系统软件与软件安全实验室

Lab of System Software and Software Security

随着大数据、云计算、移动计算、物联网等计算机技术的变革性发展，系统软件和软件安全也面临新的挑战和机遇：如何让操作系统和编程语言充分发挥新型（多核/众核、GPU 等）处理器的计算能力？如何让编译器生成更加可靠、高效、节能的代码？如何适应多变的计算设备、集群和网络结构，迅速开发应用？如何在移动和网络环境下有效保护（移动支付、社交网络、数据挖掘等）用户的隐私和安全？如何确保系统在（核电、医疗、航空、航天、汽车、高铁等）安全攸关或任务攸关领域中的高度可靠性？

欢迎你加入我们的队伍，与我们一起迎接挑战，开发新一代的系统软件和软件安全技术！

主要研究方向

面向多核的新型操作系统和程序语言：随着多核处理器的广泛使用，日益增长的应用必须通过并行代码才能有效利用多核资源。然而并行编程比串行编程困难得多，并行程序的执行可能产生不确定的结果，从而导致并发错误和性能故障，且错误和问题难以诊断和再现，严重影响了软件的可靠性以及多核资源的利用率。

我们面向多核计算平台，从程序语言、运行时系统、操作系统等方面，研究和开发用于改进现实软件系统的可靠性和性能的技术、工具和系统。

主要研究人员：张昱副教授、冯新宇教授

网络和多核计算：面对日益多变的应用需求和网络架构，传统的定制网络设备已经难以满足人们快速开发和部署新型应用的需要。未来的运营商网络及数据中心网络将只有三种标准设备：标准服务器，标准存储设备，标准交换机。利用虚拟化技术，网络设备功能将不再依赖于专用硬件，而是可以按需部署在网络中任意一台服务器上（**网络功能虚拟化**）。交换机不再执行控制面功能，而是接收网络中一个集中式控制器计算的流表，并按照流表转发数据包（**软件定义网络**）。拥有多核处理器（多核 CPU、GPU）和高速网络适配器的通用服务器成为网络系统的标准化平台（**基于通用服务器的网络系统**）。我们研究和开发**基于多核服务器的网络系统性能优化和网络功能虚拟化**技术，以及新型的**软件定义网络编程环境**。

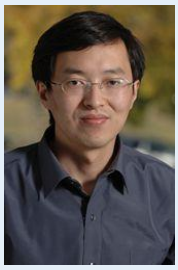
主要研究人员：华蓓教授、冯新宇教授

软件可靠性和安全性分析和验证：随着计算机应用的日益推广，我们对软件可靠性和安全性的需求也越来越高。这些需求即体现在任务攸关和安全攸关的基础设施和系统上，包括核电、航空、航天、军事、金融等领域；也体现在人们日常生活中，如电子支付、医疗、汽车等。

面对这些需求，我们一方面采用**静态程序分析和动态检查的技术**来自动检查和定位操作系统和应用中的安全漏洞，以满足日常生活中的需要（如安卓系统下的隐私保护）；另一方面采用**形式化验证的技术**，采用数学和逻辑手段，严格证明我们的系统软件（如操作系统、编译器等）满足一定的可靠性和安全性，以满足核电、航天等安全攸关应用领域的需要。

主要研究人员：冯新宇教授、邵中教授、陈意云教授、张昱副教授

实验室人员介绍



冯新宇 教授

2007 年于耶鲁大学获博士学位，2010 年加入中科大计算机学院，任教授、博士生导师。2010 年入选教育部新世纪优秀人才支持计划。**主要研究方向为程序分析和验证、软件安全、程序设计语言理论**等。主持和参加多项国家自然科学基金项目、国家 863 项目和中科院先导专项子课题。在顶级国际期刊和会议（TOPLAS、POPL、PLDI、LICS 等）上发表论文多篇，其中指导学生发表在 POPL 2012 上的论文是中国大陆高校和科研院所作为第一单位在程序设计语言领域的顶级会议 POPL 上发表的第一篇论文。

http://staff.ustc.edu.cn/~xyfeng; **xyfeng@ustc.edu.cn**

华蓓 教授

毕业于中国科学技术大学，主要从事**计算机网络及多核计算方面的教学与研究工作**，先后承担了国家自然科学基金项目（1 项）、国家 863 项目（5 项）以及与企业（华为、英特尔等）的合作项目，在相关领域的知名国际会议（PPoPP，ICS）及国际期刊（TECS，JPDC）上发表了高水平的论文，其中指导学生发表在 PPoPP 2006 上的论文，是中国大陆高校和科研院所作为第一单位在并行处理领域的顶级会议 PPoPP 上发表的第一篇论文，实现了“零的突破”。

http://staff.ustc.edu.cn/~bhua; **bhua@ustc.edu.cn**

邵中 教授

耶鲁大学教授，中科大“大师讲席”教授。是学术界和工业界科研项目中广泛使用的 SML/NJ 函数式编程语言的编译器的主要设计和实现者之一。近年来，**研究重点集中在开发新的程序验证理论和技术，目标是为开发经过验证的大规模系统软件构建一种实用的基础平台。**

注：邵中教授在计算机学院有招收研究生的名额。

主页：http://www.cs.yale.edu/~shao； **联系方式：**通过陈意云/冯新宇联系

张昱 副教授

分别于 1993 年和 1996 年在合肥工业大学获计算机应用学士、硕士学位，2005 年 1 月在中国科学技术大学获计算机软件与理论博士学位。2010 年 10 月底公派赴美国耶鲁大学访问一年。自 1996 年到科大计算机系工作以来，从事数据结构、编译原理等课程的教学与研究工作。**研究兴趣包括可伸缩并行系统与运行时环境、程序分析与变换、程序设计理论与实现技术等。**主持四项和 Intel 公司合作的项目和三项中科院项目；作为技术骨干参与多项国家级项目。

http://staff.ustc.edu.cn/~yuzhang; **yuzhang@ustc.edu.cn**

陈意云 教授

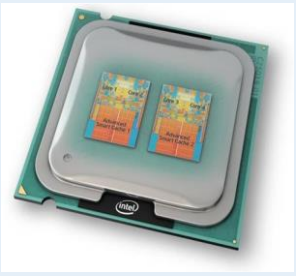
自 2000 年起至今，一直在高可信软件领域展开研究，**研究方向集中于在源语言一级提供程序验证和分析工具，帮助程序员杜绝内存安全方面的错误，保障程序满足预期的规范。**团队的工作在微软举办的 VS 2009 验证软件研讨会上进行了报告和原型工具的演示，受到学术界的广泛关注和赞誉。

注：陈意云教授已退休，仍将继续指导研究生的课题，但不再单独招生。

http://staff.ustc.edu.cn/~yiyun; **yiyun@ustc.edu.cn**

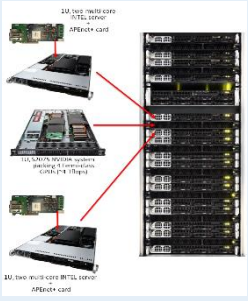
在研项目简介

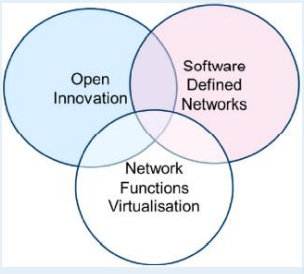
确定性并行：确定性并行编程模型具有易编程、易理解、且能够能再现程序的执行结果等优点。我们围绕确定性并行开展如下研究：1）确定性共享虚拟内存模型及其对各种并行编程模式的支持；2）现有多线程程序的确定性并行执行；3）并发错误（如数据竞争）检测及修复；4）时空性能评测方法和工具的研制；5）性能故障的检测和修复。课题组已在 Linux 用户空间模拟建立支持并发任务确定性共享的单生产-多消费虚拟内存模型，并以此为基础构建了确定性消息传递编程库、确定性 MapReduce 编程库等。



程序分析和变换技术及工具：研究如何帮助用户快速地理解程序行为、检测程序错误或故障，总结错误的模式特征，以期能对其中的部分错误进行自动修复。课题组已在一个实际的 Java 虚拟机(Apache Harmony)上研制了**即时编译器辅助的垃圾收集**，可以通过即时编译器分析识别应用程序中的短生命期对象，并在程序中插入显式回收的指令，再由垃圾收集器回收和尽快复用这些对象所占的内存。课题组在 Clang、LLVM 编译基础设施上研制了跨文件的 C **函数调用图构建工具**、支持代码重构的**代码段分离工具**，等等。

基于通用服务器的高性能网络系统：研究网络算法及网络系统在多核 CPU 及 GPU 上的实现及性能优化。利用多核服务器实现的**网络流量监视系统**可支持 10Gbps 链路速度和几百万 TCP 连接规模，已由合作企业转化成产品。基于 GPU 实现的 **SRTP 反向代理**，首次将 GPU 应用于实时流处理系统（视频流加/解密），获得了超过 10Gbps 的吞吐量。基于 GPU 实现的**内存键值对存储系统**，首次将 GPU 应用于 NoSQL 高速查询，获得了超过 160Mops 的吞吐量。





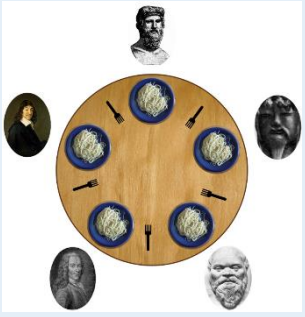
软件定义网络（SDN）/ 网络功能虚拟化（NFV）：SDN/NFV 是未来运营商网络和数据中心网络的基础，NFV 实现网络设备功能，SDN 提供网络连接，它们是新兴的软件定义生态系统（Software-Defined Ecosystem）的组成部分。本课题研究**高性能 NFV 平台、SDN 辅助的流量迁移、SDN 编程等关键技术。**

嵌入式操作系统内核验证：操作系统内核的正确性是航空、航天、核电、医疗等安全攸关系统的可靠性和安全性的前提。通过形式化验证确保操作系统内核不会崩溃的“防崩溃代码”技术被 MIT 出版的 Technology Review 评选为 2011 年十大新兴技术之一。实验室在本领域的研究处于国际前沿，冯新宇教授被上述的“防崩溃代码”技术的报道列为国际上从事此项研究的主要研究人员之一。目前我们正在开展**对商业化的嵌入式实时操作系统 uC/OS-II 内核的验证**，并将其移植到无人飞机等关键应用上。

在研项目简介（续）

程序可靠性和安全性分析：采用程序静态分析和动态监控技术，自动发现程序中的常见缺陷和安全漏洞。围绕该技术开展的研究包括**C 程序分析工具** ShapeChecker 和**安卓应用的隐私泄露检测。**前者能够自动检测 C 程序中的内存泄漏、空指针引用、下标越界、常用数据结构的完整性破坏等缺陷；后者则通过对信息流的静态分析和动态检查，不仅能够发现单个安卓应用对隐私信息的泄露，还能够有效发现多个应用合谋泄露信息的漏洞。

并发算法验证：由于执行的不确定性，多核下的并发算法的正确性难以保证，特别是在库函数中广泛采用的无锁并发算法，更加容易出错。我们通过形式化验证技术，采用数学和逻辑手段，严格证明并发算法的正确性、终止性等关键性质。我们提出的新的程序逻辑已经被成果用于多个经典算法的验证，包括 Java 并发包中的 Michael-Scott 队列和 Harris-Michael 无锁链表。在试图验证一种外科手术机器人手臂控制代码过程中还发现了程序的一个并发错误，这一错误可关系到人的生命安全。



实验室和平台

实验室分布于合肥（校本部）和苏州（中科大苏州研究院）两地，依托**中国科大-耶鲁高可信软件联合研究中心**、**中国科大-国创高可信软件工程中心**、**苏州市软件安全与移动计算重点实验室**等平台，在研究课题和工作环境等方面为学生提供多种选择。

加入我们的五条理由

- **选择最基础又最热门的研究方向：系统软件和软件安全**
- **热门的方向意味着大量的工作机会：**实验室毕业的研究生去向包括微软、Intel、思科、华为、阿里巴巴、百度、腾讯等公司和中科大、中科院深圳先进技术研究院等高校和科研机构
- **广阔的发挥个人兴趣的空间：**中国科大-耶鲁高可信软件联合研究中心侧重基础研究，而中国科大-国创高可信软件工程中心则侧重实际应用；充分尊重并满足你的爱好
- **广泛的国际交流机会：**和耶鲁大学等国际一流大学保持着良好的合作关系
- **良好的学习、生活环境，合肥/苏州可选**