkers and mobile workers to connect securely to the agency network over the public Internet. “If a vendor does not properly implement cryptography, a hacker might be able to decipher the data going over a wire,” says Chris Romeo, certification solutions program manager, Cisco Systems®. “But if a product has earned FIPS 140 certification, the federal agency can be confident that cryptography was implemented properly – and without investing considerable time and money to develop and conduct its own tests.”

By boosting confidence in communications security, security certifications contribute to the success of federal continuity of operations (COOP) and collaboration initiatives. “Agencies that trust the security of communications can more comfortably share sensitive information with other agencies, and use networked communications to assemble virtual response teams,” says Romeo.

COMMON CRITERIA, FOR UNCOMMON SECURITY

The other major standard for security products in government networks is the Common Criteria, an international standard for evaluation administered by the International Standards Organization (ISO). This 582-page compendium outlines security properties required in a broad range of products, from network devices to wireless devices to smart cards. For each type of product, the National Security Agency (NSA) pulls together individual properties in the Common Criteria to create different “protection profiles.” The protection profile for firewalls, for example, combines three criteria: handling identification and authentication properly, the ability to block traffic from specified addresses, and logging attempts to get into the network from prohibited addresses. “Some agencies include protection profiles in their request for proposal (RFP), both to save time and to make sure they have not left out any requirements,” says Romeo. “The NSA does not skimp when it creates protection profiles. Therefore, an agency that purchases a Common Criteria product can be confident in its security capabilities.”

SIMPLIFIED PURCHASE DECISIONS

Certifications and evaluations simplify purchasing decisions in several ways. “The primary value of security testing and certification for federal agencies is allowing them to adopt newer technologies and yet have better assurance that they are secure,” says Ed Morris, director of Atlan Laboratories, one of several independent laboratories authorized to perform security testing for IT security products. Certifications also simplify purchase decisions for network products by making sure that product comparisons are fair. That is, for some agencies, a VPN solution that is certified to Common Criteria Evaluation Assurance Level (EAL) 4 – there are seven levels – is worth more than one certified to EAL 2. Yet another advantage is helping agencies comply with the Federal Information Security Management Act (FISMA) and other regulations.

BEHIND THE SCENES

Certifications and evaluations are performed by independent third parties, such as Atlan, which are licensed and accredited by the National Institute of Standard Technologies (NIST). The third parties perform independent reviews, including testing as well as documentation review, to validate that the product conforms to the requirements. Results of FIPS 140 testing are also submitted to NIST for independent validation.

The process is rigorous: 7 to 12 months for FIPS 140 and up to 18 months for Common Criteria. And that does not include the time the vendor has already spent developing documentation and conducting its own tests. Cisco®, which has 37 certifications, decides which ones to pursue based on input from its federal customers. The latest product to pass the Common Criteria evaluation is the Cisco Adaptive Security Appliance (ASA), which combines VPN, firewall, and intrusion prevention capabilities.

For a list of Cisco security certifications, including FIPS 140, Common Criteria, and others, visit: http://www.cisco.com/go/securitycert.

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

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

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Printed in USA C11-359696-00 07/06