全方位解密信息安全国家重点实验室

技术耕耘　延伸安全产业疆界

本刊记者　周 雪　白 洁

编者按：想针对中国科学院信息工程研究所的信息安全国家重点实验室做一个采访专题，这个想法在脑里已经酝酿很久了。

细细想来，有这样的一群人，他们在信息安全产业中低调且神秘，默默地做着大量的工作，虽然大家对其大多只闻其名，未见其人，但这群人，他们掌握着信息安全科研领域最前沿的技术，了解信息安全科技领域的每一处细节，知晓产业最新的热点，洞悉产业动荡背后的本质。他们，就是信息安全国家重点实验室的研究人员。

他们究竟每天做些什么？他们研究的领域究竟如何推动产业发展？这个实验室成立的初衷是什么？它的价值究竟体现在哪里？它为我国信息安全人才的培养做出怎样的贡献？一连串的问号，都将在记者大量的采访中得到解答。或许这不是针对信息安全国家重点实验室最全面的报道，但记者相信，在受访的这些研究员对答之间，在他们办公桌上厚厚的资料文案之中，在成果展示室那一本本著作一台台设备里，读者能感受到更多深入、精彩的正能量。

信息安全国家重点实验室专题之综述篇

是参与者，更是引领者

受访人：信息安全国家重点实验室常务副主任，研究员 / 博士生导师　林东岱

记者对林东岱老师并不陌生，在过去的采访中，他总能够针对记者提出的一些信息安全热点问题侃侃而谈，逻辑缜密滴水不漏。但这次请林东岱老师谈谈信息安全国家重点实验室的采访却明显不同，他的谈话中处处流露出的对实验室未来发展规划的责任感，甚至说到实验室目前研究工作时那种毫不掩饰的自豪感，让记者心生敬意。

做信息安全造梦人

“谈到信息安全国家重点实验室的名字，每次我都会很佩服前辈工作者前瞻性的眼光。”林东岱老师谈道，1989 年，在申请国家重点实验室时，当时领导就定下了用“信息安全”这 4 个字，事实证明，这 4 个字抓住了本质。这个信息安全领域唯一的国家重点实验室，立足于信息安全，经过两年建设期后，1991 年正式通过科技部验收，并对外开放。

在实验室走廊的两侧，挂满了实验室的成立情况和研究成果。记者发现，经过 20 多年的发展，实验室的总体定位依然未变：瞄准国际信息安全学科发展前沿，密切结合国家信息安全战略需求，进行信息安全前沿性和前瞻性科学问题创新性研究和自主信息安全关键技术研发。

记者也在实验室简介的墙板上找到了总体目标：为国家信息安全保障体系建设提供理论指导和科学依据，对前沿性和前瞻性信息安全科学问题进行创新性研究，以促进和推动信息安全学科的发展，研发具有自主知识产权的关键安全技术和系统，以满足国家和行业部门的需求，为国家培养高水平的信息安全专业人才。“实验室一直在向当初定下的总体目标努力，虽然目前仍然是最初规划的 4 个发展方向，但是其内涵在随着时代不断延伸和丰富。”林东岱总结道。

林东岱老师告诉记者，信息安全国家重点实验室不仅要做基础理论研究，更要研究信息安全关键性技术及其应用。“此外，还要为学者营造一个良好的学术环境，不仅能系统地培养人才，还能让他们能够潜下心踏踏实实做研究。”

5 年 5 大成果

虽然信息安全国家重点实验室主要的工作是研究信息安全中面临的各种问题，承担各类项目课题，但实际上实验室仍然有自己的运营压力。“每隔 5 年，国家相关部门就会组织专家组对各个实验室进行综合评审，排名最后就会被挂‘黄牌’，如果下一个 5 年评审依旧是最末，那么这个实验室就会面临被摘牌的风险。”林东岱老师解释道，每到专家组评审的时候，都会有很多硬性指标来衡量实验室成绩，例如人才队伍、取得的成果等等，过去还以发表多少文章为指标，但近几年越来越注重实际研究成果，例如获得多少科研经费、申请多少专利、产生多大影响……“在这些评测指标中，最重要的指标就是代表性的成果，即取得的顶尖科研成就。”


林东岱

2012 年，信息安全国家重点实验室刚刚经历过专家组评审，林东岱老师非常详细地阐述了实验室在 2007 年到 2012 年这 5 年中取得的 5 大代表性成果。

一是零知识证明及应用。林东岱老师认为信息安全中的一个最大的问题就是身份的确认，这就需要安全的认证协议。一个协议到底是不是安全的？复杂的网络环境下究竟存在不存在安全的认证协议？这是一个公开问题，被称为双重可重置猜想。在这个猜想被证明之前，虽然大家都在使用认证协议，但其安全性，特别是在互联网这种复杂的环境下的安全性并没得到理论的保障。实验室在零知识证明方面的工作可以说“是基础性、指导性的，为认证协议等很多研究都提供了理论依据，是非常有价值的研究成果。”

二是可信计算安全支撑平台及其关键技术研究与应用。可信计算是为解决平台完整性问题从系统架构层提出一个解决方案。实验室在这方面的工作受到了国家 863 计划、国家发改委高技术产业化专项的大力支持，突破了信任链构建与修复技术、基于安全芯片的远程证明协议、基于规约的测试用例自动生成方法等关键技术，成功研制了具有自主知识产权、技术先进的可信计算安全支撑平台，形成了支持标准符合性、安全性和实现特性的自主可信计算平台测评系统。相关技术成果已实际应用于企业产品，并在金融、科研等许多领域得到了实际应用。

三是网络信息隐蔽特征分析。将实现特定目的的程序、进程、信息或者通信隐藏于正常的操作或数据中，是网络攻击的核心手段之一，包括恶意代码对操作行为的保

护以及隐蔽通信对通信事实的保护。实验室在恶意代码和隐写特征的分析方面突破了一批关键技术，提高了对隐藏和异常行为的检测能力，增强了对恶意代码的描述和特征提取能力，完成了首个隐写分析计算机辅助设计系统，对新出现的隐写能够很快生成新的识别方法。

四是密码算法分析与检测技术。“实验室诞生于密码学，发展于密码学，可以说密码学研究是实验室的立室根本。”林东岱老师认为，密码的分析与检测需要很多的工作积累和经验积累。实验室近些年来在基础密码分析方法、实用密码测评技术、自主标准规范编制、先进基础平台研制与基准实验环境建设等方面，取得了一系列具有重要国际影响的创新研究成果，对密码的分析结果曾被两位设计者本人评价为“2000 年至 2008 年期间，对 AES 分析的最好结果”；许多研究成果也已成为国家密码标准体系的重要组成部分。

五是序列密码设计与国际化标准。这个领域的研究成果也是实验室长期积累的结果。实验室在序列密码研究方面有着优良的光荣传统，具有深厚的积淀和丰硕的研究积累。实验室面向第四代移动通信 LTE 的加密标准需求，主持设计了序列密码算法——祖冲之算法 (ZUC)，并和国家工业与信息化部及国家密码管理局一道在推动祖冲之算法的国际标准化方面做了大量的工作。目前，祖冲之算法 (ZUC) 已被移动通信领域最权威的国际组织 3GPP 采纳为第四代移动通信 (LTE) 的国际标准。这是我国密码算法首次走出国门成为世界标准。

这 5 大研究成果并不能涵盖实验室的所有研究，但的确代表了实验室研究的水平和方向。

新的起点新的机遇

信息安全国家重点实验室过去依托于中国科学院软件研究所和中国科学院研究生院，但是从 2012 年开始，实验室依托于中国科学院新成立的信息工程研究所。林东岱老师认为，信息工程研究所的成立是中国科学院因应形势的发展做出的一项战略决策，符合国际学术前沿发展方向和国家战略需要。研究所按照“软硬兼修，矛盾兼容，开合有法，张弛有度”的办所方针，秉承“打造一流平台，集聚一流人才，支撑国家需求，引领学科发展，努力成为国家在信息工程领域的战略科技力量”的组织目标，面向国家战略需求，在信息安全科技领域，开展基础理论与前沿技术研究，开发应用性技术与系统，为国家信息化进程提供核心关键技术支撑与系统解决方案。这些都与实验室的定位非常契合，因此新的环境意味着新的开始，全新的氛围更有利于实验室未来的研究和发展。

林东岱老师给记者介绍了一个目前实验室正在参与承担的项目，这是中国科学院的面向感知中国的 A 类先导科技专项，项目启动资金达 13 亿，涉及中国科学院 18 个研究机构。战略性先导科技专项是中国科学院在中国至 2050 年科技发展路线图战略研究基础上，瞄准事关我国全局和长远发展的重大科技问题提出的，集科技攻关、队伍和平台建设于一体，能够形成重大创新突破和集群优势的战略行动计划。分为前瞻战略科技专项 (A 类) 和基础与交叉前沿方向布局 (B 类) 两类。

林东岱老师表示，在专项中，人们将未来信息技术面临的挑战分为 4 类，一是能源能耗挑战；二是效率速度挑战；三是规模挑战，如物联网、云计算这样节点很多的网络应用；四是安全挑战。这个 A 类项目就是要研究和解决这 4 大挑战。信息安全国家重点实验室在其中承担了海云计算信息安全体系与关键技术的研究任务。

“关于这个项目，有很详细的考核标准，评判其研究是否是领先的关键技术，实验室每年都要论证研究课题，确定总体目标、阶段目标，确保技术的先进性，及在关键技术上有所突破。”林东岱老师表示，例如 CPU 与操作系统、智能信息处理、新媒体等等都是专项研究的领域。

在采访中，林东岱老师表示，现在的物理世界和计算机网络、和人已经紧密地结合在了一起，其特点就是“人－机－物”融合、“海－网－云”协同，海即是海量的客户端，网是网络，云是强大的计算云端，这也是实验室课题作用对象。“安全不是一个个独立的单位，必须是一个完整的体系，通过不同机制相互协调，构成一个整体。安全不再是建立体系之后需要去完善的环节，而是在最开始设计之初就融入到体系架构中来。”林东岱老师认为，实验室的任务就是研究其中的关键技术，最终提出一个解决方案。

采访最后，林东岱老师坦言，实验室是汇聚信息技术人才的地方，也是研究信息安全热点难点的中坚力量，实验室不仅要做信息安全产业发展的参与者，更要登高望远，做信息安全产业的引领者。

实验室一进门就可以看到中科院院长白春礼的题词

信息安全国家重点实验室专题之研发篇

研究务实 为了天堑变通途

编者按：这是记者采访生涯里第一次这么密集地采访多位专家学者。在记者大致相同的采访提纲下，不同研究方向不同研究领域的学者呈现的是完全不同的状态：或是见解独到先谋而后定，或是一针见血直击本质，或是惜字如金谨慎谦和，或是旁征博引视角开阔……

但无论是哪一种学者，记者发现，他们都存在一个特质，那就是务实。务实地研究，务实的课题，务实的为人师表……正是这种务实，让他们的研究为信息安全产业创造更大的价值。记者相信，他们眼中的信息安全，一定有更独特的视角，更深入的剖析层面。

专家谈之密码工程

受访人：信息安全国家重点实验室研究员、博士生导师 周永彬

信息安全国家重点实验室研究员、博士生导师 张 锐


周永彬


张 锐

张锐和周永彬都是密码学方向中研究理论与密码相结合的工程领域的教授。密码学是研究保护信息安全的科学，而密码工程学侧重于密码算法、协议等的实现。两位老师谈得最多的也是应用二字。

应用为本

张锐表示，同其他各种自然科学一样，密码学也是因为应用才诞生的，通过软件、硬件以及系统的实现，最终成为安全的应用。“例如，现在社会生活中应用到的智能手机、智能卡、信用卡芯片、门禁系统、公交卡都属于密码工程学研究的范畴。”张锐认为，密码学或者任何自然科学并不能单独解决全部实际生活中的安全问题，只有从系统层面、社会层面、工程学等多层面的办法相结合，才能解决各种复杂的安全问题。

周永彬是信息安全专家卿斯汉研究员的学生。同他的老师一样，周永彬的言谈逻辑缜密，非常有条理。他举了一个例子让记者更形象地认识到密码工程的重要性。他说核裂变是原子核物理学中的一条并不复杂的原理，任何一个物理系的本科生都可以掌握。但是，仅仅掌握了这条原理，并不能等同于就可以制造原子弹，因为原子弹制造不是简单的一个物理方程式所能代替的，还涉及到很多其他技术与工艺环节。实际上，原子弹的制造原理早已公开，但工艺技术却不易攻克。“同理，有了基本的密码算法（等价于有了基本的数学表达式），也不等同于现实中使用的密码设备和密码系统就一定是安全的。”他解释道，密码工程实践中需要密码学理论和技术，但在具体应用中，由于作用环境与作用方式等各种复杂因素的影响，即便理论上具有足够安全强度的密码算法，在实践中也不意味着使用这些密码算法的密码系统或密码设备就一定是安全的。实际上，多数情况下，将安全的密码算法简单应用于工程实践会带来许多意想不到的严重安全隐患。“密码工程学旨在解决密码系统构建工程实践过程中所需要的理论与技术问题，面向工程实践是它的显著特点。”

张锐也用了一个例子来解释不同应用场景需要不同的密码环境，这也是密码工程对应用的帮助。他以公交卡为例，像公交卡这样的大众应用，首先考虑的是成本，其次才是安全问题。如果盲目地去研发一套特别安全的系统，虽然可以大幅度提升公交卡的安全性，但是每张卡的成本需要增加上百元，运营成本增加几十倍，那么没有一家公交公司会考虑使用。但是，如果是政府的秘密档案系统，以安全保密 30 年至 50 年的标准来计算，那么即便是成本很高，投入大量资金研发也是物有所值的。

用作品说话

“信息泄露无处不在。”这是周永彬在谈及自己研究领域时说的第一句话。他的研究方向之一是

侧信道密码分析，这属于物理安全性研究的范畴，这个问题已成为密码分析学的一个重要分支。“例如，电磁辐射也会造成信息泄露。实践表明，通过监测智能手机产生的电磁辐射，就可以恢复出智能手机应用中所使用的(部分)秘密信息。”他告诉记者，信息泄露的方式多种多样，某国情报机构就曾经通过在另一个国家驻该国大使馆密码机旁的电话机上安装窃听器的方法，利用密码机上不同按键发出声音的微弱差异，破译了大使馆的大量通信。

周永彬谈到了实验室侧信道密码分析团队在DPA攻击研究工作中取得的成绩。他告诉记者，DPA国际大赛是国际密码学界与产业界共同参与的国际学术大赛，由法国高科电信学院等学术机构主办，始自2008年8月，目前已经进展到第四阶段，每一个阶段的主要技术目标均不相同。

今年3月份，由他带领的研究小组的一项DPA研究工作公开之后引起国际同行的关注，并被称为“原创性工作”。DPA国际大赛的组织者之一Sylvain Guilley博士主动给周永彬带领的研究小组发来邀请函，邀请将该项工作的一项成果作为一种“基准”提交给DPA国际大赛。周永彬认为原创性的工作非常重要，做这类研究最忌讳“闭门造车，孤芳自赏”，必须让国际市场听到中国的声音。“侧信道密码分析的实用性非常强，对于检测评估密码设备与密码系统的实际安全保障能力有很重要的现实意义。”

把阻力当动力

记者了解到，周永彬研究的这个领域，在国内已经处于前列，并开始引起更多国内外同行的关注。

其实说到国内外密码学的应用，周永彬也坦言会有不小的阻力。很多先进水平的电子辐射检测设备都不对国内开放，很多情况下，只能摸着石头过河，一点点钻研。对此，在2000年就出国做研究的张锐特别有感触。他从形势的层面对记者做了比较详细的分析。他认为，其实国内的研究环境并不差，在资金、学术氛围方面都不错。信息安全是一个比较特殊的行业，具有较强的应用背景，中国人要想在国外做比较深入的研究，就需要面临更加严格的审查，很难进入核心技术研究项目。

在国外待了十多年之后，张锐发现，其实回国能够做的更多，而且国内的信息安全产业机会更大，他可以分享一些国外的经验和教训，避免我们重复走弯路。

周永彬表示，设计密码系统就是要抵抗所有的攻击，这是一个看似不可能的任务，“但是密码学本身就是反常规，反传统的。我们的研究就是让理论成为现实，成为坚实的理论基础，而这恰恰正是密码学与密码工程学的魅力所在。”


薛锐


徐静


邓燚

专家谈之安全协议

受访人：信息安全国家重点实验室研究员、博士生导师　薛锐

信息安全国家重点实验室研究员、博士生导师　徐静

信息安全国家重点实验室研究员、博士生导师　邓燚

“安全协议是信息安全保障的灵魂。”这是薛锐谈到自己研究方向时的第一句开场白。在他看来，加密、解密都需要通过安全协议去实现和应用，多方主体使用的加密、解密才有意义。而安全的合作，多方主体考量的算法都离不开安全协议。“直观地说，登录网络密码而得到认证，这个过程就是依赖认证协议而体现的。”任何的安全保障系统都是依靠安全的密码协议为前提，所以说，安全协议是安全保障的灵魂。

密码协议的安全性主要体现在正确地使用密码学的手段，达到某个安全的目的。比如上面说的安全认证就是一个安全目标。安全协议好比一个要防盗的门，这里的防盗就是安全目的，而使用的锁就好比密码算法，这把锁安装在门把手附近，就可以与门框相关联起来，起到防盗的作用，但如果把锁(不恰当地)安装在门轴上，即使这把锁再牢固，也起不到任何防盗作用。如此可见，并非有了安全的密码算法就会必然地形成安全的协议。

安全协议就是密码应用的一个形式，它的目的就是保证保密内容的安全传递与处理，人们需要通过安全协议进行实体之间的认证、在实体之间安全地分配密钥或其他各种秘密、确保发送和接收的消

息的非否认性，“可以把安全协议看作一种服务手段”。

测评不能等于分析验证

薛锐告诉记者，目前安全协议研究领域有不少国家研究性项目，比如863项目，主要就是关于协议验证方面的研究。在实际环境中，除了攻击者的威胁外，安全协议本身就非常复杂，加上系统本身就会存在漏洞，因此要进行安全性的验证并非易事。理论很难与真正应用结合起来，达到预期的效果。

“目前，安全协议验证大多都是与国际上开放的协议研究相融合，如与欧洲、美国的系统建立联系。但是建立自己封闭的安全协议验证系统还比较少。”薛锐透露道，总体而言实用的系统很少。

在谈到安全协议领域的发展时，薛锐指出，在实际应用中，真正的安全协议验证和分析体系很少。很多机构的安全协议分析都是在偷换概念，实际上只是安全协议的检测。“事实上，检测无法保障安全协议的安全性，大多数情况下只是检测协议有无实现方面的缺陷，无从判断安全协议本身是否安全。”薛锐表示，这就好比校对一本小说进行翻译或评析，某些检测机构只能检测翻译版本的小说有没有与原版在语义上存在差异，但即便是没有语义差异，也根本不能说对原版本小说进行了评析，不能够指出其结构上的缺陷或思想上的优劣。

零知识证明

在信息安全重点实验室里，和邓燚一样，研究数学出身，转而投向信息安全专业的人并不少。邓燚研究生阶段学习的是基础数学，在进入信息安全国家重点实验室进行博士深造后，他选定了零知识证明作为研究方向。

“零知识证明”指的是证明者能够在不泄漏任何有用的信息的情况下，使验证者相信某个论断是正确的。例如，证明者可以生成两个很大的素数 p 和 q，做乘法运算得到 $a=pq$，然后向验证者证明 a 确实是两个素数的乘积，而不泄漏 p 和 q 本身。零知识证明在密码学中的应用价值是不言而喻的，此外，这一概念本身也给理论计算机科学带来了革命性的进展，如PCP定理和不可近似的发现。

记者问邓燚选择这个方向的原因，他坦言是因为这个领域进展缓慢，有一定难度，也就意味着有不少机会，可以让他慢慢研究。邓燚告诉记者，零知识证明这一概念是由麻省理工学院机电工程与计算机科学系RSA教授和以色列魏茨曼科学研究所计算机科学与应用数学教授Shafi Goldwasser、麻省理工学院工程学教授Silvio Micali和他们当时的学生Rockoff在1985年提出来的，Goldwasser和Micali教授也因此获得了今年的图灵奖。他们的研究为密码学从艺术变为一门科学奠定了坚实的基础。

涉及到应用时，效率可能是最优先考虑，行业应用尤其如此。而实验室的研究就是尽量在安全与效率之间把握住那个平衡点。例如现在的网络系统真的如他们所言非常安全，万无一失吗？邓燚笑称那很大程度是建立在用户信心的基础上，其安全性可能无法通过技术的考验。“理论研究与应用研究的鸿沟很大。”

理论研究需要成熟数学背景

薛锐在进入信息安全国家重点实验室之前学习的是数学，对抽象代数、数理逻辑、计算复杂性理论、形式化方法非常熟稔。而在他2002年进入信息安全这个行业后，他发现，用形式化方法描述安全协议非常有效。但事实上，既有数学层面的形式化背景，又有密码学安全协议的相关知识的全面人才太少了。

“从事密码专业的学生，再进行形式化方法的学习会很痛苦。而对于形式化方法专业的学生而言，密码领域的协议又是一个完全陌生的领域。”他坦言，安全协议形式化分析领域的人才培养还是一个任重道远的过程。

近代密码学就是数学加上计算机复杂性，在安全协议领域，需要纯理论研究去分析协议中那些进步的、精华性的东西。但也需要工程学去研究解决工程中遇到的难题，例如云计算。

记者了解到，研究员徐静也是学习数学出身。她认为数学基础对密码学研究非常重要，学数学出身转密码学方向有很多优势。她目前的研究工作主要集中于两方面：一方面是安全协议的基础理论研究，具体包括安全协议可证明安全性的基本方法论、新的安全论断以及推理证明技术、安全认证器的构

造和基础安全假设的选取等问题；另一方面是实用安全协议研究，具体包括传感器网络密钥管理协议的设计与分析方法、云计算环境下隐私保护协议的设计与分析方法、异构网络融合的设计新思想等。

专家谈之网络安全

受访人：信息安全国家重点实验室研究员、博士生导师　武传坤
信息安全国家重点实验室副研究员　徐 震

武传坤研究员是我国密码学知名专家肖国镇教授的学生，于 2003 年 1 月 1 日来到重点实验室，当时得到中科院百人计划资助。他表示，重点实验室是一个相当不错的平台，可以说是该领域具有引领地位的研究机构。刚来实验室时，他还继续自己过去的研究方向，即流密码相关的数学问题，也研究一些安全协议，特别是针对群组环境的安全协议 (群组密码学)。在此期间，考虑到中国经济的飞速发展，也不断寻找自己的研究能用在什么地方，他表示，如果偏重于理论研究就要有所创新，而如果偏重于工程，就要真正地做出应用，曾经也面临过思考和困惑。到 2009 年，武传坤研究员参加了国务院发展研究中心和中科院有关专家组成的《中国物联网产业发展研究报告》调研团，很看好这个方向，而且他判断，物联网方向将是未来一个非常有前景，也能够把理论应用于实际的一个方向，便很快把精力放在物联网安全这个研究方向上来了。

武传坤表示，产学研说起来容易，做起来难。信息安全方面的研究成果转化更难，一方面信息安全不是独立的产品，另一方面就是谁来买单的问题。政府部门对信息安全很重视，但最终都是企业在提供解决方案，而企业在信息安全领域的高度比实验室的研究还是有差距的，“ 但他们的实现能力较强，至少能很快拿出东西来，这是我们所缺乏的。为什么会有这种差距？我理解主要是考核标准的问题。对某些研究工作来说，研究成果要有 ‘ 创新性 ’，是不是有市场价值并不重要；而对企业来说，是否有创新不重要，能否赚钱才是目标。 ”

从长远发展来看，有创新的研究和能产品化的研发有机结合，才能产出具有竞争力的产品，包括信息安全 “ 产品 ”。 信息安全产品商业化程度不尽如人意的另一个原因是整个社会的安全意识较差。武传坤在报告中多次提到，对待信息系统的安全保护，不能亡 “ 羊 ” 之后才想到 “ 补牢 ”，一方面信息领域的 “ 羊 ” 亡之后都不能意识到，另一方面亡“ 羊 ”和“ 补牢 ” 的成本可能超出人们目前的想象。因此，应该把信息安全基础设施铺设到所有可能需要信息安全保护的领域，特别是物联网领域。


武传坤


徐 震

据了解，武传坤研究员所在的信息安全重点实验室，其中一个重要的方向就是物联网安全。物联网的安全不是一个很深的技术，而是现有技术的落地和实现，还关系到性能的问题，因为物联网还要考虑到安全和能耗的问题，所以原有的技术可能不实用。“ 这就需要设计一种新的方式，这个方式就需要一个很好的平台去测试，所以我们现在所做的工作就是在一个现实的平台中去设计、测试、实现，这样看起来好像没有什么创新，但是要满足可用。 ”

武传坤研究员表示，目前做安全的人很多，做物联网的人也很多，但是这两个方向的交集特别少。因为做物联网安全很难进行理论上的提升，如果不断地追求理论上的深度，可能就会走到一个很窄的范围内，而要满足工程上的实现，一般都会利用较为成熟的技术，这样又不能满足科研人员的创新要求，另外还有成本和风险的增加。“ 我们目前正在搭建这样一个环境，从而为未来的测试做准备。 ”

对于物联网安全，如果要追求很高的安全性，可能就要降低性能的提升；如何达到一个平衡，就要在这个环境中设计、测试、修改。所以现在做物联网安全的人很少，其实安全是物联网性能的一部分。任何事物都有两方面：物联网这方面很有前途，但是进展不是很明显。

云计算与智能移动终端

当讨论到信息安全热点研究时，徐震非常有自己的见解，他帮助记者了解到很多概念炒作背后的真相。就云计算而言，徐震认为云安全已经成为不容忽视的话题，他把云安全分为两个层面来分析：一是云自身的安全，二是用云的计算能力做安全的服务。“ 我认为国内的安全厂商应该更多关注第二点，这个领域还有不少发挥的空间。 ”

徐震表示，由于虚拟化、虚拟技术的核心技术都在国外厂商手里，这些厂商很早就开始布局，他们对

云计算的发展规模有详细的步骤，这个方面国内厂商的竞争很难与之抗衡。但是国内安全厂商依然可以充分利用资源，开发出更多云的安全服务，如网络防御，如杀毒软件厂商的云查杀。“中国互联网中对安全有思想的人很多，阿里云的数据分享和云解决方案都比较实用，不仅能满足自己的需求还能有自己的布局，这一点值得其他同行借鉴。”

除了云计算，徐震认为智能移动终端也是非常值得关注的一个领域。过去人们都是关注电脑的使用安全，但是随着智能手机的推广，其安全问题越来越为人所诟病。他透露，目前已经有基于硬件芯片的研发，能够对手机进行保护。“无论是 SD 卡还是 SIM 卡，都可以用专用的芯片，基于硬件加上虚拟化软件，最终实现安全可靠运行。”徐震表示，“未来移动安全将在支付环节上引发高增长爆点。”

专家谈之信息隐藏与版权保护

受访人：信息安全国家重点实验室研究员、博士生导师　赵险峰

赵险峰将自己的研究方向划分为两个方面，一是信息隐藏，二是数字知识产权保护。在记者看来，这是与实际应用结合得非常紧密的研究方向。

信息隐藏检测难易被忽视

他介绍道，过去保密通信都是通过加密来完成，但是，现在随着多媒体技术的发展，保密通信的方式发生了变化。由于用密码加密的方式传播信息，其保密通信的事实很容易被检测出来，而将需要保密的消息隐藏在多媒体信息中，通过公开信道传播，这就给检测带来很大的难度。“像一张照片、一段视频，其内容数据有很大的冗余，要想隐藏进去一些保密信息非常容易，而且并不会造成照片或视频的感知质量发生易察觉的变化。”

赵险峰说：“想在隐藏了机密信息的多媒体中找到隐藏的信息非常困难，有些网络上可下载信息隐藏工具，由于技术门槛较低，还相对容易提取出隐蔽的消息，但对较为高档次的信息隐藏方法，在缺乏授权的情况下，提取隐蔽信息的难度就很大了。当前，主要的分析方法仅仅能够判定信息隐藏的存在性。”

正所谓“道高一尺魔高一丈”，还有隐蔽通信工具通过网络包序列来隐藏信息，它们将网络包按照不同节奏发送，表面上看是一个个正常的网络包，但通过特殊的解析，接收者可以提取出传输的机密信息。“现在检测这些隐蔽通信的存在是重点的研究工作之一。”


赵险峰

“在信息系统等级保护中，要求系统的安全程度到了一定等级，就必须防止隐通道泄露信息，据查证，5 级以上就必须有隐通道保护，但是事实上，若把以上隐蔽通信方式也算作隐通道的话，目前这个方面的安全工作做得还非常不到位。”赵险峰坦言。

数字知识产权保护应重在事前

上世纪 90 年代末，随着数字多媒体应用的普及，数字版权保护的需求变得非常普遍。在这一点上，赵险峰认为，国外的一些举措非常及时，值得国内相关部门借鉴。“中国数字版权损失非常大，这是因为在运用数字知识产权保护技术方面没到位。”

在国外，数字内容生产企业的收入除了通过电视台获得外，还主要依赖于数字内容的直接售卖，如 DVD 发行或者在线点播。而中国的影视产业在这方面的收益比例较小，商业数字内容在网络上被大量散布。“一谈到对内容分发的版权保护，人们一般想到的是线路保护，实际上，线路保护只是一个方面，媒体终端更容易出现问题。终端保护国内还非常欠缺，而国外很早就针对电视终端安装或者改造了相关设备，制约转录以及非法的散布。”

目前国内的知识产权保护，主要通过事后追踪来追查责任，但是追踪起来会有很大的技术困难，事后追踪机制也不完善。赵险峰认为，与其通过法律约束，不如通过技术约束，在事前就为事件追踪提前做好技术准备。目前，知识产权保护技术主要通过在数字内容中隐藏难以去除的标志来实现这一点，这些标志一般被称为数字水印或者数字指纹等，通过检测它们的存在，可以验证版权所有者或者内容的购买者，从而约束非法的散布行为。

赵险峰还指出，数字媒体版权保护的一个特殊子领域是多媒体加密，他详细分析了多媒体加密与普通加密的区别。他告诉记者，多媒体信息量大，全部加密的成本高，但是，实际只需要加密多媒体编码中的一部分，或者扰动其编码过程，就可以实现快速的内容加密。

虽然在数字知识产权技术的应用方面还存在诸多问题，但是赵险峰依然有信心，他认为国家的重视程度在不断加深，未来这个方面的技术将得到更多人的认可。

信息安全国家重点实验室专题之人才篇

人才培养不是名利场

21 世纪什么最贵？人才！《天下无贼》中黎叔的这句话多多少少喊出了信息安全业内的心声。经常有企业在抱怨，很难招到“靠谱”的信息安全人才，可另一方面信息安全专业毕业的学生也叫苦不迭，因为他们即将遭遇‘史上最难就业季”。毫不夸张地说，人才培养与人才运用，是信息安全产业未来很多年内都亟待磨合的课题。

过去人们常说的人才培养，其实包含了两个方面，一是指教书育人培养人才，二是指招纳人才后，如何提供一个环境让人才发挥。记者采访的信息安全国家重点实验室学者中，有的人是刚做完博士后没有几年，有的人已经在研究员的岗位上传道授业十余年，对于人才培养，他们显然有很多心得体会可以谈。

不拘一格降人才

《史记 · 鲁周公世家》记载周公“一沐三捉发，一饭三吐哺，起以待士，犹恐失天下之贤人”。后来，“吐哺握发”这句成语就成了求贤若渴的代名词。记者想来，把这句成语用在信息安全圈子内也恰如其分。

林东岱老师告诉记者，信息安全国家重点实验室现在有 103 名科研人员，其中研究员有 24 人。信息人才的汇聚对实验室开展工作也是一大助力。“实验室成立以来，已经为国家信息安全领域培养了一批优秀人才，他们的足迹遍及国家机关部委、研究机构、高校、IT 行业、银行证券系统等各部门，成为活跃在信息安全领域的一批骨干力量。”林东岱老师告诉记者，对于那些十分优秀的人才，实验室也会尽力挽留下来。2008 年，研究员邓燚当时在中国科学院软件所读博士毕业，后来在零知识证明领域研究取得非常好的进展，不仅在欧密会上，还在知名的理论计算机会议上发表论文，他还获得了中国密码学会首届优秀青年奖，今年又破格聘任他为研究员。

“我们努力给人才提供一个宽松的环境，即使有运营压力，也尽量不会干扰研究人员正常的研究方向。”林东岱老师的这番话被很多研究员证实。张锐表示，实验室给研究人员比较大的弹性空间，学术氛围浓厚。徐静认为实验室研究队伍实力强，这也是当时加入其中的一大吸引力。

学术是一个奢侈品

邓燚研究的是基础理论，他坦言，在目前国内大环境下，很少人能够潜下心来做研究，理论研究这方面在很多方向上缺乏学术传承，但是像中国这么一个大国完全没有学术研究也很难想象。“纯学术研究并不需要太多人来参与，理论研究本身就是一个奢侈品，不是每个国家都能买得起单的。”他认为中国的密码学基础还比较薄弱，要想构建一个强大的学科，可能经过一两代人的努力都不够，幸运的是，这种情况正一点点好转。“我作为其中的一员，希望能起到一点作用，让学生看到除了金钱物质上的追求，还有学术上的价值值得推崇，这儿就是老师的价值。”

实验室为国家输送了大量人才

正因如此，邓燚认为人们都谈人才培养，其实真正的人才并不需要刻意培养。“老师能够做的，就是为其提供土壤、阳光、水分，只要条件具备，他自己就能长成参天大树。”在邓燚看来，培养学生对研究领域的兴趣非常关键，他认为老师的职责，一是要尽可能去点燃学生对学术的激情，二是提高学生对研究方向的品味，如研究价值、研究方向等。

不做家长式老师

张锐告诉记者，在美国，大学与企业的结合很紧密，很多公司都让大学研究相关课题，学术方向与应用密切结合。在日本，主要由政府指导项目，公司接下项目后，与大学研究结合，都有产出。但由于是政府项目，在时间上没有刻意追求，学术研究的周期也比较长。在欧洲，国家对学术的影响更大，公司参与到大学中的也有，二者不分伯仲。

“不论是采取何种方式，其实每种制度都有大量的诺贝尔获奖者一级的人才出现，中国的教育方式也有优点，很多传统的教育模式也非常值得推崇。”张锐补充道，他个人认为对于人才的培养，谁主导实际上无所谓，只要是真正懂的人在主导就会达到事半功倍的效果。此外，集体决策以及百花齐放总是能够促进创新。

当然，目前的教育也存在一些弊端，张锐阐述道，目前国内对人才的培养方面，眼光还不够长远，功利心较重，而一旦人有了功利心，就很难潜下心做研究。他认为在培养学生时，导师有责任把除专业外的其他可能性尽可能地罗列出来，不要家长式地去管理学生，而是应该正确引导，告诉学生真正有价值的东西在哪里，在一定范围内，让学生自己选择。所谓良师益友，说的正是这个道理。

这与徐静的做法不谋而合。她主要是根据不同学生的特点来培养学生。对于学习能动性强、基础扎实的学生，徐静不给他限定研究方向，鼓励他自己找问题，然后不断地讨论与交流；而对于基础一般的学生，徐静的指导可能更细一些，会给他一些具体的学习要求和学习内容。“我希望最终学生学到的是一种科研的能力。目前具有创造精神的顶尖人才奇缺并不是信息安全领域存在的问题，而是我国学术界面临的主要问题。这需要的是大环境的改善以及整个教育体系的反思。”

教育机制待改善

其实，对整个教育体系的反思引起了不少人的共鸣。武传坤告诉记者，他是从理论转向工程，曾经两次招收实习生，但遗憾的是两次都半途而废。“我不认为中国信息安全方面的人才培养有什么问题，归根结底还是考评机制的问题。”他解释道，研究生毕业要有论文发表，导师只能让学生完成这一指标；工程类研发项目需要专利指标，导师也必需完成这一指标，于是制造了很多不切实际的论文和专利。但是他认为，“这不是我们的错，甚至不完全是坏事，适当调整后可以变成好事，比如更多地考核论文质量而不是数量，把对学生的要求转嫁到对导师的要求，由导师主要负责学生的质量，工程项目要看后续市场化（或产业化）程度，这样做可能会产生这样那样的问题，但总体上会引导出更多精品论文和精品专利。”

希望教育机制略加改善的还有赵险峰。他告诉记者，单从硬件条件来看，国内很多大学和研究所的条件其实比国外要好，无论是学生的办公学习环境，还是网络基础设施都比国外优越。但是国外有比较成熟的奖学金制度，一般研究工作做得好的研究生可以通过获得奖学金免除学费并能够接受课题经费的资助，其待遇与未获奖学金的学生相差较大，更利于形成激励机制。

“对待学生要因势利导，我把学生分为两种类型。一类学生是兴趣型，这类学生特别喜欢钻研，荣誉感非常强。另一类学生是应用型，希望能多学技术，将来能够在企业用上学到的技术。”赵险峰表示，学术研究与其他专业不同，对专业领域有兴趣非常重要，这也能使人的能力增加，学术界单枪匹马、千里走单骑的人并不罕见，对这类学生就要注重开发他的开创能力。第二类学生就要培养他的动手能力，与应用相结合。但无论对哪一种学生，他都注重两个层面的培养，一是理论结合实践的能力，二是创新思维的能力。

勤能补拙

薛锐在到实验室之前就曾经当过一段时间的老师，在他身上，那种为人师表的感觉非常明显。他告诉记者，他非常愿意授课，密码学理论是非常复杂性理论的研究，他愿意将自己的心得传授给学生。“在授课的过程中，准备和讲授知识对自己也是一种梳理，一种再思考和体验，既要深入浅出讲清楚，又要详略得当让学生理解接受。这不仅要求学生静下心来学习，而且也要求老师必须静下心来做教学。”

薛锐最看重学生的主动性，他认为勤能补拙，老师能做的，可能只是去告诉学生可以读哪些文章，该如何理解问题，但有主动性的学生就会多阅读文章，锻炼自己解决问题的能力，完善自己的个人背景，充实自己的知识结构。

宽有边 严有度

与薛锐不同，周永彬当上老师其实是背离了当初的梦想。出身于教师之家的他，大学毕业后最不想选择的职业之一就是教师，因为他从小就切身感受到社会对教师这个职业的种种不尊重。但是，偏偏阴差阳错，博士研究生毕业之后他选择当了老师，而且一教就是十几年。他从柜子里拿出几本厚厚的讲义，几十页厚的讲义上密密麻麻全是他的标注。“两个小时的课，可能我要用两天甚至更多的时间去准备。虽然这些知识已经烂熟于心，但是我还会重新准备，做足功课，力争把最新的资讯准确地传递给学生。”

他用 4 个词来表达自己对学生的期望：敬业、诚信、乐群、感恩。同样，他也时刻审视自己，看自己有没有做到。“敬业，就是对自己选择的职业尽职尽责，‘做一天和尚，就坚决撞好一天钟’。我自己招收的研究生一进入实验室，我就会给他们 3 个月的时间，让他们就环境、管理方式、学习方向发表看法，提出意见，而后做自由选择，甚至换导师都可以。3 个月之后，确定研究方向，就必须对自己的选择负责，我会尽心尽力辅导他，告诉他我的意见和经验；但是，更多情况下，我会与他们分享我个人所经历的失败与教训，旨在给他们一些启发与思考，并希望他们在未来的人生道路上不会或避免我所犯过的那些错误。”

对于乐群，周永彬也非常看重，他认为这就是一种团队精神，大家要在一个团队中学习，必须要具备团队理念，从团队利益出发。“我认为要与学生充分地沟通，鼓励学生讲出自己的看法，敢于讲真话，我作为导师，就从

来不对学生讲假话。”周永彬略加思索，“我希望将来学生能够并且敢于做一个有风骨的知识分子，而不是流于表面做人圆滑。”

对学生的关爱和培养，不仅仅只是学习，学生的为人处事周永彬认为自己同样有责任去指点。在他的电脑里，有一封学生在 2012 年教师节发给他的邮件，这位学生现在就读美国范德堡大学攻读博士学位，她在邮件里写到，“感谢您在我硕士 3 年中给予的指导与帮助，更加感谢您对我的严格要求、批评与包容。没有您的要求和批评，我可能要很久以后才能发现自己在学习与做人上的陋习；而您的鼓励和包容，则给了我继续前进的动力。”周永彬坦言，有学生的这句话，他觉得付出有了回报，再辛苦也值得了，他认为“这是我 2012 年教师节收到的最好礼物”。

采访快结束时，周永彬拿出了档案袋，里面有一本简易装订册。他告诉记者，这是他所有带过的研究生的论文评阅书与答辩决议复印件，记者看到，每一个学生的论文评阅书与答辩决议后面，都有评语专家与答辩委员会专家的评语，这些复印件被整整齐齐梳理成册。记者不解，问他这样做的目的是什么，他告诉记者，“在我看来，这是学生的青春岁月，也是我的青春岁月。这些材料部分见证了我们师生共同度过的青春岁月。”

科研成果及获奖情况

至 2012 年底，实验室在科学研究、人才培养、学术交流、专利申请、科研成果转化等方面取得了丰硕成果。

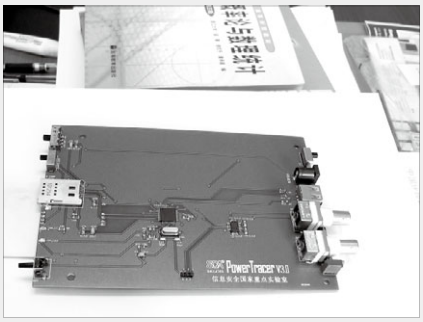
在密码理论与技术、PKI 技术、可信计算、网络安全关键技术、安全协议理论与技术、入侵检测与监控技术等方面取得了一系列重要成果，其主要成果达到了国际先进水平。

获奖情况

国家科技进步一等奖 1 项
国家科技进步二等奖 5 项
国家自然科学三等奖 2 项
省部级一等奖 10 项
省部级二等奖 7 项
中国科学院青年科学家奖 1 项
国家重点实验室计划先进个人奖 1 项
中国科学院第五届十大杰出青年奖 1 项
中国密码学会优秀青年奖 1 项

专著 (译著) 和学术论文

在国内外学术刊物上发表论文 2 700 多篇
出版专著 73 部
译著 14 部
主编会议论文集 16 部
发明专利、软件著作权
撰写国际标准 4 项
取得软件著作权 226 项
取得国家发明专利 76 项


侧信道分析研究用的芯片模板


一本本书凝结着实验室的心血


展示室里罗列着大量的成果