中国科学院学部“科学与技术前沿论坛”
——软件与网络安全

会议手册

主办单位：中国科学院学部

承办单位：中国科学院信息技术科学部

中国科学院学部学术与出版工作委员会

协办单位：中国科学院软件研究所

《中国科学》杂志社

中国.北京

2014 年 11 月 13 日

目录

会议须知.....1

论坛日程.....2

参会代表名单.....3

摘要文集.....5

会议须知

1、会议时间：2014 年 11 月 13 日

2、会议地点：中国科学院学术会堂

3、报到时间：2014 年 11 月 13 日 8:00~8:30

4、报到地点：中国科学院学术会堂

5、会议就餐：11 月 13 日午餐，中国科学院学术会堂自助餐厅

6、会务组：

中国科学院软件研究所：

朱雪阳，负责：会场、会议资料

吕毅，负责：会场、会议资料

费腾，负责：餐饮、住宿、交通

中国科学院学部工作局：

魏秀

7、会议注意事项：会议期间，参会人员凭会务组制发的证件参加会议及用餐。请妥善保管有关证件，并遵守会议时间。会堂内禁止吸烟。

论坛日程

8:00-8:30 论坛报到
8:30-8:40 学部主任致辞
8:40-10:10　软件安全分析与漏洞检测（1）　　主持人：吕　建
8:40－9:00 邹　维:系统安全中的若干科学问题 9:00－9:20 张　路:程序分析与软件安全 9:20－9:40 苏璞睿:为软件产品“探伤”—以攻击者思维分析软件安全问题 9:40－10:10 **讨论**
10:10-10:30 茶歇
10:30-12:00　Web 与移动系统安全（1）　　主持人：郑建华
10:30－10:50 陈　硕:Mobile 和 Cloud 时代的软件安全研究新课题 10:50－11:10 段海新:SSL 协议在 Web 服务中的实现和部署安全分析 11:10－11:30 梁　彬:不依赖于脚本的浏览历史嗅探 11:30－12:00 **讨论**
12:00-2:00 午餐、午休
2:00-3:30 Web 与移动系统安全（2）　　主持人：梅　宏
2:00－2:20 杜文亮:移动系统的安全:攻击和防御 2:20－2:40 梁振凯:Web 平台和移动平台上面向数据的保护机制 2:40－3:00 杨　珉:基于权限机制的安卓软件分析和系统加固研究 3:00－3:30 **讨论**
3:30－3:50 茶歇
3:50－5:20 软件安全分析与漏洞检测（2）　　主持人：林惠民
3:50－4:10 王怀民:开源软件更安全更可信吗？ 4:10－4:30 石文昌:云环境软件可信状态探测机制 4:30－4:50 武成岗:内构安全的软件开发和运行时环境 4:50－5:20 **讨论**

参会代表名单

序号	姓名	职称/职务	单位
论坛执行主席及特邀嘉宾			
1.	李未	院士	北京航空航天大学
2.	梅宏	院士	上海交通大学
3.	吕建	院士	南京大学
4.	郑建华	院士	中国人民解放军保密委员会
5.	董韫美	院士	中国科学院软件研究所
6.	林惠民	院士	中国科学院软件研究所
论坛报告人（按报告人姓氏拼音排序）			
7.	陈硕	研究员	微软研究院雷德蒙分部
8.	杜文亮	教授	美国雪城大学
9.	段海新	教授	清华大学
10.	梁彬	副教授	人民大学
11.	梁振凯	副教授	新加坡国立大学
12.	石文昌	教授	人民大学
13.	苏璞睿	研究员	中国科学院软件研究所
14.	王怀民	教授	国防科学技术大学
15.	武成岗	副研究员	中国科学院计算技术研究所
16.	杨珉	副教授	复旦大学
17.	张路	教授	北京大学

序号	姓名	职称/职务	单位
18.	邹维	研究员	中国科学院工程信息研究所
研讨专家（排名不分先后）			
19.	李舟军	教授	北京航空航天大学
20.	陈钟	教授	北京大学
21.	梁洪亮	副教授	北京邮电大学
22.	陈钢	研究员	中国航天科工三院
23.	王颖		中国航天科工三院
24.	冯晓兵	研究员	中国科学院计算技术研究所
25.	金舒原	副研究员	中国科学院计算技术研究所
26.	张健	研究员	中国科学院软件研究所
27.	王永吉	研究员	中国科学院软件研究所
28.	丁丽萍	研究员	中国科学院软件研究所
29.	李昂生	研究员	中国科学院软件研究所
30.	张文辉	研究员	中国科学院软件研究所
31.	蒋颖	研究员	中国科学院软件研究所
32.	焦莉	研究员	中国科学院软件研究所
33.	刘剑	副研究员	中国科学院软件研究所
34.	李广元	副研究员	中国科学院软件研究所
35.	李勇坚	副研究员	中国科学院软件研究所
36.	杨绍发	副研究员	中国科学院软件研究所
37.	吕毅	副研究员	中国科学院软件研究所

摘要文集

目录

MOBILE 和 CLOUD 时代的软件安全研究新课题 6
移动系统的安全:攻击和防御 8
SSL 协议在 WEB 服务中的实现和部署安全分析 10
不依赖于脚本的浏览历史嗅探 12
WEB 平台和移动平台上面向数据的保护机制 14
云环境软件可信状态探测机制 16
为软件产品“探伤”—以攻击者思维分析软件安全问题 18
开源软件更安全更可信吗？ 20
内构安全的软件开发和运行时环境 22
基于权限机制的安卓软件分析和系统加固研究 24
程序分析与软件安全 26

Mobile 和 Cloud 时代的软件安全研究新课题

陈硕

微软研究院(Microsoft Research Redmond)

这个报告的重点是对近年来 Mobile 和 Cloud 安全领域的研究方向和文献做一个综述。对比传统软件安全问题，我认为 Mobile 和 Cloud 带来了四个新的挑战：

(1)更多样的 Trust Model： Mobile 和 Cloud 计算的参与方比传统软件复杂，包括了 Mobile 端用户、Mobile 应用、Cloud 平台、Cloud 应用(tenant)、Cloud operator 等等。他们之间不完全信任，因此产生了很多新课题。比如 sandboxing, 权限，可验证计算，homomorphic encryption, 跨虚拟机的测信道等亟待解决的问题。

(2) 多方（跨公司）分布/协同： cloud 应用往往是跨公司的分布/协同，比如第三方支付、第三方认证等。每个公司开发自己的服务，以 Web API 形式供其它方调用。这意味着系统的安全性取决于各方是否充分互相理解。遗憾的是，目前的软件开发方法没有充分保证安全性，各种逻辑漏洞非常普遍。

(3) 采用异构技术及平台： Mobile/Cloud 系统通常是许多技术的集成——多种语言、不同的执行平台这使得安全性取决于程序员及验证工具对这些语言和平台的细微差别的了解。

(4) 对高可靠性的需求：传统程序在不安全情况下可以终止，而 Cloud 服务通常不允许由用户导致的程序终止。这对程序安全性的要求更高：程序员如何才能预见和处理所有可能的 exception，包括来自他自己程序的和来自底层系统的?

因为时间关系，我将重点介绍前两点。报告中提及的文献并不全面，只希望能抛砖引玉。

报告人简介

陈硕

现任微软研究院(Microsoft Research Redmond)资深研究员。其主要研究方向是软件系统安全，尤其关注于发现和思考实际系统中的安全漏洞和挑战。2007-2009 年，他研究浏览器安全，期间发现一系列“用户界面逻辑错误”，可以导致严重的钓鱼攻击；并且发现所有浏览器在处理 HTTPS 响应中均存在一类逻辑漏洞，导致 HTTPS 失效。这些发现大多数被厂商确认和修复。2010 年，他发现“Web 侧信道(side channel)”问题在使用 Web 2.0 技术的网站中非常普遍且危险。用户隐私信息，如投资、收入、医疗等，即使加密传输，仍然通过侧信道暴露给网络监听者。2011 年至今，他关注云服务集成中的逻辑正确性问题。他和同事发现许多使用第三方支付和第三方认证的系统存在逻辑漏洞，使得攻击者可以免费购物或在不知密码的情况下登陆别人的网站。针对这些问题，他们提出了一系列分析方法和安全编程方法。

他的工作曾获得 IEEE S&P 会议最佳实践论文奖和两次微软 Gold Star 奖。许多研究项目受到科技传媒的报道，包括 CNN, CNET, MIT Technology Review, ArsTechnica, Computer World, 等。他经常担任主要安全会议的程序委员，包括 IEEE S&P，USENIX Security, ACM CCS, WWW, 等。他毕业于北京大学、清华大学和伊利诺伊大学 Urbana-Champaign 分校，获得计算机科学学士、硕士和博士学位

移动系统的安全:攻击和防御

杜文亮

美国 Syracuse 大学

这个报告主要包括两个方面，一个是移动安全的研究，另一个是关于计算机和信息安全教育的研究。在移动安全方面我主要研究两个方向。第一个是对 Android 系统的各个 Component 的设计进行深入的分析，寻找可能的攻击和它们存在的本质问题。我们在对 WebView 的研究上取得了不少成果，其中包括发现了 WebView 设计上的一系列的安全隐患，并指出很多基于 HTML5 的手机 App（iOS 和 Android）存在严重的 Code Injection 问题。我们的这项发现被许多新闻媒介转载。我研究的第二个方向是 Access Control。我们的目的是对 Android 现有的 Access Control 机制进行深入的研究，寻找它们在设计上的不足之处，提出创新的想法和新的模式，然后在 Android 系统上实现，并设计试验去验证我们的想法是否真正达到了对 Access Control 的改进。报告中我会对我们在这个方向上的研究项目做一个概述。

报告的第二部分介绍我在计算机和信息安全教育方面的研究成果。在过去的十二年里，我一直在做一个叫 SEED 的项目，目的是开发一系列的可以用在安全教育上的动手的试验教材(SEED Labs)。这些试验可以让学生通过真正的动手经历去了解攻击和防御的原理，而不是只是从课本上学。目前我们开发了 30 个基于 Linux 的 Labs，涉及系统安全，网络安全，Web 安全，软件安全，和加密。这些 Labs 的使用完全是免费的。迄今为止它们被大约 30 个国家共 250 所学校采用。我目前正在开发基于 Android 的 SEED Labs。

报告人简介

杜文亮

教授。1993 年从中国科技大学本科毕业, 2001 年获得普渡大学计算机专业博士学位, 同年开始在 Syracuse 大学电子工程和计算机系任教, 2012 年晋升为教授。主要研究方向是计算机安全。在安全领域发表近一百篇论文。论文总引用次数达 8890 次(来源 Google Scholar)。2013 年荣获 ACM CCS 会议 Test-of-Time 奖。CCS 是计算机安全的顶尖会议, 它每年评出十年前在 CCS 发表的文章中最有影响的两篇论文授予该奖。

他现在的研究兴趣是计算机系统的安全, 主要集中在 Web 系统和移动操作系统(Android)。他的主攻方向是对这些系统的设计进行深入的分析, 从系统设计的角度去了解为什么它们的应用程序会有各种各样的安全问题, 如何改进系统的设计或提出安全方面的新的设计, 从而减少应用程序的安全隐患。他的这项研究获得美国自然科学基金和 Google 的资助(总金额 108 万美金)。他对计算机安全教育的研究也颇有兴趣。在过去的十二年里, 他设计了将近 30 个给计算机和网络安全课程用的实验教材。这项研究获得美国自然科学基金的多次资助(总金额 150 万美金)。全世界有超过 250 所学校在用这些实验教材, 中国也有些大学在使用。

SSL 协议在 Web 服务中的实现和部署安全分析

段海新

清华大学

基于公钥基础设施（PKI）的 SSL/TLS 是目前应用最为广泛的安全通信协议，是目前 Web 应用系统安全的基础。然而，无论从设计、实现还是部署方面，SSL 在 Web 应用中存在着许多安全问题。此报告从安全通信涉及到的多个参与方（Browser、Web Server、CA、DNS、CDN 等）分析 SSL 协议在 Web 应用中存在的安全隐患，包括信任模型的问题、证书撤销的问题、浏览器的同源问题、DNS 绑定问题、CDN 的授权代理等，并分析可能的攻击方式。最后介绍 DANE、Keyless SSL 等最新的研究进展，分析增强 SSL 安全性的未来发展。

报告人简介

段海新

博士，研究员，博士生导师。就职于清华大学网络科学与网络空间研究院，网络和信息安全研究室主任，加州大学伯克利访问学者。长期致力于网络安全相关的教学、科研和运行管理工作。主要研究兴趣：网络基础设施（域名、路由、公钥基础设施等）安全、Web 安全、网络协议安全性分析、入侵检测、网络测量、匿名通信等。

从研究生开始进入网络安全研究领域，二十年来一直从事网络和信息安全相关的研究、教学工作，并作为中国教育和科研计算机网应急响应组（CCERT）负责人参与网络运行安全管理工作，主要研究方向包括网络基础设施安全、Web 安全、入侵检测等。承担国家 973、863、自然科学基金项目多项，在国际顶级会议上有多篇学术论文发表，研究成果在国际工业界和学术界引起了广泛关注。中国密码学会协议安全专业委员会委员，多次担任国际学术会议程序委员或期刊审稿人。

不依赖于脚本的浏览历史嗅探

梁彬

中国人民大学

现代软件系统日益复杂，大大地增加了对其安全性分析的难度。同时，软件系统中不断引入的新特征还可能导致攻击面（Attack Surface）扩大。此报告将展示一种微妙的浏览器中新一代网页样式表 CSS3（Cascading Style Sheets 3）支持等新特性所导致的浏览历史嗅探（History Sniffing）攻击。传统的浏览历史嗅探攻击依赖于在客户端浏览器中执行一些嗅探脚本，如 JavaScript 脚本。现今，业界提出了很多防御技术来阻止可疑脚本的运行。我们发现可借助 CCS3 中的一些特性来间接地监控目标资源的渲染过程，从而可以不依赖于执行脚本来进行有效的浏览历史嗅探。对此，我们提出了两种不依赖于脚本的嗅探方法：基于度量的嗅探攻击和基于比较的嗅探攻击。实验表明，这两种攻击方法都能够应用于当前主流的桌面和智能手机浏览器，且能够获得非常高的准确度。报告工作表明：即使是在脚本阻断技术保护下的浏览器中，也仍然存在严重的隐式信息泄露风险。

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。2004 年博士毕业于中国科学院软件研究所。研究方向为信息安全与软件分析。近年来的工作主要集中在软件缺陷/漏洞和恶意软件的检测与分析，涉及到源码静态分析、动态污点分析及代码挖掘等方面。领导研发了多个相关检测分析工具，发现了 Linux、Android、浏览器等系统中存在的多个未知高危安全漏洞，及数十个被 Linux 内核开发组织确认了的内核缺陷。还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。近年来，担任了包括 3 个国家自然科学基金在内的多个软件分析及信息安全方面科研项目的负责人。

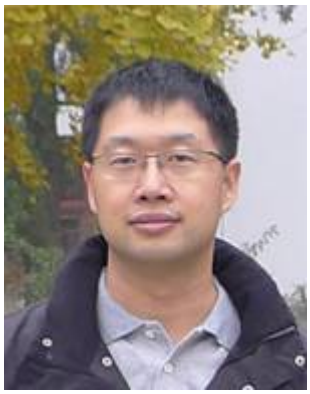
Web 平台和移动平台上面向数据的保护机制

梁振凯

新加坡国立大学

近年来，移动应用、Web 服务以及云服务的整合提供了一个全新的信息服务平台。与此同时，也对数据安全提出了新的挑战。在这样的复合信息平台中，用户数据被异构的复杂系统环境处理，其中的软件组件质量（可靠性、安全性）很难依据单一标准进行控制。传统的安全机制，如访问控制和权限分离，无法确保用户的关键数据不被恶意的代码访问、篡改。本报告介绍保障数据安全的另一个视角：通过提供面向数据的保护机制，即便平台中的组件存在软件漏洞，也可以确保用户的关键数据在其整个生命周期都会得到的安全保证。报告主要内容包括面向数据保护机制的设计，相关的研究进展，以及研究团队对软件和数据安全的未来研究规划。

报告人简介



梁振凯

博士，新加坡国立大学计算学院副教授。主要研究领域为系统安全与 Web 安全，目前研究主要集中于基于浏览器的 Web 应用安全检测与防护、远程攻击的响应和分析、以及软件调试研究。对操作系统安全机制、二进制代码分析、浏览器中的恶意行为检测与防护有坚实的工作积累，相关工作发表于 *ACM CCS, ACM SIGSOFT FSE, NDSS, IEEE S&P, Usenix Security, ACSAC, ESORICS* 等顶级国际会议和 *IEEE Transactions on Dependable and Secure Computing (TDSC)*、*ACM Transactions on Software Engineering and Methodology (TOSEM)*、*ACM Transactions on Information and System Security (TISSEC)*等顶级国际期刊。曾获得多个会议奖项，其中包括：2014 年 ICECCS 最佳论文奖，2014 年 W2SP Workshop 最佳论文奖，2009 年 *ACM SIGSOFT 杰出*论文奖（*ESEC/FSE*）、2007 年 *USENIX Security Symposium* 最佳论文奖、2003 年 *Annual Computer Security Applications Conference (ACSAC)*突出论文奖。2008 年获得新加坡国立大学的青年研究人员奖（Young Investigator Award），并于 2014 年获新加坡国立大学年度杰出教学奖。梁振凯博士 2006 年自纽约州立大学石溪分校（Stony Brook University）获得博士学位，1999 年于北京大学获得计算机学士和经济学双学士学位。2008 年至 2013 年为新加坡国立大学计算学院助理教授，2014 年晋升为副教授。

云环境软件可信状态探测机制

石文昌

中国人民大学

软件可信状态的在线监测是解决软件系统安全问题的重要措施之一，它涉及两方面的工作，其一是如何确定被监测对象的可信状态，其二是如何确保监测机制的可信性，后者是前者的保障，本报告重点关注后者，由于纯软件很难确保甚至判定自身的可信性，人们自然希望借助硬件提供必要的支撑，从上世纪八十年代起，无论是学术界还是工业界都开展了很多工作试图解决这类问题，面对云计算环境，业界也付出了很多新的努力，例如，Intel 着力为可信云环境的建立提供新的硬件支撑，而 IBM 则力图把传统的可信证明机制拓展到云环境之中，然而，在云环境中，本属一体化框架内的计算、存储和网络资源都分离到了独立的载体之中，使得支撑一个软件系统的组件失去了原有的绑定关系，传统的可信证明机制难以再适用，为监测机制可信性的判定提出了新的挑战，本报告探讨新挑战下的问题解决思路。

报告人简介

石文昌

博士，中国人民大学信息学院教授，博士生导师，计算机系主任，兼中国科学院信息工程所研究员及博士生导师，电子证据国家司法鉴定人，教育部信息安全专业教学指导委员会委员。北京大学理学学士，中国科学院工学硕士和工学博士，中国科学院院长奖获得者。主要研究方向为操作系统及基础软件安全。曾任中国科学院软件所研究员，中国科学院研究生院教授。率先完成 UNIX 操作系统在我国的成功移植，率先研究并开发实施国际信息安全 CC 标准，成功研制遵循国际和国家标准的安全操作系统，主持承担一系列国家科研项目，发表学术论文百余篇，编著了《信息系统安全概论》、《操作系统访问控制研究》和《安全操作系统原理与技术》等书籍，在安全、可信基础软方面取得过多项重要的理论研究成果和技术开发成果。

为软件产品“探伤”
—以攻击者思维分析软件安全问题

苏璞睿

中国科学院软件研究所

软件产品中存在的漏洞已成为网络安全的主要威胁之一，而攻击者对软件漏洞的利用这将威胁变成了实质性破坏。由于软件漏洞的隐蔽性和复杂性，软件漏洞的发掘、分析与利用已成为攻防双方关注的重要方向。从攻击者分析利用的角度分析软件漏洞，既是发现软件安全隐患的重要思路，也是评估漏洞危害，防御漏洞利用的重要方法。报告将分析当前典型软件漏洞分析工作模式，总结相关技术、方法的研究进展，并介绍团队在软件漏洞分析、软件漏洞利用自动生成（AEG）方面的工作，我们基于动态污点传播分析和符号执行，实现了对控制流劫持漏洞的多样性攻击代码自动生成，实验中，对于特定漏洞，最多生成了 4000 余种不同的攻击代码变种，该工作可为漏洞危害评估，入侵检测规则生成等工作提供支撑。

报告人简介

苏璞睿

中国科学院软件研究所研究员，博士生导师，中国科学院软件研究所可信计算与信息保障实验室副主任，中国密码学会安全协议专业委员会委员，国家网络安全实验平台特聘专家，北京市计算机网络病毒与预警专家组成员。曾任第一届中国网络攻防与系统安全会议(NADSS2010)会议，国际信息安全学术会议 OTM-IS’09，2014 年安全协议进展国际会议（PSP 国际会议）等学术会议程序委员会委员。长期从事软件安全性分析、恶意代码分析与防御、信息对抗与信息保障等研究工作，近年来共主持相关国家科技支撑计划、国家 863 计划、国家自然科学基金等各类科研项目十余项，在基于硬件虚拟化的软件动态逆向分析、软件漏洞分析与利用等方面取得进展，发表学术论文四十余篇，组织研发的恶意软件深度分析平台、APT 攻击检测系统、动态污点传播分析系统等系统和平台已在国家多个部门或机构得到应用，取得了良好的应用效果，曾获中国科学院院长奖、北京市科技进步奖等多项奖励和荣誉。

开源软件更安全更可信吗？

王怀民

国防科技大学

相对非开源的商用软件，开源软件不仅提供了一种全新的软件开发模式和商业模式，也为我国用户摆脱国外商用基础软件的制约提供了一种有效途径，由此带来了一个争论：开源软件比非开源的商用软件更安全更可信吗？本报告就此问题谈三个观点。第一，从经典计算理论与技术的角度讲，“开源软件比非开源的商用软件更安全更可信”（或相反）是伪命题，也就是说这个问题在经典计算理论范畴中没有答案。第二，从经济学和管理学的角度讲，开源软件与非开源的商用软件博弈是保护创新与保护创收的博弈，有充分的实践证明，在网络时代，开源优于非开源。对于我国而言，开源软件带来的安全性好处不是软件客观质量层面上的好处，而是经济学和管理学的好处，即“开源软件相当于国外非开源的商用软件，可以降低软件供应链的安全管理风险”。第三，从发展软件开发新技术的角度讲，支持开源软件及其与非开源软件博弈的技术大有可为。报告结合我们的研究实践，介绍了软件系统的成长性构造与适应性演化的思想，以及软件创作与软件生产紧密耦合的群体化软件开发方法。

报告人简介

王怀民

博士，国防科技大学教授，长江学者，国家杰出青年基金获得者，中国计算机学会会士，计算机学会第十届理事会常务理事，国际开源软件联盟 OW2 理事会主席，入选国家和军队科技领军人才工程、教育部“跨世纪优秀人才培养计划”，首届中创软件人才奖获得者。曾任国家 863 计划信息领域先进计算机主题专家组成员、国家自然科学基金委员会信息领域咨询专家委员会委员。

长期从事分布计算技术与系统研究，主持国家 863 计划、国家 973 计划、国家自然科学基金、国防预研和型号工程等 20 多项科研课题，在大型分布式软件系统成长性构造方法与技术、互联网规模的虚拟计算理论与技术、可信软件大规模协同开发方法和关键技术等方面取得了多项成果。获国家科技进步特等奖 1 项、二等奖 2 项，军队/省/部级自然科学一等奖 1 项、技术发明一等奖 1 项、科技进步一等奖 3 项。发表学术论文 150 余篇。

内构安全的软件开发和运行时环境

武成岗

中国科学院计算技术研究所

内构安全是指在软件的设计和开发过程中，通过某种机制尽可能地减少软件中可被利用的缺陷，从而提升其免疫力，以抵御攻击。2011年 12 月，美国总统行政办公室发布了《可信网络空间：联邦网络安全研究和开发项目的战略计划》，该计划将内构安全作为彻底改变网络安全游戏规则的一个重要主题。

目前，软件行业的现状是，大部分开发人员从未接受过安全训练，即使某些人曾经接受过相关培训，但他们的精力也主要集中在软件本身功能的开发上，很少去关注安全问题，这致使软件产品中的安全缺陷频繁出现。为了使普通软件从业人员能够开发出高安全的软件产品，本团队正在研发内构安全的软件开发和运行时支撑环境，该环境将通过基于知识的缺陷挖掘，把人们在安全实践中的经验融入进来，减少软件产品中的安全缺陷；并通过多角度的完整性以及全方位的随机化，进一步提升软件的免疫力；另外，还将通过知识演进，将新型缺陷特征增添到知识库中，使得本开发环境的安全能力持续进化。报告将介绍当前研究进展、关键技术和所面临的挑战，并对未来的发展趋势进行展望。

报告人简介

武成岗

中国科学院计算技术研究所计算机体系结构国家重点实验室副研究员，博士生导师。从事基于编译技术的软件安全的研究，旨在通过编译技术手段，增强软件的安全性、可靠性、和高效性。他在程序缺陷定位、二进制代码的分析变换及优化、运行时程序行为监测、软件安全免疫等方面，有着较深的技术积累。发表论文近 30 篇，部分发表在 TPDS、TACO、SIGMETRICS、ASE、PACT、CGO、DATE 等学术期刊和会议上，获得授权专利 16 项，软件著作权 5 项，并于 2012 年荣获北京市科学技术二等奖。担任国际学术会议 CGO 2013 大会主席、APPT2013 程序委员会主席，还担任 CGO2015、CCGrid 2015、ICPADS 2014、PPPJ2014、PLDI2012 等会议的程序委员会委员，并在中国计算机学会担任专委工作委员会委员和体系结构专委会常务委员。

武成岗是首个担任编译顶级国际学术会议 CGO 大会主席的国内学者，也是首次应邀参加编译旗舰会议 PLDI 程序委员会的两位国内学者之一。

基于权限机制的安卓软件分析和系统加固研究

杨珉

复旦大学

权限机制是安卓系统采用的资源访问控制模型。安卓系统通过权限机制将各个程序运行在互相隔离的沙箱中，程序需要申请相应的权限才能访问对应的系统资源。这种新型的安全机制为软件行为分析方法和系统的安全框架带来了新的挑战。报告人将立足于安卓平台的权限机制，介绍我们针对安卓软件行为分析和安卓系统安全加固方面的研究进展。针对软件行为分析技术，报告人将介绍一种新型的基于权限使用的分析方法，对程序内部行为以及程序和系统的交互行为进行构建，进而支持软件行为的可视化描述。针对安卓系统访问控制框架的安全威胁和安全需求，在权限泄露问题普遍的现状下，报告人将分析目前权限机制在系统实施过程中存在的缺陷，介绍我们提出的新型权限管理模型，用以解决因应用软件存在安全缺陷导致的多种安全问题。

报告人简介

杨珉

副教授，复旦大学软件学院网络空间安全战略与技术研究工作室执行主任，复旦-斐讯系统安全技术联合研究中心主任。973 首席科学家（青年）。主研方向为系统软件与系统安全，近年在安卓系统安全技术领域取得较大进展，研究成果得到多位国家领导人多次批示，为有关部门提供多次关键技术支撑，得到社会各界的广泛关注。2012 年为新华社《瞭望》封面报道，2013 年、2014 年两度为中央台“3-15 晚会”专题报道，并作为复旦大学近期的三项代表性成果之一为人民日报头版报道。

留校迄今，承担国家、上海市及企业的研究课题 10 余项，总经费 2000 余万，部分成果已实现产业化应用。担任国家自然科学基金、上海市科委和上海市经信委评审专家。在国际顶级学术会议和各类期刊上发表论文 40 余篇，申报国家发明专利 16 项，取得授权 2 项。

程序分析与软件安全

张路

北京大学

程序分析已成为软件安全研究的一个重要手段。从宏观的视角看，程序分析为软件安全的研究提供了一种更细粒度的手段。也就是说，通过程序分析我们可以不再把程序当作黑盒，而是可以进一步深入到程序的内部。然而，程序分析最初并不针对软件安全，这使得许多传统的程序分析技术并不能很好地适应软件安全研究的需要。软件安全的研究通常可以从攻击和防御两个角度展开，而主流的程序分析技术是以编译和软件验证为目标的，更适合防御的研究（即通过程序分析验证不存在漏洞），并不完全适合攻击的研究（即通过程序分析发现漏洞）。虽然已有一些工作利用程序分析发现漏洞，但这些研究基本上是采用特有的分析技术。因此，软件安全领域的研究人员可能有必要与程序分析领域的研究人员密切地合作，针对软件安全的需要系统地研究相应的程序分析技术。

报告人简介

张路

教授，北京大学信息科学技术学院博士生导师，“国家杰出青年科学基金”获得者，主要研究领域为软件工程。2000 年获北京大学计算机软件博士学位，师从杨芙清教授。2000 年 9 月至 2003 年 1 月在英国布鲁斯大学（2000 年 9 月至 2001 年 2 月）和英国利物浦大学（2001 年 4 月至 2003 年 1 月）从事博士后研究。2003 年 2 月回国，加入北京大学信息科学技术学院。曾获 2006 年国家科技进步二等奖（排名第 6）、2009 年北京市科学技术奖技术发明类二等奖（排名第 4）、2010 年 CCF 青年科学家奖，2010 年教育部自然科学一等奖（排名第 3）、2010 年中创软件人才奖，2012 年国家自然科学二等奖（排名第 3）。入选教育部 2008 年度“新世纪优秀人才支持计划”。曾担任国际期刊 Software Testing, Verification and Reliability 和 Journal of Software Maintenance and Evolution: Research and Practice 编委，和 Information and Software Technology (2009)的 Guest Editor，以及包括 ACM International Symposium on the Foundations of Software Engineering、ACM International Symposium on Software Testing and Analysis、International Conference on Automated Software Engineering 、International Conference on Software Maintenance 在内的多个知名软件工程会议的程序委员会委员。研究方向为软件分析与测试、软件维护与演化、程序理解、软件复用以及基于构件的软件开发。已在国内外主要学术期刊和会议上发表论文 100 余篇，其中两篇获得 ACM SIGSOFT 杰出论文奖。

系统安全中的若干科学问题

邹维

中国科学院信息工程研究所

从学术角度，信息安全一般可简单地划分为系统安全与密码学两大分支。密码学有坚实的数学及计算理论基础，所建立的密码系统可证明性强、体系持续时间长。而系统安全与密码学相比，更多呈现的是博弈和对抗。那么，系统安全中有科学问题吗？

本报告阐述系统安全中七个方面的科学问题，并重点介绍系统安全中与软件相关的若干基础性问题，抛砖引玉，与大家共同研讨。

报告人简介

邹维

研究员，现任中国科学院信息工程研究所学术委员会主任、中国计算机学会计算机安全专业委员会常务委员、中国信息协会信息安全专业委员会副主任委员、国家计算机网络与信息安全管理中心学术委员会技术组委员、教育部全国计算机等级考试委员会委员。曾两次获得国家科技进步二等奖、国务院颁发的政府特殊津贴、“新世纪百千万人才工程”北京市级人选称号、中国科学院国内“百人计划”人选、中国计算机学会及北京大学优秀博士论文指导教师。科技部 863 计划/支撑计划、国家基金委自然科学基金、国家发改委信息安全专项、国家保密局科技项目、国家 242 信息安全计划等评审专家。

邹维研究员长期致力于网络与软件安全研究，带领团队在整数溢出漏洞挖掘、模糊测试中穿透校验和（Checksum）检查、漏洞消减、移动终端软件安全检测等方面取得重要突破，运用所研究的技术成功发现 10 多个零日漏洞，获中国国家漏洞库 CNNVD 及美国漏洞管理机构 CVE 收录确认。发表学术论文 50 余篇，研究成果在 TISSEC、JCS、S&P、NDSS、ACSAC、ESORICS 等国际顶级或著名期刊及会议上发表，获得国际同行关注，作为国内首位学者入选信息安全国际顶级会议 S&P2013 程序委员会。

会议记录

会议记录

会议记录