A23-005: Open Source, High Assurance Hardware and Software Co-Design

ADDITIONAL INFORMATION
N/A

TECHNOLOGY AREAS:
Electronics | Information Systems

MODERNIZATION PRIORITIES:
Advanced Computing and Software | Microelectronics

KEYWORDS:
RISC-V, seL 4, high assurance, softcore procressor, FPGA, computer architecture

OBJECTIVE:
Open source hardware and software offer new opportunities for creating high assurance computing. Currently, seL 4 microkernel uses blocks of assembly language instructions for security primitives. Hardware primitives and software instructions can be added to the extensible RISC-V architecture to support seL 4 and other high assurance microkernels. Offer shall proposed a FPGA softcore RISC-V architecture to support and simplify the seL 4 high assurance microkernel.

ITAR:
The technology within this topic is restricted under the International Traffic in Arms Regulation (ITAR), 22 CFR Parts 120-130, which controls the export and import of defense-related material and services, including export of sensitive technical data, or the Export Administration Regulation (EAR), 15 CFR Parts 730-774, which controls dual use items. Offerors must disclose any proposed use of foreign nationals (FNs), their country(ies) of origin, the type of visa or work permit possessed, and the statement of work (SOW) tasks intended for accomplishment by the FN(s) in accordance with section 3.5 of the Announcement. Offerors are advised foreign nationals proposed to perform on this topic may be restricted due to the technical data under US Export Control Laws.

DESCRIPTION:
Current generation aviation systems were not developed with strong computer security requirements. Past cyber threats, [1]-[2], Spectre [3], Meltdown [4], current cyber treats, and future cyber treats need to be countered. Embedded system designs are typically based on commodity hardware optimized exclusively for speed – leading to critical cyber vulnerabilities that can have devastating effects on safety and mission effectiveness. This has also led to the unsustainable “Perimeter, Patch, Pray” Information Assurance strategy [5] that is simply impractical for fielded aviation and missile systems.

De Clercq and Verbauwhede [6] have recommended more hardware based security over software. Hardware based operating systems concepts began in the 1970’s [7]-[9]. The Intel iAPX 432 [10] pioneered protected objects in 1983. Nakano [11] developed the first practical hardware based operating system in 1995. Renesas released a commercial microcontroller [12] with a simple hardware based operating system in 2014. The RISC-V family of instruction set architectures was published open source in 2010 [13]. RISC-V was designed to be extendable. The high assurance microkernel, seL 4, was developed in 2009 [14]-[15].

We are interested in hardware/software co-design based on open source RISC-V and seL4 microkernel. The seL4 microkernel has blocks of assembly code that are not as rigorously proven as the C code for seL4. By extending RISC-V using hardware based operating system principles, a more streamlined and secure version of seL4 is possible. The offeror is asked to develop a RISC-V and seL4 high assurance FPGA softcore processor.

PHASE I:
For the Phase I proposal, research team shall describe the feasibility (1)-(6) of developing a RISC-V softcore processor with hardware security primitives to simplify, and create a more secure seL4 microcontroller.

(1) describe multidiscipline research team
(2) advantages of developing a seL4 microkernel with fewer blocks of assembly code
(3) advantages seL4 microkernel with fewer blocks of assembly code for formal proof of correctness
(4) describe the design features of RISC-V that allow for implementing hardware security primitives to support high assurance microkernel's like seL4.
(5) describe how (2)-(4) can simplify machine proof-of-correctness.
(6) propose a Future of Vertical Lift application for RISC-V/seL4 co-design for "Open Source, High Assurance Hardware and Software Co-Design."

For the phase I effort, the offeror shall demonstrate the feasibility and performance benefits of RISC-V/seL4 co-design for "Open Source, High Assurance Hardware and Software Co-Design." Offeror shall develop models, simulations, prototypes, etc. to determine technical feasibility (1)-(6) of RISC-V/seL4 co-design for "Open Source, High Assurance Hardware and Software Co-Design."

PHASE II:

Research team shall develop a RISC-V/seL4 co-design for "Open Source, High Assurance Hardware and Software Co-Design" for Future of Vertical Lift application. Research team shall deliver a year 1 report and a year 2 report describing system architecture and test results. Offeror shall deliver to the government point of contact for test and evaluation: 2 prototype RISC-V/seL4 co-design for "Open Source, High Assurance Hardware and Software Co-Design" systems including all codes, software, etc. and licenses for all development tools to build and use the system. Research team shall provide 3 days of on-site training for the system.

PHASE III DUAL USE APPLICATIONS:

Offer shall commercialize RISC-V/seL4 co-design for "Open Source, High Assurance Hardware and Software Co-Design" for both government and commercial application spaces. Offeror will develop and market high assurance system based on phase II development work and marketing plans from phase I and II. Offeror will integrate high assurance system into an Army Aviation or Missile subsystem currently under development or via technology refresh.

REFERENCES:

1. S. King, et al.: "SubVirt: implementing malware with virtual machines," IEEE Symposium on Security and Privacy, pp. 1-14, 21-24 May 2006.
2. R. Fannon: An analysis of hardware-assisted virtual machine based rootkits, Thesis, Naval Postgraduate School, June 2014. calhoun.nps.edu/handle/10945/42621
3. P. Kocher, et al.: "Spectre Attacks: Exploiting Speculative Execution," Cornell University Library, 3 Jan 2018. https://arxiv.org/pdf/1801.01203.pdf
4. M. Lipp, et al.: "Meltdown," Cornel University Library, 3 Jan 2018. https://arxiv.org/pdf/1801.01207.pdf; [5] Darpa: "Baking Hack Resistance Directly into Hardware," 4/10/2017. https://www.darpa.mil/news-events/2017-04-10
5. R. De Clercq and I. Verbauwhede: "A survey of Hardware-based Control Flow Integrity (CFI)," pp. 4-5, 31 Jul 2017. arxiv.org/ftp/arxiv/papers/1706/1706.07257.pdf
6. G. Sockut: "Firmware/hardware support for operating systems: principles and selected history," ACM SIGMICRO Newsletter, Volume 6 Issue 4, pp. 17 - 26, Dec. 1975. dl.acm.org/citation.cfm?id=1217198; [8] G. Brown, et al.: "Operating system enhancement through firmware," Proceedings of the 10th annual workshop on Microprogramming, ACM SIGMICRO Volume 8 Issue 3, pp. 110-133, Sept. 1977. https://dl.acm.org/citation.cfm?id=800102.803324
7. Higher Order Software: "Techniques for Operating System Machines," Technical Report # 7, July 1977. www.dtic.mil/dtic/tr/fulltext/u2/772809.pdf
8. I. Witten, et al.: "An introduction to the architecture of the Intel iAPX 432," IEEE Software & Microsystems, Vol. 2 , Issue 2, pp. 29-34, April 1983
9. T. Nakano: "Hardware Implementation of a Real-time Operating System," IEEE TRON Project International Symposium, Tokyo, Japan, pp. 34-42, 28 Nov – 2 Dec, 1995
10. https://www.renesas.com/en-us/products/factory-automation/multi-protocol-communication/r-in32m3-hardware-rtos.html
11. A. Waterman: "Design of the RISC-V Instruction Set Architecture," Thesis, EECS Department, University of California, Berkeley 2016. http://www2.eecs.berkeley.edu/Pubs/TechRpts/2016/EECS-2016-1.pdf
12. L4 microkernel family, accessed 12/7/22, https://en.wikipedia.org/wiki/L4_microkernel_family

13. G. Klein, et al.: "seL4: Formal verification of an OS kernel," ACM Symposium on Operating System Principles, Big Sky, MT, USA October 2009,
14. V. Ushakov, et al.: "Trusted Hart for Mobile RISC-V Security," https://arxiv.org/pdf/2211.10299.pdf
15. R. Nair: "Evolution of Memory Architecture," IEEE Proceedings, Vol. 103, No. 8, pp. 1331 – 1345, August 2015
16. P. Karger and R. Schnell: "Thirty Years Later: Lessons from the Multics Security Evaluation," IEEE Annual Computer Security Applications Conference, pp. 119-126, Las Vegas, NV, 9-13 Dec. 2002.
17. Tiwari, M., et al.: "Crafting a Usable Microkernel, Processor, and I/O System with Strict and Provable Information Flow Security," ACM Proceedings of the 38th annual international symposium on Computer architecture, pp. 189-200, San Jose, CA, 4-8 June 2011
18. M. McCoyd, et al.: "Building a Hypervisor on a Formally Verifiable Protection Layer," https://people.eecs.berkeley.edu/~mmccoyd/papers/minvisor-hicss-12.pdf

TOPIC POINT OF CONTACT (TPOC):

TPOC-1: William Crowe
PHONE: 2568764956
EMAIL: william.m.crowe12.civ@army.mil

TPOC-2: Patrick Jungwirth
PHONE: 4102786174
EMAIL: patrick.w.jungwirth.civ@army.mil