

Drive-Level Security:

Innovation for Securing Data at Rest

Robert Thibadeau, Ph.D.
Chief Technologist
Seagate Technology, LLC

Full Disk Encrypting Drive w/ Enhancements



Trusted Computing Group
www.trustedcomputinggroup.org

Storage Workgroup : Disk Drives and other Storage Devices (including flash)

Enterprise Storage Key Management Subgroup : Key management for disk drive and system controller encryption and other security functions.

Interfaces Subgroup : ATA and SCSI and other Interfaces

Compliance and Conformance Subgroup : Functionality and Security



Main “Use Cases” of the SWG

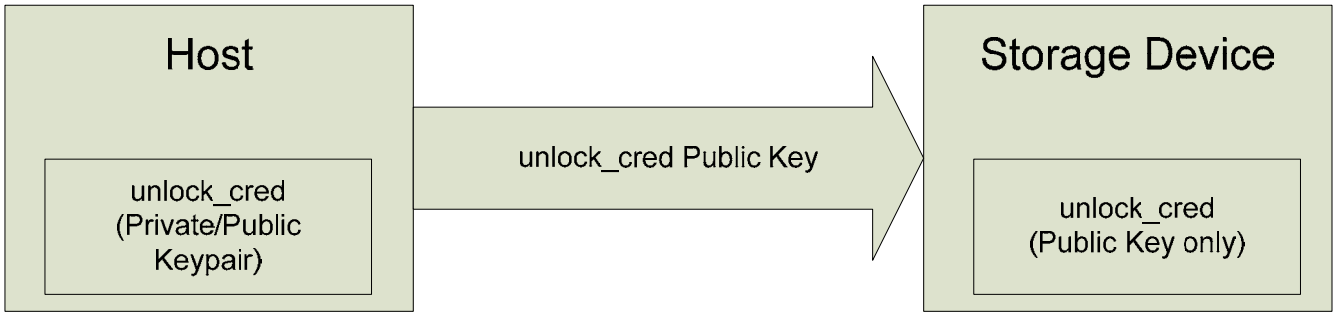
Enrollment and Connection

Locking and Encryption of User Data

Protected Storage



Enrollment Example

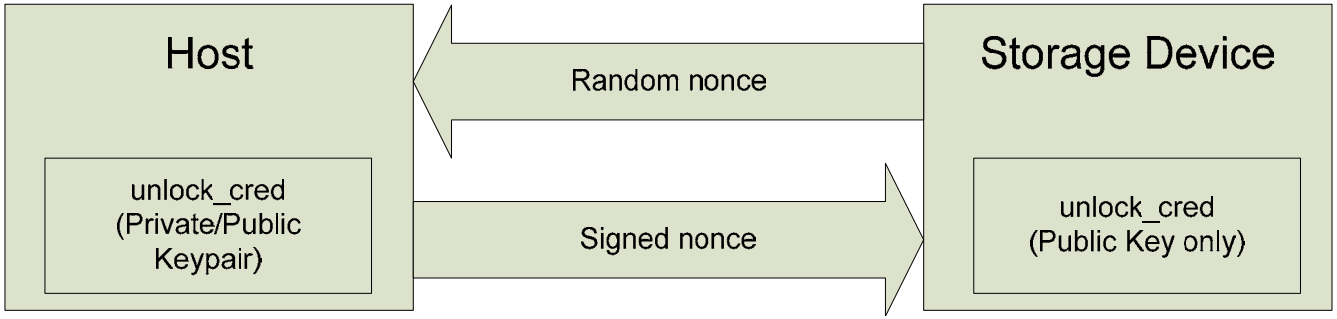


Host generates a public/private keypair called “unlock_cred” (stored in its TPM)

Host injects the public key of “unlock_cred” into the storage device

Host configures the storage device to only allow access to hosts that can prove knowledge of the “unlock_cred” private key

Connection Example



Storage device generates a random nonce and sends it to the host

Host digitally signs the nonce using the “unlock_cred” private key, sends it back to storage device

Storage device verifies the signed nonce with the “unlock_cred” public key, unlocks itself for access

Locking and Encryption of User Data

Allows read/write locking of multiple user partitions on the device. Different credentials can be configured for each partition.

Each user partition can be encrypted with a different key.

Encryption provides additional protection beyond the “Enrollment and Connection” locking (the media will appear to contain random data if the locking is somehow bypassed).

Encryption also allows for “instant” secure erase of the device. Simply changing the encryption key renders the old data useless. Allows the HDD to be securely disposed of or repurposed.



FDE Drives

- *Fast* disk disposal/repurposing
- *Protect* of all data against computer theft
- Is *independent of operating system*
- Lock individual drives to particular machines *makes a hard drive useless to a drive thief*
- *Fastest* FDE security solution combines Windows XP/Vista OS with a Seagate DriveTrust hard drive with FDE
- Substantially improves system protection provided by Trusted Computing Group's TPM



Protected Storage

"Secure Partitions" (SPs) are secure data areas that are separate from the user data area.

SPs can be created and deleted, and access controls can be set up such that a host application has exclusive access to the data contained in the SP. Useful for storing:

- Private data (social security numbers, etc.)
- Software licenses
- Digital cash (some day)



Protected Storage also gives….

Code that loads automatically on USB Attachment!

- If foreign machine, collect info and mail to me about thief!



Full Disk Encrypting Drive w/ Enhancements

