2016年全国软件分析与验证研讨会
（SAVE 2016）

会议程序手册

承办单位：国防科技大学计算机学院计算机系

2016.12.10-12.11

湖南，长沙

目　录

研讨会议程安排

时间	内容	主持人	地点
12 月 9 日 星期五	参会者报到		延年世纪酒店 一楼
12 月 10 日 星期六 上午 研讨会报告			
08:25-08:30	开幕式：召集人讲话	张健	延年世纪酒店 负一楼会议中心
08:30-09:30	特邀报告：Abstract Interpretation Patrick Cousot（纽约大学）		
09:30-10:10	特邀报告：移动平台隐私数据保护的研究 杨珉（复旦大学）		
10:10-10:40	**茶 歇**		
	Session 2：程序分析平台		
10:40-11:05	安全 C 语言程序验证器原型的研发经验与成果 陈意云（中国科学技术大学）	严俊	延年世纪酒店 负一楼会议中心
11:05-11:30	静态分析工具原理、现状及解决方法 李炼（中科院计算所）		
11:30-11:55	A Practical Verification Framework for Preemptive OS Kernels 付明（中国科学技术大学）		
	Session 3：工具展示报告		
11:55-12:05	Wukong 李炼（中科院计算所）	陈振邦	延年世纪酒店 负一楼会议中心
12:05-12:15	VolCE 葛存菁（中科院软件所）		
12:15-12:25	Java 切片工具 王璐璐（东南大学）		
12 月 10 日 星期六 中午 午餐			
12:25-13:30	自助午餐		延年世纪酒店 一楼咖啡厅

12 月 10 日 星期六 下午 研讨会报告			
13:30-14:10	特邀报告：航空机载软件研制过程的主要挑战及应对 李迅（中航工业成都飞机设计研究所）	董威	延年世纪酒店负一楼会议中心
	Session 4：动态分析		
14:10-14:35	Parametric Runtime Verification of C Programs 陈哲（南京航空航天大学）	董威	延年世纪酒店负一楼会议中心
14:35-15:00	基于扩展 LSC 的列控系统运行时验证 柴铭（北京交通大学）		
15:00-15:15	利用动态分析结果对 Android 应用程序插桩 程志超（中国科学技术大学）		
15:15-15:35	**茶 歇**		
	Session 5：形式化验证		
15:35-16:00	限界正确性与程序的模型检测 张文辉（中科院软件所）	卜磊	延年世纪酒店负一楼会议中心
16:00-16:25	A Complete Decision Procedure for Linearly Compositional Separation Logic with Data Constraints 吴志林（中科院软件所）		
16:25-16:50	Analyzing divergence in bisimulation semantics 于婷婷（中科院软件所）		
	Session 6：安全分析		
16:50-17:15	C 内存安全缺陷分析工具现状及演示 李兆鹏（中国科学技术大学）	陈雨亭	延年世纪酒店负一楼会议中心
17:15-17:30	Securing a Compiler Transformation 邓超强（纽约大学）		
17:30-18:30	**Panel Discussion：程序分析与软件安全** **主持人：张健**		

12 月 10 日 星期六 晚上 晚餐			
18:30-20:00	晚餐		延年世纪酒店二楼万事如意厅
12 月 11 日 星期天 上午 研讨会报告			
08:00-09:00	特邀报告：Impact-Driven Research on Software Testing Tools: Getting Real 谢涛（University of Illinois at Urbana-Champaign）	赵建华	延年世纪酒店负一楼会议中心
09:00-09:40	特邀报告：基于分类器知识抽取的绕开攻击 梁彬（中国人民大学）		
09:40-10:10	**茶 歇**		
	Session 8：混成及嵌入式系统		
10:10-10:35	Pareto Optimal Scheduling for Synchronous Data Flow Graphs on Heterogeneous Multiprocessor 朱雪阳（中科院软件所）	詹乃军	延年世纪酒店负一楼会议中心
10:35-11:00	Darboux-type Barrier Certificates for Safety Verification of Nonlinear Hybrid Systems 林望（中国科学院数学与系统科学研究院）		
11:00-11:15	基于仿真的可达集一致性测试 张勇（北京交通大学）		
	Session 9：软件可靠性与测试		
11:15-11:40	一种路径感知的变异体精简方法 孙昌爱（北京科技大学）	刘静	延年世纪酒店负一楼会议中心
11:40-12:05	软件运行环境依赖缺陷及其挑战 郑征（北京航空航天大学）		
12:05-12:30	覆盖率导引的针对 Java 虚拟机实现的差别测试 陈雨亭（上海交通大学）		
12 月 11 日 星期六 中午 午餐			
12:30-14:00	自助午餐		延年世纪酒店一楼咖啡厅

12 月 11 日 星期天 下午 研讨会报告			
	Session 10：程序分析及应用		
14:00-14:25	代码分析、验证技术的集成 赵建华（南京大学）	陈立前	延年世纪酒店负一楼会议中心
14:25-14:40	代码坏味的检测与演化分析 刘辉辉（东南大学计算机科学与工程学院）		
14:40-14:55	C 代码重构的研究现状与思考 宁宇（中国科学技术大学）		
14:55-15:10	基于机器学习约束求解的复杂代码符号执行 李鑫（南京大学）		
15:10-15:40	**茶 歇**		
	Session 11：并发程序分析		
15:40-16:05	LockPeeker：一种检测 Java API 中的隐式锁的方法 林子熠（上海交通大学）	刘万伟	延年世纪酒店负一楼会议中心
16:05-16:30	Towards Certified Compositional Compilation for Concurrent Programs 梁红瑾（中国科学技术大学）		

请注意：工具现场展示和交流安排在 12 月 10 号下午 14:10-17:30，地点在延年世纪酒店负一楼多功能厅。

研讨会特邀报告

报告题目: Abstract Interpretation

报告人: Patrick Cousot（纽约大学）

报告人简介：

Patrick Cousot is Silver Professor of Computer Science at the Courant Institute of Mathematical Sciences, New York University, USA. Patrick Cousot is the inventor, with Radhia Cousot, of Abstract Interpretation. Patrick Cousot was awarded the Silver Medal of the CNRS (1999), a honorary doctorate from the Fakultät Mathematik und Informatik of the Universität des Saarlandes (2001), the Grand Prix of Computer Science and its Applications of the Fondation Airbus Group attributed by the French Academy of Sciences (2006), a Humboldt Research Award (2008), and, with Radhia Cousot, the ACM-SIPLAN Programming Languages Achievement Award (2013) and the IEEE Harlan D. Mills Joint Award (2014). He is Member of the Academia Europaæ, Informatics section (since 2006).

报告题目：移动平台隐私数据保护的研究

报告人：杨珉（复旦大学）

报告摘要：

移动互联生态系统中，个人隐私数据已经成为攻击者青睐的目标，围绕隐私数据的攻防博弈日渐激烈。报告人将介绍近些年围绕移动平台隐私保护领域的一些工作和研究心得，助力更多的国内学者投身于这个领域的研究。

报告人简介：

杨珉，国家 973 首席科学家，复旦大学软件学院教授、博士生导师。 主研方向为系统软件与系统安全，在国内率先开展移动安全问题研究，在系统安全缺陷检测和防护方法领域中取得了一系列的进展。在国际顶级学术会议和各类期刊上发表论文 40 余篇，2011 年在系统软件领域顶级学术会议 USENIX Annual Technical Conference 发表的研究论文是国内高校的第一篇，2013 年在信息安全领域顶级会议 20th ACM Conference on Computer and Communications Security 同时发表了两篇关于安卓系统安全问题研究的学术论文，引起学术同行与行业的高度关注。现任中国网络空间安全协会理事、中国计算机学会（CCF）优秀博士生论文终评专家、国家自然科学基金评审专家、多个信息安全重要学术会议及期刊的审稿人等学术兼职。

报告题目：Impact-Driven Research on Software Testing Tools: Getting Real

报告人：谢涛（University of Illinois at Urbana-Champaign）

报告摘要：

Producing industry impact has been an important, yet challenging task for the research community. This talk presents our recent experiences on impact-driven research on software testing tools, in collaboration with the industry to transfer software testing tools to practice. For example, we have collaborated with Microsoft Research on Pex (http://research.microsoft.com/projects/pex), which has been shipped as part of Visual Studio 2015 Enterprise Edition. More recently, we have collaborated with Salesforce.com (http://taoxie.cs.illinois.edu/publications/fse16industry-learning.pdf) on a test prioritization tool, which is currently in pilot use at Salesforce. We have collaborated with Tencent, Inc. (http://taoxie.cs.illinois.edu/publications/fse16industry-wechat.pdf) on applying and improving Google's Monkey testing tool on WeChat, a popular messenger app with over 800 million monthly active users.

报告人简介：

Tao Xie is an Associate Professor and Willett Faculty Scholar in the Department of Computer Science at the University of Illinois at Urbana-Champaign, USA. He worked as a visiting researcher at Microsoft Research. His research interests are in software engineering, focusing on software testing, program analysis, software analytics, software security, and educational software engineering. He received a 2016 Microsoft Research Outstanding Collaborators Award, a 2014 Google Faculty Research Award, 2008, 2009, and 2010 IBM Faculty Awards. He is an ACM Distinguished Speaker and an IEEE Computer Society Distinguished Visitor. He is an ACM Distinguished Scientist. His homepage is at http://taoxie.cs.illinois.edu.

报告题目：基于分类器知识抽取的绕开攻击

报告人：梁彬（中国人民大学）

报告摘要：

Various classifiers based on the machine learning techniques have been widely used in security applications. Meanwhile, they also became an attack target of adversaries. However, the security of the classifiers deployed in the client environment has not got the attention it deserves. Besides, the security of widely-used commercial classifiers still remains unclear. We use the *Google's phishing pages filter* (GPPF), a classifier deployed in the *Chrome* browser and with over one billion users, as a case to investigate the security challenges for the client-side classifiers. A new attack methodology targeted to client-side classifiers, called *classifiers cracking*, is presented. According to the methodology, we successfully crack the classification model of GPPF and extract sufficient knowledge from it for performing effective evasion attacks, including the classification algorithm, scoring rules and features, etc. Based on the cracked information, we perform two kinds of evasion attacks to GPPF, using 100 real phishing pages as the target of evaluation. The experiments show that all the phishing pages (100%) can be easily manipulated to bypass the detection of GPPF. Our study demonstrates that the existing client-side classifiers are very vulnerable to classifiers cracking attacks.

Besides, deep neural networks (DNNs) play a key role in many applications, which have exhibited state-of-the-art performance. Meanwhile, their robustness has also raised concerns. Current studies focus on crafting adversarial samples against DNN-based image classifiers by introducing some imperceptible perturbations to the input. However, DNNs for natural language processing have not got the attention they deserve. We present a simple but effective method to attack DNN-based text classifiers. Three perturbation strategies, namely *insertion*, *modification*, and *removal*, are designed to generate an adversarial sample for a given text. By computing the cost gradients, what should be inserted, modified or removed, where to insert and how to modify are determined effectively. The experimental results show that the adversarial samples generated by our method can successfully fool a state-of-the-art model to misclassify them as any desirable classes without compromising their utilities. At the same time, the introduced perturbations are difficult to be perceived. Our study also demonstrates that DNN-based text classifiers are also prone to the adversarial sample attack.

报告人简介：

梁彬，中国人民大学信息学院副教授，博士生导师，研究方向为软件安全性分析。长期从事软件缺陷/漏洞和恶意软件的检测与分析技术研究，主要在代码静态分析、动态分析、代码挖掘、智能手机安全等方面开展研究，实现了多个较为成熟相关的原型系统。基于所研究的技术，在 Linux 内核、Android 基础架构、Chrome 等主流浏览器等重要基础性信息系统中成功发现了相当数量的未知漏洞/缺陷。

被遴选为中国政府与微软公司签署的 GSP 政府安全计划授权专家，获得授权查看微软产品源代码。目前已在 ICSE 2016，WWW 2016, ICSE 2014, DSN 2014 等重要会议和刊物上录用和发表了四十余篇学术论文，近年来作为项目负责人承担过多个国家级科研项目。近期研究成果：

[1] Bin Liang, Pan Bian, Yan Zhang, Wenchang Shi, Wei You, Yan Cai. AntMiner: Mining More Bugs by Reducing Noise Interference. In Proceedings of the 38th International Conference on Software Engineering (ICSE 2016), May 2016.

[2] Wei You, Bin Liang*, Wenchang Shi, Shuyang Zhu, Peng Wang, Sikefu Xie, Xiangyu Zhang. Reference Hijacking: Patching, Protecting and Analyzing on Unmodified and Non-Rooted Android Devices. In Proceedings of the 38th International Conference on Software Engineering (ICSE 2016), May 2016.

[3] Bin Liang, Miaoqiang Su, Wei You, Wenchang Shi, Gang Yang. Cracking Classifiers for Evasion: A Case Study on the Google's Phishing Pages Filter. In Proceedings of the 25th International World Wide Web Conference (WWW 2016), April 2016.

[4] Jianjun Huang, Xiangyu Zhang*, Lin Tan, Peng Wang, and Bin Liang*. AsDroid: Detecting stealthy behaviors in Android applications by user interface and program behavior contradiction. In Proceedings of the 36th International Conference on Software Engineering (ICSE 2014), May-June, 2014.

[5] Bin Liang, Wei You, Liangkun Liu, Wenchang Shi, Mario Heiderich. Scriptless Timing Attacks on Web Browser Privacy. In Proceedings of the 44th International Conference on Dependable Systems and Networks (DSN 2014), June 2014.

研讨会报告

报告题目：安全 C 语言程序验证器原型的研发经验与成果

报告人：陈意云（中国科学技术大学）

报告摘要：

简要介绍安全 C 语言程序验证器原型的验证流程；通过验证一些不同特色的 C 语言小程序，重点介绍验证器的技术特点。

1．循环不变形状图的推断：对于操作易变数据结构的程序，自动推断有关堆指针的循环不变式。

2．形状系统的设计：模仿类型系统那样设计形状系统。

3．程序员提供的引理的自动证明：数据类型的一些归纳性质，不是基于演绎推理的自动推理证明器能够发现的，系统自动证明程序员提供的归纳引理。

4．对模块化验证的支持：各个 C 源文件可以分别验证，然后进行 C 源文件的连接检查和调用 main 函数的验证，以达到整个程序的完整验证。

5．系统提供的辅助排错功能：对于没有被证明的验证条件，系统通过对其进一步分析，给出一些排错提示。

报告人简介：

1946 年生，1965 年中学毕业，随后上山下乡当了 13 年知青。1978 年考取中国科大，1980 年专科毕业于中国科大，1982 年 12 月研究生毕业于上海华东计算所，获硕士学位。1983 年开始一直在中国科大计算机系工作，其中 1989 年到美国芝加哥大学访问两年。

主要研究方向：程序设计语言理论和实现技术、程序验证、软件安全等。主持完成了多项国家自然科学基金面上项目以及若干其它项目。

近期与报告相关的论文：

1．Zhao-Peng Li, Yu Zhang, and Yi-Yun Chen. A shape graph logic and a shape system. Journal of Computer Science & Technology, Vol. 28, No. 6, pp. 1063-1084, Nov. 2013.

2．张昱、陈意云、李兆鹏，形状图理论的定理证明，计算机学报，Vol. 39, No. 12, Dec. 2016.

报告题目：静态分析工具原理、现状及解决方法

报告人：李炼（中科院计算所）

报告摘要：

静态程序分析检错通过静态分析源程序来计算程序运行时可能出现的各种状态，从而有效发掘出程序中可能潜在的 bug 和安全漏洞。它是业界公认的能够有效提高程序可靠性和安全性的重要手段：各种商业和开源的静态分析检错工具，如 Coverity、Fortify、Facebook Infer、Clang STA 等也都在一定程度内得到了比较广泛的应用。本报告将回顾静态分析检错原理以及其面临的一些关键难点：其中一个重要的基本的问题是如何高效地进行全局分析(例如涉及复杂指针和别名关系的全局指针分析)而不影响检错准确性。这一问题目前的静态检错工具工具并未有效解决，其结果是通常导致比较严重的漏报。针对这一问题，我们提出了一个全新的方法并开发出了静态分析检错原型系统 wukong, 能够有效准确地检测出涉及复杂指针别名关系的各种错误。初步实验结果表明 Wukong 可以在 1 分钟内有效分析近 10 万行代码，并能准确检测出数十个全新的深层次错误。

报告人简介：

李炼目前是中科院计算所的百人计划研究员，领导着程序分析小组的研究工作。李炼于 1998 年毕业于清华大学工程物理系，并于 2007 年在澳大利亚新南威尔士大学获得博士学位，长期在 Oracle 澳大利亚实验室担任主管研究员。其研究集中于编译和程序分析方向，研究目标是开发出有实际应用价值的程序分析工具，帮助解决软件开发、测试、调试过程中的重要问题。李炼曾在软件工程和编译领域顶级会议和刊物如 FSE、PACT、TC、TACO、TECS、LCTES 上发表多篇文章。其作为关键和主要研发人员开发的静态分析检错工具 Parfait 已经成功转变为 Oracle 公司内部产品，成为上万名 Oracle 工程师日常使用的开发工具。

报告题目：A Practical Verification Framework for Preemptive OS Kernels

报告人：付明（中国科学技术大学）

报告摘要：

We propose a practical verification framework for preemptive OS kernels. The framework models the correctness of API implementations in OS kernels as contextual refinement of their abstract specifications. It provides a specification language for defining the high-level abstract model of OS kernels, a program logic for refinement verification of concurrent kernel code with multi-level hardware interrupts, and automated tactics for developing mechanized proofs. The whole framework is developed for a practical subset of the C language. We have successfully applied it to verify key modules of a commercial preemptive OS uC/OS-II, including the scheduler, interrupt handlers, message queues, and mutexes, etc. We also verify the priority-inversion-freedom (PIF) in uC/OS-II. All the proofs are mechanized in Coq. To our knowledge, our work is the first to verify the functional correctness of a practical preemptive OS kernel with machine-checkable proofs.

报告人简介：

付明，男，1982 年生，博士，特任副研究员。分别于 2004 年和 2010 年获中国科学技术大学学士和博士学位。2009 年 11 月至 2010 年 10 月访问美国耶鲁大学计算机系。2010 年 11 月至 2016 年 7 月任中国科学技术大学计算机学院博士后研究员。2016 年 8 月起任中国科学技术大学计算机学院特任副研究员。

近期研究成果：

A Practical Verification Framework for Preemptive OS Kernels.
Fengwei Xu, Ming Fu*, Xinyu Feng, Xiaoran Zhang, Hui Zhang and Zhaohui Li. Proc. 28th International Conference on Computer Aided Verification (CAV'16), Toronto, Ontario, Canada, Part II, pages 59-79 July, 2016.
Jingyuan Cao, Ming Fu* and Xinyu Feng. Practical Tactics for Verifying C Programs in Coq. Proc. 4th ACM-SIGPLAN Conference on Certified Programs and Proofs (CPP'15), Mumbai,India, pages 97-108, January, 2015.

报告题目：Parametric Runtime Verification of C Programs

报告人：陈哲（南京航空航天大学）

报告摘要：

Many runtime verification tools are built based on Aspect-Oriented Programming (AOP) tools, most often AspectJ, a mature implementation of AOP for Java. Although already popular in the Java domain, there is few work on runtime verification of C programs via AOP, due to the lack of a solid language and tool support. In this paper, we propose a new general purpose and expressive language for defining monitors as an extension to the C language, and present our tool implementation of the weaver, the MOVEC compiler, which brings fully-fledged parametric runtime verification support into the C domain. This paper has been published in TACAS 2016.

报告人简介：

1. Zhe Chen, Zhemin Wang, Yunlong Zhu, etc. Parametric Runtime Verification of C Programs. In *Proceedings of the 22nd International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS 2016)*, *Lecture Notes in Computer Science*, vol. 9636, pp. 299-315. Springer, 2016.
2. Zhe Chen, Ou Wei, Zhiqiu Huang, etc. Formal Semantics of Runtime Monitoring, Verification, Enforcement and Control. In *TASE 2015*, pp. 63-70. IEEE Computer Society, 2015.
3. Zhe Chen, Yi Gu, Zhiqiu Huang, etc. Model Checking Aircraft Controller Software: A Case Study. *Software-Practice & Experience*, vol. 45(7), pp. 989-1017. Wiley, 2015.
4. Zhe Chen. Control Systems on Automata and Grammars. *The Computer Journal*, vol. 58(1), pp. 75-94. Oxford University Press, 2015.
5. Zhe Chen, Daqiang Zhang and Yinxue Ma. Modeling and Analyzing the Convergence Property of the BGP Routing Protocol in SPIN. *Telecommunication Systems*, vol. 58(3), pp. 205-217. Springer, 2015.

报告题目：基于扩展 LSC 的列控系统运行时验证

报告人：柴铭（北京交通大学）

报告摘要：

对于列控系统这样的复杂系统而言，仅依靠传统的实施于开发阶段的模型检验和测试等方法很难保证系统的安全。运行时验证通过对系统实际运行的监控，可在运营阶段实现对系统持续性防护。建立运行时验证系统的主要问题是定义合适的监控规约语言，即建立一个便于理解、复杂度合理且具备足够表达能力的语言用于描述监控性质。我们通过对活动序列图（live sequence chart）引入必要前图、串接以及条件和赋值结构实现对语言的扩展。基于该扩展语言，包含充分和必要条件的命题，以及包含参数的性质可被直观表达。我们证明引入必要前图后的语言表达能力强于标准 LSC；不包含迭代的 eLSC 表达能力等同于 LTL；以及 eLSC 在否定上是闭合的。为生成监控器，我们将 eLSC 转为混成逻辑，并证明 eLSC 随输入迹的增长复杂度是线性的。因此，该形式语言适用于对列控系统的监控。

报告人简介：

柴铭：2011 年-2015 年与柏林洪堡大学攻读博士学位，同期作为德国弗劳恩霍夫协会柏林 FOKUS 研究所的外聘人员，从事运行时验证方面的研究工作。2015 年至今在北京交通大学轨道交通运行控制系统国家工程研究中心任讲师。主要研究领域为规范逻辑语言、多真值逻辑、模型检验、运行时验证、基于模型的测试及其在轨道交通领域的应用等。

主要论文：

1.Ming Chai and Bernd-Holger Schlingloff. System Monitoring with a Five-valued LTL [J], Journal of Multiple-Valued Logic and Soft Computing, Vol. 26, pp. 33–54, 2016.

2.Ming Chai and Bernd-Holger Schlingloff. Monitoring Systems with Extended Live Sequence Charts [C], In: 14th International Conference on Runtime Verification (rv' 14), 2014.

3.Ming Chai and Bernd-Holger Schlingloff. Online Monitoring of Distribute Systems with a Five-valued LTL [C], In: 44th IEEE International Symposium on Multiple-Valued Logic (ISMVL 2014).

报告题目：利用动态分析结果对 Android 应用程序插桩

报告人：程志超（中国科学技术大学）

报告摘要：

Android 动态代码加载和反射技术，允许 Android 应用程序在运行时动态改变行为。这给 Android 开发者带来了方便，可以利用动态加载技术在程序安装后安装插件程序。该技术也给了恶意应用可乘之机。恶意软件可能在应用商店审核的时候表现为正常应用，但是当用户下载安装后，在运行时下载恶意代码并执行，这样便能规避应用商店的检测，威胁着智能手机的安全。我们的工作就是利用动态分析记录应用运行时的行为，包括加载的代码以及反射相关的调用，然后根据这些行为信息对 Android 应用程序进行插桩，使其能够被当前的静态分析工具更加精确地分析，比如构建更加完整的控制流图和进行更加精确地数据流分析。

报告题目：限界正确性与程序的模型检测

报告人：张文辉（中国科学院软件研究所）

报告摘要：

我们首先讨论限界正确性检查方法的原则，然后讨论限界正确性检查与传统符号模型检测及相关工具在算法设计与程序验证方面的可能应用，并讨论模型检测与测试的比较。我们认为模型检测与测试相比，在一些问题上是有优势的，模型检测方法应用的关键是需要有对正确可靠的程序的真正需求。

报告人简介：

1．Wenhui Zhang. QBF Encoding of Temporal Properties and QBF-Based Verification. IJCAR 2014:224-239.
2． Wenhui Zhang. Bounded Semantics. Theor. Comput. Sci. 564:1-29. 2015

报告题目：A Complete Decision Procedure for Linearly Compositional Separation Logic with Data Constraints

报告人：吴志林（中国科学院软件研究所）

报告摘要：

Separation logic is a widely adopted formalism to verify programs manipulating dynamic data structures. Entailment checking of separation logic constitutes a crucial step for the verification of such programs. In general this problem is undecidable, hence only incomplete decision procedures are provided in most state-of-the-art tools. In this paper, we define a linearly compositional fragment of separation logic with inductive definitions, where traditional shape properties for linear data structures, as well as data constraints, e.g., the sortedness property and size constraints, can be specified in a unified framework. We provide complete decision procedures for both the satisfiability and the entailment problem, which are in NP and Pi^ P_3 respectively.
This is a joint work with Xincai Gu, Taolue Chen

报告人简介：

吴志林，中国科学院软件研究所计算机科学实验室，副研究员。主要研究方向为软件形式化分析与验证，计算逻辑、自动机理论等。

报告题目：Analyzing divergence in bisimulation semantics

报告人：于婷婷（中国科学院软件研究所）

报告摘要：

通过应用一些著名的互模拟（bisimulation）等价关系（例如 weak bisimulation 和 branching bisimulation）验证程序正确性时，可能会得到发散（divergent）的系统与收敛（convergent）的系统相等。然而程序的发散性是一个很重要的性质，所以我们通过对内部迁移（τ-transition）的简单观察提出一个刻画保持发散性（divergence preserving）的互模拟等价关系的新方法。这个方法可以应用于弱互模拟（weak bisimulation）和分支互模拟（branching bisimulation）。我们用保持发散性的互模拟等价关系验证了 HSY-collision stack 的正确性。

报告人简介：

中国科学院软件研究所 2016 级博士生。

X. Liu, T. Yu, W. Zhang: Analyzing Divergence in Bisimulation Semantics. POPL2017.

报告题目：C 内存安全缺陷分析工具现状及演示

报告人：李兆鹏（中国科学技术大学）

报告摘要：

C 语言应用广泛，但由于其动态存储分配及无动态越界检查等语言特性，导致 C 语言程序在内存安全方面缺陷问题突出且难于通过测试发现。这里内存安全缺陷主要包括内存泄漏、空指针解引用（Dereference）、悬空指针使用、多次释放、释放栈变量、栈地址逃逸、只读数据区写操作、缓冲区溢出等。
静态分析是目前较为经济的发现代码 bug 的方法。本工作的目标是提供一个不需要用户提供任何额外标注的分析工具，该工具利用符号执行和自动定理证明技术、结合程序验证的霍尔逻辑及形状分析方法完成对代码内存安全问题的静态检测。其中，着重解决路径敏感的符号执行中状态爆炸等问题。
本次介绍 C 内存安全缺陷分析工具的研发现状、工具演示。

报告人简介：

李兆鹏，博士，副研究员，目前就职于中国科学技术大学计算机学院。报告人的工作集中在程序分析与验证方面，尤其是 C 语言程序的分析与验证方法方面。目前的工作思路是借助 C 程序验证方面的经验，将验证的思想应用于 C 程序分析。该工作目前进展中，未来条件成熟时尝试商业化。

报告题目：Securing a Compiler Transformation

报告人：邓超强（纽约大学）

报告摘要：

A compiler can be correct and yet be insecure. That is, a compiled program may have the same input-output behavior as the original, and yet leak more information. An example is the commonly applied optimization which removes dead (i.e., useless) stores. It is shown that deciding a posteriori whether a new leak has been introduced as a result of eliminating dead stores is difficult: it is PSPACE-hard for finite-state programs and undecidable in general. In contrast, deciding the correct- ness of dead store removal is in polynomial time. In response to the hardness result, a sound but approximate polynomial-time algorithm for secure dead store elimination is presented and proved correct. Furthermore, it is shown that for several other compiler transformations, security follows from correctness.

报告人简介：

邓超强，目前于纽约大学 Courant 学院计算机系攻读博士学位，导师是 Patrick Cousot 教授。2010 年，毕业于哈尔滨工业大学，获得学士学位。2013 年，毕业于中国科学技术大学，获得硕士学位，导师是曾凡平教授。详情请见个人主页 http://cs.nyu.edu/~deng/。

近期发表论文有：C. Deng, K. S. Namjoshi, “Securing a Compiler Transformation,” in International Static Analysis Symposium (SAS), pp. 170–188. Springer Berlin Heidelberg, Sep 2016.

报告题目：Pareto Optimal Scheduling for Synchronous Data Flow Graphs on Heterogeneous Multiprocessor

报告人：朱雪阳（中国科学院软件研究所）

报告摘要：

以数据驱动为显著特征的应用广泛存在于信号处理、通信、多媒体、家用电器、雷达等领域。这类系统一般是在嵌入式环境下运行的、处理无限长数据流的不终止程序，在运行时间和系统资源如处理器个数、缓存空间、能耗等方面受到严格限制。同步数据流（SDF）是一特殊的数据流语言，具有良好的可分析特性，已在这类系统的建模方面得到广泛应用。本报告将简要介绍我们近期关于 SDF 的吞吐量与能耗双目标优化调度方面的研究进展（发表于 ICECCS 2016）。

报告人简介：

朱雪阳（http://lcs.ios.ac.cn/~zxy/），博士，中国科学院软件研究所计算机科学实验室副研究员。作为技术骨干，先后参加了多项国家自然科学基金、863 项目的研究工作；目前主持一项基金面上项目。在嵌入式系统设计及形式化方法领域的主流国际期刊（IEEE Trans. On CAD）、国际会议(DATE、RTAS、FM、ICFEM、ICECCS)及国内一级学报发表多篇论文。主要研究领域：嵌入式系统设计、性能分析与优化及形式化方法。

近期研究成果代表作：

1. Yu-Lei Gu, **Xue-Yang Zhu**, Guangquan Zhang, Yifan He. Pareto Optimal Scheduling for Synchronous Data Flow Graphs on Heterogeneous Multiprocessor. In Proc. Of the 21st International Conference on Engineering of Complex Computer Systems (ICECCS 2016). Dubai, UAE, 6-8 Nov., 2016.
2. **Xue-Yang Zhu,** Marc Geilen, Twan Basten, and Sander Stuijk. Multi-Constraint Static Scheduling of Synchronous Dataflow Graphs via Retiming and Unfolding. IEEE Trans. on Computer-Aided Design of Integrated Circuits and Systems. vol. 35, no. 6, Pages 905-918，2016.
3. Yu-Lei Gu, **Xue-Yang Zhu** and Guangquan Zhang. Pareto Optimal Scheduling of Synchronous Data Flow Graphs via Parallel Methods. In Proc. Of the 1st International Symposium on Dependable Software Engineering: Theories, Tools and Applications (SETTA 2015). Nanjing, China, November 4-6, 2015. LNCS, vol. 9409, pp.217-223.
4. **Xue-Yang Zhu**, Rongjie Yan, Yu-Lei Gu, Jian Zhang, Wenhui Zhang and Guangquan Zhang. Static Optimal Scheduling for Synchronous Data Flow Graphs with Model Checking. In Proc. Of the 20th International Symposium on Formal Methods (FM 2015). LNCS, vol. 9109, pp. 551–569, 2015.
5. Gaogao Yan, **Xue-Yang Zhu**, Rongjie Yan and Guangyuan Li. Formal Throughput and Response Time Analysis of MARTE Models. In Proc. Of the 16th International Conference on Formal Engineering Methods (ICFEM 2014), LNCS, vol. 8829, pages 430-445, Luxembourg, 3-7 November, 2014.

6. Xue-Yang Zhu, Marc Geilen, Twan Basten, and Sander Stuijk. Memory-Constrained Static Rate-Optimal Scheduling of Synchronous Dataflow Graphs via Retiming. In Proc. Of the17th Design, Automation and Test in Europe (DATE2014), Dresden, Germany, 24-28 March, 2014.

报告题目：Darboux-type Barrier Certificates for Safety Verification of Nonlinear Hybrid Systems

报告人：林望（中国科学院数学与系统科学研究院）

报告摘要：

Benefit from less computational difficulty, barrier certificate based method has attracted much attention in safety verification of hybrid systems. Barrier certificates are inherent existences of a hybrid system and may have different types. A set of well-defined verification conditions is a prerequisite for successfully identifying barrier certificates of a specific type. Therefore, how to define verification conditions that can identify barrier certificates invisible to existing conditions becomes an essential problem in barrier certificate based verification. This paper proposes a set of verification conditions that helps to construct a new type of barrier certificate, namely, the Darboux-type barrier certificate made of Darboux polynomial. The proposed verification conditions provide powerful aids in non-linear hybrid system verification as the Darboux-type barrier certificates can verify systems that may not be settled by existing verification conditions.

Furthermore, we give a novel computational approach, combining the sampling-based relaxation method with least-squares and quadratic programming (LS-QP) alternating projection, to find Darboux-type barrier certificates. We demonstrate on the benchmark examples from the literature that our verification conditions can enhance the capability of barrier certificate based approaches through successfully verifying those systems that are difficult to be handled by existing verification conditions, and our algorithm is efficient.

报告人简介：

现于中科院数学与系统科学研究院从事博士后研究工作，主要研究方向为符号与数值混合计算、形式化方法，已在《ACM Transactions on Embedded Computing Systems》、《The Computer Journal》等期刊以及 EMSOFT、FM 等国际会议上发表论文多篇。

近期研究成果代表作：

1、 Xia Zeng,Wang Lin, Zhengfeng Yang, Xin Chen and Lilei Wang, Darboux-type Barrier Certificates for Safety Verification of Nonlinear Hybrid Systems, ACM/IEEE Conference on Embedded Software (EMSOFT),Article 11, 10 pages,2016.

2、 Zhengfeng Yang, Chao Huang, Xin Chen, Wang Lin and Zhiming Liu, A Linear Programming Relaxation Based Approach for Generating Barrier Certificates of Hybrid Systems, accepted for publication in 21st International Symposium on Formal Methods(FM2016),17 pages.

3、 Zhengfeng Yang, Wang Lin and Min Wu, Exact verification of hybrid systems based on bilinear SOS representation. ACM Transactions on Embedded

Computing Systems, 14(1), 1-19,2015.
4、 Wang Lin, Min Wu, Zhengfeng Yang and Zhenbing Zeng, Verification for non-polynomial hybrid systems using rational invariants, accepted for publication in The Computer Journal, 14 pages, 2017.

报告题目：基于仿真的可达集一致性测试

报告人：张勇（北京交通大学）

报告摘要：

一般的形式化方法无法直接在复杂的实际系统中使用，因此一般情况下是对真实系统的抽象系统进行验证。因此，我们需要确保真实系统同样满足抽象系统所具有的被验证的性质。研究中我们使用基于仿真的方法计算抽象系统的可达集，并对抽象系统的性质进行了验证，通过 scade 构建了真实系统的模型，并收集了郑西线真实车载设备的实际数据，通过两系统间可达集一致性关系的满足与否判断真实系统是否满足相应的性质。

报告题目：一种路径感知的变异体精简方法

报告人：孙昌爱（北京科技大学）

报告摘要：

变异测试（也称变异分析）是一种基于故障的软件测试技术。大量的实践表明，变异测试具有较强的故障检测能力，广泛用来评估测试用例集的充分性与某个软件测试技术的有效性。由于变异测试产生大量的变异体，存在计算开销高等问题，变异测试在软件测试实践中并没有得到广泛应用。本报告中，我们从程序结构分析角度出发探讨变异体精简问题，介绍一种基于路径深度的变异体精简方法及其相应的支持工具。该方法首先定义模块深度和循环/分支深度的概念，然后设计一组基于深度优先的变异体选择启发式规则，通过赋予启发式规则不同的优先级设计多种变异体精简策略。此外，本报告简要介绍课题组在非均匀分布的变异分析方法、面向 BPEL 程序的变异测试技术方面的研究进展。

报告人简介：

孙昌爱，博士，教授，博士生导师，现任北京科技大学计算机与通信工程学院院长助理、软件工程与网络空间安全研究所所长。2002 年毕业于北京航空航天大学，获计算机软件与理论博士学位（硕博连读）；1997 年毕业于北京科技大学，获计算机应用学士学位。曾在美国普渡大学（2013-2014）、荷兰格罗宁根大学（2005-2006, 2012）、澳大利亚斯文本大学（2004-2006）、德国帕德博恩大学（2012）、香港理工大学（2003）从事学术研究与交流。长期从事软件工程与服务计算方面的研究与实践，侧重于软件测试、程序分析、软件体系结构、服务计算等方向。在 ACM Transactions on the Web、IEEE Transactions on Services Computing、Journal of Systems and Software、计算机学报、软件学报等国内外重要学术刊物和国际会议上发表论文 70 余篇、申请国家发明专利 5 项、登记计算机软件著作权 18 项，出版译著 3 部。主持完成国家自然科学基金、北京市自然科学基金等十余项研究课题。中国计算机学会高级会员、IEEE 高级会员、中国计算机学会服务计算专委常委、中国计算机学会软件工程专委委员、入选北京市优秀人才培养计划（2012）。担任国际会议“12th IEEE International Conference on Ubiquitous Intelligence and Computing （UIC 2015）”、“Special track on Reliability Technologies and Tools for Services-based Systems (RTTSBS) in APSCC 2014”、“First International Symposium on Trusted Computing（TrustCom 2008）”程序委员会主席、国际会议“8th IEEE International Conference on Service Oriented Computing and Applications （SOCA 2015）”研讨会主席、“2015 年服务软件的测试与分析研讨会”大会主席、“2013 年中荷双边国际研讨会”大会主席。

- **C. Sun**, L. Pan, Q. Wang, H. Liu, X. Zhang. An Empirical Study on Mutation Testing of WS-BPEL Programs, ***The Computer Journal,*** 2016, in press (DOI:10.1093/comjnl/bxw076)
- **C. Sun**, F. Xue, H. Liu, X. Zhang. A Path-aware Approach to Mutant Reduction in Mutation Testing, ***Information and Software Technology***, Elsevier, 2017, 81(1):65-81.
- **C. Sun**, Y. Zhao, L. Pan, H. Liu, T.Y. Chen. Automated Testing of WS-BPEL

Service Compositions: A Scenario-Oriented Approach, ***IEEE Transactions on Services Computing***, 2016, in press (DOI: 10.1109/TSC.2015.2466572)

- **C. Sun**, Y. Zhao, L. Pan, X. He, D. Towey. A Transformation-based Approach to Testing Concurrent Programs using UML Activity Diagrams, ***Software: Practice and Experience***, Wiley, 2016, 46(4):551–576.

C. Sun, Y. Shang, M. Aiello. Integrating Transactions into BPEL Service Compositions: An Aspect-based Approach. ***ACM Transactions on the Web***, 2015, 9(2): 9:1-9:31.

报告题目：软件运行环境依赖缺陷及其挑战

报告人：郑征（北京航空航天大学）

报告摘要：

应用软件在设计和编写时通常假设其处于一个良好的并且可以预测的运行环境中。然而，近期研究以及大量的软件失效案例表明，由于软件运行环境（例如，操作系统等）的不可预测性和不当行为，导致应用软件正在经历着越来越多的相关失效。本报告主要围绕这类软件运行环境依赖缺陷的特征、触发及传播特性展开讨论，并对其为调试和容错技术带来的挑战和机会进行分析。

报告人简介：

郑征，中科院计算所博士，目前为北京航空航天大学副教授，博士生导师，系副主任。曾获中国科学院院长奖、北京市英才计划、工信部唯实人才计划等，主要研究方向包括软件可靠性与测试、机载软件适航。发表论文 60 余篇，参与 C919，MA700，运 20 等重要航空型号安全关键软件可靠性设计、测试和评估以及机载软件适航审定工作。

2016 年发表相关论文：

[1] Zheng Zheng, Kishor Trivedi, Kun Qiu, Semi-Markov Models of composite Web services for their performance, reliability and bottlenecks, 6(1), IEEE Transactions on Service Computing, Available online, 2016.

[2] Guanping Xiao, Zheng Zheng*, Haoqin Wang, Evolution of Linux operating system network, Physica A, Available online, 2016.

[3] Fangyun Qin, Zheng Zheng*, Yu Qiao, An Empirical Investigation of Fault Triggers in Android Operating System, PRDC, Accepted, 2017.

报告题目：覆盖率导引的针对 Java 虚拟机实现的差别测试（Coverage-Directed Differential Testing of JVM Implementations）

报告人：陈雨亭（上海交通大学）

报告摘要：

Java virtual machine (JVM) is a core technology, whose reliability is critical. Testing JVM implementations requires painstaking effort in designing test classfiles (*.class) along with their test oracles. We tackle this challenge by introducing classfuzz, a coverage-directed fuzzing approach that focuses on representative classfiles for differential testing of JVMs' startup processes. Our core insight is to (1) mutate seeding classfiles using a set of predefined mutation operators (mutators) and employ Markov Chain Monte Carlo (MCMC) sampling to guide mutator selection, and (2) execute the mutants on a reference JVM implementation and use coverage uniqueness as a discipline for accepting representative ones. The accepted classfiles are used as inputs to differentially test different JVM implementations and find defects.

We have implemented classfuzz and conducted an extensive evaluation of it against existing fuzz testing algorithms. Our evaluation results show that classfuzz can enhance the ratio of discrepancy-triggering classfiles from 1.7% to 11.9%. We have also reported 62 JVM discrepancies, along with the test classfiles, to JVM developers. Many of our reported issues have already been confirmed as JVM defects. This work was presented at PLDI 2016 and some future work on JVM testing is ongoing.

报告人简介：

陈雨亭，上海交通大学副教授，研究方向为程序分析与测试、形式化方法。

1. Yuting Chen, Ting Su, Chengnian Sun, Zhendong Su, and Jianjun Zhao. Coverage-Directed Differential Testing of JVM Implementations. In Proc. ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI 2016), Santa Barbara, CA, June 13-17, 2016.
2. Yuting Chen, Zhendong Su. Guided differential testing of certificate validation in SSL/TLS implementations. ESEC/SIGSOFT FSE 2015: 793-804

报告题目：代码分析、验证技术的集成

报告人：赵建华（南京大学计算机系）

报告摘要：

代码验证的自动化是促进代码验证技术应用的重要手段。我们正在做的工作是以 Scope Logic 为逻辑基础，将各类静态分析验证技术集成起来获得一个有效的代码验证工具。首先，我们把代码验证工作分解成三种基本的操作：即公式的生成、传播、和逻辑推理；然后讲各类静态验证、分析工作集成起来提高代码验证的效率。从理论上讲，只要一个静态分析技术能够保证分析得到的性质是正确的、且分析结果能够用逻辑公式表示，那么我们就可以把它集成起来，提高工具的自动化程度。这些技术可以是数据流分析技术、最弱前置条件计算技术、符号执行、逻辑推理技术。我们的工具研发经验表明这个路线具有可行性和可扩展性。

报告人简介：

1989 年到 1993 年进入南京大学计算机系本科学习，获得学士学位。1993 年 9 月到 1996 年 1 月，在南京大学计算机系学习，获得硕士学位。1999 年 3 月毕业于南京大学计算机科学与技术系，同年 5 月获得博士学位。毕业后留校任教，2005 年晋升为南京大学计算机科学与技术系教授。主要研究方向为形式化方法与软件工程。1998 年到联合国大学国际软件技术研究所（澳门）学习研究，主要方向为形式化方法。2002 年 9 月-2002 年 12 月，赴加拿大 Calgary 大学进修。主持或作为骨干成员参与了包括 973 项目，863 项目，国家自然科学基金项目在内的多项科研项目。1998 年获得教育部科技进步二等奖，获奖名称《软件工程中的若干理论、技术和工具研究》，第六完成人。2003 年 1 月获得教育部科技进步二等奖，获奖名称《软件工程中的形式化方法和面向对象技术研究》，第 4 完成人。2005 年入选教育部新世纪人才培养计划、江苏省青蓝工程学术骨干培养计划.在国际国内学术会议和学术期刊发表科研论文 30 余篇。

[1]. Dingbao Xie, Lei Bu, Jianhua Zhao, Xuandong Li: SAT-LP-IIS joint-directed path-oriented bounded reachability analysis of linear hybrid automata. Formal Methods in System Design 45(1): 42-62 (2014)

[2]. Zhanqi Cui, Linzhang Wang, Xi Liu, Lei Bu, Jianhua Zhao, Xuandong Li: Verifying Aspect-Oriented Models against Crosscutting Properties. International Journal of Software Engineering and Knowledge Engineering 23(5): 655-676 (2013)

[3]. 5、 Xuandong Li, Minxue Pan, Lei Bu, Linzhang Wang, Jianhua Zhao: Timing analysis of scenario-based specifications using linear programming. Softw. Test., Verif. Reliab. 22(2): 121-143 (2012)

[4]. Lei Bu, Qixin Wang, Xin Chen, Linzhang Wang, Tian Zhang, Jianhua Zhao, Xuandong Li: Toward online hybrid systems model checking of cyber-physical systems'time-bounded short-run behavior. SIGBED Review 8(2): 7-10 (2011)

[5]. Jianhua Zhao, Xuandong Li: Scope Logic: An Extension to Hoare Logic for Pointers and Recursive Data Structures. ICTAC 2013: 409-426

[6]. Jiantao He, Linzhang Wang, Jianhua Zhao: Supporting Automatic Code

Review via Design. SERE (Companion) 2013: 211-218
[7]. Fengling Zhang, Lei Bu, Linzhang Wang, Jianhua Zhao, Xuandong Li: Poster Abstract: Numerical Analysis of WSN Protocol Using Probabilistic Timed Automata.ICCPS 2012: 237
[8]. Enyi Tang, Linzhang Wang, Jianhua Zhao, Xuandong Li: Time-leverage point detection for time sensitive software maintenance. ICSM 2012: 567-570
[9]. Zhanqi Cui, Linzhang Wang, Xi Liu, Lei Bu, Jianhua Zhao, Xuandong Li: Verifying Aspect-Oriented Activity Diagrams Against Crosscutting Properties with Petri Net Analyzer. SEKE 2012: 369-374
[10]. Xiaoyu Zhou, Qian Li, Jianhua Zhao: A New Approach of Partial Order Reduction Technique for Parallel Timed Automata Model Checking. SERE (Companion) 2012: 158-167

报告题目：代码坏味的检测与演化分析

报告人：刘辉辉（东南大学计算机科学与工程学院）

报告摘要：

代码坏味（code smell）是代码设计中潜在问题的警示信号, 与程序中具体的结构元素相关。它的出现将导致代码难于理解和修改，部分类型的坏味还与 bug 具有显著的相关性。当前，研究代码坏味的检测方法及重构推荐较多，分析代码坏味的演化较少。基于此，针对 Java 语言，我们开发了一款代码坏味演化分析工具 SmellEvolver，旨在通过对代码坏味的演化分析，使得软件利益相关者更加方便地管理坏味，当前，SmellEvolver 可检测 17 种代码坏味。通过对一些开源软件的检测，发现有些代码坏味在演化的过程中处于稳定状态，有些类型的代码坏味经常会“结队”出现，当多种类型的代码坏味出现在同一个代码实体（类或方法）中时，该代码实体在日后的演化过程中变更会更加频繁，因此，这些代码坏味需要重点关注。另外，SmellEvolver 还为用户提供可定制的 smell 检测和结果可视化功能。

报告人简介：

刘辉辉，男，1983 年生，东南大学计算机科学与工程学院在读博士生，研究方向是软件维护与演化，特别地，对代码变更检测，代码坏味的检测与演化分析感兴趣，当前，已完成两篇论文《CCEvaluator:Evaluating Cyclomatic Complexity Variation in the context of software evolution》《Java 类和包的易替换性度量与影响因素分析》均在评审中。

报告题目：基于机器学习约束求解的复杂代码符号执行

报告人：李鑫（南京大学计算机科学与技术系软件工程组）

报告摘要：

符号执行是一个被广泛应用的软件分析技术。该技术极大地依赖于底层的约束求解能力，而现有的约束求解器对非线性、三方库函数等复杂约束的支持能力非常有限，难以对相关代码进行分析。本报告从基于机器学习的约束求解展开，提出了面向复杂程序的基于机器学习的符号执行框架——MLB，将复杂路径约束可满足性问题转化为特定优化问题，并利用机器学习技术以取样、验证并迭代的方式快速收敛至正确解。实验表明，MLB 不仅能够很好的支持包含非线性复杂约束的程序，对于第三方库函数调用的程序也有很好的支持。

报告人简介：

李鑫，南京大学计算机科学与技术系软件工程组在读硕士生，主要工作集中于复杂代码分析验证方向，特别是对非线性代码的符号执行及有界验证。本报告工作发表于 2016ASE《Symbolic Execution of Complex Program Driven by Machine Learning Based Constraint Solving》

报告题目: LockPeeker：一种检测 Java API 中的隐式锁的方法（LockPeeker: Detecting Latent Locks in Java APIs）

报告人：林子熠（上海交通大学）

报告摘要：

Detecting lock-related defects has long been a hot research topic in software engineering. Many efforts have been spent on detecting such deadlocks in concurrent software systems. However, latent locks may be hidden in application programming interface (API) methods whose source code may not be accessible to developers. Many APIs have latent locks. For example, our study has shown that J2SE alone can have 2,000+ latent locks. As latent locks are less known by developers, they can cause deadlocks that are hard to perceive or diagnose. Meanwhile, the state-of-the-art tools mostly handle API methods as black boxes, and cannot detect deadlocks that involve such latent locks.

In this research, we propose a novel black-box testing approach, called LockPeeker, that reveals latent locks in Java APIs. The essential idea of LockPeeker is that latent locks of a given API method can be revealed by testing the method and summarizing the locking effects during testing execution.

We have evaluated LockPeeker on ten real-world Java projects. Our evaluation results show that (1) LockPeeker detects 74.9% of latent locks in API methods, and (2) it enables state-of-the-art tools to detect deadlocks that otherwise cannot be detected.

报告人简介：

林子熠 上海交通大学软件学院博士生，研究方向为 Java 并发程序错误检测和分析。

1. Ziyi Lin, Hao Zhong, Yuting Chen and Jianjun Zhao. LockPeeker: Detecting Latent Locks in Java APIs. In Proc. ASE, 2016.

2. Ziyi Lin, Darko Marinov, Hao Zhong, Yuting Chen and Jianjun Zhao. JaConTeBe: A Benchmark Suite of Real-World Java Concurrency Bugs. In Proc. ASE, 2015

报告题目: Towards Certified Compositional Compilation for Concurrent Programs

报告人: 梁红瑾（中国科学技术大学）

报告摘要：

Certified compositional compilation is important for establishing end-to-end guarantees for certified systems consisting of separately compiled modules. In this talk, we propose a framework consisting of the key semantics components and verification steps that bridge the gap between the compilers for sequential programs and for (race-free) concurrent ones, so that the existing efforts on certified sequential compilation can be reused for concurrent programs. Contributions of the framework include an abstract formulation of race-freedom in an interaction semantics, and a footprint-preserving compositional simulation as the compilation correctness criterion.

报告人简介：

梁红瑾，2014 年 7 月毕业于中国科学技术大学，获博士学位。现任中国科学技术大学计算机学院特任副研究员。主要从事程序验证、并发理论、程序设计语言理论方面的研究。

研讨会工具展示报告

工具名称: Wukong

报告人: 李炼（中科院计算所）

工具基本介绍：

WuKong 是中科院计算所程序分析小组正在开发的静态分析检错工具：其针对的错误类型是 C/C++程序中常见的内存崩溃类型错误，如释放后引用(useafter-free)、内存泄漏(memory leak)、空指针引用(null pointer dereference)等。
和其他众多静态分析检错工具不同，Wukong 提出了一种全新的方法有效地解决了不精确的全局分析(如指针分析等)应用于检错时引起的误报率过高的问题，使其能够准确检测出涉及复杂指针操作的各种深层次错误。

工具名称: VolCE

报告人: 葛存菁（中科院软件所）

工具基本介绍：

计算一组约束的可满足的解个数被称作模型计数问题，这是一个经典的问题。VolCE 是一个计算或者估算 SMT(LA)公式（命题逻辑公式与线性算术理论混合）解空间的工具。该工具在之前的原型工具的基础上整合了新的凸多面体体积估算算法，并添加了若干改进策略。其体积估算功能可以处理几十维的问题。VolCE 将 SMT(LA)公式的解空间划分成若干个凸多面体，再对每个凸多面体的解空间进行计算或估计，最后求和得到解空间总的体积或者整点个数。它在处理每个凸多面体时使用如下三个工具：

(1) PolyVest，一个基于多相位蒙特卡洛算法的凸多面体体积估算工具；
(2) Vinci，一个实现了多个凸多面体体积算算法的软件包；
(3) LattE，一个基于 Barvinok 算法的软件包，可以用来统计凸多面体包含的整点个数。

工具名称: Java 切片工具

报告人: 王璐璐（东南大学）

工具基本介绍：

基于现有程序依赖图和切片算法，针对 Java 1.7 语言版本具体实现了生成、存储依赖图和动态、静态切片算法，具有较高的精度和实用性。

参会人员名单（按姓名排列）

姓名	单位	教师/学生	Email	研究方向
白石磊	中国人民大学	本科生	bslbaishilei@163.com	Android 系统安全
边攀	中国人民大学	博士生	bianpan@ruc.edu.cn	静态代码分析
卜磊	南京大学	副教授	bulei@nju.edu.cn	模型检验 CPS 系统
柴铭	北京交通大学	讲师	chaiming@bjtu.edu.cn	形式化方法在列控领域的应用
陈立前	国防科大	助理研究员	lqchen@nudt.edu.cn	程序分析、抽象解释
陈意云	中国科学技术大学　计算机学院	教授	yiyun@ustc.edu.cn	基于演绎推理的程序验证、程序分析
陈振邦	国防科技大学计算机学院	副研究员	zbchen@nudt.edu.cn	程序分析、形式化方法
陈英杰	国防科大	研究生	chenyingjie_nudt@163.com	程序分析
陈雨亭	上海交通大学	副教授	chenyt@cs.sjtu.edu.cn	程序分析与测试
陈哲	南京航空航天大学	副教授	zhechen@nuaa.edu.cn	软件验证，形式化方法
程成	北京理工大学	副教授	guoguocheng@vip.sina.com	人机交互，软件工程
程志超	中国科学技术大学	硕士研究生	czc1991@mail.ustc.edu.cn	Android 应用安全
池书琪	国防科大	硕士生	chishuqi16@nudt.edu.cn	软件可靠性
邓超强	纽约大学	博士生	deng@cs.nyu.edu	程序分析和验证，抽象解释，程序安全
邓茜	中国科学院软件研究所	研究生	dengxi_whu@163.com	程序分析；新型程序测试
董威	国防科技大学计算机学院	教授	wdong@nudt.edu.cn	高可信软件
方莹	国防科大	硕士生	2291875207@qq.com	信息安全
冯晓兵	中国科学院计算技术研究所	研究员	fxb@ict.ac.cn	编译与编程
冯志敏	国防科大	硕士生	374648064@qq.com	软件可靠性
付明	中国科学技术大学	副教授	fuming@ustc.edu.cn	操作系统内核验证、并发程序验证以及定理证明工具
葛存菁	中国科学院软件研究所	学生	gecj@ios.ac.cn	自动推理、约束求解
龚伟炜	国防科大	硕士生	2279423453@qq.com	程序分析
郭树利	中国科学技术大学 计算机科学	博士研究生	slguo@mail.ustc.edu.cn	网络安全

	与技术学院			
何春晖	中国科学技术大学	研究生	hchunhui@mail.ustc.edu.cn	软件分析和验证
侯刚	大连理工大学软件学院	讲师	hg.dut@163.com	模型检测
胡驰	国防科大	博士生	Superman@caep.cn	
胡燕	大连理工大学	讲师	huyan@dlut.edu.cn	软件测试
纪涛	国防科大	博士生	taoji@nudt.edu.cn	程序自动修复、克隆代码检测
贾维熙	国防科大	研究生	jiaweixi1016@163.com	软件程序代码分析
贾向阳	武汉大学	讲师	jxy@whu.edu.cn	程序分析、符号执行、模型检测
贾周阳	国防科大	博士生	jiazhouyang@nudt.edu.cn	软件可靠性
姜加红	国防科大	博士生	jhjiang@nudt.edu.cn	程序分析、抽象解释
蒋瀚如	中国科学技术大学	学生	hanru219@mail.ustc.edu.cn	可信编译技术
焦莉	中科院软件所	研究员	ljiao@ios.ac.cn	形式化方法
孔维强	大连理工大学	教授	wqkong@dlut.edu.cn	模型检测
李朝晖	中科大软件安全实验室	学生	812120868@qq.com	操作系统的形式化验证
李广元	中科院软件所	研究员	ligy@ios.ac.cn	形式化方法，实时系统形式验证，模型检测
李国强	上海交通大学软件学院	副教授	li.g@sjtu.edu.cn	形式化验证
李炼	中科院计算所	研究员	lianli@ict.ac.cn	程序
李珊珊	国防科大	副研究员	shanshanli@nudt.edu.cn	软件可靠性
李鑫	南京大学计算机科学与技术系软件工程组	硕士生	lixin@seg.nju.edu.cn	软件测试与验证
李薛剑	安徽大学，计算机科学与技术学院	讲师	wind1999@mail.ustc.edu.cn	程序分析与验证
李尧	国防科大	硕士生	401005445@qq.com	网络安全
李云峰	国防科大	硕士生	13203100054@163.com	软件可靠性
李兆鹏	中国科学技术大学	副研究员	zpli@ustc.edu.cn	程序分析、程序验证
郦旺	国防科大	硕士生	liwang2015@nudt.edu.cn	软件可靠性
梁彬	中国人民大学	副教授	liangb@ruc.edu.cn	软件安全、Android 系统安全、静态代码分析
梁红瑾	中国科学技术大学	副研究员	lhj1018@ustc.edu.cn	程序验证、并发理论
梁洪亮	北京邮电大学	副教授	hliang@bupt.edu.cn	可信软件、系统安全

林望	中国科学院数学与系统科学研究院	无	linwang@wzu.edu.cn	符号数值混合计算、形式化方法
林子熠	上海交通大学	博士生	linziyi@sjtu.edu.cn	Java 并发程序错误和错误检测
刘斌斌	国防科大	博士生	liubinbin09@nudt.edu.cn	群智化软件开发
刘波	西南大学	讲师	liubocq@swu.edu.cn	软件工程
刘丹军	国防科大	硕士生	1992332182@qq.com	软件安全
刘峰宇	国防科大	硕士生	xuan-ling-2008@163.com	DLL 劫持防御
刘宏杰	北京交通大学	讲师	hjliu2@bjtu.edu.cn	形式化方法在列控领域的应用
刘辉辉	东南大学计算机科学与工程学院		lhhshuxue@126.com	代码坏味的检测与演化分析，代码变更检测
刘洁瑞	中国科学院软件研究所	研究生	liujr@ios.ac.cn	Android 程序分析
刘晋宇	国防科大	硕士生	liujinyu2016@yeah.net	软件可靠性
刘静	华东师范大学	教授	jliu@sei.ecnu.edu.cn	软件工程
刘怡君	国防科大	研究生	yjunjunliu@163.com	程序分析
刘宇	硕士生	软件分析	ly_nudt@126.com	软件分析
刘万伟	国防科技大学计算机学院	副教授	wwliu@nudt.edu.cn	模型检验、定理证明
陆柏霖	国防科大	研究生	920362672@qq.com	高可信软件
罗炜麟	南京航空航天大学	研究生	luoweilin@nuaa.edu.cn	形式化方法
吕成成	中国科学技术大学计算机科学与技术学院	研究生	lvcc@mail.ustc.edu.cn	网络安全
吕继东	北京交通大学	讲师	jdlv@bjtu.edu.cn	形式化方法在列控领域的应用
马恒太	中国科学院软件研究所	副研究员	hengtai@iscas.ac.cn	漏洞挖掘
马骁	硕士生	网络安全	527349148@qq.com	网络安全
糜娴雅	博士生	软件安全	mixianya@126.com	软件安全
宁宇	中国科学技术大学计算机科学与技术学院	硕士生	sirning@mail.ustc.edu.cn	程序分析与软件重构
牛旭	国防科大	硕士生	993273596@qq.com	软件故障诊断
钮俊	宁波大学计算机系	副教授	niujun@nbu.edu.cn	模型检测、服务计算、开源软件搜索、软件演化
潘临杰	中国科学院软件	博士研	panlj@ios.ac.cn	程序分析

	研究所	究生在读		
秦晓霞	安卓系统、应用程序安全	研究生	qinxx@mail.ustc.edu.cn	中国科学技术大学计算机科学与技术学院
裘宗燕	北京大学	教授	qzy@math.pku.edu.cn	形式化方法，程序理论
瞿靖东	中国人民大学	本科生	qujingdong2013@163.com	Web 安全
史浩	国防科大	硕士生		运行时验证
孙昌爱	北京科技大学	教授/博导	casun@ustb.edu.cn	软件测试, 程序分析, 故障定位, 软件体系结构, 服务计算
唐勇	副研究员	软件保护、系统安全、网络安全	ytang@nudt.edu.cn	软件保护、系统安全、网络安全
王海峰	北京交通大学	教授	hfwang@bjtu.edu.cn	形式化方法在列控领域的应用
王海军	西安交通大学	学生	hjwang@sei.xjtu.edu.cn	软件分析与测试，符号执行
王璐璐	东南大学	讲师	wanglulu@seu.edu.cn	软件工程
王雪飞	中国科学院软件研究所	助理工程师	xuefei13@iscas.ac.cn	漏洞挖掘
王戟	国防科技大学计算机学院	教授	wj@nudt.edu.cn	高可信软件
王毅	硕士生	恶意代码分析	wydexx@gmail.com	恶意代码分析
魏欧	南京航空航天大学	副教授	owei@nuaa.edu.cn	软件验证
文艳军	国防科大	副教授	yjwen@nudt.edu.cn	可信软件设计、形式化方法
吴顺	北京交通大学	学生	16111037@bjtu.edu.cn	形式化建模与验证
吴添勇	中国科学院软件研究所	博士研究生	wuty@ios.ac.cn	软件测试数据生成及 Android 静态分析
吴学光	国防科大	博士生	xueguangwu@nudt.edu.cn	程序分析、抽象解释
吴志林	中国科学院软件研究所	副研究员	wuzl@ios.ac.cn	形式模型，软件分析与验证
谢念念	中国科学技术大学计算机科学与技术学院	研究生在读	xnn@mail.ustc.edu.cn	安卓安全
谢涛	University of Illinois at Urbana-Champaign	副教授	taoxie@illinois.edu	软件工程
徐立华	华东师范大学	副教授	lhxu@cs.ecnu.edu.cn	软件测试，错误定位，

				移动安全
徐鲁杭	国防科大	硕士生	me@xuluhang.cn	软件程序代码分析
徐向阳	国防科大	硕士生	xuxiangyang11@nudt.edu.cn	软件可靠性
徐雄	中国科学院软件研究所	无	xux@ios.ac.cn	搜索测试，启发式算法，Petri 网理论
玄跻峰	武汉大学	研究员	jxuan@whu.edu.cn	软件分析与测试
闫爽	国防科大	硕士生	1559005094@qq.com	软件可靠性
严俊	中国科学院软件研究所	副研究员	yanjun@ios.ac.cn	程序分析与测试
燕东	中国科学院软件研究所	硕士研究生	yandong14@otcaix.iscas.ac.cn	程序分析，软件测试
燕季薇	中国科学院软件研究所	学生	yanjw@ios.ac.cn	安卓软件测试
杨栋	国防科大	硕士生	yangdong5002@163.com	运行时验证
杨克	中国科学院软件研究所	博士研究生	yangke2015@iscas.ac.cn	漏洞挖掘
杨玲	中国科学院软件研究所	研究生	yangling@ios.ac.cn	程序分析、软件测试
杨珉	复旦大学	教授	m_yang@fudan.edu.cn	系统软件与系统安全
易昕	国防科大	博士生	yixin09@nudt.edu.cn	程序自动修复、浮点程序分析
尹良泽	国防科大	讲师	yinliangze@163.com	程序分析、形式化方法
于恒彪	国防科大	博士研究生	hengbiaoyu@nudt.edu.cn	程序分析、形式化方法
于婷婷	中国科学院软件研究所	博士生	yutt@ios.ac.cn	CCS、Linearizability
余凯	国防科大	助理工程师	chinakevinyu@163.com	程序分析、形式化方法
俞昕	硕士生	信息安全	1595183098@qq.com	信息安全
喻波	助理研究员	网络安全		网络安全
曾凡平	中国科学技术大学 计算机科学与技术学院	副教授	billzeng@ustc.edu.cn	软件分析与测试，网络与信息安全
张广泉	苏州大学计算机学院	教授	gqzhang@suda.edu.cn	软件建模与验证
张凯	上海市华东师范大学计算机科学与软件工程学院	学生	735618296@qq.com	形式化验证，定理证明，模型检测，Runtime Verfication
张丽	国防科大	硕士生	1446417628@qq.com	软件质量
张龙	中国科学院软件研究所	博士研究生	zlong@ios.ac.cn	程序分析与测试

张健	中科院软件所	研究员	zj@ios.ac.cn	自动推理和约束求解、程序分析与软件测试
张圣迪	同济大学软件学院	学生	1641504@tongji.edu.cn	形式化方法
张文辉	中国科学院软件研究所	研究员	zwh@ios.ac.cn	形式模型、数理逻辑与程序逻辑、推理与模型检测、软件正确性的理论与方法
张文敏	国防科大	职工	249892475@qq.com	软件可靠性
张啸然	中国科学技术大学	研究生	clouilt@gmail.com	软件分析与验证
张银珠	国防科大	硕士生	344609397@qq.com	安全分析
张迎周	南京邮电大学计算机学院	教授	zhangyz@njupt.edu.cn	程序分析、程序切片、形式化方法
张勇	北京交通大学	学生	zhangyong15@bjtu.edu.cn	形式化建模与验证
张昱	中国科学技术大学计算机科学与技术学院	副教授	yuzhang@ustc.edu.cn	程序分析,可靠高效并行系统构建
赵恒军	西南大学	讲师	zhaohj2016@swu.edu.cn	软件形式化方法
赵建华	南京大学计算机系	教授	Zhaojh@nju.edu.cn	形式化方法，代码验证
詹乃军	中国科学院软件研究所	研究员	znj@ios.ac.cn	形式化方法
郑征	北京航空航天大学	副教授，博导	zhengz@buaa.edu.cn	软件可靠性与测试，机载软件适航
仲星球	中国科学技术大学	硕士研究生	Zh2789@mail.ustc.edu.cn	Android 应用安全
周戈	国防科大	博士生	zhouge1009@163.com	运行时验证
周寒茹	华东师范大学	学生	sei_zhr2011@126.com	软件分析与测试，形式化验证
周明松	中国科学技术大学计算机科学与技术学院	研究生	mingsong@mail.ustc.edu.cn	Android 安全
周书林	国防科大	硕士生	zhoushulin@nudt.edu.cn	软件可靠性
周旭	助理研究员		zhouxu@nudt.edu.cn	信息安全
周钰钦	国防科大	硕士生	834803632@qq.com	程序分析、形式化方法
朱丽华	国防科大	硕士生	hello_zhulihua@163.com	软件分析与代码演化
朱雪阳	中国科学院软件研究所	副研	zxy@ios.ac.cn	嵌入式系统设计、性能分析与优化及形式化方法
朱自明	中国科学院软件研究所	博士	zhuzm@ios.ac.cn	软件测试

会场和住宿酒店

1. 湖南长沙延年世纪酒店（会议酒店）

地址：湖南省长沙市开福区三一大道与车站北路交汇处

联系人：夏云飞经理（13548591765）

说明：该酒店是本次会议召开和就餐所在地。附近有火车票代售点，麦德龙超市，杨裕兴、博禧楼等餐馆。

2. 长沙金汇国际大酒店

地址：长沙开福区三一大道 332 号（延年酒店对面）

联系人：周丹经理（13786180016）

会务组联系信息

会务组在延年世纪、金汇国际两个酒店都有会务人员，具体联系信息如下：

昌灵：15874978290，save2016@sina.cn

陈振邦：13574866832，zbchen@nudt.edu.cn

董威：13873105966，wdong@nudt.edu.cn

王戟：13975151973，wj@nudt.edu.cn