Trusted Computing Platform Alliance

–

Introduction and Technical Overview

–

Joe Pato

HP Labs

MIT 6.805/6.857

17 October 2002

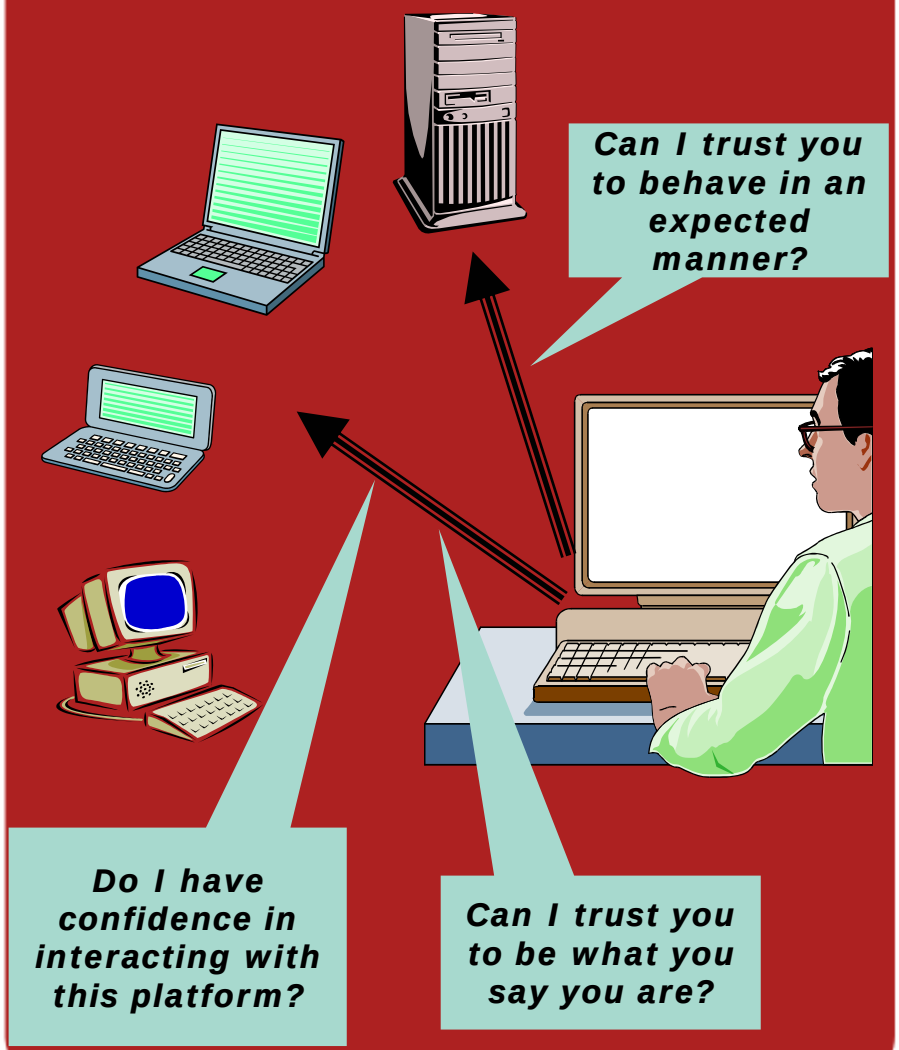
Why Trusted Computing Platforms?

- Increase consumer and businesses confidence

- Reduce business risks
  - by enabling trust in the behavior of critical information systems

- Protect end-user private data
  - by enabling trust in end systems behavior

Trusted Computing Platform properties



- Recognize that a platform has known properties
  - Mobile platform access to corporate network.
  - Remote Access via known public access point.
- Identify that a system will behave as expected:
  - Mobile access to corporate network with firewall and antivirus requirements.
  - Outsourced platform administration
- Enable a user to have more confidence in the behavior of the platform in front of them
  - Trust a platform to handle my private data I.e banking, medical…etc…
  - Achieving WYSIWYS: What You Sign Is What You See…

The Trusted Computing Platform Alliance

- TCPA -

AKA???

The Conspiracy in Prelude to Apocalypse

How?

The Cleverly Parboiled Amphibian

The Trusted Computing Platform Alliance

- TCPA -

- An Industry work group focused on defining and advancing the concept of Trusted Computing

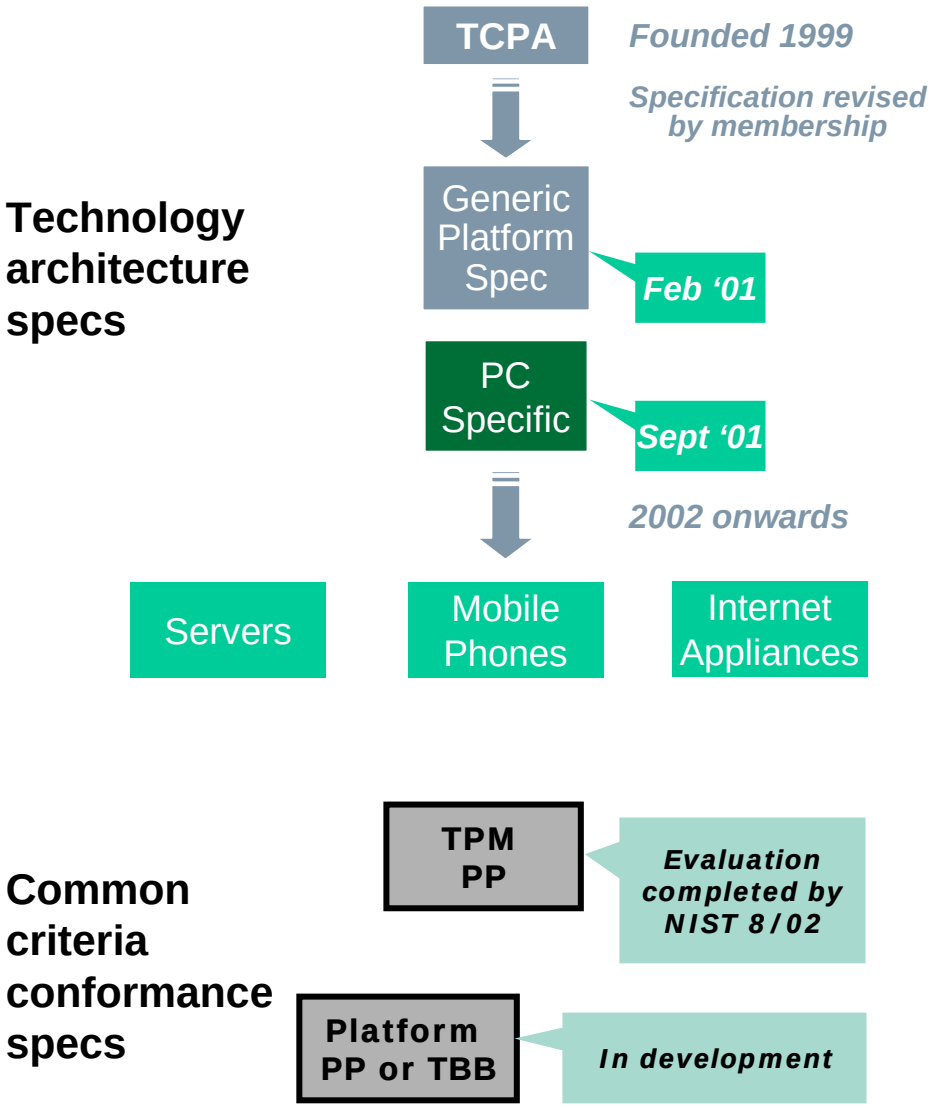
- Founded in 1999 by Compaq, HP, IBM, Intel, and Microsoft.

- 180+ members from the hardware, software, communications, and security technology industries

- Provide a ubiquitous and widely adopted means to address trustworthiness of computing platforms
- Publish an open specification for public review – Not security by obscurity
- Define a technology specification that can be applied to any type of computing platform (not just PCs!)

The TCPA charter

TCPA specification activity



TCPA concepts

- Definition:

  A platform can be trusted if it behaves in the expected manner for the intended purpose

- TCPA technology provides mechanisms for:

  – Platform Authentication and Attestation

    - Identify the platform and its properties to a challenging party

  – Platform Integrity Reporting

    - Reliably measure and report on the platform's software state

  – Protected Storage

    - Protect private and secret data. Protect integrity and identity information against subversion

How does TCPA achieve this?

The TCPA architecture relies on the concept of a Root of Trust

- **A third party can rely on information provided by a platform's Root of Trust**
- **The root of trust must be able to report on software that has executed**
- **The root of trust must be able to keep secrets from the rest of the platform**

⇒ measure the first piece of code that executes when the platform boots
⇒ independent computing engine
⇒ "secret" storage

Two Roots of Trust: Measurement, Reporting

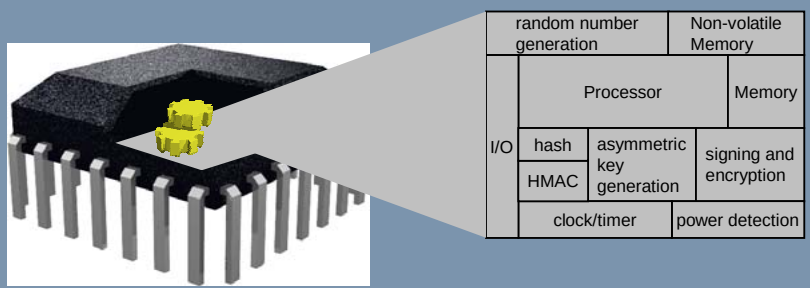
- A Root of Trust for Reporting
  - The component that can be trusted to store and report reliable information about the platform

- A Root of Trust for Measurement
  - The component that can be trusted to reliably measure and report to the Root of Trust for reporting what software executes on platform boot

- It is necessary to trust these Roots of Trust for TCPA mechanisms to be relied upon

  => Conformance and Certification

The Trusted Platform Module - TPM -



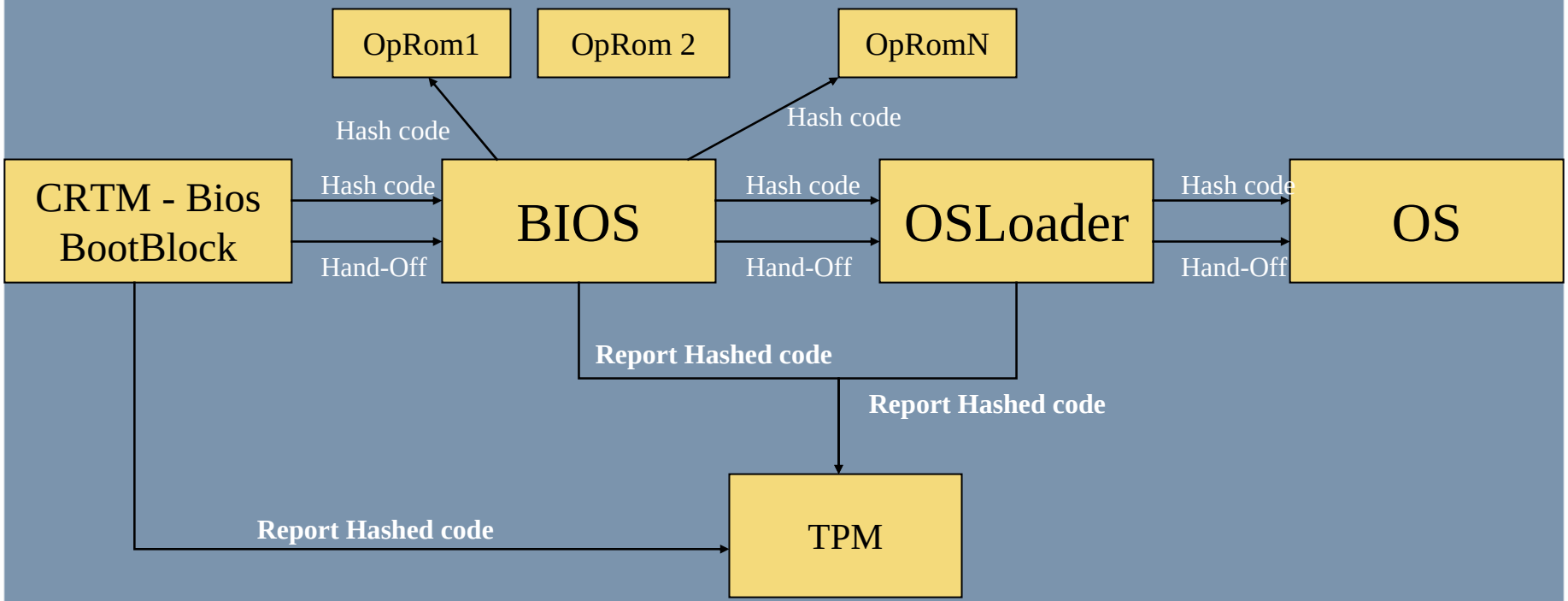
- The TPM is the Root of Trust for Reporting
  - Think: smartcard-like security capability embedded into the platform
  - The TPM is uniquely bound to a single platform
  - TPM functions and storage are isolated from all other components of the platform (e.g., the CPU)

The Core Root of Trust for Measurement - CRTM -

- The CRTM is the first piece of code that executes on a platform at boot time. (I.e. Bios or Bios BootBlock in an IA-32 platform)
  - It must be trusted to properly report to the TPM what software executes after it.
  - Only authorized entities must be able to reflash the CRTM… (those that vouch for its behavior)

CRTM and TPM during the boot process

The Authenticated boot process



TCPA feature-set

- Platform authentication
- Integrity Reporting
- Protected Storage

Platform Authentication

- TCPA provides for the TPM to have control over "**multiple pseudonymous** attestation identities"

- **TPM attestation identities** do not contain any owner/user related information

  => A **platform** identity attests to **platform** properties

- No single TPM "identity" is ever used to digital sign data

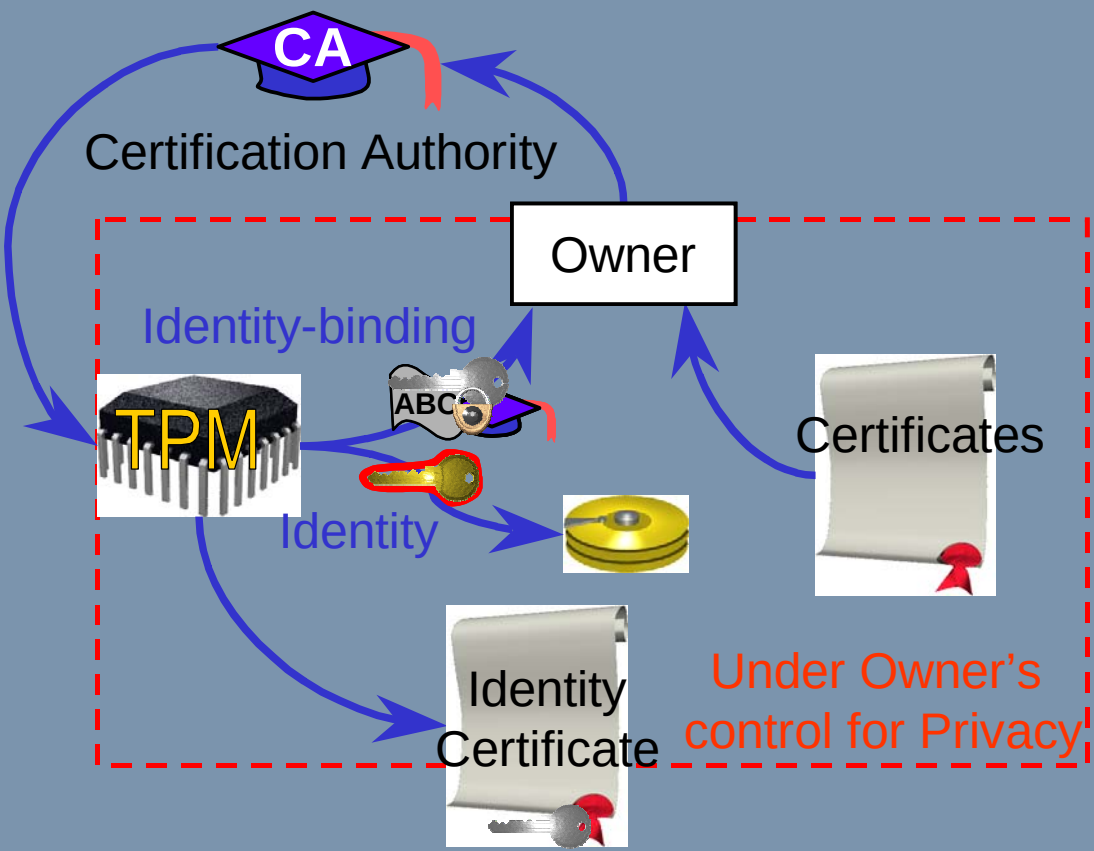
  => **privacy protection**

- TPM Identity certification is required to attest to the fact that they identify a genuine TCPA platform

- The TPM Identity creation protocol allows for to choose different Certification Authorities (Privacy-CA) to certify each TPM identity

  => prevent correlation

Generating an identity



- Measurements reported to the TPM during (and after) the boot process can not be removed or deleted until reboot

  => No hiding code that has executed on the platform

- The TPM will use an attestation identity to sign the integrity report

- The recipient of integrity information can evaluate trustworthiness of the information based on the certificate of attestation identity

  ➞ Trust that the TPM is a genuine TPM on a genuine Trusted Platform

Integrity Reporting

Integrity Reporting (2)

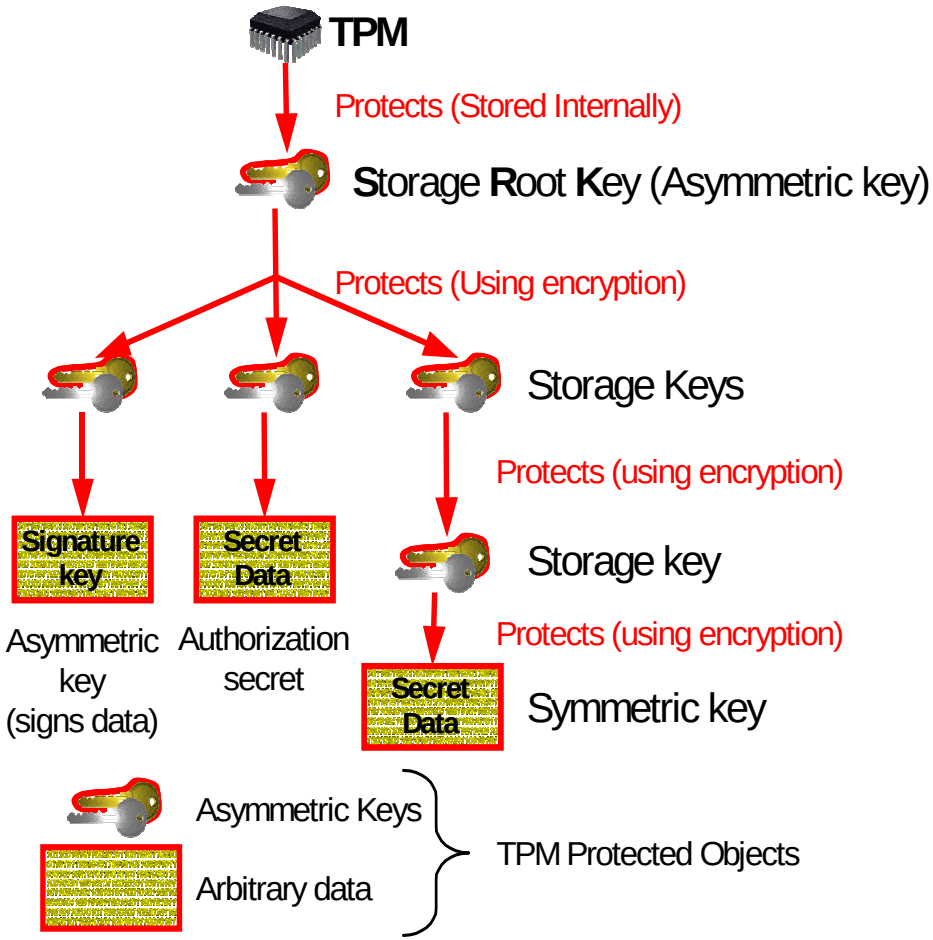
- The recipient of reporting information relies on “signed certificates” that attest that a given measurement represents a known piece of code
  - Cert(Phoenix BIOS v1.2 has hash value of H)
  - Cert(CorpIT config, combined hash value)
- The recipient can verify these Integrity Metrics Certificates and compare certified metrics to reported metrics
  - ➞ Trust that the reported metrics correspond to certified software

Trusting the reported software is dependent on the recipient’s policy, for a given application context

Protected Storage

- No generic encryption device – no export control pb
- Cryptographic keys can be created that are protected by the TPM
- Data can be encrypted using the TPM, that can only be decrypted using this same TPM
- A specific software configuration can also be specified, that will be required for the TPM to allow data to be decrypted, or keys to be used
  - ➞ This is called Sealing: parameters define which Integrity Metrics the data should be sealed to

Protected Storage Hierarchy



Privacy-positive design

- Notion of TPM Owner, think Platform Administrator
- Ultimate TPM functionality control goes to the Owner
- TPM Activation controlled by the Owner, and deactivation available to the User
- No single TPM “identity” is ever used to digitally sign data
- Multiple pseudonymous IDs (limits correlation)
- Remote control of the TPM enabled by challenge response protocols for authorization mechanisms
- Can prevent the revelation of secrets unless the software state is in an approved state

About Conformance

- Common Criteria based
- TCPA:
  - TPM Protection Profile completed
  - Platform Protection Profile to include CRTM and connection to platform
- Manufacturers role
  - Create Security Target, and produce product design evaluation

Short term TCPA benefits – protected storage

(Platform with a TPM, associated software provided by the TPM manufacturer)

Customers can encrypt the data on their hard disks in a way that is much more secure than software solutions.

- The TCPA chip is a portal to encrypted data.
- Encrypted data can then only ever be decrypted on the same platform that encrypted it.
- TCPA also provides for digital signature keys to be protected and used by the embedded hardware chip

Middle term TCPA benefits – integrity checking

(Short term solution plus additional software)

Protection against hacker scripts, by automatically preventing access to data if unauthorised programs are executed.

- TCPA provides for the measurement of integrity metrics of the software environment on the TCPA platform.
- Allows for a remote party to verify what the software environment on a TCPA platform is.
- The TCPA chip can then be used to encrypt data to disk so that this data can only ever be decrypted on that same platform, and ONLY if the platform has a given set of software environment integrity metrics.

Long term TCPA benefits – e-commerce

Customers and their partners/suppliers/customers can connect their IT systems and expose only the data that is intended to be exposed.

- TCPA is designed so that platform identities and Integrity Metrics can be proven reliably to previously unknown parties.

- Secure online discovery of platforms and services: confidence in the information about the software environment and identity of a remote party, enabling higher levels of trust when interacting with this party.

and now

Palladium

For more information

- The Book
  - "Trusted Computing Platforms: TCPA technology in context" By Boris Balacheff, Liqun Chen, Siani Pearson, David Plaquin, and Graeme Proudler
  - Order at **www.hp.com/hpbooks**

- The "hairy" TCPA specification at www.trustedcomputing.org

- HPLabs Trusted Systems Lab

joe.pato@hp.com