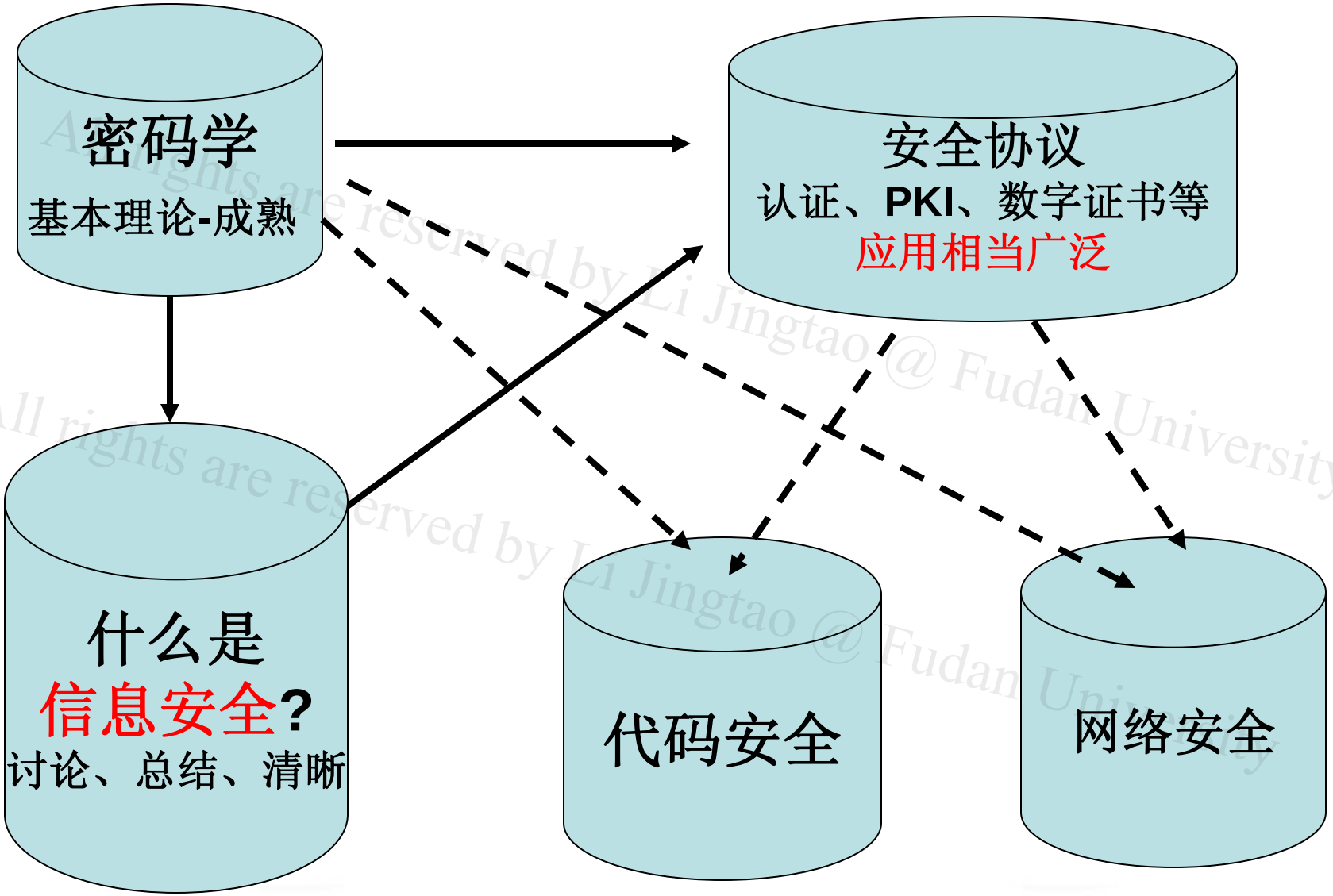
信息安全（06）

信息安全概述

-迟到的序言

内容间的联系



本讲内容

- 信息安全的学科内容
- 信息安全的层次
- 安全威胁
- 引起安全问题的原因
- 信息安全评价标准

信息技术的概念

- 人类的一切活动都可以归结为认识世界和改造世界
- 从**信息**的观点来看，人类认识世界和改造世界的过程，就是一个不断从外部世界的客体中获取信息，并对这些信息进行变换、传递、存储、处理、比较、分析、识别、判断、提取和输出，最终把大脑中产生的决策信息反作用于外部世界的过程。
- **信息技术**是指在计算机和通信技术支持下用以获取、加工、存储、变换、显示和传输文字、数值、图像、视频、音频以及语音信息，并且包括提供设备和信息服务两大方面的方法与设备的总称。

信息安全的概念

- 信息安全的任务是保护信息财产，以防止偶然的或未授权者对信息的恶意泄露、修改和破坏，从而导致信息的不可靠或无法处理等。——“一个勉强的定义”

- 信息安全可以分为数据安全和系统安全两个层次
  - 1. 从数据的层次来看，
    - 包括信息的完整性（Integrity），即保证数据的来源、去向、内容真实无误；
    - 保密性（Confidentiality），即保证数据不会被非法泄露扩散；
    - 不可否认性（Non-repudiation），也称为不可抵赖性，即保证数据的发送和接受者无法否认自己所做过的操作行为。

信息安全的概念

- 信息安全可以分为两个层次：
  数据安全和系统安全。

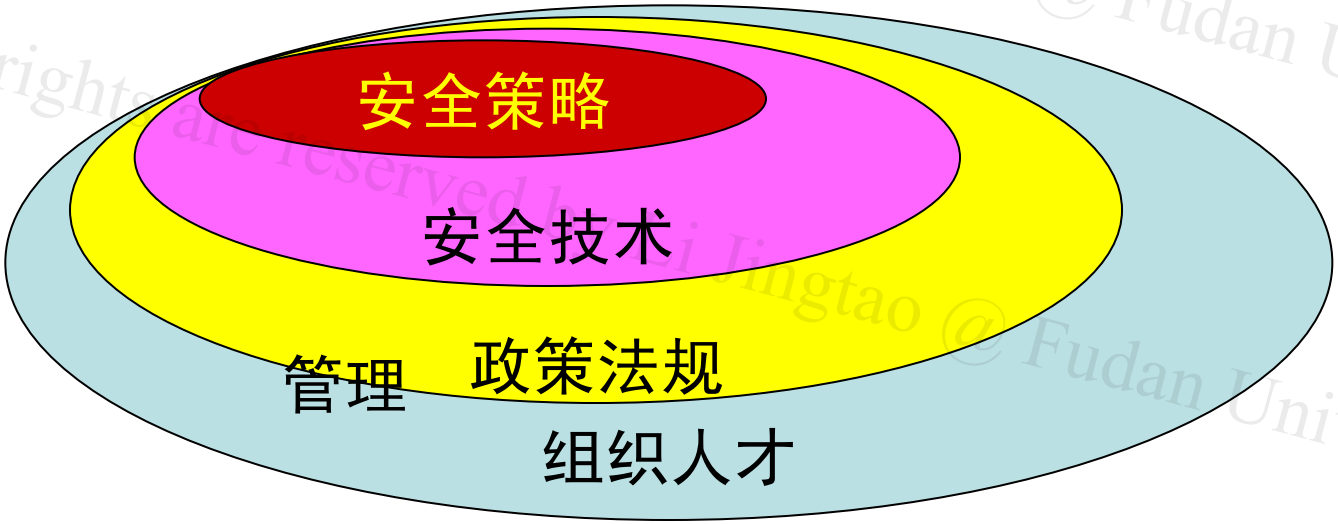
  – 2. 从系统层次来看，包括
    - 可用性（Availability），即保证网络和信息系统随时可用，运行过程中不出现故障，若遇意外打击能够尽量减少并尽早恢复正常；
    - 可控性（Controllability）是对网络信息的传播及内容具有控制能力的特性。
    - ……

问题

- 已学过的密码学技术、方法能否提供上述安全服务？
- 如果能，可提供哪些服务？
- 如果不能，为什么？

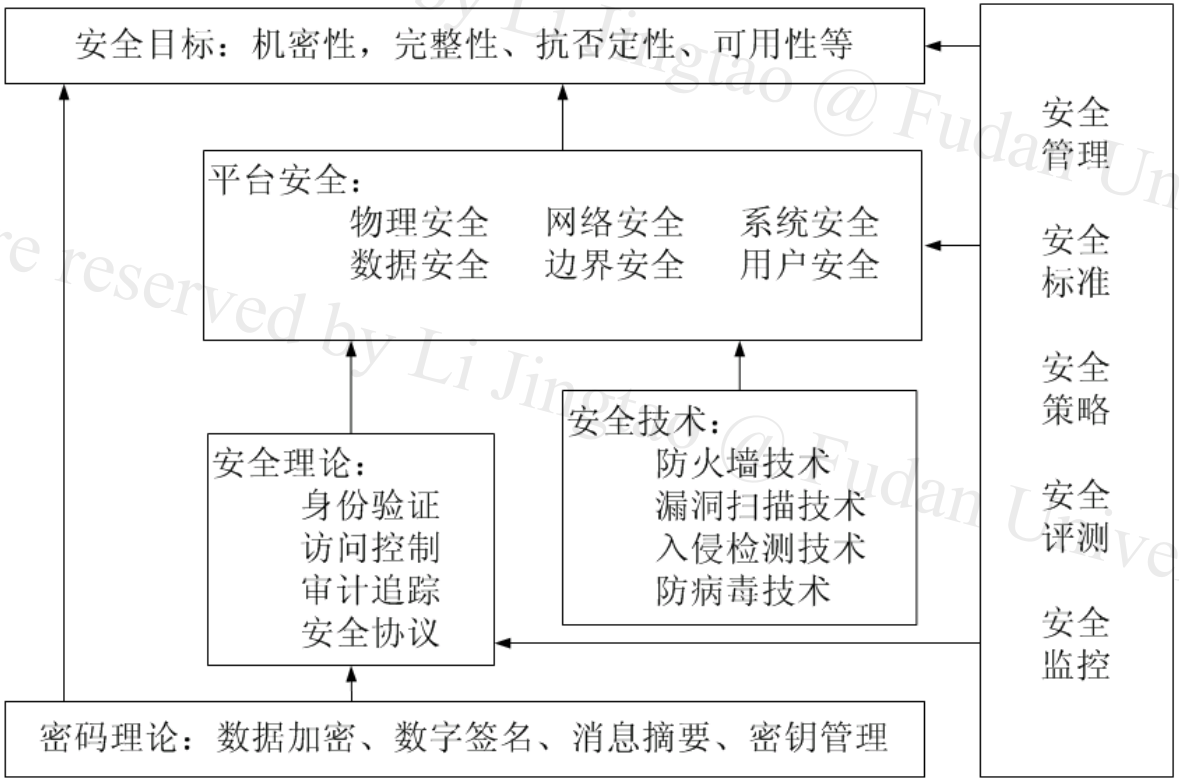
信息安全理念

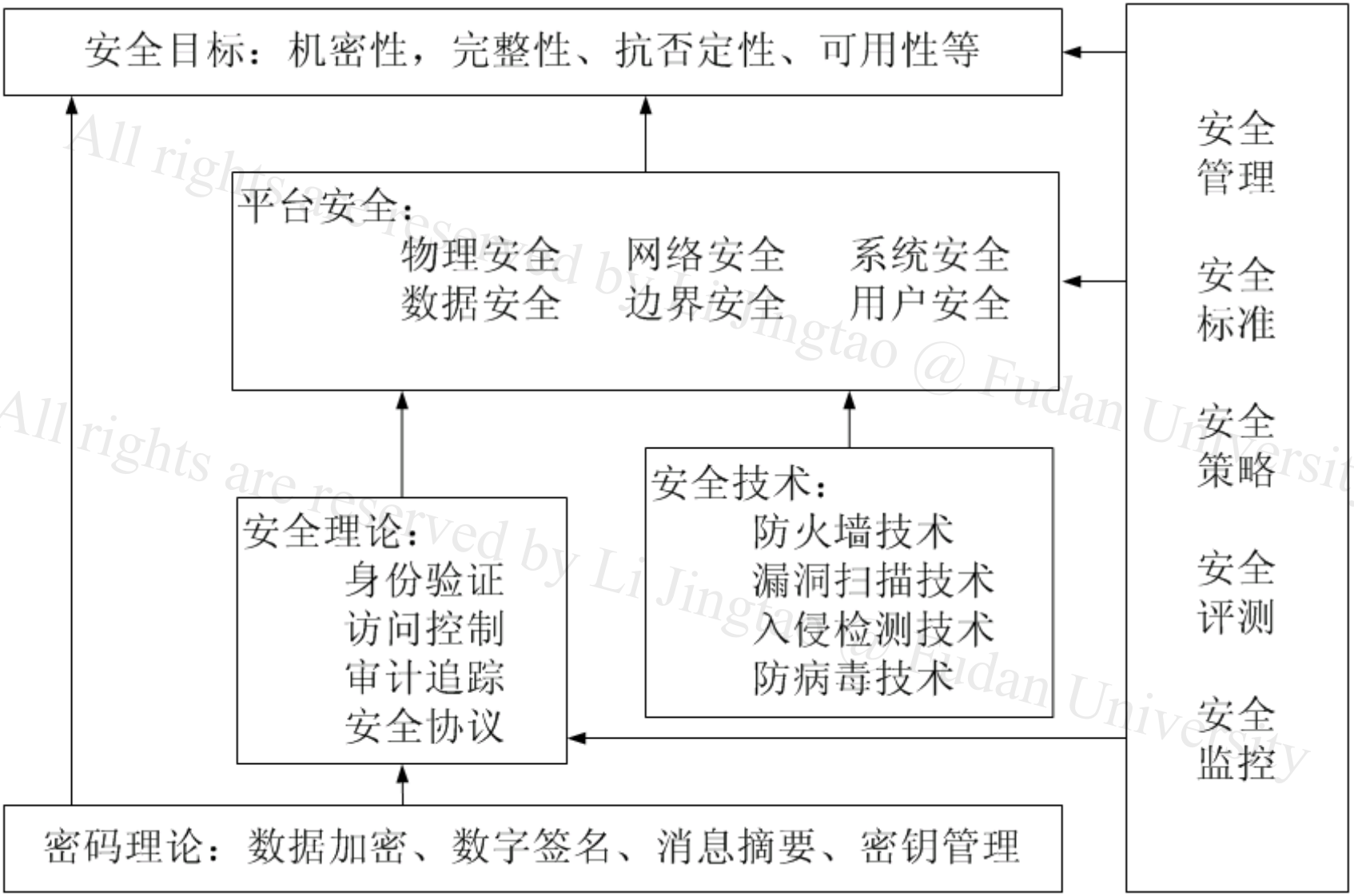
- 安全不是纯粹的技术问题，是一项复杂的系统工程—信息安全工程论
- 安全是策略，技术与管理的综合



信息安全学科内容

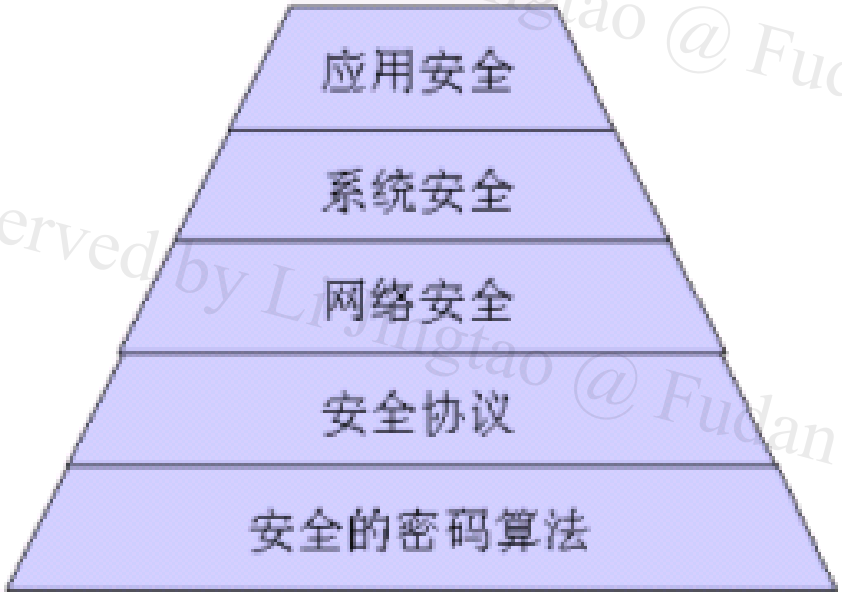
- 信息安全是一门交叉学科。广义上，信息安全涉及多方面的理论和应用知识，除了数学、通信、计算机等自然科学外，还涉及法律、心理学等社会科学。狭义上，也就是通常说的信息安全，只是从自然科学的角度介绍信息安全的研究内容。信息安全各部分研究内容及相互关系如图





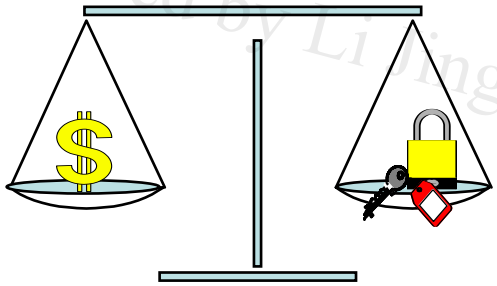
信息安全研究层次

- 信息安全从总体上可以分成5个层次：



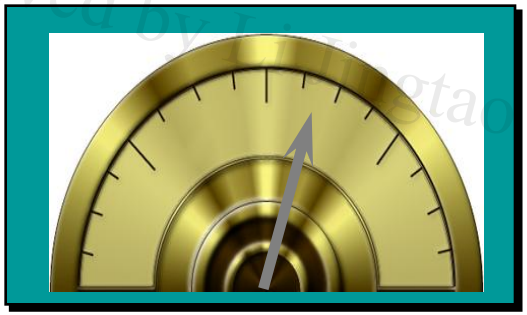
理解安全理念

- 两对“舍与得”



Access **Security**

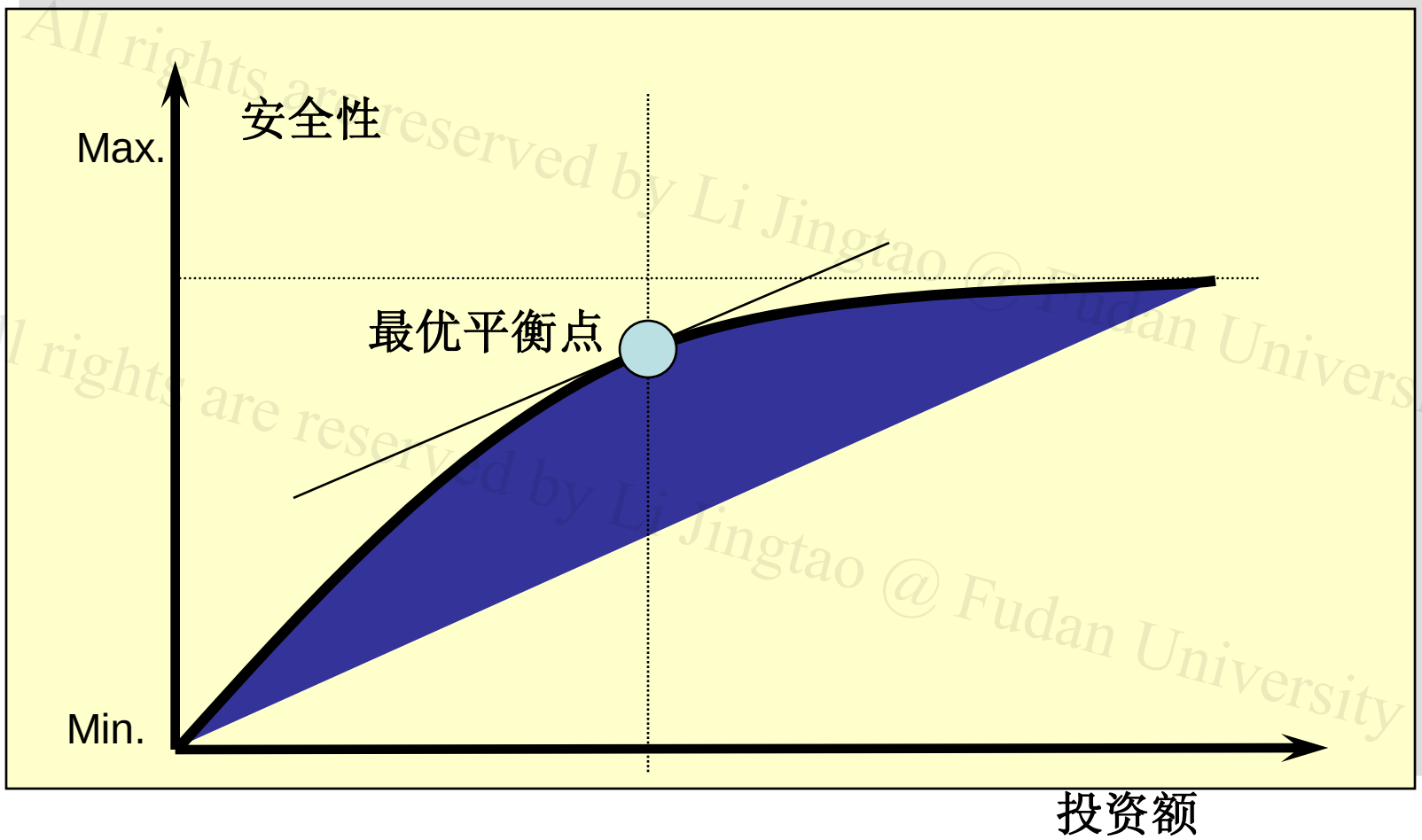
Connectivity
Performance
Ease of Use
Manageability
Availability



Authentication
Authorization
Accounting
Assurance
Confidentiality
Data Integrity

安全策略管理

理解安全理念...



从信息安全的发展来看

- 通信保密， 50s, 60s，
- 计算机安全， 70s, 80s
- 信息安全， 80s, 90s
- 信息保障

军用

↓

民用

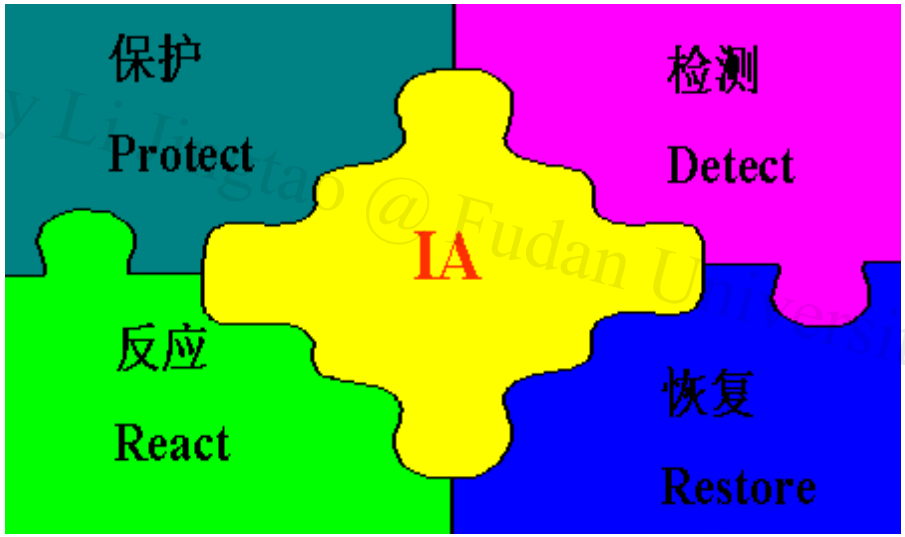
安全技术 = 军火

出口限制

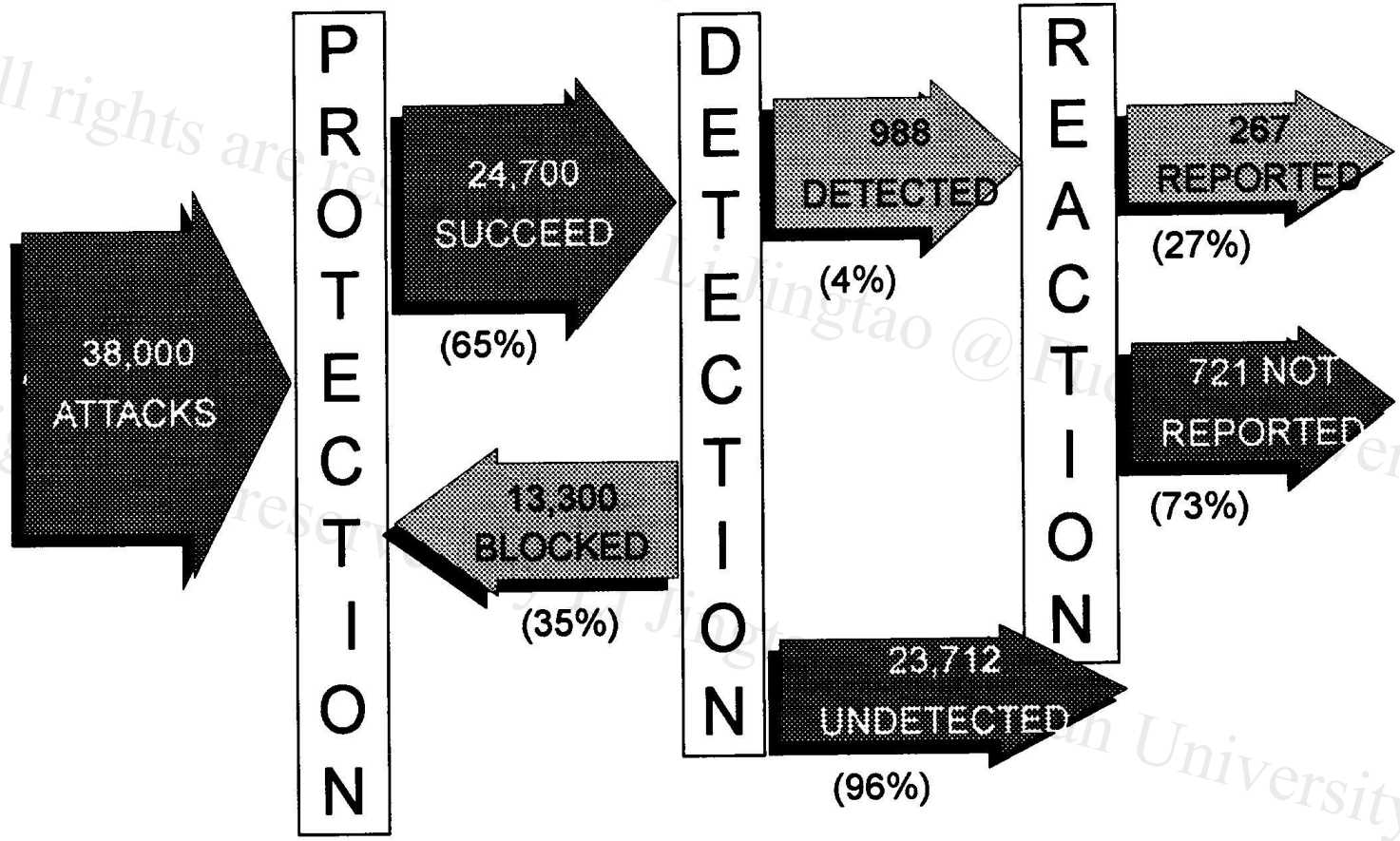
注意两个时间点

信息保障-PDRR模型

- 安全（security）：侧重于“防范潜在的危机”。
- 保障（assurance）：更侧重于可用性和业务的连续性
- 信息保障（IA，Information Assurance）的核心思想是对系统或者数据的4个方面的安全要求（注意是有纵深的）：



PDRR保障体系



主、可

滥等

害的进

报务。

本讲内容

- 信息安全的学科内容
- 信息安全的层次
- 安全威胁
- 引起安全的原因
- 信息安全评价标准

术语

- 脆弱性/漏洞
  - weakness in security system
- 威胁
  - set of circumstances with potential to cause harm
- 例子
  - wall, crack (vulnerability), water (threat), person
- 攻击– exploit of a vulnerability
- 防御
  - action, device, procedure or technique that removes or reduces vulnerability
  - *Threat blocked by control of a vulnerability*

保密性的威胁

- 窃听/搭线攻击 (sniffers)
  - –窃听敏感信息, ...
  - – 电磁辐射泄露
- 非法拷贝
  - – 内部拷贝，防水墙
  - – 非电子: “dumpster diving”, 社会工程

完整性的威胁

- 篡改
  - 篡改数据
  - 篡改程序 (viruses, backdoors, trojan horses, game cheats, ...)
  - 非法终止
- 可认证性的威胁

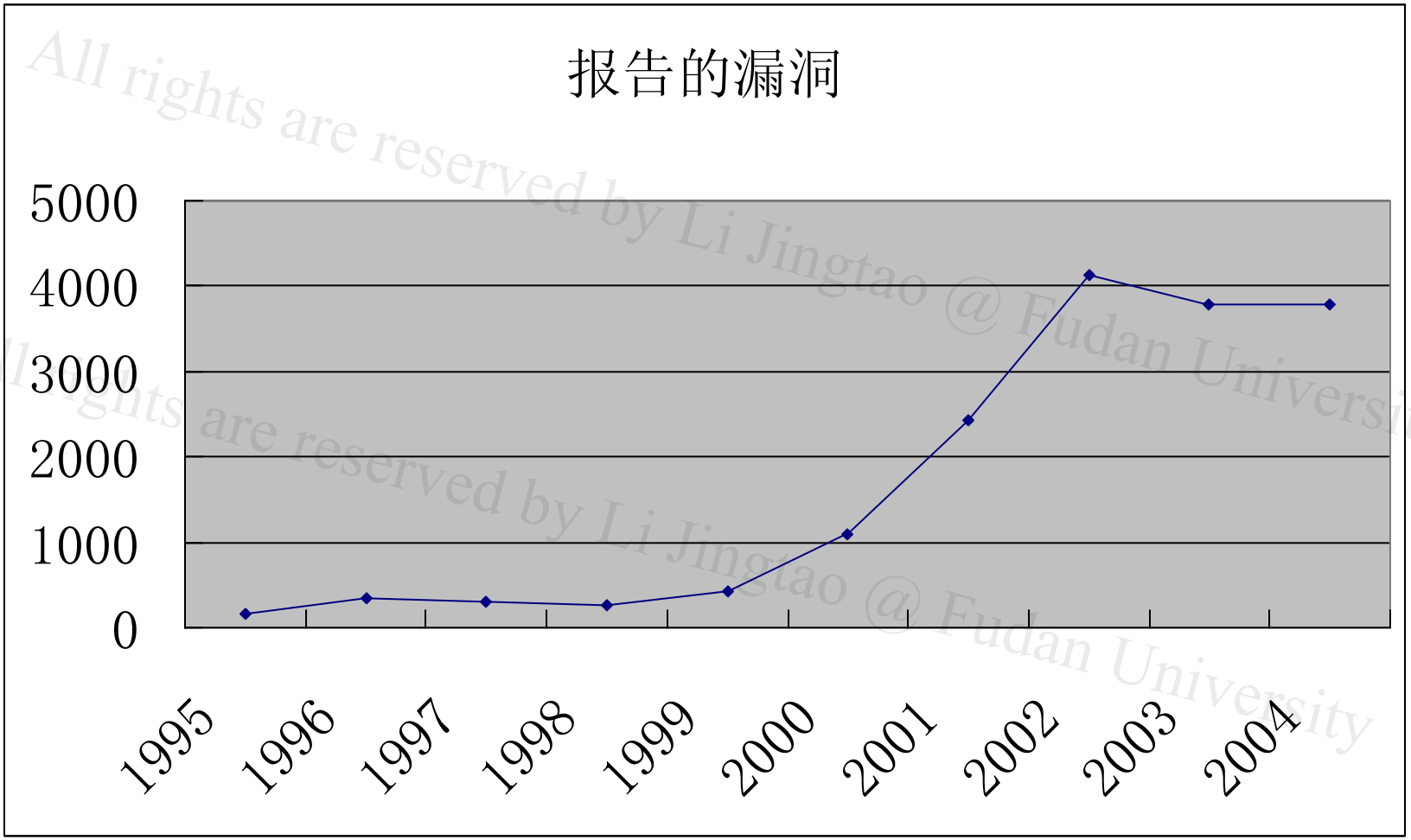
可用性的威胁

- 拒绝服务攻击, Denial of Service (DoS)
- 分布式拒绝服务攻击，Distributed DoS (DDoS)
  - 肉鸡现状
  - Discovery of botnets with 10-100 systems is a daily occurrence; 10,000 system botnets are found almost weekly; and one botnet with 100,000 hosts has even been found (according to Johannes Ullrich, CTO of the Internet Storm Center).

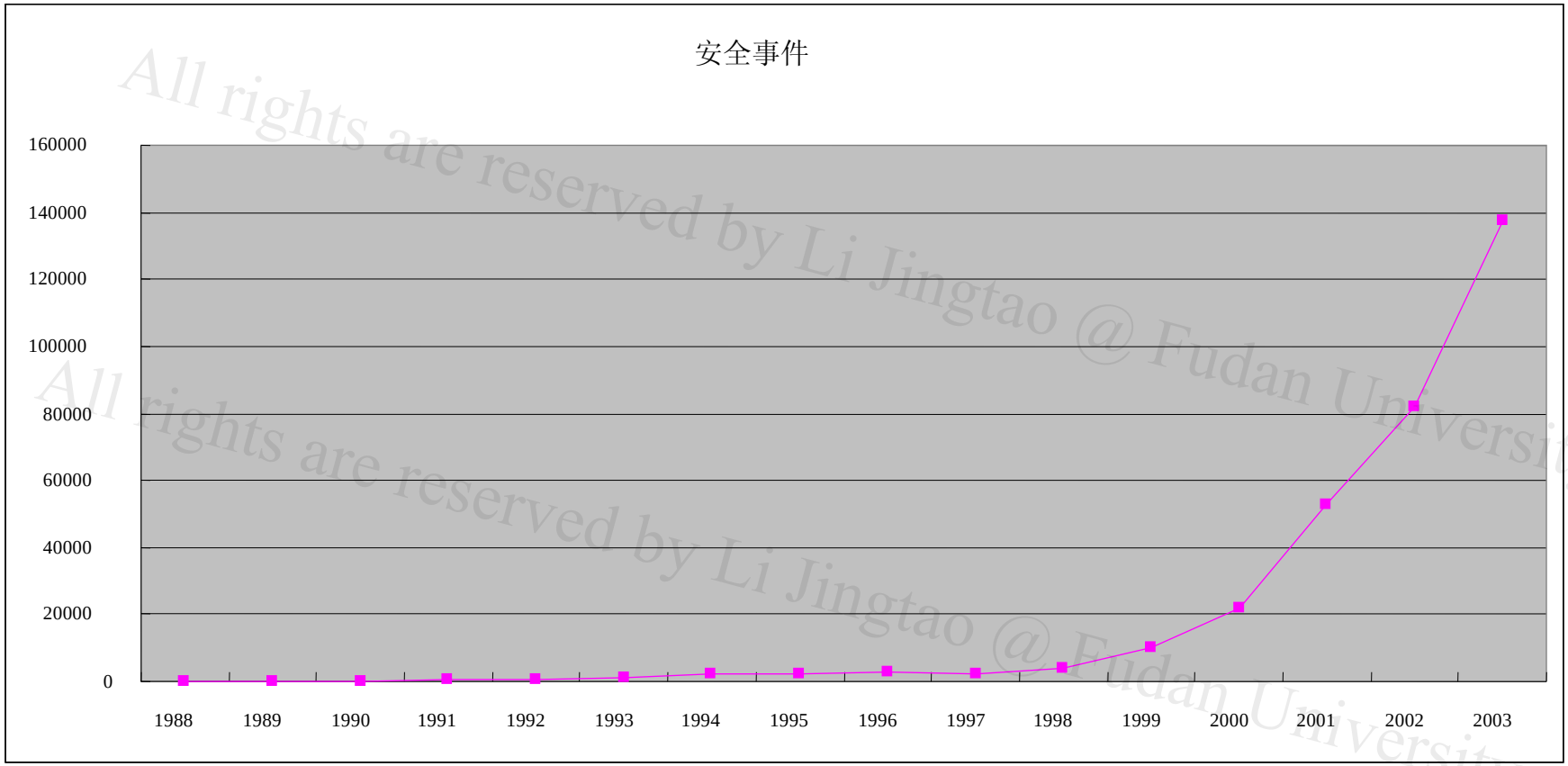
本讲内容

- 信息安全的学科内容
- 信息安全的层次
- 安全威胁
- 引起安全问题的原因
- 信息安全评价标准

1995-2004年报告的漏洞数目统计 (CERT)



1988-2003年报告的安全事件统计 (CERT)



带有政治性的网上攻击有较大增加

- 过去两年，我们国家的一些政府网站，遭受了四次大的黑客攻击事件。
  - 第一次在99年1月份左右，但是美国黑客组织“美国地下军团”联合了波兰的、英国的黑客组织，世界上各个国家的一些黑客组织，有组织地对我们国家的政府网站进行了攻击。
  - 第二次，99年7月份，台湾李登辉提出了两国论。
  - 第三次是在1999年5月8号，美国轰炸我国驻南联盟大使馆后。
  - 第四次在2001年4月到5月，美机撞毁王伟战机侵入我海南机场

信息安全与经济

- 一个国家信息化程度越高，整个国民经济和社会运行对信息资源和信息基础设施的依赖程度也越高。
- 我国计算机犯罪的增长速度超过了传统的犯罪
  - 97年20几起，98年142起，99年908起，2000年上半年1420起。
- 利用计算机实施金融犯罪已经渗透到了我国金融行业的各项业务。
  - 近几年已经破获和掌握100多起。涉及的金额几个亿。

黑客攻击事件造成经济损失

- 2000年2月份黑客攻击的浪潮，是互连网问世以来最为严重的黑客事件
- 99年4月26日，台湾人编制的CIH病毒的大爆发，有统计说我国大陆受其影响的PC机总量达36万台之多。有人估计在这次事件中，经济损失高达近12亿元。
- “爱虫”病毒
- **1996年4月16日，美国金融时报报道，接入Internet的计算机，达到了平均每20秒钟被黑客成功地入侵一次的新记录**

信息安全与社会稳定

- 互连网上散布一些虚假信息、有害信息对社会管理秩序造成的危害，要比现实社会中一个造谣要大的多。
- 99年4月，河南商都热线一个BBS，一张说交通银行郑州支行行长协巨款外逃的帖子，造成了社会的动荡，三天十万人上街排队，挤提了十个亿。
- 网上治安问题，民事问题，进行人身侮辱。
  - 来自上海，四川的举报

原因浅析

- 计算机越来越多
- Internet上关键应用与非关键应用并行
- 家庭用户
- 安全措施是反映式的/缺乏前瞻
- 成本过高
- 永远不会有完美的安全方案

攻击者类型

国家安全威胁	**信息战士**	减小美国决策空间、战略优势，制造混乱，进行目标破坏
	情报机构	搜集政治、军事，经济信息
共同威胁	**恐怖分子**	破坏公共秩序，制造混乱，发动政变
	工业间谍	掠夺竞争优势，恐吓
	犯罪团伙	施行报复，实现经济目的，破坏制度
局部威胁	**社会型黑客**	攫取金钱，恐吓，挑战，获取声望
	娱乐型黑客	以吓人为乐，喜欢挑战

原因浅析

- 内因
  - 人们的认识能力和实践能力的局限性
  - 系统规模
    - Windows 3.1 ——300万行代码
    - Windows 2000 ——5000万行代码
  - 网络规模

我国立法情况

- 计算机软件保护条例（1991年6月4日 ）
- 中华人民共和国计算机信息系统安全保护条例（1994年2月18日 ）
- 商用密码管理条例（1999年l0月7日）
- 互联网信息服务管理办法（2000年9月20日 ）
- 中华人民共和国电信条例（2000年9月25日 ）
- 全国人大常委会关于网络安全和信息安全的决定（2000年12月29日）

初步修订增加了条款的国家法律

- 中华人民共和国刑法
  - 为了加强对计算机犯罪的打击力度，在1997年对刑罚进行重新修订时，加进了以下计算机犯罪的条款：
    - 第二百八十五条 违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的，处三年以下有期徒刑或者拘役。
    - 第二百八十六条 违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行，后果严重的，处五年以下有期徒刑或者拘役,后果特别严重的，处五年以上有期徒刑。违反国家规定，对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作，后果严重的，依照前款的规定处罚。故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，后果严重的，依照第一款的规定处罚。
    - 第二百八十七条 利用计算机实施金融诈骗、盗窃、贪污、挪用公款、窃取国家秘密或者其他犯罪的，依照本法有关规定定罪处罚。

国际立法情况

- 美国和日本是计算机与网络安全比较完善的国家，一些发展中国家和第三世界国家的信息安全方面的法规还不够完善。
- 欧盟在诸多问题上建立了一系列法律，
  - 具体包括：竞争（反托拉斯）法；产品责任、商标和广告规定；知识产权保护；保护软件、数据和多媒体产品及在线版权；数据保护；跨境电子贸易；税收；司法问题等。这些法律若与其成员国原有国家法律相矛盾，则必须以共同体的法律为准。

本讲内容

- 信息安全的学科内容
- 信息安全的层次
- 安全威胁
- 信息安全的社会意义
- 信息安全评价标准

国际标准的发展

- 国际上著名的标准化组织及其标准化工作
  - ISO，NIST
- 密码标准
  - DES
  - AES
  - NESSIE(New European Schemes for Signature, Integrity, and Encryption)
  - 140-2 （NIST FIPS PUB 密码模块）
- 可信计算机系统评价准则
  - TCSEC-ITSEC-CC

国际标准的发展

- 信息安全管理标准
  - BS7799, ISO 17799
  - ISO/IEC 27001
    - 信息安全管理体系 (ISMS)
    - 27002: 实施指南
    - 27005: 风险管理

权威的传统评估标准

- 美国国防部在1985年公布
  - 可信计算机安全评估准则
  - Trusted Computer Security Evaluation Criteria (TCSEC)
- 为安全产品的测评提供准则和方法
- 指导信息安全产品的制造和应用

安全级别

类别	级别	名称	主要特征
D	D	低级保护	没有安全保护
C	C1	自主安全保护	自主存储控制
	C2	受控存储控制	单独的可查性，安全标识
B	B1	标识的安全保护	强制存取控制，安全标识
	B2	结构化保护	形式化模型，面向安全的体系结构，较好的抗渗透能力
	B3	安全区域	存取监控、高抗渗透能力
A	A	验证设计	形式化的最高级描述和验证

传统评估标准的演变

- 美国DoD
  - DoD85 TESEC
  - TCSEC网络解释（TNI 1987）
  - TCSEC数据库管理系统解释（TDI 1991）
  - 彩虹系列Rainbow series
- 欧洲 – ITSEC
- 美国、加拿大、欧洲等共同发起Common Criteria(CC)

ITSEC（又称欧洲白皮书）

- 90年代初西欧四国（英、法、荷、德）联合提出了信息技术安全评价标准（ITSEC）
- 除了吸收TCSEC的成功经验外，首次提出了信息安全的保密性、完整性、可用性的概念，把可信计算机的概念提高到可信信息技术的高度上来认识。他们的工作成为欧共体信息安全计划的基础，并对国际信息安全的研究、实施带来深刻的影响。

通用评价准则（CC）

- 美国为了保持他们在制定准则方面的优势，不甘心TCSEC的影响被ITSEC取代，他们采取联合其他国家共同提出新的评估准则的办法体现他们的领导作用。
- 91年1月宣布了制定通用安全评价准则（CC）的计划。它的全称是Common Criteria for IT security Evaluation 。
- 制定的国家涉及到六国七方，他们是美国的国家标准及技术研究所（NIST）和国家安全局（NSA），欧州的荷、法、德、英，北美的加拿大

通用评价准则（CC）

- 它的基础是欧州的ITSEC，美国的包括TCSEC 在内的新的联邦评价标准，加拿大的 CTCPEC，以及国际标准化组织ISO :SC27 WG3 的安全评价标准
- 1995年颁布0.9版，1996年1月出版了1．0版。 1997年8月颁布2.0 Beata版， 2.0 版于1998年5月颁布。
- 1998-11-15 成为ISO/IEC 15408信息技术-安全技术-IT安全评价准则

CC标准的读者对象

- **用户**：通过风险和策略的分析，比较评价的不同产品和系统，选择适合自己使用的产品和系统。
- **开发者**：支持开发者认识满足自己产品和系统的安全要求，制定保护轮廓（PP），确定安全目标（ST），支持开发者开发自己的评价目标（TOE），在评价方法学帮助开发者，以共识的评价结果评价自己开发的产品和系统。
- **评价者**：正式审查评价目标时为评价者提供一个评价准则，用于评价评价目标（TOE）和安全要求的一致性
- **其它**：对于对IT安全有兴趣和有责任的人起到一个导向和参考材料的作用，机构中的系统监管和安全官员确定安全策略和要求

我国评价标准

- **在我国根据《计算机信息系统安全保护等级划分准则》，1999年10月经过国家质量技术监督局批准发布准则将计算机安全保护划分为以下五个级别**
  - 第一级为用户自主保护级：它的安全保护机制使用户具备自主安全保护的能力，保护用户的信息免受非法的读写破坏。
  - 第二级为系统审计保护级：除具备第一级所有的安全保护功能外，要求创建和维护访问的审计跟踪记录，使所有的用户对自己的行为的合法性负责。
  - 第三级为安全标记保护级：除继承前一个级别的安全功能外，还要求以访问对象标记的安全级别限制访问者的访问权限，实现对访问对象的强制保护。
  - 第四级为结构化保护级：在继承前面安全级别安全功能的基础上，将安全保护机制划分为关键部分和非关键部分，对关键部分直接控制访问者对访问对象的存取，从而加强系统的抗渗透能力
  - 第五级为访问验证保护级：这一个级别特别增设了访问验证功能，负责仲裁访问者对访问对象的所有访问活动。

评估标准间的关系

- TCSEC主要规范了计算机操作系统和主机的安全要求，侧重于对保密性的要求。该标准至今对评估计算机安全仍然具有现实意义。
- ITSEC将信息安全由计算机扩展到更广的实用系统，增强了对完整性和可用性的要求，发展了评估保证概念。
- CC基于风险管理理论，对安全模型、安全概念和安全功能进行了全面系统描绘，强化了评估保证。
- 我国的评价标准GB17859与TCSEC、ITSEC以及CC评价安全等级的大体对应关系如表1-2所示。

我国GB17859	美国TCSEC	欧洲ITSEC	通用标准CC
--	D：低级保护	E0：	--
--	--	--	EAL1：功能测试
GB1：用户自主保护级	C1：自主保护级	E1：功能测试	EAL2：结构测试
GB2：系统审计保护级	C2：受控存储控制	E2：数字化测试	EAL3：方法测试与检验
GB3：安全标记保护级	B1：标识的安全保护	E3：数字化测试分析	EAL4：设计措施与评审
GB4：结构化保护级	B2：结构化保护	E4：半形式化分析	EAL5：半形式化设计与测试
GB5：访问验证保护级	B3：安全区域	E5：形式化分析	EAL6：半形式化验证设计测试
--	A：验证设计	E6：形式化验证	EAL7：形式化验证和测试

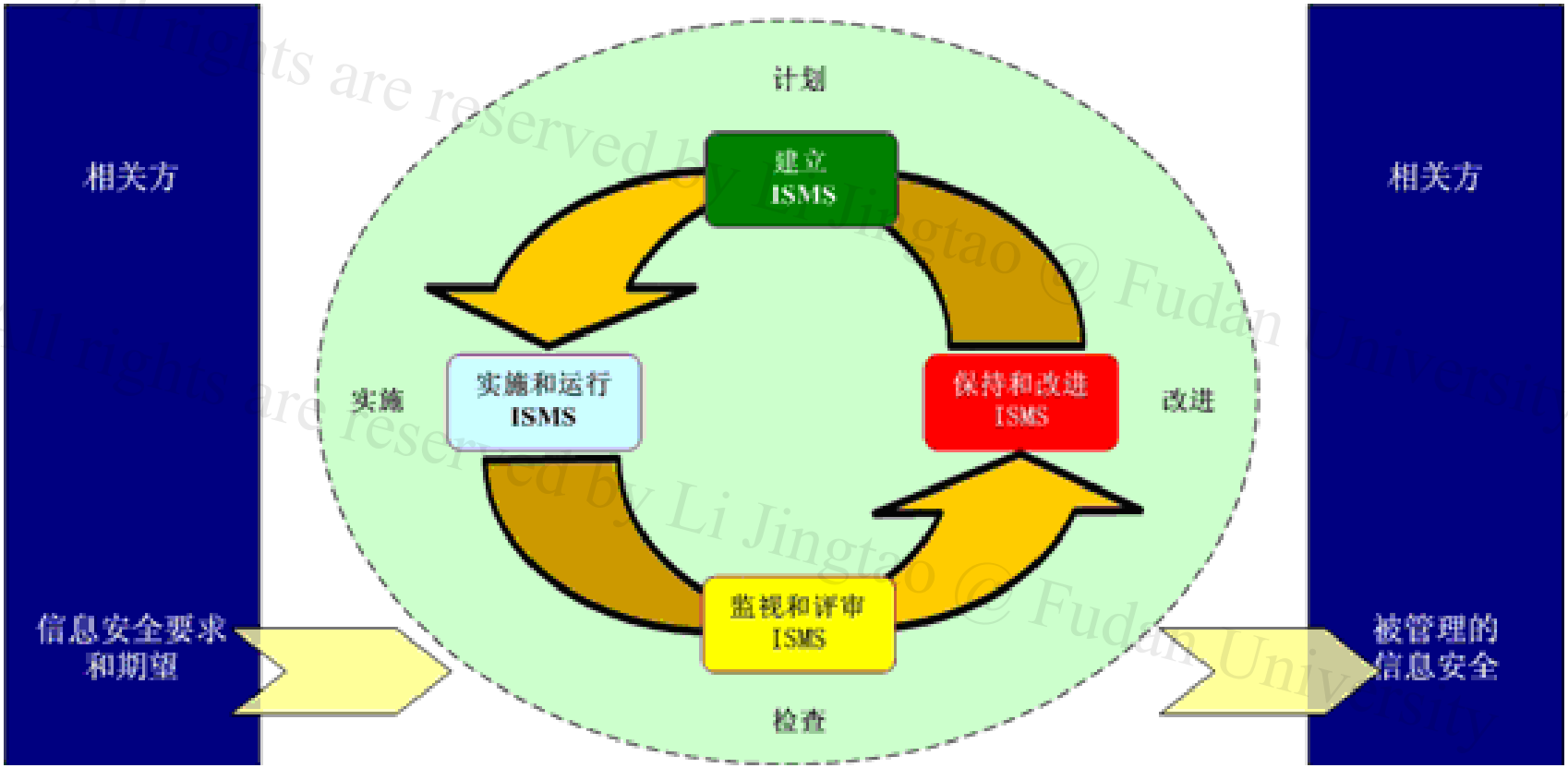
我国标准应用情况

- 大致分两大体系：
  - 等级保护派，公安
  - CC派，质量监督局

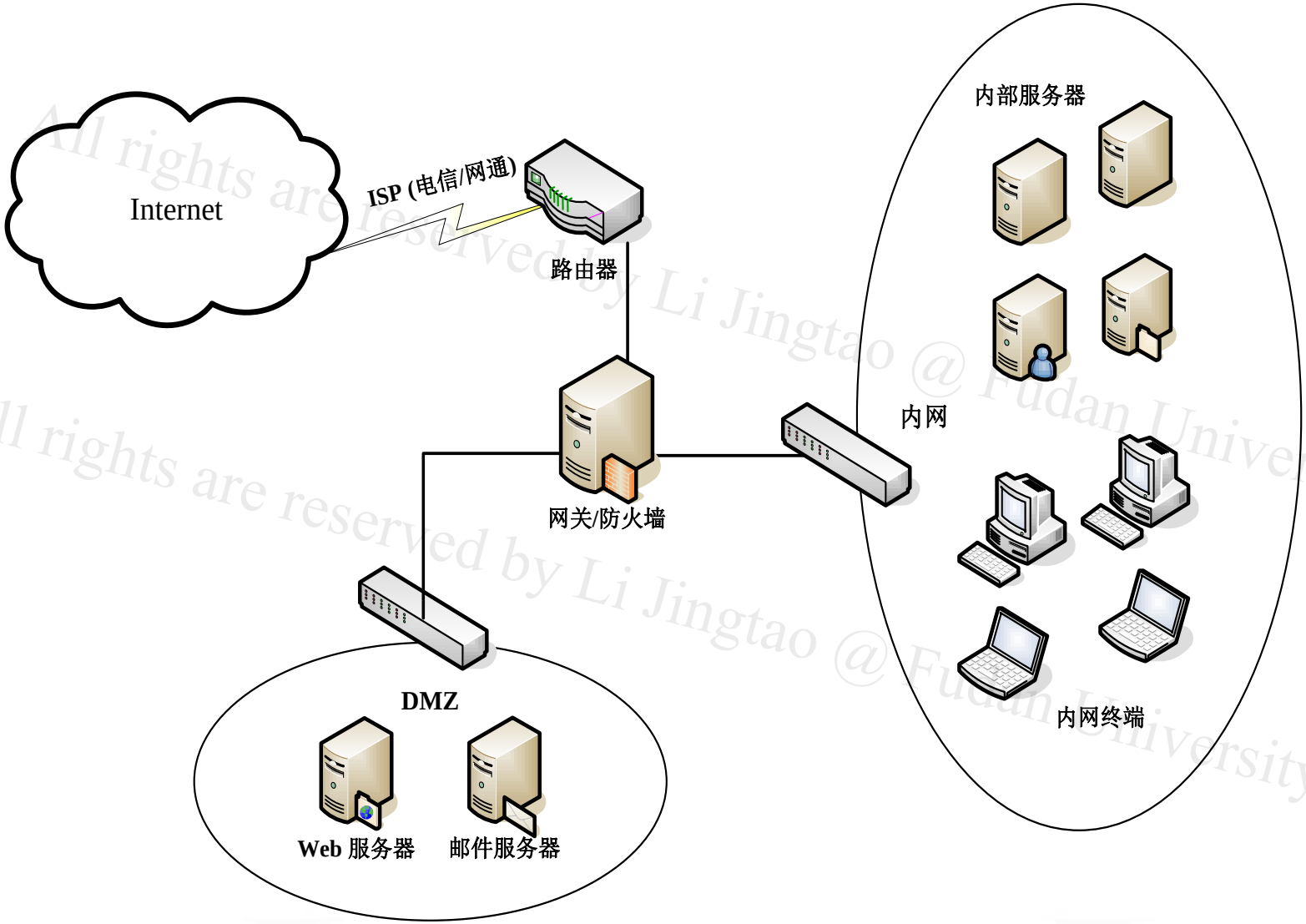
案例研究

- 中小企业的Web站点
  - 业务需求？
  - 风险分析？
  - 安全策略？
  - 采取措施？

一般化流程



风险分析



技术措施– 例子

- 保密措施 – 加密.....
- 身份认证 (pw, advanced: smart cards, tokens, ...)
- 访问控制
  - 操作系统层面的控制 (文件访问权限,, ...)
  - 应用的访问控制 (DB, web server, ...)
  - 网络边界控制 (firewall, VPN, ...)
- 网络安全
  - 检测技术 (IDS, virus scanners)
  - 漏洞扫描Regularly test/evaluate (“penetration testing”)
- 软件安全
  - 安全开发控制 (secure software development)
- 物理安全(door locks, media management)
- ??