CMP
United Business Media

Embedded Systems Design

State of security technology: embedded to enterprise

By David N. Kleidermacher, Green Hills Software, Inc.
09/26/07

In "a recent *EE Times* article," Rob Hoffman, a vice-president at Wind River said "no system can be hacker-proof." The sentiment is echoed by Microsoft, as Stephen Toulouse, a member of the company's security technology group, said "The finding of vulnerabilities in any software is to be expected. No one will ever get the software right 100% out of the gate."

These and other statements made by software vendors paint a bleak picture of the state of security technology. I assert the contrary: although high assurance is indeed a high bar, it can be reached, and we must not give up on that aspiration. Furthermore, IT security could well be enhanced by techniques conceived in the embedded arena.

Because it controls the hard resources of the computer, the operating system bears a tremendous burden in security. Yet today, there are no operating systems evaluated at the highest security levels—Evaluated Assurance Level (EAL) 6 or 7—of the Common Criteria, an international security standard. The high levels require a formal design and proof that security policies are upheld.

A main reason for the lack of secure operating systems is in their architecture; most provide a kitchen sink of services, all running in the computer's supervisor mode. A single flaw can spell disaster. In addition, weak access controls allow simple errors in application programs to compromise large swathes of a system.

Recently, companies in the embedded space have taken a new, layered approach in which critical components are strictly partitioned away from other software. At the foundation of the concept is a small, real-time microkernel that implements a critical set of strong access control and data isolation policies.

As an example, Green Hills Software's INTEGRITY operating system was developed for the highest level of security (EAL 7) and is under evaluation by the National Security Agency (NSA). In addition to formal methods, the software must withstand penetration testing by the NSA's expert hackers who have the source code.

Such operating systems are used in top secret communications devices, flight-control systems, medical devices, and various other safety- and security-critical systems. Provable security is achievable, and computers from embedded to enterprise stand to benefit.

David Kleidermacher *is chief technology officer at Green Hills Software where he has been designing compilers, software development environments, and real-time operating systems for the past 15 years. David is a frequent publisher in trade journals and presenter at conferences on topics relating to embedded systems. David has a B.S. in Computer Science from Cornell University.*

References

Goering, Richard. "RTOSes step in to avert network vulnerability 'crisis'," *EETimes*, December 11, 2006.

Keitzer, Greg. "Microsoft: Vista's Secure, Not Perfect," *Information Week*, December 28, 2006.