RV与芯片评论.20210410：2021年第15周(总第37期)

[PDF] RECLAIMING THE UTOPIA: ALTERNATE ECOSYSTEMS FOR SAFEGUARDING HUMAN RIGHTS IN...

Towards Verifiable Phrase Search over Encrypted Cloud-Based IoT Data

[PDF] Compiler-Assisted Hardening of Embedded Software Against Interrupt Latency Side-Channel Att...

[PDF] Speedster: A TEE-assisted State Channel System

本期概要

- 芯来支持鸿蒙系统
- GreenWaves的超低功耗处理器
- OpenEuler支持RISC-V果壳处理器
- RISC-V安全论坛将于14日召开

重点聚焦

相关周报

- semi engineering Week In Review:
  - Blog Review:
  - Design, Low Power:
  - Manufacturing, Test:
  - Auto, Security, Pervasive Computing:
- IoT News: （Site）:
- OSDT Weekly:（zhihu，Github）:
- 泰晓咨询: （Site）:
- PLCT开源进展:（Github，zhihu）:
- RT-Thread: （oschina）:
- 科技爱好者周刊: （yuque）:
- 硅农亚历山大: RISC-V双周报：3月26日-4月8日
- 痞子衡嵌入式半月刊: （zhihu）:
- 半导体一周要闻－莫大康: （eet-china）:

技术动态

"利用GreenWaves的RISC-V打造纳米无人机大脑 (From news.moore.ren 2021.04.10)"

> 展示了一种并行超低功耗（PULP）处理器和卷积神经网络（CNN），可以赋予现成的Crazyflie 2.1纳米无人机实现 "顶级自主导航能力"——尽管体积和重量都很小
> GreenWaves开发的首款GAP 8 处理器，于2020年1月批量生产。该处理器适用于物联网应用场景，如人员或物体计数与注意力检测，同时可大幅度降低系统整体功耗，延长电池寿命。第二代GAP 9处理器为可听设备提供领先技术，如神经网络控制、超低延迟、主动降噪、基于神经网络的降噪和3D环绕音等
> - "聚焦边缘AI，GreenWaves携超低功耗GAP处理器亮相2021慕尼黑上海电子展 (From www.eet-china.com 2021.04.10)"

"苹果iPhone 13 A15芯片下月量产,2021新机芯片、售价、上市时间锁定 (From www.eet-china.com 2021.04.10)"

"芯来科技 RISC-V 处理器宣布支持鸿蒙 LiteOS-M 内核 (From www.sohu.com 2021.04.10)"

> 芯来科技表示，为方便客户进行基于鸿蒙生态的 RISC-V 软件开发，在 Nuclei RISC-V 32 位处理器上移植并适配了鸿蒙 LiteOS-M 内核。目前该内核已可支持 Nuclei Demo SoC——FPGA 评估软核，和基于芯来科技的 RISC-V 内核的 MCU——GD32VF103。

"北京君正：公司已经展开了基于RISC-V的CPU内核研发 (From www.nbd.com.cn 2021.04.10)"

"华为 openEuler 已支持 RISC-V 架构，成功支持果壳处理器 (From www.sohu.com 2021.04.10)"

> 据 openEuler 社区官方发布，近日，优矽科技签署 CLA，正式加入 openEuler 社区。

产业风云

"变频智能芯片吃紧本土配套率不足 部分家电价格或上涨10%-20% (From finance.sina.com.cn 2021.04.10)"

> 目前，家电芯片的主要应用是变频智能家电领域，主要芯片包括MCU主控方案、AC-DC芯片、PFC芯片等，变频家电中整机芯片成本约为10%-15%，随着变频智能性能升级同步增加。
> 头部家电企业很早就进入芯片领域，且能够在部分环节实现自给自足，但目前大部分家电企业自主研发的芯片还不能覆盖全产业链，产品部分主要芯片还是依赖进口，短期内，部分家电产品会在原材料涨价、芯片等短缺的多重压力下，价格出现10%-20%左右的上涨。

"乐鑫科技3月下旬接待19家机构调研 AI计算是一大发力点 (From finance.eastmoney.com 2021.04.10)"

> 表示AI计算将是之后新产品的一大发力点。除了Wi-Fi6芯片，目前尚有RISC-V核处理器、低功耗蓝牙、Wi-Fi6FEM等在研项目正常进行中，去年底推出的ESP32-C3芯片，已内含自研的RISC-V处理器；新品ESP32-C3和ESP32-S3在射频性能上已经有了非常出色的表现，TX在802.11n/HT40/MCS7模式下典型发射功率可达到18.5dBm，对于公司在研的其他带射频的芯片项目来说是很好的技术基础。

"全志科技：基于平头哥内核进行的研发项目进展顺利 (From kuaixun.stcn.com 2021.04.10)"

> "全志科技与平头哥合作的RISC-V开发板即将推出 (From finance.sina.com.cn 2021.04.10)"

"为芯片，高通阿蒙“彻夜难眠”，台积电也可以走后门了 (From www.eet-china.com 2021.04.10)"

> 芯片行业的缺货涨价已经不是什么新闻，今天我们来看看这个行业的“众生相”，首先是高通即将上任的阿蒙突然发现：台积电也可以走后门了；而另一边，为了解决芯片问题，特别是汽车芯片问题，美国参议院又准备对半导体立法；同样是汽车芯片短缺的锅：现代汽车在经历过每周检查库存的艰难日子后，其电动汽车”终于“停产了；在苹果芯片也将面临短缺的时候，调查公司的一项结果让我们同样震惊：美国青少年其实也把iPhone当成奢侈品；我们就来看看iPhone的“内芯”中苹果与Arm的那段过往；最后，我们来介绍阅读美国作者的文章：RISC-V的兴起，让开源从软件普及到硬件。

"国产EDA换道超车，5年内实现全流程基本没有问题 (From finance.sina.com.cn 2021.04.10)"

> 邸志雄说：“芯华章的数字验证工具实现了国内从无到有的突破，其‘灵验（EpicFV）’开源形式验证EDA也是全球第一款。验证类型的工具销售额占所有EDA工具销售额的30%左右，需求量大且市场价值高。”

"易灵思钛金系列FPGA扩充至包含 1M 逻辑单元器件 (From www.eet-china.com 2021.04.10)"

> FPGA 资深专家 施伟 (Rich Sevcik) 说：“易灵思技术是真正富有突破性的。钛金系列FPGA 提供了可再编程的灵活性和低功耗，以及先前只有高端和极其昂贵的 FPGA 才能达到的性能水平，因此随着边缘计算需求的持续激增，它们有望取代很多的ASIC。”

评论文集

"谈谈ARM v9指令架构的技术亮点以及SoC设计壁垒 (From zhuanlan.zhihu.com 2021.04.10)"

> – 向量架构/SIMD：对比RISC-V标准版仅有一个开源的Hwacha可用 [且是协处理]，V9的向量架构(SIMD)是2048位宽，且是个CPU核，精准投射RISC-V的短板（SiFive等厂商的扩展暂且不谈）；以及针对那些买Mali GPU核堆砌算力卡的低壁垒公司（国内最高堆砌32个Mali core）。设想倘若CPU core能在2048位宽翻炒矩阵，便可以大幅替代臃肿的传统意义Mali板卡方案。而SVE又是传承自Fujitsu Sparc64的传家宝超算技艺，曾经A64FX的笑傲江湖级设计。
> – 片上网络/NoC： 在ARM生态版图里，NOC技术会成为未来SoC设计的重要护城河。
> – 仅列举综上两个技术路线来看，RISC-V恐怕就要沉沦个3-5年了

"RISC-V能否复制Linux的成功? (From www.ednchina.com 2021.04.10)"

> 今年是Linux内核发布三十周年。这一开源代码催生了数百个项目，出现了一大批稳健而灵活的产品。这种成功是否可以复制到开源硬件上呢？RISC-V这样的指令集架构是否也可以像Linux内核作为开源软件的基础一样，成为开源硬件发展的基石呢？

"老将新策 芯片巨头英特尔的“归途”or“去路” (From finance.eastmoney.com 2021.04.10)"

> 郭启祥认为，从长远看来，先进制程本已是寡占市场，英特尔不会轻易放弃，若再搭配先进封装，未来将更容易形成“赢者全拿”之局，只有少数几家厂商瓜分市场。而英特尔坚持IDM模式并开放晶圆代工，业者未来将多一个选择，这对于半导体产业发展是好的。

"RISC-V开源优势愈加显著，CPU架构三足鼎立之势已成? (From www.sohu.com 2021.04.10)"

> 在 CPU 架构领域，Arm 架构和英特尔 x86 架构分别在移动端和桌面端占据了绝大部分市场份额。但是，Arm 架构的收费授权模式和 x86 架构的不对外授权使得越来越多的芯片研发企业转向了开源架构 RISC-V，其开源性和易用性为芯片市场打开了另一扇大门。近日，IEEE Spectrum 的一篇文章详述了 RISC-V 在全球芯片开发商中的崛起态势，并强调开源将在芯片架构竞争中发挥关键作用。

"“每个人都从RISC-V看到了控制自己命运的机会“ (From posts.careerengine.us 2021.04.10)"
"四个领域将获最大红利 | RISC-V全新报告 (From mp.weixin.qq.com 2021.04.10)"

> Semico的调查报告《RISC-V市场蓄势待发》显示，在所有主流终端应用中，人们对RISC-V产品的兴趣日益浓厚，并投入了大量精力从事重大开发。RISC-V器件提供了广泛的性能水平。2020-2025年，RISC-V内核的年复合增长率接近160%。其中，汽车是其服务市场中增长最大的板块，预计其年复合增长率将达到217.7%。
> Semico Research预测，到2025年，RISC-V内核将占据整个CPU内核业务的14%以上。我们还预计，随着RISC-V获得更大的市场份额以及生态系统的不断发展和成熟，这个高度增长的趋势将持续到2025年以后。

其他动态

课程推荐

- "《RISC体系结构与编程语言》 (From zhuanlan.zhihu.com 2021.04.10)"

> 主要讲解物联网和AIoT时代，目前流行的各种RISC处理器（ARM32/64、RISC-V）的体系架构和汇编语言。

- 「线上学习室」学习 Linux和RISC-V基金会共同发起的 RISC-V 课程

- 编译技术入门与实战·第三期·2021春季（连载中）

> https://www.bilibili.com/video/bv14b4y1X7uX
> slides地址：
> https://github.com/lazyparser/becoming-a-compiler-engineer
> 提问和讨论地址：
> https://github.com/lazyparser/becoming-a-compiler-engineer/issues

- 开发一个RISC-V上的操作系统 – 汪辰 – 2021春 – PLCT实验室

> https://www.bilibili.com/video/BV1Q5411w7z5

博文推荐

"【漫画】20多年了，为什么国产CPU还是不行？ | 码农翻身 (From zhuanlan.zhihu.com 2021.04.10)"

> 中国CPU绝对不会就此止步，开源的RISC-V也许就是一个突破点。

"机器学习系统 • 提问 (From mp.weixin.qq.com 2021.04.10)"

> 一个实际运作的机器学习系统包括算法，软件栈，系统硬件，芯片等内容。如何设计，实现和优化一个高效的机器学习系统是一个很重要的话题。最近我和一些系统方向（特别是软件栈）的一线工程师和学

者进行了讨论，大家提出很多有意思的问题。即使还没有明确的答案，好的问题引起的思考和讨论本身就很有价值。下面整理了一些问题，抛砖引玉，也希望更多朋友提出自己的见解。

一周论文

[PDF] A First Look at RISC-V Virtualization from an Embedded Systems Perspective

B Sá, J Martins, S Pinto - arXiv preprint arXiv:2103.14951, 2021

> 本文描述了在火箭芯片核心中对最新版本RISC-V管理程序扩展(H-extension v0.6.1)规范的首次公开实现和评估。为了对现代多核嵌入式和混合临界系统进行有意义的评估，我们将开源静态分区管理程序Bao移植到RISC-V中。我们还扩展了RISC-V平台级中断控制器(PLIC)，以支持具有低和确定性延迟的直接客户中断注入，我们还增强了计时器基础设施，以避免陷阱和仿真开销。在周期精确、fpga加速模拟器FireSim上进行了实验，该系统也在Zynq UltraScale+ MPSoC ZCU104上成功部署并进行测试。我们的硬件实现是开源的，目前正在被RISC-V社区用于批准H-extension规范。

Information Leakage Analysis using a Co-design-Based Fault Injection Technique on a RISC-V Microprocessor

J Plusquellic, DE Owen, TJ Mannos, B Dziki - ... Aided Design of Integrated Circuits and ..., 2021

> RISC-V指令集体系结构开放许可政策催生了大量的开发活动，使一系列实现公开可用。RISC-V操作的环境也相应地扩展了，这就需要一种通用的方法来评估RISC-V实现在不利操作条件下或在正常磨损期后的可靠性。故障注入(FI)是指永久或暂时改变寄存器或线路的状态，然后观察执行行为的过程。该分析提供了对防范可能由于意外执行行为而发生的敏感信息泄漏或损坏的对策的开发的洞察力。在本文中，我们开发了一个软硬件协同设计体系结构，它可以实现快速的、可配置的故障模拟，并利用它来进行信息泄漏和数据破坏分析。现代片上系统fpga支持建立一个评估平台，其中控制元件在处理器上运行，目标设计在可编程逻辑(PL)中运行。FI系统的软件组件引入故障并报告执行行为。创建并配置了一对RISC-V使用fi的实现来执行高级加密标准和绕口令算法。在模拟故障的一个子集的输出中，可以观察到密钥和明文信息泄漏以及退化的伪随机序列。

[PDF] A Multipurpose Formal RISC-V Specification

T Bourgeat, I Clester, A Erbsen, S Gruetter, A Wright... - arXiv preprint arXiv ..., 2021

> RISC-V是一个相对较新的、开放的指令集体系结构，具有成熟的生态系统和正式的机器可读规范。因此，这是一个很有前途的形式方法研究领域。然而，我们注意到不同的形式方法研究项目对RISC-V的不同方面感兴趣，并希望对其他方面进行简化、抽象、近似或忽略。通常，它们还需要不同的编码风格，导致每个项目从头开始一个新的形式。我们开始识别项目之间的共性，并将RISC-V规范表示为一个带有漏洞的程序，这些漏洞可以通过不同的项目进行不同的实例化。我们对RISC-V规范的形式化是用Haskell编写的，并利用了现有的工具，而不是需要新的特定于领域的工具，这与其他方法不同。据我们

所知，它是第一个能够作为处理器正确性证明和编译器正确性证明之间的接口的RISC-V规范，同时也支持其他几个有不同需求的项目。

Design and Implementation of Arbitrary Point FFT Based on RISC-V SoC

Z Zheng, X Zhu, H Qian – 2021 IEEE 5th Advanced Information Technology ..., 2021

本文设计并实现了一种基于RISC-V(第五代简化指令集计算)的专用微处理器体系结构，该体系结构仅包含20条任意点FFT(快速傅立叶变换)算法指令。此外，还建立了相应的片上系统SoC (System-on-Chip)，实现了系统的可扩展性和可重构性。采用软硬件协同验证的方法，对比MATLAB、Visual Studio 2019和VIVADO 2019.1的仿真结果，验证系统功能的正确性。最后，使用Xilinx Artix-7 (XC7A100TFGG484-2) FPGA(现场可编程门阵列)平台来实现和原型化所提出的硬件系统，该硬件系统共使用1897 LUTs(查表)、361 FFs(触发器)和25 BRAMs(块随机存取存储器)，在100MHz时消耗2.016W。实验结果表明，该系统通过对软件参数的重新配置和内存容量的扩展，可以在任何时刻实现FFT算法，且由于面积小、功耗低，适合嵌入式应用。

Efficient Transform Algorithms for Parallel Ultra-Low-Power IoT End Nodes

B Mazzoni, S Benatti, L Benini, G Tagliavini – IEEE Embedded Systems Letters, 2021

现代物联网终端节点必须在有限的功率预算下支持计算密集型工作负载。并行超低功耗架构是这个场景的一个有前途的目标，高度优化的软件库的可用性对于利用并行性和降低软件开发成本是至关重要的。这封信提出了一种针对超低功耗物联网设备的广泛使用的STFT和DWT变换的高效并行设计。我们解决了与共享内存中的细粒度同步和银行业务冲突相关的关键性能挑战。我们在8个RISC-V核簇上实现了高吞吐量(平均50.95个样品/μs)、良好的并行加速(高达6.79×)和高能源效率(高达172.55 GOp/s/W)。

RTL-ConTest: Concolic Testing on RTL for Detecting Security Vulnerabilities

X Meng, S Kundu, AK Kanuparthi, K Basu – ... on Computer-Aided Design of Integrated ..., 2021

RTL- contest是一种寄存器传输级(RTL)安全漏洞检测算法，它从RTL设计中提取关键进程流，并执行RTL级concolic测试，生成安全测试用例，用于识别片上系统(SoC)中的关键漏洞。在基于开源risc - v的soc上对该方法的有效性进行了评估。我们的技术成功地检测出了表现在处理器核心以及SoC其余部分(如调试模块、外设等)的安全漏洞，从而对整个硬件设计提供了全面的漏洞检测。我们的实验结果表明，在常规安全验证工具有限的情况下，RTL-ConTest显著提高了检测SoC安全漏洞的效率。

[PDF] Solver-Aided Constant-Time Circuit Verification

RG Kici, K Gleissenthall, D Stefan, R Jhala – arXiv preprint arXiv:2104.00461, 2021

我们提出了Xenon，这是一种求解器辅助的方法，用于正式验证Verilog硬件在恒定时间内执行。Xenon通过一种新的常数时间反例概念，极大地减少了定位验证失败的根本原因所需的努力，从而扩展到现实的硬件设计，Xenon使用这个概念自动合成了一组最小的保密假设。Xenon通过模块摘要的概念进一步利用了Verilog代码中的模块性，从而避免了跨多个模块实例化的重复工作。我们展示了Xenon的假设综

合和总结如何支持各种电路的验证，包括AES(一种高度模块化的AES-256实现，其模块化程度将验证时间从6小时缩短到不到3秒)，以及ScarV，一个定时通道硬化RISC-V微控制器，其尺寸超过先前验证的设计一个数量级。

Neutron Radiation Testing of a TMR VexRiscv Soft Processor on SRAM-based FPGAs

AE Wilson, S Larsen, C Wilson, C Thurlow, M Wirthlin - IEEE Transactions on Nuclear ..., 2021

软处理器通常用于FPGA设计中辐射危险环境。这些系统容易受到SEUs的影响，这些SEUs会破坏硬件配置和软件实现。减轻这些seu可以通过对处理器应用TMR技术来完成。本文介绍了linux TMR VexRiscv处理器的故障注入和中子辐射结果。TMR处理器在SEU诱导的平均故障通量上实现了10倍的改进，而资源利用成本为4倍。为了进一步了解TMR系统故障，我们对辐射数据生成的目标进行了额外的辐射后故障注入。该分析表明，并不是所有的故障都是由于单位故障引起的，而是由多位故障、非三倍IO和无监控的非cram SEUs引起的。

HAM: Hotspot-Aware Manager for Improving Communications with 3D-Stacked Memory

X Wang, A Tumeo, J Leidel, J Li, Y Chen - IEEE Transactions on Computers, 2021

数据密集型工作负载通常表现为具有有限或没有数据局部性的细粒度内存访问，从而导致频繁的缓存丢失和内存带宽的低利用率。3d堆叠的内存设备，如混合内存立方体(HMC)和高带宽内存(HBM)，可以提供比传统内存模块明显更高的带宽。然而，JEDEC DDR设备的传统接口和优化方法不能充分利用数据密集型应用程序的大量不规则内存访问的3d堆叠内存的潜在性能。在本文中，我们提出了一种新颖的热点感知管理器(HAM)基础设施，用于3d堆叠内存设备，能够通过请求聚合、热点检测和内存预取来优化内存访问流。我们提出了HAM的设计和实现，并在一个使用RISC-V嵌入式核心和附加HMC器件的系统上进行了仿真。我们用超过12个基准测试和代表不同不规则内存访问模式的应用程序广泛评估HAM。结果表明，与基线流预取器相比，HAM平均减少了37.51%的冗余请求，提高了4.2倍的预取缓冲区命中率。在选定的基准测试集上，HAM比标准3d堆栈内存平均提高了21.81%的性能，节省了35.07%的电能。

[PDF] CPUs, GPUs, and More From Hot Chips '32

LK John - IEEE Micro, 2021

Best Papers From Hot Chips 32

P Raina, C Young - IEEE Micro, 2021

[PDF] Synch: A framework for concurrent data-structures and benchmarks

ND Kallimanis - arXiv preprint arXiv:2103.16182, 2021

多核计算机最近的进步突出了简化并发编程的需要，以便利用它们的计算能力。实现这一目标的一种方法是设计高效的并发数据结构(如栈、队列、哈希表等)和同步技术(如锁、组合技术等)，这些技术在具有大量核的机器上表现良好。与普通的顺序数据结构不同，并发数据结构允许多个线程同时访问和/或修改它们。sync是一个开源框架，它不仅提供了一些常见的高性能并发数据结构，而且为研究人员提供了设计和测试高性能并发数据结构的工具。同步框架包含大量的并发数据结构，如队列、堆栈、组合对象、哈希表、锁等，并且它为开发并发数据结构并对其进行基准测试提供了一个用户友好的运行时。在其他特性中，所提供的运行时提供了轻松创建线程(POSIX和用户级线程)的功能，以及度量性能的工具等。此外，所提供的并发数据结构和运行时是高度优化的当代NUMA多处理器，如AMD Epyc和英特尔Xeon。

[PDF] Enabling Design Methodologies and Future Trends forEdge AI: Specialization and Co-design

C Hao, J Dotzel, J Xiong, L Benini, Z Zhang, D Chen – arXiv preprint arXiv ..., 2021

人工智能(AI)技术近年来突飞猛进，给人们的生活带来了革命性的变化。在边缘计算的支持下，人工智能工作负载正从集中式云架构迁移到分布式边缘系统，引入了一种称为边缘人工智能的新范式。虽然edge AI有希望通过普通edge设备将自主性和智能显著提升到日常生活中，但它也带来了新的挑战，特别是在算法的开发和服务部署方面，这需要新的设计方法来应对这些独特的挑战。在这篇论文中，我们提供了一个最新的使能设计方法的全面调查，这些方法跨越了整个边缘AI开发堆栈。我们建议有效的边缘AI开发的关键方法是单层专业化和跨层协同设计。我们将详细讨论每个类别中的代表性方法，包括设备上培训方法、专用软件设计、专用硬件设计、基准测试和设计自动化、软件/硬件协同设计、软件/编译器协同设计和编译器/硬件协同设计。此外，我们试图揭示隐藏的跨层设计机会，可以进一步提高未来边缘人工智能的解决方案质量，并提供对未来方向和需要增加研究重点的新兴领域的见解。

⭐ [HTML] Today's computing challenges: opportunities for computer hardware design

W Bae – PeerJ Computer Science, 2021

由于数字数据的爆炸式增长，对计算能力提高的要求也越来越高。然而，我们用于持续改进计算机三个元素(进程、内存和互连)的遗留方法已经开始面临它们的局限性，因此它们不再像过去那样有效，而且预计在不久的将来也会走到尽头。显然，这对计算机硬件行业是一个巨大的挑战。然而，与此同时，它也为硬件设计行业提供了巨大的机会，以开发新技术，并从现有的领导地位。本文回顾了当今计算系统所面临的技术挑战，并介绍了计算能力持续发展的潜在方向，并讨论了计算机硬件设计人员在哪些方面找到了很好的机会可以做出贡献。

[PDF] (No) Compromis: Paging Virtualization Is Not a Fatality

BT Djomgwe, P Yuhala, A Tchana, F Hermenier... – VEE 2021-17th ACM ..., 2021

嵌套/扩展页表(EPT)是当前用于在虚拟化系统中虚拟化内存的硬件解决方案。由于需要2D页面遍历，这导致了显著的性能开销，因此TLB miss上有24个内存访问(而不是本机系统中的4个内存访问)。这种2D页面遍历约束来自于使用分页来管理虚拟机(VM)内存。本文表明，在管理程序中不需要分页。我们的解决方案的折衷方案是一个新颖的内存管理单元，它使用直接段来管理VM的内存，并结合VM进程的分页。这是第一次证明基于直接段的解决方案可以在保持应用程序不变的情况下适用于整个VM内存。根据310所研究的数据中心轨迹，本文表明可以使用单个内存段提供高达99.99%的vm。本文提出了一种在硬件、管理程序和数据中心调度器中实现折衷的系统方法。评估结果表明，折衷比两个流行的内存虚拟化解决方案:影子分页和EPT的性能分别高出30%和370%。

[PDF] Spons & Shields: Practical Isolation for Trusted Execution

VA Sartakov, D Eyers, L Vilanova, P Pietzuch – 2021

可信执行环境(tee)为在不可信的云中部署安全敏感的应用程序提供了一种成本效益高的“提升和转移”解决方案。为此，它们必须支持丰富的、多组件的应用程序，冒着TEE内部存在大量可信计算基础的风险。细粒度的分区化可以通过深度防御提高安全性，但当前的解决方案要么在同一个TEE中运行未受保护的所有软件组件，缺乏共享内存支持，要么使用单独的TEE隔离应用程序进程，影响性能和兼容性。

[PDF] Twine: An Embedded Trusted Runtime for WebAssembly

J Ménétrey, M Pasin, P Felber, V Schiavoni – arXiv preprint arXiv:2103.15860, 2021

WebAssembly是一种日益流行的轻量级二进制指令格式，它可以有效地嵌入和沙箱。像C、c++、Rust、Go和许多其他语言都可以编译成WebAssembly。本文描述了TWINE，一个WebAssembly可信运行时，设计用来执行未经修改的、独立于语言的应用程序。我们利用Intel SGX来构建运行时环境，而不需要处理特定于语言的复杂api。虽然SGX硬件提供了在处理器内的安全执行，TWINE提供了一个嵌套在SGX enclave中的安全的沙箱软件运行时，具有与未修改的WebAssembly应用程序兼容的WebAssembly系统接口(WASI)。我们用大量通用基准和实际应用来评估TWINE。特别是，我们使用TWINE实现了一个安全、可信的SQLite版本，SQLite是一个知名的、功能齐全的嵌入式数据库。我们相信，这样一个受信任的数据库将是构建许多大型应用程序服务的合理组件。我们的评估表明，SQLite可以通过WebAssembly和现有的系统接口在SGX enclave中完全执行，平均性能开销也差不多。我们估计，额外的安全保证及其与标准WebAssembly的完全兼容性在很大程度上补偿了评测的性能损失。对结果的深入分析表明，通过修改一些底层库，性能可以大大提高。我们在文中描述并实现了一个这样的修改，达到了4.1× speedup。TWINE是开源的，可以在GitHub上下载，还有复制我们实验的说明。

Zynq System-on-Chip DMA Messaging for Processor Monitoring

D Koranek, D Hodson, S Graham – International Conference on Cyber Warfare and ..., 2021

Xilinx Zynq-7000系统片上架构结合了ARM Cortex-A9核心和FPGA fabric。这种混合架构的一个好处是，它允许快速设计原型，处理系统(PS)的安全性由可编程逻辑(PL)监控，反之亦然。在PS或PL中实现设计的选择取决于跨许多因素的成本效益分析。本工作审查了构建同时使用PS和PL的安全监视设计所

需的设计过程。作为背景，本工作审查了类似的安全监视项目。为此，实现了一个PL外设来处理数据传输。这个外设实现了axis – stream协议，并允许FIFO行为，但可以修改以允许处理传入和传出的数据。该设计通过了仿真测试，但在物理硬件上实现并使用系统ILA进行监控时，并不总是通过测试。失败归因于未知方面的综合和实施过程，加上系统的相互作用的ILA。进一步研究的两个途径是:1)使用Zynq ARM Cortex–A9核心上的软件监控软核处理器;或者，2)或者，利用FPGA fabric监控来自ARM Cortez–A9核心的CoreSight跟踪输出，目的是将任一跟踪系统耦合到基于机器学习的恶意软件检测系统。如果进一步的研究成功，它将能够动态地分析处理器的执行情况，以检测恶意软件，并适合于嵌入式系统的使用。这种类型的一个障碍动态分析系统的带宽AXI系统,跟踪信息的大小,和相对的时钟频率的PS和PL。处理这种障碍,动态监测系统将只使用实时数据的一个子集和调整时钟频率的系统设计。

[PDF] Domain–specific programming assistance in an embedded DSL for generating processor emulators

K Okuda, S Chiba – 2021

本文提出了一种设计方法，在领域特定编程的帮助下开发嵌入式领域特定语言(DSL)。为了演示所提出的方法，我们描述了称为MELTRANS的处理器描述语言的设计，这是一种由Java承载的嵌入式DSL。MELTRANS用于生成一个具有动态二进制转换的快速处理器模拟器。尽管这样的嵌入式领域特定语言仅为编程提供了较差的领域特定帮助，MELTRANS改善了这种不足。我们的想法是让宿主语言的集成开发环境(IDE)使用特定领域的知识提供更好的编程帮助。为此，我们将MELTRANS中的程序分解为几个Java类，它们对应于不同的关注点，并为描述顺序设置规则。语言运行时接受每个类，不仅为处理器模拟器生成代码，还为以后编写的类生成超类。用户编写描述关注的每个类，作为生成的类的子类。生成的类使用户能够从Java ide以更特定于领域的风格提供的编程帮助中受益。虽然MELTRANS托管在Java中，但生成的模拟器是用c++编写的。为了验证我们的设计，我们在MELTRANS中实现了几个仿真器并使用它们进行实验。结果表明，我们的领域特定编程辅助可以有效地减少用户需要编写的代码量，生成的仿真器可以达到1000 MIPS以上。

[PDF] RECLAIMING THE UTOPIA: ALTERNATE ECOSYSTEMS FOR SAFEGUARDING HUMAN RIGHTS IN THE HIGH–PERFORMANCE BRAIN MACHINE INTERFACE ...

SM Zanjani, A Ghazizadeh – addiction, 2021

脑机接口(BMI)长期以来一直是治疗神经疾病和增强人类心智能力的候选方法。最近，在全球大规模研发投资的推动下，神经科学和神经技术取得了引人注目的进展，从而催生了高性能BMI解决方案，即将进入人类生活的各个方面。然而，IT硬件和软件基础设施的状况引发了人们对违反道德的严重担忧，因为在这个时代，人类大脑将暴露在生态系统中强大参与者的有争议的意图之下。由于专有的BMI解决方案所提供的便利和更高生产力的吸引力，特别是在公众对即将到来的BMI时代的影响浑然不觉的情况下，阻碍风险特别高。在此，我们认为，尽管机会之窗正在迅速关闭，但可以实现一个基于开放性、模块化、离线可部署性和最低特权四项原则的替代生态系统，通过自然实现的神经隐私安全保护措施，创建一个更安全的游戏领域，neurosecurity和agency，同时促进了商业高性能BMI应用的光明前景。

Towards Verifiable Phrase Search over Encrypted Cloud–Based IoT Data

X Ge, J Yu, F Chen, F Kong, H Wang – IEEE Internet of Things Journal, 2021

短语搜索加密是基于云的物联网系统中的一项重要技术，允许用户检索包含一组连续关键词的加密物联网数据。它在基于云的电子医疗诊断系统、基于云的物联网系统的机器学习应用等方面发挥着重要作用。然而，就我们所知，现有的短语搜索加密方案不能实现对搜索结果的完全验证。他们要么不能验证返回的文件是否正确地包含了查询短语，要么不能验证是否返回了所有包含该查询短语的文件。结果验证对于一些基于云的物联网应用非常重要。在基于云的电子医疗诊断系统中，如果搜索结果不正确，就会导致误诊，甚至危及患者的生命。为了解决这一问题，本文探讨了如何在基于云的物联网加密数据上实现可验证短语搜索。具体来说，我们设计了新的查找表，可以用来确定和验证关键字之间的位置关系。同时，我们采用了一种两阶段查询策略。在第一查询阶段，数据用户可以知道查询短语中包含关键字的文件的标识符，并根据这些标识符生成下一阶段的搜索trapdoor。在第二查询阶段，数据用户可以获取验证信息，检查包含查询短语的所有文件是否正确返回。我们对我们的方案进行了安全性分析，并进行了大量的实验。实验结果表明，该方案具有较高的安全性和有效性。

[PDF] Compiler-Assisted Hardening of Embedded Software Against Interrupt Latency Side-Channel Attacks

H Winderix, JT Mühlberg, F Piessens

最近的受控通道攻击利用了处理器基本的获取–解码–执行逻辑中的时间差异。这些新的攻击也对嵌入式系统上的软件构成了威胁。即使使用了受信任的执行环境(tee)，中断延迟攻击也允许不受信任的代码通过调度受攻击的enclave的中断来提取应用程序机密。常量时间编程对这些攻击是有效的，但是，正如我们在本文中解释的那样，它可能会带来一些性能方面的缺点。为了应对这种新的威胁，我们提出了一种新的算法，在编译过程中通过对齐依赖秘密的分支中相应指令的执行时间来加固程序。我们的结果表明，在一类具有确定执行时间的嵌入式系统上，这种方法消除了中断延迟侧通道泄漏，并减轻了常数时间编程的限制。我们已经在Sancus TEE的LLVM编译器基础架构中实现了我们的方法，它扩展了openMSP430微控制器，我们还讨论了对其他架构的适用性。我们提供我们的实施和基准，以供进一步研究。

[PDF] Speedster: A TEE-assisted State Channel System

J Liao, F Zhang, W Sun, W Shi – arXiv preprint arXiv:2104.01289, 2021

状态信道网络是解决公共区块链网络可扩展性、高交易费用和低交易吞吐量问题的最常用的第二层解决方案。然而，现有作品存在的局限性限制了该技术的广泛应用，如创建和关闭渠道的成本较高、主链和链下渠道的严格同步、冻结存款、无法执行多方智能合约等。在这项工作中，我们提出了Speedster，一个基于账户的状态通道系统，旨在解决上述问题。为此，Speedster利用最新的安全硬件开发，创建无争议的认证通道，可以在区块链之外有效运行。Speedster是完全分散的，并提供更好的隐私保护。它支持快速的本地多方合约执行，这在以前支持tee的信道网络中是缺失的。与Lightning网络相比，Speedster将吞吐量提高了约1万倍，在类似的网络规模下生成的链上数据减少了97%。

RISC-V与芯片评论编辑部 – RISC-V和芯片动态周报

每周六发布

欢迎批评，指正，评论和加入

关于本刊:

- 非特殊注明，本刊消息均来自于网络，如有版权问题，我们会立刻处理。
- 本刊部分消息来源

语雀	微信公众号	Gitee	Github	Inspur
RISC-V和芯片动态简报 riscv rvnews	高效服务器和存储技术国家重点实验室	inspur-risc-v RVWeekly	inspur-risc-v RVWeekly	riscv RVWeekly