SKLOIS
信息安全国家重点实验室

信息安全国家重点实验室通讯

STATE KEY LABORATORY OF INFORMATION SECURITY

2016年第3期（总第5期）

信息安全国家重点实验室办公室
电话：+86-10-82546611
传真：+86-10-82546564
邮箱：sklois@iie.ac.cn
网站：http://www.sklois.cn

SKLOIS
信息安全国家重点实验室

实验室举办国际会议通知

第十二届信息安全与密码学国际会议通知

由信息安全国家重点实验室（SKLOIS）和中国密码学会（CACR）主办、国际密码协会（IACR）协办的“第十二届信息安全与密码学国际会议”（Inscrypt 2016）将于2016年11月4 - 6日在北京举办。

本次会议涉及网络与操作系统安全、数据库安全、无线网络安全、电子商务、信息隐藏、密码学、可证明安全、多方安全计算与安全协议、物联网安全和云计算安全等20多个主题，会议论文集将在会后由国际著名出版社Springer Verlag正式出版。会议详细信息请参看会网页http://www.inscrypt.cn/ .

第十四届密码学理论国际会议通知

第十四届密码学理论国际会议（Theory of Cryptography Conference，TCC 2016-B ）由国际密码协会（IACR）主办、信息安全国家重点实验室（SKLOIS）承办，将于2016年10月31日至11月3日在北京举办。

TCC是针对密码学理论的国际密码学会领域会议（IACR Area Conference），旨在讨论安全性的规范定义与严格论证，讨论对象包括混淆、密码协议、安全多方计算、对称与非对称密码学系统等。会议详细信息请参见主页http://tcc2016b.sklois.cn/及TCC manifesto：http://www.iacr.org/workshops/tcc/manifesto.html。

第二届国际数字犯罪与取证会议
暨第六届中国计算机取证研讨会通知

由中科院广东软件所、网络空间安全协会、西安交通大学智能网络与网络安全教育部重点实验室、中科院信息安全国家重点实验室和中国电子学会计算机取证专家委员会联合主办的“第二届国际数字犯罪与取证会议暨第六届全国计算机取证技术研讨会”(IWDCF2016 & CCFRW2016)将于2016年12月17日 - 18日在南京举行。

会议涉及犯罪现场成像技术研究；数据雕刻和恢复技术研究；电子文档检测；电子证据分析；用于犯罪侦查的数字图像处理技术研究；小型数字设备取证技术研究；数字信息隐藏和逆向分析检测技术研究；视觉密码、视觉安全及应用技术研究；云取证；移动智能终端取证；大数据取证；互联网取证技术研究等主题。会议论文将经过程序委员会的严格挑选，收录在International Journal of Digital Crime and Forensics (EI检索)。

本次会议将云集世界各国的信息安全、数字取证等领域相关领域专家学者。会议程序委员会主席将由著名数字取证专家Liping Ding、WeiQi Yan和Chang-Tsun Li联合担任，程序委员会将由全世界知名专家30多人组成。诚邀信息安全、数字取证等领域广大研究人员和管理人员踊跃参加。会议详细信息请参见http://www.wikicfp.com/cfp/servlet/event.showcfp?eventid=56756。

目　录

第七届有限域及其应用国际研讨会顺利召开

2016 年 6 月 19 日至 23 日，第七届有限域及其应用国际研讨会在南开大学陈省身研究所顺利召开，该次会议由信息安全国家重点实验室与南开大学联合主办 ,会议主题为有限域理论及其有限域在组合学、通讯理论、密码学、编码理论、组合设计等方面的应用。国内外七十余位专家学者参加了会议。

会议邀请了密码和编码领域多位国际知名的专家学者做了特邀报告。其中 ,IEEE 信息论学会最佳论文奖（1995）得主、法国 ENST 教授 Patrick Sole 介绍了关于 Z_4 码的一些研究；加州大学 Irvine 分校的万大庆教授做了题为《Higher moment subset sums over finite fields》的特邀报告；香港科技大学的丁存生教授做了关于近 50 年来对于 BCH 码的研究的报告；俄克拉荷马大学的程岐教授做了题为《Survey on the Lattice-based cryptography》报告。信息安全国家重点实验室的王明生研究员做了题为《轻量扩散层的构造》的特邀报告，介绍了多种由 MDS 矩阵构造轻量级扩散层的设计方法。

全体参会人员合影

会议还邀请了多位国内外青年学者介绍他们最新的研究成果，信息安全国家重点实验室助理研究员姜宇鹏、庄金成、王安宇分别做了《Affine sub-families of Grain-like structure》、《Classifying and generating exact coset representatives of PGL_2(F_q) in PGL_2(F_{q^2})》和《两类（r,t）局部修复码的构造》的学术报告。

研讨会现场气氛活跃，大会为该领域的学者提供了交流最新研究成果的平台。

实验室举办 2016 年网络空间安全论坛

2016 年 8 月 22 日至 8 月 23 日，信息安全国家重点实验室中国科学院数据与通信保护研究教育中心成功举办了 2016 年网络空间安全论坛。本次会议旨在加强网络空间安全领域的学术交流，进一步开阔学术视野、探索学术前沿、激励学术创新，为全国网络空间安全领域的研究人员和学者提供一个交流平台，分享研究成果，推进在计算机网络安全领域里的先进研究。

会上，汇报人员分别针对自己的研究领域进行讲解，之后展开深度的交流和探讨。内容包含用户密码安全研究、加密云邮件系统的商业价值与关键科学问题、基于口令的跨层密钥协商、端到端通信中的中间盒子、操作系统内核堆区安全监控技术、面向移动设备的云存储数据共享方案、死锁的自动修复技术、拟态网络操作系统等。此次会议在浓郁的学术氛围下圆满结束。

论坛现场

实验室成功举办第十五届国际数字取证和数字水印会议

2016 年 9 月 17 日至 19 日，在中国科学院面向感知中国的新一代信息技术战略性先导专项支持下，由信工所信息安全国家重点实验室主办、中国电子学会多媒体安全专委会协办的“第十五届国际数字取证和数字水印会议”（英文名称：15th International Workshop on Digital-forensics and Watermarking，简称：IWDW 2016）在北京香山饭店召开，来自 10 个国家和地区的 150 余人参加了会议。

中国科学院副院长谭铁牛院士及三名来自数字取证和水印领域的国际著名专家作了精彩的特邀报告。谭铁牛院士以“Digital forensics for network information credibility evaluation”为题，探讨了数字取证技术在网络信息可信性评估的应用前景，为数字取证技术的应用发展开辟了新的方向；韩国高丽大学的 Hyoung Joong Kim 教授以“Future Directions of Reversible Data Hiding”为题，总结了近年来可逆信息隐藏的研究进展，并指出了可逆信息隐藏的未来研究方向，对于信息隐藏方向的相关研究人员十分具有启发性；美国纽约州立大学的 Matthias Kirchner 助理教授以“The Good, the Bad and the Public: Sensor-based Device Identification beyond Media Forensics”为题，介绍了当前基于智能手机传感器数据的多媒体取证技术发展近况，并将传感器数据的应用范围从取证应用扩展到多因素认证，对解决指纹泄露问题具有重要的研究意义；英国华威大学的 Chang-Tsun Li 教授以“Multimedia Forensics: Source Inference from Uncertainty and Enormity”为题，重点介绍了基于设备指纹分析的多媒体取证研究近况，并展示了他们在设备指纹应用的最新研究成果。

中国科学院副院长谭铁牛院士
出席大会并做特邀报告

会议期间，共组织了数字取证、数字水印、可逆数据隐藏、隐写及隐写分析和视觉安全方向的四十五篇论文进行学术报告。会议还邀请了来自北京邮电大学、中科院自动化研究所、北京中科虹霸科技有限公司、智能感知与计算研究中心、杭州电子科技大学、中科院信息工程研究所、北京交通大学及日本冈山大学的八个工业产品展示。在为期三天的会议中，与会者对数字取证和数字隐写领域的前沿和热点问题进行广泛的讨论和交流，学术氛围浓郁。大会为数字取证、水印、隐写、视觉安全的国际间交流提供了一个重要的平台，大力推动了国内外相关方向的研究发展，提高了我国在国际信息安全领域的地位和影响。


数字取证和数字水印领域国际著名专家合影


大会现场

2016 年暑期期间，依托实验室承担的天元基金“促进学科交叉融合平台建设项目——《编码和信息安全中的数学问题》”，实验室联合中国科学技术大学、贵州大学等国内高校成功组织举办了高级研讨班、暑期学校、青年教师培训班、国际会议等系列学术活动，受到了国内科研人员、研究生、博士生的积极关注和参与，取得了良好的效果，进一步提升了实验室的影响力。

天元基金项目
“编码和信息安全中的数学问题”简介

编码学和密码学是现代信息科学的两大核心学科。特别是随着大数据、云计算、物联网等新兴技术的发展，编码与密码已变得与经济社会的发展和人们的日常生活息息相关，其研究更是至关重要。在编码学、密码学的研究中，数学一直发挥着不可或缺的作用，各种代数的、数论的、几何的、组合的工具和方法成为研究编码、密码领域相关问题的基础。另一方面，编码、密码学的研究中也天然地产生了大量数学问题，其中一些问题的研究也推动了数学中某些问题的研究进展，丰富了数学的研究对象。我国在编码、密码及其相关数学理论的交叉研究方面已有数十年的积累，国内目前已形成老中青三代组成的强大研究队伍，并取得了许多有国际影响力的研究成果。此外，国内一些编码、密码数学理论方面的学术活动也在不断增多，规模在不断扩大，国内专家学者与国际上的交流合作也在不断深化和加强。在此背景下，以中国科学院信息工程研究所为依托单位，首都师范大学为合作单位，南开大学为协作单位，共同承担了数学天元基金“促进学科交叉融合平台建设项目”，项目名称为“编码和信息安全中的数学问题”，项目批准号：11526215。

天元基金项目“编码和信息安全中的数学问题”的目标是以京津为中心，面向全国，通过构建一个数学、编码、密码学交流与合作研究平台，组织形式多样的学术活动，促进我国在编码、密码数学理论方面的研究进展，特别是在一些编码、密码领域国际前沿课题的研究进展，提升我国在编码、密码数学理论方向的研究

水平，促进数学与编码、密码学的交叉融合。研究课题主要包括但不局限于：

●密码设计和分析中的数学问题（例如，代数动力系统及序列密码相关问题、密码函数的理论与方法、格的理论、算法和格密码等）

●基于稀疏信息的离散模型与方法（例如，LDPC 码、压缩感知、数字指纹等）

●面向网络环境的编码理论（例如，网络编码、分布式存储编码等）

为探索符合数学特点和发展规律的资助方式，适应数学研究的特殊需求，提升中国数学创新能力，国家自然科学基金委员会于 2014 年开设了数学天元基金“促进学科交叉融合平台建设项目”。此类项目以构建交流平台、合作平台与研究平台为主旨，针对若干数学交叉领域或专题，通过学术活动凝聚国内相关研究队伍，深化国内外多领域科学家紧密合作，促进数学与其他学科、数学各分支间的交叉融合，造就在国际上有影响的学科方向。

第一次编码与密码学高级研讨班在北京香山成功举办

2016 年 7 月 2 日至 8 日，受天元基金资助，由信息安全国家重点实验室主办的“2016 年第一次编码与密码学高级研讨班“ 在北京香山首农会议中心成功举办。来自我国 30 多家科研单位的 50 余位编码密码领域专家和青年学者参加了此次研讨。

此次研讨班由信息安全国家重点实验室胡磊研究员负责组织。研讨班分密码组和编码组平行开展。密码组研讨的主题为“非线性驱动序列和基于非线性驱动序列的序列密码与分组密码的分析”，编码组研讨的主题为“网络存储可修复码和网络编码“与“压缩感知及相关稀疏信息模型“。两个研讨组分别由解放军信息工程大学戚文峰教授和南开大学符方伟教授、首都师范大学葛根年教授负责主持。研讨班的开展形式为由主持人安排或参加人自荐作专题学术报告，提出相关课题的研究背景、国际进展和关键科学问题，进而研讨班参加成员对报告人提出的问题集中讨论，提出解决问题的可能思路、工具和方法。在为期一周的研讨中，报告人认真细致，参加人积极提问，深入探讨。研讨班气氛活跃，场面热烈，收到了良好的研讨效果。

编码与密码学高级研讨班是依托天元基金组织举办的一项特色学术活动，通过邀请国内编码密码领域的顶级专家和近年来活跃的拔尖青年学者集中研讨，集智攻关，旨在促进我国在编码密码领域一些前沿课题的研究中取得突破性进展。此次研讨班研讨的专题也是天元基金项目“ 编码和信息安全中的数学问题“ 研究内容范围中提出的部分专题。

密码组研讨现场

编码组研讨现场

实验室 2016 年“密码学中的序列理论”暑期学校圆满结束

2016 年 7 月 9 日至 7 月 20 日，信息安全国家重点实验室在北京怀柔区中国科学院大学雁栖湖校区国际会议中心举办了“密码学中的序列理论”暑期学校。此次暑期学校以序列密码为主题，主要面向国内高等学校、科研机构和其它单位相关领域的研究生，邀请了包括中国科学院院士在内的国内著名专家学者，开设序列密码专业课程、前沿热点专题讲座，组织挑战性竞赛，旨在拓展学术视野，活跃学术思想，鼓励学术创新和加强学员之间的交流。

本次暑期学校以序列密码的理论基础为主题，讲授和研讨的具体内容包括域上线性递归序列、线性序列的非线性变化、域上非线性递归序列、环上线性递归序列以及序列密码算法的介绍。开办此次暑期学校，对于国内开展此方面研究的科研工作者来说，是一次非常好的学习交流机会。

暑期学校采用了专题课程和讲座相结合的形式。在专题课程中，内容涵盖了序列密码的一系列数学基础理论。在讲座环节，暑期学校邀请到了多位国内外知名的学者做了专题讲座和报告，他们介绍了各自领域内的国际最新进展及其自身的工作。具体的，林东岱研究员介绍了欧洲 e-stream 序列密码工程的主要算法，宏观地阐述了序列密码的发展历程及一些关键问题；孙兵副教授讲授了序列密码入门必学的基础知识——域上线性递归序列，深入浅出地带领学员们进入序列密码研究的大门；胡红钢教授介绍了数论中的 Stickelberger 定理及其在密码学中的应用，展示了数论与密码学间的密切关系；黄民强院士讲授了环上线性递归序列和本原序列的非线性前馈序列等知识，黄院士详尽系统的讲解让学员们学习到如何利用数学作为工具开展密码的研究；戚文峰教授通过基础知识和前沿研究介绍相结合，讲授了钟控序列、带进位反馈移位寄存器序列和非线性移位寄存

论方法，展示了对非线性反馈移位寄存器研究的另一种可能；林志强助理研究员介绍了进位反馈移位寄存器的结构设计，是序列密码理论面向应用的研究；冯秀涛副研究员介绍了 ZUC 算法，ZUC 算法由我国学者自主设计的加密和完整性算法，已经被国际组织 3GPP 选为 LTE 加密标准；王丽萍研究员讲授了环上线性递归序列的综合算法，综合算法是序列密码基础理论中不可或缺的一部分。

本次暑期学校共招收了 78 名学员，他们分别来自复旦大学、南开大学、中国科学技术大学、浙江大学、西安电子科技大学、山东大学、武汉大学、四川大学、湖南大学、西南交通大学、暨南大学、国防科技大学、解放军信息工程大学、中国科学院大学等国内著名高校和研究机构。在为期 11 天的学习中，学员相互交流，共同提高。在暑期学校结束之际，学员纷纷表示这是一次难得的学习机会，收获良多，希望下次还有更多类似的学习活动。

暑期学校全体学员合影

实验室与贵州大学联合举办“密码学与编码学边远地区青年教师培训班”

2016 年 8 月 1 日至 8 月 10 日，由信息安全国家重点实验室主办、贵州大学密码学与数据安全研究生承办的“密码学与编码学边远地区青年教师培训班”在贵州大学博学楼成功举办。来自我国西南、西北等边远地区高校的 80 余位青年教师参加了此次培训。

此次培训班邀请到清华大学冯克勤教授、北京大学冯荣权教授以及信息工程研究所林东岱研究员、胡磊研究员为学员授课，讲授内容包括我国编码密码学发展综述、有限域及其应用、密码学基础、数论基础等。培训班的目的是通过专家讲授编码密码基础理论及其相关数学基础方面的知识、方法，促进我国编码密码研究相对薄弱的边远地区的高校教师加深对编码密码学的认识和理解，增进其相互间的交流与合作，进一步提高我国边远地区密码学和编码学的研究深度和教学水平。在为期 10 天的培训中，学员们认真听课，并积极与授课专家讨论、交流，取得了良好的效果。培训班受到了学员们的一致好评，结课仪式上，许多学员表达了对再次参加此类学术活动的期待。

此次培训班受到了信息工程研究所承担的国家自然科学基金天元基金促进学科交叉融合平台建设项目“编码和信息安全中的数学问题”的大力支持。该项目是国家自然科学基金委天元基金开设的一类专项基金，旨在通过资助举办形式多样的学术活动，促进数学与其它学科的交叉融合。2016 年全国仅有 12 家单位获得了此类项目资助。信息工程研究所作为项目承担单位之一，目前已组织举办多次学术活动，以促进数学与信息科学的两大重要分支—编码学和密码学的交叉融合。此次边远地区青年教师培训班是依托该项目举办的一项特色学术活动，旨在推进我国边远地区编码密码研究水平的提升和研究队伍的壮大，促进我国数学与编码密码学科发展在地域上的合理布局。

培训班现场

实验室与中国科大联合举办“2016 编码密码中的数学基础暑期班”

2016 年 7 月 17 日 -29 日，由中国科学技术大学数学科学学院和信息安全国家重点实验室联合组织的“2016 编码密码中的数学基础暑期班”在中国科大数学科学学院成功举办。本次暑期班共邀请到清华大学冯克勤教授、新加坡南洋理工大学邢朝平教授、美国特拉华大学向青教授、北京大学冯荣权教授、苏州大学殷剑兴教授五位国内外编码、密码及相关数学基础领域的资深专家为学员授课，并邀请到中国科学技术大学张先得教授在暑期班期间作学术报告。来自全国 30 多家单位的 80 余名研究生、博士生、青年学者参加了暑期班。

编码、密码是现代信息科学的两大核心学科，其研究与数学密不可分，数学中代数、数论、几何、组合等领域的工具、方法是研究编码、密码学的基础。本次暑期班，授课专家和报告专家由浅入深、循序渐进地系统介绍了指数和、代数数域、代数函数域、差集、置换多项式等数学工具及其在编码密码中的应用，对提高研究生和青年学者的知识水平、提升其科研能力起到了很好的推动作用，受到了学员们的一致好评。

冯克勤教授为学员授课

冯荣权教授为学员授课

暑期学校全体人员合影

实验室举办第三届中韩编码理论及相关领域国际会议

会议程序委员会主席冯克勤教授讲话

实验室主任林东岱研究员讲话

2016 年 8 月 12 日至 16 日，由信息安全国家重点实验室和韩国西江大学（Sogang University）联合组织的“第三届中韩编码理论及相关领域国际学术会议 (The 3rd Sino-Korea International Conference on Coding Theory and Related Topics)”在北京首农香山会议中心召开。来自韩国、日本、新加坡、美国等地的 14 位邀请专家和来自国内 20 余家单位的 50 余位代表参加了会议。

会议程序委员会主席由清华大学冯克勤教授担任，组织委员会主席由北京大学冯荣权教授和韩国西江大学 Jon-Lark Kim 教授担任。会议共邀请到国内外 23 位专家作大会特邀报告，议题涉及线性码理论、序列设计、秘密共享、代数组合、代数图论等编码密码及相关数学理论领域的多个前沿方向。在为期五天的会议中，参会代表与邀请报告专家进行了热烈讨论和深入交流。

中韩编码理论及相关领域国际学术会议是我国发起的编码及相关领域的专业性小型国际会议，通过我国高校或科研院所与韩国高校联合组织，邀请国际上编码及相关领域的专家做大会报告，共同研讨该领域国际上的前沿研究课题。此次会议的召开，为我国从事编码密码理论及相关领域研究的科研人员提供了良好的研讨交流机会，能够有力地推动该领域的研究进展。

认识隐写术与隐写分析技术

（关晴骁 ,赵增振）

隐写术（Steganography）是一种将信息隐藏至数字媒体文件中的技术，该技术对数字媒体文件的内容数据进行少量的修改，从而可以将任意的计算机文件或信息嵌入到媒体文件内容的数据中，同时不改变该媒体文件的格式信息、视觉外观、媒体可理解的内容等因素，具有不可见性。因此，隐写术是一种可对信息进行伪装的信息隐藏技术。

隐写术与传统的加密方法相比，具有较大的差别。加密方法能够保证信息的内容不被别人破解获取。而隐写术使用公开媒体文件传输隐秘信息，对外表现为媒体文件的特性，不会引起第三方的怀疑，从而降低了秘密信息被发觉并被获取的可能性。值得一提的是，隐写术与加密技术是并存关系，传输者可使用任意加密方法将信息加密后嵌入至媒体文件，而接收者收到载体后先从媒体中提取密文，然后解密得到明文。

在隐写术中所采用的主流媒体文件包括数字图像、音频、视频等。其中数字图像作为在各大网站、社交平台等的主要组成部分，作为嵌入秘密信息的载体文件具有较高的隐蔽性。而数字视频因其具有较高的嵌入容量作为载体文件同样具有非常好的效果。然而数字媒体在被用来进行传递信息的同时也被不法分子及敌对势力所利用。例如在美国被捕获的俄罗斯间谍安娜查普曼，就是采用隐写术将情报信息隐藏在图像中，并发布在俄罗斯的某社交网站，以此来传递情报信息。

按照隐写术的发展历程可以将其分为传统隐写术和自适应隐写术。传统隐写术主要目的在于通过高效率的编码方案在对媒体文件修改点一定的条件下，将尽可能多的秘密信息隐藏到载体文件中。而自适应隐写术目的在于在保证隐写嵌入效率的同时，将嵌入秘密信息对载体的扰动集中到对载体影响较小的位置，从而使得载体文件嵌入信息后更不易被第三方所察觉。例如 JPEG 域图像自适应隐写算法 J-UNIWARD 和 STCs 的组合则是将秘密信息嵌入到图像的纹理区域，从而极大地保证了隐写后图像的安全性。

图：JPEG 域图像自适应隐写算法应用实例，从上到下依次为
原始图像、嵌入后图像、嵌入对图像最低比特位改动分布图

为应对隐写术被不法分子及敌对势力所利用带来的危害 ,隐写分析（Steganalysis）应运而生。另一方面，进行隐写术的研究也依赖于隐写分析方法对其进行安全性验证，因此不少的研究机构都在开展相应的工作。目前隐写分析技术主要包括 3 类：感官检测法、标识特征检测法、统计检测法。其中统计检测法又分为特定隐写检测和通用盲检测。而随着自适应隐写术的进步，感官检测法及标识特征检测法均无法满足隐写分析的要求，基于高维度特征的通用盲隐写分析技术成为如今的主流。其中空域图像隐写分析富模型 Rich Model 已经达到 3 万维以上，对分类器同样是一种挑战。

关于隐写术与隐写分析技术的博弈在时刻进行中。

首届网络空间战略论坛暨中国信息安全网上线发布会举行

（2016 年 08 月 29 日 文章来源：人民网）

2016 年 8 月 27 日，由国家军民融合委员会、中国互联网发展基金会和中国信息安全测评中心联合指导《中国信息安全》杂志社和北京华夏文化交流促进会联合主办的“首届网络空间战略论坛暨中国信息安全网上线仪式”（以下简称“会议”）在国际关系学院召开。会议以“聚焦网络空间军民融合”为主旨，坚持“自主可控”导向，从产学研等多个视角展开了深入的交流探讨。来自军队、政府部门、科研院所、网络安全企业、新闻媒体的 300 余位嘉宾到场参会。

会议在《网络空间战略之歌》中开场。国防大学副校长毕京京中将、中国互联网发展基金会马利理事长、中国信息安全测评中心朱胜涛主任、国际关系学院刘慧党委书记、《中国信息安全》杂志社徐平社长发表致辞。

会议有四项主要议程：“中国信息安全网上线仪式”、“网络空间战略论坛年度人物颁奖仪式”、“网络中国 繁荣世界高端对话”，以及“网络空间军民融合主题演讲”。

徐平社长主持“中国信息安全网上线仪式”。中国信息安全网紧紧围绕网络强国、大数据战略和“互联网 +”行动，力求从事件驱动、责任驱动向文化驱动转化，持续提升网络空间生产力、文化力、国防力，旨在为各级主管部门提供决策支撑平台，为网络安全和信息化产业提供媒体传播平台，为广大学者专家提供交流互动平台。

“网络空间战略论坛年度人物颁奖仪式”中，毕京京中将、魏正耀院士、马利理事长、龙永图先生、郝叶力少将、冯燕春少将、蒋亚民少将、朱胜涛主任、徐平社长、刘慧党委书记作为颁奖嘉宾，向安卫平、叶征、吴世忠、马民虎、王世伟、程琳、肖新光、秦安、张乐天、谈剑峰等十位对“网络空间战略论坛”做出突出贡献的人物颁发荣誉证书和奖杯。来自《中国信息安全》杂志社的彭琳和来自互联网发展基金会的张佑任担当主持。

“网络中国 繁荣世界高端对话”由“网络空间战略论坛”主编秦安主持，龙永图、刘慧、安卫平、富彦斌、肖新光、张文木参与对话并分别作为“从睁开眼睛看世界到睁大眼睛看网络”的中国视野、“以前瞻性发展，和平共赢走出去”的中国方案、“以忠诚铸就网络国防，以实力维护网络繁荣”的中国力量、“网络化和国际化双轮驱动，中国创新与世界同步”的中国格局、“铸造威胁检测中国引擎，坚持开放博弈网络强国”的中国产业和“国家战略事关国家兴衰，大数据话语决定网络强国”的中国战略，表述了“网络中国、繁荣世界”的总体构想和实现路径。

“网络空间军民融合主题演讲”环节，北部战区副参谋长安卫平、上海金盾云计算有限公司董事长唐荣喜、军事科学院军队建设研究部国防综合研究室主任于川信、成都立鑫新技术科技有限公司总裁王汝君、中国科学院信息安全国家重点实验室教授翟起滨、成都科来软件有限公司联合创始人游浣权、中国信息安全测评中心总工王军、898 创新空间董事长兼总裁李建新、国防科技大学国际问题研究中心研究员杜雁芸、中国科学技术大学副教授张卫明、战略支援部队某部队主任张乐天、空军工程大学信息导航学院原院长吴耀光、中国工程院院士倪光南、安天创始人肖新光、北京航空航天大学战略问题研究中心教授张文木，分别从军事理论、信息产业、工程技术方面对网络空间安全发展、数字资产安全保护、网信领域军民融合等话题做了精彩发言，从各自研究领域深入阐述了对“网络空间军民融合”主题的观点，明晰网络空间军民融合的决心、恒心、重心，增强全天候全方位网络安全态势感知、整体防御和综合威慑能力，加速推动我国从网络大国走向网络强国。

具有网络空间军民融合潜力的北京卫达科技、上海金盾云计算、成都立鑫新技术、成都科来软件特别赞助本次大会，威客安全、安天、山石网科、四叶草安全、898 创新空间、十月天传媒等企业协助支持。

网络间谍组织 Buckeye 将攻击目标转至中国香港

（2016 年 9 月 18 日 文章来源：赛门铁克）

Buckeye 网络间谍组织正将数家中国香港机构作为攻击目标，Buckeye 网络间谍组织又被称为 APT3、Gothic Panda、UPS Team 和 TG-0110，该组织已经成立超过五年，并主要针对美国及其他目标国家的企业组织开展攻击行动。但自 2015 年 6 月起，Buckeye 似乎逐渐将攻击重点转向中国香港的政府机构。2016 年 3 月至今，该组织集中针对中国香港的相关机构进行恶意攻击。最近一次攻击发生在 8 月 4 日，Buckeye 犯罪组织企图通过发送恶意电子邮件至被入侵的目标网络，以实现盗取信息的目的。

通过赛门铁克与 Blue Coat Systems 的联合威胁情报服务，赛门铁克的安全团队清晰掌握了 Buckeye 组织在近几年的策略演变。这一发现能够帮助赛门铁克进一步增强安全防护功能，并帮助企业用户抵御该组织的攻击活动。

背景

在 2009 年，赛门铁克已发现 Buckeye 针对多个地区的多家机构展开攻击。Buckeye 曾通过远程访问木马 (Backdoor.Pirpi) 对一家美国机构的网络展开攻击。该犯罪组织通过附带 Backdoor.Pirpi 或链接的鱼叉式网络钓鱼电子邮件对目标进行攻击。如今，赛门铁克已经识别出该组织所使用的其他黑客工具。

过去，Buckeye 组织因利用零日漏洞进行攻击而臭名昭著，包括在 2010 年攻击中使用的 CVE-2010-3962 和在 2014 年使用的 CVE-2014-1776。尽管 Buckeye 利用其他零日漏洞进行的攻击也被发现，但这些攻击活动并未得到赛门铁克的证实。赛门铁克安全人员表示，所有已知的或疑似被 Buckeye 组织利用的零日漏洞均来自 Internet Explorer 和 Flash。

攻击重心转变

2015 年 8 月起，赛门铁克遥测技术发现中国香港的部分计算机感染 Backdoor.Pirpi。2016 年 3 月底至 4 月初，该恶意程序的感染数量出现大幅增长。不仅如此，赛门铁克同样在其他调查中发现与该恶意程序相关的恶意软件样本，并从而确定该犯罪组织的攻击目标为中国香港的政府机构。

在近期的部分攻击中，Buckeye 使用带有恶意压缩附件 (.zip) 的鱼叉式网络钓鱼电子邮件，这些电子邮件的压缩文档附件中包含带有 Microsoft Internet Explorer 标识的 Windows 快捷方式 (.lnk) 文件。受害者一旦点击该快捷方式，计算机将会下载 Backdoor.Pirpi 恶意程序，并在受感染的计算机中执行。

攻击目标

从 2015 年至今，赛门铁克发现在不同地区的大约 82 家组织机构的网络中发现 Buckeye 工具，但该现象无法准确反映出 Buckeye 攻击组织所感兴趣的攻击目标。赛门铁克认为，该组织通过采取“广撒网”的方式寻找攻击目标，但只在感兴趣的企业机构网络中保持攻击活跃度。通过设定监测指标和深入观察，例如：Buckeye 对某机构保持攻击活跃度超过 1 天、部署额外工具，针对多台计算机进行病毒传播等，赛门铁克发现 Buckeye 的攻击目标主要针对中国香港 (13)、美国 (3) 和英国 (1) 的 17 家组织机构。

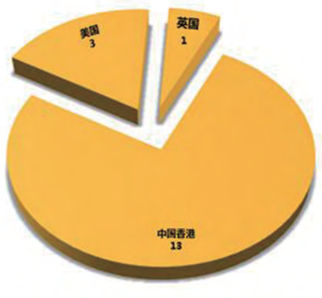


图 1. Buckeye 感兴趣的攻击对象地区分布（2015 年至今）

赛门铁克的监测数据从 2015 年开始统计，但值得注意的是，在 2016 年 3 月，针对中国香港的攻击比例出现大幅增长。2015 年中期之前，Buckeye 的传统攻击目标主要为不同类型的美国和英国组织机构。而在 2015 年 6 月，Buckeye 的攻击目标发生巨大转变，开始攻击中国香港，并逐渐停止对英国和美国的攻击。

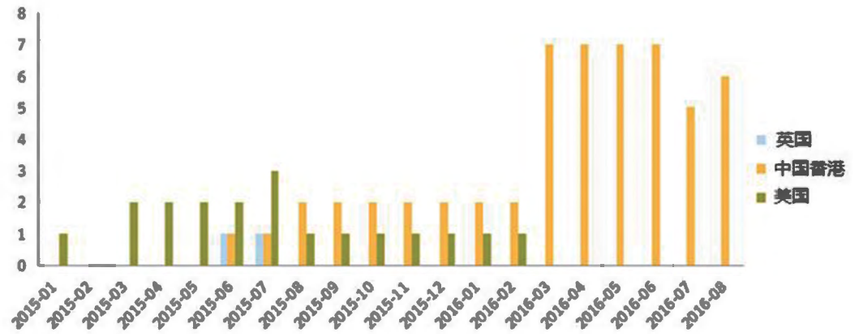


图 2. 在不同时期及不同地区中，Buckeye 攻击目标分布图

恶意软件和黑客工具

Buckeye 攻击组织采用多种黑客工具和恶意软件进行攻击，其中，许多黑客工具为开源应用。此外，为了躲避检测，Buckeye 对这些工具还进行了一定程度的修补或调整。

Buckeye 通过使用远程访问木马 Backdoor.Pirpi，来读取、写入和执行文件与程序，以及收集攻击目标的本地网络信息，包括域控制器和工作站等。

Buckeye 所采用的黑客工具包括：

Keylogger：Keylogger（键盘记录器）可通过使用命令行参数网络服务、替换、安装、注销进行配置。这些参数可以作为服务被安装，然后 Keylogger 开始记录如 thumbcach_96.dbx 等加密文件的击键次数。该工具将记录如 thumbcach_96.dbx 等加密文件的键盘输入信息。此外，Keylogger 还能够收集 MAC 地址、IP 地址、WINS、DHCP 服务器和网关等网络信息。

RemoteCMD：RemoteCMD 工具类似于 PsExec 工具，主要用于在远程计算机上执行命令。用法为：%s shareIp domain [USER INFORMATION|[USER NAME AND PASSWORD]] [/run:[COMMAND]]，能够传递的命令包括上传、下载、服务（创建、删除、开始、停止）、删除、重命名和 AT。

PwDumpVariant：RemoteCMD 工具可以导入 lsremora.dll（通常攻击者将其作为工具箱的一部分一同下载），并使用 GetHash 导出 DLL 文件。该工具可在执行过程中，将自身注入到 lsass.exe 中，并通过参数 “dig” 触发。

OSinfo：OSInfo 是一种通用系统信息收集工具。它具有丰富的命令行参数帮助指令

ChromePass：一种来自 NirSoft 的工具，可用于恢复保存在 Chrome 浏览器中的密码。

Lazagne：一种编译的 Python 工具，可从安装在本地的多个应用类别中提取密码，例如，Web 浏览器。这些应用类别包括：聊天、Svn（一种版本管理工具）、无线网络、电子邮件、Windows、数据库、系统管理和浏览器。

Buckeye 似乎将文件和打印服务器作为主要攻击目标，因此，赛门铁克认为该组织的目的很有可能是盗取文件。结合该组织在过去利用的零日漏洞、定制工具以及攻击目标的组织类型等因素，这表明 Buckeye 是一家拥有国家支持背景的网络间谍组织。

操晓春研究员赴美国参加 IEEE(CVPR)2016 国际会议

2016 年 6 月 25 日至 7 月 2 日，实验室操晓春研究员赴美国参加 IEEE 国际计算机视觉与模式识别会议。

国际计算机视觉与模式识别会议（CVPR）是 IEEE 一年一度的学术性会议，是世界顶级的计算机视觉会议。CVPR 有着较为严苛的录用标准，会议整体的录取率通常不超过 30%，而口头报告的论文比例更是不高于 5%。在各种学术会议统计中，CVPR 被认为有着很强的影响力和很高的排名。目前在中国计算机学会推荐国际学术会议的排名中，CVPR 为人工智能领域的 A 类会议。

此次会议的主要内容是计算机视觉与模式识别技术。深度卷积神经网络已经被广泛应用于图像内容理解等相关研究方向，并且取得了令人满意的实验结果。操晓春研究员发表的论文通过利用深度卷积神经网络对轮廓图像与真实图像之间的共享潜在结构进行挖掘，从而提高轮廓图像特征表达的判别性和鲁棒性。为了达到上述目的，构建训练数据三元组，该三元组由轮廓图像、同类别真实图像和不同类别真实图像构成。会议期间，操晓春研究员对该项技术及课题组近年来取得的一系列的研究成果进行了介绍，并同与会专家进行了深入交流。

陈恺研究员应邀访问新加坡管理大学

2016 年 7 月，应新加坡管理大学（Singapore Management University，SMU）信息系统学院（School of Information Systems）的邀请，实验室陈恺研究员赴新加坡进行学术交流。陈恺研究员与 SMU 多位老师在移动平台恶意代码检测等方面准备开始进行实质性合作并建立良好的合作关系。

访问期间，陈恺研究员介绍了实验室概况和课题组近年来取得的系列成果，包括安卓恶意代码检测（发表于 USENIX Security 2015）和苹果恶意代码的检测（发表于 IEEE S&P2016）等。随后，双方就软件安全分析等方面的合作研究展开了深入讨论。以上研究内容是国家自然科学基金等项目的重要组成部分，后续将会进一步改进现有方案和原型系统，力求取得世界一流的研究成果。

此外，双方还就中新研究生联合培养、科研选题、论文发表等问题进行了深入交流。

王安宇助理研究员参加 ISIT 2016 国际会议

2016 年 7 月 10 日至 15 日，实验室王安宇助理研究员参加了在西班牙巴塞罗那举行的 2016 年信息论国际研讨会（2016 IEEE International Symposium on Information Theory，简称 ISIT 2016）。ISIT 是通信领域重要国际会议，每年举办一次。本次会议由美国电子电气工程师协会（IEEE）主办，西班牙朋培法普拉大学协办。会议的主题是信息理论相关方向的最新研究进展。

实验室文章《Two Classes of (r,t)-Locally Repairable Codes》被本次会议接收。该文给出了两种具有可并行性质的局部修复码的新构造，其中一种构造突破了已知最高的信息率，而另一种构造能够达到很高的节点可用性。会议期间，王安宇对实验室近年来在分布式存储领域取得的成果进行了介绍，并与信息论研究领域的国际著名学者 P. V. Kumar 和 A. Barg 等进行了深入的讨论交流。

王安宇助理研究员和与会专家交流讨论

实验室林东岱研究员、胡磊研究员、陈恺研究员参加“贵州省科协第 41 期学术讲坛—大数据安全与隐私保护”并做特邀报告

2016 年 8 月 4 日，由贵州省科学技术协会主办，贵州大学密码学与数据安全研究所、贵州省计算机学会、贵州省公共大数据重点实验室承办，蓝盾信息安全技术股份有限公司、北京安码科技有限公司协办的“贵州省科协第 41 期学术讲坛—大数据安全与隐私保护”在贵州大学北校区召开。130 余名国内专家教授、研究学者、企业精英、工程技术人员和在校研究生参加了会议，共同探讨大数据隐私与安全领域最新研究进展和发展趋势。实验室林东岱研究员、胡磊研究员、陈恺研究员受邀参会并作大会特邀报告。

林东岱研究员在会上作了题为《海云环境下的信息安全》的报告，阐释了对安全和隐私的独到见解，进而介绍了面向感知中国的新一代信息技术—海云安全体系架构和关键技术，以及信息安全国家重点实验室在这方面所做的工作；胡磊研究员作了题为《密码学中的随机数问题与破解分析》，介绍了在现代密码学中有重要应用的随机数生成问题与破解分析，并介绍了其在信息保护与信息获取中的应用；陈恺研究员作了题为《大数据时代下的软件安全》的报告，介绍了其研究团队在大数据环境下软件漏洞分析及恶意软件发掘方面所做的工作。

会后，三位研究员还与参会代表进行了深入研讨和交流，贵州省公共大数据重点实验室常务副主任彭长根教授等专家也表达了今后与实验室在大数据安全和隐私保护方面开展科学研究、人才培养等方面合作的意愿。

1 2
3

1、林东岱研究员作题为《海云环境下的信息安全》的特邀报告

2、胡磊研究员作题为《密码学中的随机数问题与破解分析》的特邀报告

3、陈恺研究员作题为《大数据时代下的软件安全》的特邀报告

实验室博士生常冰赴新加坡管理大学交流访问

2015 年 8 月至 2016 年 8 月，应新加坡管理大学李迎九（Yingjiu Li）教授的邀请，实验室博士生常冰同学赴新加坡管理大学信息系统学院进行了为期一年的交流访问。

李迎九教授是新加坡管理大学信息系统学院副教授，主要研究方向为 RFID 安全，移动系统安全，应用密码学与云安全。李迎九老师与实验室保持着良好的学术交流联系，开展了派遣交流学生、提供博士后岗位、合作研究等多种形式的交流。

常冰同学的研究方向是移动安全，目前专注于移动设备上可否认加密系统的研究。在访问期间，常冰同学与李迎九教授及实验室人员进行了广泛的交流与合作，取得了一系列研究进展。首先，在之前发表在 ACSAC’15 的文章的基础上，对方案进行了改进，引入了 NFC 技术，增强了系统的可否认性与可用性；其次，还提出了一种全新的可否认加密系统，这种系统可以抵御更强的可对磁盘进行多次快照的敌手，用户还可以在不同的加密模式之间进行快速切换，这些都是原有系统不具备的特性；再次，还对智能手表对口令认证系统的影响做了深入的研究，提出了一种利用智能手表来加强口令认证系统安全性的方案。

实验室博士生常冰

法国巴黎八大 Sihem Mesnager 教授访问实验室

2016 年 9 月 12 日至 9 月 16 日，应信息安全国家重点实验室邀请，法国巴黎八大 Sihem Mesnager 教授来实验室进行学术访问和交流。

来访期间，Sihem Mesnager 教授作了题为《Bent Functions: Algebraic constructions from the Desarguesian spread》、《Codes from Boolean Functions》和《Optimal LRC Codes From Good Polynomials over Finite Fields》的三个学术报告，分别介绍了基于有限几何的 Bent 函数的构造，基于布尔函数的良好线性码的构造，以及基于有限域上一些“好”多项式的 LRC 码的构造。Mesnager 教授的报告深入浅出地介绍了 Bent 函数、线性码和 LRC 码的相关研究背景及其本人的相关突破性工作，吸引了实验室多名成员以及来自清华大学、中科院数学院等多家兄弟单位科研人员、研究生的参加，引起了听众浓厚的兴趣和热烈的讨论。

访问期间，Mesnager 教授与实验室科研人员就密码函数、线性码等方面的相关问题进行了深入交流，并探讨了双方进一步研究中可以开展合作的研究课题。

Sihem Mesnager 教授在实验室作报告

刘偲（副研究员，硕士生导师）

刘偲，女，信息安全国家重点实验室副研究员，硕士生导师。2012 年于中国科学院自动化研究所获得博士学位。2009 年至 2014 年赴新加坡国立大学从事研究助理以及博士后研究工作。2014 年 12 月至今在中国科学院信息工程研究所信息安全国家重点实验室从事科研工作。主要研究方向为机器学习、多媒体及计算机视觉。目前已发表 40 多篇学术论文，其中，多数学术成果发表于：TPAMI、IJCV、IEEE TIP、IEEE TMM、IEEE TCSVT 等国际权威期刊，以及 ICCV、CVPR、ECCV、ACM MM、AAAI 等国际顶级会议上。2012 年获得ACM多媒体大会(ACM MM)最佳技术展示奖，2013年荣获ACM多媒体大会(ACM MM)最佳论文奖。

代表性成果主要包括：

首次在计算机视觉和多媒体领域提出了并部分解决了服饰识别的课题(发表于CVPR 2012 ,接受率2.5%)，提出了一套服饰推荐和妆容推荐的框架（获得 ACM MM 2012 最佳技术展示奖，ACM MM 2013 最佳论文奖）。深入研究了人像解析课题，获得了世界最高的性能（发表于 TPAMI 2015，CVPR 2016, ICCV 2015, ACM MM 2014, TMM 2015 等 ），相关论文引用次数超过 2000。

刘美成（副研究员 ,硕士生导师）

刘美成，男，信息安全国家重点实验室副研究员，硕士生导师。2013 年于信息安全国家重点实验室获博士学位。主要从事密码函数、代数攻击、对称密码组件设计与算法分析的研究，在 IEEE Transaction on Information Theory、Discrete Applied Mathematics 和 CRYPTO、EUROCRYPT、ASIACRYPT、FSE 等著名期刊和会议发表论文 20 余篇，曾获中国科学院院长优秀奖和中国科学院优秀博士学位论文奖，主持国家自然科学基金 2 项。

代表性成果主要包括：

给出了布尔函数抵抗快速代数攻击的免疫性上确界 ,解决了自 2003 年快速代数攻击提出以来的未决难题。证明了 Carlet-Feng 函数具有最优快速代数免疫性 ,解决了 Carlet 和 Feng 在 ASIACRYPT 2008 提出的猜想。给出了对称布尔函数的分解表达式，并发现几乎所有的对称布尔函数具有较差的快速攻击免疫性，包括具有高代数免疫度的对称布尔函数，因而对称布尔函数不适用于流密码。首次解决了 Keccak 团队提出的 3 轮和 4 轮原像挑战。

荣誉

实验室李凤华、操晓春研究员“百人计划”终期评估结果为优秀

近日，根据《中国科学院人事局关于公布 2012 年度“百人计划”入选者终期评估结果的通知》（科发人函字〔2016〕53 号），实验室李凤华、操晓春研究员考核结果为优秀。

李凤华研究员，2012 年获得中国科学院“百人计划”择优资助。在百人计划执行期间，获得国家自然基金、国家 863 计划等 10 余项科研项目资助；出版学术专著 1 部，在 IEEE TIFS、中国科学等国内外期刊或会议上发表学术论文 53 篇，其中 SCI 检索 9 篇、EI 检索 41 篇 ,申请国家发明专利 12 项；获得省部级科技进步（或技术发明）一等奖 3 项（第 1、2、3 完成人）、三等奖 1 项（第 1 完成人）。

操晓春研究员，2012 年获得中国科学院“百人计划”择优资助。期间获得了中组部万人计划青年拔尖人才计划和国家自然科学基金优秀青年基金等支持，担任 CCF-A 类期刊编委，英国工程技术学会会士，曾兼任网络空间大数据协会筹备组组长、曾兼任网络多媒体北京市重点实验室学术委员会委员。

喜报

为庆祝中国共产党成立九十五周年，深入落实“十八大”精神，中国科学院京区党委和中国科学院信息工程研究所党委组织了“两优一先”评选、表彰活动。信息安全国家重点实验室多个党组织、多名党员获得表彰。

实验室多个党组织获先进基层党组织荣誉称号。其中，第三研究室党总支获得“中国科学院 2016 年度先进基层党组织”荣誉称号；第一党总支第三支部、第三党总支第二支部获得“中国科学院信息工程研究所 2015 年度先进党支部”荣誉称号。

活动还表彰了在科技创新工作中涌现出的优秀共产党员、优秀党务工作者，实验室吕克伟、寇春静、刘淼、戴琦、韩言妮等多名党员获得表彰。

信息安全国家重点实验室将以改革创新精神全面加强党建工作，进一步推进“两学一做”学习教育，号召广大党员立足岗位做贡献，为实施所“一三五”规划、实现“四个率先”而努力奋斗！

实验室第三研究室党总支获
“中国科学院先进党组织”荣誉称号

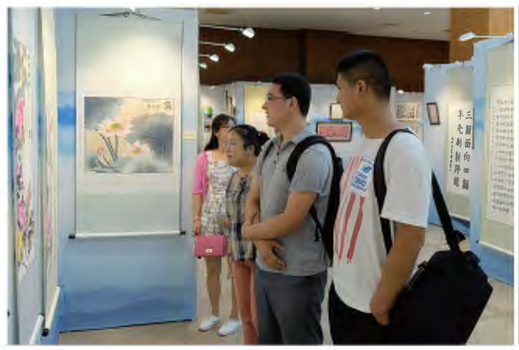
“中国科学院信息工程研究所 2015 年度
先进党支部”获奖单位代表领奖

第一研究室参观中国科学院京区职工纪念建党 95 周年书法、绘画、篆刻、摄影和微电影展

2016 年 7 月 11 日，第一研究室团支部组织青年职工和学生到中科院文献情报中心参观了中国科学院京区职工纪念建党 95 周年书法、绘画、篆刻、摄影和微电影展。

展览以“报党恩、科学情、创新美”为主题，主要体现建党 95 周年以来中国共产党团结带领全国各族人民进行革命、建设、改革的伟大历程和丰功伟绩，中科院建院以来优良的院风院训，知识创新工程和率先行动计划实施以来取得的丰硕成果等内容。参展作品主题鲜明、思想深刻、构思独特，体现了时代精神，讴歌了新中国建设的辉煌成就，弘扬了科学创新精神。活动结束后，参加人员撰写了参观心得并做了交流和分享。

本次活动激发了青年职工和学生的爱党、爱国、爱院情怀，增强了凝聚力、和战斗力。相信在以后的工作和学习中，大家将以实际行动践行，牢记使命、努力奋斗，为建设世界科技强国贡献力量。



展览现场

部分活动参加人员合影

第一研究室开启京郊“红色之旅”

2016 年 8 月 12 日，第一研究室组织了京郊“红色之旅”活动。活动主要分为两个部分：参观平西抗日战争纪念馆和十渡东湖港拓展培训。

平西抗日战争纪念馆展出的是以平西抗战史料为主要内容的抗战历史长廊。抗日战争时期，中共中央北方局和八路军总部在这里开辟了平西抗日根据地，涌现了许多可歌可泣的英雄人物和动人事迹。许多图片和文物都是第一次与观众见面，从不同侧面、多个角度介绍了全国抗战形势和晋察冀抗日根据地的创建过程，反映了创建和巩固平西抗日根据地的全过程。在 8 月 15 日日本无条件投降 71 周年纪念日前夕组织此次活动具有特别的意义。参加活动的职工党员、群众都接受了一次生动的爱党、爱国教育：铭记历史，警钟长鸣；珍惜现在，共筑未来。

参观平西抗日战争纪念馆

部分活动参与人员合影

《信息安全国家重点实验室通讯》征稿启事

为推进实验室科研工作，营造浓郁的学术氛围，加强实验室文化建设，为广大职工、学生提供一个展示自身才华的舞台，在实验室领导的指导和大力支持下，在全体职工、学生的积极配合和参与下《信息安全国家重点实验室通讯》于 2015 年 11 月正式和大家见面了。现实验室面向全体职工、学生征稿，具体信息如下：

征稿内容需与实验室建设相关或展现实验室职工、学生风采（比如实验室要闻、科研进展、交流与合作、荣誉、文化生活等）；此外，近期行业快讯、科普文章、学术研究成果、战略研究报告、综述文章等相关稿件均可。

稿件要求信息真实、可靠；图文并茂；一般不超过 1000 字。

投稿请发送邮件至 sklois@iie.ac.cn，邮件主题请注明“实验室通讯投稿”。本征稿启事常年有效。

望大家踊跃投稿，拿起笔，描绘事业的点和线，抒写生活的酸与甜，在实验室科研、学习的征途中留下坚实而清晰的足印！

信息安全国家重点实验室办公室

2016 年 1 月