Michael Willett, Storage Security Strategist, Samsung

TITLE

Self-Encrypting SSDs: Self-contained, Solid and Secure

ABSTRACT

Storage is the last frontier of a totally secure I.T. ecosystem. Traditionally, security controls have been implemented on platforms - host processors, centralized servers, laptop CPUs - especially for mobile devices that are not always centrally connected. But, the 'platform', with its attendant open operating system, has proven to be the most vulnerable to viruses and other cyber-attacks. The Trusted Computing Group (TCG) realized that for protection of stored data (where data spends most of its useful life), put the security controls where the protected data resides: directly in the storage device. Self-Encrypting Drives (SED), both HDD and SSD, have been specified in technical detail by TCG and implemented by all the major drive manufacturers. The encryption logic is built directly into the drive hardware electronics. A standards-based interface is provided for both local and centralized SED management. SEDs are now a mature technology and have proven superior to platform-based, software-based encryption. And, SEDs provide unique enhancements, such as Crypto Erase: delete and replace the on-board encryption key and the drive is instantly erased, yet still operable as a 'new' drive. Self-encryption combines with solid-state to tackle the last frontier - storage - with a simple solution that is self-contained and solidly secure.

BIOGRAPHY

Dr. Michael Willett received a Bachelor of Science degree from the US Air Force Academy (Top Secret clearance) and a Masters and PhD in mathematics from NC State University. After a career as a university professor of mathematics and computer science, Dr. Willett joined IBM as a design architect, moving into IBM's Cryptography Competency Center. Later, Dr. Willett joined Fiderus, a security and privacy consulting practice, subsequently accepting a position with Wave Systems. Recently, Dr. Willett was a Senior Director at Seagate Research, focusing on security functionality on hard drives, including self-encryption, related standardization, product rollout, patent development, and partner liaison. Currently, Dr. Willett serves as a consultant on the marketing of storage-based security. Dr. Willett also co-chairs the Privacy Management Reference Model Technical Committee of OASIS, which has developed an operational reference model for implementing privacy requirements. Presently, Dr. Willett is working with Samsung as a storage security strategist, helping to define their self-encryption strategy across Samsung’s portfolio of solid-state storage products.