Leveraging Hardware Capabilities for Building Dependable Many-Core Operating Systems (WIP)

Poster Companion Video

Nathan S. Rutherford

Email: nathan.rutherford.2019@live.rhul.ac.uk

Twitter: @rutherfordns

Website: nsrutherford.com

HP Day: 14^{th} - 15^{th} December 2020

Centre for Doctoral Training in Cyber Security for the Everyday,
Information Security Group,
Royal Holloway, University of London

End of Moore's Law [3, 4]

End of Moore's Law [3, 4]

- General Processor Technology (GPT) $\rightarrow$ increased core count

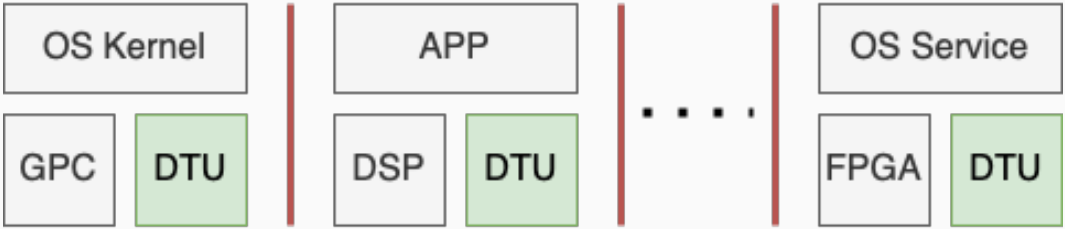
End of Moore's Law [3, 4]

- General Processor Technology (GPT) $\rightarrow$ increased core count
- Specialised Processor Technology (SPT)

End of Moore's Law [3, 4]

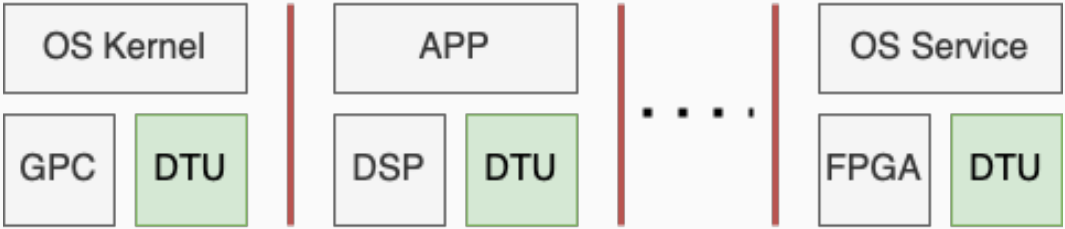
- General Processor Technology (GPT) $\rightarrow$ increased core count
- Specialised Processor Technology (SPT)
- Operating System design that supports heterogeneity

M^3 [1, 2]



Many-core Architectures

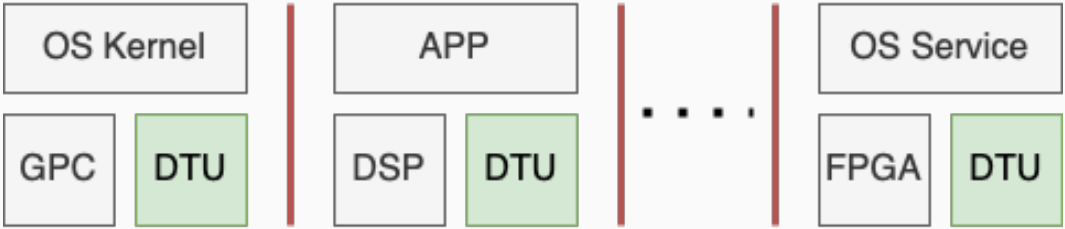
M^3 [1, 2]



Many-core Architectures

- Support for heterogeneity

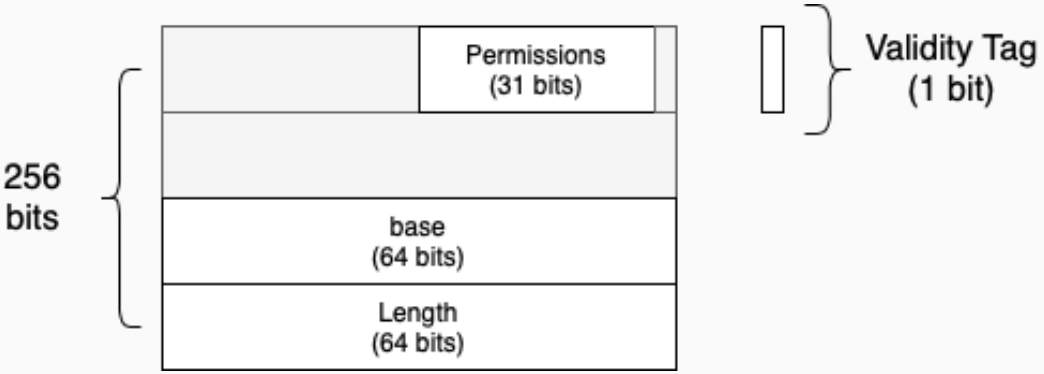
M^3 [1, 2]



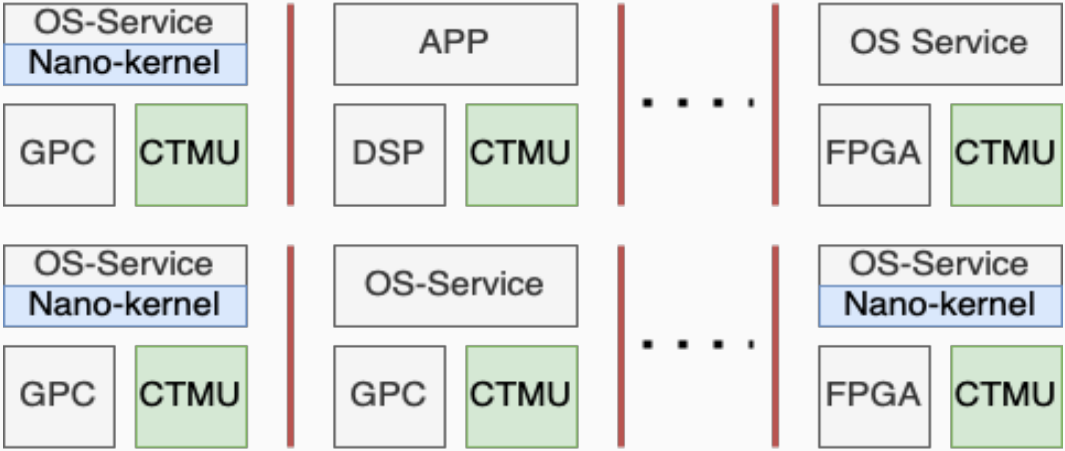
Many-core Architectures

- Support for heterogeneity
- Little attention to dependability

Background: CHERI [5]

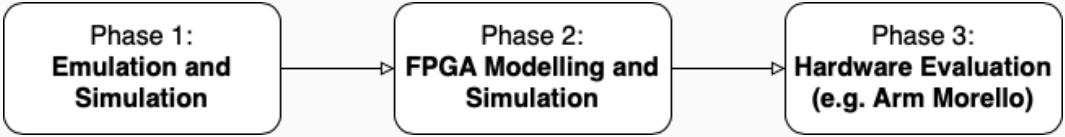


Kernsensus Overview



GPC = **G**eneral **P**rocessor **C**ore, FPGA = **F**ield **P**rogrammable **G**ate **A**rray,
DSP = **D**igital **S**ignal **P**rocessor

Evaluation Plan



Summary

Post Moore $\rightarrow$ SPT, GPT++, heterogeneity

Summary

Post Moore $\rightarrow$ SPT, GPT++, heterogeneity

- **Many-cores**?

Summary

Post Moore $\rightarrow$ SPT, GPT++, heterogeneity

- **Many-cores**?$\rightarrow$ little focus on dependability

Summary

Post Moore $\rightarrow$ SPT, GPT++, heterogeneity

- **Many-cores**?$\rightarrow$ little focus on dependability

Hardware Capabilities (CHERI)

Summary

Post Moore $\rightarrow$ SPT, GPT++, heterogeneity

- **Many-cores**?$\rightarrow$ little focus on dependability

Hardware Capabilities (CHERI)

- Native spacial and support for temporal safety

Summary

Post Moore $\rightarrow$ SPT, GPT++, heterogeneity

- **Many-cores**?$\rightarrow$ little focus on dependability

Hardware Capabilities (CHERI)

- Native spacial and support for temporal safety
- Not yet seen in many-core context

Summary

Post Moore $\rightarrow$ SPT, GPT++, heterogeneity

- **Many-cores**?$\rightarrow$ little focus on dependability

Hardware Capabilities (CHERI)

- Native spacial and support for temporal safety
- Not yet seen in many-core context

Kernsensus: A consensus driven kernel design for Many-core OSs

References i

Nils Asmussen et al. “M3: A Hardware/Operating-System Co-Design to Tame Heterogeneous Manycores”. In: *Proceedings of the Twenty-First International Conference on Architectural Support for Programming Languages and Operating Systems*. ASPLOS ’16. event-place: Atlanta, Georgia, USA. New York, NY, USA: Association for Computing Machinery, 2016, pp. 189–203. ISBN: 978-1-4503-4091-5. DOI: 10.1145/2872362.2872371. URL: https://doi.org/10.1145/2872362.2872371.

Matthias Hille et al. “SemperOS: A Distributed Capability System”. In: *2019 USENIX Annual Technical Conference (USENIX ATC 19)*. Renton, WA: USENIX Association, July 2019, pp. 709–722. ISBN: 978-1-939133-03-8. URL: https://www.usenix.org/conference/atc19/presentation/hille.

References ii

- John Shalf. "The future of computing beyond Moore's law". In: *Philosophical Transactions of the Royal Society A* 378.2166 (2020). Publisher: The Royal Society Publishing, p. 20190061.
- Neil Thompson and Svenja Spanuth. "The decline of computers as a general purpose technology: why deep learning and the end of Moore's Law are fragmenting computing". In: *Available at SSRN 3287769* (2018).
- Robert N.M. Watson et al. "CHERI: A Hybrid Capability-System Architecture for Scalable Software Compartmentalization". en. In: *2015 IEEE Symposium on Security and Privacy*. San Jose, CA: IEEE, May 2015, pp. 20–37. ISBN: 978-1-4673-6949-7. DOI: 10.1109/SP.2015.9. URL: https://ieeexplore.ieee.org/document/7163016/ (visited on 07/27/2020).