

The Talos™ Secure Workstation

Restoring Trust and Owner Control to General Purpose Computing

Timothy Pearson
tpearson@raptorengineering.com

Raptor Engineering, LLC
<https://www.raptorengineering.com>

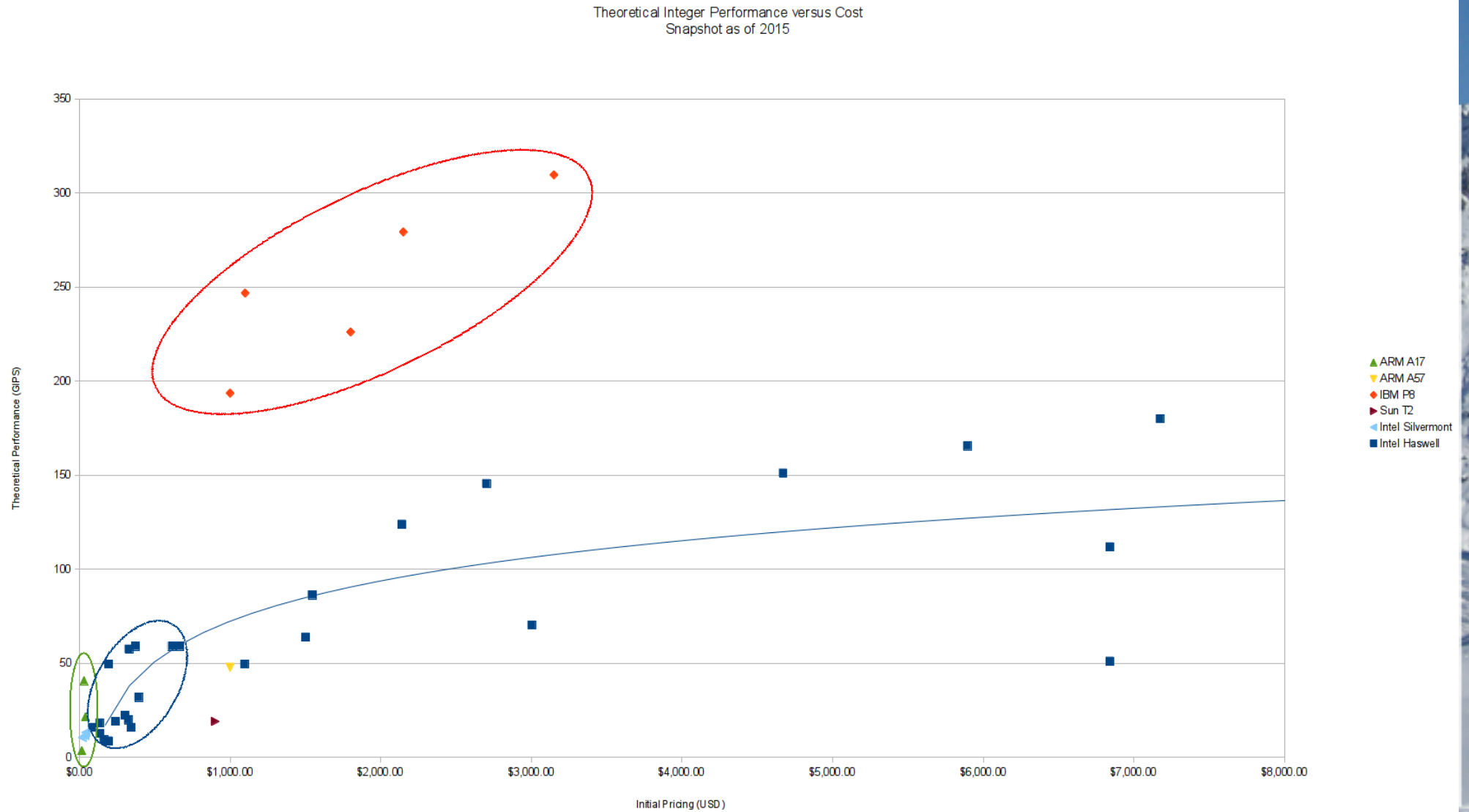
The Talos™ Secure Workstation

- Why is Owner Control important?
 - Freedom
 - Flexibility
 - Reliability
 - Privacy
 - Security
 - Continuance
 - Competition / multi-source capability

Closed Firmware Risk, Relative



Architecture Market Segmentation



The Talos™ Secure Workstation

- POWER
 - ONLY libre-capable core on par with x86 cores
 - Multiple firmware components, on-die CPUs
 - Source available / modifiable on OpenPOWER
 - Traditional microcode
 - Unlike x86, can be read back out and verified
 - Microcode not lost on power off / reset
 - Can be locked in hardware to prevent updates

The Talos™ Secure Workstation

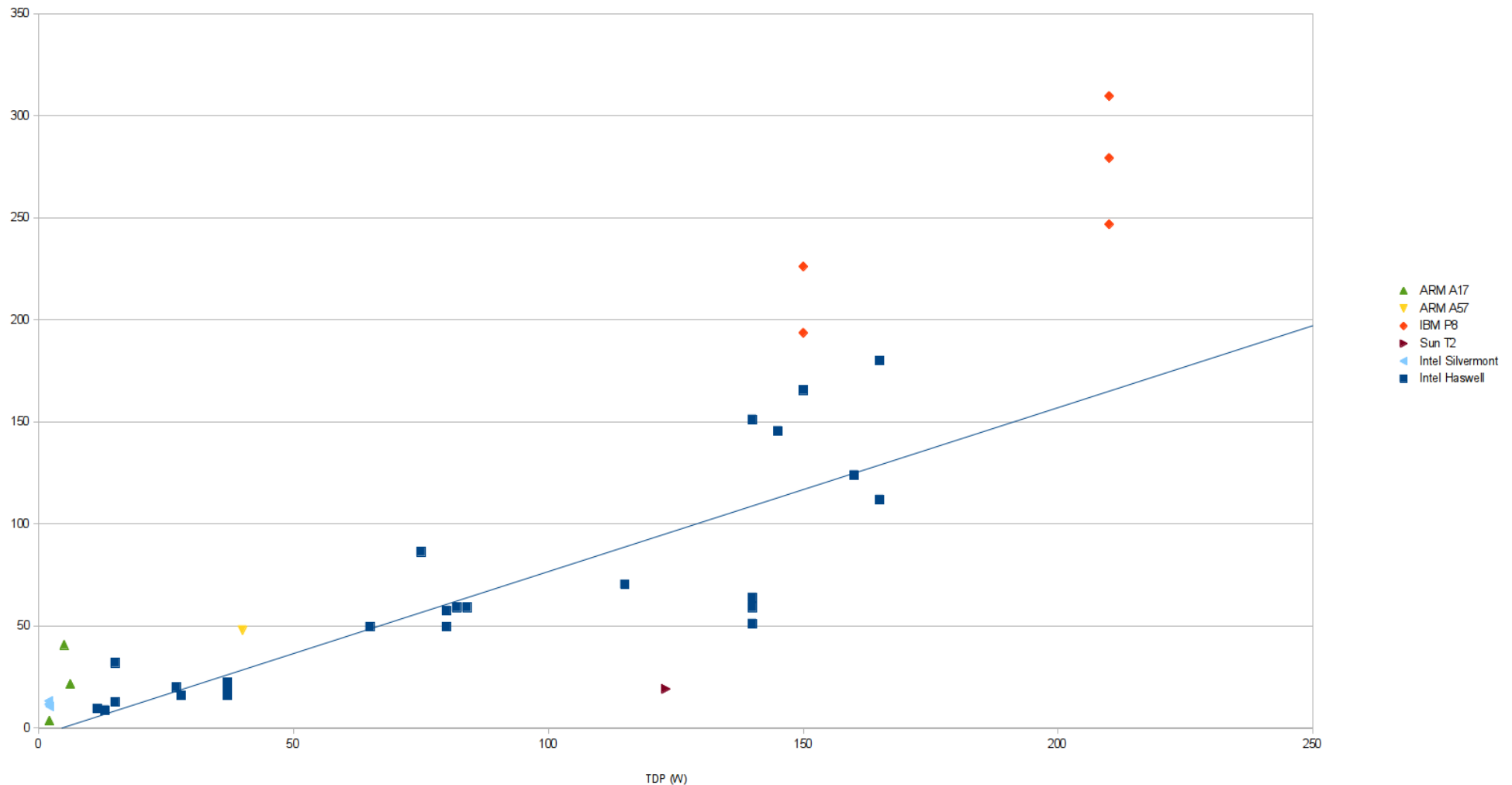
- POWER (cont.)
 - Historically big endian (BE)
 - Hardware little endian support as of P8
 - Allows non-endian-aware code to function
 - Eases porting burden
 - Bi-endian capable
 - Booted kernel sets endianness
 - Bare metal firmware can boot BE or LE
 - KVM VM kernels can select either endianness

The Talos™ Secure Workstation

- POWER (cont.)
 - OpenPOWER “Turismo”
 - Single Chip Module (SCM)
 - Up to 12 “chiplets” (core, L2, and sharable L3)
 - Expansive cache hierarchy
 - L3 and L4 cache
 - eDRAM allows large caches
 - Large die size, high TDP
 - TDP in line with similarly performant CPUs

Theoretical Performance Versus TDP

Theoretical Integer Performance versus TDP
Snapshot as of 2015



The Talos™ Secure Workstation

- POWER (cont.)
 - Significant investment in Linux ecosystem
 - Debian archive coverage > 97%!
 - Full KVM support including TCE
 - Unprecedented level of firmware access
 - No regions cryptographically locked by hardware
 - OCC firmware is open source
 - Hardware capable of ChromeOS security model
 - Keeps full control in hands of machine owner

The Talos™ Secure Workstation

- OpenPOWER Firmware
 - OCC
 - On-chip power management / thermal control
 - Hostboot
 - Low-level startup
 - Skiboot
 - OPAL runtime services

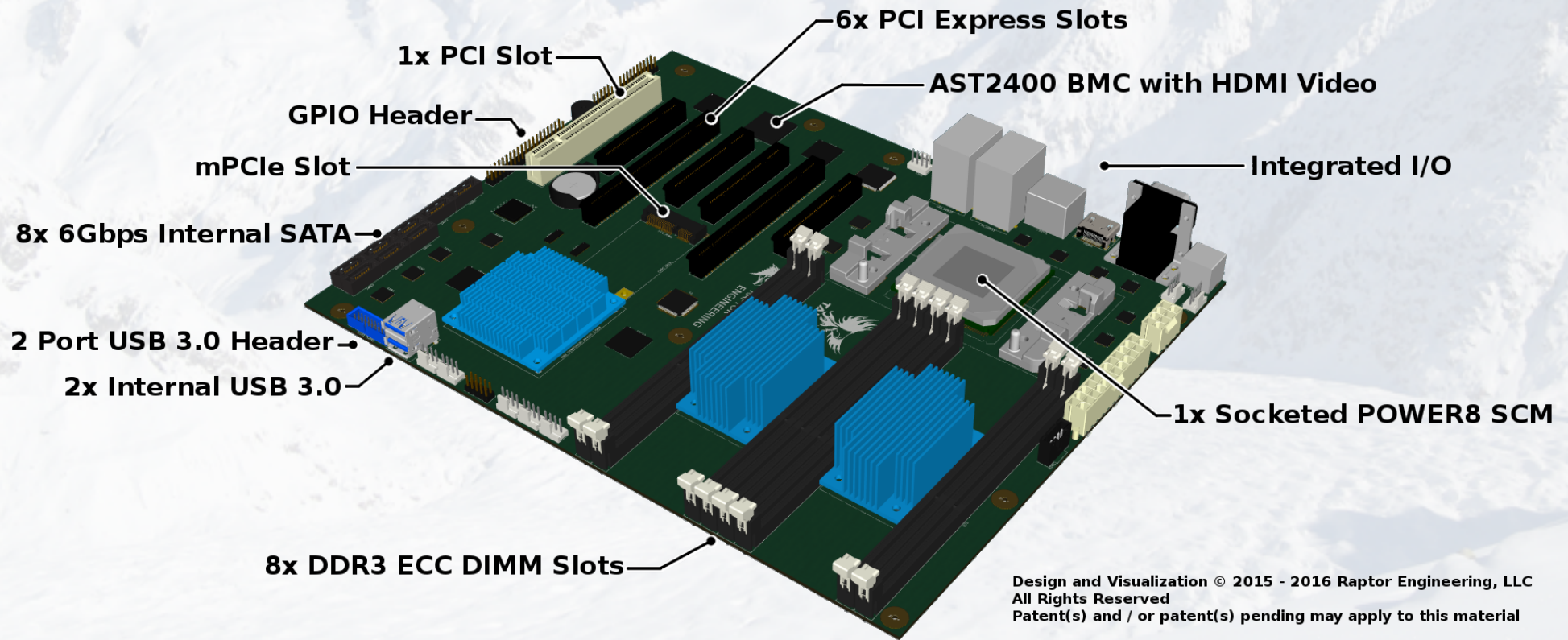
The Talos™ Secure Workstation

- OpenPOWER Firmware (cont.)
 - Petitboot
 - User interaction / final bootloader
 - GRUB (on disk / distro provided)
 - IEEE 1275-1994

The Talos™ Secure Workstation

- Raptor Engineering's Talos™ system
 - Standard ATX-compatible mainboard
 - Specifically targeted at workstation market
 - 1 POWER8 CPU – 130W stock, 190W optional
 - Up to 256GB DDR3 w/ ECC
 - High PCIe lane count
 - SATA, USB 3.0, etc.
 - Fully open firmware
 - Includes schematics for most hardware!

The Talos™ Secure Workstation



The Talos™ Secure Workstation

- Raptor Engineering's Talos™ system (cont.)
 - Unique Features
 - Open toolchain FPGAs for signal routing
 - Programming headers for firmware development
 - Will ship with OpenBMC & OpenPOWER firmware
 - Multiple hardware-enforced security options
 - Flash partition / key store write protect switches
 - BMC network disable switch
 - LPC Guard™ anti-snooping system
 - FlexVer™ integrity monitoring technology with TPM

The Talos™ Secure Workstation

- Raptor Engineering's Talos™ system (cont.)
 - Primary goals
 - Allow trusted, complex general purpose computing
 - Encourage development of libre low-level firmware
 - Provide a viable x86 workstation alternative
 - Enable innovation through OpenPOWER access
 - Status
 - System development well underway
 - Crowdfunding campaign active – ends shortly!

The Talos™ Secure Workstation

- Summary (cont.)
 - Era of cheap, commodity GPC has ended
 - Consumer machines are cryptographically locked
 - Consumer markets have shifted to rental / cloud
 - Libre software advocates have three choices
 - Use cheap, low-end, reverse engineered machines for as long as they remain unlocked
 - Accept loss of owner control (and libre software)
 - Pay for full featured, owner-controlled machines

The Talos™ Secure Workstation

- Summary (cont.)
 - OpenPOWER has re-enabled trusted GPC
 - Still needs more support from libre community
 - Trends are encouraging
 - Projects such as Talos™ need market demand!
 - After battle for control of CPU has concluded...
 - ...battle for control of GPU begins!

The Talos™ Secure Workstation

Thank you for your attention!

Check out the Talos™ Secure Workstation

<https://www.crowdsupply.com/raptor-computing-systems/talos-secure-workstation>

Follow us on Twitter or GNU Social!

<https://twitter.com/RaptorEng>

<https://social.raptorengineering.io/raptoreng>

The Talos™ Secure Workstation

- Additional Resources

- Platform Embedded Security Technology Revealed: Safeguarding the Future of Computing with Intel Embedded Security and Management Engine
 - <http://www.apress.com/9781430265719>
- Intel x86 considered harmful - The Invisible Things
 - http://blog.invisiblethings.org/2015/10/27/x86_harmful.html
- Intel & ME, and why we should get rid of ME
 - <https://www.fsf.org/blogs/licensing/intel-me-and-why-we-should-get-rid-of-me>
- Debian archive coverage for supported machine architectures over time
 - <https://buildd.debian.org/stats/graph-quarter-big.png>
- OpenPOWER machine firmware
 - <https://github.com/open-power>