تحلیل مقاله در رابطه با درس معماری پیشرفته

تهیه و ارائه از: مسعود باقری

دوره کارشناسی ارشد

Design High-Confidence Computers using Trusted Instructional Set Architecture and Emulators

طراحی کامپیوترهایی با قابلیت اعتماد بالا با استفاده از معماری مجموعه دستورالعمل‌های ایمن شده و شبیه‌سازها

شاونگ بائو

تعریف مسأله و هدف اصلی مقاله:

سوال اصلی مطرح شده در مقاله:

- توجه زیادی در طراحی، توسعه، شبیه سازی (سیمولاتور) و الگوبرداری یا تقلید (امولاتور) از پردازنده‌های جدید که در برابر سو استفاده‌ها و حملات ایمن هستند، لازم است. و سوال اصلی این است که؛ آیا می‌توان در طراحی پردازنده‌های نسل جدید، از روش‌هایی استفاده کرد که امنیت لازم تأمین شده و بتوان حملات کانال جانبی را دفع نمود؟

چه مشکلی باید برطرف شود؟

- Spectre و Meltdown، پردازنده‌های مدرنی را که از پیش‌بینی انشعاب و خطوط لوله استفاده می‌کنند، مورد سوء استفاده قرار داده و آسیب پذیر می‌کنند. محاسبات با اطمینان بالا، به معماری مجموعه دستورالعمل قابل اعتماد، هسته های نفوذناپذیر و غیرقابل تغییر و سیستم عامل های امن، متکی است. هدف از این تحقیق پیشنهاد روش‌هایی در طراحی پردازنده‌های نسل جدید عنوان شده که قابل اعتماد بوده و در برابر این حملات مصونیت دارند.
- Spectre یک آسیب پذیری است که امکان خواندن مکان‌های دلخواه در حافظه اختصاص یافته به یک برنامه را فراهم می‌کند.
- Meltdown یک آسیب پذیری سخت افزاری است که بر ریز پردازنده‌های Intel x86 پردازنده‌های IBM POWER و برخی از ریز پردازنده های مبتنی بر ARM تأثیر می گذارد و به فرایند تقلبی اجازه می‌دهد تا تمام حافظه را بخواند ، حتی اگر مجاز به انجام آن نباشد.

چه ضرورتی برای مطرح شدن مسئله است؟

- حملات کانال جانبی و بطور مشخص Spectre و Meltdown، پردازنده‌های جدید را آسیب پذیر می‌کند و آنها را به عنوان نقطه‌ای جهت سواستفاده هکرها قرار می دهد.
- غیرفعال کردن پیش بینی کننده انشعاب و خط لوله قطعاً راه حل خوبی نیست.
- غیرفعال کردن خطوط لوله، افزایش سرعت کلی حاصل از موازی سازی را محدود می‌کند، بنابراین پردازنده ها به طور قابل توجهی، کند می‌شوند.
- درعین حال، حملاتی که از نشتی حاصل از اشکال زدایی استفاده می‌کنند، می‌تواند مهاجمان را به عبور از ماشین‌های مجازی در یک محیط رایانش ابری هدایت کنند .
- وصله‌های نرم افزاری فعلی فقط می‌توانند مسائل غیر ضروری اطراف Meltdown را برطرف کنند.

چه روشهایی قبلا برای این کار انجام شده؟

- پیاده سازی ماشین تورینگ با استفاده از مفهوم برنامه انباشته Turing Machine
- مجموعه دستورالعمل‌های مبتنی بر دسترسی پی‌درپی یا متوالی و محاسبات خطی برای مدت طولانی از دهه ۱۹۴۵ تاکنون بر معماری کامپیوتر مسلط بوده‌اند.
- جان. ال هنسی، مجموعه دستورالعمل‌های کاهش یافته RISCرا در دهه ۱۹۸۰ پیشنهاد کرد. در معماری RISC کلیه دستورالعمل‌ها با تعداد چرخه مساوی اجرا می‌شوند Reduced Instruction Set Computer
- طرح سیلیکون جدید اپل، از معماری RISC همراه با بهبود امنیت برای کاهش خطرات مرتبط با حمله روز صفر و محافظت در برابر اجرای کد از راه دور استفاده می‌کند.
- مولدر و همکاران، معماری اصلاح شده ای را ارائه می‌دهد که در آن برای محافظت از نشت کانال جانبی برای مدار، تولید ماسک می‌شود.
- صدیقی و همکاران، طرحی را برای استفاده از FPGA در پیاده سازی RISC-V برای جلوگیری از نشتی در برابر حملات بدافزار ارائه داد.

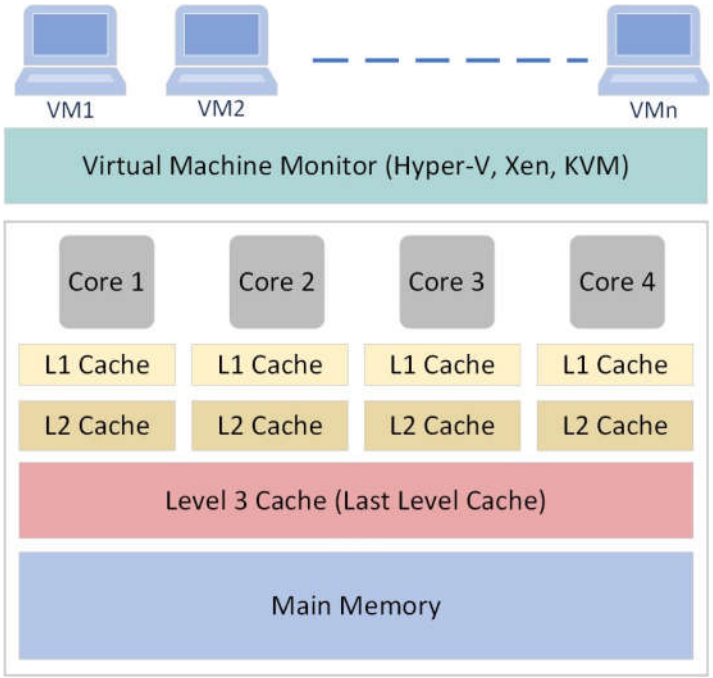
روش پیشنهادی ارائه شده چیست؟

- استفاده از برنامه‌ها و بستر های متن باز
- تأکید بر استفاده از امولاتورها در شبیه سازی برای آشکار شدن صحیح و دقیق رفتار سیستم در مواجهه با تهدید. Qemu
- استفاده از پردازنده‌های RISC-V برای استفاده از حداکثر توان توسعه دهندگان در مقابل تهدید.
- تصحیح ساختار و معماری مجموعه دستورالعمل‌ها و پیاده سازی برای ایجاد حداکثر امنیت.

توضیح راه حل پیشنهادی مقاله برای حل مسئله:

- برای توضیح نحوه عملکرد روش پیشنهادی لازم است مروری بر نحوه عملکرد حملات کانال جانبی و بطور مشخص،Spectre و Meltdown داشته باشیم.
- متأسفانه، وصله‌های نرم افزاری که برای مقابله با حمله Meltdown رایج هستند، سربار قابل توجهی برای پردازنده‌ها به ارمغان می‌آورند ، بنابراین سرعت را کاهش می‌دهند. تقسیم حافظه سخت روش دیگری برای حل این مشکل است. اینتل و بسیاری از پردازنده‌ها از فناوری تقسیم حافظه استفاده کرده‌اند. اما فضای هسته اصلی یا کرنال موجود و تقسیم فضای کاربر "امن" تلقی می‌شود که این خود یک حفره محسوب می‌شود.

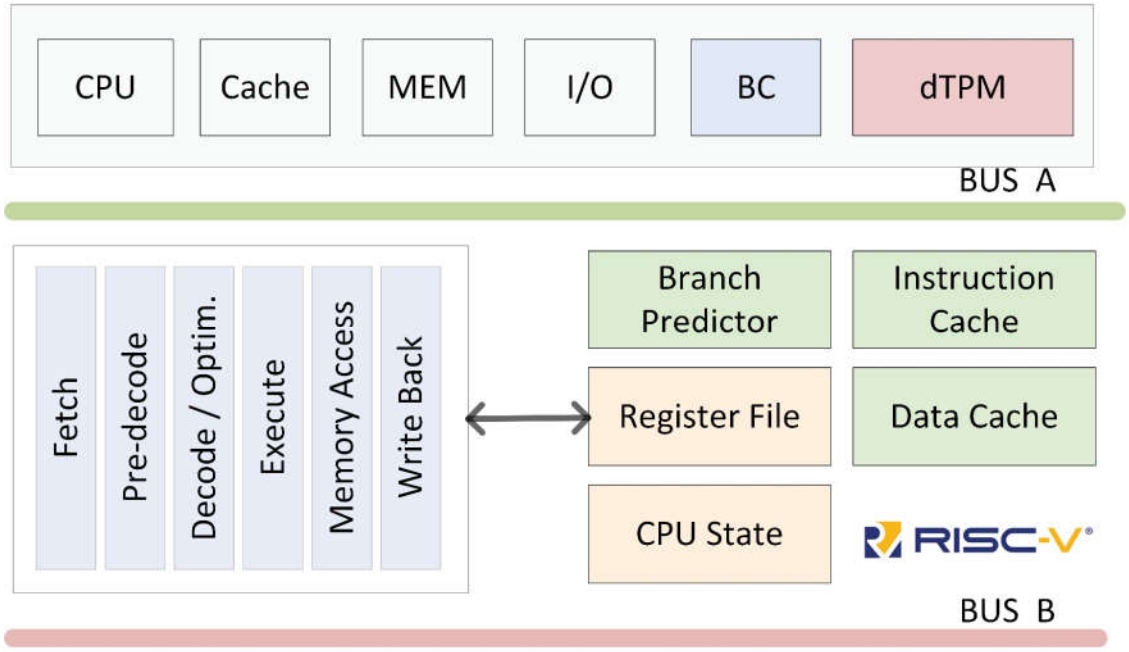
معماری عمومی که سیستم را آسیب‌پذیر نموده:



روش پیاده سازی شده برای حل مسئله مقاله به چه صورت است؟

- همانطور که نویسندگان مقاله اشاره کردند، حملات کانال جانبی بسیار گسترده بوده و تقریبا تمام تولیدکنندگان بر این موضوع اتفاق نظر دارند که راهکار مقابله با حملات Spectre و Meltdown در اصلاح معماری پردازنده‌ها می‌باشد
- اصلاح معماری از دو بخش اصلاح مجموعه دستورالعمل‌ها و پیاده‌سازی تشکیل می‌شود.
- اصلی‌ترین اقدام امنیتی درنظر گرفتن ماژول مجزای تعییین کننده اعتبار dTPM بصورت یک تراشه یا میکروکنترلر جداگانه و ایزوله شده است که تمام منابع محاسباتی لازم در این بسته تراشه مجزا وجود دارد. discrete Trusted Platform Module
- در ISA پیشنهادی دو باس یا گذرگاه وجود دارد.

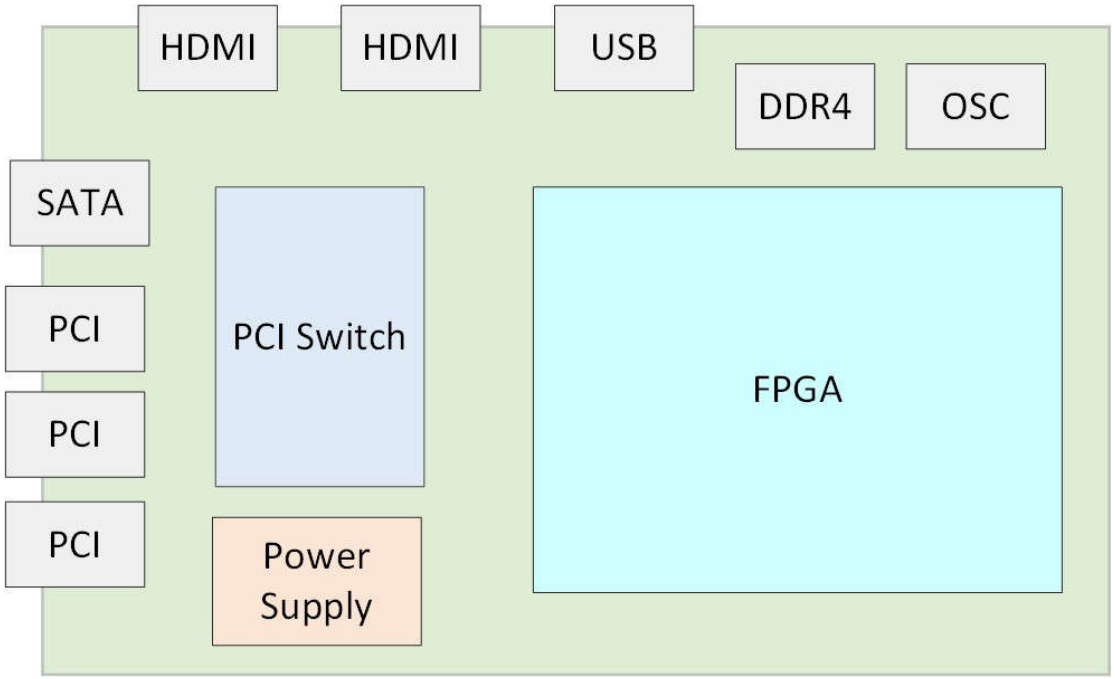
معماری پیشنهادی:



روش ارائه شده به چه صورت پیاده سازی شده؟

- QEMU بهترین انتخاب برای شبیه سازی پردازنده‌های مختلف است.
- دستورالعمل های RISC با توانمندی ارتقا یافته سخت افزاری (CHERI) ISAهای معمولی را با ویژگی جدیدی برای محافظت از حافظه ریز و تقسیم بندی نرم افزار گسترش و پیشرفت می‌دهد.
- استفاده از QEMU-CHERI در RISC-V، امنیت سطح سخت افزاری را فراهم می‌کند که می‌تواند برای پردازنده‌های واقعی تقلید شود.
- Chisel یک زبان طراحی سخت افزار با ویژگی‌های پیشرفته تولید مدار است. علاوه بر این، می‌تواند برای طراحی هر دو طرح منطق دیجیتالی ASIC و FPGA استفاده شود. The constructing hardware in a Scala Embedded Language
- TRISA در سیستم ۶۴ بیتی لینوکس (اوبونتو ۱۸.۱۰)، آزمایش می‌شود.
- RISC-V Linux در یک برد توسعه یافته است یعنی SiFive HiFive Unleashed

بُورد HiFive دارای ویژگی‌های است که باعث شده در تمام دنیا برای اهداف توسعه‌ای بکار برده شود.



نحوه مقایسه ایده مطرح شده با دیگر ایده‌های مطرح شده در مقاله:

- با توجه به دامنه خسارات وارده و گستردگی حملات Spectre و Meltdown اقدامات زیادی نیز بخصوص از جانب تولید کنندگان پردازنده ها برای مقابله با آن صورت گرفته. لذا اقدامات شاخص معرفی شده و درباب مقایسه به تفاوت تکنیک‌ها ابزار و زیرساخت این روش پرداخته شده است. مثلا قابلیت‌هایی که دستورالعمل‌های کاهش یافته و پردازنده‌ها و شبیه‌سازهای متن باز و ... ایجاد می‌کنند.

نقاط قوت و ضعف مقاله:

- مقاله حاضر، ایده بسیار خوب و عالی با دلایل محکم و قوی ارائه نموده ولی عملا هیچگونه پیاده سازی انجام نشده. نه کدی در اختیار قرار داده شده و شکل و نمودار و نتایج آزمایش در برابر حمله و ...
- تمام تمرکز مقاله و ایده مطرح شده بر روی استفاده از تکنیک‌های نرم افزاری و سخت افزاری متن باز برای حذف نقش زنجیره تأمین کنندگان و مالکین است درحالیکه خودش هیچ جزییاتی در اختیار قرار نداده. مثلا اصلاحات در چگونگی آدرس دهی، واکشی و رمزگشایی بخش آپکد و ...

جمع بندی و پیشنهادات برای کارهای آتی:

- نویسندگان مقاله عقیده دارند که شبیه سازی ۶۴ بیتی RISC-V TRISA نشان می‌دهد که از طریق بازنگری اساسی در سطح ISA با ملاحظاتی برای افزایش سرعت سخت افزار، امنیت با کمک حفاظت از حافظه، کنترل بهتر پیش بینی انشعاب یا پیش بینی کننده پرش، جلوگیری از خالی کردن حافظه ریز معماری ایمن، افزایش کنترل یکپارچگی، موتور رمزنگاری خارجی و استفاده از RISC-V TCB، بهبود می‌یابد.
- تعمیم دادن این شبیه سازی به رایانه‌های نسل بعد برای تولید رایانه‌هایی با قابلیت اطمینان بالا در محاسبات، می تواند یک چشم انداز ملی ایجاد نماید.

خدا یار و نگهدار شما