MILS BACKGROUND

MILS: Emerging Software Architecture for Security-critical Systems

Why MILS?
Standard commercial operating systems were not built for security. Security is bolted on as an afterthought. These systems, although useful and necessary, are too large to be secure. Their many vulnerabilities can too easily be exploited by hackers and other people with malicious intent.

What is MILS?
MILS (Multiple Independent Levels of Security) was first developed by Dr. John Rushby of Stanford University in the 1980's. MILS is a software architecture for security-critical systems such as national defense systems, aeronautics, nuclear power plants, etc. MILS is also useful for public utilities, financial systems, network infrastructure and more. The fundamental idea behind MILS is to have a few, small core components of software that can be mathematically proven to be secure. Large applications and large operating systems are then run on top of these core, security-proven software foundations. This contrasts with the idea of having one large, homogeneous operating system.

MILS was a good idea when it was first invented, but it was hampered by a lack of processing power—as early-generation microprocessors weren't powerful enough to handle all of the partitioning required to make it work.

20 years later, the NSA and the United States Air Force Research Laboratory (U.S. AFRL) started to work with software vendors like us to have us to develop products based on MILS. Operating systems vendors such as LynuxWorks, Green Hills and Wind River got involved. These companies have designed MILS "Separation Kernels"—very low-overhead real-time operating systems (RTOS) that will be security-certified.

Objective Interface's Involvement
The NSA and U.S. AFRL also worked with Objective Interface Systems on MILS middleware. Objective Interface is the architect of the core communications middleware for MILS. On October 17th, Objective Interface will announce PCS*express*, the first MILS middleware communications product on the market. MILS requires both a Separation Kernel (the RTOS) and Partitioning Communications System (PCS) in order to communicate on a secure basis.

MILS Products
These products are all being designed for EAL-7 certification of the Common Criteria. The Common Criteria is a worldwide, internationally accepted standard for the highest level of security certification. EAL-7 is the highest attainable certification within the Common Criteria. The standard rule of thumb for EAL-7 certification is for every 1000 lines of code you write, you write approximately 50,000 lines of mathematical proofs. The goal is to have software that does exactly what it should do: nothing more or less.

The concept of MILS is focused on layered security. So the Separation Kernel and PCS (middleware) are layered separately.

How We Handle this Problem Today
Today, critical data is separated via air gap. If you are considering data separation among coalition forces, you may see 40 tents behind the generals in Iraq. You may also see a member of the DoD with several workstations on a desk: one connected to the Internet, one connected to a private network and one not connected to any network. Information, in this case, is still transferred via 'sneaker net.' Obviously, this is an onerous way to transfer information.

The Value of MILS
The MILS architecture can exist harmoniously with legacy hardware and software systems. For example, you could have a MILS workstation with Windows NT running in a partition. The data in that MILS partition would be secured and you could still use Windows or Linux to develop your applications. Thus, MILS works with your existing hardware-software infrastructure.

With PCS*express*, you can send this information (top secret, secret and unclassified data) over a single wire. It keeps data separate while suppressing covert channels. It encrypts the data, handles network synchronization and more.

The Market for MILS
The MILS software architecture was originally designed for the high-performance needs of the embedded market. It was designed to meet the harsh requirements of weapons systems, unmanned aerial vehicles, autonomous robots, etc., all communicating with a high degree of assurance that no one could hack into these systems. The MILS architecture has been extended to include workstations, servers and enterprise systems—which also have a need for high levels of security for their data.

Availability
Green Hills, LynuxWorks and Wind River are each working on MILS Separation Kernels.

Objective Interface will announce its MILS communications middleware product, PCS*express*, on October 17th. This completes the software requirements for MILS: Separation Kernel + PCS = MILS foundation.