Trusted Storage

Dave Anderson
Seagate Technology

- TRUST -

system behaves as designed

Cryptographic **SIGNING**

- PlaintextMessage + Signed(Hash(PlaintextMessage))
  - **Hash** = Reduces message to 20 Bytes (2^160th number)
  - **Sign** = Encrypts with a private key that only the corresponding public key can decrypt and verify
- Microsoft signs the Microsoft software proving it is the software from Microsoft…
- X signs Y and Y signs Z -- **Chain of Trust**

CREDENTIALS: X.509 Certificate is a SIGNED attestation of a fact or claim

- Basis for Trust in ALL BANKING WORLDWIDE
- Basis for Trust in Windows and Linux and Web

Seagate

Root of Trust

Hardware that

cannot change

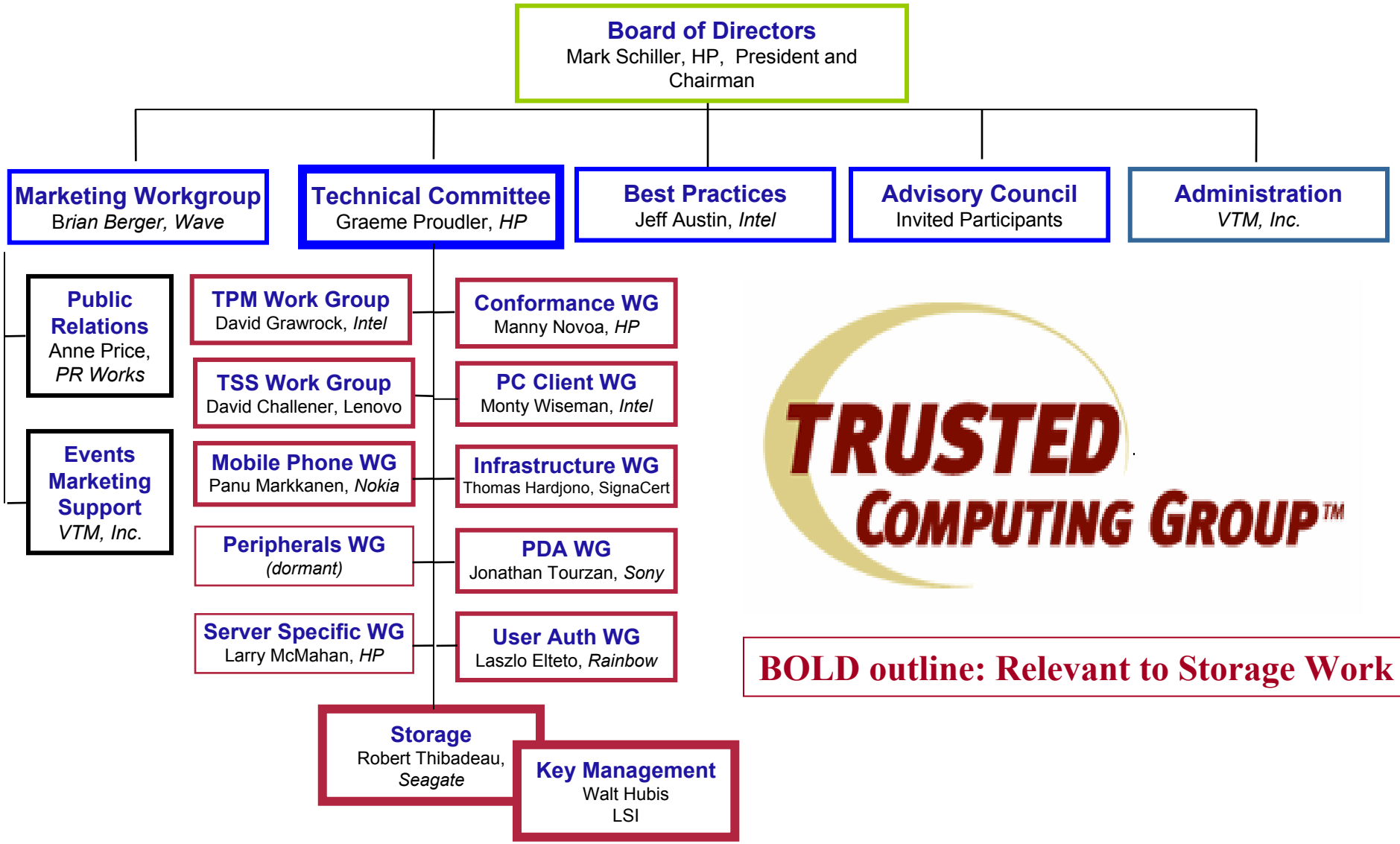
can digitally sign

and therefore can start off a chain of trust.

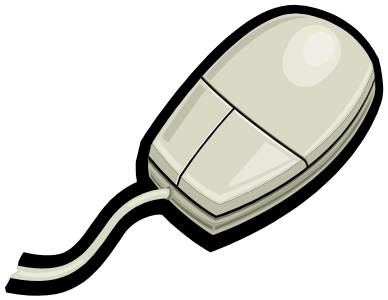
A TPM (trusted platform module) is a tiny processor on the motherboard that can sign and can't have its firmware modified.

Disk Drives can be roots of trust since you can't upload firmware to change them.

Seagate


Board of Directors
Mark Schiller, HP, President and Chairman
Marketing Workgroup
Brian Berger, Wave
Technical Committee
Graeme Proudler, HP
Best Practices
Jeff Austin, Intel
Advisory Council
Invited Participants
Administration
VTM, Inc.
Public Relations
Anne Price, PR Works
Events Marketing Support
VTM, Inc.
TPM Work Group
David Grawrock, Intel
TSS Work Group
David Challener, Lenovo
Mobile Phone WG
Panu Markkanen, Nokia
Peripherals WG
(dormant)
Server Specific WG
Larry McMahan, HP
Conformance WG
Manny Novoa, HP
PC Client WG
Monty Wiseman, Intel
Infrastructure WG
Thomas Hardjono, SignaCert
PDA WG
Jonathan Tourzan, Sony
User Auth WG
Laszlo Elteto, Rainbow
Storage
Robert Thibadeau, Seagate
Key Management
Walt Hubis
LSI
TRUSTED COMPUTING GROUP™
BOLD outline: Relevant to Storage Work
Seagate

Extending Trust to Platform Peripherals

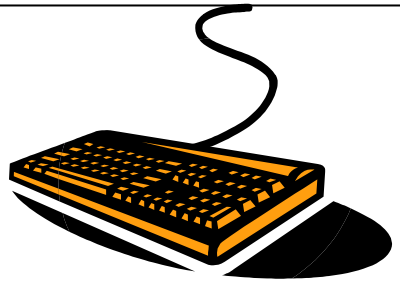


Ability to interact with the Platform

Authentication/Attestation

LOW HIGH

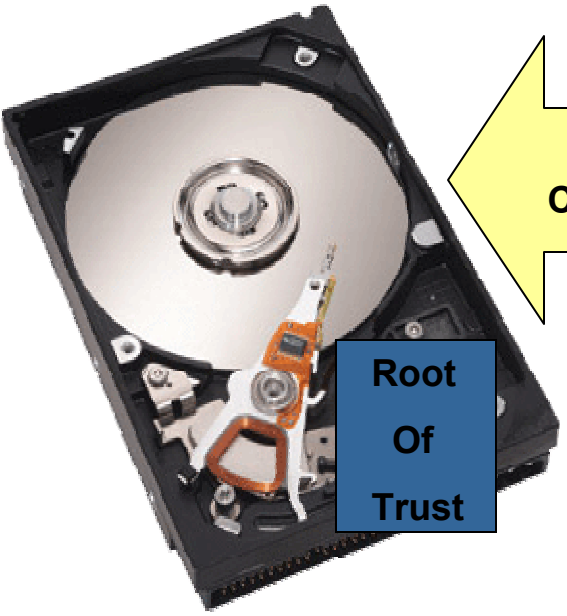
Capability Level



Seagate

Trusted Peripheral with Trusted Platform

Trusted Peripheral



Secure
Communications

Trusted Platform

TPM

Life Cycle: Manufacture, Own, Enroll, PowerUp, Connect, Use, …

Seagate

Joint Work with ISO T10 (SCSI) and T13 (ATA)

TRUSTED SEND/IN

(Protocol ID = xxxx …..)

TRUSTED RECEIVE/OUT

T10/T13 defined the "**container commands**"

TCG/Storage defining the "**TCG payload**"

Protocol IDs assigned to TCG, T10/T13, or reserved

Seagate

TCG Storage WG Specification

SPs (Security Partitions/Providers)

- Logical Groupings of Features
- SP = Tables + Methods + Access Controls

Tables

- Like “registers”, primitive storage and control

Methods

- Get, Set – Commands kept simple with many possible functions

Access Control over Methods on Tables

Seagate

TCG Storage Work Group Use Cases

- **Published Storage WG White Paper and FAQ**
- **Illustrative Subset of Total Storage Device Use Cases**
- **Specification "Solving" Use Cases Expected 1Q/2007**

- **Enrollment and Connection:** trusted relationship – Storage Device and host
- **Protected Storage:** for storing sensitive data
- **Locking and Encryption:** mating SD and host; encrypting stored data
- **Logging:** for forensic purposes
- **Cryptographic Services:** supporting a variety of security services
- **Authorizing Storage Device Feature Sets to Hosts:** trusted/exclusive use
- **Secure Download of Firmware:** trusting firmware upgrades

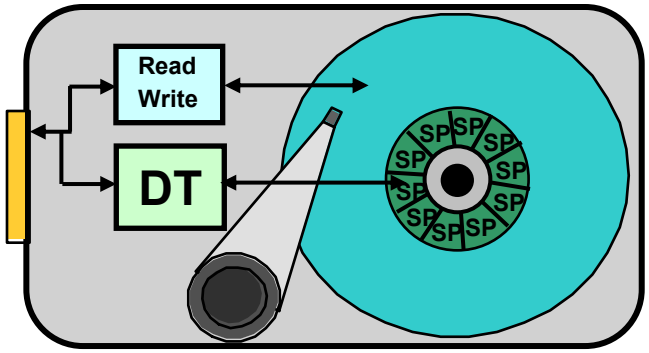
** See https://www.trustedcomputinggroup.org/home/ for Use Case paper and FAQ

Seagate

TCG Security Functions

3 Advantages in HDD's

- Arbitrarily large secrets storage
- Complete CPU for crypto operations
- Custom ASIC logic for high speed



Components:

Secret storage (SP's, or Security Providers)

- Inaccessible to standard Read/Write
- Multiple, separate spaces, each hidden from each other
- Impervious to reformat, OS load, virus attack

Operations (Methods)

- Create, manage, deactivate SP's
- Create, store, retrieve information in SP's
- Perform cryptographic operations – encrypt, decrypt, sign, hash, etc
- Provide services: logging, secure clock, RNG
- All with access control – permiting only authorized operations

Seagate

Applying TCG Protocol - Momentus FDE*

Purposes

- Protect data from exposure due to equipment loss,
- Enable instant, cryptographic erase of drive

TCG Security services provide key management interface

- Key and passwords cryptographically protected on media
- None accessible using ATA READ/WRITE commands
- Strong TCG defined access control governs access to passwords

Closed, permanent encryption device

- Encryption key generated in drive during manufacturing
- Encryption key never leaves drive
- Encryption cannot be turned off

*FDE = Full Disk Encryption

Seagate

www.trustedcomputinggroup.org

THANK YOU!

Seagate