



Robert Thibadeau, Chief Technologist, Seagate Research/Chair, TCG Storage Work Group

TITLE

Content Protection Using Self-Encrypting Hard Drives: Use It or Lose It

ABSTRACT

Breach notification laws in 40+ states require that the affected public be notified if sensitive data is breached (such as through loss or theft), unless it can be proved that the stored data was encrypted. In addition, it is sound security practice to always encrypt data at rest. Data at rest on storage can be encrypted (and decrypted) “upstream” of the storage device, in a host application or appliance, or in the storage device itself, using self-encrypting hard drives. Self-encrypting hard drives offer clear advantages against upstream encryption for data at rest. The Trusted Computing Group has recently published a trusted storage specification, developed primarily by all the major hard drive manufacturers, that defines in detail the definition and management of self-encrypting hard drives. Encrypting all data at rest on storage devices, combined with the robust authentication and access controls in the TCG storage specification, provides essential content protection for sensitive or valuable content in storage.

BIOGRAPHY

Dr. Robert Thibadeau is chief technologist at Seagate Research in Pittsburgh, Pennsylvania on long-term leave as a professor in the School of Computer Science at Carnegie Mellon University. He was one of the founding Directors of the Robotics Institute in 1980. Since 1998 to the present, he teaches Computer Security in a joint graduate program between computer science and the business school at CMU. In his role at Phoenix, he was one of the initiators and promoters of the concept of measurement now incorporated in the TCG/TPM. He is also well known for his work in privacy. His work on the W3 P3P formed the basis for the European Commission's Java reference for use by business (<http://p3p.jrc.it>). His original reference code was in Microsoft Jscript and ASP and was similarly released in source code for use by industry from CMU in 2001 (<http://yuan.ecom.cmu.edu/psp>). After 9-11, he founded and managed a series of internationally recognized and well-received workshops in platform security, trust, and privacy (<http://www.security.scs.cmu.edu>). As an entrepreneur, Dr. Thibadeau has founded over a dozen companies since 1969, and participated on a number of boards including positions as chairman. The companies founded in the 1990s have received well over \$100M in aggregate venture funding and most thrive to this day (<http://www.nomos.com>). Dr. Thibadeau holds a number of patents, three of which have formed the basis for launching companies. In the area of standards, Dr. Thibadeau was the principal contributor to the ISO/ANSI-approved SMPTE (Society of Motion Picture and Television Engineers) digital broadcast naming standards where he introduced ASN.1-based SMPTE 98e globally unique naming now in use in digital broadcasting worldwide. He is also co-chair of the Framework Committee of the International Security Trust and Privacy Alliance (www.istpa.org) that has introduced a basic IT framework for responsibly handling personally identifiable information. Currently, Dr. Thibadeau is chairman of the TCG Peripherals Workgroup and the Storage Workgroup.