Research Summary

Yuanchao Xu

My research interest lies in the intersection of computer architecture and computer security. Cybercrime already costs over 1% of the world's economy and it is growing in scale and cost [1]. Many security techniques are impractical due to their high performance overheads. Improving their performance through hardware-software codesigns not only makes them more practical, but also gives them the needed margin for future security improvements.

My research focuses on the compound complexities in memory security, reliability, and performance caused by emerging memory technology in the approaching post-Moore era. **My research cuts across the stack**, from **compilers** to **operating systems**, **memory**, and **processors/accelerators**. With *vertically-integrated solutions*, my research pioneered several distinctive directions toward secure, efficient memory, including new temporal exposure reduction protection for persistent memory, scalable intra-process isolation isolations, the decoupled trusted execution environment, persistent memory reliability, and architectural designs in the approaching post-Moore era. The results have influenced the recent development of memory designs and support in both academic research and industrial practitioner, leading to 10 publications in top-tier architecture conferences (ISCA (×3), ASPLOS (×2), MICRO, HPCA (×4)) and **an impact on real-world products through my 20-month internship at SystemsResearch@Google.**

Current Research

With Moore's law coming to an end, it is imperative to seek revolutionary approaches of computer architecture for sustained advancement of computing. Alternatives to traditional architectures are emerging, exemplified by quantum computing, computing and storage, and more. The changes will prompt a plethora of exciting new challenges and opportunities for research on efficient hardware security, which is my long-term research focus.

In the near term, I will focus on the many open problems to security brought by recent trends in computing, including emerging memory technologies and extreme heterogeneity in System on Chip (SoC).

New attacks and defenses in emerging memory technologies. Computer architecture is in the post-Moore era and approaches the memory wall. New hardware is consistently proposed to improve performance and power efficiency or break the memory wall. The new complexities hence call for a systematic understanding of the implications of security and the creation of protection techniques that fit new hardware. This is particularly urgent as new hardware is getting into various computers, from data centers, to servers, laptops, and even IoT devices. Proactive research is especially essential in security, as history has repeatedly taught us. My future research will explore new attacks and defenses in emerging hardware, including emerging memory [2, 3], memory pooling and memory semantic SSD through Compute eXpress Link (CXL), process-in-memory, and others. This research seeks to advance the understanding of security implications and potential new defenses before new hardware is widely adopted in the real world.

Secure heterogeneous system-on-chips. Secure SoC designs are essential, as SoCs introduce unprecedented challenges with untrusted on-chip heterogeneous Intellectual Properties (IPs) and new physical attacks (e.g., advanced invasive attacks). From an architectural design perspective, SoC security designs pursue minimal area and energy overhead to be applicable to a wide range of complex situations. In facing these challenges, how to isolate or minimize potential attacks from other accelerators through software and hardware interfaces is a promising direction. Emerging heterogeneous chiplet-based architecture for SoCs further complexes the above problems due to more independent components. Based on my previous research about reducing memory exposure [2, 4] and SoC understanding [5, 6], this research could enable novel SoC-level security techniques with reduced area and power overhead, including new SoC isolation, new SoC communication protocols, and holistic approaches from software to hardware.

References

[1] O Sviatun, O Goncharuk, Chernysh Roman, Olena Kuzmenko, and Ihor V Kozych. Combating cybercrime: economic and legal aspects. *WSEAS Transactions on Business and Economics*, 18:751–762, 2021.

[2] **Yuanchao Xu**, Yan Solihin, and Xipeng Shen. Merr: Improving security of persistent memory objects via efficient memory exposure reduction and randomization. In *Proceedings of the Twenty-Fifth International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS)*, pages 987–1000, 2020.

[3] **Yuanchao Xu**, Chencheng Ye, Xipeng Shen, and Yan Solihin. Temporal exposure reduction protection for persistent memory. In *2022 IEEE International Symposium on High-Performance Computer Architecture (HPCA)*, pages 908–924, 2022.

[4] **Yuanchao Xu**, Chengchen Ye, Yan Solihin, and Xipeng Shen. Hardware-based domain virtualization for intra-process isolation of persistent memory objects. In *2020 ACM/IEEE 47th Annual International Symposium on Computer Architecture (ISCA)*, pages 680–692, 2020.

[5] **Yuanchao Xu**, Mehmet Esat Belviranli, Xipeng Shen, and Jeffrey Vetter. Pccs: Processor-centric contention-aware slowdown model for heterogeneous system-on-chips. In *54th Annual IEEE/ACM International Symposium on Microarchitecture (MICRO)*, pages 1282–1295, 2021.

[6] Hsin-Hsuan Sung, **Yuanchao Xu**, Jiexiong Guan, Wei Niu, Bin Ren, Yanzhi Wang, Shaoshan Liu, and Xipeng Shen. Brief industry paper: Enabling level-4 autonomous driving on a single $1 k off-the-shelf card. In *2022 IEEE 28th Real-Time and Embedded Technology and Applications Symposium (RTAS)*, pages 297–300. IEEE, 2022.