回顾上次课后作业

- 阅读书本第3章
- 思考以下问题 （下次课提问）
  - 什么是信息安全?
  - 信息安全的三个基本目标是什么?
  - 计算机网络面临哪些安全威胁?
  - 什么是数据的完整性?

第3章 信息安全基本概念与原理

- 引言：
  - 随着社会信息化水平的不断提高和电子政务与电子商务的快速发展，信息系统与计算机网络的基础性、全局性作用日益增强，国民经济与社会活动之间的依赖关系不断加强。
  - 在日常工作和生活中，人们越来越依赖信息系统，越来越多地通过信息系统管理企业的产、供、销、人、财、物，越来越多地使用计算机网络来传递敏感信息。

- 信息系统的一次故障或事故会造成巨大的影响，甚至是灾难。特别是对于军事、航空航天、金融、电力等关键信息系统而言，其安全性、可信性就更加重要。
- 物联网（The Internet of things）技术进一步促进了信息化的发展。

信息安全的概念

- 数据与信息
- 不同的角度：计算机安全，网络安全
- 信息安全的目标（三要素CIA）
  - 保密性
  - 完整性
  - 可用性
- AAA 概念
  - 保证性 (Assurance)
  - 真实性 (Authenticity)
  - 匿名性 (Anonymity)

信息安全的发展历程

- 物理安全
- 网络安全
- 应用安全
- 数据安全

信息安全的主要威胁

- 窃听
- 重传
- 伪造
- 篡改
- 拒绝服务攻击
- 行为否认
- 非授权访问
- 传播病毒

信息安全体系结构

- 面向目标的
  - 三元素 CIA
- 面向过程的
  - 信息安全保障
  - 信息系统的保护、检测、相应、恢复
  - 信息保障技术框架(IATF)，人、操作、技术
- 面向应用的
  - 基于人员、信息、系统的层次体系
- 面向OSI标准网络的
  - 安全服务
  - 安全机制

补充内容

一、信息化社会的发展

二、信息安全现状分析

一、信息化社会的发展

- 信息化社会的发展
- 信息化社会的特点
- 信息化社会中的挑战
- 我国信息化的现状

1.信息化社会的发展

- 信息是构成任何系统的三大要素之一，另外两个是物质和能源。信息虽然是无形的和抽象的，但它是系统的灵魂。
- 1948年C. E. Shannon的《通信的数学理论》，宣告了一门崭新的学科—信息论的诞生。它是通信技术领域技术革命的数学或理论基础。
- 1946年的计算机和1947年晶体管的诞生和相应技术的发展是这一革命的物理或物质基础。

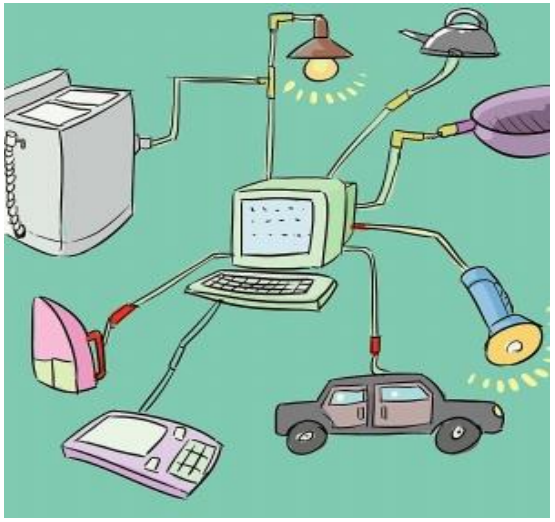
- 六十多年后的今天，通信、计算机和半导体技术的发展已将人类社会推进到一个崭新的信息时代。特别是 Internet的出现，加上九十年代开始了通信、计算机和消费电子（3C ——Communications, Computers, Consumer electronics）的三结合，信息高速公路或全球信息基础设施（GII）的提出和建设，构成了人类生存的信息环境，即信息空间（Cyberspace）。这个虚拟空间的形成和发展将人类社会推进到一个新的发展阶段，即信息化社会阶段。
- 互联网实现了计算机之间的互联，万维网（Web）实现了信息的互联，物联网则是物的互联，社会网络（social network）是人的互联。

- 在信息化社会中信息的作用愈来愈大，社会对信息的需求愈来愈大。通信、广播、影视、出版等正在从模拟到数字，从单一媒体到多媒体，从人工、机械化到智能化、从局部联网到全球通信网。Internet的出现，为人类交换信息，促进科学、技术、文化、教育、生产的发展，提高现代人的生活质量提供了极大的便利，大大加速了人类社会的进程。

- 物联网通过传感器、射频识别技术、全球定位系统等技术，实时采集任何需要监控、连接、互动的物体或过程，采集其声、光、热、电、力学、化学、生物、位置等各种需要的信息，通过各类可能的网络接入，实现物与物、物与人的泛在链接，实现对物品和过程的智能化感知、识别和管理。

物联网

Internet of Things



生活在数字时代

- 生活、工作、出行、学习、游戏、上网、吃饭购物……
- 美国人每天的生活平均涉及250多台电脑

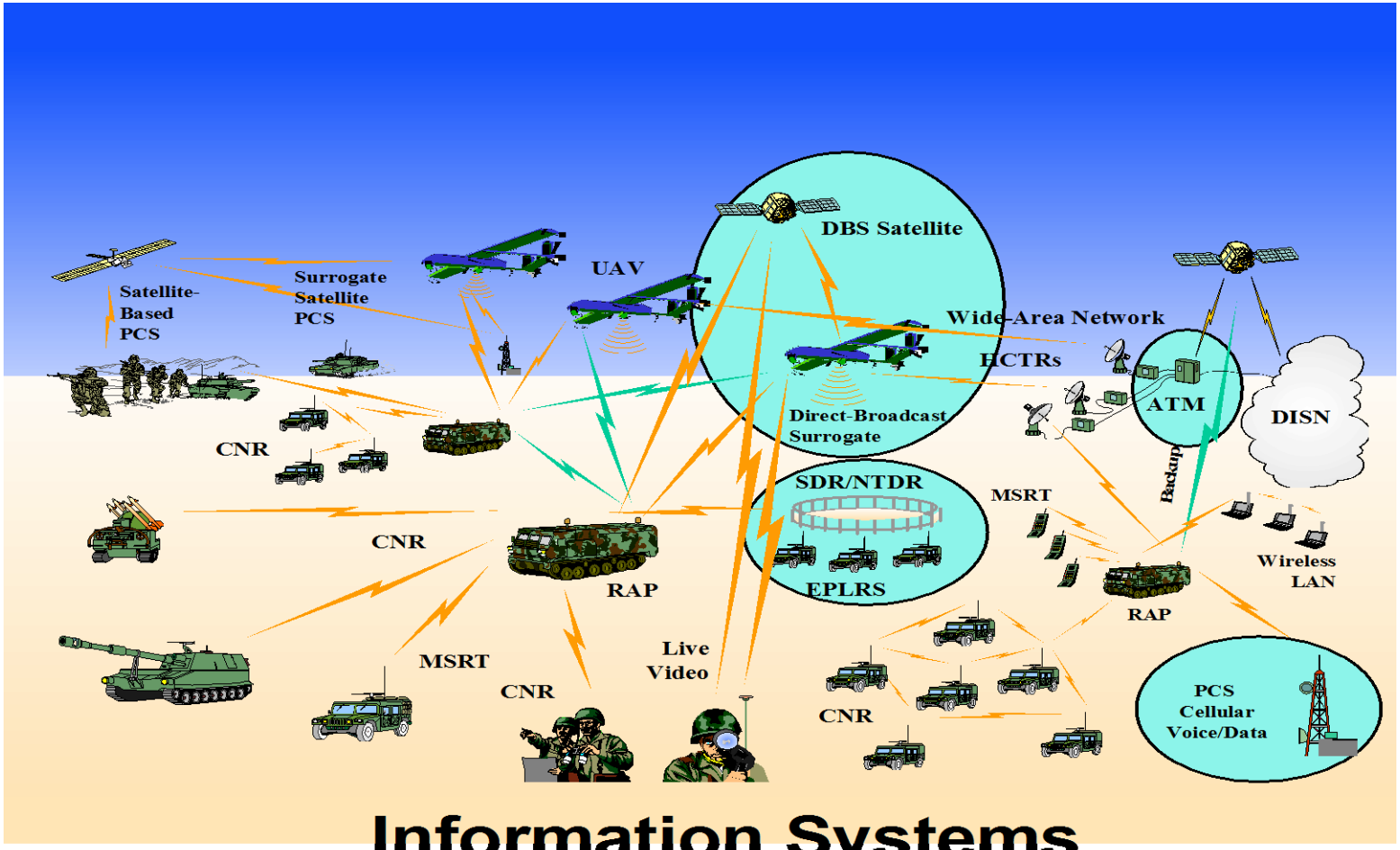
- “互联网+”成为国家经济社会发展的重要战略
  - 互联网+传统集市=淘宝
  - 互联网+传统百货卖场=京东
  - 互联网+传统红娘=相亲网站
  - 互联网+传统银行=支付宝
  - 互联网+传统交通=嘀嘀打车
  - 互联网+传统新闻=新媒体
  - 互联网+通讯=即时通信
  - 互联网+审计=？
  - ……
- 互联网与各行各业之间并不是替代关系，而是提升关系。
- 互联网时代：创新是互联网时代的核心力量，只有想不到，没有做不到。
- 2015年中国计算机大会的主题：互联网+重构经济

2.信息化社会的特点

- 在信息化社会中，一个国家、一个地区、一个单位、乃至一个家庭和个人，如果没有好的信息基础设施，它在现代信息社会的激烈竞争中，就会落后和失败。
- 信息化社会导致经济全球化和知识化。互联网已成为社会资源重新分配的根本工具，美国最近5年在Internet上创造的百万富翁比过去50年所有工业所创造的百万富翁还要多。

- 信息化社会中人们的一切活动都将 在信息空间中进行竞争和接受检验。
- 信息化社会中许多有形的东西开始向无形的数字化方向转变。
- 信息化社会导致第三次军事革命，联合作战和信息作战成为重要的作战形式，数字化部队和数字化战场诞生。信息和技术在战争中的作用越来越大。

C4I:Command, Control, Communications, Computers and Intelligence



3.信息化社会中的挑战

- 信息过量，难以消化：《纽约时报》由60年代的10－20版扩张至现在的100－200版，最高曾达1572版；而人均日阅报时间通常为30－45分钟，只能浏览一份24版的报纸。

  数据生产、传输能力 >> 数据分析能力；

  人们被数据淹没，人们却饥饿于知识；

IDC（International Data Corporation ）在2006年估计全世界产生的数据量是0.18ZB，而2011年这个数字已经提升了一个数量级，达到1.8ZB，差不多对应全世界每个人一块100多GB的硬盘。这种增长还在加速，预计2015年将达到近8ZB。

存储单位

1KB （Kilobyte 千字节）=1024B

1MB （Megabyte 兆字节 简称“兆”）=1024KB

1GB （Gigabyte 吉字节 又称“千兆”）=1024MB

1TB （Trillionbyte 万亿字节 太字节）=1024GB

1PB（Petabyte 千万亿字节 拍字节）=1024TB

1EB（Exabyte 百亿亿字节 艾字节）=1024PB

1ZB （Zettabyte 十万亿亿字节 泽字节）= 1024 EB

3.信息化社会中的挑战（续）

- 信息真假，难以辨识；
- 信息的表示不一致，难以统一处理；
- 信息系统的质量难以保证；
- 信息安全，难以保证；
- 信息化社会很不稳定。

信息安全与信息产业

- 信息安全保障能力是21 世纪综合国力、经济竞争实力和生存能力的重要组成部分，是世界各国在奋力攀登的制高点。当前，在我国经济发展的进程中，信息安全的影响越来越大。
- 信息社会是一个信息技术占主导地位，信息产业成为主导产业，信息经济是其主要经济形态，信息资源变成重要经济资源，信息、知识和智力决定发展力量的社会。

信息的重要性

- 在信息社会，没有各种信息的有效支持，没有信息安全作保障，企业就不可能生存和发展。试想，如果信息不加以妥善保护，那么一旦由于人员（疏忽、跳槽、破坏）、竞争对手（商业间谍、收买、盗窃、网络攻击）、设备故障、系统缺陷和灾害（爆炸、雷击、火灾、地震）等原因，造成在一瞬间信息资产的毁灭、消失、损坏、盗窃、转移，那必然会给企业带来致命的打击。

例如

- 2006年4月20日，中国银联网络长时间瘫痪，从上午10时56分起至晚上20时，银行卡交易大面积停止，据估计涉及全球至少34万家商户以及6万台ATM机，很多人不能取款转账，不能刷卡消费。给消费者带来不便，商家蒙受损失。银联方面表示，此次事故是由于最近准备上线的某外围设备的隐性缺陷诱发了跨行交易系统主机的缺陷，使主机发生故障。
- 2007年8月11日，由于美国洛杉矶国际机场的海关电脑发生故障，造成约6000名乘客滞留机场长达 6 小时。

例如

- 2009年5月19日，我国部分省份互联网出现严重网络故障，20多个省份互联网域名解析服务无法正常工作，导致大量网民无法正常访问网站。
- 2010年2月，民生银行核心系统故障，导致数小时内业务不能进行，经查，是由于新产品上线时存在技术性缺陷、且未能严格测试，导致上线后引发事故，同时也暴露出信息系统的故障应急响应及支持机制有待改进。

试想：现代社会如果没有信息系统会怎么样？

- 美国明尼苏达大学Bush-Kugel的研究表明，企业在没有信息资料可用的情况下，金融业至多只能运作出2天，商业企业为3.3天，工业企业为5天，保险业为5.6天。从经济状况而论，约有25%的企业，会因为数据的损毁而立即破产，40%会在两年内宣布破产，只有7%的企业能生存到5年之后。可见，信息安全对企业的极端重要性。信息安全也是国家安全的需要，信息安全是组织持续发展的需要，信息安全是保护**个人隐私**与财产的需要。

安全威胁来自哪里？

- 内因
  - 人们的认识能力和实践能力的局限性
  - 系统规模越来越大，越来越复杂
    - Windows 3.1 ——300万行代码
    - Windows 2000 ——5000万行代码

外因

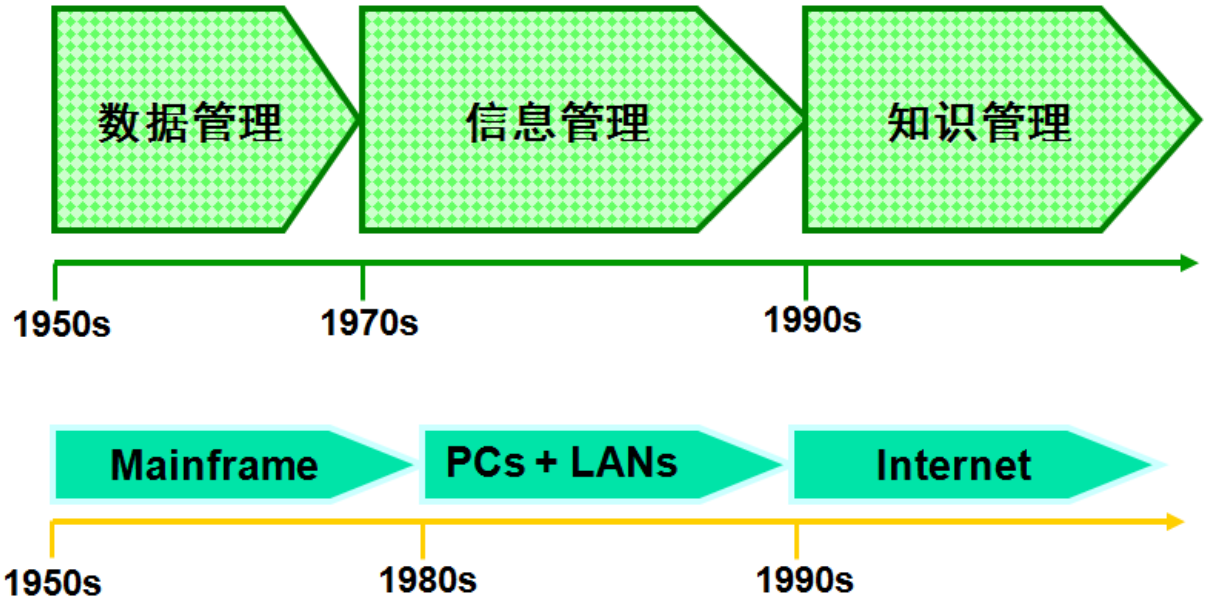
国家安全威胁	**信息战士**	减小美国决策空间、战略优势，制造混乱，进行目标破坏
	情报机构	搜集政治、军事，经济信息
共同威胁	**恐怖分子**	破坏公共秩序，制造混乱，发动政变
	工业间谍	掠夺竞争优势，恐吓
	犯罪团伙	施行报复，实现经济目的，破坏制度
局部威胁	**社会型黑客**	攫取金钱，恐吓，挑战，获取声望
	娱乐型黑客	以吓人为乐，喜欢挑战

在成本与风险间进行平衡

4.我国的信息化的现状

- 胡锦涛总书记2012年11月8日向党的十八大所作的报告中，有19处表述提及信息、信息化、信息网络、信息技术与信息安全。
- 报告明确把“信息化水平大幅提升”纳入全面建成小康社会的目标之一，并提出了走中国特色新型工业化、信息化、城镇化、农业现代化道路，促进这“四化”同步发展。这充分反映了在我国进入全面建成小康社会的决定性阶段，党中央对信息化的高度重视和认识的进一步深化。
- 2014年2月27日，**中央网络安全和信息化领导小组**宣告成立，既表明了网络信息安全目前面临的形势任务复杂和所处地位的重要，也标志着中国已把信息化和网络信息安全列入了国家发展的最高战略方向之一。

信息技术应用重点的转变



启动重大系统工程（1991～2000）

- 1993-1994年，中国政府开始建设三个重大的政府信息系统工程，即“金卡工程”、“金关工程”、以及“金桥工程”，即所谓的三金工程，揭开了大规模建设中国政府信息系统的序幕。
- 中国政府的重大信息系统工程均被冠以“金”字前缀，均以政府信息化为主要目标，“服务”问题并没有提上议事日程。
- 中国政府信息化建设取得了重大的进展，特别是2002年以后，在一些“电子政务” 重大工程的带动之下，政府信息化进入发展的快车道。

互联网上网人数位居世界前列

- 2014年是我国接入国际互联网20周年。
- 2014年7月，中国互联网络信息中心（CNNIC）最新发布的《第34次中国互联网络发展状况统计报告》显示，截至2014年6月，我国网民规模达6.32亿（其中手机网民达5.27亿），互联网普及率达到46.9%，互联网对社会的影响越来越大。
- 手机网络各项指标增长速度全面超越传统网络，手机在微博用户及电子商务应用方面也出现较快增长。

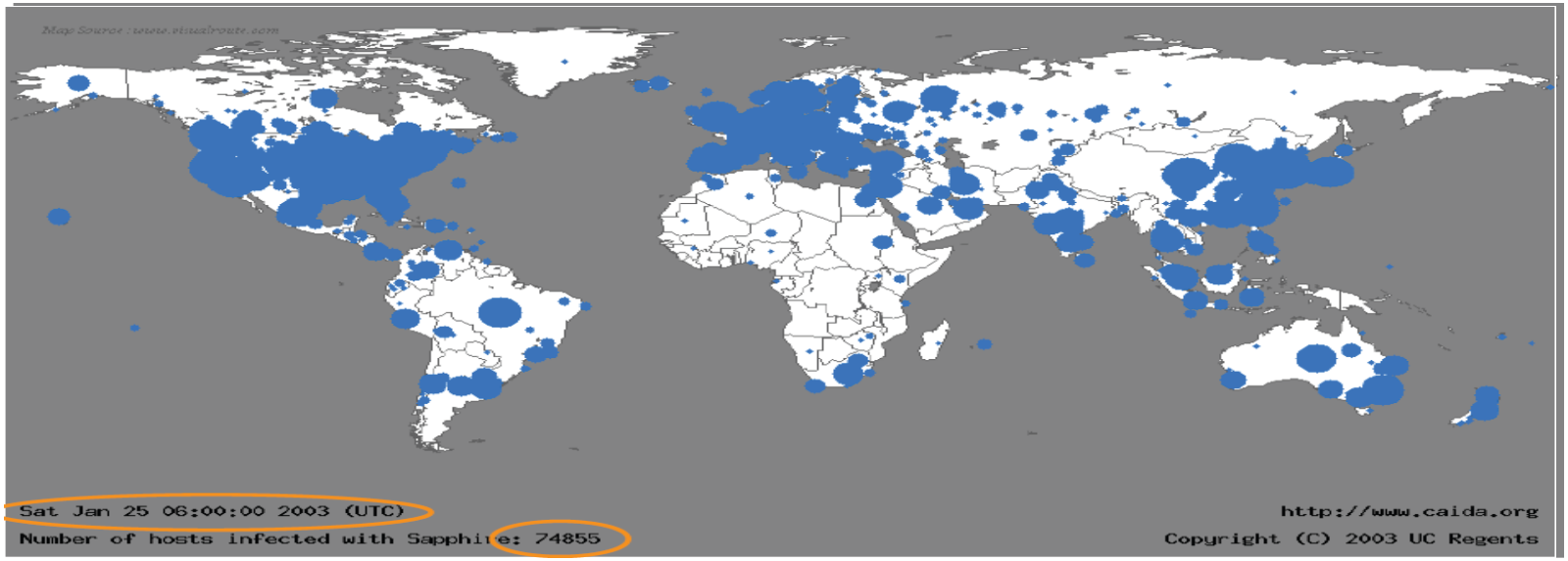
二、信息安全现状分析

- 计算机与Internet相连；
- Internet的四个特点：国际化、社会化、开放化、个人化。
  - 国际化：网络的攻击不仅仅来自本地网络的用户，它可以来自Internet上的任何一个机器。
  - 社会化：全球信息化飞速发展，信息化系统已经成为国家关键基础设施，诸如电信、电子商务、金融网络等，社会对计算机网络的依赖日益增强。
  - 开放化：网络的技术是全开放的，任何一个人、团体都可能获得。开放性和资源共享是网络安全的根源。
  - 个人化：随着网络应用的深入，人类的生活越来越离不开网络，人们可以自由地访问网络，自由地使用和发布各种类型的信息，但同时也面临着来自网络的安全威胁。

信息安全现状分析

Life just before Slammer worm attack

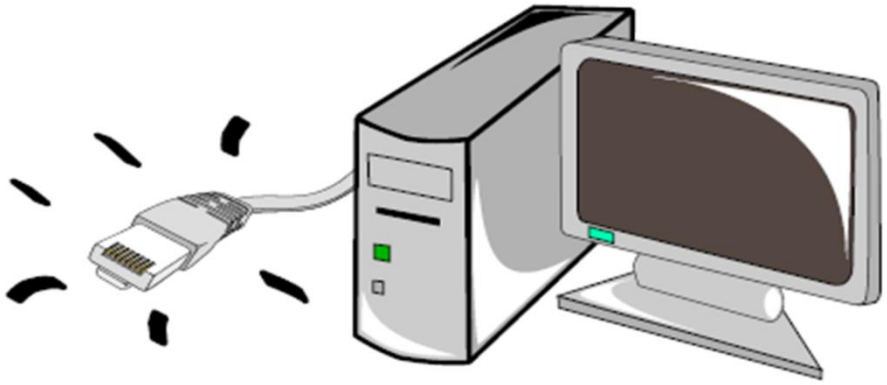
30 minutes later!



Source: CAIDA, www.caida.org/publications/papers/2003/sapphire/sapphire.html

“The most secure computer is the one unplugged from the network.”

——The U.S. Department of Defense C2 rating of Windows NT 3.5 only applied to a computer unplugged from the network!

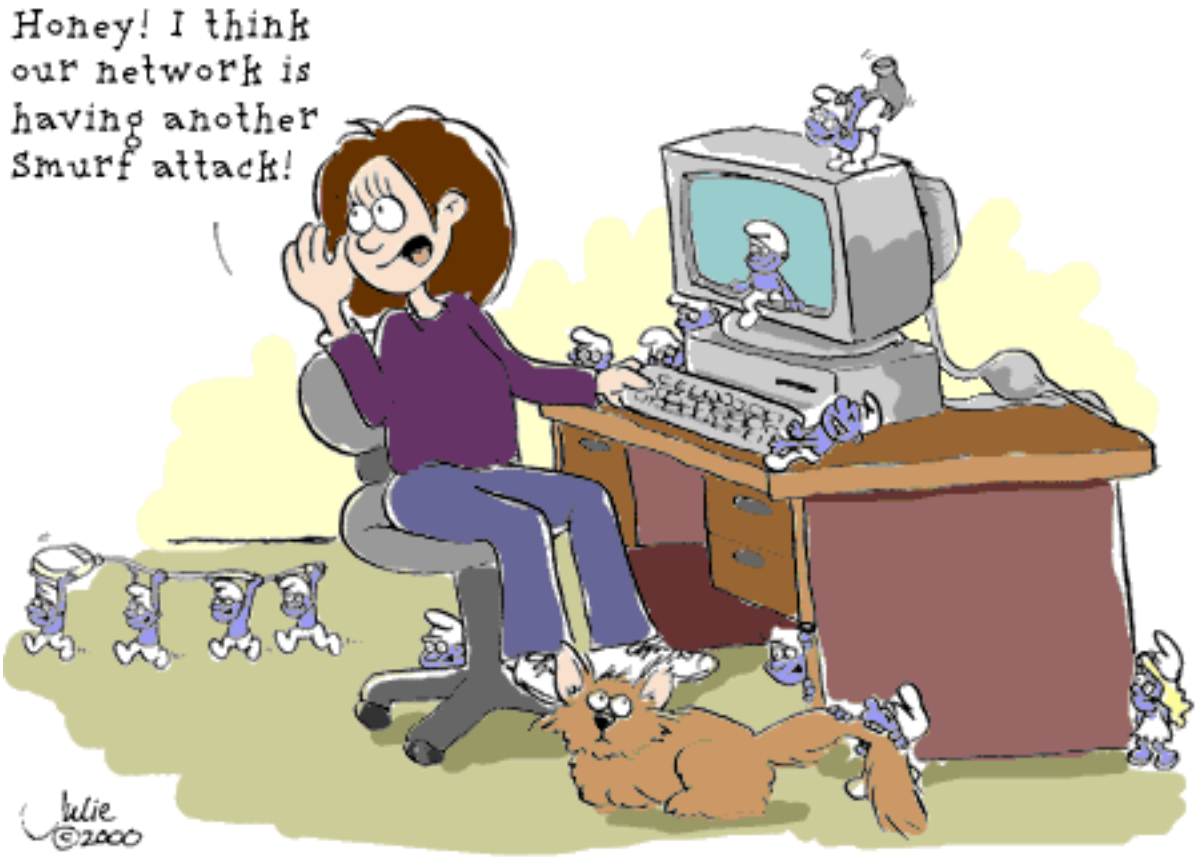


信息安全现状分析

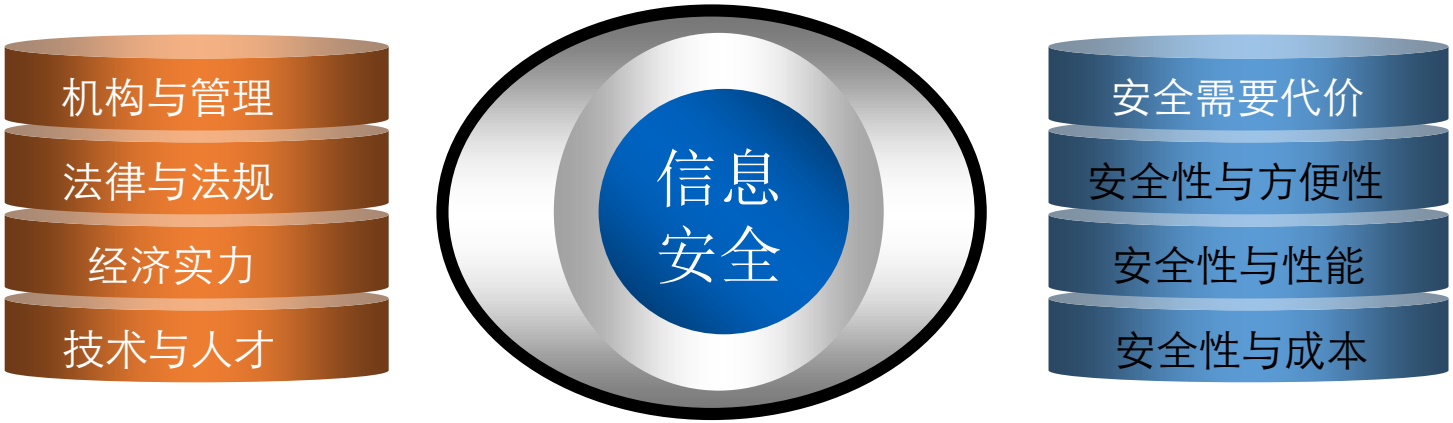
计算机不安全的原因

- 自身缺陷
- 开放性
- 黑客攻击

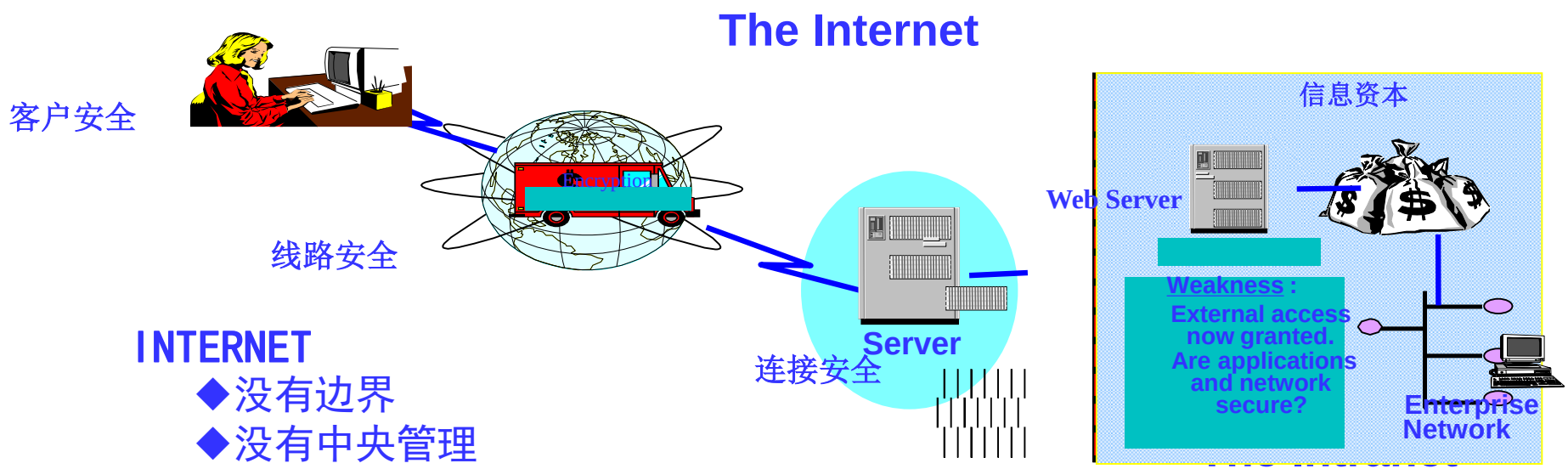
Smurf attack



信息安全不仅是技术问题



为什么网络安全如此重要?



INTERNET

- ◆没有边界
- ◆没有中央管理
- ◆是开放的、标准的
- ◆没有审计记录

- 在信息社会中**信息是一种重要的战略资源，因特网已经成为世界各国获取经济、军事和科技情报的重要战场。信息高速公路为跨国搜集各种战略信息提供了新的机会，国际上围绕信息的获取、使用和控制的斗争愈演愈烈。**“**谁掌握了信息，控制了网络，谁就将拥有整个世界**”（托夫勒）。一个国家的信息获取能力及在社会生产生活领域中的“**制信息权**”，将成为这个国家在新世纪的生存与发展竞争中能否占据主动的关键。

安全事件

- 1986 年Basit和Amjad两兄弟编写的Pakistan 病毒（brain)。
- 1996年9月18日，美国“中央情报局”→“中央愚蠢局”
- 1996年12月，黑客侵入美国空军的全球网网址并将其主页肆意改动，迫使美国国防部一度关闭了其他80多个军方网址。

安全事件

- 2000年2月，在7日、8日和9日三天的时间里，包括Yahoo, Amazon, eBay, CNN.com, BUY.com, ZDNet.com和Excite.com在内的许多著名网站连续三天受到分布式拒绝服务（DDoS）攻击，使美国的这些顶级网站陷入瘫痪。虽然这场对美国8大超级商务网站的攻击只持续了短短三天，但它给美国乃至世界却造成了深远与广泛的影响。据美国杨基集团公司估算，这场由匿名黑客发动的网络攻击事件已经给美国信息产业造成了约12亿美元的巨大损失。

计算机犯罪

- 计算机犯罪是一种新的犯罪形态。归纳为四种：
  - 破坏计算机：是指以计算机作为犯罪行为客体，加以暴力或技术性的破坏。
  - 擅用信息系统：是指无权使用信息系统的人擅自使用。
  - 滥用信息系统：是指以计算机为工具，进行欺诈、侵占、散布非法信息等各种犯罪目的之行为。
  - 破坏安全系统：是指以技术性的方法破坏信息系统在安全方面所采取的措施。

安全隐患

a) 硬件的安全隐患；

b) 操作系统安全隐患；

c) 网络协议的安全隐患；

d) 数据库系统安全隐患；

e) 计算机病毒；

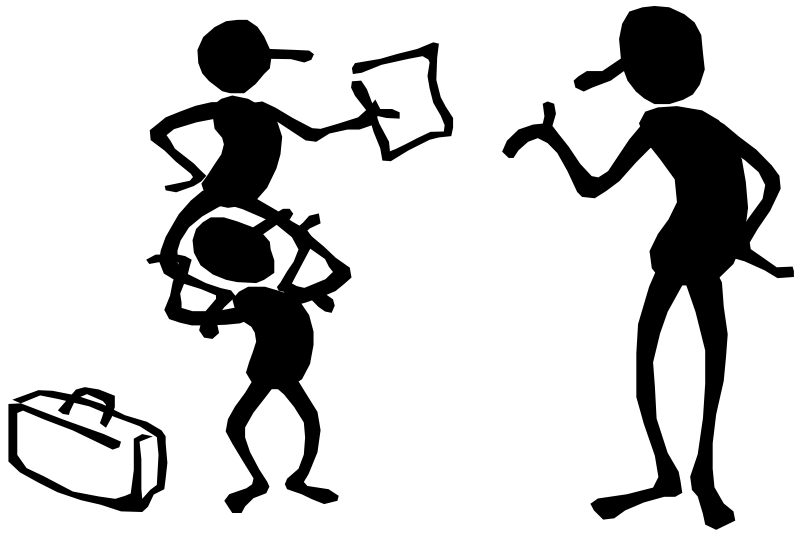
f) 管理疏漏，内部作案。

网络入侵者

- 间谍（商业间谍及其他间谍）
- 盗窃犯
- 破坏者
- 寻求刺激者
- “记录”追求者

网络安全不单是技术问题

- 机构与管理
- 法律与法规
- 经济实力
- 技术与人才



安全需要代价

- 安全性与方便性
- 安全性与性能
- 安全性与成本

作业

- 阅读第4章
- 思考问题：
  - 为了保证加密安全性，加密算法本身应该保密。你怎么看？
  - 密码分析里，什么是统计分析攻击？
  - 分组密码和序列密码之间的区别是什么？
  - 对称密码体制和非对称密码体制的不同之处是什么？