第二十四章　实验 6: 进阶实践

24.1　简介

课程配套的前五个实验主要面向初学操作系统的本科生，以帮助学生掌握操作系统的基本实现为目标。作为进阶性的实验，实验 6 旨在让有兴趣的读者尝试理解、设计和实现较为复杂的一些操作系统功能或模块。下一节将列出一些在 ChCore Labs 中没有出现但值得尝试的实践内容，其中大多实践内容我们在 ChCore 微内核操作系统中已经验证过可行性。读者可以根据自身的兴趣选择并实践。

24.2　实践内容

- **系统虚拟化**：利用 AArch64 提供的硬件虚拟化能力，在微内核架构下实现一个精简的虚拟机监控器，能够支持运行多个虚拟机。可以参考的工作包括：微内核架构下的虚拟化设计 [9]、在 ARM 体系结构上实现 KVM [2] 等。

- **可信执行环境**：利用硬件使能的可信执行技术（比如 ARM TrustZone 和 Intel SGX），实现对安全应用的保护，使得即便是运行在特权级的微内核也不能访问安全应用的数据和运行状态。可以参考的工作包括：通过 TrustZone 技术保护手机应用 [7]、使用 SGX 技术保护应用程序 [1] 等。

- **用户态网络协议栈**：在微内核架构下实现一个用户态网络服务，支持应用能够使用 socket 等常见接口进行网络编程。可以参考的工作包括：微内核式的网络服务 [6]、轻量级的网络协议栈 lwIP [4] 等。

- **文件系统**：面向新型存储设备，在微内核架构下设计并实现高性能的用户态文件系统（或移植现有文件系统到微内核架构上）。可以参考的工作

包括：面向非易失性内存的用户态文件系统 [10, 3] 等。

- **进程间通信优化**：进程间通信的开销对微内核操作系统的整体系统性能非常重要。请尝试利用软件设计或软硬件协同的方法降低进程间通信的开销。可以参考的工作包括: 通过软件方法降低系统调用的开销 [8]、利用新型硬件加速进程间通信 [5] 等。

参考文献

[1] Andrew Baumann, Marcus Peinado, and Galen Hunt. Shielding applications from an untrusted cloud with haven. *ACM Transactions on Computer Systems (TOCS)*, 33(3):1–26, 2015.

[2] Christoffer Dall and Jason Nieh. Kvm/arm: the design and implementation of the linux arm hypervisor. *Acm Sigplan Notices*, 49(4):333–348, 2014.

[3] Mingkai Dong, Heng Bu, Jifei Yi, Benchao Dong, and Haibo Chen. Performance and protection in the zofs user-space nvm file system. In *Proceedings of the 27th ACM Symposium on Operating Systems Principles*, pages 478–493, 2019.

[4] Adam Dunkels. Design and implementation of the lwip tcp/ip stack. *Swedish Institute of Computer Science*, 2(77), 2001.

[5] Jinyu Gu, Xinyue Wu, Wentai Li, Nian Liu, Zeyu Mi, Yubin Xia, and Haibo Chen. Harmonizing performance and isolation in microkernels with efficient intra-kernel isolation and communication. In *2020 USENIX Annual Technical Conference (USENIX ATC 20)*, pages 401–417, 2020.

[6] Michael Marty, Marc de Kruijf, Jacob Adriaens, Christopher Alfeld, Sean Bauer, Carlo Contavalli, Michael Dalton, Nandita Dukkipati, William C Evans, Steve Gribble, et al. Snap: a microkernel approach to host networking. In *Proceedings of the 27th ACM Symposium on Operating Systems Principles*, pages 399–413, 2019.

[7] Nuno Santos, Himanshu Raj, Stefan Saroiu, and Alec Wolman. Using arm trustzone to build a trusted language runtime for mobile applications.

In *Proceedings of the 19th international conference on Architectural support for programming languages and operating systems*, pages 67–80, 2014.

[8] Livio Soares and Michael Stumm. Flexsc: Flexible system call scheduling with exception-less system calls. In *Osdi*, volume 10, pages 1–8, 2010.

[9] Udo Steinberg and Bernhard Kauer. Nova: a microhypervisor-based secure virtualization architecture. In *Proceedings of the 5th European conference on Computer systems*, pages 209–222, 2010.

[10] Haris Volos, Sanketh Nalli, Sankarlingam Panneerselvam, Venkatanathan Varadarajan, Prashant Saxena, and Michael M Swift. Aerie: Flexible file-system interfaces to storage-class memory. In *Proceedings of the Ninth European Conference on Computer Systems*, pages 1–14, 2014.

实验 *6*：扫码反馈