

Green Hills OS gets approval from National Security Agency

By David Worthington

November 19, 2008 — The process took nearly a decade, but embedded software maker Green Hills Software has proven the mettle of its INTEGRITY-178B operating system, obtaining a high security certification from the US National Security Agency.

On Monday, Green Hills announced that it had obtained Common Criteria Evaluation Assurance Level (EAL) 6+ from the National Information Assurance Partnership (NIAP), an initiative operated by the National Security Agency. EAL has seven assurance levels, with EAL7 being the most secure.

The certification is meaningful because it permits information with different levels of classification to reside on a single computer that runs INTEGRITY, said Dan Mender, vice president of business development for Green Hills. He noted that the cost of federating the separation of data is high.

For instance, in Iraq, the US military maintains hundreds of computers: some are for top secret and classified data, and others connected to the Internet, he said. As a consequence, the military must handle the complexities of integration and communication between machines, as well as space, weight and power demands. "It takes more power to cool the computers than it does to run them," he said.

"The key issue in allowing different tiers of information to reside on a single machine is the separation provided for the different tiers. We have many networks with multiple levels of classified data, but all are treated at the highest level of classification permitted on the system," said a senior official in the Information Assurance Directorate (IAD) of the NSA who asked not to be identified.

"While some operating systems provide the mechanisms to protect multiple tiers, the remaining difficulty lies in codifying and instantiating the rules necessary to sufficiently protect the different tiers. Reliable multi-level security requires more than just the operating system," the official added.

Green Hills sees INTEGRITY's role as a foundational component for secure infrastructure. It provides secure virtualization for guest operating systems, including Linux, Solaris and Windows. INTEGRITY can also run as the host operating system, with secure Linux or Windows partitions, without fear of cascading events, Mender explained in a previous interview.

Much of the United States' critical infrastructure is running on software that is less secure, he said, alluding to the NIAP's certifications of Linux, Solaris and Windows as EAL4. EAL4 certifies that an operating system has been methodically designed, tested and reviewed,

whereas EAL6-rated operating systems offer higher assurance with a design that is almost totally verified as being secure.

Designs are verified by mathematical proofs of security policies, formal specifications and how closely implementation follows design, Mender said.

"National Infrastructure relies heavily on the operating system. The OS controls the functioning, and it is a key link in the overall security, which includes confidentiality, integrity, authentication and availability. Having an evaluated OS, whether the evaluation is NIAP or some other appropriate approved method, is important to the assurance of the infrastructure, but the OS is only a part, albeit a key part, of that protection," the IAD official said.

INTEGRITY had over three years of NSA penetration testing, said Mender. "It was not breached." He credits its design: INTEGRITY was developed for an EAL7 assurance rating and is approximately 4,000 lines of code long, he noted.

While the security of an individual operating system is important, a network is only as good as the sum of its parts, the IAD official noted. "There are several operating systems that have successfully undergone evaluation. Each must be considered as a part of a network solution when one determines what assurance the overall solution provides; none can be considered in isolation."