



CONTACT: Anne Price
1-602-840-6495
press@trustedcomputinggroup.org

BETTER DATA PROTECTION FROM CLIENT TO DATA CENTER MADE POSSIBLE WITH NEW TRUSTED COMPUTING GROUP STORAGE DEVICE SPECIFICATIONS

Group Also Addresses Interfaces to Ensure Interoperability Among Trusted Storage

PORTLAND, Ore., Jan. 27, 2009 – The Trusted Computing Group (TCG) today released final versions of three storage specifications that will enable stronger data protection, help organizations comply with increasingly tough regulations and help protect important information from loss and theft. The Privacy Rights Clearinghouse estimates that in the United States alone, 251,154,519 records have been lost or stolen since January 2005*. Some 12,000 notebook PCs are lost or stolen in airports in the United States, with only 33 percent recovered by owners.**

Said Robert Thibadeau, chair, Trusted Computing Group Storage Work Group, “Lost and stolen data costs industry and consumers hundreds of millions of dollars, not to mention loss of credibility, legal issues and lost productivity. TCG’s approach to Trusted Storage gives vendors and users a transparent way to fully encrypt data in hardware without affecting performance so that data is safe no matter what happens to the drive.”

TCG’s Storage Work Group has been working on specifications to add security to PC and data center storage devices. These final specs, known as the Opal Security Subsystem Class Specification for PC clients and the Enterprise Security Subsystem Class Specification for data center storage, now are available at <https://www.trustedcomputinggroup.org/groups/storage/> with an additional specification, the Storage Interface Interactions Specification, that focuses on interactions between these storage devices and underlying SCSI/ATA protocols. Storage device specifications give vendors a blueprint for developing self-encrypting storage devices (e.g., hard drives) that lock data, can be immediately and completely erased, and can be optionally combined with the Trusted Platform Module, or TPM, for safekeeping of security credentials.

“With 48 states and many countries enforcing data protection laws, it has become crucial for enterprises to protect all data to avoid fines, lawsuits or even being put out of business. Encryption with authentication directly in the drive or enterprise storage devices as outlined in the Trusted Computing Group specifications is one of the most effective ways to ensure data is secure against virtual and physical attacks,” noted Jon Oltsik, senior analyst, Enterprise Strategy Group.

-- more --

The Opal specification outlines minimum requirements for storage devices used in the PC client and enterprise markets. It outlines for vendors required and optional TCG capabilities and it specifies how to activate and customize the trusted storage device. Some vendors are starting to ship products based on the OPAL specification and have demonstrated how these are interoperable with those from other vendors.

The Enterprise Security Subsystem Class Specification extends the concepts of trusted storage devices to those used in data centers and high-volume applications, where typically there is a minimum security configuration at installation, a requirement to bring devices on-line quickly and the need for high performance with low overhead. The specification defines encryption of data on media and enables support for strong access control to support organizational security.

Finally, the Storage Interface Interactions Specification specifies how the TCG's existing Storage Core Specification and the other specifications interact with other specifications and standards for storage interfaces and transports. For example, the specification supports a number of transports, including ATA parallel and serial, SCSI SAS, Fibre Channel and ATAPI. It was developed with input from representatives of those organizations. Importantly, it enables interoperability of trusted drives in legacy environments.

The Storage Work Group also has addressed trusted optical storage with a specification that was released in late 2008. This specification, which will enable trusted storage in standard recordable optical discs, is targeted for applications in governmental agencies, financial services, healthcare, insurance, and military. Eventually, the functionality will be available for all optical consumer applications, giving all users a secure way of protecting their data on removable optical discs. That specification also is available at TCG's website.

Trusted Computing Group, an industry organization that enables computing security, has created a portfolio of specifications to enable more secure computing across the enterprise in PCs, servers, networking gear, applications and other software, hard drives and embedded devices. More information and the organization's specifications and work groups are available at the Trusted Computing Group's website, www.trustedcomputinggroup.org.

-- 30 --

Brands and trademarks are the property of their respective owners.

* Source: Privacy Rights Clearinghouse: <http://www.privacyrights.org/ar/ChronDataBreaches.htm>

** Ponemon Institute, 2008

Trusted Computing Group Members Support New Trusted Storage Specifications with Products

Jan. 27, 2009

Hard Drive Suppliers:

"By standardizing notebook PC HDD encryption management, the Opal Security Subsystem Class Specification allows software vendors to fully utilize the security capabilities built into the drives and roll out comprehensive solutions for both large IT organizations and individual client machines," said David James, vice president, advanced product engineering, **Fujitsu Computer products of America, Inc.** "Once again, TCG's specifications offer industry best practices that improve security, user experience and total cost of ownership. Fujitsu is proud to be among the leaders in demonstrating Opal-based HDDs for mobile applications."

"**Hitachi** fully supports Trusted Computing Group efforts to enhance data security standards for consumers," said Brendan Collins, vice president, Product Marketing, Hitachi GST. "Hitachi has a history of backing open industry standards and has now shipped four generations of encrypted hard disk drives. The new TCG Opal specification has the potential to extend the reach of data encryption technology and provide additional safeguards for notebook users at risk of exposing confidential information following a system loss or theft."

"**Seagate** has previously announced self-encrypting hard drives for the data center supporting the Enterprise Security Subsystem Class Specification, which provides numerous benefits to the enterprise," said Henry Fabian, Seagate executive director of core marketing. "Self-encrypting drives not only deliver AES government-grade encryption, but offer key encryption technology, effectively making existing data unreadable once the encryption key is erased. This technology is ideal for data center drives that are repurposed, reused, recycled, or returned for expired lease, repair or warranty."

"**Toshiba** supports the TCG Storage Work Group principle that storage device security is best achieved by embedding security features inside the hard disk drive," said Maciek Brzeski, vice president of marketing at Toshiba America Information Systems, Inc. Storage Device Division. "The new TCG specifications play an important role in promoting broad industry adoption of secure storage devices and we commend the TCG SWG on achieving this important milestone."

Applications Providers:

"By standardizing the means of managing and operating secure devices, the TCG Storage Work Group has achieved a critical step in enabling solutions which combat the rising impact of data breaches. Today's release of the OPAL and Enterprise SSC specifications ushers in a new generation of storage hardware that allows us at **CryptoMill** to bring our innovation to an even wider audience," said Nandini Jolly, president and CEO at CryptoMill Technologies. "In addition to managing these self-encrypting drives, CryptoMill's SEAhawk security solution extends the TCG capabilities by protecting user data after it leaves the trusted storage device, preventing it from migrating to other devices in an unauthorized or unsecure manner, by binding it to the organization that owns the data. With SEAhawk and secure storage devices based on TCG specifications, an organization is protected from both the perils of lost or stolen equipment and from threat of exposure from the inside – all managed by a single management platform."

“The TCG Opal specification represents a critical industry milestone for the development of standardized self-encrypting hard drives,” said Lark Allen, executive vice president of **Wave Systems**. “By ensuring interoperability across storage vendors, encryption technologies and platforms, Opal sends a strong signal that hardware FDE is the best option for businesses today. Wave is the first ISV to announce and demonstrate robust policy management for a wide range of encryption technologies, including FDE drives from leading vendors Seagate, Fujitsu and Toshiba, along with coming Opal drives from Hitachi and other drive vendors. For businesses with mixed environments or those looking to ‘bridge the gap’ from software to hardware FDE, Wave’s flagship management solution, EMBASSY® Remote Administration Server (ERAS), now provides robust policy management for SafeNet’s award-winning ProtectDrive™ software FDE. Now businesses can roll out a single, universal policy management server that works seamlessly across heterogeneous FDE client applications. Moving full disk encryption out of software and into hardware will make it much more secure, higher performing and easier to use.”

“These TCG specifications for trusted storage solutions help **WinMagic** to streamline support and integration efforts for ‘self encrypted’ devices as part of a broader security strategy for data-at-rest with SecureDoc,” said Garry McCracken, vice president of technology relationships, WinMagic Inc. He continued, “Protection of sensitive and mission-critical information across a heterogeneous mobile environment (including ‘OPAL’ devices, legacy devices, removable media and other endpoints) is a challenge; the interoperability and standards offered by the TCG specifications will enable WinMagic and our customers to meet that challenge more rapidly, at a lower total cost of ownership.”