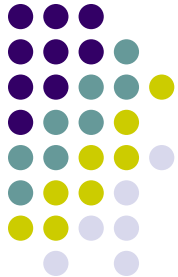
关于信息安全概述

一、信息安全概论

我的信息感受

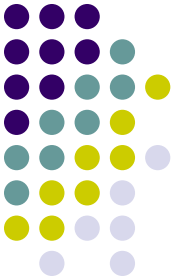
- 电脑的不断普及
- 露天电影——家庭影院
- 银行业务
- 电话的改变
- 邮局业务
- ——电子邮件
- ——电子商务
- ……

信息化出现的新问题



- IT泡沫破裂
- 失业，再就业的起点更高
- 互联网经营模式是什么？
- 网上信息可信度差
- 垃圾电子邮件
- 安全
  - 病毒
  - 攻击
- ……

信息安全形势严峻



- 2000年问题总算平安过渡
- 黑客攻击搅得全球不安
- 计算机病毒两年来网上肆虐
- 白领犯罪造成巨大商业损失
- 数字化能力的差距造成世界上不平等竞争
- 信息战阴影威胁数字化和平

Information and Network Security

We will demonstrate that 62% of all systems can be penetrated in less than 30 minutes.

More than half of all attacks will come from inside your own organization

from TNN.com

什么是安全

- 国际标准化委员会
  - 为数据处理系统和采取的技术的和管理的安全保护，保护计算机硬件、软件、数据不因偶然的或恶意的原因而遭到破坏、更改、显露。
- 美国国防部国家计算机安全中心
  - 要讨论计算机安全首先必须讨论对安全需求的陈述，……。 一般说来，安全的系统会利用一些专门的安全特性来控制对信息的访问，只有经过适当授权的人，或者以这些人的名义进行的进程可以读、写、创建和删除这些信息。
- 公安部计算机管理监察司
  - 计算机安全是指计算机资产安全，即计算机信息系统资源和信息资源不受自然和人为有害因素的威胁和危害。

信息安全的级别

- 按照范围和处理方式的不同，通常将信息安全划分为三个级别：
  - 第1级为计算机安全
  - 第2级为网络安全
  - 第3级为信息系统安全

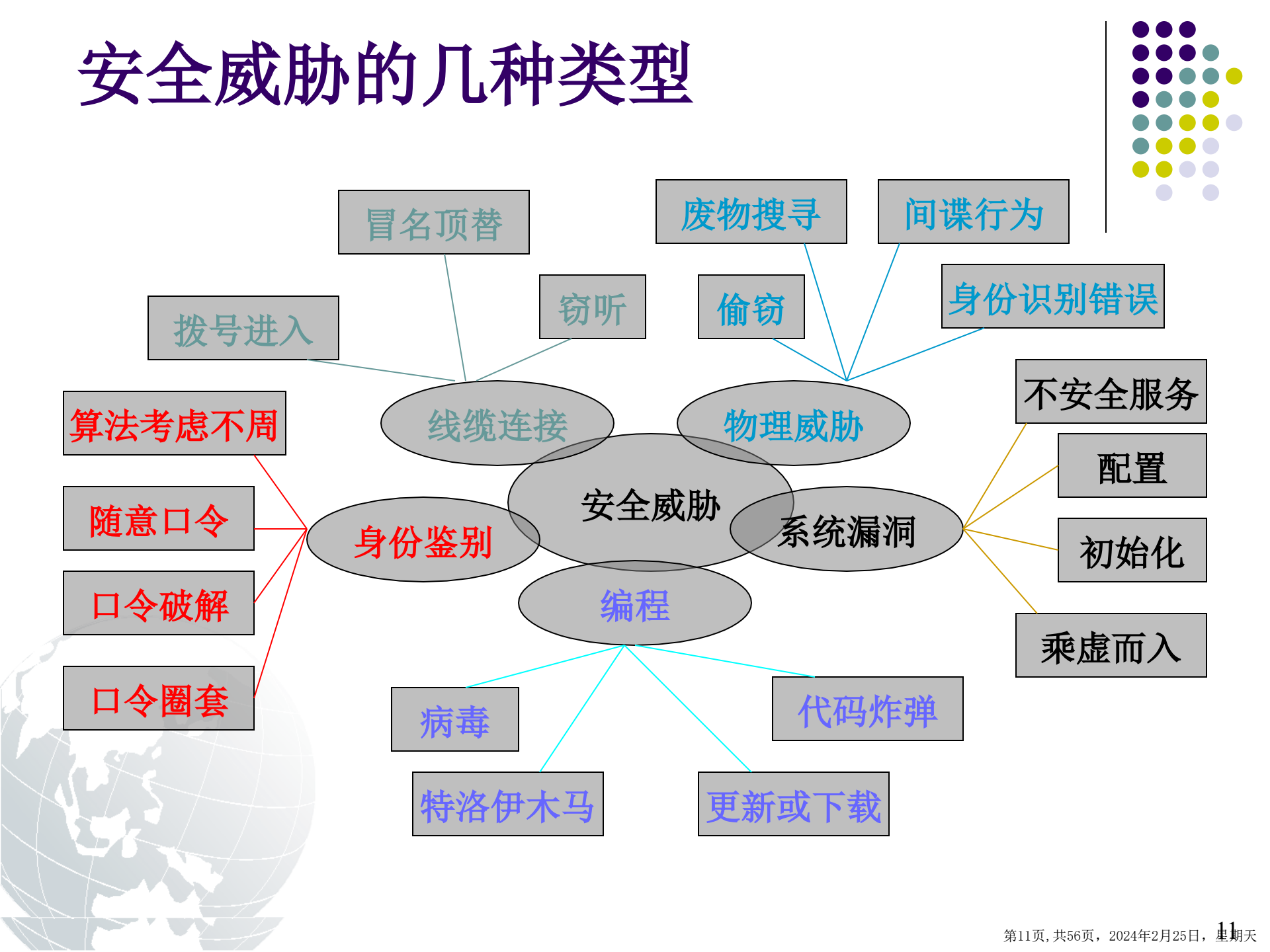
安全的几个要素

- 可用性
  - 授权实体有权访问数据。
- 机密性
  - 信息不暴露给未授权实体或进程。
- 完整性
  - 保证数据不被未授权修改。
- 可控性
  - 控制授权范围内的信息流向及操作方式。
- 可审查性
  - 对出现的安全问题提供依据与手段。

安全威胁的来源

- 外部渗入
  - 未被授权使用计算机的人。
- 内部渗入者
  - 被授权使用计算机，但不能访问某些数据、程序或资源，它包括
    - 冒名顶替:使用别人的用户名和口令进行操作；
    - 隐蔽用户:逃避审计和访问控制的用户；
- 滥用职权者
  - 被授权使用计算机和访问系统资源，但滥用职权者。

安全威胁的几种类型


安全威胁
线缆连接
物理威胁
身份鉴别
系统漏洞
编程
冒名顶替
拨号进入
窃听
废物搜寻
间谍行为
偷窃
身份识别错误
算法考虑不周
随意口令
口令破解
口令圈套
不安全服务
配置
初始化
乘虚而入
病毒
特洛伊木马
代码炸弹
更新或下载

安全的目标

- 保障安全的基本目标就是要能具备
  - 安全保护能力
  - 隐患发现能力
  - 应急反应能力
  - 信息对抗能力

信息对抗能力已经不只是科技水平的体现，更是综合国力的体现。未来的战争无疑是始于信息战，以网络为基础的信息对抗将在一定程度上决定战争的胜负

二、信息安全概况

信息安全概况

- CERT有关安全事件的统计

1988-1989

Year	1988	1989
Incidents	6	132

1990-1999

Year	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999
Incidents	252	406	773	1,334	2,340	2,412	2,573	2,134	3,734	9,859

2000-2003

Year	2000	2001	2002	2003
Incidents	21,756	52,658	82,094	137,529

- **CERT有关安全事件的统计**

1995-1999

Year	1995	1996	1997	1998	1999
Vulnerabilities	171	345	311	262	417

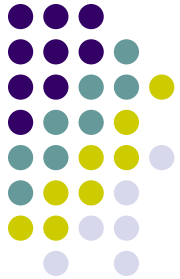
2000-2006

Year	2000	2001	2002	2003	2004	2005	2006
Vulnerabilities	1,090	2,437	4,129	3,784	3,780	5,990	8,064

Total vulnerabilities reported (1995-2006): **30,780**

三、信息安全体系

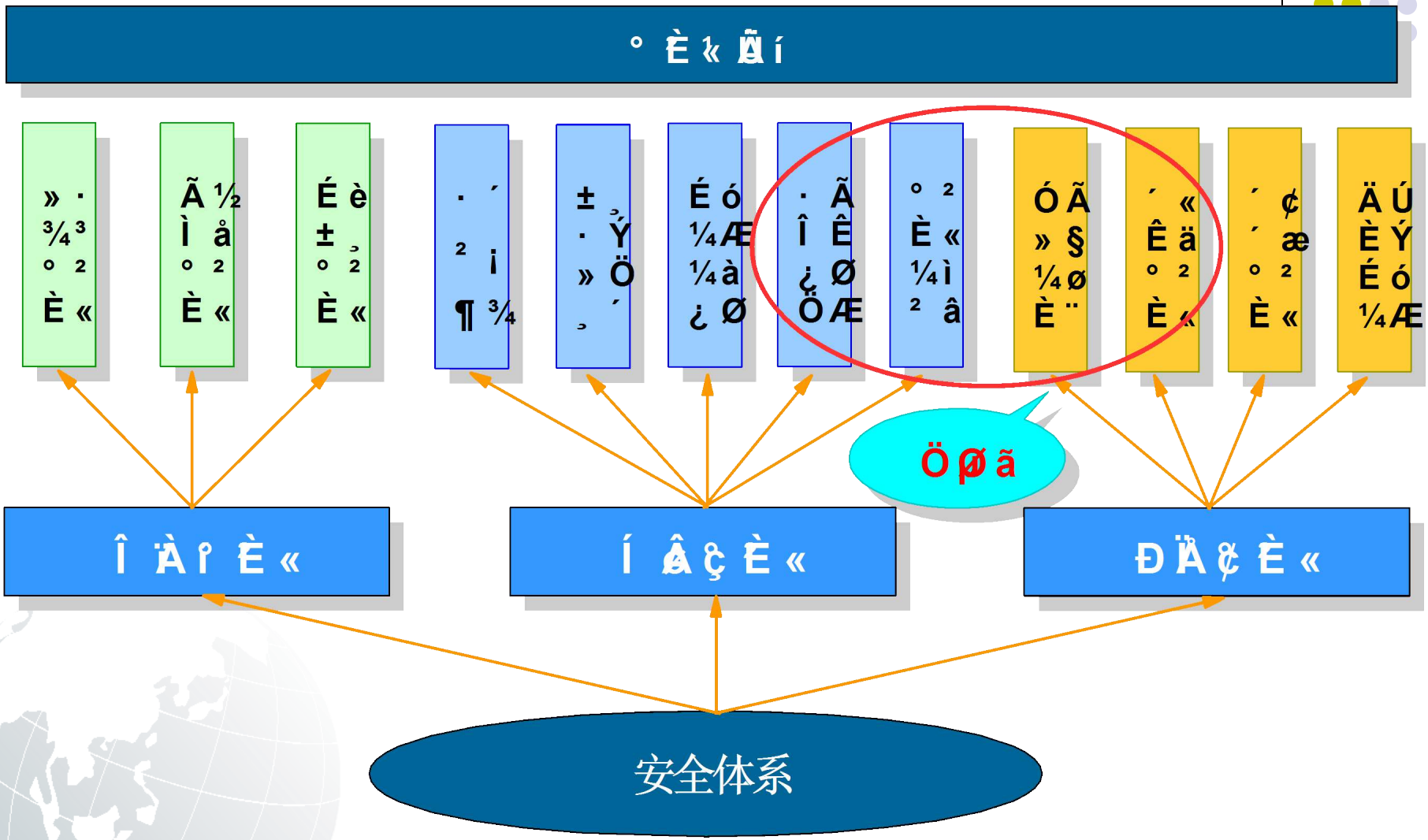
信息安全体系



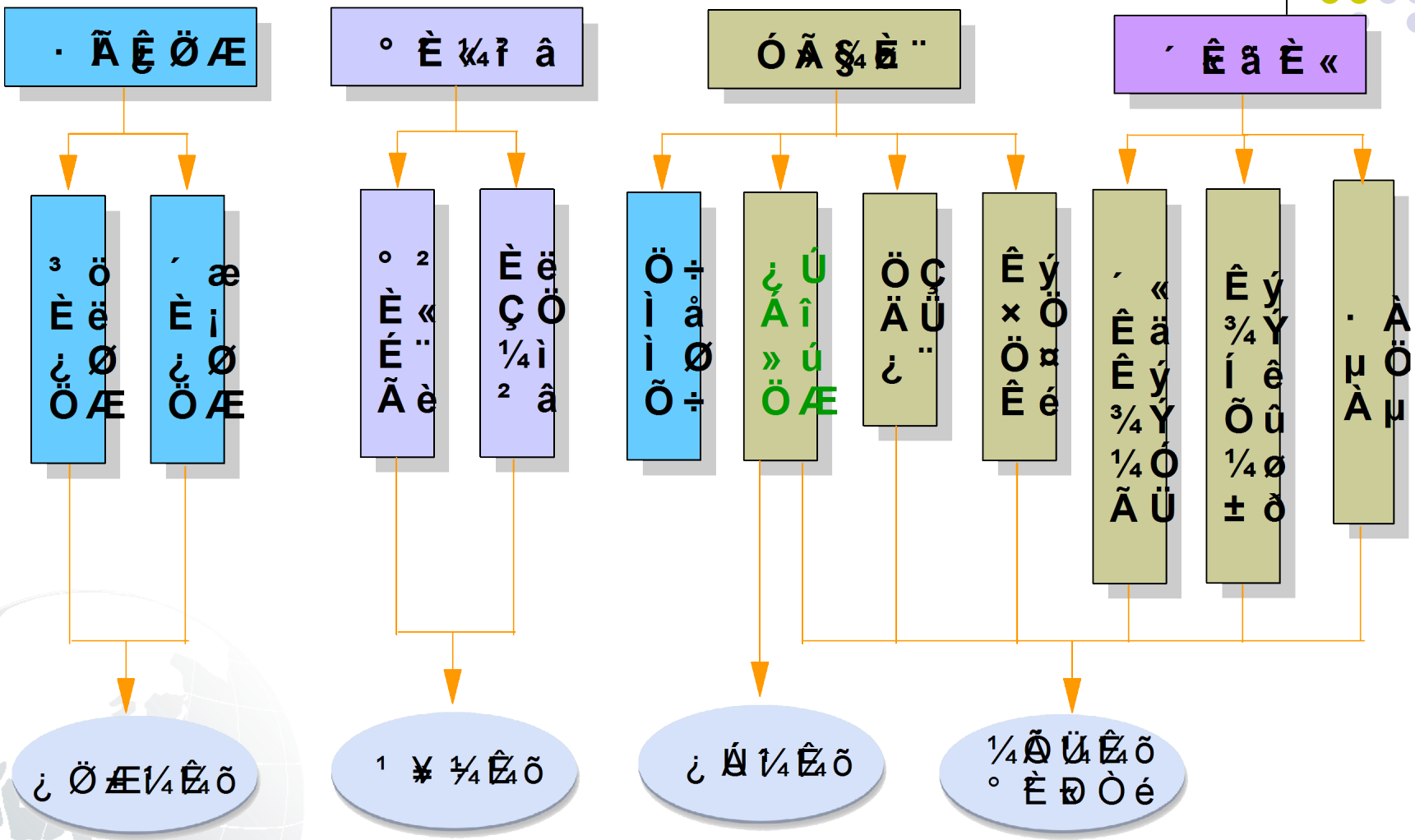
安全必要性

- 伴随互联网发展重要信息变得非常容易被获取
  - 个人数据
  - 重要企业资源
  - 政府机密
- 网络攻击变的越来越便利
  - 黑客（crack）技术在全球范围内共享
  - 易用型操作系统和开发环境普及

信息安全体系

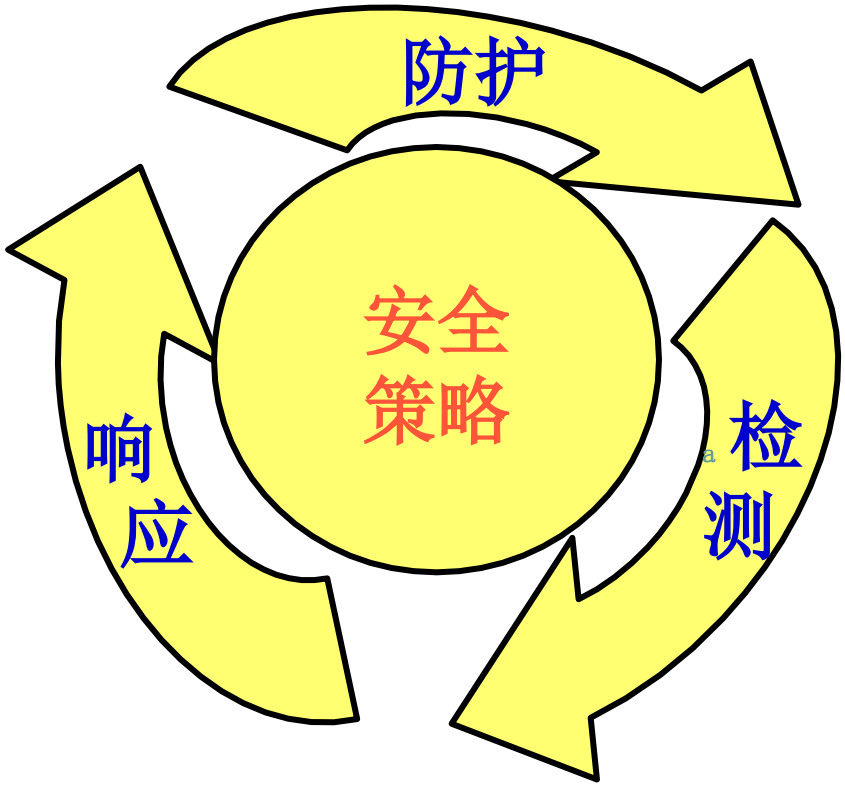

° È « ÑÃ í
» · ¾ ³ ° ² È «
Ã ½ Ì å ° ² È «
É è ± ¸ ° ² È «
· ´ ² ¡ ¶ ¾
± ¸ · Ý » Ö ¸ ´
É ó ¼ Æ ¼ à ¿ Ø
· Ã Î Ê ¿ Ø Ö Æ
° ² È « ¼ ì ² â
Ó Ã » § ¼ ø È ¨
´ « Ê ä ° ² È «
´ ¢ ´ æ ° ² È «
Ä Ú È Ý É ó ¼ Æ
Ö ø ã
Î ÄÎ È «
Í ÂÇ È «
Ð ÄÇ È «
安全体系

信息安全体系



安全体系结构

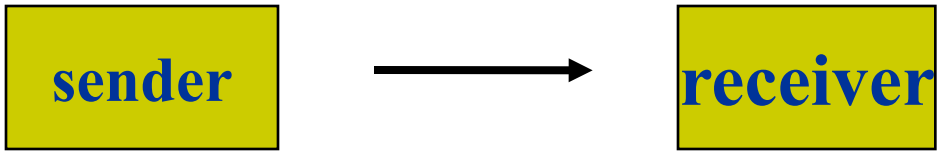
安全模型——P2DR



P2DR（Policy、Protection、Detection、Response）模型是安全管理基本思想，贯穿IP网络的各个层次

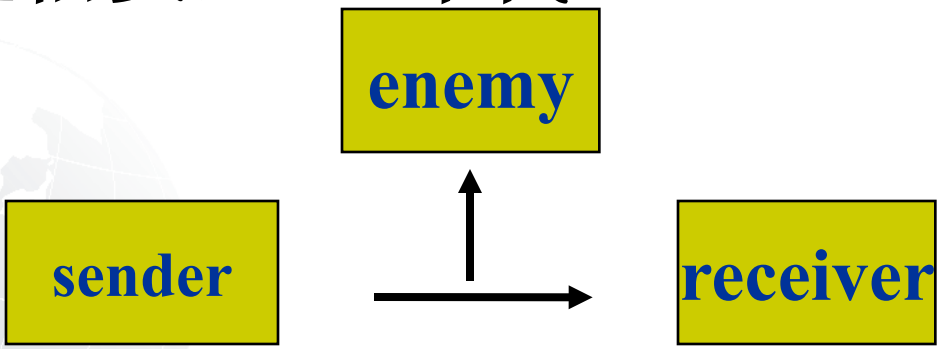
信息通讯环境

- 基本的通讯模型



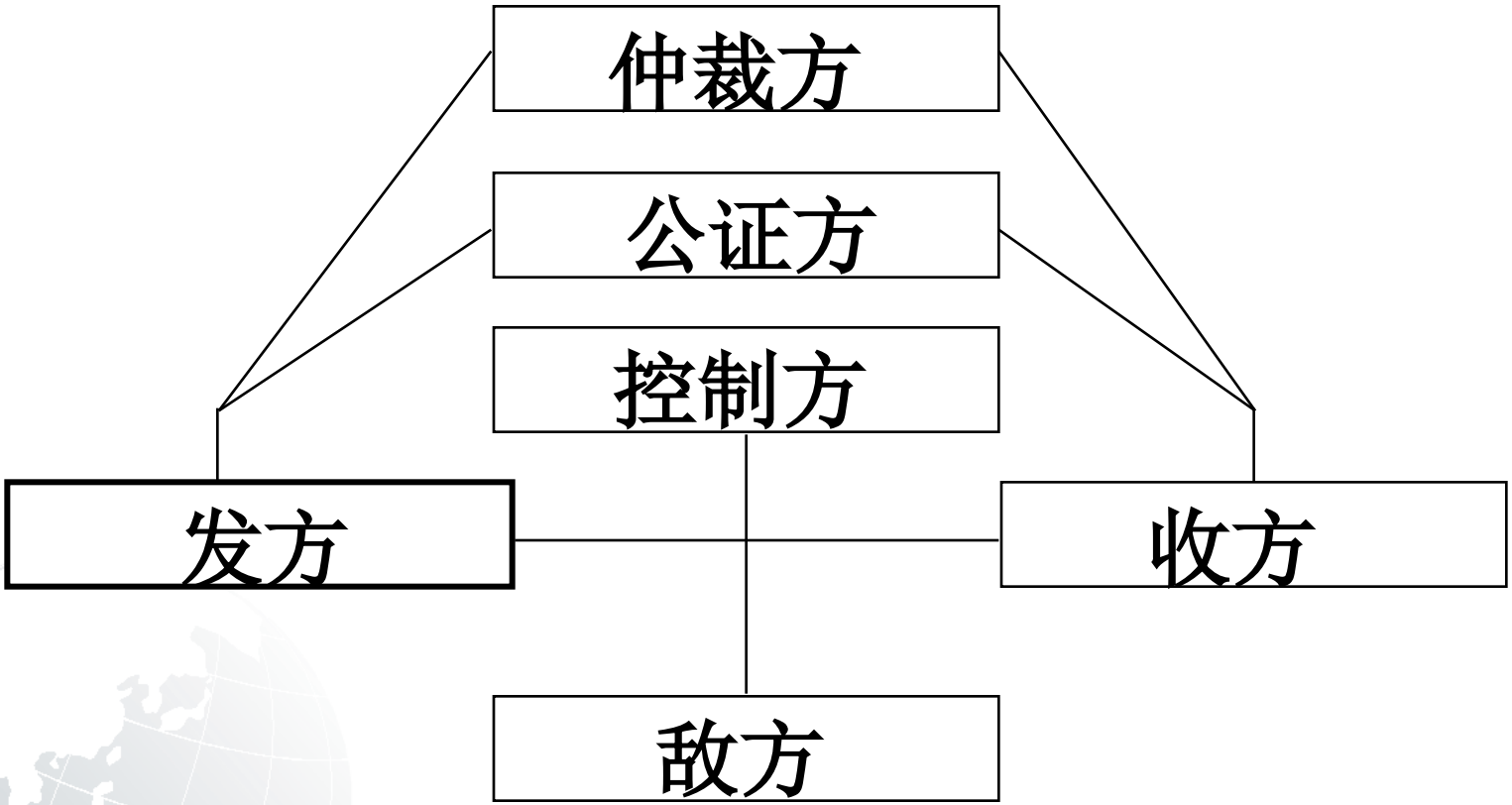
信源编码
信道编码
信道传输
通信协议

- 通信的保密模型
  通信安全-60年代（COMSEC）

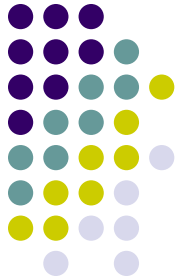


信源编码
信道编码
信道传输
通信协议
密码

网络通讯的信息安全模型



从信息安全到信息保障

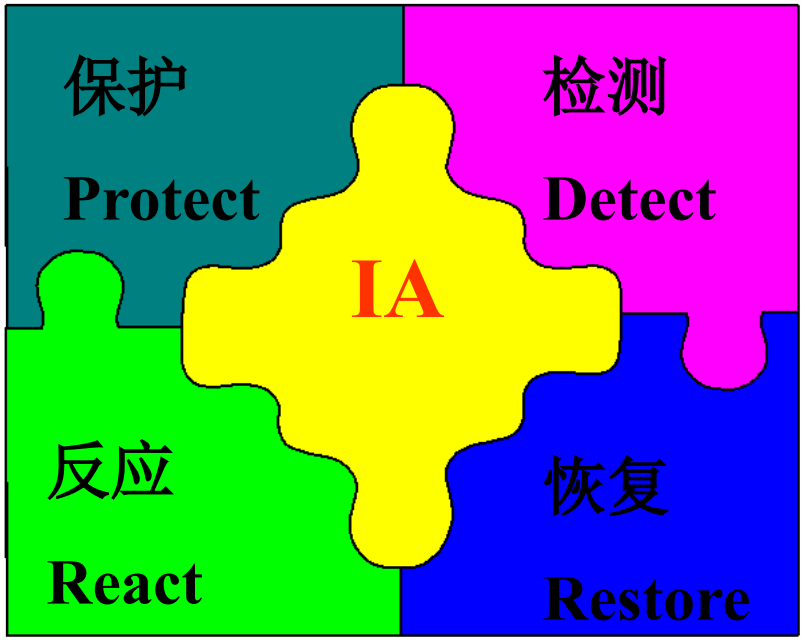


- 通信保密（COMSEC）：60年代
- 计算机安全（COMPUSEC）：60-70年代
- 信息安全（INFOSEC）：80-90年代
- 信息保障（IA）：90年代-

四、信息系统安全保障体系

什么是信息保障

- Information Assurance
  - 保护（Protect）
  - 检测（Detect）
  - 反应（React）
  - 恢复（Restore）



PDRR

- 保护（Protect）
  - 采用可能采取的手段保障信息的保密性、完整性、可用性、可控性和不可否认性。
- 检测（Detect）
  - 利用高级术提供的工具检查系统存在的可能提供黑客攻击、白领犯罪、病毒泛滥脆弱性。
- 反应（React）
  - 对危及安全的事件、行为、过程及时作出响应处理，杜绝危害的进一步蔓延扩大，力求系统尚能提供正常服务。
- 恢复（Restore）
  - 一旦系统遭到破坏，尽快恢复系统功能，尽早提供正常的服务。

国内外现状及发展趋势

- 美国：
  - 1998年5月22日总统令(PDD-63)：《保护美国关键基础设施》
  - 围绕“信息保障”成立了多个组织，包括：全国信息保障委员会、全国信息保障同盟、关键基础设施保障办公室、首席信息官委员会、联邦计算机事件响应行动组等十多个全国性机构
  - 1998年美国国家安全局（NSA）制定了《信息保障技术框架》（IATF），提出了“深度防御策略”，确定了包括网络与基础设施防御、区域边界防御、计算环境防御和支撑性基础设施的深度防御目标
  - 2000年1月，发布《保卫美国计算机空间—保护信息系统的国家计划》。分析了美国关键基础设施所面临的威胁，确定了计划的目标和范围，制定出联邦政府关键基础设施保护计划（民用机构和国防部），以及私营部门、洲和地方政府的关键基础设施保障框架。

国内外现状及发展趋势

- 俄罗斯：
  - 1995年颁布《联邦信息、信息化和信息保护法》，为提供高效益、高质量的信息保障创造条件，明确界定了信息资源开放和保密的范畴，提出了保护信息的法律责任。
  - 1997年出台《俄罗斯国家安全构想》。明确提出“保障国家安全应把保障经济安全放在第一位”，而“信息安全又是经济安全的重中之重。
  - 2000年普京总统批准了《国家信息安全学说》，明确了联邦信息安全建设的任务、原则和主要内容。第一次明确了俄罗斯在信息领域的利益是什么，受到的威胁是什么，以及为确保信息安全首先要采取的措施等。