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

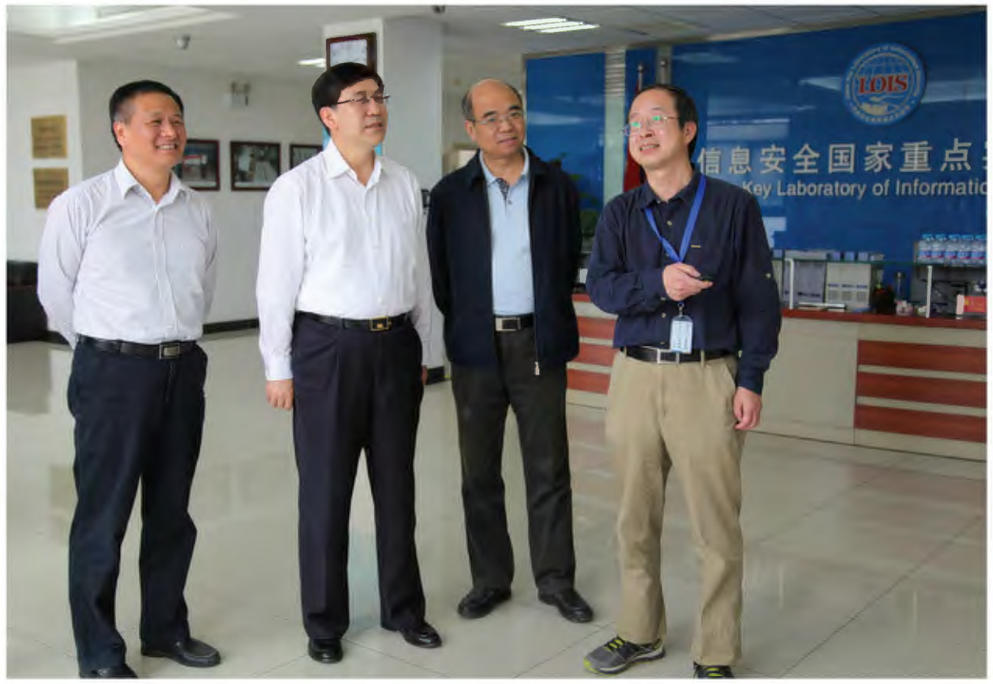
STATE KEY LABORATORY OF INFORMATION SECURITY

2016年第2期（总第4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

领导关怀



科学技术部副部长、党组成员阴和俊视察实验室
（左一：保密局局长田静；左二：阴和俊；右二：中科院副院长相里斌）

中科院党组副书记、副院长刘伟平视察实验室

目　录

实验室要闻

中科院党组副书记、副院长刘伟平视察实验室 ……1
实验室举办2016年科技活动周 ……2
实验室举办2016年公众科学日 ……4
第七届有限域及其应用国际研讨会顺利召开 ……6

科普园地

认识Gröbner基（孙瑶、李婷） ……7

行业资讯

美国国土安全部试图商业化的八种网络安全新技术 ……9
微软研究院最新论文：机器具备连续图像叙事能力 ……14

交流与合作

美国马里兰大学吴旻教授访问实验室 ……18
新西兰奥克兰理工大学Reinhard Klette教授访问实验室 ……19
澳大利亚新南威尔士大学Jiankun Hu教授访问实验室 ……20
新加坡科技研究局Khin Mi Mi Aung、徐泉清研究员访问实验室 ……21
美国康奈尔大学唐强博士访问实验室 ……22
实验室刘丽敏高级工程师赴美国参加ISO/IEC JTC 1/SC 27 工作组会议 ……22
实验室陈恺研究员赴美国参加IEEE S&P (Oakland) 2016国际会议 ……23
实验室最新研究成果被ICML2016录用 …… 23

青年风采

陈恺（研究员，博士生导师） ……24
孙思维（副研究员，硕士生导师） ……25

文化生活

实验室举办“信息工程领域免费信息资源的查找与利用”主题讲座 ……26
第一研究室党总支召开“学党章，坚定理想信念”主题党会 ……27
第一研究室举办“关爱环境，关爱你我”志愿活动 ……28

通知公告

信息安全国家重点实验室2016年暑期学校招生简章 ……29
关于举办首届（2016）全国高校密码数学挑战赛的通知 ……30
第十二届信息安全与密码学国际会议征稿通知 ……30

实验室要闻

中科院党组副书记、副院长刘伟平视察实验室

2016年4月22日上午，中国科学院党组副书记、副院长刘伟平来实验室视察。实验室主任林东岱向刘伟平一行介绍了实验室的基本情况，实验室科研人员在展室介绍并演示了代表性科研成果。

刘伟平充分肯定了实验室在支撑国家战略需求方面取得的优异成绩，并对实验室以党建工作的新成效为保障，打造一支政治上忠诚可靠、服务国家战略需求的高水平科研队伍提出要求。他强调，实验室要严格按照中央决策部署和中科院党组要求，努力在“两学一做”学习教育中走到全院的前列。要注重发现和树立忠于党、忠于人民、忠于祖国，在科技工作中做出突出贡献的优秀党员典型，树立学习标杆，发挥好示范带动作用。要按照国家战略科技力量的要求加强实验室思想政治建设，增强党员科技人员实现习近平总书记视察中科院时提出的“四个率先”目标的责任感、使命感。

科研人员介绍实验室代表性成果

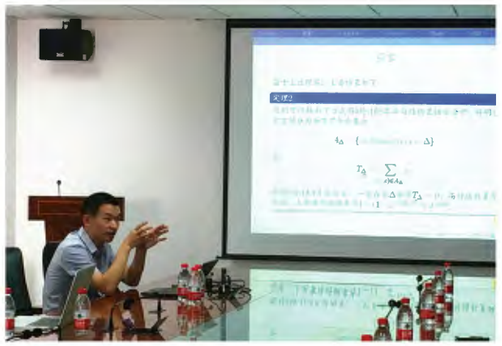
刘伟平一行视察实验室办公环境

实验室举办 2016 年科技活动周

2016年5月16日至20日，信息安全国家重点实验室举办了2016年科技活动周活动。活动周期间举办了七场特邀讲座和公众科学日，活动吸引了众多科技爱好者的积极参与。

科技周活动的系列特邀讲座中，既有基础性较强的密码学理论研究，如上海交通大学的郁昱教授讲解了基于LPN困难问题的后量子密码设计，信息工程所助理研究员庄金成介绍了在小特征域上对离散对数的求解问题，国防科大讲师孙兵就区分5轮的AES和随机置换展示了自己的最新成果，密码科学技术国家重点实验室助理研究员张江则介绍了格和群签名的相关理论知识；又有与现实生活密切相关的应用方面的安全介绍，如清华大学研究员段海新针对在互联网上有广泛应用的CDN及相关的CDN循环转发攻击做了精彩的演讲，信息工程所研究员陈恺就恶意软件的检测做了题为“Scalable Detection of Unknown Malware from Millions of Apps”的讲座，中国科学院软件研究所李新宇介绍了他们在TLS多重握手功能组合运行的最新安全性分析。七位特邀主讲人就各自研究领域向与会人员精彩而详实地介绍了相关科普知识及最新研究成果。

5月20日的公众科学日活动，实验室副主任薛锐、办公室主任刘峰向来访人员介绍了实验室的基本情况；实验室一线科研人员科普化地介绍了几项代表性科技创新成果。



1、国防科技大学讲师孙兵

2、密码科学技术国家重点实验室助理研究员张江

3、清华大学段海新教授

4、上海交通大学特别研究员郁昱

5、信息工程研究所研究员陈恺

6、信息工程研究所助理研究员庄金成

7、中科院软件研究所博士生李新宇

1	2
3	4
5	6
7	

实验室举办 2016 年公众科学日

2016年5月20日，信息安全国家重点实验室举办了公众科学日活动。中国人民大学、北京邮电大学等高校团队、来自全国各地的近百位科技爱好者参加了此次活动。

实验室副主任薛锐、办公室主任刘峰向来访人员介绍了实验室的基本情况；实验室一线科研人员向来访人员演示了几项代表性科技创新成果，如海量软件恶意代码和克隆检测系统、侧信道密码分析技术、隐写与隐写分析的对抗性研究及图像盲检测技术等。科研人员科普化地介绍了研究学科知识点及其应用，来访人员就自己感兴趣的问题与科研人员进行了互动、交流。

此次公众科学日活动也是信息安全国家重点实验室2016年科技活动周活动的一部分。实验室充分利用自身的科研、人才和资源优势，面向广大科技爱好者开展科普教育，让一般公众走进了信息技术的科学殿堂，近距离接触实验室的科研环境，切实感受了信息科技带来的变化与便利；同时，公众科学日的举办也在扩大实验室知名度、拓宽生源渠道、提高生源质量、展示实验室实力等方面打开了新的局面。

活动背景介绍：

公众科学日是科技部国家重点实验室面向全国范围的大规模群众性科技活动。今年公众科学日的主题是“科技创新、追梦未来”，具体内容为：以开放科普场馆的形式展示实验室科技创新成果，让一线科研人员科普化地介绍研究学科知识点、宣传自己的科研成果，让兄弟院所或高校的师生和广大群众以此为机会走进实验室，了解实验室。

实验室副主任薛锐研究员介绍实验室基本情况

实验室办公室主任刘峰研究员介绍实验室基本情况

科研人员讲解隐写与隐写分析的对抗性研究及图像盲检测技术

科研人员演示海量软件恶意代码和克隆检测系统

科研人员讲解侧信道密码分析技术

实验室副主任薛锐研究员向来访学生团体介绍实验室招生情况

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。

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。

认识 Gröbner 基

（孙瑶，李婷）

Gröbner基是计算代数几何中的一个基本概念，是由一组(通常是有限个)多项式组成的特殊集合。Gröbner基广泛应用于数学和科学工程各领域。其中，最直接的应用是在代数方面，例如求解非线性多项式系统，求解模多项式的一致性问题以及求解线性丢翻图多项式方程。在交换代数领域，Gröbner基可用于求解理想的交集。此外，Gröbner基在计算曲线族的包络线，确定几何体的Hilbert维数等问题中都发挥重要作用。Gröbner基在理论上的应用并不局限于代数问题，还能用于求解其他数学领域的问题，例如几何定理证明问题、图形着色问题以及整数规划问题。

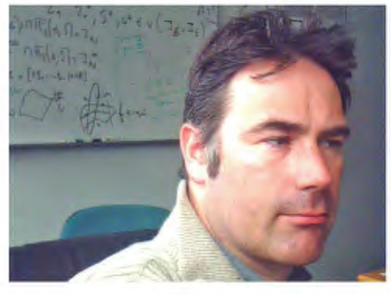
Gröbner基不仅能帮助数学家们攻克难题，作为一种强而有力的数学工具，它还能够解决很多科学工程领域的实际问题。其中，最主要的应用在密码学方面，计算密码系统的Gröbner基是代数攻击中最有效方法的方法之一。在编码理论中，Gröbner基可以用于识别可信编码。这主要是由于在信道传输过程中并不总是保证正确性，可能由于一些原因导致接收到的编码包含错误信息，因此需要从接收到的纷繁复杂信息中识别出可信编码。在机器人科学中，广义逆运动问题可以转换成Gröbner基求解问题，这个问题主要研究的是机器人上的多个关节如何配合转动才能到达指定位置，为了求解关节转动角度可以列出非线性方程然后用Gröbner基求解。Gröbner基还有一些让人意想不到的应用。例如在软件工程中，可以通过计算 Gröbner基找到程序循环中的不变量，这可以应用在自动程序验证中。在石油工业领域，Gröbner基还可以用于分析和优化的海洋平台中的石油生产量。

我们今天之所以能够使用的如此强大的Gröbner基解决各种问题，主要应归功于以下四个人：Wolfgang Gröbner, Bruno Buchberger, Daniel Lazard, Jean-Charles Faugère。

Wolfgang Gröbne

Bruno Buchberger

Daniel Lazard



Jean-Charles Faugère

1965 年，Bucbherger 在博士期间为了计算商环等价类的基时提出了一组特殊的基，为了感谢其博士导师 Gröbner 教授在计算这组基时提出的关键性建议，Buchberger 把这组特殊的基命名为 Gröbner 基。但是由于 Gröbner 基的计算复杂度过高而导致 Gröbner 基在其提出后很长一段时间里都没有用武之地，没有被用来解决任何实际问题 .。鉴于此，Lazard 教授于 1983 年首次揭示了 Gröbner 基与线性代数的关系，并创造性地提出了使用线性化方法计算 Gröbner 基的思想。最终实现这一思想的是 Lazard 教授的学生 Faugère，Faugère 于 1999 年和 2002 年提出了目前效率最高的计算 Gröbner 基的算法 F4 和 F5 算法。

在 Gröbner 基的研究中，如何高效地计算 Gröbner 基始终是一个广受学者关注的课题。第一个计算 Gröbner 基的算法是 Buchberger 算法，很多学者都为提高该算法的计算效率添砖加瓦，做出了重要贡献。Gröbner 基算法的改进主要体现在三个方面。一方面，为了提高算法中基本运算的效率，在 Lazard 指出 Gröbner 基与线性代数的关系，将 Gröbner 基的计算问题转化为线性代数问题；Gebauer 与 Möller 随后提出线性基算法 (1986)；经过一系列的优化后 ,Faugère 提出 F4 算法。在另一方面 ,为了避免算法中的冗余计算，Bucbherger 提出了两条算法准则 (1979)；之后 ,Möller 等提出利用何冲计算 Gröbner 基的算法 (1992)，算法去除冗余计算效果虽好，但计算复杂度较高；最后，Faugère 在 F5 算法中提出了两条新标准，几乎可以去掉所有冗余计算，使计算效率得到大幅提升。Gao 等提出的 GVW 算法只是从另外一个角度彻底解决了 F5 算法的很多理论难题 (2010)。最后一方面的改进是在计算过程中计算顺序的改进，主要工作是 Giovini 等人提出的 sugar 策略 (1991)。目前主流计算机代数平台 (如 Magma, singular, Maple 等) 均集成了高效的 Gröbner 基算法 ,用户可以方便的调用。

随着 Gröbner 基算法的不断改进，以及计算机硬件能力日益增强，Gröbner 基将会在更加广阔的科学舞台中扮演更为重要的角色。

美国国土安全部试图商业化的八种网络安全新技术

2016 年 4 月 25 日　　文章来源：安全牛

经联邦政府批准，美国国土安全部 (DHS) 公开最新开发的 8 种网络安全技术，并准备投入 10 亿美金，寻求私营企业的帮助，以将其转化为实用型的商业产品。

在 DHS 发布的第四份《网络安全部门转为实用技术指导方案》(http://t.im/13f40) 中，国土安全部列出了恶意软件分析、行为分析、保护 Windows 应用的随机化软件等 8 项技术。

该方案旨在对非机密的网络安全研究项目进行实用化探索。报告中称：**“联邦政府在非机密网络安全技术上的投入每年超过10亿美金，然而这些技术极少进入市场。”**

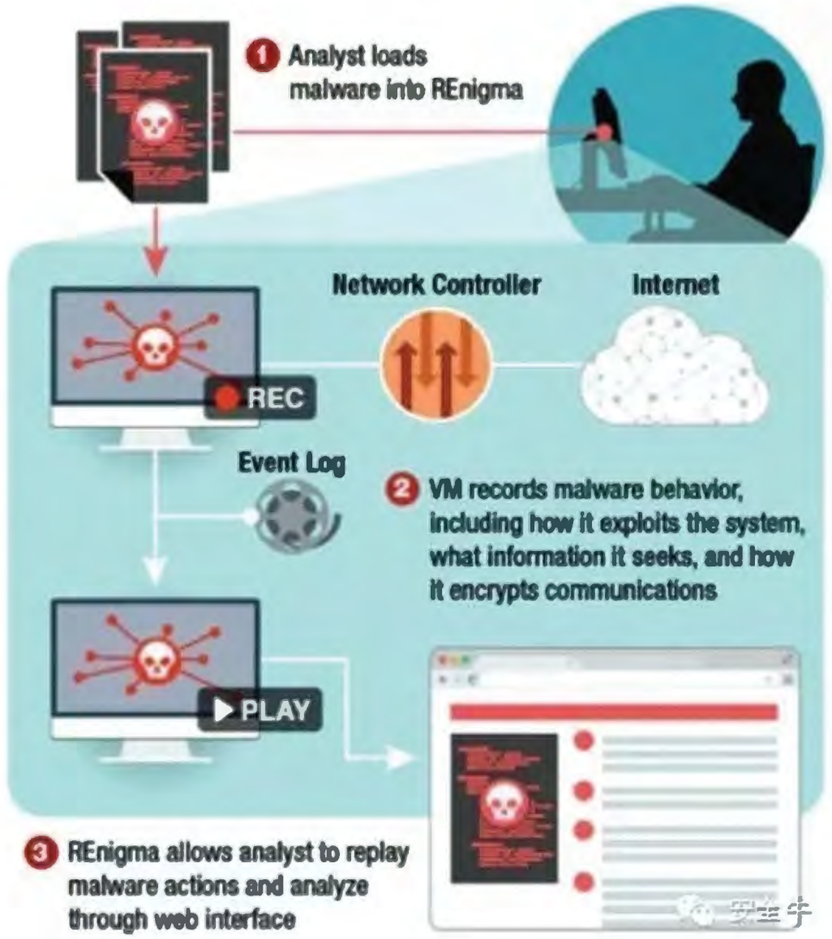
下面是报告中这8项新技术的简要介绍：

1、REnigma

该软件的功能是在虚拟机中运行恶意软件，观察其行为，以供后期分析。它可以让安全研究人员更方便地分析恶意软件，并详细了解其行为方式和原理，而不用亲自进行逆向工程。

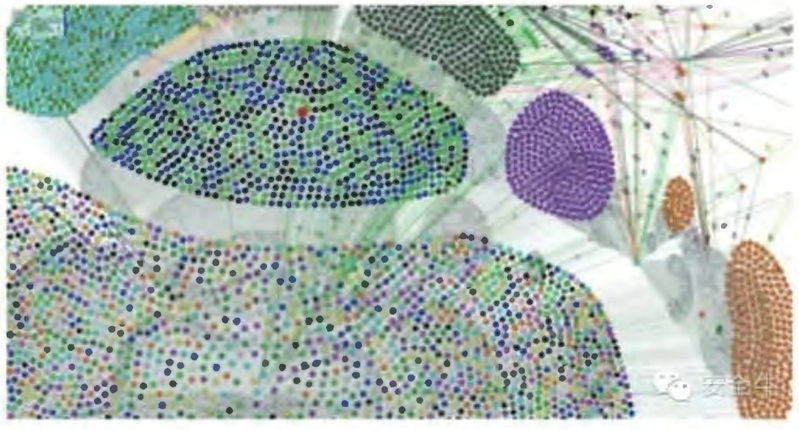
关键的进步是约翰霍普金斯大学应用物理实验室开发的虚拟机录像和回放技术。通过该技术，研究人员可以在恶意软件运行过程中对其使用分析工具，同时对恶意软件的反分析技术保持隐身。

报告中提到：“举例而言，如果恶意软件代码样本向网络输出了一串加密数据，分析师可以使用REnigma回溯到内存中的明文信息，并恢复出数据外泄中利用的加密秘钥。”



2、Socrates

该软件平台会在数据集里寻找模式，并可以引诱出可能为安全威胁的那些。它能够同时提供分析和计算机科学能力，而这种能力的组合往往是人类所缺失的。

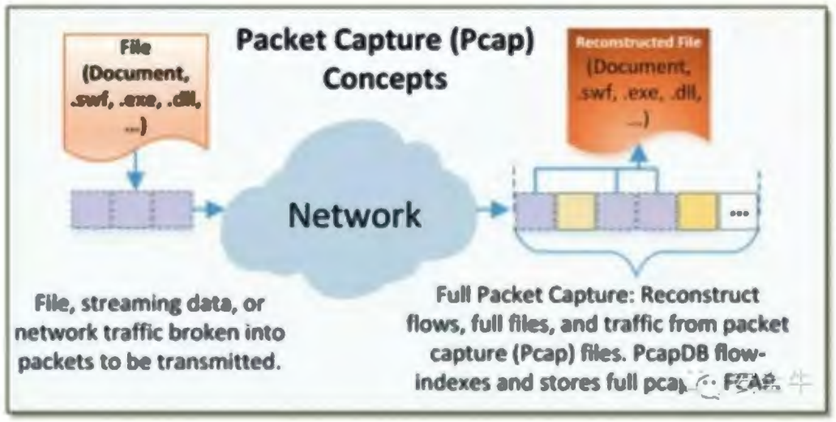


在 200 万个链接的网络里检测异常活动

该平台能够对数据进行无监督分析，寻找可能带来产出的模式。Socreates已经被用于学习大量人群的出行模式，以发现与目标人物有联系的个人。

3、PcapDB

这是一个软件数据库系统，能够通过将包数据组织成数据流，抓取并分析网络流量。

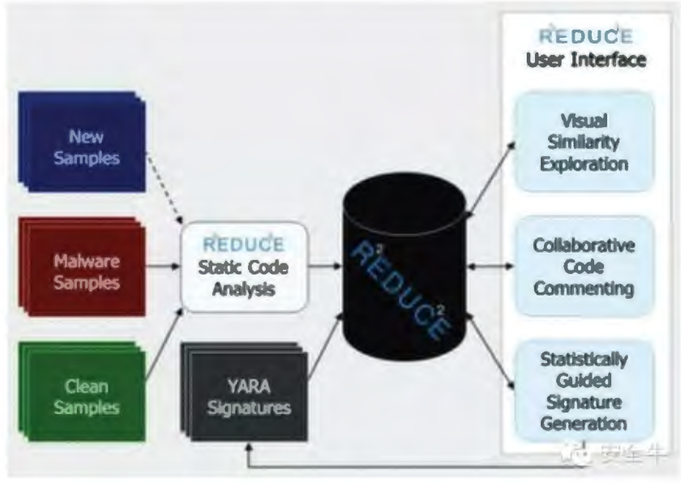


该技术的开发者将其功能比作飞机上的黑盒子：“Pcap可以重建恶意软件的传输、下载、命令、控制信息，并提取其中数据。”

该平台能够优化抓取到的数据，减少其存储空间，加快分析时的读取速度。通过缩减不必要的功能，PcapPB能够存储常见串行SCSI (Serial Attached SCSI, SAS) 硬盘数个月间产生的流量数据，这将为调查入侵事件提供强大的助力。开发者写道：“在调查网络安全事件时，最关键的一个指标就是能上溯到的最远日期。”

4、 REDUCE

这是一个软件分析工具，能够发现恶意软件样本之间的联系，并创建可用于甄别威胁的特征签名。



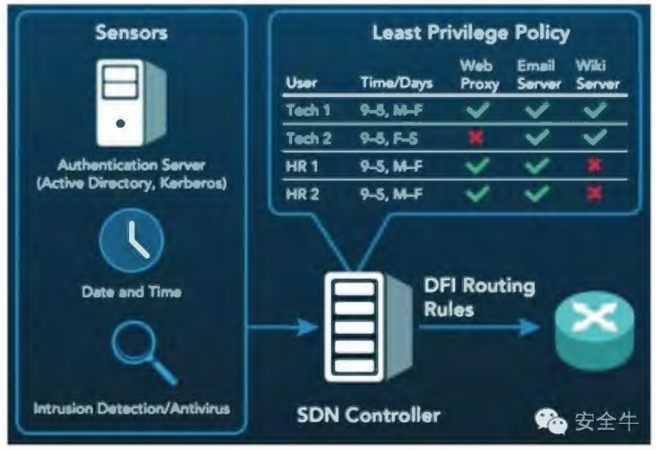
该软件对恶意软件样本进行静态分析，寻找其和历史样本之间使用相同代码的段落。这可以让研究人员快速推断出新型恶意软件的作者，确定其技术特点。

REDUCE 与一些只能同时对比两种恶意软件的商业化工具有所不同，它可以同时比较多种样本。当它发现代码段之间的相似之处时，也会与历史上的所有记录进行比对。

该技术适用于反向工程背景没有那么强的网络安全人员。

5、 动态流隔离 (Dynamic Flow Isolation)

动态流隔离 (DFI) 利用软件定义网络，基于企业所需的运行状态，按需部署安全策略。



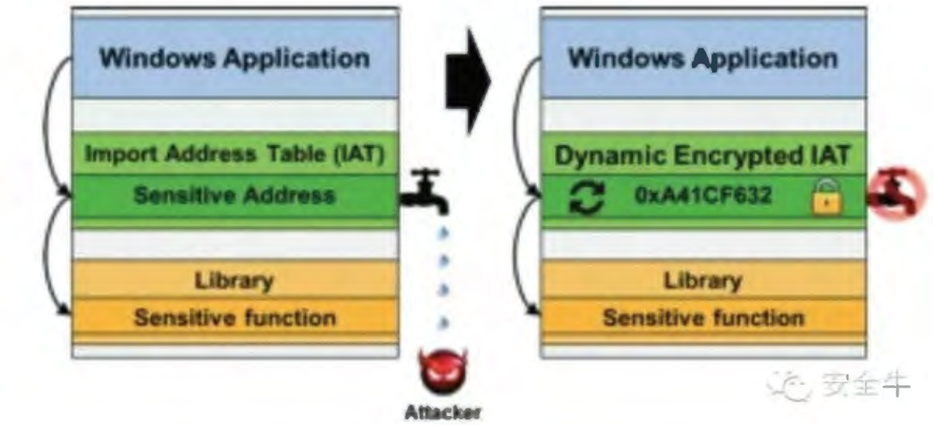
不论过程是手动还是自动，通过启用、禁用或对个人用户及网络服务之间的通信进行频率限制，均可以实现其功能。

通过与认证服务器、入侵检测系统进行整合，该软件能够对网络的运行状态产生情景感知。如果网络状态发生变化。它也会与软件定义网络控制器进行整合，改变目前允许的网络连接。这使得隔离特定设备或组，并拦截试图访问关键资产的攻击者成为可能。

该软件包括策略强制执行内核，它与软件定义网络控制器一同部署，可以更新网络中交换机的访问规则。该过程可以与企业现有的软件定义网络硬件设备整合，在多个软件定义网络控制器之间移动起来也很方便。

6、 TRACER

TRACER 是“运行时间内对常见可执行文件应用实时随机化”(Timely Randomization Applied to Commodity Executables at Runtime) 的简称，它可以改变 Adobe Reader、IE、Java、Flash 等闭源 Windows 应用的内部布局和数据。



由于这类应用属于闭源，其数据和内部布局均为静态的，威胁源对其的攻击将产生巨大的影响面。

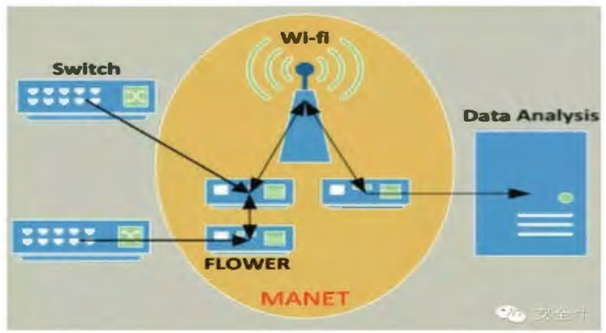
数据和布局的信息在输出过程中遭到泄露，其结构在应用下一次输出时也将完全不同。

因此，TRACER 能够挫败针对这些 Windows 应用的控制劫持攻击 (control-hijacking attack) 。该软件会被安装到所有设备上，不会干预其日常运行。其缺陷在于将平均增加 12% 的运行时长。

地址空间布局随机化 (Address Space Layout Randomization) 、基于编译器的代码随机化、入侵集随机化等其它随机化方案均为一次性的。耐心的攻击者可以等待更长时间，在获取应用泄露的更多信息后再展开攻击。

7、 FLOWER

网络流分析器 (Network FLOW AnalyzER, FLOWER) 可以分析 IP 包头，双向收集数据流的信息，并利用信息甄别正常与异常数据流，进一步寻找潜在的数据泄露和内部人员威胁。



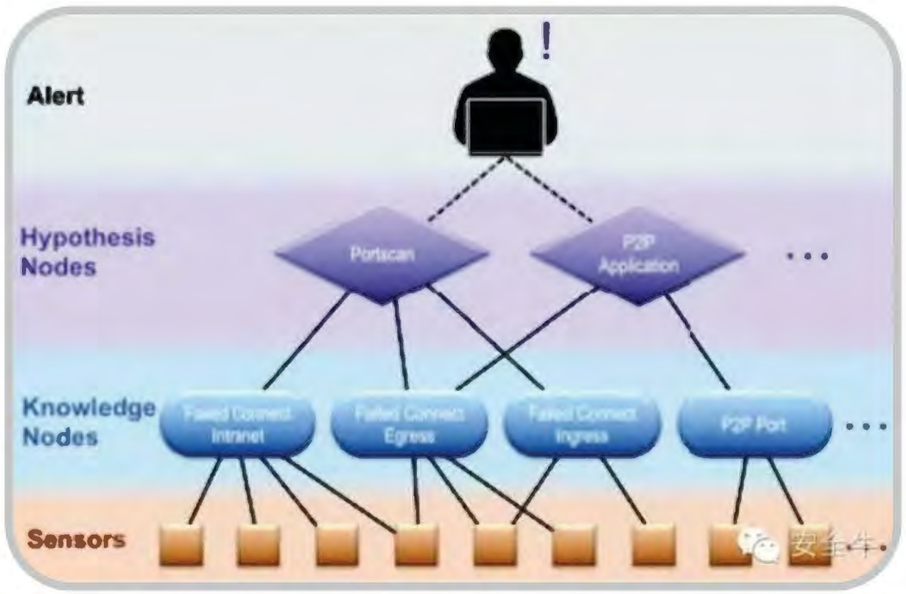
8、SilentAlarm

该平台分析网络行为 ,甄别可能存在的恶意行为 ,制止并不存在特征签名的零日攻击等威胁。

传感器会将网络事件信息发送到其分析引擎。该引擎包含知识节点、针对成功或失败的 SMTP 尝试及失败的互联网连接等不同类型的网络行为调整的分析模块。基于历史行为 ,每个新事件都会被标为正常或不正常。

这些特征信息会被传输到假设节点 ,它会决定观察到的行为是否意味着恶意活动。如果发现恶意活动 ,SilentAlarm 可以发出警报或直接进行干预。

在这份报告的最后 ,还分别介绍列出了 2013 到 2015 年 3 个财年的网络安全新技术。



微软研究院最新论文：机器具备连续图像叙事能力

2016 年 6 月 23 日　　文章来源：新智元

摘要

我们介绍首个用于连续视觉 - 语言转换的数据集 ,并探索在视觉叙事任务中如何应用该数据集。在该数据集首次发布的版本——SIND v.1——中 ,包括 81,743 个不同照片 ,排列成符合文字描述和故事情节的 20,211 个序列。我们为叙事任务建立了一些高性能的基线 ,并对评测过程制定了自动化指标。通过对该数据集及叙事任务中提供的具体描述和形象的社交化语言进行建模 ,有望将人工智能的水平从只能对典型视觉场景进行基本的理解 ,提高到对基础的事件结构和主观表达能够越来越接近人类理解的水准。

1、引言

除了对简单对象和具体场景的理解之外，还要解释其中的因果结构；理解视觉输入需要将不同时刻绑定在一起，因为不同的时刻在时间上会产生紧密联系的事件描述。这就需要将推理的对象从静态时刻的、没有上下文的单一图片，转变为描述事件发展的图片序列。

在视觉方面，从最初的单一图片变为有上下文关系的图片，让我们开始创造出一个可以根据之前见过的视觉事件推断当前的视觉事件的人工智能。

在语言方面，从最初的文字描述到故事叙述有助于学习更多的评价、会话以及抽象的语言。这之间的差别就像，"坐在一起"和"度过愉快的时光"之间的差别，或者"太阳正在落山"和"天空映射着晚霞的光辉"之间的差别（如图 1）。前者描述捕捉到的图片的内容是具体文字；而后者的描述则需要进一步判断什么样的情景才是"愉快的时光"，或者对于一个特定的日落，什么才是特别的和值得分享的。

我们介绍的首个带有相应描述的连续图像数据集，它掌握了其中一些微妙但重要的差异，促进了视觉叙事任务的发展。对相同的图像，我们从三个语言层面来发布数据：（1）独立图像描述（DII, Descriptions of images-in-isolation）；（2）连续图像描述（DIS, Descriptions of images-in-sequence）；（3）连续图像叙事（Stories for images-in-sequence）。

这种分层的方法揭示了时间先后和叙事语言的影响。由于所有层次都是来自相同的图像，数据集直接提高了对文字和更抽象的视觉概念之间关系，以及视觉图像和典型事件模式之间关系的建模效果。另外，我们还提出了一个与人类判断关联最大的自动评价指标，并建立了视觉叙事任务的若干性能优越的基线。

2、背景

叙事本身就是最古老的人类活动之一，提供了教育、保护文化、灌输道德、以及建议的方式方法；将 AI 的研究方向汇集于叙事任务将有望带来更多的类人智能以及做出更像人类的理解。

			
DII	A group of people that are sitting next to each other.	Adult male wearing sunglasses lying down on black pavement.	The sun is setting over the ocean and mountains.
SIS	Having a good time bonding and talking.	[M] got exhausted by the heat.	Sky illuminated with a brilliance of gold and orange hues.

图 1：独立图像描述（DII）和连续图像故事（SIS）之间差别的语句举例

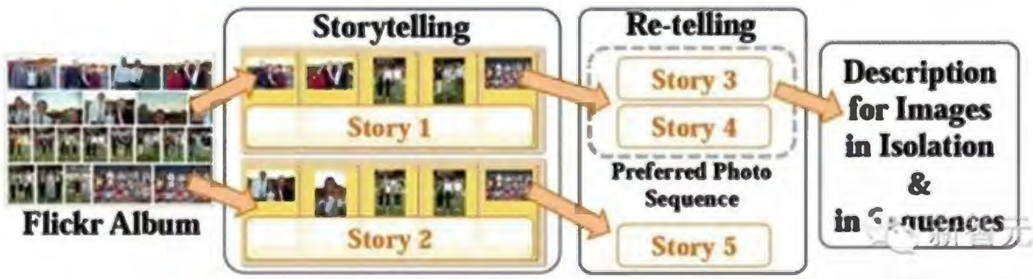
3、数据集构成

提取照片（略）

连续画面的众包故事 我们开发一个2段众包的工作流来收集符合图像的自然的故事文本。第一阶段是叙事，在这个阶段，参与者会从指定的相册中选择一个照片子集，形成一个照片序列，并为这个照片序列写一个故事（如图3）。第二个阶段是复述，在这个阶段中参与者会根据第一阶段中产生的照片序列，来写出一个故事。

图 3：故事叙述任务的界面，包括：1）照片专辑，2）故事情节板

独立图像及连续图像的众包描述我们也用众包来收集DII及DIS的描述，其中带有故事描述的照片序列来自于第一个任务中的大多数参与者（如图2↓）。



后期数据处理我们用CoreNLP分词器对所有的故事叙述和描述进行分词，然后将所有人名用更一般化的男性/女性来代替，将所有被命名的实体用其类别来代替。

DII	A black frisbee is sitting on top of a roof.	A man playing soccer outside of a white house with a red door.	The boy is throwing a soccer ball by the red door.	A soccer ball is over a roof by a frisbee in a rain gutter.	Two balls and a frisbee are on top of a roof.
DIS	A roof top with a black frisbee laying on the top of the edge of it.	A man is standing in the grass in front of the house kicking a soccer ball.	A man is in the front of the house throwing a soccer ball up	A blue and white soccer ball and black Frisbee are on the edge of the roof top.	Two soccer balls and a Frisbee are sitting on top of the roof top.
SIS	A discus got stuck up on the roof.	Why not try getting it down with a soccer ball?	Up the soccer ball goes.	It didn't work so we tried a volley ball.	Now the discus, soccer ball, and vol[illegible]ball are all stuck on the roof.

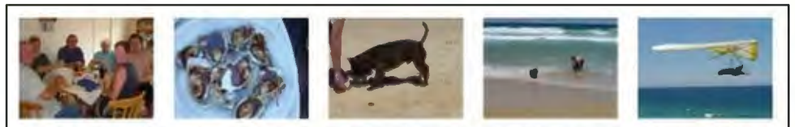
图 4：独立图像描述（DII）；连续图像描述（DIS）；以及连续图像叙事（SIS）举例

4、数据分析（略）

5、自动化评测标准

鉴于故事叙述任务的复杂性，对于生成的故事的质量的评估，最好的并且最可靠的评价方法就是依靠人类的判断。然而，自动评价指标对于进行快速测试是很有用的。

为了更好的了解哪些指标可以代替人力评估，我们从SIS训练集中抽样了3000个故事，并分别计算了自动指标和人类判断之间的相关系数。



+Viterbi	This is a picture of a family. This is a picture of a cake. This is a picture of a dog. This is a picture of a beach. This is a picture of a beach.				
+Greedy	The family gathered together for a meal. The food was delicious. The dog was excited to be there. The dog was enjoying the water. The dog was happy to be in the water.				
-Dups	The family gathered together for a meal. The food was delicious. The dog was excited to be there. The kids were playing in the water. The boat was a little too much to drink.				
+Grounded	The family got together for a cookout. They had a lot of delicious food. The dog was happy to be there. They had a great time on the beach. They even had a swim in the wa[illegible]				

Table 5: Example stories generated by baselines.

6、结论及未来工作

我们介绍了首个用于连续视觉-语言转换的数据集，该数据集逐步地从独立图像转变为连续的故事。我们认为对从该数据集中捕获的更形象和社交化的语言进行建模，对于推动AI向更接近人类的方式理解问题有着极其重要的作用。对于视觉叙事的任务我们建立了性能优越的基线，并且利用METEOR作为自动指标来评价该工作的进展情况。

美国马里兰大学吴旻教授访问实验室

2016年4月28日，应信息安全国家重点实验室邀请，美国马里兰大学吴旻教授来实验室进行访问和交流。

来访期间，实验室主任林东岱研究员向吴教授介绍了实验室的基本情况和代表性成果；吴旻教授作了题为《Seeing the Invisibles: Micro-Signals for Information Forensics》的学术报告，重点介绍了微信号在防止秘密信息泄露、图像篡改检测以及多媒体信息定位等方面的应用研究成果；报告结束后，吴教授与实验室科研人员就信息隐藏方向的应用研究进行了深入探讨。

实验室主任林东岱研究员向吴教授介绍实验室

报告现场

新西兰奥克兰理工大学 Reinhard Klette 教授访问实验室

2016年4月28日至5月1日，应信息安全国家重点实验室邀请，新西兰奥克兰理工大学Reinhard Klette教授来实验室进行交流访问。来访期间，Reinhard Klette教授作了题为《Progress and Challenges in Vision-based Driver Assistant Systems》的学术报告，重点介绍了自动驾驶电动车的相关研究成果。

报告现场

澳大利亚新南威尔士大学 Jiankun Hu 教授访问实验室

2016年6月1日至2016年6月18日，应信息安全国家重点实验室邀请，澳大利亚新南威尔士大学Jiankun Hu教授来实验室进行学术访问和交流。

来访期间，Jiankun Hu教授做了题为《Energy Big Data Analytics and Security: Challenges and Opportunities》的学术报告。报告综述了能源大数据的特点以及对其进行分析和安全保护的重要性，并着重介绍了能源大数据分析和安全保护目前所面临的挑战。随着化石能源的逐渐枯竭，怎样高效节俭地使用现有能源得到越来越多的关注，通过智能网络监控大众能源使用情况以调节能源的分配是一条有效的解决途径，但通过智能网络得到的大众使用化石能源的数据具有规模大、更新速度快、数据结构多样化等特点，而且这些数据涉及个人隐私，需要隐私保护，Jiankun Hu教授的报告深入浅出地介绍了对能源数据进行分析和安全保护所面临的挑战，并提出数据挖掘和数据加密同时设计的新思路。

访问期间，Jiankun Hu教授与实验室科研人员就云计算中访问控制、对称可搜索加密(SSE)、生物密码生成算法等研究方面的有关问题进行了深入探讨，并就双方进一步的科研合作进行了交流

报告现场

附：Jiankun Hu教授简介

Jiankun Hu教授现为澳大利亚新南威尔士大学教授，新南威尔士大学网络安全实验室主任。Jiankun Hu教授主要研究领域包括网络安全（包括生物密码）、生物特征识别，论文主要发表在顶级学术期刊和会议(包括IEEE TPAMI,TIFS，TPDS, TOC, ICC，Globecom)，同时担任七个国际期刊的编委，现已获得七项澳大利亚研究理事会的资助项目。

新加坡科技研究局 Khin Mi Mi Aung、徐泉清研究员访问实验室

2016年6月22日，新加坡科技研究局数据存储研究院Khin Mi Mi Aung、徐泉清研究员来实验室进行考察访问和学术交流。

来访期间，Khin Mi Mi Aung、徐泉清研究员考察了实验室的科研学习环境和学术研究情况，与实验室研究人员进行了深入交流，表达了今后在数据存储安全领域开展合作研究的愿望。Khin Mi Mi Aung研究员做了题为《Hyperscale and Intelligent Data Center Technologies》的报告，介绍了新加坡数据存储研究院在下一代非易失性存储器（NVM）技术、大数据存储、数据安全、数据中心管理等领域所开展的研究和取得的成果，并就目前国际热门的全同态加密技术、分布式存储技术等前沿课题与听众进行了热烈讨论。徐泉清研究员向实验室研究生介绍了在新加坡学习、工作、生活的相关情况，并欢迎他们毕业后去数据存储研究院应聘科研岗位。

Khin Mi Mi Aung 研究员作报告

附：Khin Mi Mi Aung和徐泉清研究员简介

Khin Mi Mi Aung研究员毕业于韩国航空大学计算机工程专业，现为新加坡科技研究局数据存储研究院助理经理、高级科学家，主要研究领域为数据和信息安全、数据中心管理、网络存储技术。徐泉清研究员毕业于北京大学计算机科学专业，现就职于新加坡科技研究局数据存储研究院，同时为新加坡理工学院和澳大利亚南威尔士大学兼职讲师，主要研究领域为云存储、云数据管理、大规模分布式系统等。

美国康奈尔大学唐强博士访问实验室

2016年6月27日，应信息安全国家重点实验室邀请，美国康奈尔大学唐强博士访问了实验室并做题为《超越消息恢复安全的蜜罐加密》的学术报告。

唐强博士毕业于美国康涅狄克大学，随后进入美国康奈尔大学进行博士后研究，今年秋季即将作为助理教授加入新泽西理工学院。唐强博士的研究领域为后斯诺登密码学和密码学货币等，并已在ACM CCS、Eurocrypt等国际会议上发表多篇论文。

《超越消息恢复安全的蜜罐加密》正是唐强博士在Eurocrypt 2016上新发表的论文。蜜罐加密的概念是Juels和Ristenpart在Eurocrypt 2014上提出的，Juel和Ristenpart为蜜罐加密定义并实现了消息恢复安全性。但是消息恢复安全性是相对弱的性质，并不能防止攻击者从密文中获取明文的部分信息或有效地篡改密文。唐强博士及其合作者Jaeger和Ristenpart对蜜罐加密的安全性进行了系统的研究，定义了目标分布语义安全性和目标分布不可延展性等安全性质，并证明了JR的蜜罐加密的变形方案能够满足这些性质。随后，他们为熟知结论“无限制敌手在得到有限数量的明密文对时总能成功恢复明文”给出了正式的证明。

此外，唐强博士还介绍了目前学术界对密码学货币等领域的研究进展。双方对于进一步的交流合作进行了探讨。

实验室刘丽敏高级工程师赴美国参加 ISO/IEC JTC 1/SC 27 工作组会议

2016年4月11日-15日，实验室刘丽敏高级工程师参加了在美国坦帕举办的ISO/IEC JTC1/SC 27工作组会议及全体代表大会。SC27是国际标准化组织（ISO）和国际电工委员会（IEC）的第一联合技术委员会（JTC1）中负责制定国际信息安全标准的技术组织。SC27下设5个工作组，主要负责研究和制定信息安全管理体系、密码学与安全控制、信息安全评估、安全控制与服务以及身份管理与隐私保护等领域的信息安全国际标准。ISO/IEC JTC 1/SC 27 工作组会议及全体代表大会（会议英文名称ISO/IEC JTC 1/SC 27 Working Groups and Plenary Meeting）是国际上信息安全前沿技术交流平台，每年举办两次，此次会议由美国国家标准学会（American National Standards Institute, ANSI）主办，会议的主题是前沿信息安全技术及标准化探讨。

此次参会，刘丽敏博士主要以WG2工作组专家身份参与ISO/IEC JTC 1/SC27的WG2密码与安全机制工作组部分的会议。刘丽敏在WG2会议中以联合报告人的身份就已立项的研究项目《IBS算法入选ISO/IEC 14888-3》做正式报告，以联合编辑的身份就处于第一版工作组草案阶段的《Amendment 1 to ISO/IEC 14888-3》做正式报告。并借这次机会，以ISO/IEC JTC1/SC27 WG2专家的身份与参会的国际信息安全界的学者进行学术交流，参与WG2工作组的工作。本次会议，形成决议如下：

1. 包含我国SM3密码算法的ISO/IEC 10118-3国际标准进入DIS阶段；
2. IBS算法纳入ISO/IEC 14888-3的补篇1中，与SM2数字签名算法一起进入第二版工作组草案阶段。

实验室陈恺研究员赴美国参加 IEEE S&P (Oakland) 2016 国际会议

2016年5月23日至5月25日，信息安全国家重点实验室陈恺研究员赴美国San Jose参加2016年著名信息安全会议37th IEEE Symposium on Security and Privacy（IEEE S&P）。IEEE S&P是中国计算机学会CCF推荐的网络与信息安全领域的A类学术会议，会议创办于1980年，是国际认可的信息安全领域顶级学术会议，无论是在学术界还是在工业界都具有极大的影响力，每年举办一次。

实验室文章《Following Devil’s Footprints: Cross Platform Analysis of Potentially Harmful Libraries on Android and iOS》被本次会议接收。文章提出一种跨平台的恶意代码映射检测方法，该方法在目标平台代码无法判断是否恶意的情况下进行恶意代码的检测，并以封闭的苹果官方市场为例，国际上首次完成该市场大规模恶意代码检测。具体地，利用检测安卓软件和iOS 软件间同源恶意代码的思想，将安卓恶意代码跨平台地映射到苹果软件中进行恶意代码的检测。其中映射过程使用已知的安卓恶意代码，寻找并获取其跨平台特征，通过将这些特征进行映射，获取iOS 平台具有该特征的程序，并进行行为层次的确认。首次对苹果iOS 官方市场和5 个第三方软件市场的应用软件进行了大规模的分析，超过15 万个苹果iOS软件被逐一检测。

此成果是中国大陆第7篇在该顶级学术会议上发表论文，也是国内首篇在该会议上发表的恶意代码评测相关的论文。会议期间，陈恺研究员对该项技术及课题组近年来在恶意代码检测领域取得的系列成果进行了介绍，并同与会专家进行了深入交流。

实验室最新研究成果被 ICML2016 录用

国际机器学习大会（International Conference on Machine Learning, 简称ICML）是世界顶级的机器学习会议，属于CCF A类会议，于2016年6月19日-24日在美国纽约举办。信息安全国家重点实验室许倩倩副研究员等人共同完成的工作“False Discovery Rate Control and Statistical Quality Assessment of Annotators in Crowdsourced Ranking”被ICML2016录用。

随着互联网及无线宽带网络技术的迅猛发展，网络众包因其具有成本低、参与人员广泛、数据量大等优点，提供了大数据时代下通过群体来完成任务的新途径。 由于网络众包环境收集的数据存在噪声和异常，文章提出基于knockoff filters和Inverse Scale Space dynamics的异常用户检测方法，有效提升了网络众包的数据质量。不同于传统的检测方法，该算法可有效控制其false discovery rate (FDR)，因此具有更广泛的应用前景。该项工作获得了ICML评审专家的一致认可，被邀请做17分钟的大会报告，并进行海报展示。

陈恺(研究员 ,博士生导师)

2010年于中国科学院研究生院获博士学位。主要研究领域包括软件安全、智能终端安全、安全测评和隐私保护。在IEEE S&P、USENIX Security、CCS、ICSE、ASE、IEEE Trans. on Reliability等高水平会议、期刊发表论文50余篇；获得与申请专利12项；曾主持和参加国家自然科学基金、863计划、中科院战略性先导科技专项、国家发改委信息安全专项等国家部委课题20余项；TDSC、Computers & Security等SCI期刊评审专家；AsiaCCS、SecureComm等多个国际会议委员会成员。主页：http://www.kaichen.org

代表性成果包括：有效解决多年来软件同源检测准确性与高效性难以两全的问题，使市场级规模软件（达到百万数量软件，包含约十亿个函数、万亿条指令）同源性的准确比较成为了可能（发表于ICSE 2014）。首次将Android平台未知恶意代码的检测时间从数小时（或更久）减至10秒内；基于该方法，完成目前已知世界最大规模的Android软件市场未知恶意代码的检测（发表于USENIX Security 2015）。提出跨平台的恶意代码映射检测方法，在目标平台代码无法判断是否恶意的情况下进行恶意代码的检测，并以封闭的苹果官方市场为例，国际上首次完成该市场大规模恶意代码检测（发表于IEEE S&P 2016）。

孙思维(副研究员 ,硕士生导师)

2013年于中国科学院大学获博士学位。2016年入选中国科学院信息工程研究所“青年之星”人才培养计划。主要研究兴趣为分组密码算法的自动化分析、设计与实现。参与了973等多个重要课题与项目，主持国家自然科学基金青年基金1项（基于混合整数规划的自动化密码分析）、密码专项课题一项，承担国家相关部门任务2项。

代表性成果是提出了基于整数规划的比特级算法的自动化分析技术和利用凸闭包计算精确刻画比特级密码算法差分、线性性质的方法，大大提高了分组密码分析的自动化程度，相关成果发表在亚密2014上，被CRYPTO、ASIACRYPT、FSE、TCC等国际密码学相关会议论文和杂志引用40余次，得到了国内外相关研究机构的广泛关注。基于该方法，设计并开发了一套自动化差分、线性分析软件框架，在国家多个相关部门的算法分析与设计任务中得到了重要应用。

青年风采栏目说明

青年人才是实验室人才队伍建设中最具有创新活力的群体。为展现青年职工的风采，《信息安全国家重点实验室通讯》自本期起特设立“青年风采”一栏，不定期选登两位信息安全国家重点实验室青年职工的个人简介。

实验室举办“信息工程领域免费信息资源的查找与利用”主题讲座

2016年4月14日下午，信息安全国家重点实验室邀请中科院文献情报中心的李海英老师举办了“信息工程领域免费信息资源的查找与利用”主题讲座。

讲座中，李海英老师主要介绍了标准文献、科技报告、学位论文、会议论文等信息资源的获取途径，以及中科院文献情报中心提供的产品和服务。

此次讲座对科研人员和学生更有效地利用文献资源与服务，助力科研工作有着积极意义。

讲座现场

第一研究室党总支召开“学党章，坚定理想信念”主题党会

2016年5月中旬，第一研究室党总支组织召开了“学党章，坚定理想信念”主题党会。信息工程研究所所长孟丹、第一研究室主任林东岱参加了所在党支部的学习讨论。

会议通报了支部党员学习习近平总书记在网络安全和信息化工作座谈会上讲话的情况，以及党支部“两学一做”学习教育实施方案，向与会党员征求了关于方案的意见、建议，集中学习了《中国共产党章程》。

会上，支部全体党员逐条逐句通读党章，对党的纲领、党的宗旨、党员义务和权利等进行深入学习。同志们还就学习党章的心得体会进行交流。其中，孟丹同志与支部党员一起梳理了近年来“党要管党、从严治党”的多项重大举措，从理论高度剖析“两学一做”的重要意义，使大家获益良多。孟丹同志认为，“三严三实”和“两学一做”的重要意义在于严格规范了党员行为，其中，“三严三实”主要面向党员干部，“两学一做”则主要面向基层党员，这体现了中国共产党从严治党的决心不可动摇。另外，孟丹同志也结合自身学习体会对党章学习提出建议。如将不同时期的《中国共产党章程》进行对比学习，由此了解不同时期党的工作重点，体会到党是在不断发展进步的。此外，在原原本本学党章的基础上，要创新党员集中学习的方式方法。

第一研究室党总支将继续根据《中国科学院信息工程研究所“两学一做”学习教育实施方案》中的总体要求，认真组织“两学一做”其他三个专题的学习研讨，创新活动形式、注重学习成效，完善制度建设、建立长效机制，以打造一支政治上忠诚可靠，服务国家战略需求的高水平科技队伍。

党会现场

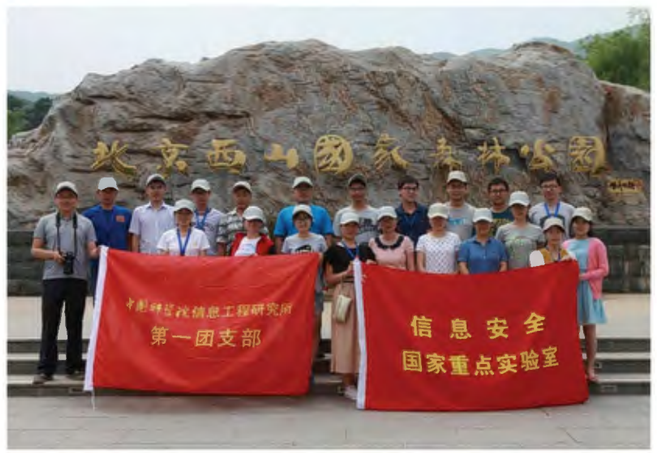
第一研究室举办“关爱环境 ,关爱你我”志愿活动

2016年6月3日，第一研究室在北京西山国家森林公园举办了“关爱环境，关爱你我”志愿活动，共吸引了近三十名志愿者参加。

活动中，第一研究室的志愿者们在西山国家森林公园感受大自然的同时，帮助清理沿途垃圾。此次活动进一步增强了大家保护环境的意识，为维护美好环境贡献了一份力量。

6月5日是“世界环境日”，世界环境日的意义在于提醒全世界注意地球状况和人类活动对环境的危害，要求联合国系统和各国政府在这一天开展各种活动来强调保护和改善人类环境的重要性。第一研究室团支部以实际行动发起倡议：从身边的一点一滴做起，不乱丢垃圾、保护花草树木、尽量绿色出行、减少在旷野烧烤，共同创造美好的生存和生活环境。

志愿者清理沿途垃圾



部分志愿者合影

信息安全国家重点实验室 2016 年“密码学中的序列理论”暑期学校招生简章

信息安全国家重点实验室将于2016年7月9日至7月20日在北京中国科学院大学雁栖湖校区举办“密码学中的序列理论”暑期学校，此次暑期学校以序列密码的理论基础为主题，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，开设序列密码的理论基础专业课程、前沿热点专题讲座。加强学员之间的交流，拓宽学术视野，活跃学术思想，激励学术创新。教学内容主要包括：

1．域上线性递归序列　　2．线性序列的非线性变化　　3．域上非线性递归序列

4．环上线性递归序列　　5．序列密码算法介绍

本次暑期学校计划招收学员50名，主要采取学生申请导师推荐的方式（每名导师限报2名），报名时间最迟至6月20日，6月27日之前反馈录取结果。实验室将为学员免费提供暑期学校期间的食宿。请有意报名的同学填写报名表，通过电子邮件形式将以下材料发至sklois@iie.ac.cn，邮件主题需注明[“密码学中的序列理论”暑期学校报名]。

1、报名表（word版及签字后的扫描件），以“推荐导师姓名-本人姓名-学校”命名；

2、汇总表（.xlsx格式），以“推荐导师姓名-本人姓名-学校”命名。

联系信息

联系人：耿娇娇老师，刘峰老师

电话：（010）82546611，（010）82546591

E-mail：sklois@iie.ac.cn, liufeng@iie.ac.cn

信息安全国家重点实验室

2016年5月17日

关于举办首届(2016)全国高校密码数学挑战赛的通知

各高等学校：

十八大以来，习总书记高度重视国家网络安全和信息化工作，多次对做好此项工作包括人才队伍建设提出明确要求，并亲自担任中央网络安全和信息化领导小组组长。数学是网络安全和信息化的重要基础，从科技角度看，相关网络安全和信息化的数学理论和方法实际决定了国家网络安全和信息化发展水平。为此，教育部高等学校数学类专业教学指导委员会决定通过军民融合的方式每年在全国高校本科生和研究生中开展密码与信息安全领域的挑战赛—全国高校密码数学挑战赛。希望通过该赛事达到如下目标：比较精准地发现和及早培养在此领域有特殊才能的创新型青年数学人才以满足国家发展需求；推动和促进高校应用数学及交叉学科课程的教学内容和人才培养模式改革；强化高校学生的创新意识，提升分析问题和解决问题的能力。由教育部高等学校数学类专业教学指导委员会主办，教育部高等学校大学数学课程教学指导委员会协办的“首届全国高校密码数学挑战赛”得到了教育部高教司支持和指导，并定于2016年6月启动。

竞赛分预选赛和决赛两个阶段进行。预选赛阶段由各赛区组委会主办，于2016年9月前结束。2016年11-12月为全国决赛阶段，由全国高校组委会与有关单位共同举办。挑战赛通知、试题、方案及评选事宜将在挑战赛网站(http://sklois.iie.cas.cn/CryptoMath/)陆续公布。挑战赛将遵循公平、公正、公开原则，组织专家对选手及其成果进行评选，对获奖选手及优秀赛区予以表彰。

请各高校、数学院系认真组织，广泛发动，积极为学生参赛创造条件。挑战赛方案及相关事宜见附件。

教育部高等学校数学类专业教学指导委员会

第十二届信息安全与密码学国际会议征稿通知

由中科院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。会议更详细信息请参看会网页 http://www.inscrypt.cn/ .欢迎大家踊跃投稿：

投稿网址：http://www.easychair.org/conferences/?conf=inscrypt2016

投稿截止日期： 2016年8月10日

录用通知：2016年10月8日

主办单位：信息安全国家重点实验室

　　中国密码学会

协办单位：国际密码协会