"Securing Flash and Solid State Drives" - F1C

Dr. Marco A.A. Sanvido
Storage Work Group
Trusted Computing Group
3855 SW 153rd Drive
Beaverton, OR 97006
marco.sanvido@hitachigst.com

Statement

As opposed to other storage media (e.g. Magnetic, Optical) NAND flash lowers the barrier for an attacker to access the raw data stored on the media. As a consequence many flash based products use raw data encryption as a mean to protect their data. Unfortunately security is more than simple data encryption; it is also about confidentiality, integrity, access control, offline and online protection, key management, etc. Consequently in order to secure flash based storage devices, a comprehensive secure storage architecture capable of addressing all these security aspects is required. Moreover in order to be able to build a viable storage security ecosystem a standardized architecture that is accepted and supported by the majority of the storage vendors becomes a requirement. This talk will present such an architecture, as well as two of its incarnations one tailored for server storage security needs, and the other addressing the needs of the customer and enterprise IT storage market. The specifications are published by the Trusted Computing Group and developed with the active participation off the major HDD manufacturers.

Biography

Dr. Marco A.A. Sanvido is a researcher at Hitachi Global Storage Technologies. Marco holds a Dipl.-Ing. degree (1996) and a Dr. techn. degree (2002) in Computer Science from the Swiss Federal Institute of Technology in Zürich, Switzerland (ETHZ). He was a co-founder of weControl, an ETHZ spin-off, where he developed low-power and real-time embedded systems for autonomous flying vehicles. He was a postdoctoral researcher in Computer Science at the University of California at Berkeley from 2002 to 2004, and thereafter he worked on virtualization at VMware. Currently Marco is working at Hitachi Research on a wide range of storage architecture projects ranging from security, hybrid-hdd to novel storage architectures, and is a member of the Trusted Computing Group (TCG) working on the TCG storage specification.

Copies of the presentation are available at www.trustedcomputinggroup.org or by emailing marco.sanvido@hitachigst.com.

About the Trusted Computing Group

The Trusted Computing Group (TCG) is a not-for-profit organization formed to develop, define, and promote open standards for hardware-enabled trusted computing and security technologies, including hardware building blocks and software interfaces, across multiple platforms, peripherals, and devices. TCG specifications will enable more secure computing environments without compromising functional integrity, privacy, or individual rights. The primary goal is to help users protect their information assets (data, passwords, keys, etc.) from compromise due to external software attack and physical theft.

Marco Sanvido, PhD
Marco Sanvido
Storage Work Group
Trusted Computing Group
3855 SW 153rd Drive
Beaverton, OR 97006
Phone: 408 717 5138