Server Hardware Design -
Thermal & Security Consideration

Richard Kuo

10/15/2010

Technology Director

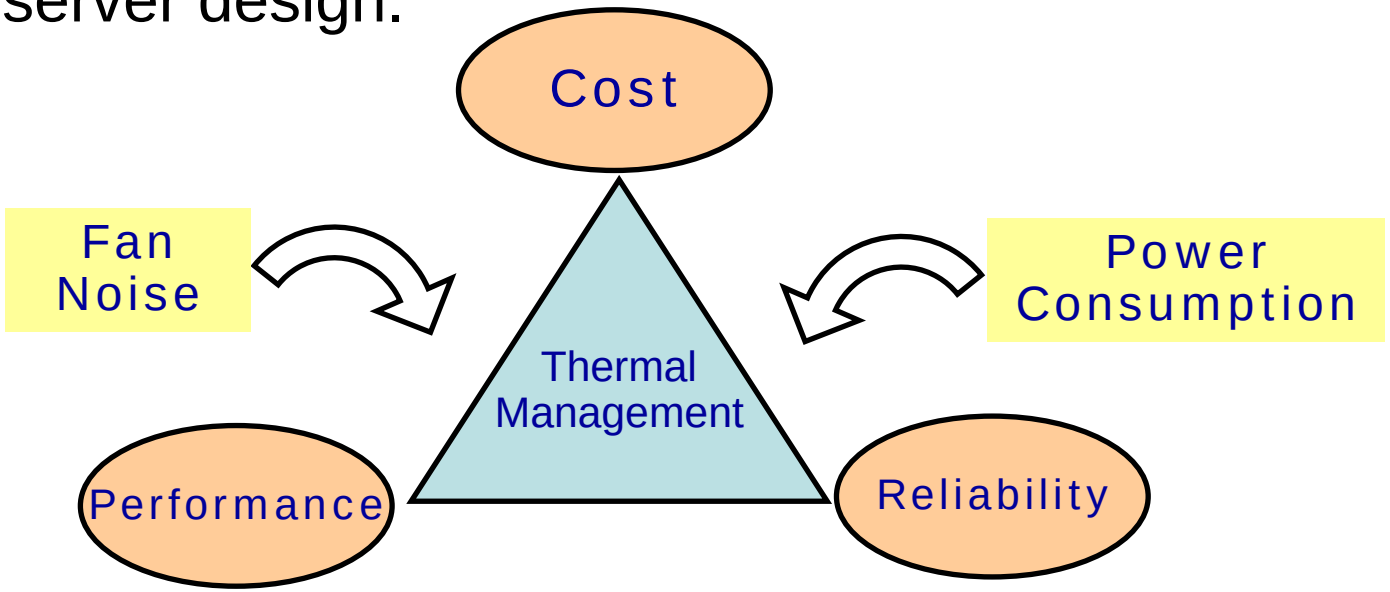
Computer Business Group

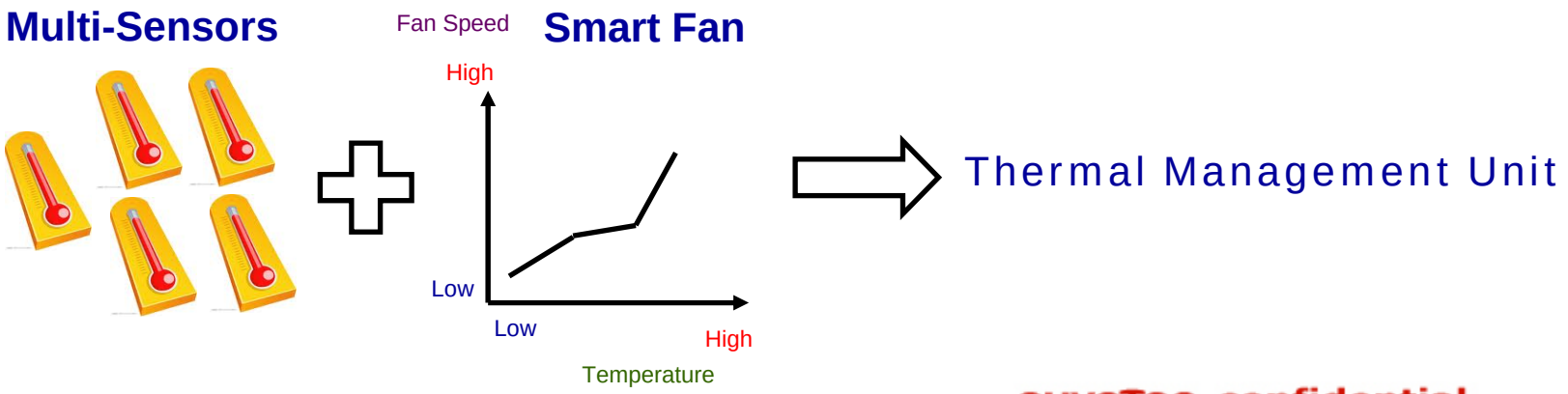
Thermal Management

- Thermal Management is a main topic in server design
- Besides Cost, Performance and Reliability, Power Consumption and Acoustic should be considered in server design.
- Thermal management requirements depend on server form factor design. All require a good plan and arrangement on thermal space.
- An independent and flexible TMU (Thermal Management Unit) IC can manage different thermal models/patterns by monitoring multiple thermal zones and controlling the fan smartly.

Thermal Management

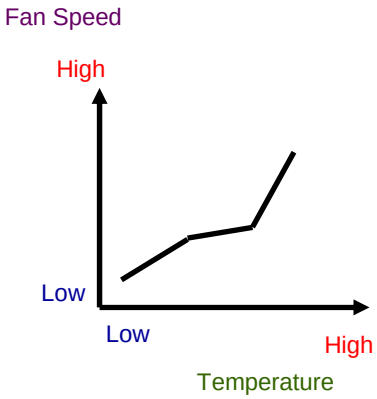
- Thermal Management is the most important topic in server design.



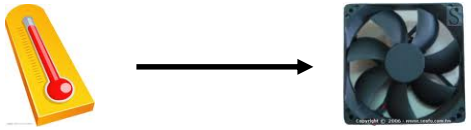


Main Factor - Temperature

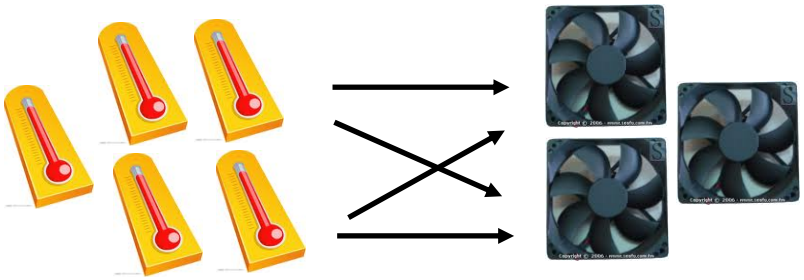
- Temperature used to be the factor which is used for fan control
  - Thermal Zones (CPU, GPU, Chipset, HDD…)
- Temperature higher → fan speed higher



- In the past, one temperature by one fan



- Now, multi-temperatures across many fans



New Factor - Energy

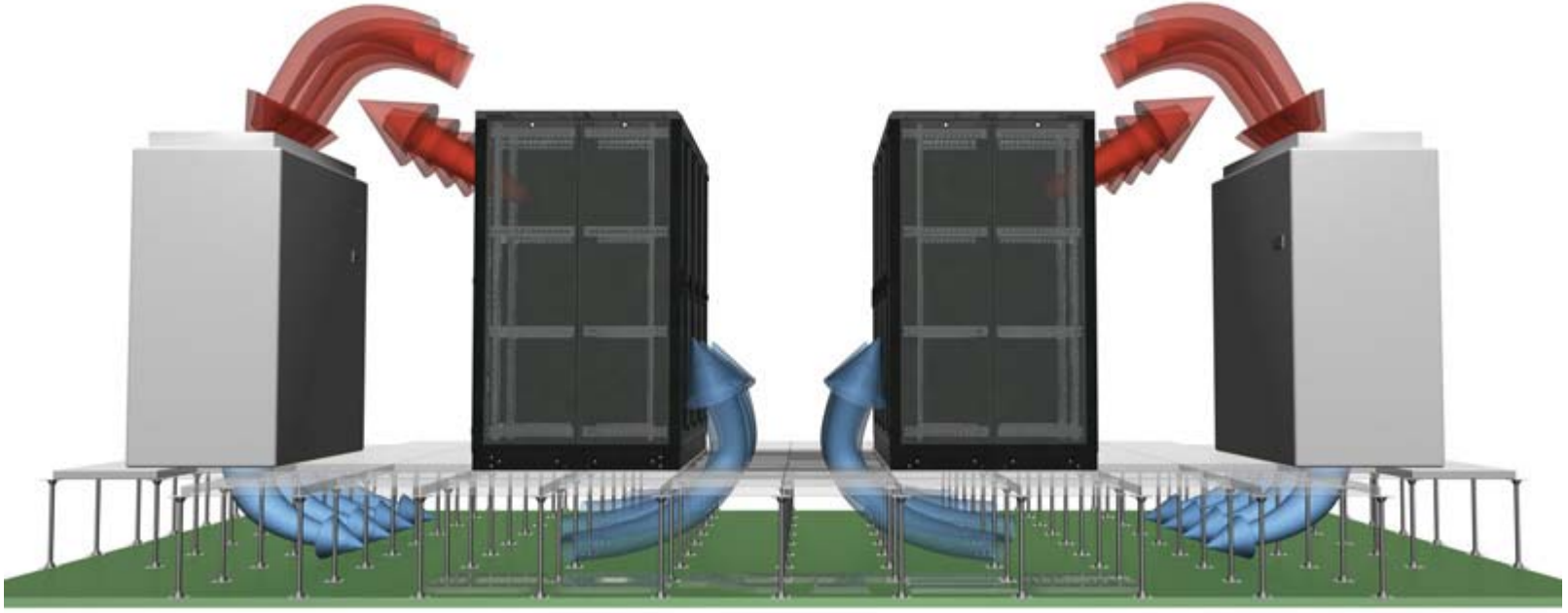
- Temperature is a lagging indicator
- Energy is the source of temperature
- More energy consumed → Higher temperature → Higher fan speed → More energy consumed by fan
- Energy is taken into consideration
  - For thermal control
  - For power saving
- When temperature is at a safe range, lower energy needed → lower fan speed
  - Saving power from dynamic fan speed
  - Better acoustic performance (lower noise)

Thermal Management

Environment Factor
- Thermal Data
- Power Consumption

→ Smart Fan Control

→
- Use Airflow to Solve Cooling Problem
- Consider Power Usage to Adjust Fan Behavior

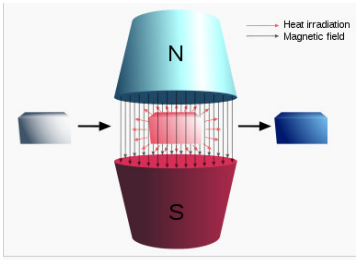


Cooling Methods

- Air Cooling : heat sink + fan
  - Traditional :
    - Generate cold air for the whole ambient, and create air flow through thermal zones.
    - The cold air is always from air conditioner and recycle
  - New :
    - Direct the cool air into the heating device directly
    - Utilize the outdoor air if it is cooler than indoor AC air.

- Liquid Cooling : heat-sink/pipes + water/coolant
  - Liquid cooling is essentially a radiator for the CPU inside of the computer. Just like a radiator for a car, a liquid cooling system circulates a liquid through a heat sink attached to the processor inside of the computer.
  - Advantage : noise reduced, efficient for overclocking
  - Disadvantage : bigger size, harder to install

- Magnetic Cooling : magnetic material
  - Magneto-caloric effect can be used to attain extremely low temperatures (well below 1K)

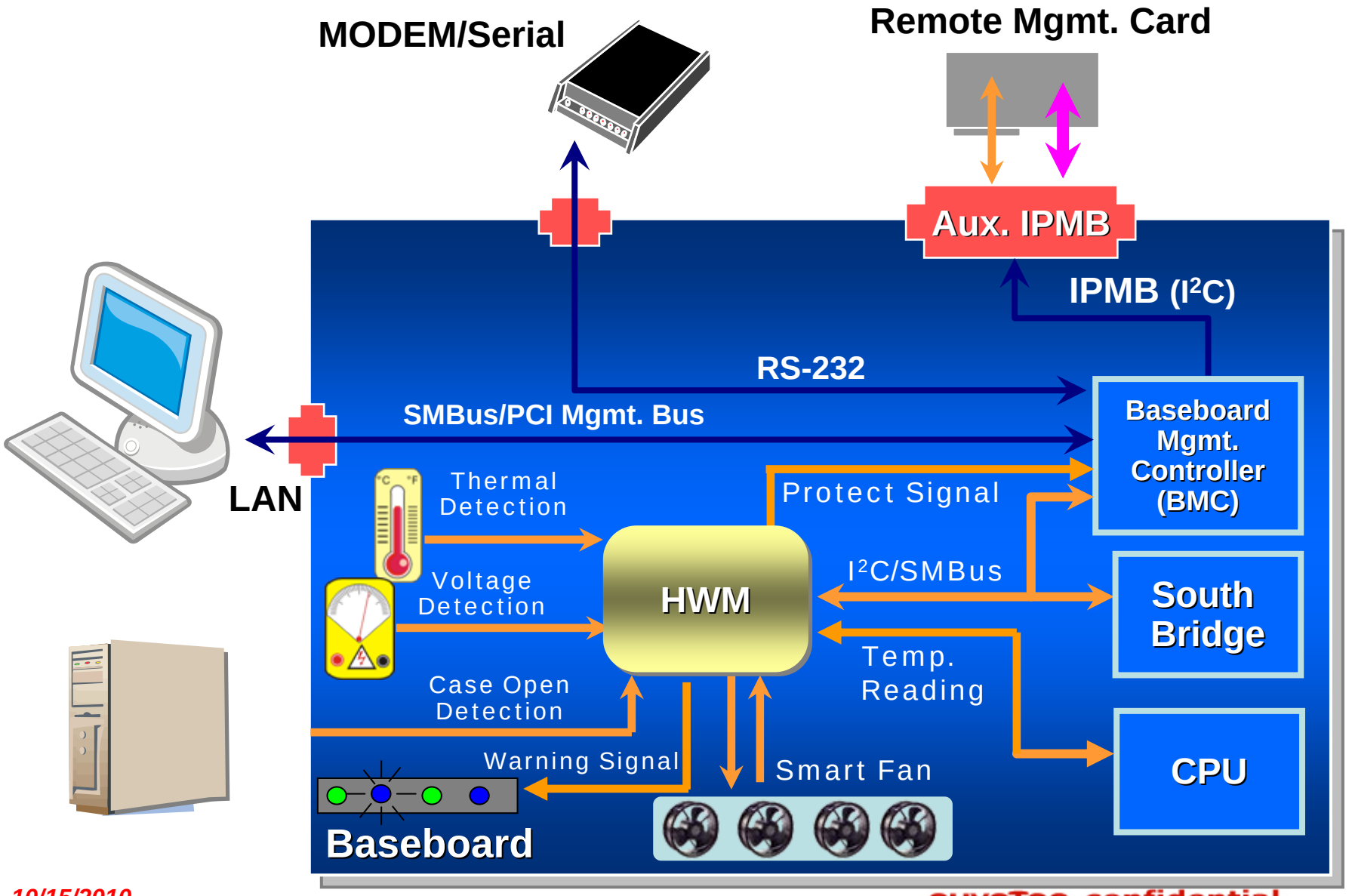


Gadolinium alloy heats up inside the magnetic field and loses thermal energy to the environment, so it exits the field cooler than when it entered.

Data Center Cooling

- Cool Air
  - Architecture : Container, Green Building
  - Elevation : Underground, Hill
  - Latitude : Finland, Iceland
- Cool Water
  - Lake Water
  - Sea Water

H/W Monitor Role in Server System



Example: H/W Monitor Operation

CPU Temp.& Energy :

Support PECI3.0

SYSTEM Temp. :

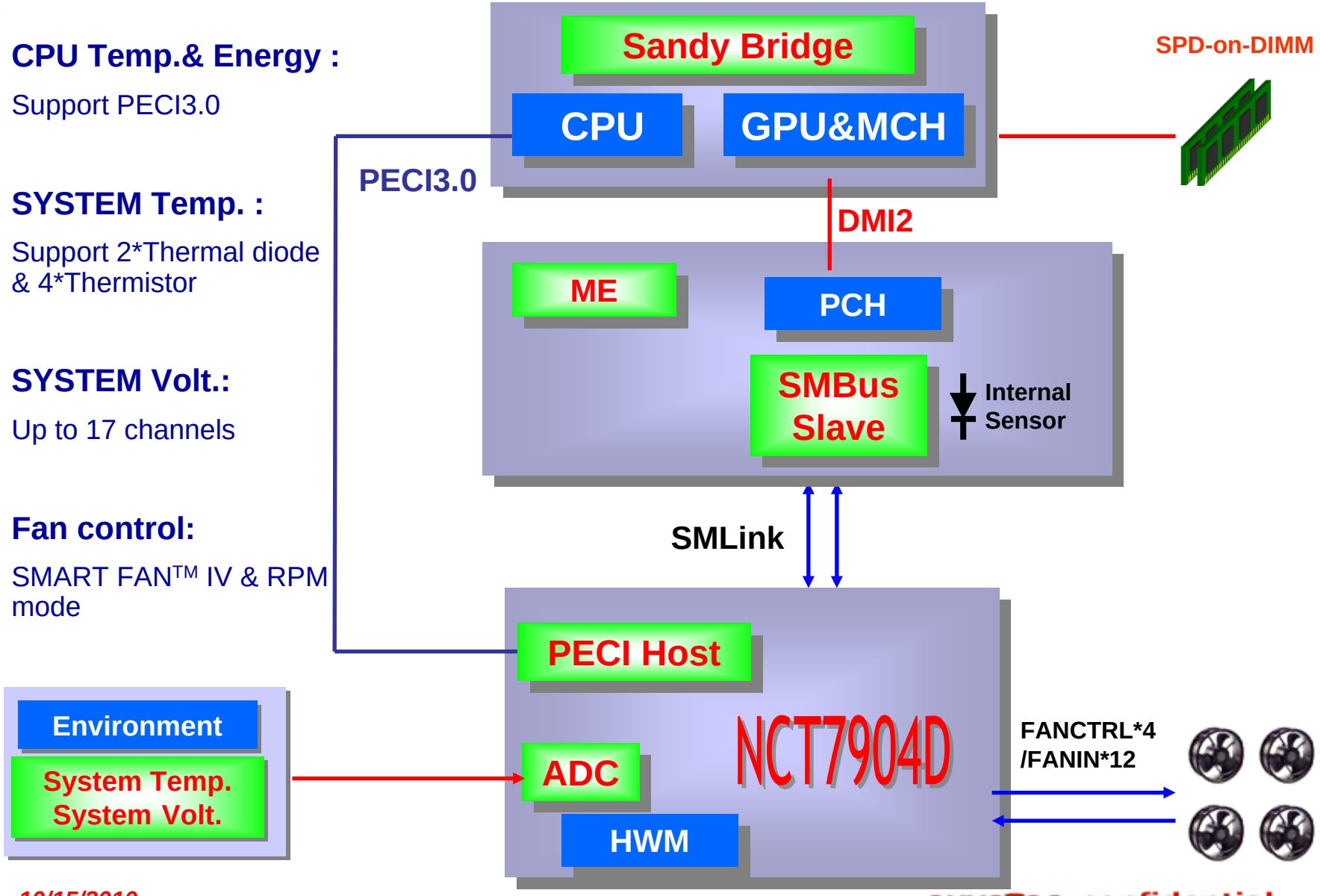
Support 2*Thermal diode & 4*Thermistor

SYSTEM Volt.:

Up to 17 channels

Fan control:

SMART FAN™ IV & RPM mode



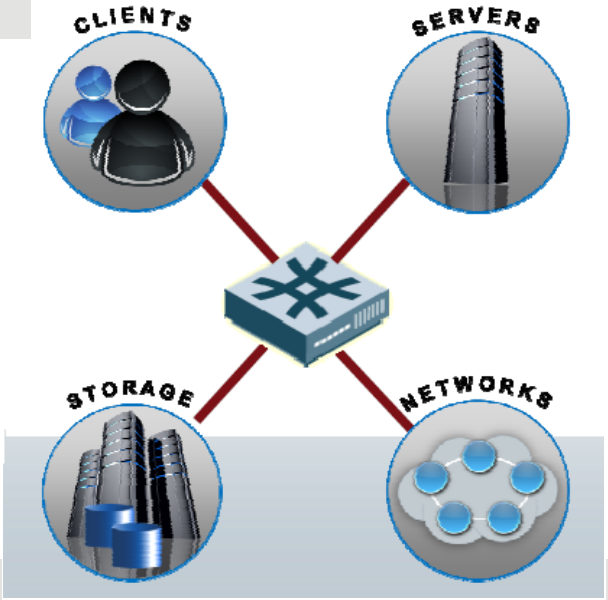
Top Threats to Cloud Computing

- Abuse and Nefarious Use of Cloud Computing
- Insecure Interfaces and APIs
- Malicious Insiders
- Shared Technology Issues
- Data Loss or Leakage
- Account or Service Hijacking
- Unknown Risk Profile

listed by Cloud Computing Alliance

TCG : Coordinated Security

Security built in
Trusted Platform Module (TPM)
Mobile Trusted Module (MTM)



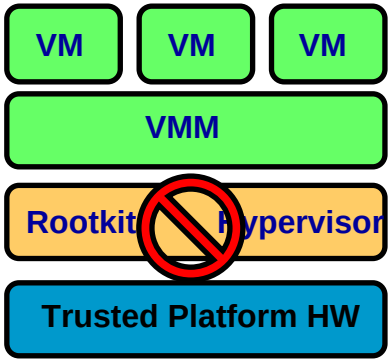
Security built in
Trusted Platform Module (TPM)
Secure Virtualization
Secure Cloud

Security built in
Self-Encrypting Drive (SED)

Security built in
Trusted Network Connect (TNC)

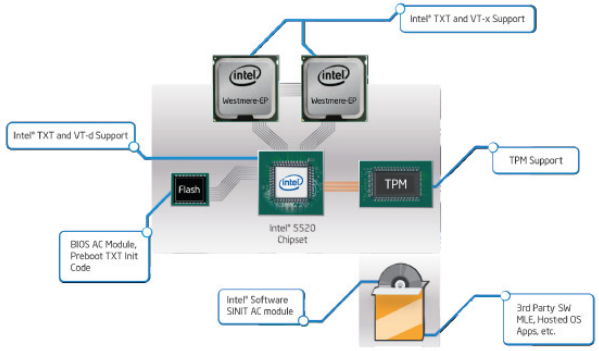
Intel Trusted Execution Technology

- OS can no longer blindly trust its environment
  - Rookit & Hijacking (OS itself is an image for provisioning)
  - reset attack (TPM)



Intel IDF Sept. 2010

- Intel TXT use TPM with its CPU & chipsets
  - Boot to a known good environment
  - Control of launch environment
  - Sealing to OS and/or Platform
  - Attest to the platform and OS/VMM authenticity
  - Memory Cleaning to protect secrets
  - Protect OS & Applications from reset attack

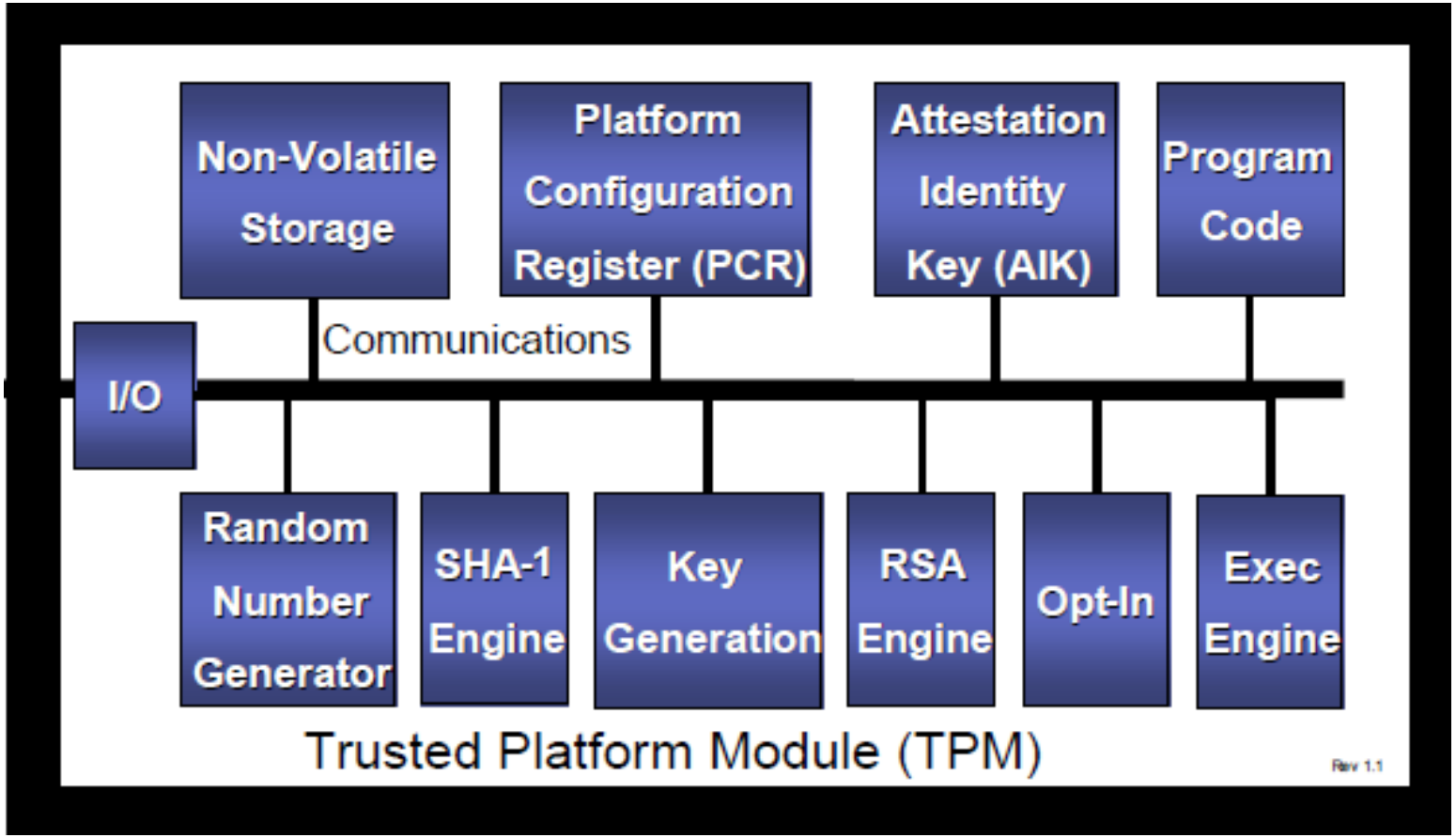


Intel TXT white paper

Rootkit Detection

- Signatures detection
  - anti-virus software
- Integrity checking
  - cryptographic hash function can compute a digital signature to detect subsequent unauthorized changes to on-disk code libraries.
- Difference-based detection
  - compared “trusted” raw data with “tainted” content returned by an API
  - Memory Dumps
- Behavioral detection
  - monitoring CPU usage or network traffic
  - profiling a system : API calls, CPU utilization

TPM component architecture



TCG Specification Architecture Overview revision 1.4 August 2nd, 2007

TPM for Servers/Cloud

- TPM in servers is used for the same services as it is used in client:
  - Secure boot, by measuring the boot code
  - SSL transactions more secure by protecting the SSL key in the TPM. If no TPM, the SSL private key is exposed to SW and may be hacked
  - Secure email, documents, etc
- However, server also has special needs:
  - Client need to verify that the server is in trusted state, before starting any sensitive data transfer
  - The server can support multiple OS and Virtual machines. Each one has its own physical/virtual TPM
  - Jobs can move between VMs

TPM Virtualization

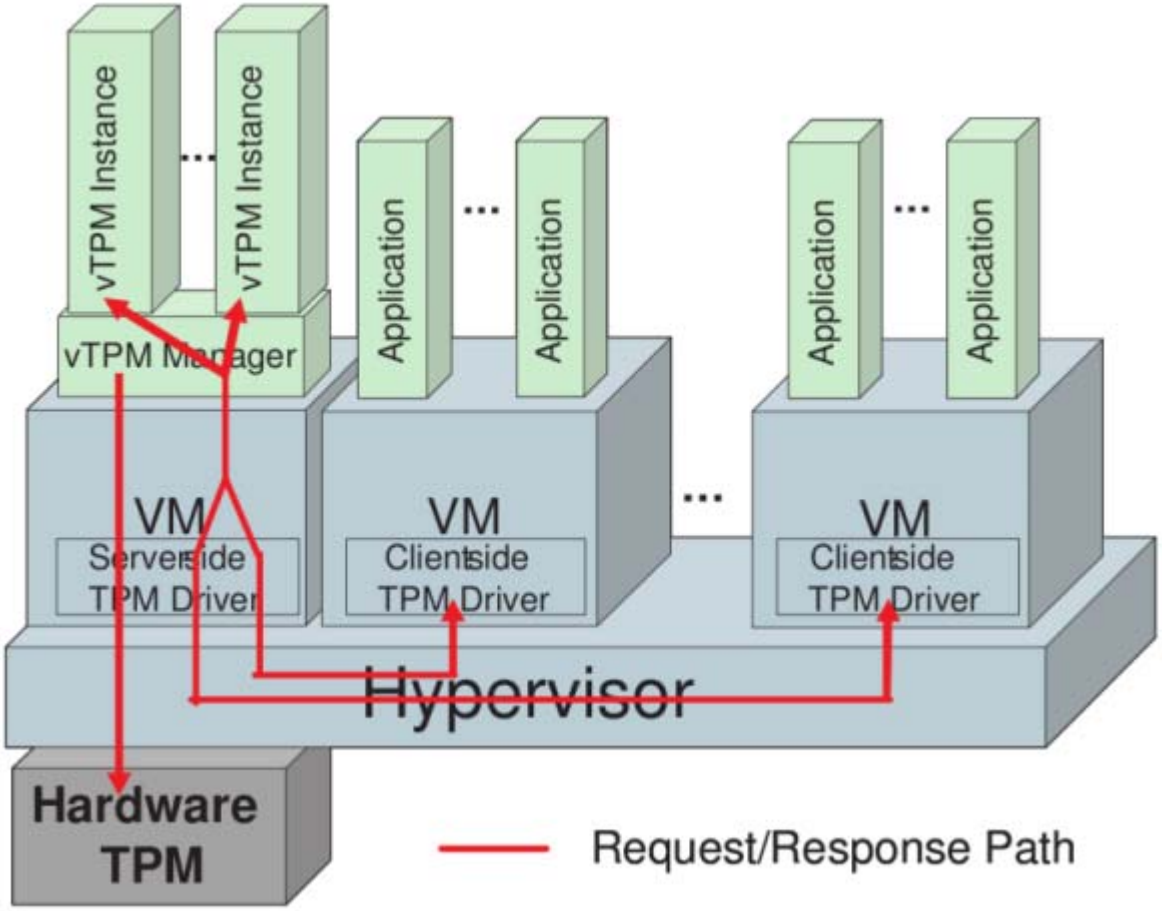
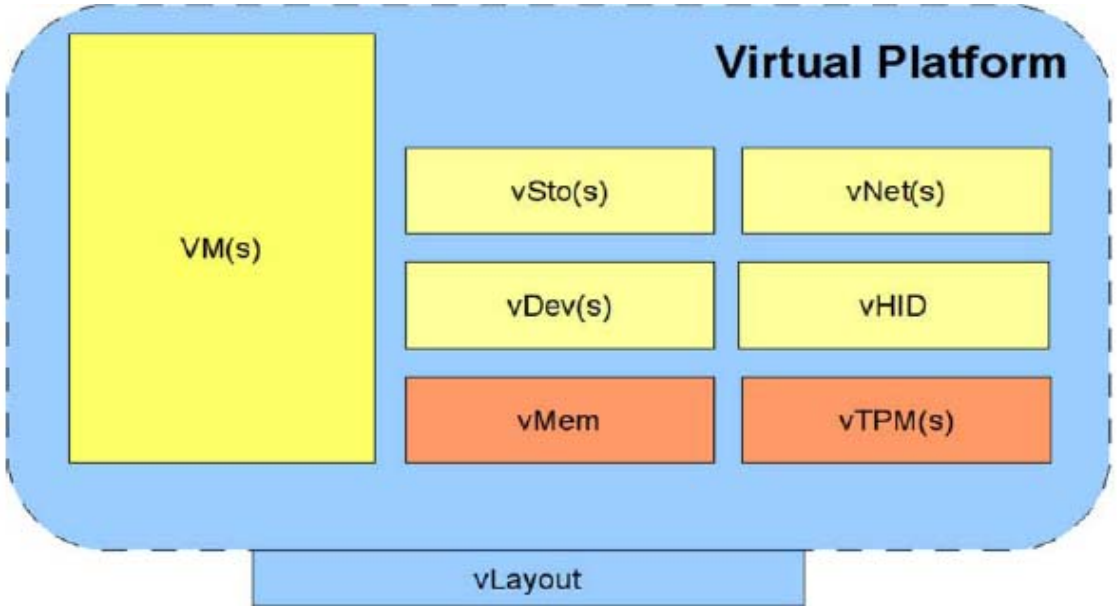


figure from the paper: "vTPM: Virtualising the Trusted Platform Module" by IBM)

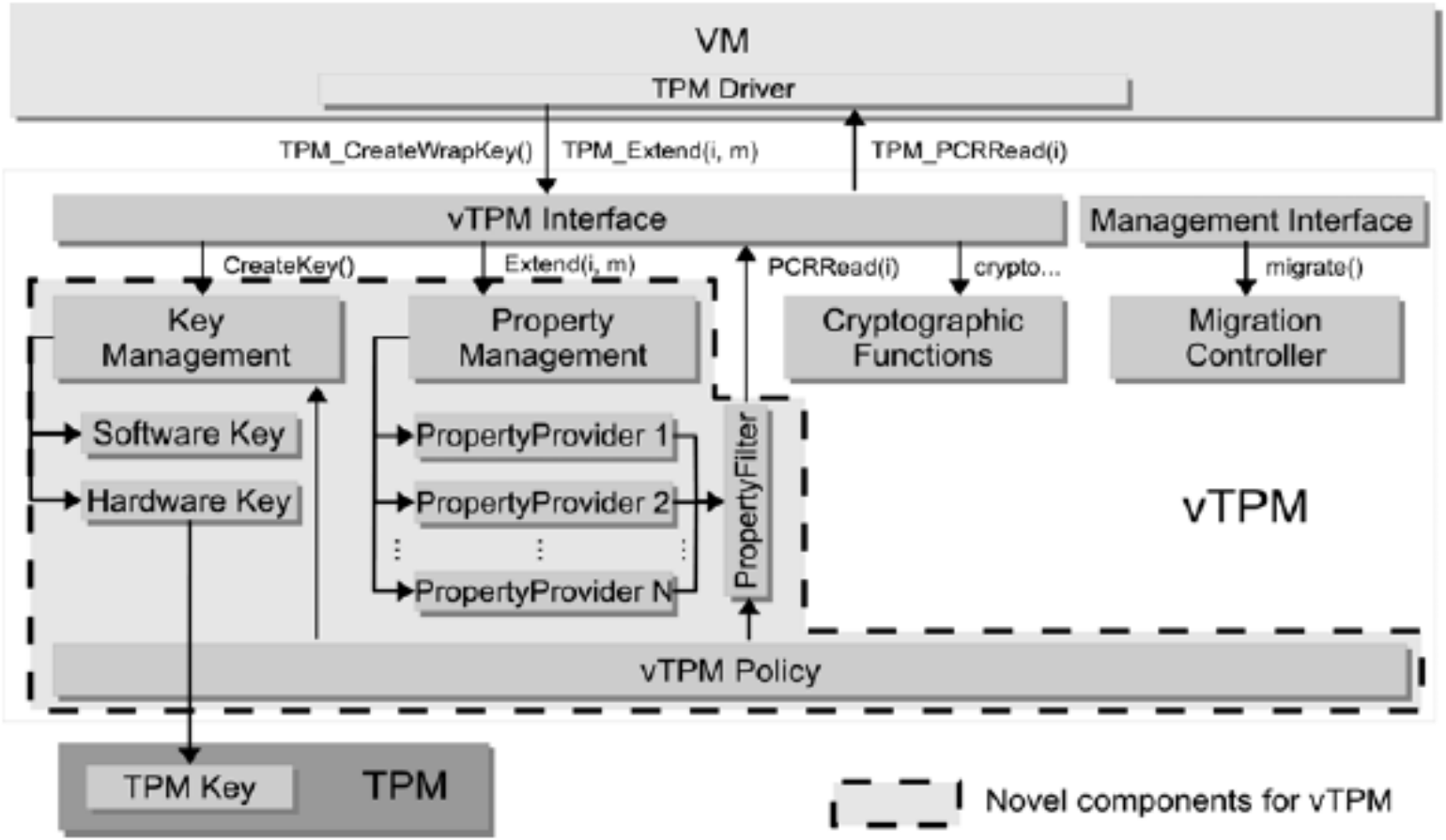
TCG VTPM architecture



VM – Virtual Machine
vSto – Virtual Storage
vNet : Virtual Networking devices
vDev : Generic Virtual Devices
vHID : Virtual Human Interface Devices

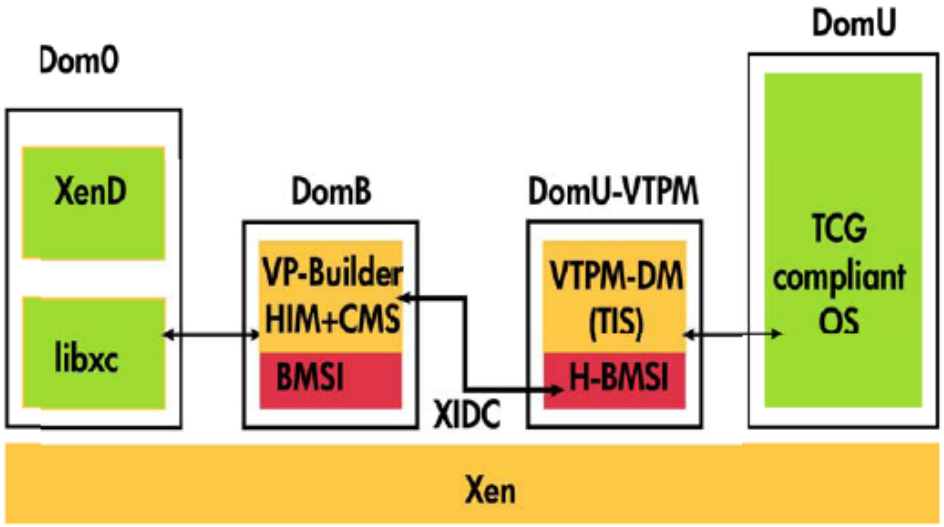
From OpenTC D04.7 TPM Virtulization Architecture Cocument v2.

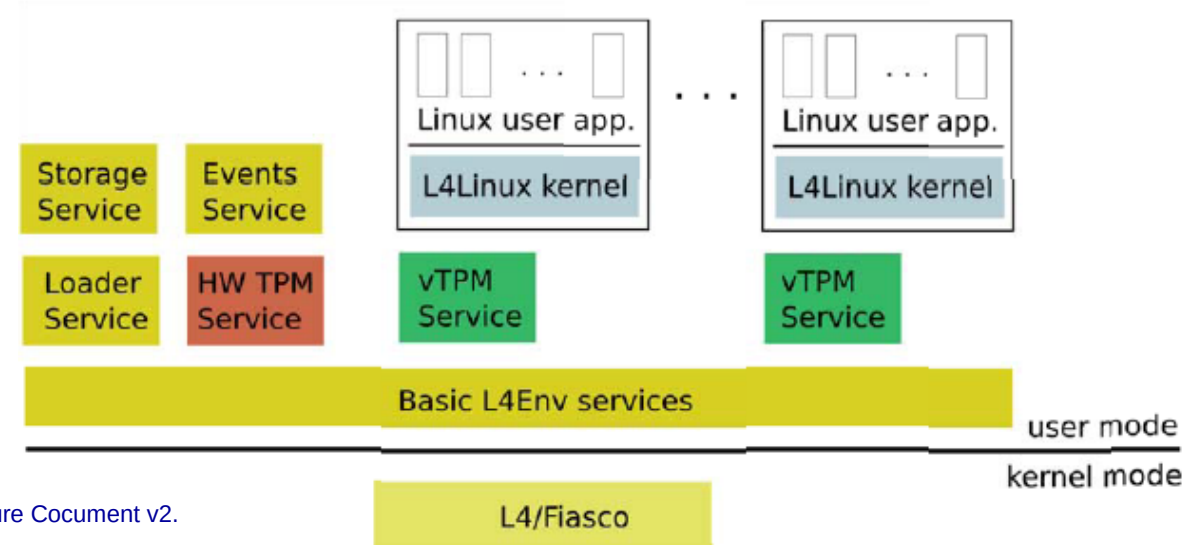
Logical architecture of property based attestation enhanced vTPM



From OpenTC D04.7 TPM Virtulization Architecture Cocument v2.

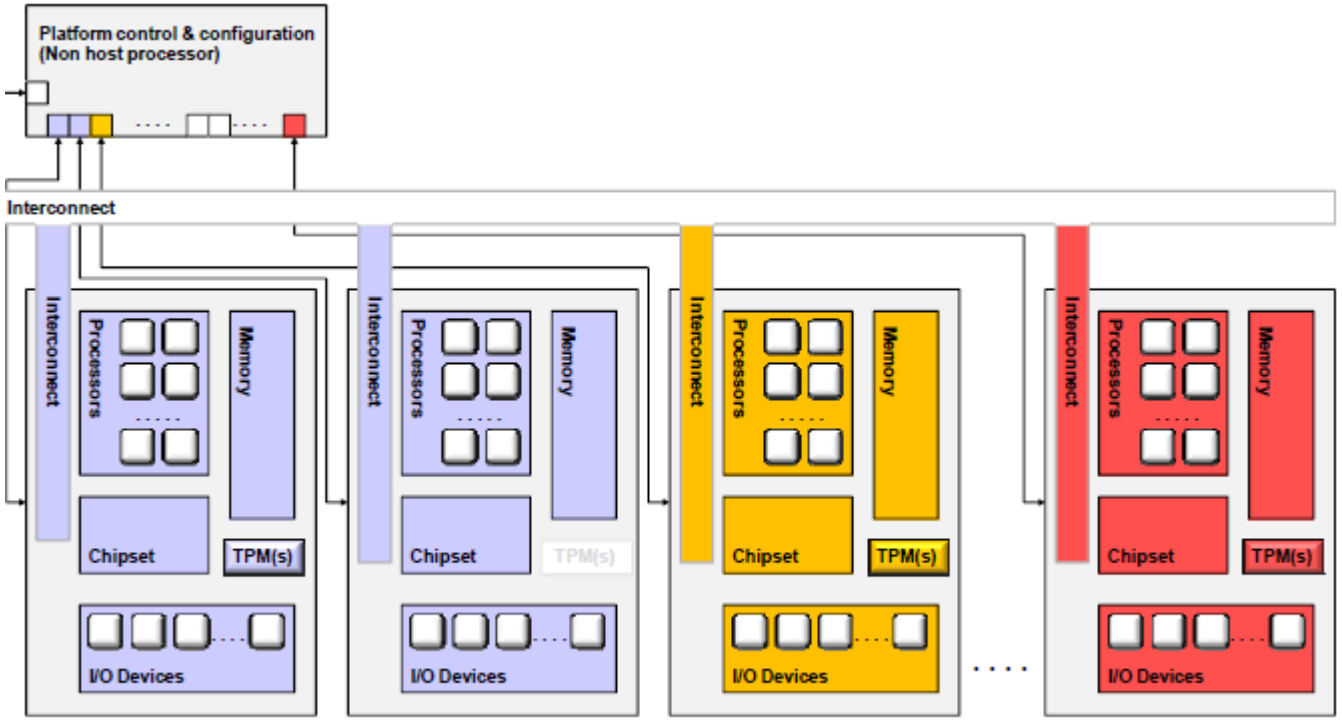
Implementation on Xen & L4Linux





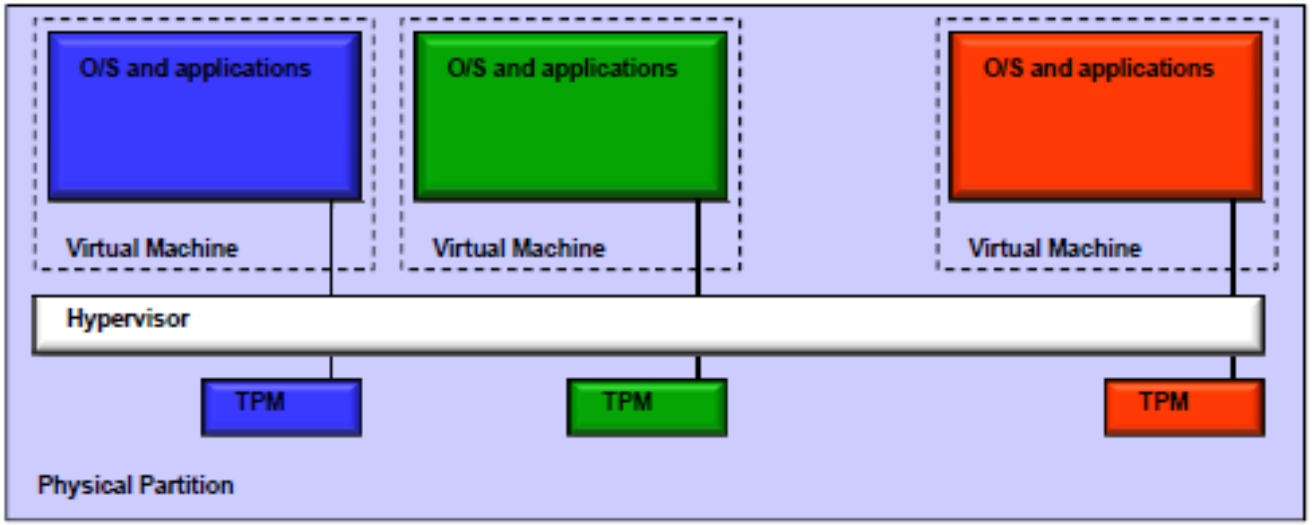
From OpenTC D04.7 TPM Virtulization Architecture Cocument v2.

Physical Partitioning



- The system appears as multiple servers each owns independent HW.
- Each server runs a different OS and uses a different TPM instance
- Since a task can span over more Physical partition, the TPM state need to be able to migrate between partitions

Virtual partitioning



- Several Virtual Machines each with its O/S instance, and each with its own TPM instance
- TPM is only one instance, but need to be able to serve multiple visrtual machines and sessions
- The Hypervisor can emulate the TPM functionality, using the real TPM only on critical areas (for example, to measure its code)

Legal Disclaimer & Risk Factors

- This presentation, including information contained in this disclaimer, is given to you in strict confidence.By attending the presentation, you agree that no part of this presentation or disclaimer may be disclosed,
  distributed or reproduced to any third party without the consent of Nuvoton Technology Corp. (“Nuvoton”).
  This presentation is being provided for the sole purpose of providing the recipients with background information about Nuvoton's business. This presentation, including the information contained in this disclaimer, does not constitute an offer, invitation or recommendation to subscribe for or purchase any security and neither the presentation, disclaimer nor anything contained in them forms the basis of any contract or commitment.
  No representation, express or implied, is made as to the fairness, accuracy, completeness or correctness of information contained in this presentation, including the accuracy, likelihood of achievement or reasonableness of any forecasts, prospects, returns or statements in relation to future matters contained in the presentation (“forward-looking statements”). Such forward-looking statements are by their nature subject to significant uncertainties and contingencies and are based on a number of estimates and assumptions that are subject to change (and in many cases are outside the control of Nuvoton) which may cause the actual results or performance of Nuvoton to be materially different from any future results or performance expressed or implied by such forward-looking statements.
- To the maximum extent permitted by law, neither Nuvoton nor its related corporations, directors, employees or agents, nor any other person, accepts any liability, including, without limitation, any liability arising from fault or negligence, for any loss arising from the use of this presentation or its contents or otherwise arising in connection with it.

THANK YOU!

Richard Kuo

TJKuo@nuvoton.com

886-3-5770066 #7057