

# SD Times

SOFTWARE DEVELOPMENT

The Industry Newspaper for Software Development Managers

JUNE 1, 2005

ISSUE NO. 127

Sun Nonplussed by Apache  
J2SE Effort .....5

Common Criteria  
Or Common Confusion? ....5

PerfectBuild Aims To  
Eliminate Code Failures .....7

IBM, Ascential Deal  
Is Completed .....8

W3C to Set Rules  
Regarding Business Rules ..10

BEA Furthers Strategy  
For SOAs .....13

Sun Builds a Fortress  
For Scientists .....14

Gluecode Buy Extends IBM  
To Low-End App Servers ...16

Sybase Makes Two  
Acquisitions  
For Data Access .....17

Insession, Pegasystems  
Update BPM Tools .....18

An Open-Source Project  
To Simplify Others .....20

FirstSQL: Keeping Up With  
The Joneses' Database ...26

Microsoft's Metro:  
Reaching Into  
Adobe's Space? .....30

Good News/Bad News  
About Windows Mobile 5 ..33

## COLUMNISTS

**O'BRIEN:**  
Shooting Silver Bullets  
At Moore's Law .....40

**BINSTOCK:**  
64 Bits And  
Nowhere to Go .....43

**HOLUB:**  
Finding Pathfinder .....45

**RUBINSTEIN:**  
Open Source  
Picks Up Speed .....46

A BZ Media PUBLICATION \$7.95

www.sdtimes.com

## Common Criteria or Common Confusion?

Misperceptions about the global security standard abound

BY JENNIFER DEJONG

Security breaches get all the attention. But Common Criteria, the process designed to certify that commercial software offerings are secure, is hardly the stuff of headline news.

Mike Wolf wants to change all that. "Common Criteria certification matters," said the general manager of the advanced products engineering group at Green Hills, which sells real-time operating systems and embedded software. But until people understand more about how the Common Criteria evaluation process works—and what the rankings mean—a more apt name for it might be "Common Confusion," he said.

Common Criteria for IT Security (CC) is an international evaluation process and a set of standards that mandates what types of security threats categories of commercial software, such as a database and an operating system, must guard against. The certification process evaluates the technical remedies a product offers to meet those

threats and assigns a level of assurance that reflects the evaluators' confidence in the product's ability to protect against those threats, Oracle's chief security officer, Mary Ann Davidson, explained in an e-mail interview.

### CONFUSION REIGNS

Evaluators examine issues such as how a product manages log-in, authentication and access control and how it encrypts critical data, as well as its ability to audit user actions, which is critical to tracking how security breaches occur. Confusion results not because the process is inherently flawed, said Wolf, but because the process has two dimensions to it. People tend to focus on the second dimension, without considering how it relates to the first, he said.

The first, known as the Protection Profile, identifies the security requirements that were tested. The second, known as the Evaluation

## GETTING A GRIP ON SECURITY

**What it is:** Common Criteria is an evaluation process and a set of standards that specify the security threats commercial software offerings must guard against. The word "common" connotes that the process is international. Prior to 1993, individual countries implemented their own security initiatives.

**What it evaluates:** How commercial software handles log-in, authentication and access control; how it encrypts critical data and audits user actions, as well as how it implements other, more advanced security features.

**Why it's confusing:** The rankings have two dimensions to them: The Protection Profile (which specifies the security requirements that were

tested) and the Evaluation Assurance Level (which, ranging from EAL1 to EAL7, signifies the level of confidence evaluators have in the product's ability to deliver on its security claims). That means evaluators can have a reasonably high degree of confidence in a product's ability to deliver a relatively low level of security.

—Jennifer deJong



Assurance Level, assigns a ranking from EAL1 (low) to EAL7 (high) that signifies the level of confidence evaluators have in the product's ability to do what it claims to do in terms of security.

An EAL4 ranking is widely considered competitive, said Dan Frye, vice president of IBM's Linux Technology Center. But knowing that a product has met EAL4 is meaningless unless the profile protection it was evaluated against is also taken into account, said Wolf. For instance, Microsoft received a Common Criteria certification for Windows 2000 at EAL4, against the Controlled Access Protection Profile (CAPP). But CAPP represents only a minimal level of security functions, defined as "casual or inadvertent attempts to breach the system security," he said. In other words, "you can have a high level of confidence about a minimal set of security functions," he said.

Novell's SUSE Linux Enterprise Server 9, running on IBM eServers, earned CAPP/EAL4+ earlier this year, said Frye. Microsoft declined a request for an interview, but a spokeswoman said in a statement: "Microsoft regards Common Criteria (CC) certification as a critical measure of a product's security assurance and quality.... We are pleased to have received CC EAL4 Augmented certification for the Windows 2000 platform (including Windows 2000, Windows 2000 Server and Advanced Server)."

Green Hills is currently seeking certification for the INTEGRITY Separation Kernel (part of its operating system for embedded development), against the Protection Profile for Separation Kernels in Environments Requiring High Robustness (SKPP). The profile represents a sophisticated set of security functions, which specifies, among other things, that programs in different partitions are isolated from one another, Wolf said.

CC originated in June 1993, when the United States, Canada and European countries joined forces to create a global standard for software security, instead of relying on country-specific initiatives. Version 1.0 of the CC was completed in January 1996 and became ISO International Standard 15408 in 1999. The current version is 2.2, according to Common Criteria Evaluation and Validation Scheme (CCEVS), which implements the certification in the United States.

Wolf said that although the CC certification rankings can be difficult to decipher, the CC process works and the key to understanding it is education. "Awareness of security is growing, but it's not yet where it needs to be." Meanwhile, the level of sophistication of attack technology is frightening, he said. ■

