When C2 is on the PO

If you sell to the federal government, there is a good chance that your product will have to run on a trusted system.

By Gary Donnelly

Consider this scenario: Your firm's marketing efforts have finally succeeded in penetrating a large federal agency. The potential for significant sales from this organization is large. Just as you begin to count your revenue (or your commission check if you're the sales person for this account), your prospect asks, "Your software does run on a C2 system, doesn't it?"

You answer, "Huh?" This might not be the best time to begin learning about trusted systems.

Do independent software vendors (ISVs) really have to worry about trusted systems? Since your software product runs at the "user level," are you affected by running on a somewhat different operating system than you currently support? Let's take a look at each of these questions.

A *trusted computer system* is one that provides a computing environment consisting of both hardware and software, and incorporates software integrity measures that allow its use to concurrently process classified or unclassified information without violating access privileges by any user, regardless of their level of classification. There are different levels of trust that are based on the ability of the computer system to enforce access privileges to authorized users and to system-protected files. There are four primary levels of trust: A, B, C and D, with A being the most trusted and D the least. Some of these levels have sublevels (1, 2 and 3). Taken together, there are seven levels (in decreasing order of security): A1, B3, B2, B1, C2, C1 and D. The technical attributes of each are detailed in the Orange Book, which is described below.

By the Book

The National Computer Security Center (NCSC) evaluates the security features of trusted products against established technical standards and criteria. It maintains the Evaluated Products List, a compilation of all computer products that have undergone formal security evaluations, and indicates the relative security merit of each computer product. The criteria against which computer systems are evaluated is the Orange Book.

In January 1981, the National Security Agency (NSA) became responsible for the security of computer systems for the U.S. Department of Defense (DOD). As a result, NCSC was formed as part of the NSA. NCSC's role was to develop and maintain a set of standards and conformance tests of those standards in the area of computer security. Then DOD could specify a certain conformance level of those standards when purchasing systems and be assured of having a known degree of security features.

These standards were published as the *Department of Defense Trusted Computer System Evaluation Criteria*. Because this publication had an orange cover, it was often referred to as the Orange Book (a cozier name than DOD TCSEC). The Orange Book was issued first in August 1983 and in December 1985 was reissued as a Department of Defense standard (DOD 5200.28-STD).

The Orange Book then became referenced as a mandatory requirement for operating systems delivered to DOD. Once that happened, anyone who sold an operating system to DOD had to implement a trusted system. This forced firms, such as DEC, Hewlett-Packard, IBM and others, to develop trusted versions of their respective operating systems. This concept has moved beyond DOD, and currently many civilian agencies, such as the IRS, the Department of Agriculture, U.S. Customs and others, require a trusted operating system on many if not all of their operating system purchases. While this often does not include desktop operating systems such as DOS and Windows, it does apply to servers.

The ISV's Involvement

Does an independent software vendor really have to worry about these issues? *Worry* is probably not the best word here. What is needed is an understanding of what your software requires in terms of privileges and its interaction with the operating system. Keep in mind that the definition of a trusted system includes both hardware and software. For a vendor to take a server with its operating system to NCSC for testing and evaluation is an involved, time-consuming process. At the end of this process, the vendor has achieved a trusted certification for that specific combination of hardware and software. If that combination changes in any way, such as a different hardware configuration or additional hardware, the certification will no longer be valid. Neither the vendor nor the federal end user will be eager to undo a process that has taken considerable effort to complete.

Since your software product runs at the "user level," you are probably not affected by running on a somewhat different operating system than you currently support. For an operating system to achieve a certified trust level, changes in the operating system—in the form of access controls, reuse of objects, identification and authentication, and audit—are required. Most of these changes may require the granting of different levels of privileges to your application, but the basic application should still run properly.

One commercially available operating system that has achieved an NCSC certification is Trusted Xenix from Trusted Information Systems (TIS) of Glenwood, MD. Trusted Xenix has been evaluated at B2 by the NCSC on a variety of 286 and 386 platforms produced by AST, Grid, Hewlett-Packard, IBM, NCR, NEC, Trend, Unisys, Wang and Zenith. From this list you should notice that being certified for one platform doesn't grant certification to others, even if both use the Intel platform. Additionally, TIS has developed Trusted Mach (Tmach), a version of Carnegie-Mellon University's Mach operating system, which is currently undergoing testing and evaluation at NCSC for a B3 rating.

Noelle McAuliffe, a systems analyst for TIS, says that her firm provides to third-party developers an application development guide to assist them in writing applications for Trusted Xenix. McAuliffe explains that as the certification level moves toward higher security (from C2 to B2, for example), special privileges may be required for applications to operate properly. These include areas such as audit, Set User ID (SUID) root, and both discretionary and mandatory access controls. As a software developer, you will have to work with the provider of the trusted operating system and do advanced testing to determine the effect of these security issues on your application.

In terms of porting your software to a trusted system, the general consensus is that your application should move over without much problem. If you are confronted with the earlier question about your software running on a trusted system, you should now at least be able to have something more to say than "Huh?" Find out what trusted platform your software is going to be required for, and then work with the vendor of that operating system. As with TIS, you may be able to obtain developer information to assist you in knowing more about that platform. You'll likely not have a major problem, but it's better to be aware of problems before having to deliver the software. And wouldn't that be a novel approach?

__Gary Donnelly__ teaches and consults in the client/server and open systems arena, focusing on federal marketing issues. He can be reached at gary@donnelly-inc.com.

ADVERTISING INDEX

ADVERTISER	PAGE #	INQUIRY #
Elan Computer Group http://www.elan.com	17	107
Fujitsu Microelectronics http://www.fmi.fujitsu.com	Cover 2	101
Hyde Co., The http://www.spatch.com	47	110
IBM Corp. http://www.ibm.com	1	102
Interex http://www.interex.org	15	106
Linux Journal http://www.ssc.com/lj	29	108
Network Computing Devices http://www.ncd.com	Cover 3	111
Santa Cruz Operation, The http://www.sco.com	2-3	103
SCO Forum http://www.sco.com	Cover 4	112
Sterling Software http://www.sterling.com	13	105
UniDirect http://www.unidirect.com	9	104
UniForum Association http://www.uniforum.org	6-7, 41	
UniSolutions Associates http://www.unisol.com	47	113
WEBsmith http://www.ssc.com/websmith	43	109

World Wide Web addresses of *UniForum's IT Solutions* advertisers are listed complimentarily each month. The ad index is published as a service. The publisher assumes no liability for errors or omissions.

ADVERTISING SALES OFFICES

Northwestern U.S. and Western Canada
Pat Macsata (510) 888-1104
R.W. Walker Co. (510) 888-0472 fax
22971 Sutro St., Ste. B
Hayward, CA 94541

Southwestern U.S.
Michael Walker (310) 450-9001
R.W. Walker Co. (310) 450-8176 fax
2716 Ocean Park Blvd.
#1010
Santa Monica, CA 90405

Midwestern U.S. and Central Canada
Thomas Fitzpatrick (708) 653-1611
TF Marketing Associates (708) 653-1612 fax
1496 County Farm Ct.
Wheaton, IL 60187

New England and Eastern Canada
Paul Moschella (617) 769-8950
Hajar Associates (617) 769-8982 fax
49 Walpole St.
Norwood, MA 02062

Mid-Atlantic U.S.
Barbara Best (908) 741-7744
Hajar Associates (908) 741-6823 fax
569 River Rd.
Fair Haven, NJ 07704

Southeastern U.S.
Scott Rickles (770) 664-4567
Ray Rickles & Co. (770) 740-1399 fax
560 Jacaranda Ct.
Alpharetta, GA 30202

Publisher's Sales Office
Richard Shippee (408) 986-8840, x17
UniForum's IT Solutions (408) 986-1645 fax
2901 Tasman Dr., #205 e-mail:
Santa Clara, CA 95054 dick@uniforum.org