



STORAGE VISIONS[®] 2007 CONFERENCE

AN ENTERTAINMENT STORAGE ALLIANCESM EVENT



Dr. Robert Thibadeau, Chief Technologist, Seagate Research

Title

Trusted Storage

Abstract

Storage Systems, such as disk drives, and other computing-system peripherals are critical components of a security, privacy, and trust configuration of a computing platform. This session provides a framework with which to understand why and how peripheral devices should be secured as independent roots of trust. The framework provides a generic security model for all peripheral devices, and shows how peripherals can be configured as roots of trust, each playing a complementary role in establishing the overall security and privacy goals of platform-based and networked computing.

The session begins with security measures for storage systems that exist today and their relative effectiveness. It will then go into where and how to secure access control of the storage system, discussing in detail what needs to be controlled and how to grant control in a secure manner.

The Trusted Computing Group's Trusted Storage Use Cases will be reviewed in depth, highlighting the technical requirements being solved by the formal specifications. Relationships and cooperation with other industry storage standards (eg, SCSI and ATA) will be discussed, and the TCG's specification for secure and trusted storage will be outlined (anticipated publication: June 2006).

Representative Use Cases for trusted storage include:

- Enrollment and Connection: trusted relationship – Storage Device (SD) + host
- Protected Storage: for storing sensitive data

Talk to be given at the Storage VisionsTM 2007 Conference at the Flamingo Hotel, Las Vegas, NV January 6th and 7th 2007



STORAGE VISIONS[®] 2007 CONFERENCE

AN ENTERTAINMENT STORAGE ALLIANCESM EVENT



- Locking and Encryption: mating SD and host; encrypting stored data at rest
- Logging: for forensic purposes
- Cryptographic Services: supporting a variety of security services
- Assigning Storage Device Feature Sets to Hosts: trusted/exclusive use
- Secure Download of Firmware: trusting firmware upgrades

All major hard drive manufacturers are participating in the development of these specifications, as well as flash, optical, and tape memory representatives. The result will be that storage systems, where sensitive data spends most of its life time, will be a source of trust for multi-component trusted platforms of the future.

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 TCPA/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.

Talk to be given at the Storage VisionsTM 2007 Conference at the Flamingo Hotel, Las Vegas, NV January 6th and 7th 2007