保卫计算机架构的新黄金时代

Microchip 技术研究员

RISC-V 基金会创始董事会成员

Ted Speers

RISC-V 社区正在转向一个全新的安全创新平台，以期凭借出色的简便性最大程度地减少攻击面，同时让设计者能够自行评估开源架构的安全性。RISC-V 平台及其安全协议栈可助力开发人员打造全新的解决方案，从而在如今互连设备激增犹如“蛮荒西部”一般的环境中抵御像 Meltdown（熔毁）和 Spectre（幽灵）这类难以规避的漏洞。

在 2018 年 6 月举办的第 45 届计算机架构国际研讨会上，计算机先驱 David Patterson 和 John Hennessy 在他们的图灵讲座中介绍了“计算机架构的新黄金时代”。他们描述的黄金时代包含以下四个要素：

- 域特定的软硬件协同设计
- 开放指令集
- 敏捷的芯片设计
- 增强型安全性

RISC-V（读作“risk-5”）采用极具吸引力的开源指令集架构，可推动域特定的架构实现快速发展并提高该领域的投入，同时，它也成为了处理器安全性的重心。

这里介绍一些背景信息，自 2014 年 12 月起，Microchip 的现场可编程门阵列（FPGA）业务部门一直致力于推广 RISC-V。我们对 RISC-V 及其潜在能力的关注涉及多个层面，包括自由创新、掌控旗下处理器产品的未来发展以及降低成本。 这些层面属于内在因素，能够帮助我们凸显差异化，从而在市场竞争中脱颖而出。对我们而言，RISC-V 还意味着一个全面把握处理器安全性的代际机遇。全面把握处理器安全性是一个协作性的外在层面，能够让全球顶级安全专家有机会开展合作，携手攻克大家共同面临的计算机安全问题。

我们在全面把握 FPGA 安全性的过程中能够获得丰富的经验，这有助于我们深入了解计算中存在的硬件安全威胁，同时应对业界在寻求这些威胁的解决方案过程中所面临的挑战。我们早在 2008 年就开始深入研究 FPGA 安全性，然后在 2012 年推出首款采用集成处理器子系统的 FPGA 并开始实现盈利。当时，为了让客户能够构建安全应用，我们需要创建一种从基础安全硬件开始的分层方法。这样，我们便可构建一个可实现设计安全或 IP 保护的层，随后客户可以依托该层建立应用层。在这一过程中，我们发现了边信道攻击的问题，例如可以轻松提取密钥的差分功耗分析（DPA）。我们因此成为了惟一部署由 CRI（已被 Rambus 收购）提供的 DPA 对策的 FPGA 供应商。

之后，我们将在 FPGA 安全性方面的经验应用到了处理器安全状态上。结果发现，在几十年前处理器安全性尚未引起市场关注之时，处理器的基础硬件层就已经建立。当时的指令集架构（ISA）通过对脆弱的系统进行不完善的修补来应对安全计算不断增长的需求。我们当然也敏锐地意识到边信道的问题，尤其是微架构边信道问题，因为通过这些边信道，可以利用编程人员已屏

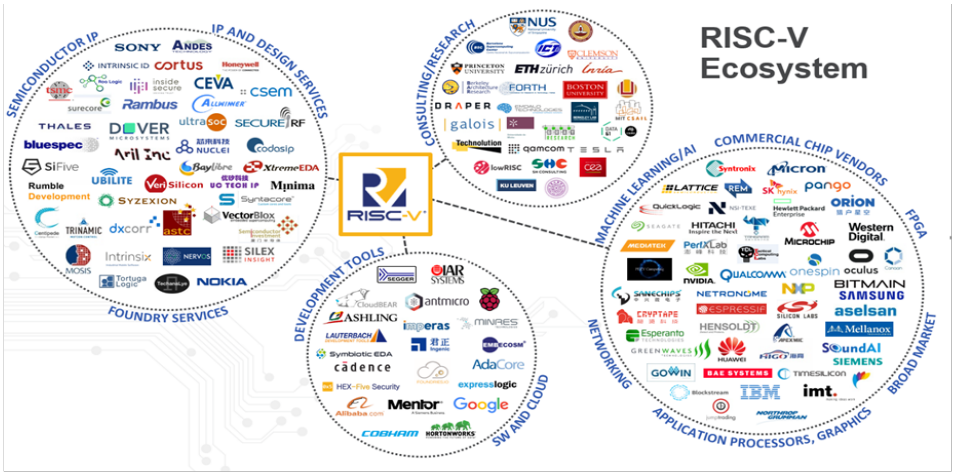
蔽的处理器实现功能来泄漏信息。随着 Spectre 和 Meltdown 漏洞的公布，整个计算行业开始意识到微架构边信道问题带来的威胁，因此亟需重建计算机架构的硬件基础。

正如我所指出的那样，我们立即发现了 RISC-V 作为重建计算硬件基础平台的潜力，而发现者并非只有我们。在最早的一场 RISC-V 专题研讨会上，LowRISC 和 Shakti 处理器项目组发表了以安全性为主要内容的演讲，自此之后，安全性一直是 RISC-V 的重要主题。这两个示例重点说明了 RISC-V 支持的协作范围。Shakti 处理器项目由印度政府提供资助，对一些国家/地区而言，这是使用 RISC-V 赢得某种技术独立的一次良机，而 LowRISC 则由快速发展的开源硬件运动提供支持。RISC-V 行业的活动在不断增加，安全相关的内容也随之快速增长，在 2018 年 12 月的首届 RISC-V 峰会中，55 场会议中有 13 场涉及到安全性。

2018 年 RISC-V 峰会 13 场安全会议的其中一个会议室

除了成为整个安全性会议的焦点之外，还有很多迹象表明，RISC-V ISA 正在成为处理器安全性的重心。

- DARPA 正不断投资于 RISC-V 和安全性，并选择 RISC-V 作为其硬件集成系统安全（SSITH）计划的评估平台。
- 在 RISC-V 基金会，有超过 30 个成员拥有安全 RISC-V 产品，或者在为安全工作组做贡献。
- 基金会有两个技术工作组（加密和可信执行环境）正致力于创建 RISC-V ISA 扩展。
- RISC-V 基金会设立了安全性常务委员会，负责确认和协调多个方面的安全相关活动，包括将 RISC-V 作为理想的安全工具进行推广，以及就物联网（IoT）和嵌入式设备的最佳安全实践达成共识。



RISC-V Ecosystem	RISC-V 生态系统
RISC-V Membership Through a Security Filter	通过安全性筛查的 RISC-V 成员

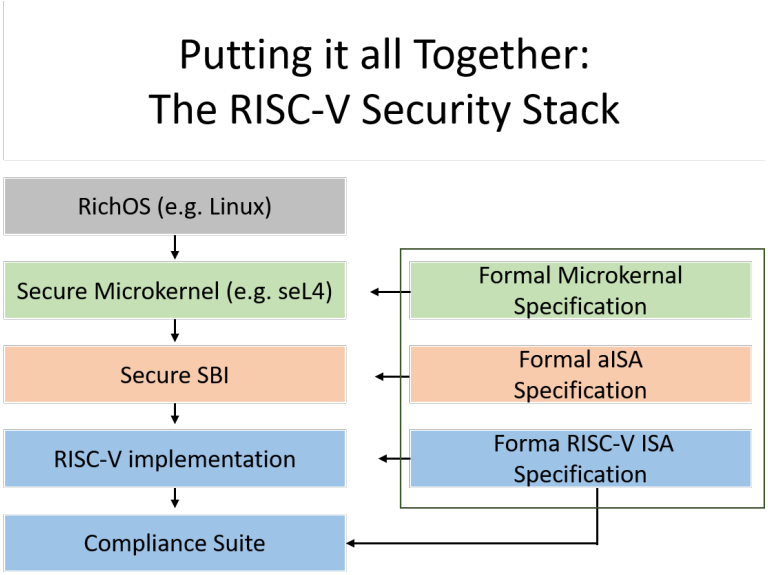
有 30 多个 RISC-V 基金会的成员拥有安全产品，或者参与了由基金会推动的安全活动。（由 RISC-V 基金会提供）

基金会安全常务委员会最显著的贡献是演讲人计划。基金会内部和外部的演讲人每月一次受邀就安全相关的各种主题发表演讲。来自 Data61 的一位演讲人 Gernot Heiser 提供了一个框架，此框架有可能指出 RISC-V 计算机安全性范例的呈现方式。Gernot 和他在 Data61 的同事在早些时候对微架构边信道进行了深入研究，并于 2016 年撰写了一篇论文（A Survey of Microarchitectural Timing Attacks and Countermeasures on Contemporary Hardware）来描述基于攻击的分类法。

他们提出了一种称为“扩充”指令集架构（aISA）的抽象概念，可将软硬件之间的协议扩展到传统 ISA 以外，作为对比，传统 ISA 有意将时间和微架构的所有概念抽象化。相比之下，aISA 加入了一些机制，允许应用程序二进制接口（ABI）对处理器系统的微架构状态施加更多控制。例如，这可能包含高速缓存刷新或分支预测逻辑运算，以提供针对高速缓存时序信道这类威胁的安全保障。

在我们定义并实现 aISA 后，就有机会创建我提到的 RISC-V 安全协议栈，这种协议栈起源于正式指定的协议栈要素的已正式验证实现中。该协议栈从硬件和基础 ISA 开始，一直扩展到实现

aISA 的层。而其中最重要的是安全微内核，它现在可以通过 aISA 访问微架构状态，并且能够实施抵御微架构边信道攻击的对策。



Putting it all Together: The RISC-V Security Stack	汇总：RISC-V 安全协议栈
RichOS (e.g. Linux)	RichOS（例如 Linux®）
Secure Microkernel (e.g. seL4)	安全微内核（例如 seL4）
Secure SBI	安全 SBI
RISC-V Implementation	RISC-V 实现
Compliance Suite	合规性套件
Formal Microkernal Specification	正式微内核规范
Formal aISA Specification	正式 aISA 规范
Formal RISC-V ISA Specification	正式 RISC-V ISA 规范

安全未来——正式指定且经过正式验证的 RISC-V 安全协议栈

RISC-V 革命已经开始，社区最初意识到的诸多未来可能已经变为现实，包括重建计算机安全的基础。Microchip 与 RISC-V 基金会的成员合作，致力于推动这项技术的发展，我们对此深感自豪，而在 RISC-V 产品领域的领导地位和未来前景同样令我们骄傲。我们期待与社区深化合作创新，充分利用当前面临的代际机遇。

Ted Speers 是 Microchip 的技术研究员，负责为低能耗、安全、可靠的 FPGA 和 SoC FPGA 定义发展路线图。他于 1987 年加入 Microsemi（已被 Microchip 收购），负责过程工程和产品工程，之后于 2003 年开始担任现职。Ted 是 35 项美国专利的共同发明人。在加入 Microsemi 之前，他就职于 LSI Logic。他拥有康奈尔大学化学工程学士学位。自 2016 年成立以来，Ted 一直是 RISC-V 基金会董事会的成员。