SPYRUS to Highlight Content Protection and New Cryptographic Products to Secure Data at Rest at Flash Memory Summit

SPYRUS expands capabilities of flash memory platforms to include integrated security for multi-function and multi-media applications

2nd Annual Flash Memory Summit

San Jose, California, August 2, 2007 – SPYRUS, Inc., an innovator in portable high-security hardware and software cryptography products, today announced a new line of hardware cryptographic processing and memory products designed to meet U.S. Government Data at Rest requirements. The new line consists of the SPYRUS Hydra Privacy Card® (Hydra PC) Series II and the SPYRUS Rosetta SD/miniSD/MicroSD Series II hardware security devices. Hydra PC is the only data storage/encryption device approved by the U.S. Government Data at Rest program and is also the first commercial-off-the-shelf (COTS) product designed to protect classified data at rest (DAR) and data in transit (DIT) at the SECRET level. The new Rosetta SD/miniSD/microSD Series II devices provide a standard SD, miniSD, and microSD form factor incorporating the same security controller chip, the Rosetta Micro, as is embedded in the Hydra PC.

Since 2005, nearly 160 million records containing personally identifiable information have been lost or compromised, placing the individuals involved at risk of identity theft. Moreover, a significant amount of classified intelligence and military operations data, including nuclear weapons secrets, has also been subjected to compromise. The common denominator in many of these incidents has been unsecured flash storage, including the popular USB flash drive and a myriad of other devices that contain flash storage.

The necessity for robust security implementations and the innovation that comprises the SPYRUS Hydra PC will be discussed in two separate sessions by SPYRUS Chief Scientist Robert R. Jueneman at the 2nd Annual Flash Memory Summit (www.flashmemorysummit.com) held August 7-9, 2007, at the Santa Clara Marriott in Santa Clara, California. Mr. Jueneman will present “Securing SSDs: Popular Myths Regarding Data at Rest, Data in Transit, and Data in Use” in Session 205 – Flash Memory Security Applications, on Thursday, August 9, from 2:00 to 3:00 p.m. He will also be an expert table leader for the topic of Security at the Experts Sessions on Wednesday, August 8, from 6:00 to 7:30 p.m.

The Hydra PC uses groundbreaking security techniques to provide data containment. The Hydra PC features a Host Authorization Code, which ensures that the Hydra PC will function only when used with system administrator-authorized computers. This prevents users from removing sensitive data or using an unauthorized computer to maliciously or inadvertently breach data security. A Hydra PC Sentry function blocks data from being read or written to other mass storage devices, including external hard drives, flash memory devices or similar storage devices. An advanced security-processing mode using integral hardware encryption uniquely encrypts and seals each file sent to the PC hard drive, external storage devices and network drives.

The Rosetta SD/miniSD/microSD Series II multi-layer chip design provides extensive protection against active and passive attacks with a high-assurance architecture and implementation suitable for the most sensitive applications. Rosetta products support high-strength cryptographic algorithms that exceed the U.S. Government Suite B standard and can be used for decades in custom and mass-market products including computers, smart phones, cameras, and other handheld computer and communicating devices.

Today's announcement recognizes the increasing role that flash memory and its supporting platforms play in the consumer, commercial, entertainment and government markets, and the need for robust and portable security for valued content of all forms and formats. To achieve these notable capabilities, the Hydra PC uses innovative security techniques from the SPYRUS security technology portfolio of patents that cover peripheral devices with integrated security functionality (U.S. Patent No. 6,088,802) and modular security devices (U.S. Patent No. 6,003,135). These patents enable portable peripheral devices such as flash drives with integral cryptographic processing to secure content for a wide range of additional functions including memory storage, wireless or wired communications, audio or video playback, and payment transactions that are integral to the platform or are interconnected by wireless communications. The '802 patent also enables mediation of communication between the host and the target function, so that the communicated data must pass through cryptographic processing.

These patents are part of the broad SPYRUS patent portfolio in the United States and abroad that enable secure authentication, conditional access, secure protection and rights management of digital content being communicated through any media.

About SPYRUS, Inc.
SPYRUS, Inc., a Microsoft Gold Certified Partner, has pioneered portable security products and solutions for the information security market since its inception in 1992. Our primary product lines of LYNKS Hardware Security Modules, Rosetta Series II smart cards and USB security devices, Hydra Privacy Card® Series II encryption and mass storage, Talisman/DS® Data Security Suite, and identity management products (Signal Identity Manager™ and SPYRUS PKI) meet customer needs for high-assurance security. Our mission is to set the standard for the new era of multinational information sharing and long-term data protection. SPYRUS, Inc. is headquartered in San Jose, CA. See www.spyrus.com for further information.

#########

For more information, press only:
Dan Chmielewski
Madison Alexander PR, Inc.
714-832-8716
949-231-2965 (cell phone)
dchm@madisonalexanderpr.com