06-240r0

Trusted Computing Group Liaison Report to T10 5/06

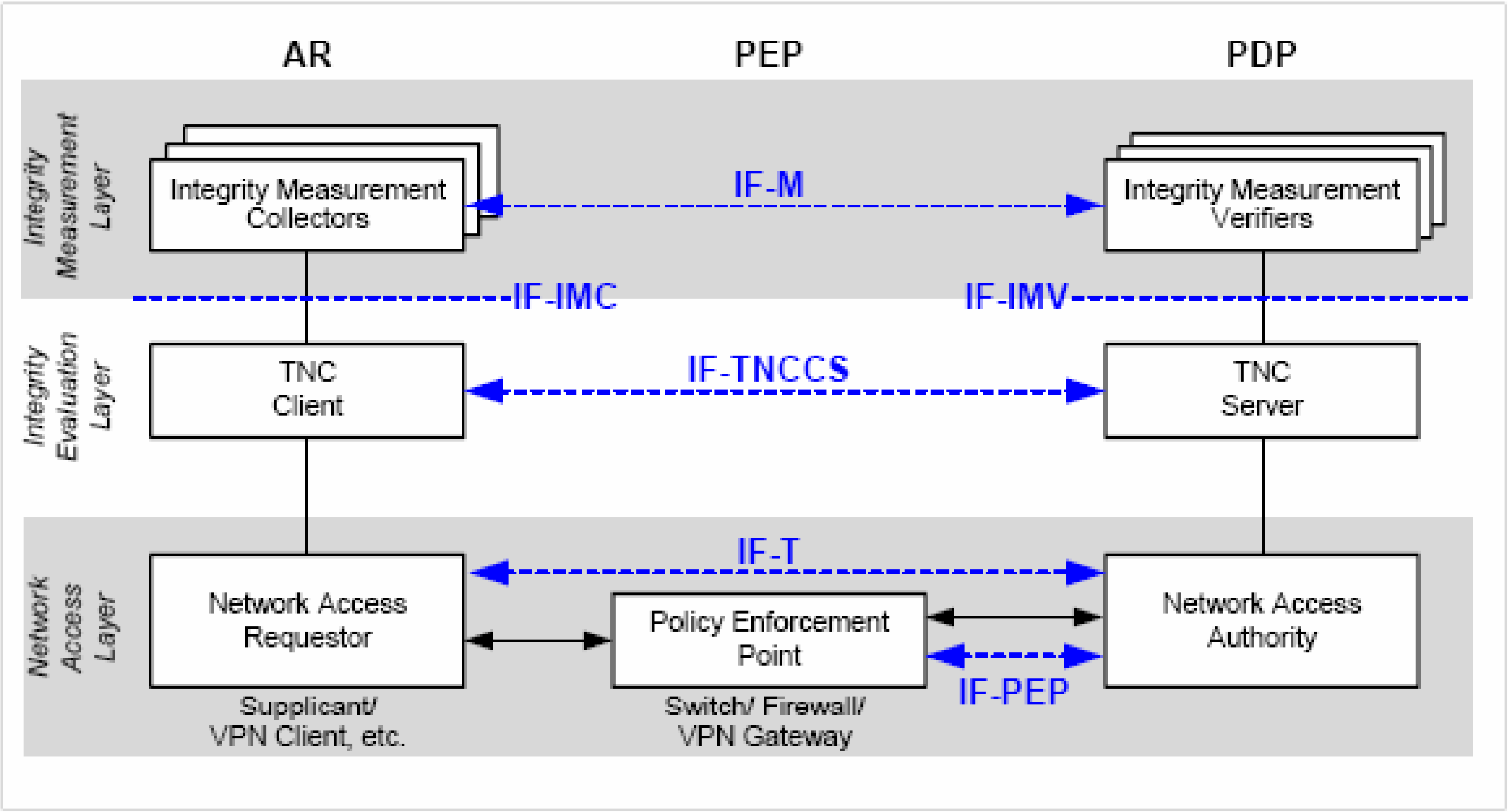
Roger Cummings

Symantec

TCG Status

- 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
- Interop testing performed at UNH

TNC Architecture


AR
PEP
PDP
Integrity Measurement Layer
Integrity Measurement Collectors
IF-M
Integrity Measurement Verifiers
IF-IMC
IF-IMV
Integrity Evaluation Layer
TNC Client
IF-TNCCS
TNC Server
Network Access Layer
IF-T
Network Access Requestor
Policy Enforcement Point
Network Access Authority
IF-PEP
Supplicant/ VPN Client, etc.
Switch/ Firewall/ VPN Gateway

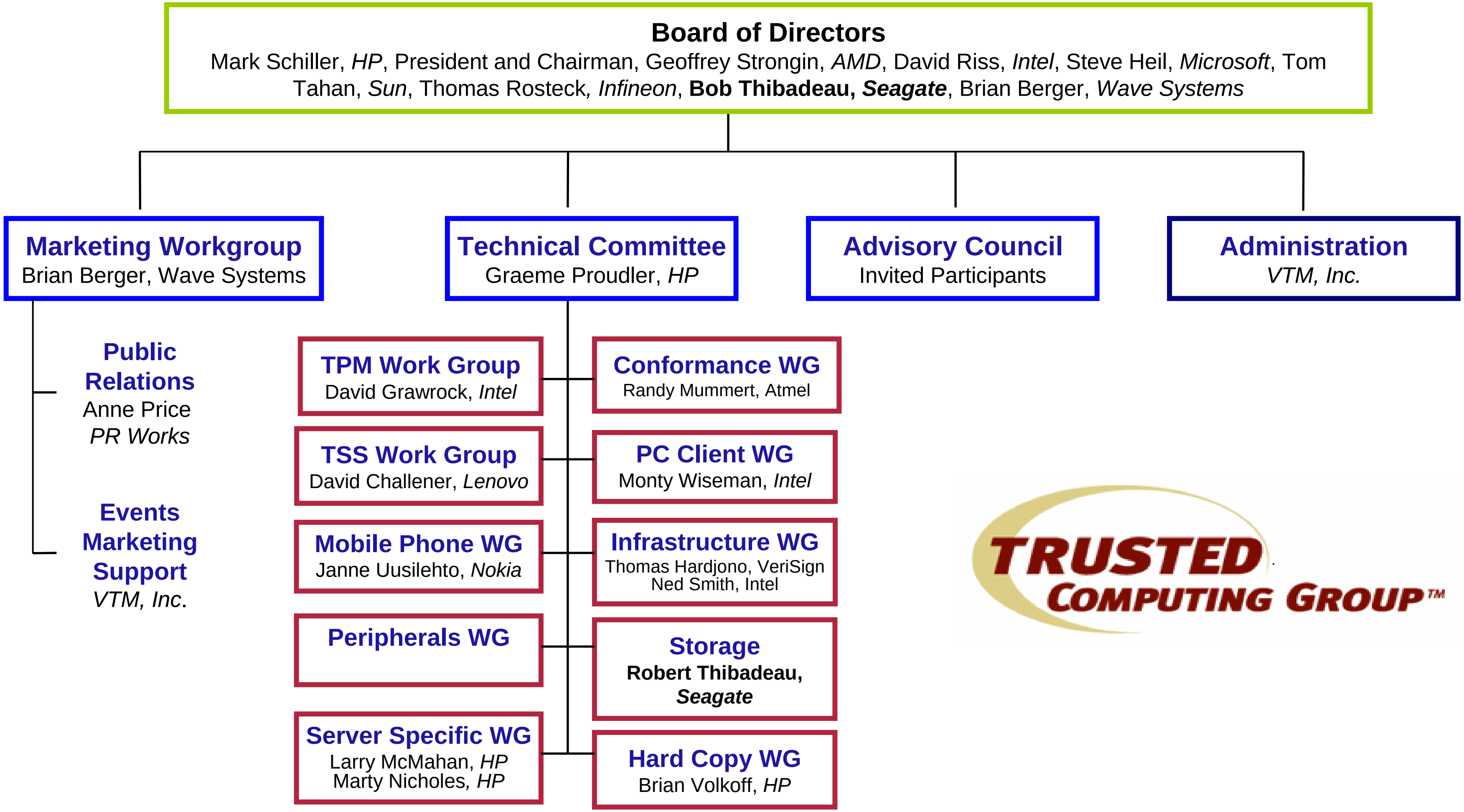
Storage WG Status

- Storage WG met f2f on Monday this week in this hotel
  - Performed comment triage on core spec
    - Core spec defines contents of Security Protocol In & Out for the first TCG code point in the Security Protocol field
  - Reviewed document restructuring
  - Spec Completion date in TCG now end of August 2006
  - Several TCG processes (incl 60 day IP review) must be completed after that date before publication

Following slides…..

- Are taken from two presentations by Bob Thibadeau given at
  - – SNW Spring 2006
  - – Network Storage Las Vegas

TCG Organization



Board of Directors

Mark Schiller, *HP*, President and Chairman, Geoffrey Strongin, *AMD*, David Riss, *Intel*, Steve Heil, *Microsoft*, Tom Tahan, *Sun*, Thomas Rosteck*, Infineon*, **Bob Thibadeau, *Seagate***, Brian Berger, *Wave Systems*

Marketing Workgroup
Brian Berger, Wave Systems

Technical Committee
Graeme Proudler, *HP*

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
Janne Uusilehto, *Nokia*

Peripherals WG

Server Specific WG
Larry McMahan, *HP*
Marty Nicholes*, HP*

Conformance WG
Randy Mummert, Atmel

PC Client WG
Monty Wiseman, *Intel*

Infrastructure WG
Thomas Hardjono, VeriSign
Ned Smith, Intel

Storage
Robert Thibadeau,
Seagate

Hard Copy WG
Brian Volkoff, *HP*

TRUSTED COMPUTING GROUP™

TCG Mission

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

Vision (Goal Constraints)

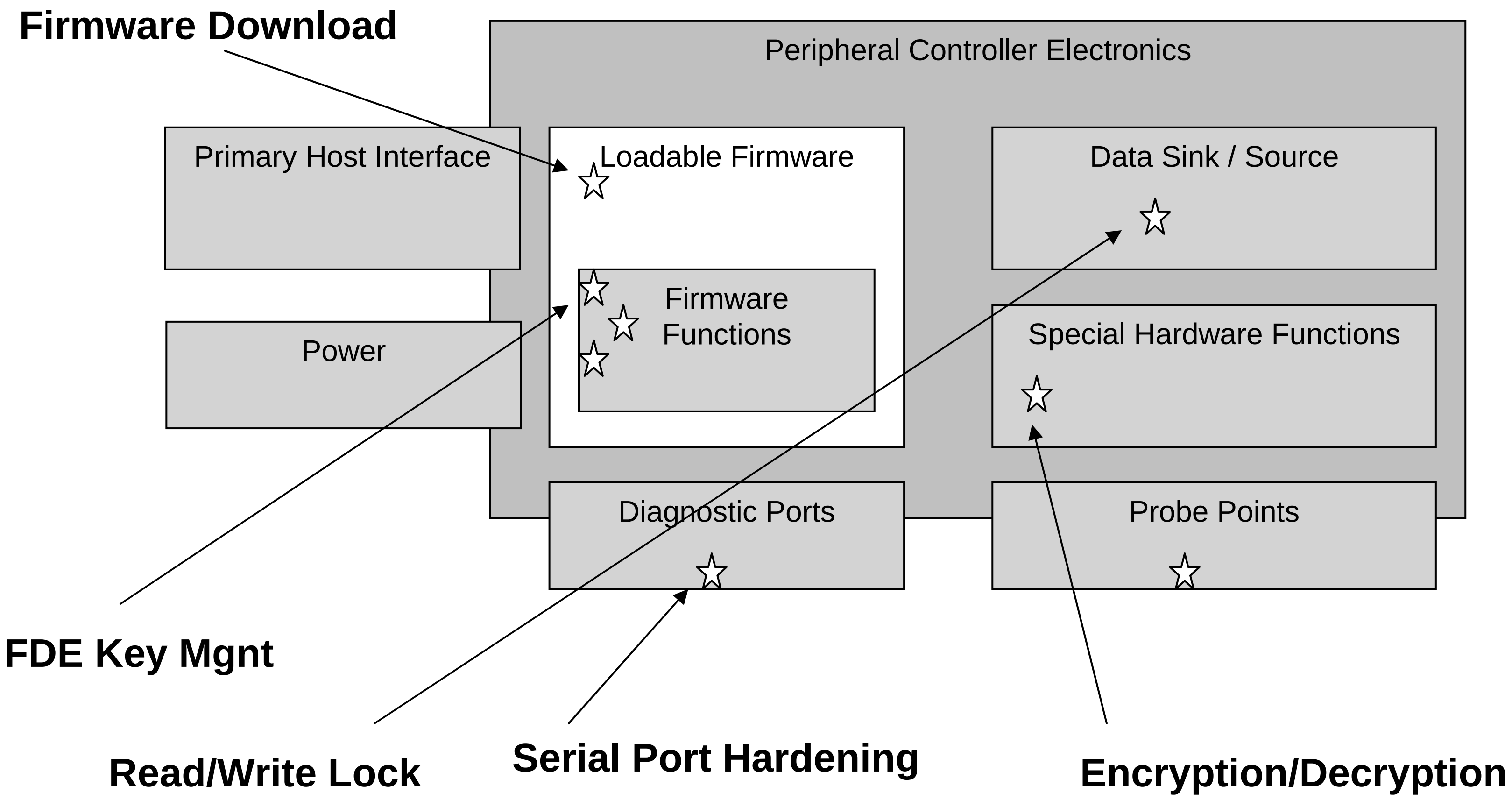
- Internet-connected devices will always have untrusted activities going on inside of them, so …
- Create internal trustable sub-units and secure paths … the building blocks, so …
- In the future, you (IT) can know the trusted subsystem won’t be compromised even if exposed to Internet (and limited physical)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

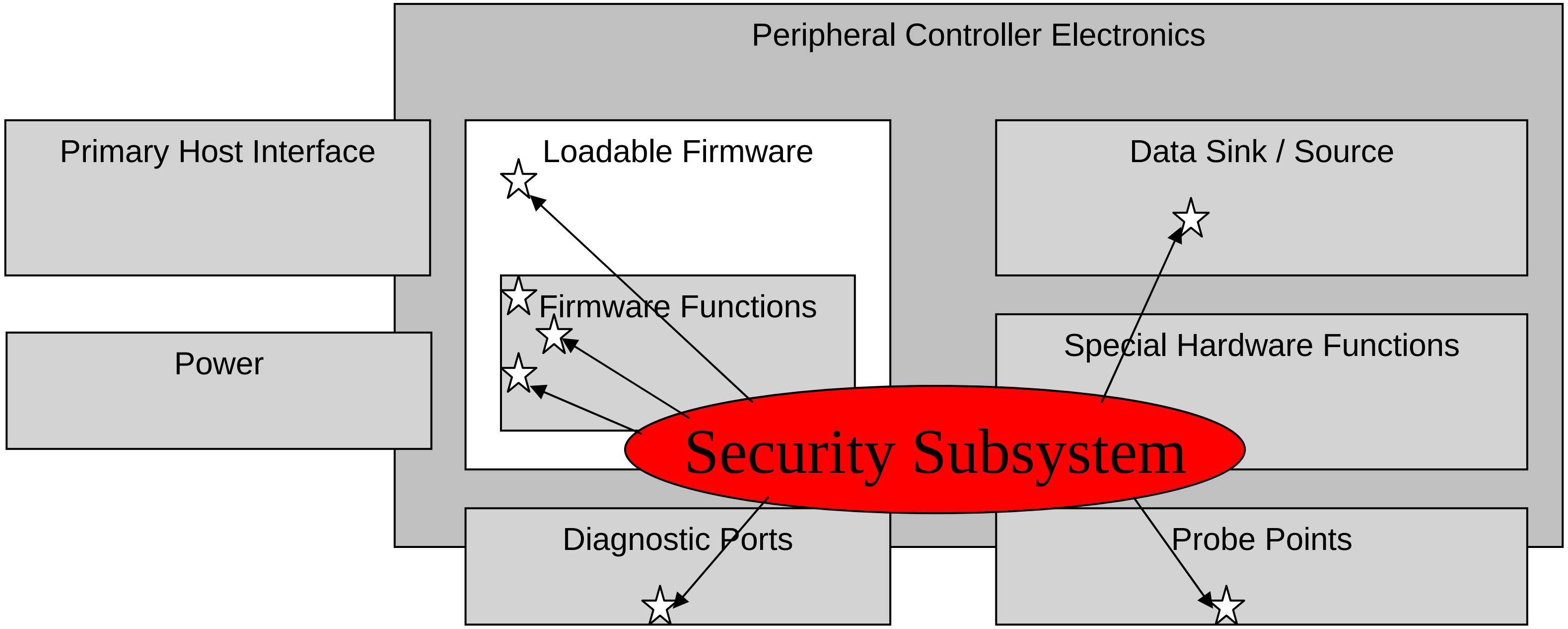
- It is cryptographic SIGNING
  - PlaintextMessage + Signed(Hash(PlaintextMessage))
    - Hash = Reduces message to 20 Bytes (2^160th number)
    - Sign = Encrypts with a private key that only the corresponding public key can decrypt and verify
  - Microsoft signs the Microsoft software proving it is 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

Storage Device
Threat Model and Solution

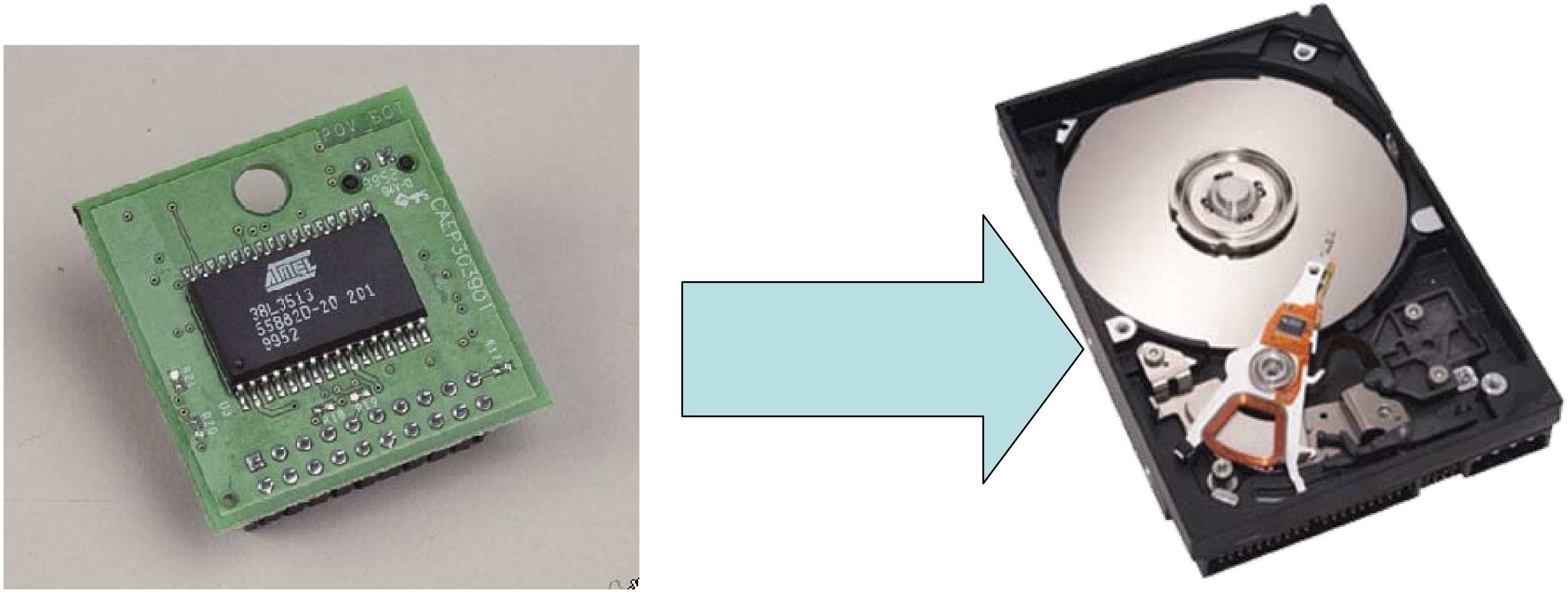
Versatile (Policy Driven) Access Control over Drive Features



Access Control over Points of Vulnerability

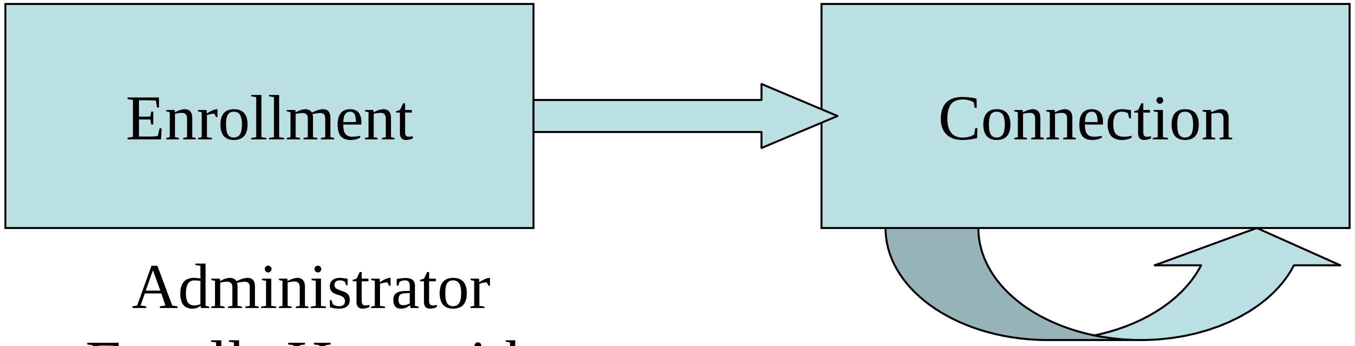


TPM *can* be used to Securely Control Drive Features



Drives do NOT have onboard TPMs

Stepped Security for Ease of Use



Enrollment

Connection

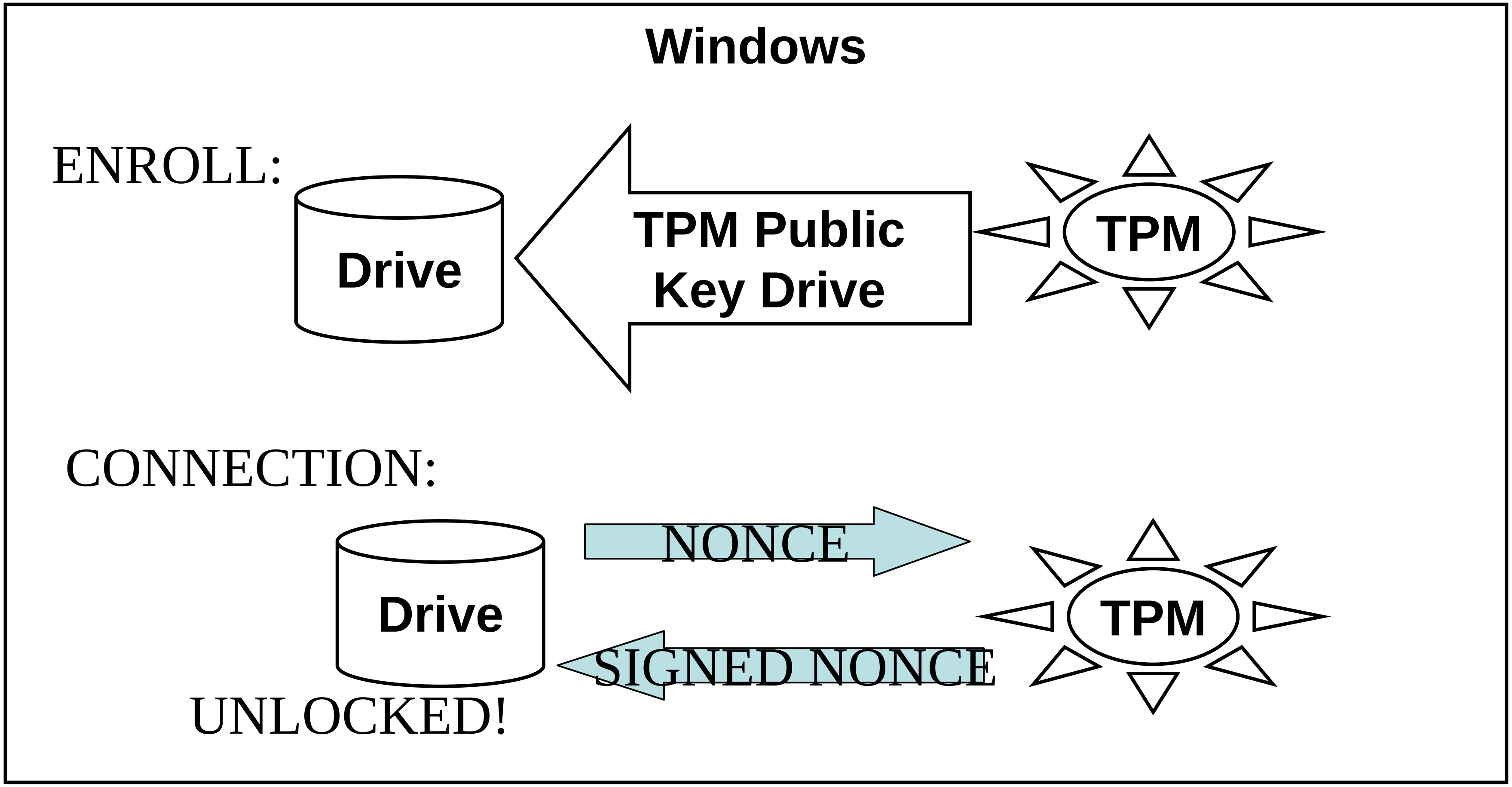
Administrator Enrolls Host with Drive

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

These are both just setting up and using access controls

Spring ‘05 IDF Demo Seagate – Intel – Wave Systems

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



Windows

ENROLL:

Drive

TPM Public Key Drive

TPM

CONNECTION:

Drive

NONCE

SIGNED NONCE

TPM

UNLOCKED!

Future Meetings

- Storage WG has 2 weekly conference calls:
  - Thursday 2-3pm Eastern for business & liaison
  - Friday 12-1pm 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
  - Specifically see https://www.trustedcomputinggroup.org/groups/storage/ for Storage Use Cases an FAQ