



中国科学院大学

University of Chinese Academy of Sciences

网络空间安全学院

School of Cyber Security

科教融合培养网络安全三型人才

中国科学院大学网络空间安全学院副院长 邹维

2019.8.23 北京

- 一 分类培养的背景
- 二 分类培养模式
- 三 分类培养案例



中国科学院 — 国家战略科技力量

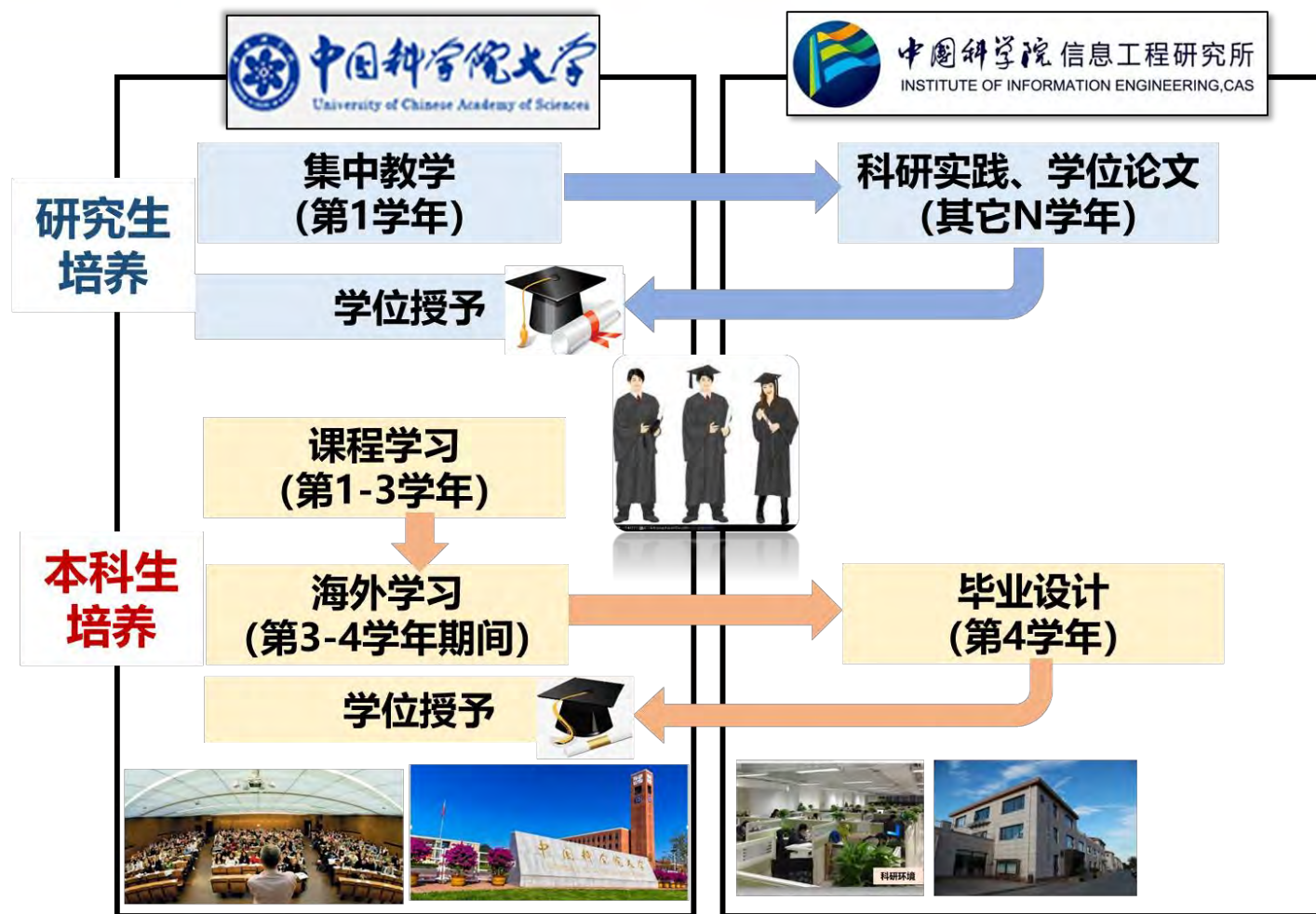
- 科研团队近10万人
- 在校研究生近5万人
- 每年毕业研究生1万名



中国科学院大学 网络空间安全学院

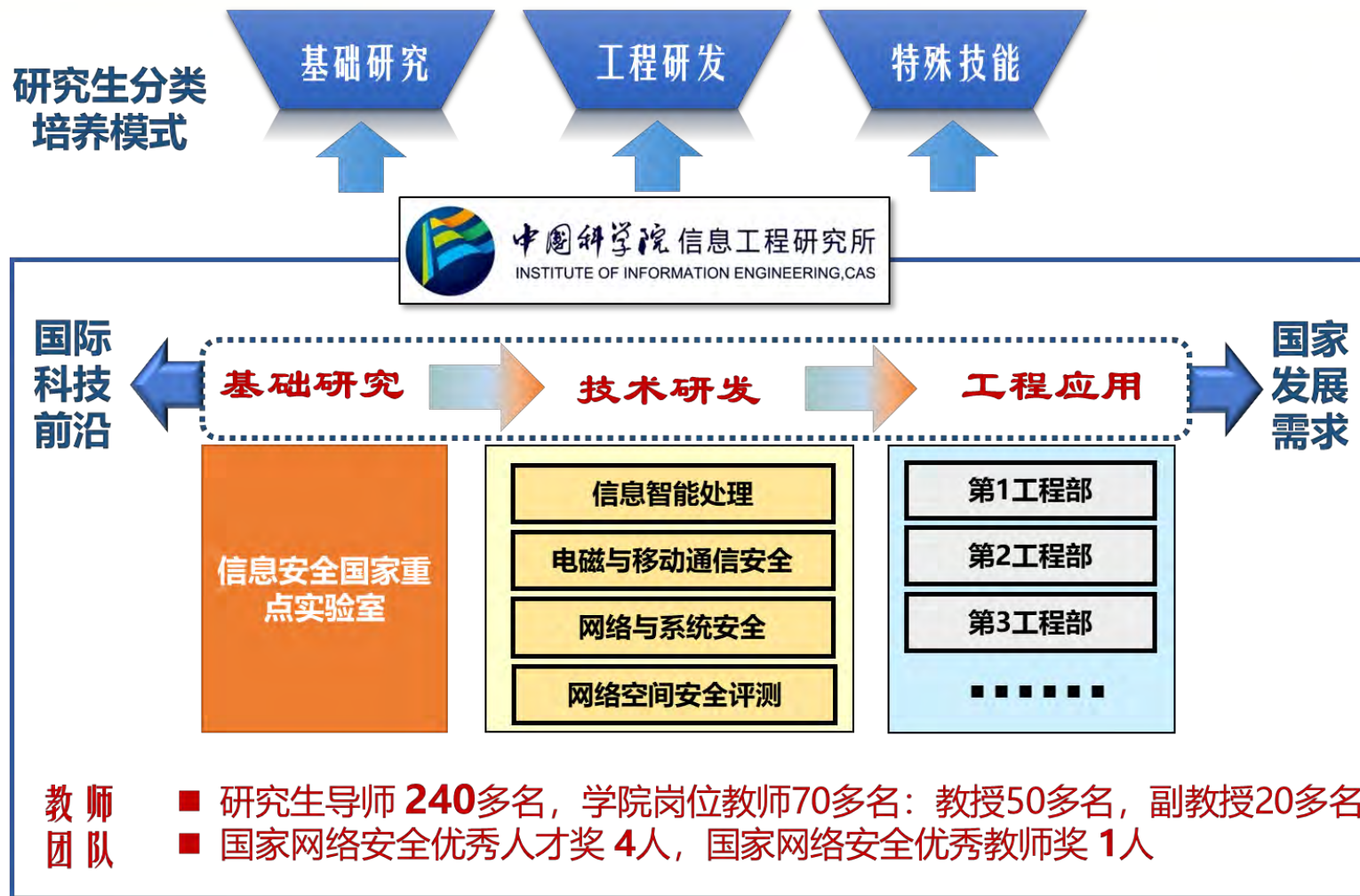


网安学院 学生培养三步曲



网安学院研究生 学位培养环境

在读研究生 1300多名
博士生 600多名
硕士生 700多名



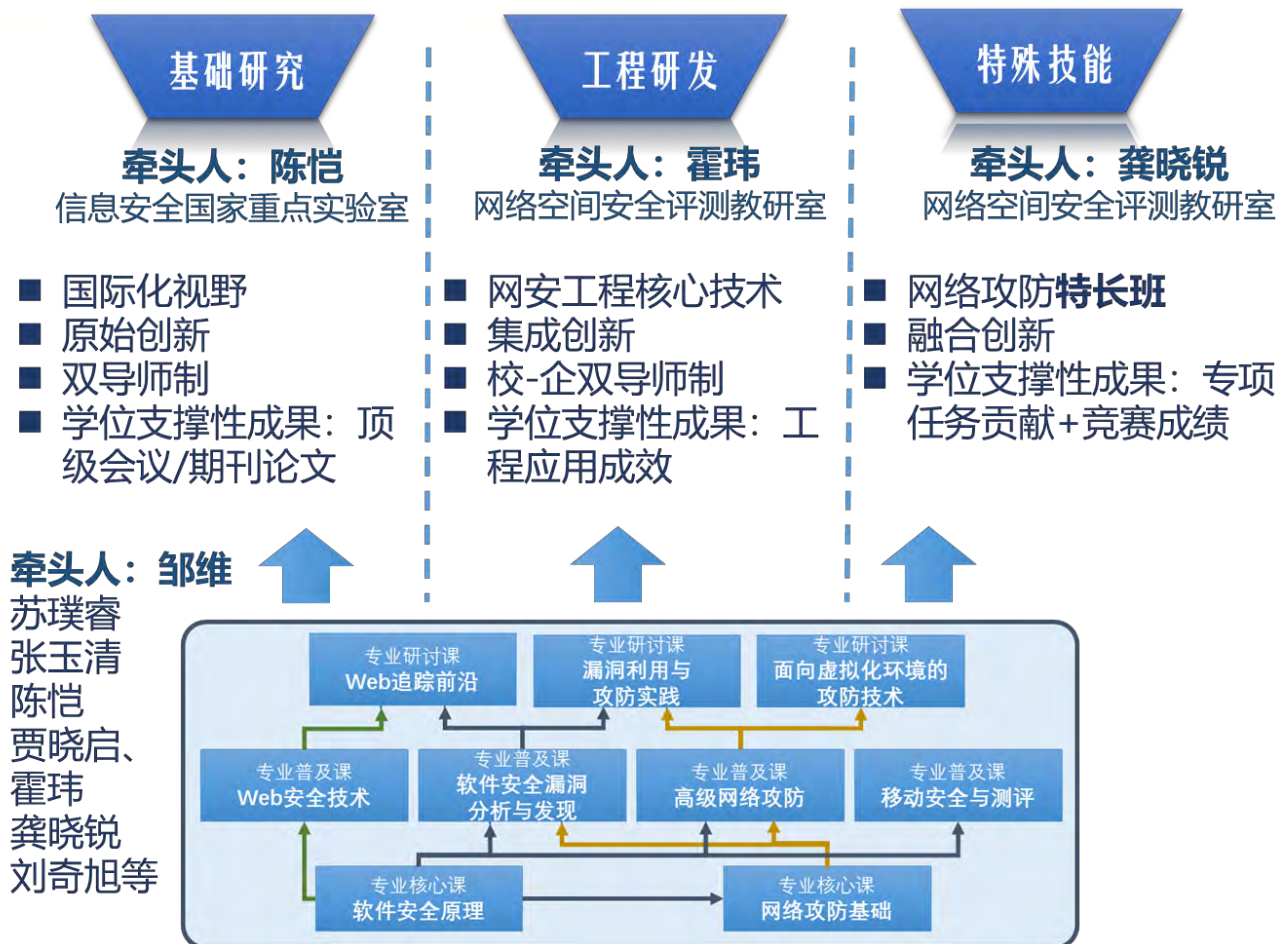
分类培养机制 (以网络与软件安全为例)

培养
类型

培养
团队

培养
模式

支撑
课程



中国科学院大学
University of Chinese Academy of Sciences

网络空间安全学院
School of Cyber Security

学院特色课程 软件安全原理

授课 团队



贾晓启
教授



邹维
教授



陈恺
教授



霍玮
教授

邹维 课程首席教授

- A类岗位教授
- 中国科学院大学信息技术学科群学位评定委员会委员
- 国家网络安全优秀人才奖、中国科学院“百人计划”
- 北京大学/中国计算机学会优秀博士论文指导教师
- S&P 2013程序委员会委员

课程特色

- 重新认识软件
- 软件安全三部曲
- 访名师、读名著



学院特色课程 软件安全原理



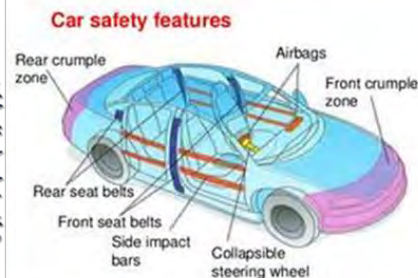
学院特色课程 软件安全原理

软件安全三部曲

软件安全防御原理

从“白帽”（white hat, 安全防御者）视角论述软件的安全防御机制及其博弈演进。

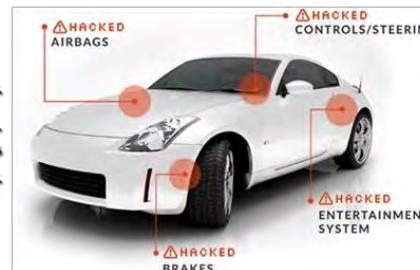
从安全保护者角度研究安全加固方法



软件代码攻防之道

从“黑帽”（black hat, 安全破坏者）视角，论述软件存在的各种安全脆弱性问题，以及如何利用它们形成有效攻击。

从攻击者角度研究渗透攻击方法



参照汽车安全

内构安全(Building Security In)

论述确保软件安全的工程化实施方法。

从生产者角度设计、生产安全的汽车



汽车安全设计与试验、(安全)生产线



中国科学院大学
University of Chinese Academy of Sciences

网络空间安全学院
School of Cyber Security

学院特色课程 软件安全原理

访名师、读名著

中国
系统安全
知名学者
代表



沈昌祥院士



方滨兴院士



何德全院士



吴建平院士

美国
系统安全
SMR

取其精华
去其糟粕



Gary McGraw



Bruce Schneier



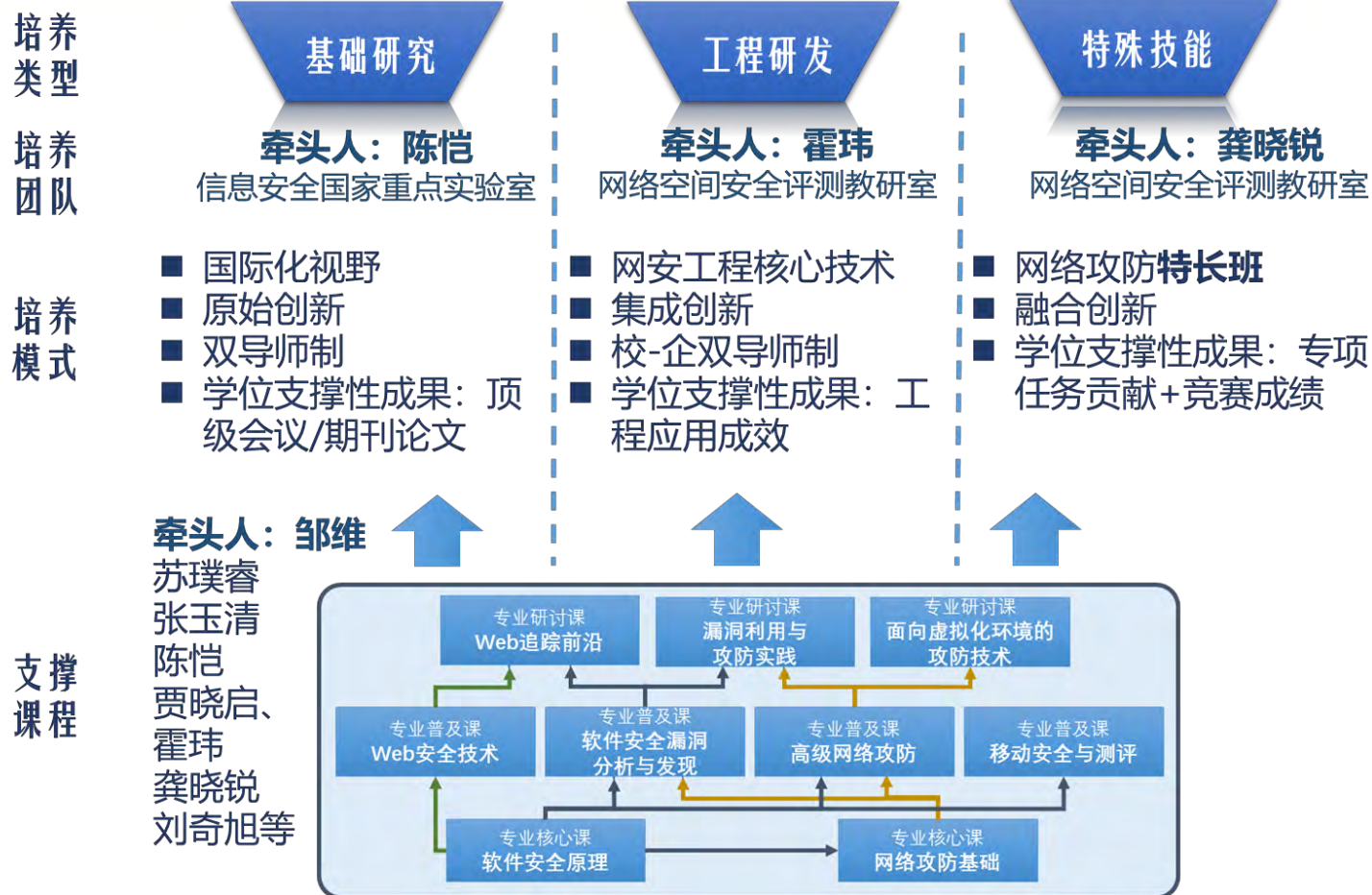
David Rice



中国科学院大学
University of Chinese Academy of Sciences

网络空间安全学院
School of Cyber Security

分类培养机制 (以网络与软件安全为例)



分类培养机制 (以网络与软件安全为例)

研 究
方 向

- 代码同源性分析
- 智能化漏洞分析
- AI算法脆弱性分析

国 际
合 作



优 秀
学 生



牵头人：陈恺教授

信息安全国家重点实验室

- 万人计划青年拔尖人才
- 北京市“杰青”
- 中科院青促会成员
- 论文IEEE S&P、USENIX Security、CCS等80余篇

- 导师：邹维
- 合作导师：陈恺、Xiaofeng Wang
- 论文：CCS 2017/ S&P 2019/ Usenix Security 2019

基础研究型



中国科学院大学
University of Chinese Academy of Sciences

网络空间安全学院

School of Cyber Security

分类培养机制 (以网络与软件安全为例)

培养模式

- 面向工程应用需求，导师、工程师与研究生密切协作
- 导师完成系统设计、分解技术难题
- 研究生突破关键技术、完成原型系统
- 工程师完成系统开发、测试、运维

科研平台



牵头人：霍玮教授

- 国科大网安学院教研小组成员
- 信工所软件安全分析研究群组负责人
- 中科院青促会委员，信工所优秀引进人才

工程研发型

优秀学生



博士研究生

方向：模糊测试种子样本智能化生成技术
论文：软件学报、信息安全学报



博士研究生

方向：自动定制化模糊测试技术
论文：信息安全学报、专利



硕士研究生

方向：可编程模糊测试技术
论文：软件学报、专利



硕士研究生

方向：模糊测试并行化技术
论文：EI论文、专利



中国科学院大学
University of Chinese Academy of Sciences

网络空间安全学院

School of Cyber Security

分类培养机制 (以网络与软件安全为例)

培养模式

- 网络攻防特长班
- 融合创新
- 成果：专项任务贡献+竞赛成绩

牵头人：龚晓锐教授

- 研究方向：逆向工程、网络攻防等
- NeSE战队发起人、指导老师
- 2018、2019年度某网络攻防演练裁判长
- 承担国家重点研发计划等项目



网络攻防特长班

CTF月赛锻炼技能

- 赛后组织技术讨论，分析赛题中涉及的技术原理，帮助大家快速掌握网络攻防技能
- 2019年推出网络攻防**本科**特长班



特殊技能型



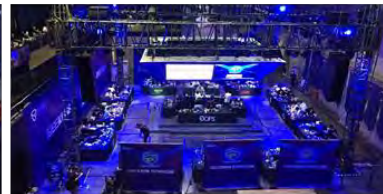
中国科学院大学
University of Chinese Academy of Sciences

网络空间安全学院
School of Cyber Security

分类培养机制 (以网络与软件安全为例)

网络攻防特长班

组建NeSE战队参加国内外竞赛
2019年受邀参加DEFCON China线下总决赛)



专项任务锻炼

- 在老师指导下担任外围分析员
- APT攻击样本逆向分析等

支撑全国高校网安联赛 X-NUCA



优秀学生代表

- 攻防对抗中艺术与科学的融合创新
- 解决Linux内核中UAF漏洞的自动化利用问题



BlackHat 2018



Usenix Security 2018

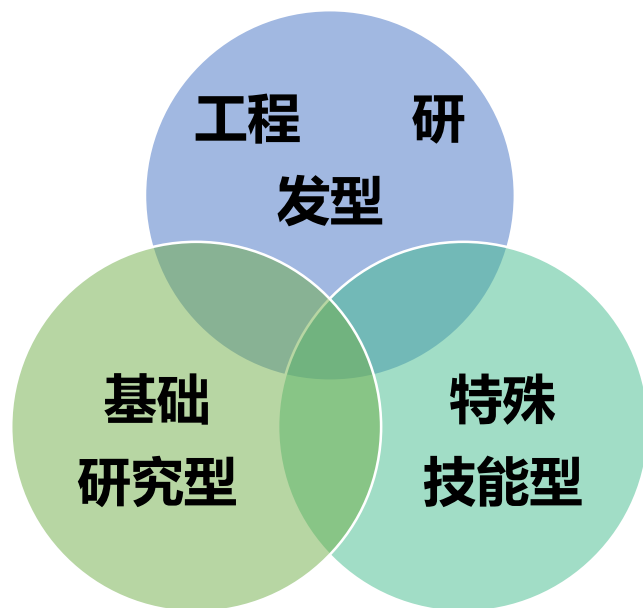
特殊技能型



中国科学院大学
University of Chinese Academy of Sciences

网络空间安全学院
School of Cyber Security

网安专业研究生 分类培养模式探索



- 面向国家和社会对网安人才的多样化需求
- 多维度认定学生学术能力
- 依据学生意向，因材施教
- 优秀学生可以跨类成长



感谢聆听 敬请指导

科教融合、育人为本、协同创新、服务国家



中国科学院大学
University of Chinese Academy of Sciences

网络空间安全学院
School of Cyber Security



2019北京网络安全大会
2019 BEIJING CYBER SECURITY CONFERENCE

网络安全人才论坛

多源化、实战化、行业化