聚力·引领
软件安全学术论坛

黑客心理学
——社会工程学原理

汇报人：陈玉玲
公共大数据国家重点实验室
2019年6月

聚力·引领
软件安全学术论坛

目录Catalog

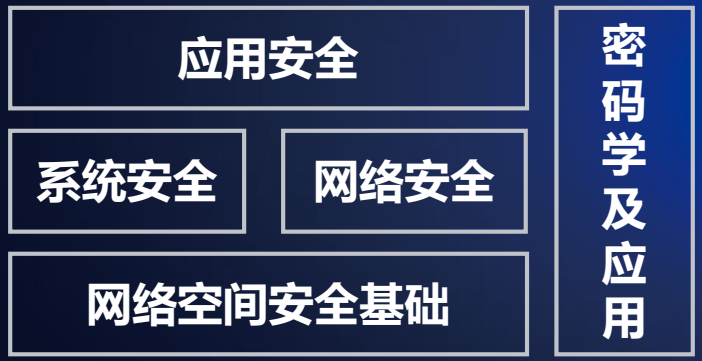
01.

聚力·引领
软件安全学术论坛

网络空间安全学科建设情况

1.网络空间安全学科建设情况

1.1 研究方向及关系



安全基础：提供理论、架构和方法学指导

密码学及应用：提供密码安全机制

系统安全：保证网络空间中的单元计算系统的安全

网络安全：保证网络自身和传输信息的安全

应用安全：保证大型应用系统的安全

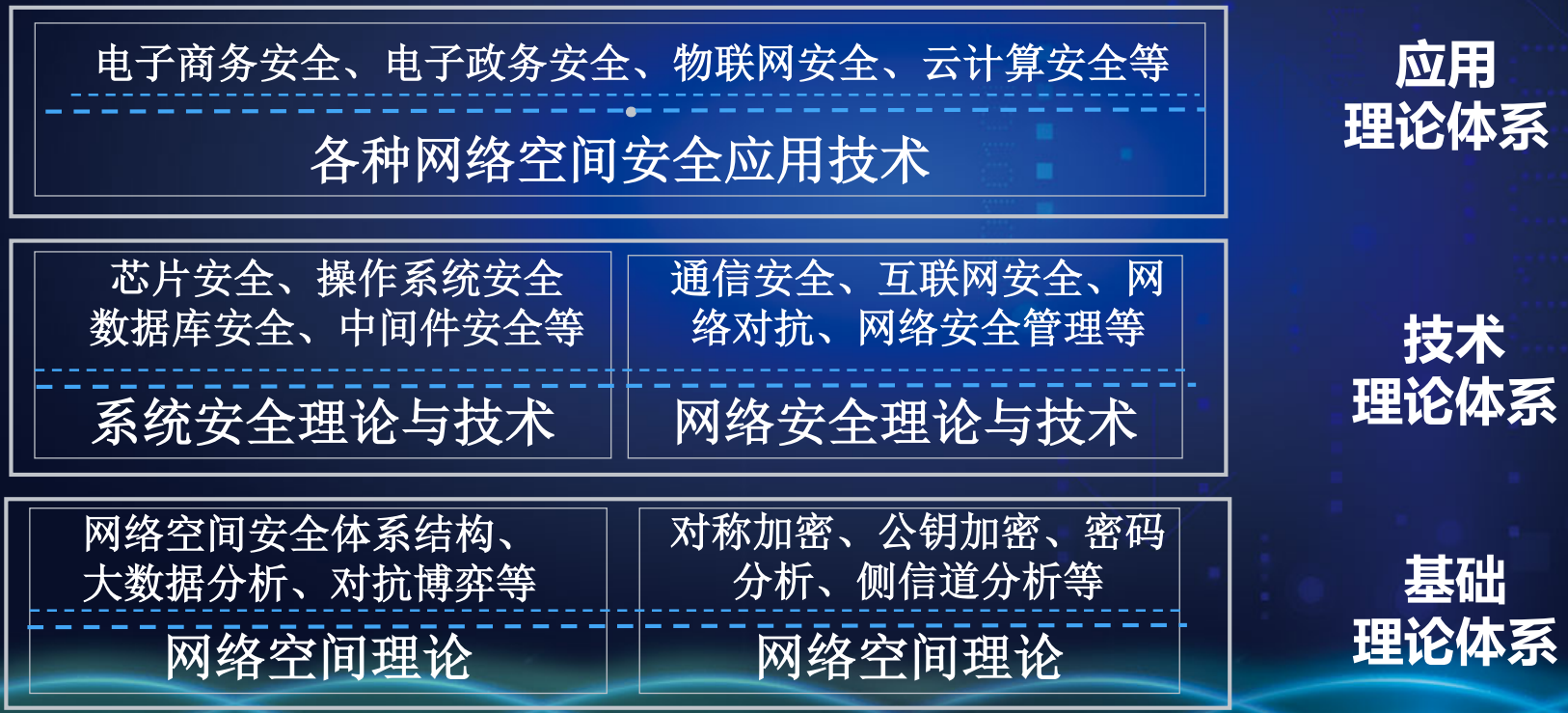
1.网络空间安全学科建设情况

1.2 主要研究内容

- 网络空间安全数学理论
- 网络空间安全体系结构
- 网络空间安全数据分析
- 网络空间安全博弈理论
- 网络空间安全治理与策略
- 网络空间安全标准与评测

1.网络空间安全学科建设情况

1.3 学科理论体系



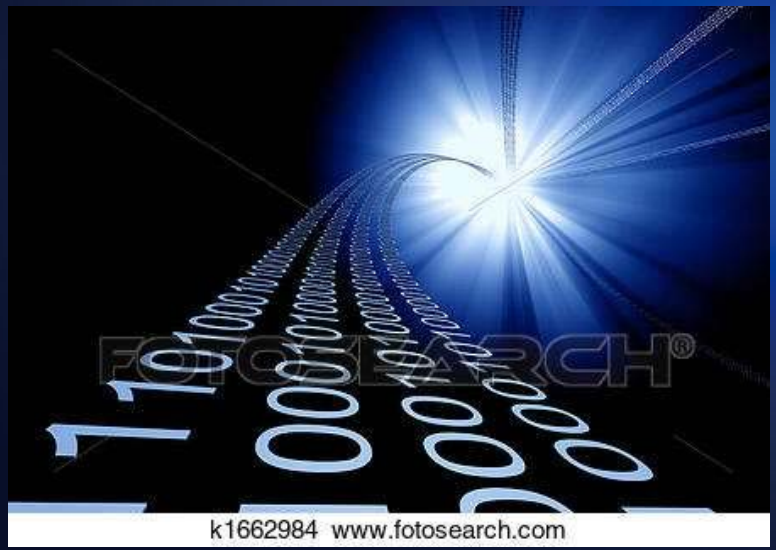
1.网络空间安全学科建设情况

1.4 学科论证专家

姓名	单位
吴建平	清华大学
吴中海	北京大学
李舟军	北京航空航天大学
杨义先	北京邮电大学
李建华	上海交通大学
王小云	山东大学
秦志光	电子科技大学
苏金树	国防科技大学

1.网络空间安全学科建设情况

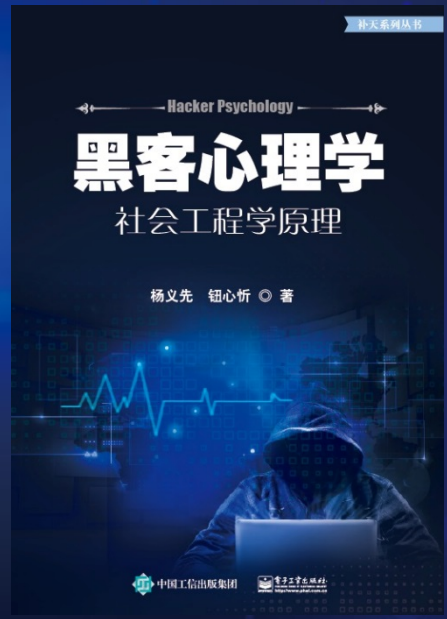
1.5 学科设置漏洞



《黑客心理学》《安全通论》《安全简史》《博弈系统论》

2017年和2018年 正式出版

2019年3月 正式出版



»"补天系列丛书"的体系

- 《安全通论》
  - 在理工科范围内，几乎没有任何限制（如设备、环境和人员等）的前提下，揭示黑客攻防和安全演化的基本规律，这些规律可以适用于网络空间安全的各主要分支。
- 《安全简史》
  - 外行不觉深，内行不觉浅的风趣幽默的**安全科普**。
  - 增强**全民**网络安全的意识。
  - 获得了2017年科技部“中国好书”等荣誉
- 《黑客心理学》
  - 填补全球信息安全界的一个重大空白，旨在努力实现人、网、环境**“闭环系统”全方位安全。**
  - 提高**全民**的防骗、防黑客意识和水平。
- 《博弈系统论》
- 黑客行为预测与管理

02.

黑客心理学

聚力·引领

软件安全学术论坛


卫视中国网


Ooops, your files have been encrypted!
我的电脑出了什么问题？
有没有恢复这些文档的方法？
Payment will be raised on
5/15/2017 20:44:36
Time Left
02:23:43:09
Your files will be lost on
5/15/2017 20:44:36
Time Left
06:23:43:09
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
Contact Us
Check Payment
卫视中国网

2.1 《黑客心理学》的动机

- 攻城为下，攻心为上；
- 攻网为下，攻人为上。
- 如何攻城，假假真真；
- 如何攻人，社会工程。

- 因此，黑客心理学的副标题叫“社会工程学原理”，即，从原理层次，穷尽所有可能的社工手段。

口 2.2 《黑客心理学》的背景（1）

但全球信息安全界，几乎都聚焦于网络或环境安全，而忽略了一个最关键的事实：

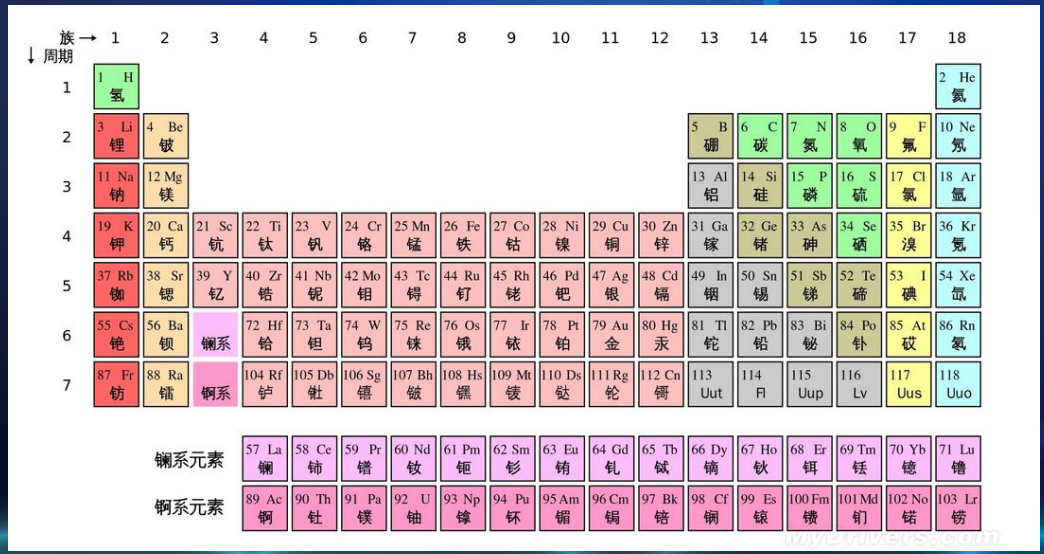
黑客是人！

- 反而是黑客们，常常基于心理学成果，利用“社会工程学”，来攻击“人”；

- “人”只不过是木偶，而人的“心理”才是拉动木偶的那根线；或者说，“人”只不过是“魄”，而“心理”才是“魂”

口 2.2 《黑客心理学》的背景（2）

- 所以，网络空间安全的根本核心，其实隐藏在人的心里。因此，《黑客心理学》希望借助心理学、社会学，来揭示信息安全的人心奥秘！



2.2 《黑客心理学》的背景（3）

- 在人、网、环境的闭环系统中，后两者“没天敌”，只需不断“水涨船高”就行；但是，**人是有天敌的**，人性的弱点有许多共同处，很难“打补丁”
- 总之，赢人者，赢天下；胜人者，胜世界！
- 由于“三种人”的目标、地位和能力等各不相同，所以，在网络空间安全攻防过程中，他们的心理因素也会不同。《黑客心理学》**重点探索最具网络特色的黑客心理**，因为，若无黑客，几乎就没有安全问题。但遗憾的是，黑客过去存在，现在存在，今后也将永远存在；甚至还可能越来越多！

2.3 黑客的动机、着眼点、机会

- 从心理学角度看，黑客行为的动机，主要基于如下几种心理：

自我表现　好奇探秘　义愤抗议

戏谑心理　非法占用　渴望认同

自我解嘲　发泄心理

- 反过来，黑客发动攻击时，又利用了被害者的哪些心理呢？归纳起来，至少有如下几种：
- 恐惧心理、服从心理、贪婪心理、同情心理
- 引发红客和用户不安全的心理因素，主要有：
- 省能心理、侥幸心理、逆反心理、凑兴心理、群体心理、注意与不注意

2.4 与安全密切相关的心理因素（1）

- 人的许多心理因素都与安全密切相关，主要有以下十类：

与安全密切相关的心理因素				
性格	能力	动机	情绪、情感	意志
感知觉	个性心理特征	气质	个性缺陷	行为退化

2.4与安全密切相关的心理因素（例如性格）

攻击型性格	性情孤僻	情绪不稳定	心情抑郁 浮躁不安
粗心大意	优柔寡断 行事鲁莽	懈怠	懦弱胆怯 没主见

2.5 黑客攻击行为的分类

- 网络黑客攻击是指，违背他人意愿，采取信息手段等非身体接触方式，以伤害他人（的财产或心灵）为目标的行为。
- 无论攻击行为是发生在网上或网下，黑客行为的最终效果都主要体现在网络空间中

- 按攻击目的划分，黑客行为可大致归类：

观点表达型

情绪宣泄型

利益诉求型

网络犯罪型

2.6 黑客攻击行为的本能说

- 本能说认为：攻击行为是由基因设定的，与遗传相关，它是人类为确保自身安全而形成的一种本能；这种本能经长期进化而来，攻击性强的个体，往往更具生存优势，
- 因此，按照本能说
- 黑客攻击是不可避免的
- 对攻击行为可定期加以发泄；以无破坏性发泄方式，代替破坏性发泄方式。

2.6 黑客攻击行为的非本能说

挫折理论

- 攻击来源于挫折
- 尽量不在网络中激发不必要的矛盾
- 构建和谐的网络社会

社会学习理论

- 攻击能力并非与生俱来、需通过后天学习获得
- 是通过观察榜样的行为及后果后学来
- 观察后，人便会形成攻击概念，并指导自己攻击行为
- 黑客的攻击行为，具有一定的传染性

2.7 黑客攻击意愿的弱化

2.8 社工黑客攻击的特点（1）

- 1）攻击的直接对象是热血的“人”，而不是冷血的“设备”，虽然可以运用各种设备来当武器。
- 2）是一种赛博式攻击，即，常常是需要与被攻击者之间进行多次信息互动，逐步诱导。
- 3）黑客与被攻击的“人”之间，并无直接的身体接触；所以，社工攻击的武器其实只是“信息”，攻击成果的表现形式也是“信息”。

2.8 社工黑客攻击的特点（2）

- 社工攻击，正在成为黑客攻击的必备手段；甚至，在所有重大黑客事件中，社工攻击几乎都是先锋队的主力军。
- 社工攻击的另一突出特点是：若你不了解它，那它将威力无穷；若你知道它正在攻击你，那你一定会逢凶化吉。

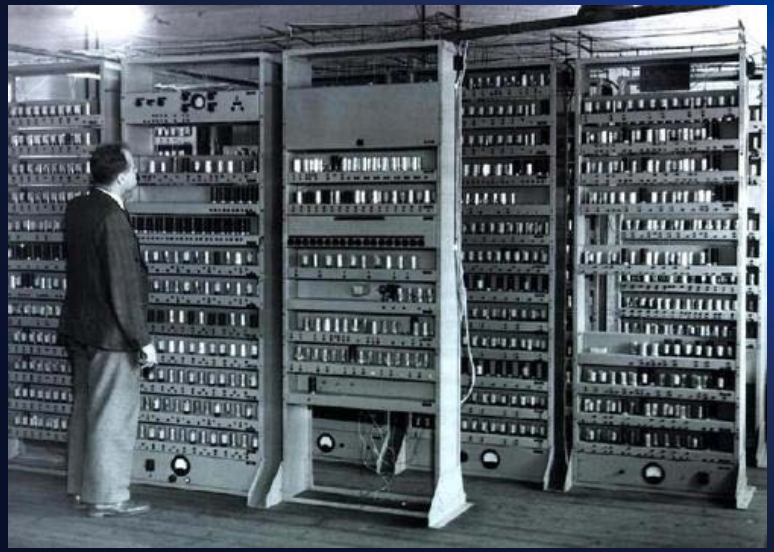
2.8 社工黑客攻击的特点（3）

2.黑客心理学

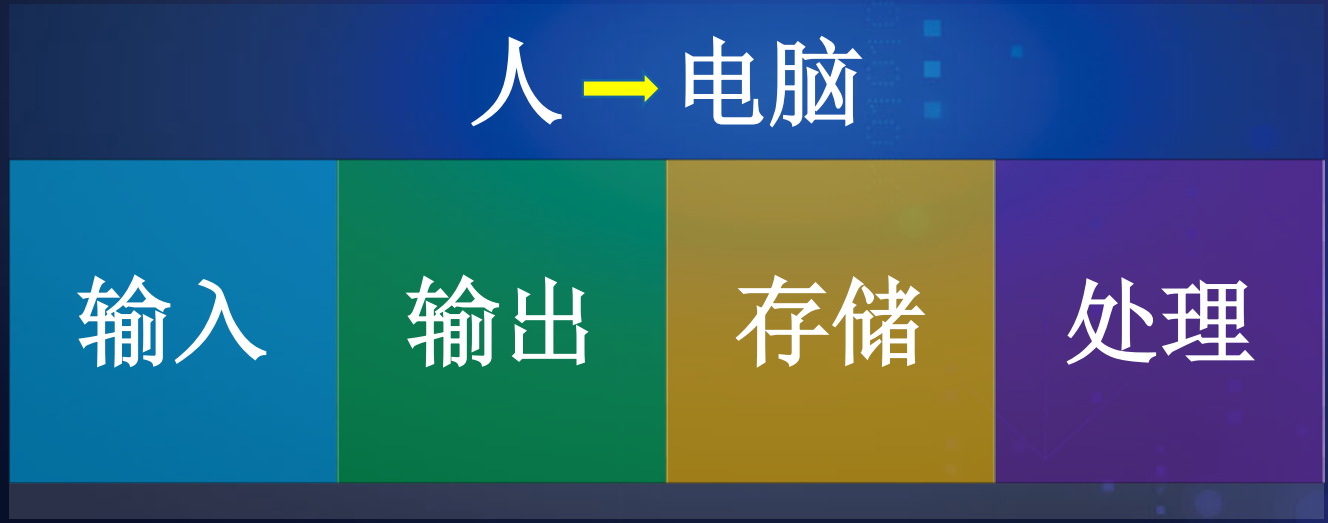
- 如果仅仅停留在外观层次，那么人类将永远无法搞清社工攻击的运行规律，更不知到底有多少种“社工攻击”手段。就像如果站在分子层次，人类将永远无法知道“世界上到底有多少种物质”一样；

- 但是，如果深入到元素的层次，那么，形成世界上所有物质的元素个数就少得可怜了，只需一张小小的“门捷列夫元素周期表”便能穷尽。

2.9 社工黑客如何看待个体（1）



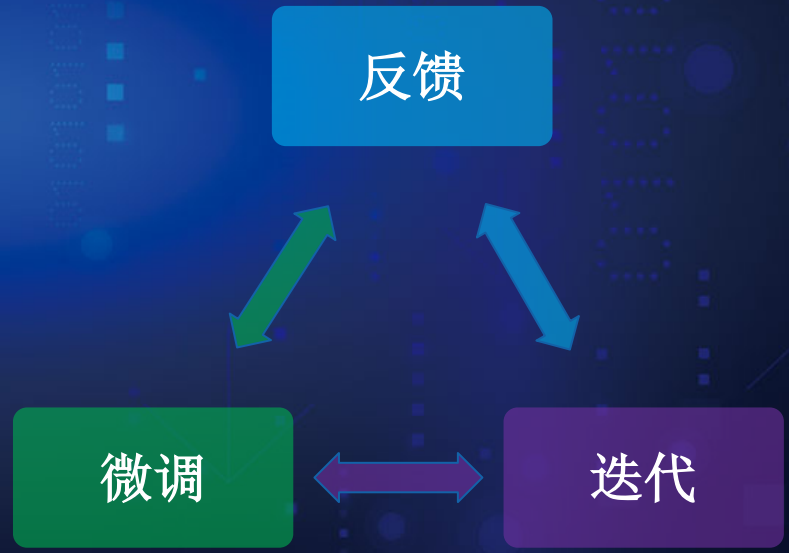
2.9 社工黑客如何看待个体（2）+社工攻击思路



2.10 社工黑客的漏洞思维（1）

2.10 社工黑客的漏洞思维（2）

- 从漏洞角度看，社工黑客比纯技术黑客处于更有利的地位；换位思考，安全更应该重视如何对抗社工黑客。
- 幸好，社工黑客的攻击，几乎都是循环反馈的“赛博式”攻击，所以，只要在其攻击过程中的任何一个环节，挡住了黑客，就算红客成功。



2.11 社工黑客的战术清单

- 感觉漏洞的挖掘和利用
- 知觉漏洞的挖掘和利用
- 记忆博弈
- 情绪博弈
- 注意控制
- 动机诱惑
- 微表情泄密
- 肢体语言泄密
- 姿势泄密
- 喜欢的引发和利用
- 利他与易控行为的利用
- 态度的控制
- 人际关系的利用和控制

03.

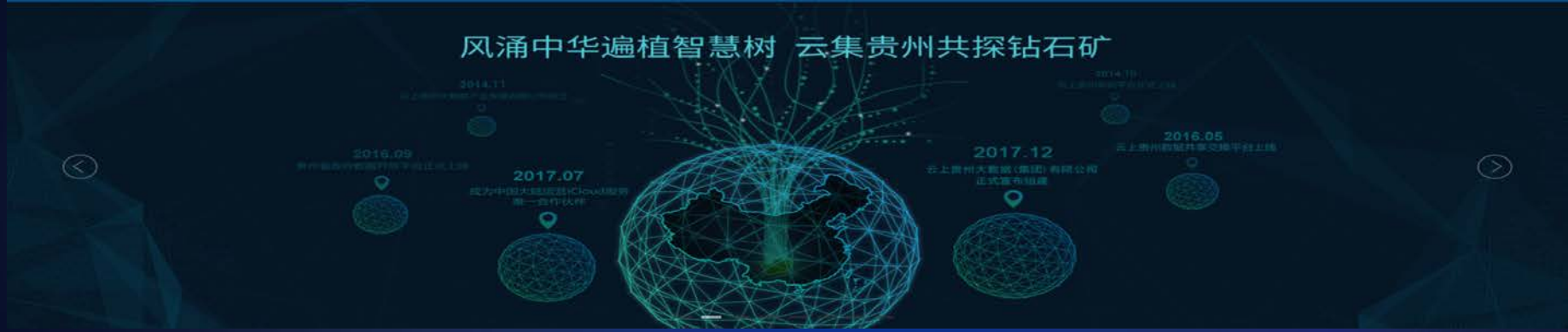
聚力·引领

软件安全学术论坛

公共大数据国家重点实验室介绍

3.公共大数据国家重点实验室介绍

1.实验室定位

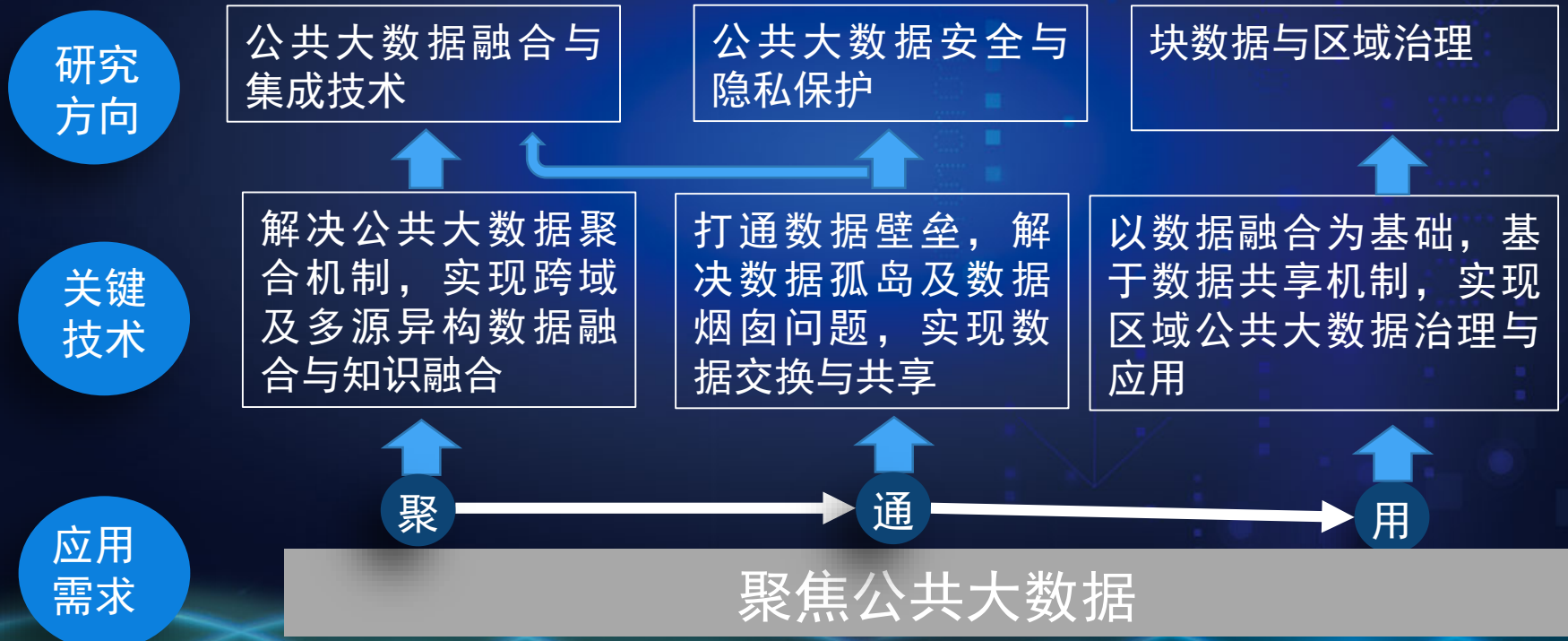


- 紧跟国家战略方向，立足贵州先行实验基础；
- 聚焦政府公共大数据的开放、共享和应用需求，开展基础研究和应用基础研究，解决政府数据“聚、通、用”中的共性关键技术问题，为国家大数据事业提供人才和技术支撑。

3.公共大数据国家重点实验室介绍

2.研究方向

关键共性技术与研究方向



3.公共大数据国家重点实验室介绍

3. 建设基础及优势

支撑单位及学科

依托单位

- 支撑单位：贵州大学（大数据与信息工程学院、计算机科学与技术学院、数学与统计学院、机械工程学院、管理学院、电气工程学院、物理学院、贵州省公共大数据重点实验室、贵州省大数据产业发展与应用研究院、现代制造技术教育部重点实验室
- 支撑学科：大数据科学与技术学科群国内一流学科（包括：软件工程、数学、电子科学与技术、机械工程、管理科学与工程5个一级学科博士点及其相关10余个一级学科硕士点）

共建单位

- 合作共建单位：北京邮电大学（包括：灾备技术国家工程实验室、信息安全中心、网络空间安全学院等）
- 伙伴实验室：北京邮电大学网络与交换技术国家重点实验室

省内单位

- 支撑高校及科研院所：贵州科学院、贵州师范大学、贵州师范学院、贵州财经大学、贵州理工学院、提升政府治理能力国家工程实验室等
- 合作企业及应用示范平台：云上贵州、国家大数据安全靶场（贵阳经开区）、食品安全云、中国电信、中国联通、智慧交通、健康云、宣传云和数据铁笼等

3.公共大数据国家重点实验室介绍

3. 建设基础及优势

硬件平台

- 科研用房：7600平方米
- 设备总值：6000万元

科研平台

关联平台

相关科研平台：贵州省智能医学影像分析与精准诊断重点实验室、贵州省先进计算与医疗信息服务工程实验室、贵州省数据保密工程技术研究中心、贵州省大数据分析技术工程实验室、贵州省博弈决策与控制系统重点实验室、大数据驱动下地方政府治理与运行监控研究创新团队等近20个关联科研平台支撑。

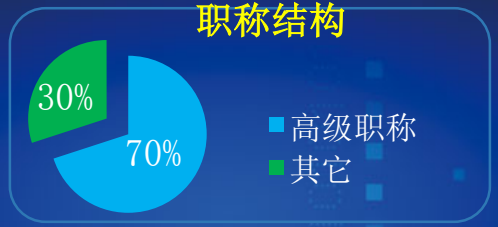
3.公共大数据国家重点实验室介绍

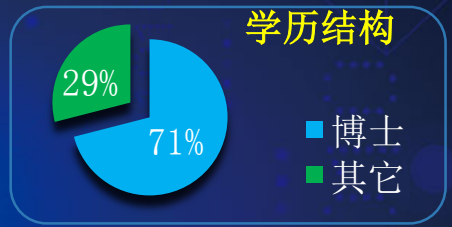
3. 建设基础及优势

科研团队

基本团队

总人数：76人
其中教授：52人
博士：53人





杰出人才

- 长江学者特聘教授2人
- 国家杰出青年基金获得者2人
- 中组部千人计划专家4人、青千1人
- 高被引科学家2人
- 教育部优秀青年科技人才2人
- 省管专家3人，百层次人才3人

学术委员会主任
梅宏 院士

实验室主任
杨义先教授，长江 杰青

3.公共大数据国家重点实验室介绍

3. 建设基础及优势

科研项目（近5年）

项目经费

- 项目总经费：科研项目数180余项，纵向科研项目总经费9000余万元

国家级项目

- 国家级项目：78项，经费6000余万元

省部级项目

- 省部级项目：共60余项，经费3000余万元

其它项目

- 横向项目、委托项目：60余项

- 国家自然科学基金重大研究计划培育项目
- 科技部国家支撑计划
- 国家自然科学基金面向项目、地区基金、青年基金等

- 教育部科研项目；
- 国家统计局、国家密码管局等科研项目
- 贵州省科技重大专项；
- 贵州省基础研究重点项目；
- 贵州省科技支撑计划；
- 贵州省自然科学基金；
- ……

3.公共大数据国家重点实验室介绍

4.管理创新与体制

机制1:创新模式-贵州省大数据领域技术榜单

- 3个项目
- 每个项目支持力度1000万元
- 签约全职引进项目成员，每年工作8个月，有相关匹配支持

贵州省科学技术厅文件

黔科通〔2017〕36号

关于发布贵州省大数据领域技术榜单的通知

各相关单位：

为贯彻落实全省科技创新大会的部署及《中共贵州省委 贵州省人民政府关于以大数据为引领实施区域科技创新战略的决定》（黔党发〔2016〕17

附件

贵州省大数据领域技术榜单

按照全省科技创新大会的部署及《中共贵州省委 贵州省人民政府关于以大数据为引领实施区域科技创新战略的决定》（黔党发〔2016〕17号）对“加快创建公共大数据国家重点实验室，着力突破大数据核心关键技术瓶颈”的具体工作要求，现发布大数据技术榜单。

总体目标：围绕贵州省大数据顶层设计中“以大数据提升政府治理能力、以大数据推动经济转型升级、以大数据服务改善民生”三个目的，开展高水平的基础和应用基础研究，瞄准大数据的“聚、通、用”，着力突破贵州省公共大数据应用中的关键共性技术问题，实现一批成果在贵州省转化。通过项目合作与研究，聚集和培养一支高水平的科研团队。

3.公共大数据国家重点实验室介绍

4.管理创新与体制

机制2：成立大数据学部支持实验室建设

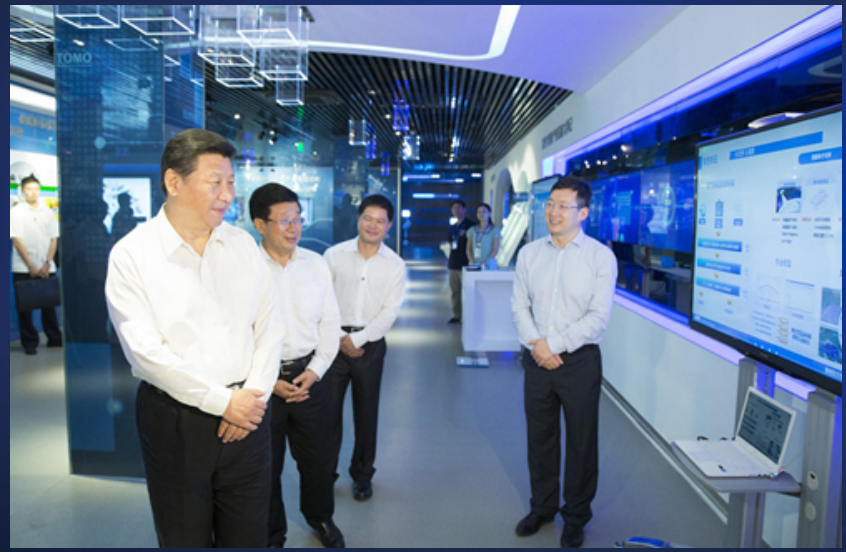
公共大数据重点实验室

贵州大学大数据学部

大数据科学与技术国内一流学科

3.公共大数据国家重点实验室介绍

结束语



“贵州发展大数据确实有道理”

——习近平总书记在2015年6月17日
在贵州考察时指出

感谢您的聆听

THANK YOU FOR LISTENING

聚力·引领

软件安全学术论坛