ProCurve Networking
HP Innovation

Trusted Computing Overview

Paul Congdon [paul.congdon@hp.com]
ProCurve Networking by HP

With the help from…

Boris Balacheff [boris.balacheff@hp.com]
HP Security Office
Trusted Systems Lab, HPLabs, Bristol

hp invent

What are the components of the DevID PAR Proposal?

ProCurve Networking
HP Innovation

- Definition of a unique per-device identifiers (DevID)
- Provisioning the DevID
- Maintaining the DevID on the device
- Using the DevID to establish a “chain of trust”
- Methods of authenticating a device with a DevID
- Other steps…

What must 802.1 define and what can be leveraged?

The Trusted Computing Group

ProCurve Networking
HP Innovation

Board of Directors
Jim Ward, *IBM*, President and Chairman, Geoffrey Strongin, AMD, Mark Schiller, HP, David Riss, Intel, Steve Heil, Microsoft, Tom Tahan, Sun, Nicholas Szeto, Sony, Bob Thibadeau, Seagate, Thomas Hardjono, Verisigin

Marketing Workgroup
Nancy Sumrall, *Intel*

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, *IBM*

Mobile Phone WG
Panu Markkanen, *Nokia*

Peripherals WG
Jim Wendorf, *Philips*

Server Specific WG
Larry McMahan, *HP*

Storage Systems
Robert Thibadeau, *Seagate*

Conformance WG
Manny Novoa, *HP*

PC Client WG
Monty Wiseman, *Intel*

Infrastructure WG
Thomas Hardjono, Verisign

PDA WG
Jonathan Tourzan, *Sony*

User Auth WG
Laszlo Elteto, *Rainbow*

Hardcopy
(TBD), Temp-chair, *HP*

Position Key

GREEN Box:	*Elected Officers*
BLUE Box:	*Chairs Appointed by Board*
RED Box:	*Chairs Nominated by WG, Appointed by Board*
BLACK Box:	*Resources Contracted by TCG*

TRUSTED COMPUTING GROUP™

TCG Membership

ProCurve Networking
HP Innovation

Promoter
AMD
Hewlett-Packard
IBM
Intel Corporation
Microsoft
Sony Corporation
Sun Microsystems, Inc.

Adopter
Ali Corporation
American Megatrends, Inc.
Enterasys Networks
Foundry Networks Inc.
Foundstone, Inc.
Gateway
Industrial Technology Research Institute
MCI
Nevis Networks, USA
OSA Technologies
Senforce Technologies, Inc
Silicon Integrated Systems Corp.
Softex, Inc.
Toshiba Corporation
ULi Electronics Inc.
Winbond Electronics Corporation

Contributor
Agere Systems
ARM
ATI Technologies Inc.
Atmel
AuthenTec, Inc.
AVAYA
Broadcom Corporation
Certicom Corp.
Comodo
Dell, Inc.
Endforce, Inc.
Ericsson Mobile Platforms AB
Extreme Networks
France Telecom Group
Fujitsu Limited
Fujitsu Siemens Computers
Funk Software, Inc.
Gemplus
Giesecke & Devrient
Hitachi, Ltd.
Infineon
InfoExpress, Inc.
iPass
Juniper Networks
Lenovo Holdings Limited
Lexmark International
M-Systems Flash Disk Pioneers
Meetinghouse Data Communications
Motorola Inc.
National Semiconductor
nCipher

Contributor
Network Associates
Nokia
NTRU Cryptosystems, Inc.
NVIDIA
Philips
Phoenix
Pointsec Mobile Technologies
Renesas Technology Corp.
RSA Security, Inc.
SafeNet, Inc.
Samsung Electronics Co.
SCM Microsystems, Inc.
Seagate Technology
SignaCert, Inc.
Silicon Storage Technology, Inc.
Sinosun Technology Co., Ltd.
Standard Microsystems Corporation
STMicroelectronics
Sygate Technologies, Inc.
Symantec
Symbian Ltd
Synaptics Inc.
Texas Instruments
Transmeta Corporation
Trend Micro
Utimaco Safeware AG
VeriSign, Inc.
Vernier Networks
VIA Technologies, Inc.
Vodafone Group Services LTD
Wave Systems
Zone Labs, Inc.

The Trusted Computing Group: recent evolutions

ProCurve Networking
HP Innovation

TCG uses majority voting

TCG has RAND IP policy

TCG is addressing all types of computer platform

TCG is starting to address the entire platform

TCG is starting to address platform interactions

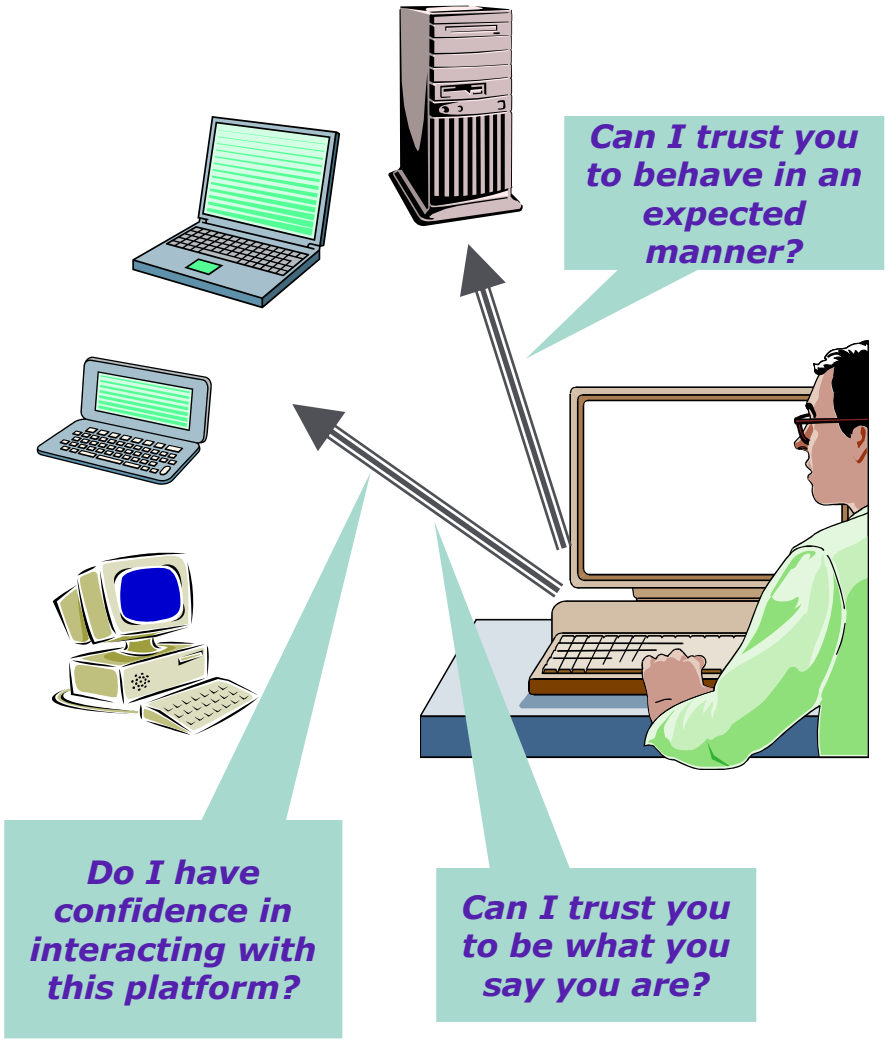
Introducing Trusted Platform Mechanisms….

ProCurve Networking
HP Innovation

TCG mechanisms for:

- Platform Authentication
  - Identify a physical platform and its physical properties to a challenging party
- Platform state attestation or Integrity Reporting
  - Reliably measure and report on the platform's software state
- Protected Storage
  - Protect private and secret data on that platform

Trusted Computing Platform Properties



Identify a physical platform

- 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. e.g. NetAccess
- Outsourced platform administration I.e. control access to private data

Enable user confidence in the behaviour of the platform in front of them

- Trust a platform to handle my private data, e.g. banking, medical…etc…
- Achieving WYSIWYS: What You Sign Is What You See…

=> Need for Roots of Trust

ProCurve Networking
HP Innovation

Two Roots of Trust

- A Root of Trust for Measurement – The component that can be trusted to reliably measure and report to the Root of Trust for Reporting (the TPM) what software executes at the start of platform boot

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

- It is necessary to trust these Roots of Trust in order for TCG mechanisms to be relied upon => Conformance and Certification

ProCurve Networking
HP Innovation

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 Boot Block in an IA-32 platform)

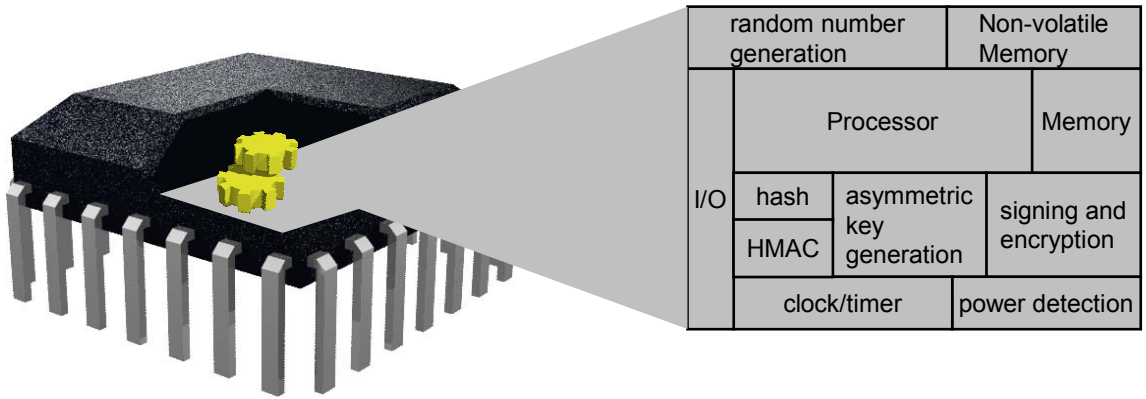
- It must be trusted to properly report to the TPM what is the first software/firmware that executes after it
- Only entities trusted by those who certify behaviour can reflash the CRTM

The Trusted Platform Module "the TPM"

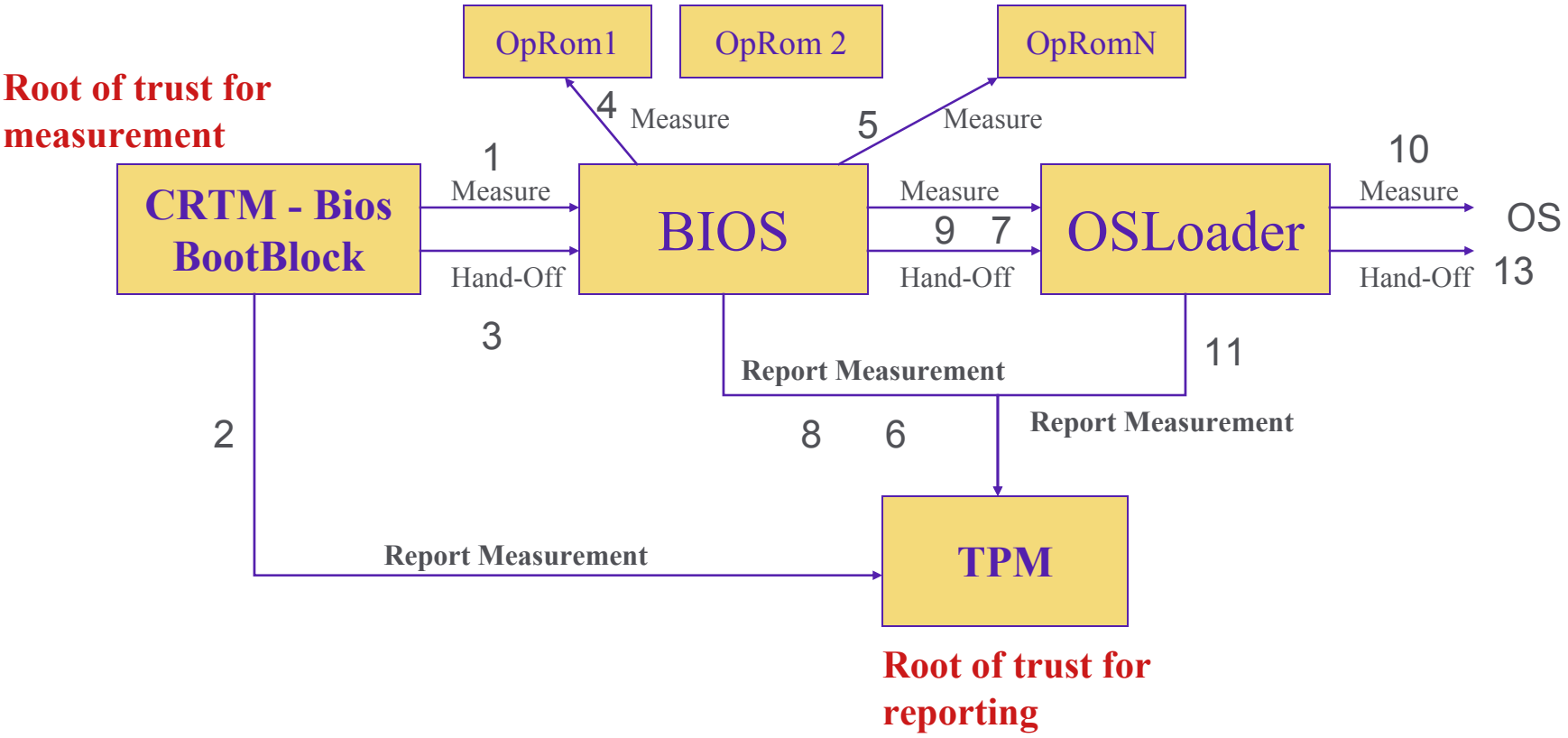
ProCurve Networking
HP Innovation

The TPM is the Root of Trust for Reporting. Think: smartcard-like security capability embedded into the platform

- The TPM is trusted to operate as expected (conforms to the TCG spec)
- 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)



TCG "chain-of-trust" The PC example



TPM features

ProCurve Networking
HP Innovation

Not a generic bulk encryption device – no export control problem

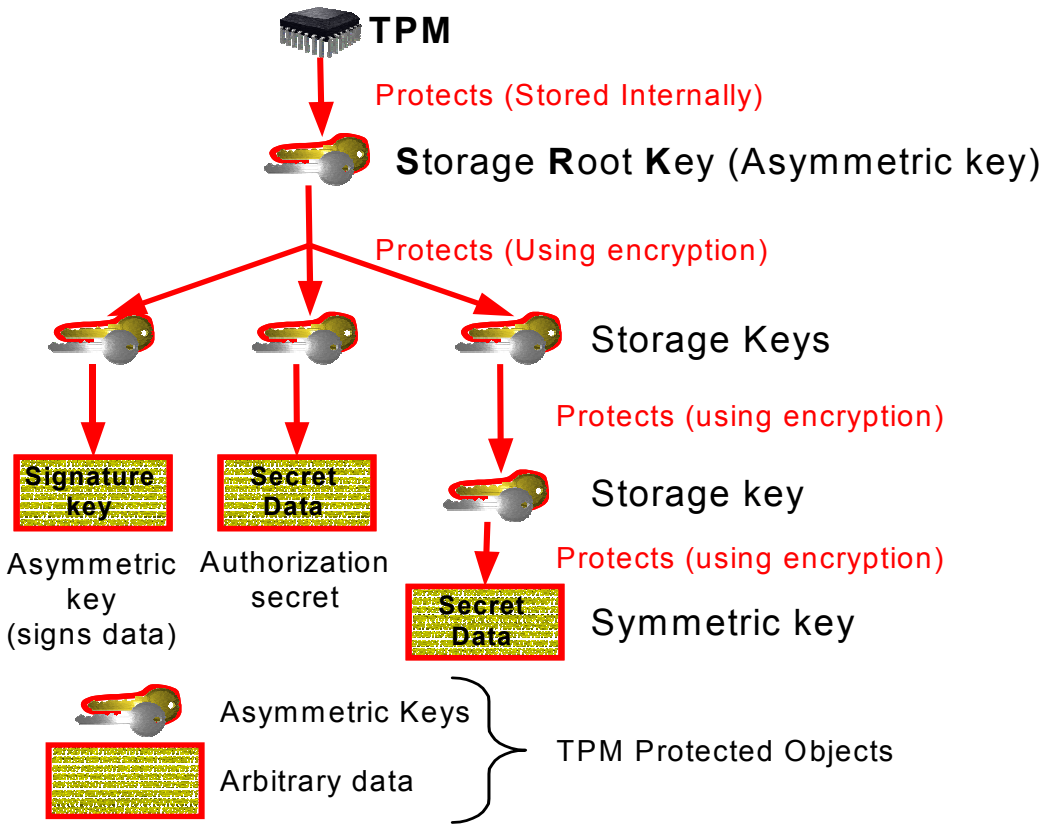
Unlimited number of cryptographic keys can be created and protected by the TPM => Protected Storage

Data/keys can be encrypted such that they can only be decrypted using this TPM => Platform identity

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



For More Information

The spec:

TCG specification v1.1b publicly available at www.trustedcomputinggroup.org

The HP book:

"Trusted Computing Platforms: TCPA technology in context"

ed. Siani Pearson

by Balacheff, Chen, Pearson, Plaquin & Proudler

pub. Prentice Hall, 2002

ProCurve Networking
HP Innovation

Conclusions

Trusted Computing is an industry effort that is beginning to reach some maturity in the PC space

TCG is now widening its efforts to other computing devices, from servers to printers, mobile phone and storage technologies…