# Trusted Computing Group

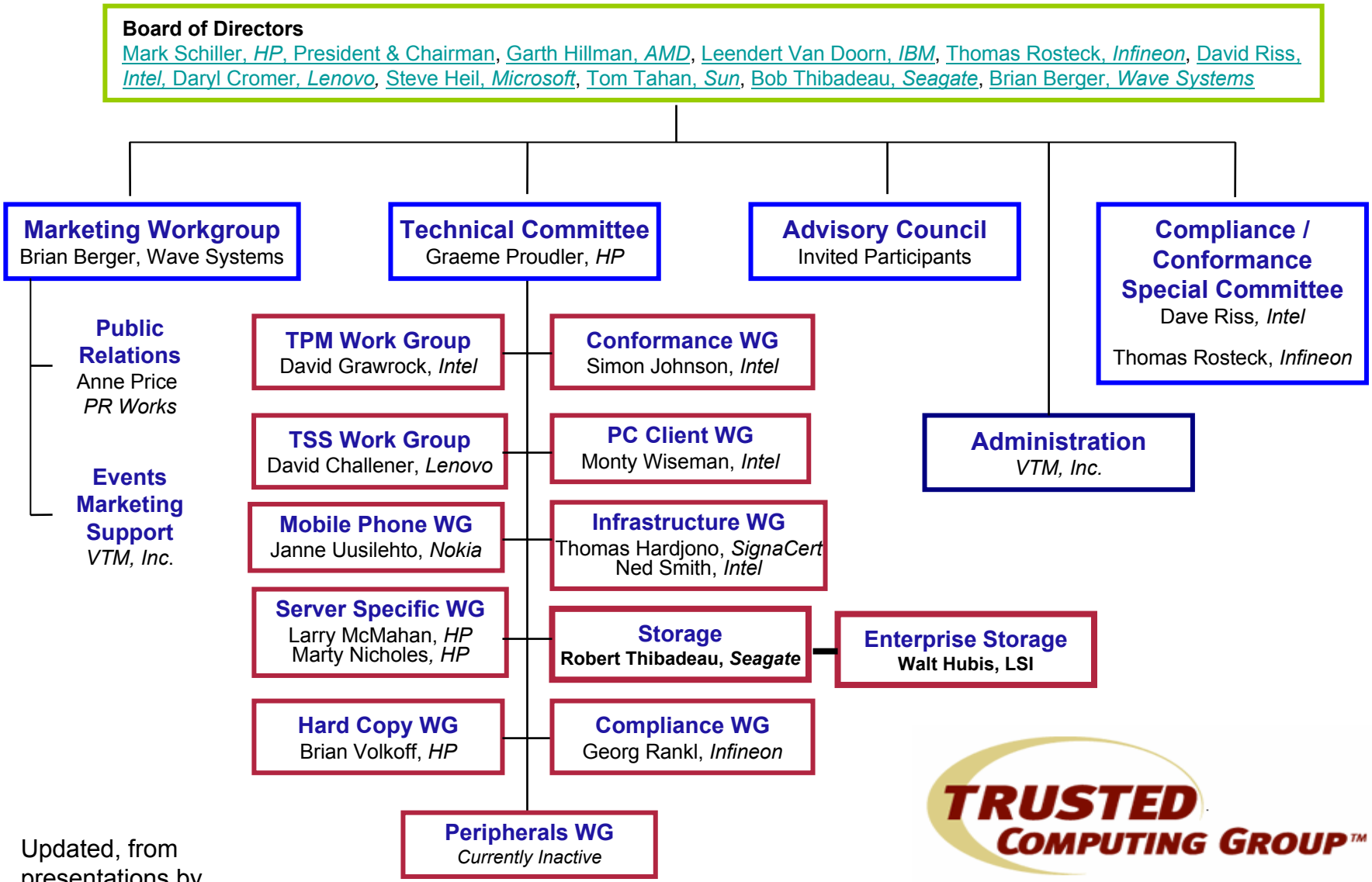
## Liaison Report to T10

September 2006

Mike Fitzpatrick

Fujitsu

# TCG Organization




Updated, from presentations by Bob Thibadeau

# TCG Updates

- Storage WG created Enterprise Storage Sub-group
- 3 new specs for Trusted Network Connect (network access control and endpoint integrity) released:
  - IF-PEP (Policy Enforcement Point) for RADIUS,
  - IFTNCCS (TNC Client Server)
  - IF-T for Tunneled EAP Methods
- Mobile Specs released at CTIA (13 Sept)

# Storage WG

- Storage WG has 3 scheduled conference calls:
  - Bi-wkly Wed 11am-12pm MT for Enterprise Storage
  - Wkly Thurs 3-4pm ET for business & liaison
  - Wkly Fri 11am-1pm ET for spec review
- Have to be a TCG member to participate
- Documents made public when development completes:
  - See https://www.trustedcomputinggroup.org/specs/ for documents already made public
  - See https://www.trustedcomputinggroup.org/groups/storage/ for Storage Use Cases and FAQs

# Storage WG Updates

- Storage WG F2F in July (w T10), Aug, Sept, Oct
  - Performed GAP Analysis on Core Specification
  - Performed updates/reviews on Core Spec
    - Core Spec defines contents of Security Protocol In & Out for the first TCG code point in the Security Protocol field
  - Spec Completion (WG approval)
    - Anticipated by end of September 2006
  - Other TCG processes (including 60 day IP review) must then be completed before publication
    - Anticipated by end of December 2006

# Backup Material

Previously presented to T10

Repeated here for reference

# TCG Mission

Develop and promote open, vendor-neutral, industry standard specifications for trusted computing building blocks and software interfaces across multiple platforms

from presentations
by Bob Thibadeau

# Vision (Goal Constraints)

- Internet-connected devices will always have untrusted activities going on inside of them, so …
- Create internal trustable sub-units and secure paths … the building blocks, so …
- In the future, you (IT) can know the trusted subsystem won't be compromised even if exposed to Internet (and limited physical) attacks (or accidents).

# What is Trust? – it does what was intended to do. The ONLY answer we have to this, is to have the publisher/manufacturer sign.

- It is 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**
- An X.509 Certificate is a cryptographically SIGNED attestation of a fact or claim.
  - Basis for Trust in ALL BANKING WORLDWIDE
  - Basis for Trust in Windows and Linux and Web

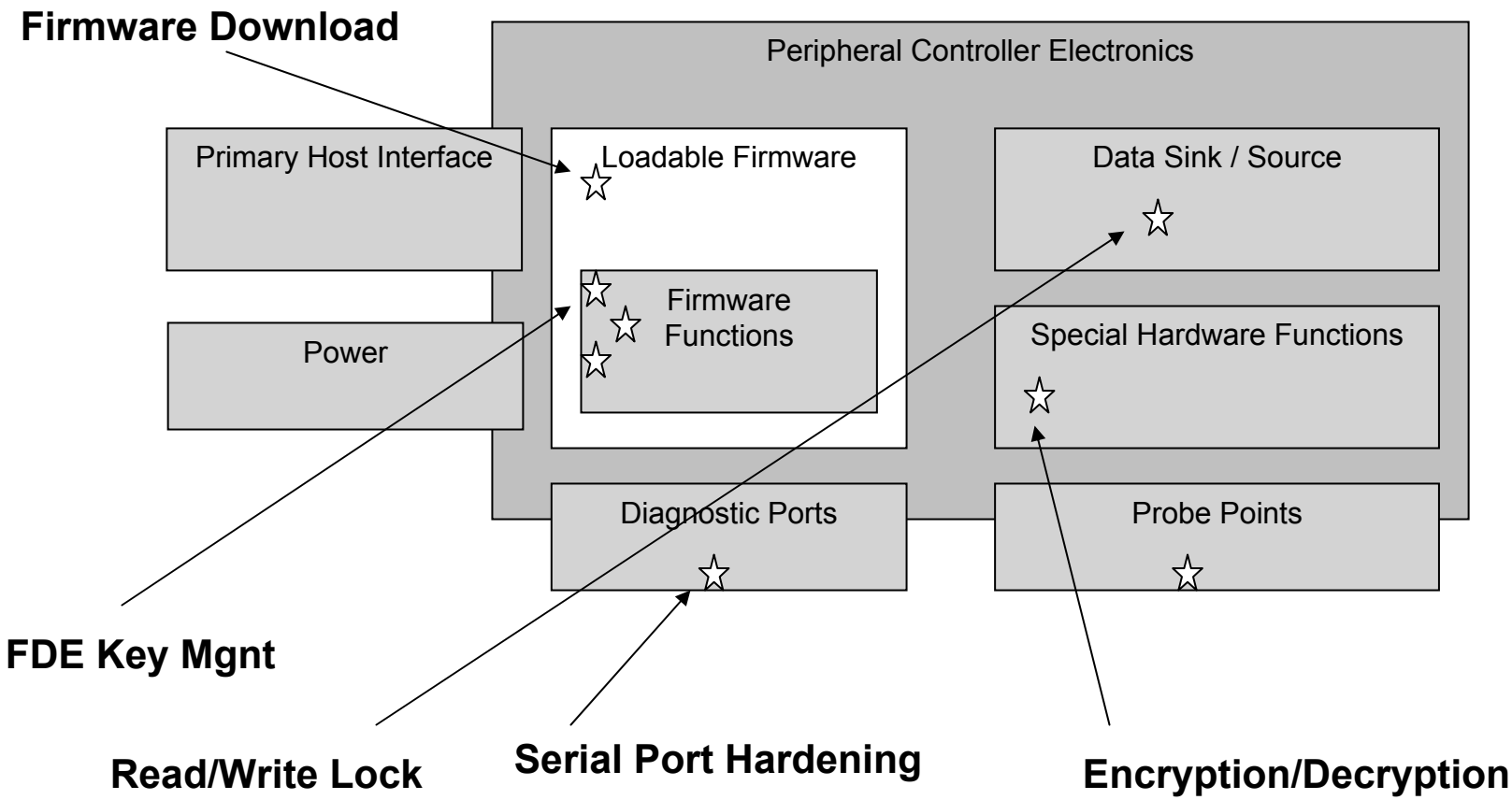
# Example Use Case

- Attached Storage device is stolen **not for the data on it**, but **for the device itself**.
  - Devices are ***more*** valuable if they ‘turn into bricks” if they are stolen.
  - (Obviously, not to the Thief! – But then he didn’t pay!)

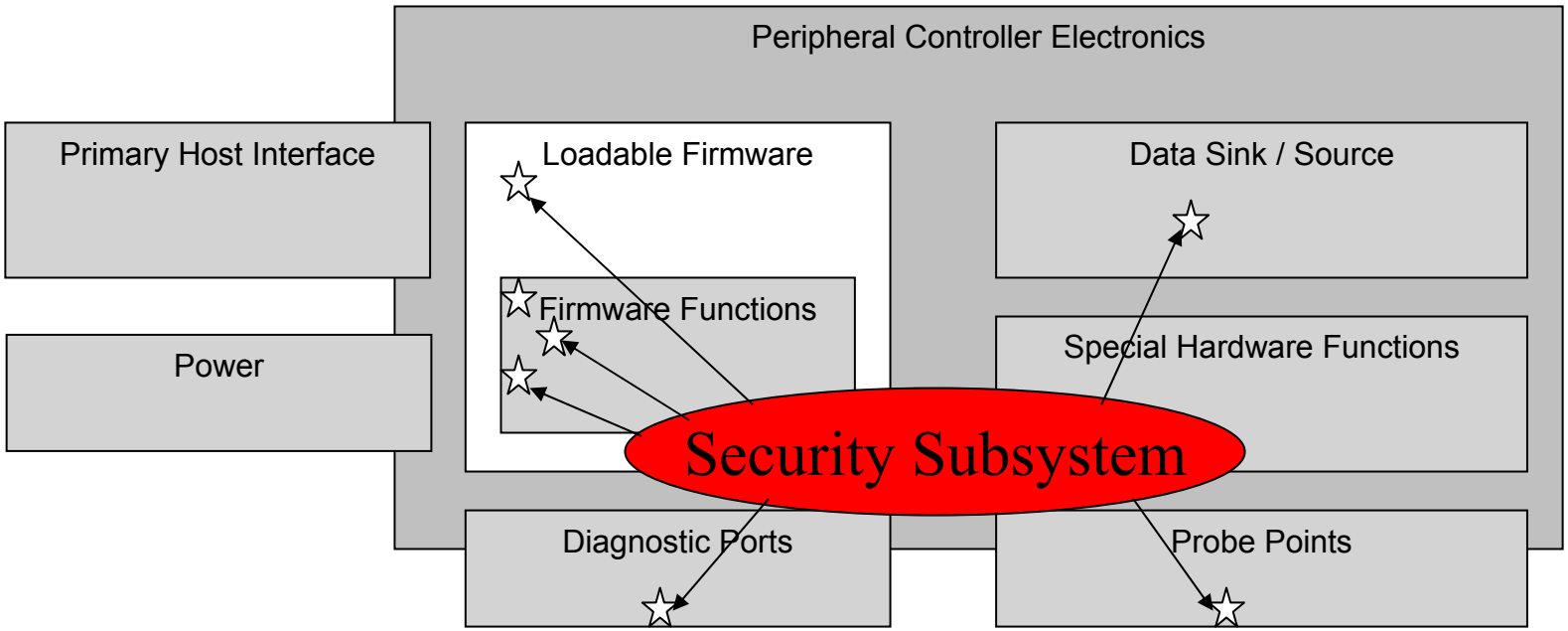
- Phone SIM Card Analogy:
  - The secret that performs the security association is hidden from the user.

# Storage Device Threat Model and Solution

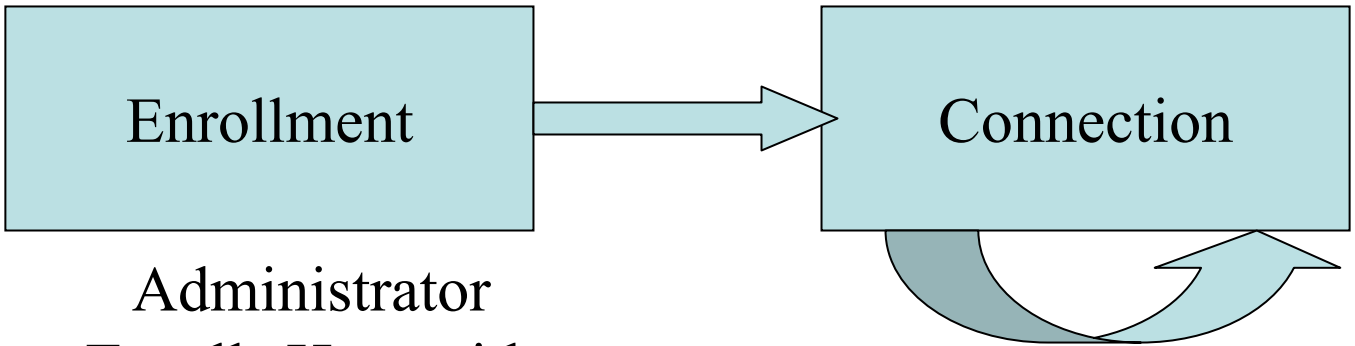
## Versatile (Policy Driven) Access Control over Drive Features



# Access Control over Points of Vulnerability



# Stepped Security for Ease of Use




Administrator Enrolls Host with Drive

TPM and Drive Automatically Connect because of Shared Secret, or Public Key

These are both just setting up and using access controls

# IDF Demo: Seagate – Intel – Wave Systems

**Drive Refuses to READ/WRITE unless sees proof of knowledge.**