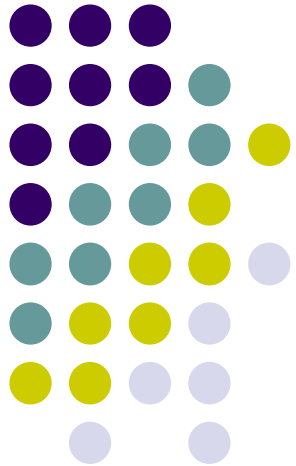
网络安全

罗　敏

网络安全学院

mluo@whu.edu.cn

13907125177　QQ: 5118924



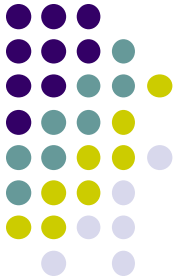
群名称：2019上网络安全

群　号：716087669

课程安排

- 课堂讲授+上机实践的教学方式；
- 了解和掌握网络与信息安全的基本原理、技术、及最新研究成果；
- 具有网络与信息安全的理论基础和基本实践能力；
- 考试分平时作业(50%)和期末笔试(50%)。

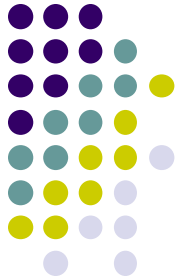
本课程的目的



- 提高安全意识
- 掌握网络攻防技术的原理、方法和工具
- 信息系统的安全解决方案
- 掌握Internet的安全性

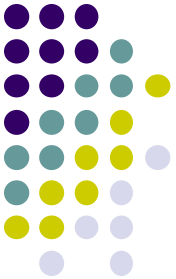
- 信息安全内容广阔
  - 密码学
  - 网络安全
  - 系统安全
  - 安全的信息系统
- 涉及到许多其它领域的知识
- 实践性强
- 学习方法
  - 阅读一些系统性较强的教材
  - 找到经典的论文
  - 案例研究

课程基础知识



- 密码学
- 计算机网络(TCP/IP)
- 操作系统(UNIX和Windows)
- 程序设计

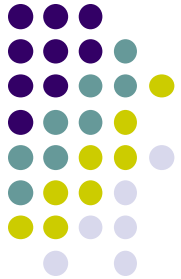
参考书籍



Required readings:

http://en.wikipedia.org/wiki/Network_security

- **William Stallings, *Cryptography and network security: principles and practice***
- **Ed Skoudis with Tom Liston: *Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses*. Prentice Hall**
- **Ross Anderson: Security Engineering: *A Guide to Building Dependable Distributed Systems*. Wiley.**
- **其他准备知识的书籍**
  - **TCP/IP\OS\Windows NT/2000**

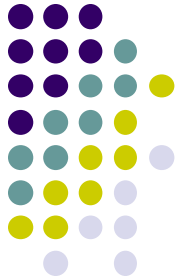


一、网络安全概论

我的信息感受

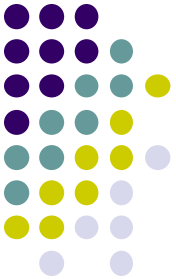
- 电脑的不断普及
- 露天电影——家庭影院
- 银行业务
- 电话的改变
- 邮局业务
- ——电子邮件
- ——电子商务
- ……

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



- 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

信息化与国家安全——信息战

“谁掌握了信息，控制了网络，谁将拥有整个世界。”

（美国著名未来学家阿尔温 托尔勒）

“今后的时代，控制世界的国家将不是靠军事，而是信息能力走在前面的国家。”

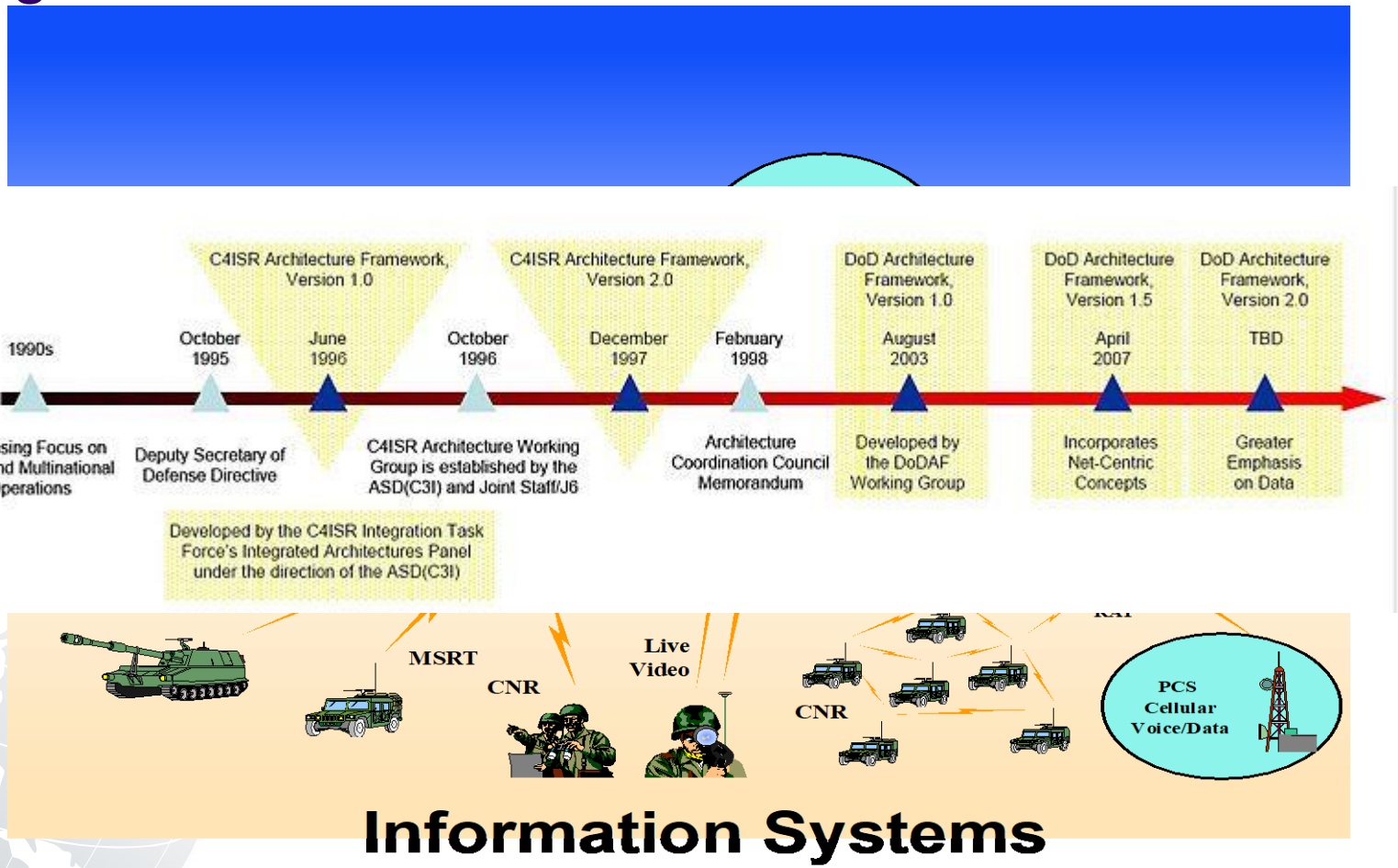
（美国总统克林顿）

“信息时代的出现，将从根本上改变战争的进行方式。”

（美国前陆军参谋长沙利文上将）

C4I(Department of Defense Architecture Framework (DoDAF))

Command, Control, Communications, Computers and Intelligence



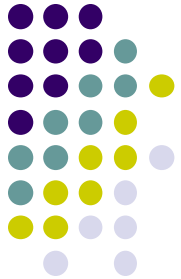
Information and Network Security

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

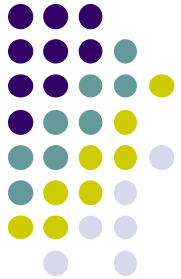
from TNN.com

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。

Recent Security News



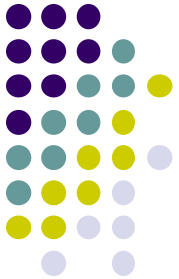
- Snowden leaks information about various NSA data collection programs
  - Phone call record
  - Supposedly email, instant message, etc.

- Facebook CEO’s page hacked by Palestinian Khalil Shreateh to demonstrate bugs in Facebook

In the News Last Year: Hackers Force Apple, Amazon to Change Security Policy

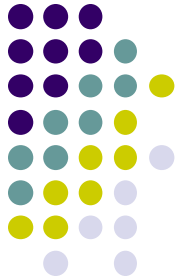
- What happened?
  - Hackers gained access to Mat Honan (a reporter)'s iCloud account, then (according to Honan)
    - At 5:00 PM, they remote wiped my iPhone
      At 5:01 PM, they remote wiped my iPad
      At 5:05, they remote wiped my MacBook Air.
- How did the attacker get access to iCloud account? Any guess?
- Lessons?
  - Security only as strong as the weakest link.
  - Information sharing across platforms can lead to unexpected vulnerabilities

Stuxnet (2010)



- Stuxnet: Windows-based Worm
  - Worm: self-propagating malicious software (malware)
- Attack Siemens software that control industrial control systems (ICS) and these systems
  - Used in factories, chemical plants, and nuclear power plants
- First reported in June 2010, the general public aware of it only in July 2010
- Seems to be a digital weapon created by a nation-state
  - 60% (more than 62 thousand) of infected computers in Iran
  - Iran confirmed that nuclear program damaged by Stuxnet
  - Sophisticated design, special targets, expensive to develop

Malware That Appear to Be Related to Stuxnet

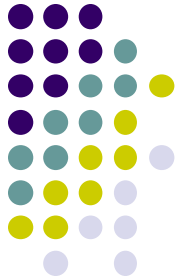


- Duqu (September 2011)
  - Use stolen certificates, exploits MS Word
- Flame (May 2012)
  - A tool for cyber espionage in Middle East (infecting approx. 1000 machines, mostly in Iran)
  - “Suicide” after being discovered
  - 20 Mbytes, with SQLLite DB to store info, hide its own presence, exploit similar vulnerabilities as StuxNet, adjust its behavior to different Anti-Virus
  - Presents a novel way to produce MD5 hash collision to exploit certificates

信息安全的级别

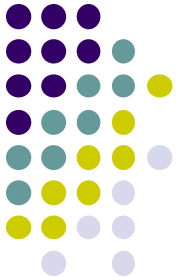
- 按照范围和处理方式的不同，通常将信息安全划分为三个级别：
  - 第1级为计算机安全
  - 第2级为网络安全
  - 第3级为信息系统安全

安全的几个要素



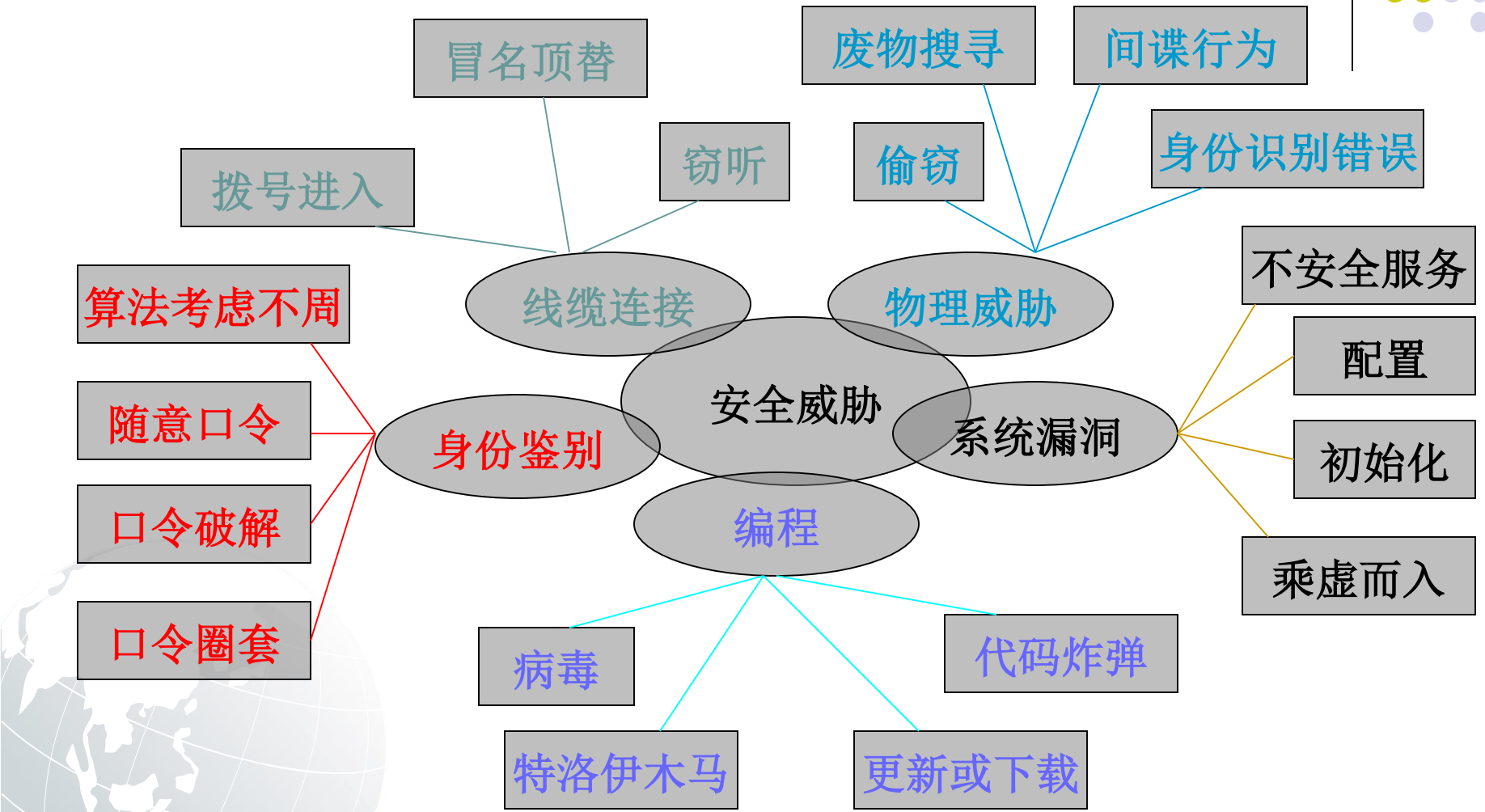
- 可用性
  - 授权实体有权访问数据。
- 机密性
  - 信息不暴露给未授权实体或进程。
- 完整性
  - 保证数据不被未授权修改。
- 可控性
  - 控制授权范围内的信息流向及操作方式。
- 可审查性
  - 对出现的安全问题提供依据与手段。

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

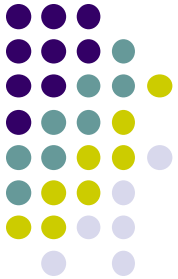

安全威胁
线缆连接
物理威胁
身份鉴别
系统漏洞
编程
冒名顶替
拨号进入
窃听
废物搜寻
间谍行为
偷窃
身份识别错误
算法考虑不周
随意口令
口令破解
口令圈套
不安全服务
配置
初始化
乘虚而入
病毒
特洛伊木马
代码炸弹
更新或下载

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

第一章回顾



- 什么是安全
- 信息安全的级别
- 安全的几个要素
- 安全威胁的来源
- 安全的目标

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**

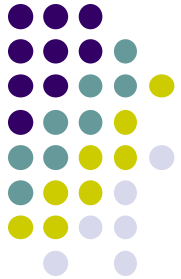
1995-1999

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

2000-2006

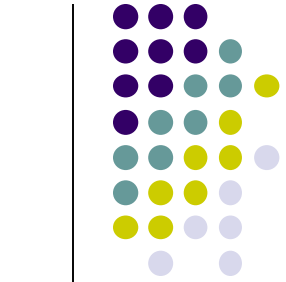
Year	2000	2001	2002	2003	2004	2005	2006
Vulnerabilities	1,090	2,437	4,129	3,784	3,780	5,990	8,064

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



三、信息安全体系

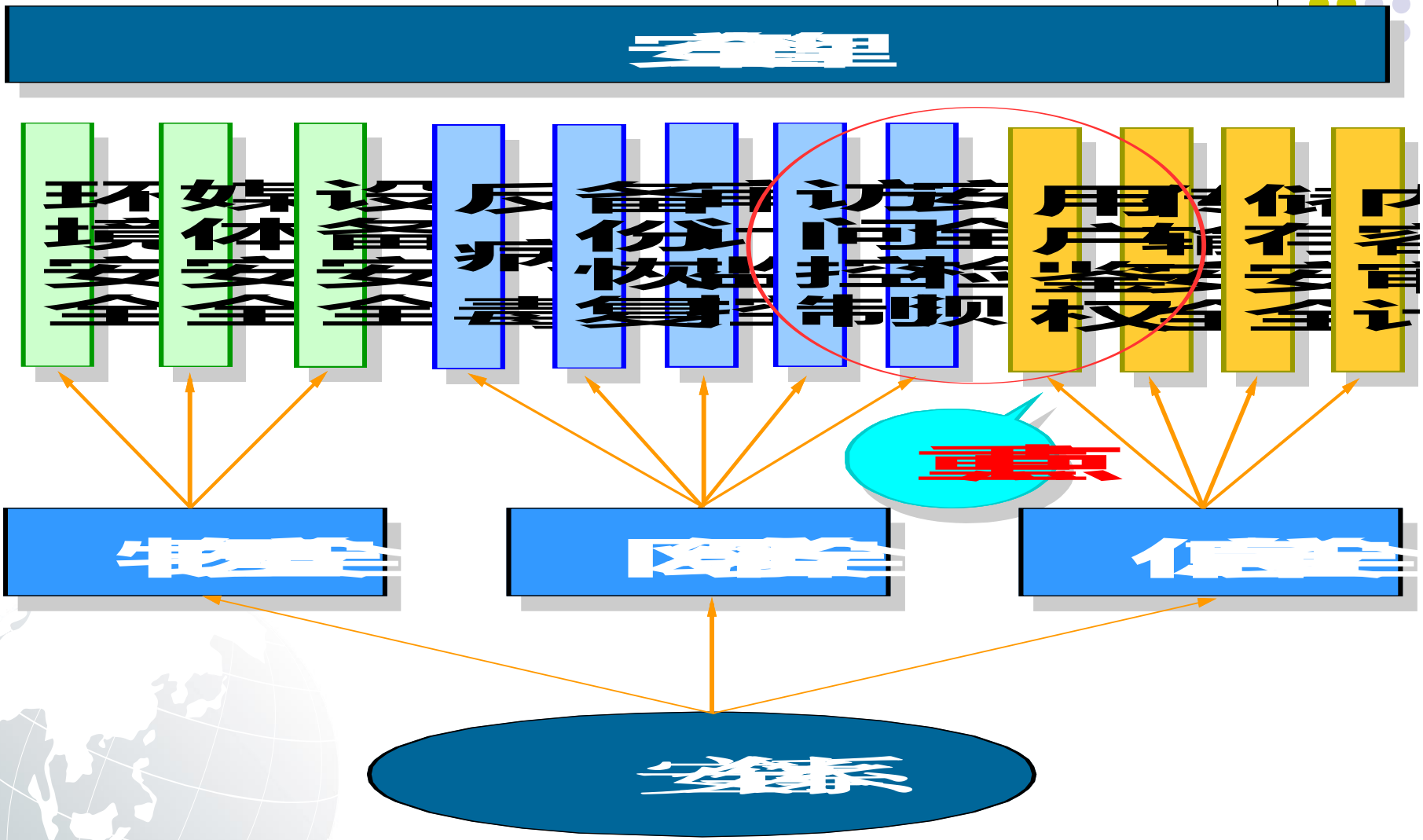
信息安全体系



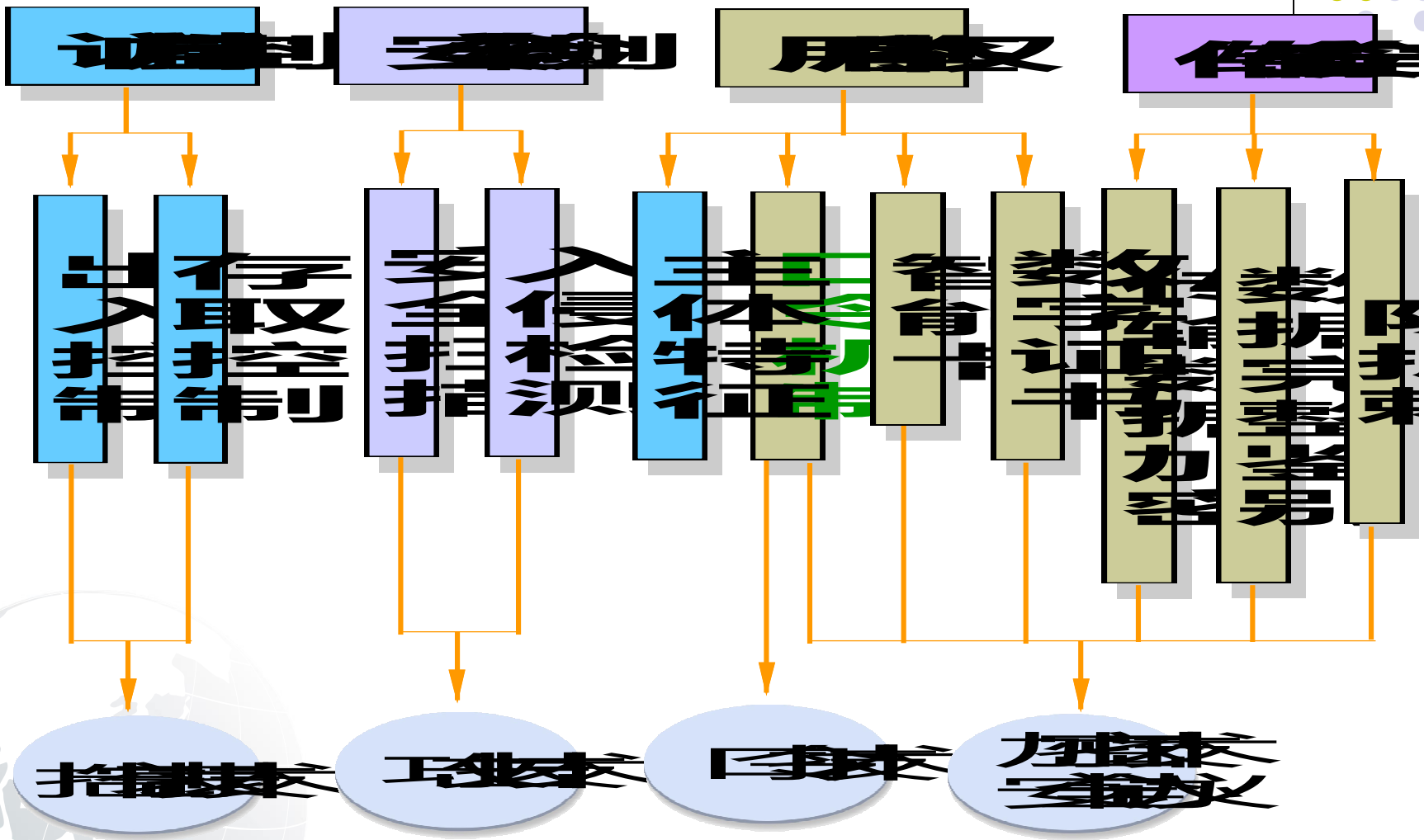
安全必要性

- 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

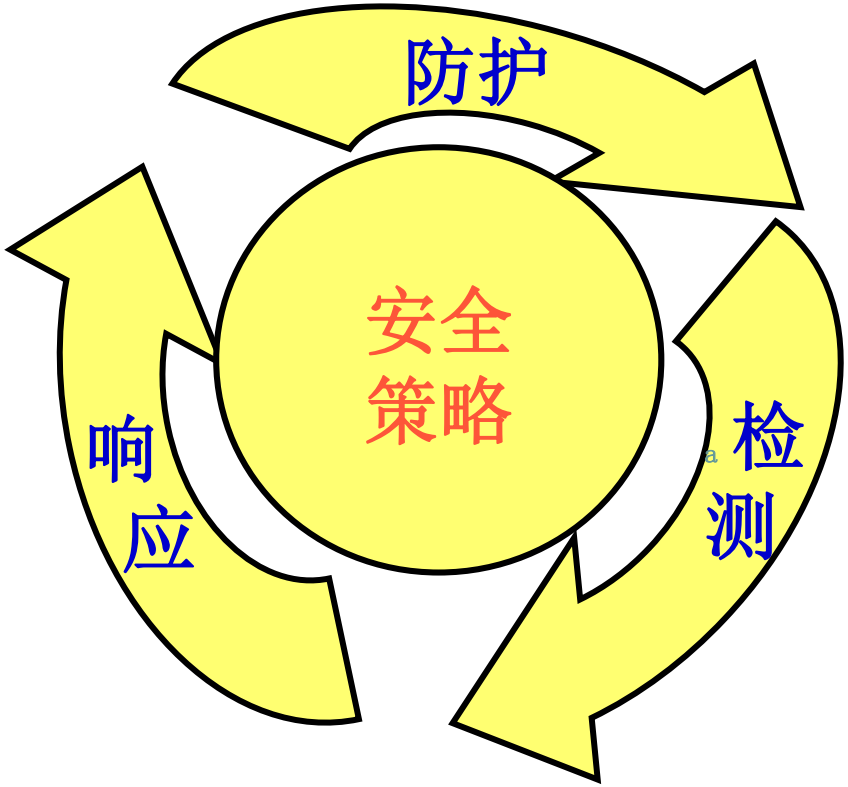

管理
环境安全
媒体安全
设备安全
反病毒
备份与恢复
审计跟踪
访问控制
身份鉴别
用户管理
授权
重点
物理安全
网络安全
信息安全
技术

信息安全体系



安全体系结构

安全模型——P2DR



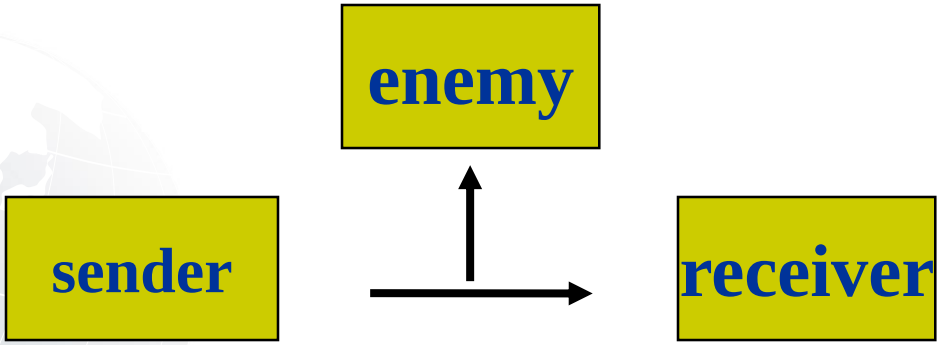
P2DR（Policy、Protection、Detection、Response）模型是安全管理基本思想，贯穿IP网络的各个层次

信息通讯环境

- 基本的通讯模型

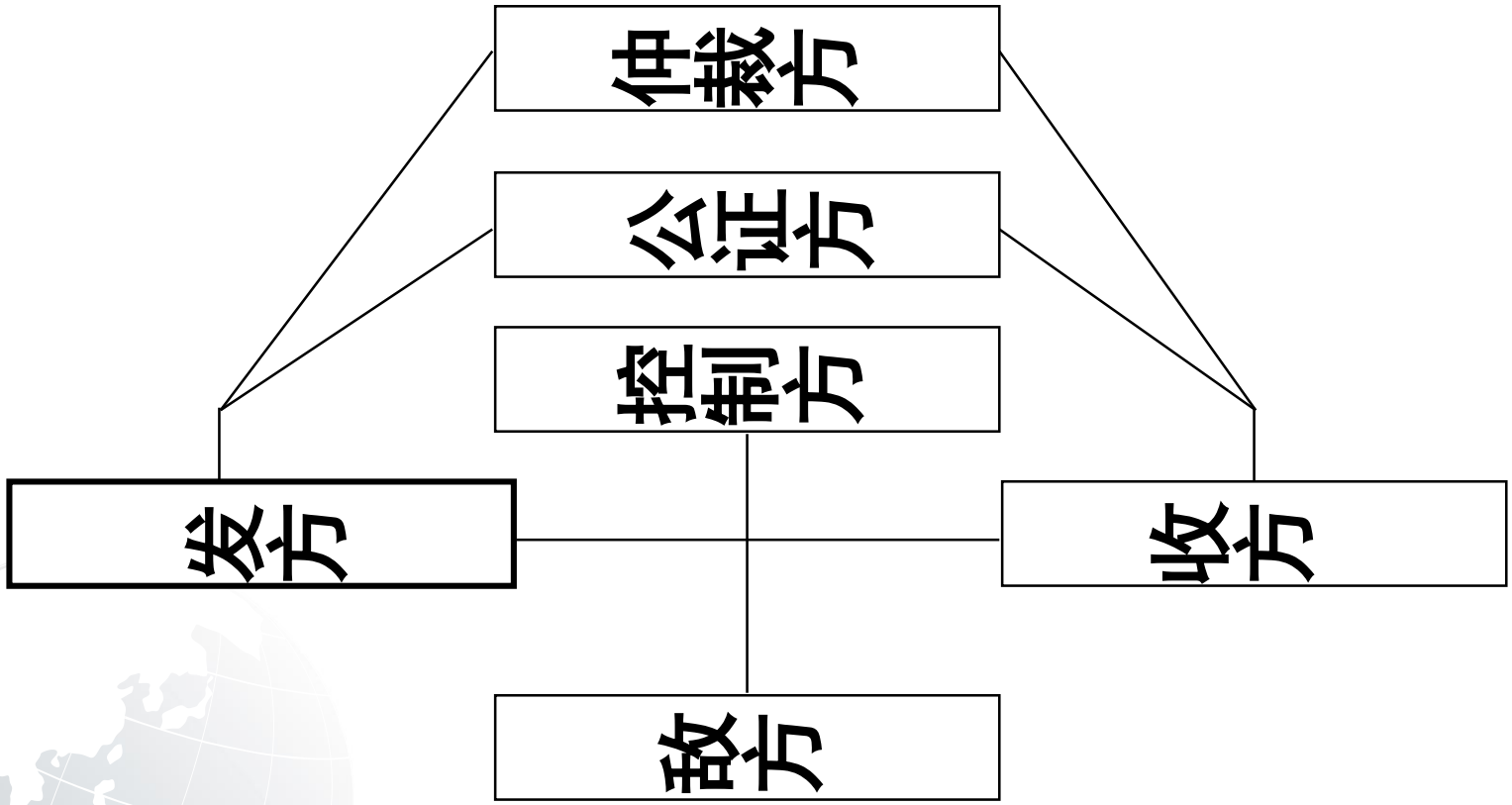
信源编码
信道编码
信道传输
通信协议

- **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



Internet网络安全技术(1)

- 安全内核技术
  - 安全等级制
- 身份鉴别技术
  - Kerberos
- Web安全技术
  - SSL
  - SHTTP
- SOCKS协议
- 网络反病毒技术
- 防火墙技术
  - 动态IP过滤技术
  - IP分片过滤技术
  - IP欺骗保护
  - 地址转换
  - 访问控制
- 保密网关技术
  - 面向信息与面向客户
  - 综合安全与保密策略实现

Internet网络安全技术(2)

- ISO7498-2，信息安全体系结构
  - 1989.2.15颁布，确立了基于OSI参考模型的七层协议之上的信息安全体系结构
    - 五大类安全服务(鉴别、访问控制、保密性、完整性、抗否认）
    - 八类安全机制(加密、数字签名、访问控制、数据完整性、鉴别交换、业务流填充、路由控制、公证）
    - OSI安全管理

Internet网络安全技术(3)

- ISO7498-2到TCP/IP的映射

安全服务	TCP/IP 协议层			
	网络接口	互联网层	传输层	应用层
对等实体鉴别	-	Y	Y	Y
数据源鉴别	-	Y	Y	Y
访问控制服务	-	Y	Y	Y
连接保密性	Y	Y	Y	Y
无连接保密性	Y	Y	Y	Y
选择域保密性	-	-	-	Y
流量保密性	Y	Y	-	Y
有恢复功能的连接完整性	-	-	Y	Y
无恢复功能的连接完整性	-	Y	Y	Y
选择域连接完整性	-	-	-	Y
无连接完整性	-	Y	Y	Y
选择域非连接完整性	-	-	-	Y
源发方不可否认	-	-	-	Y
接收方不可否认	-	-	-	Y

国际Internet安全技术活动(1)

- 互连网层安全协议
  - IPSO（IP Security Option)[RFC1108]
    - 美国国防部安全规范，仅适用军事封闭网
  - SwIPe
    - 增强IP层安全的一个早期原型实例
  - 1994年IETF/IPsec工作组：
    - 制定IP安全协议(IPSP)
    - 制定IP密钥管理协议(IPKMP)
    - 1995年公布IPv6,增加了鉴别头(AH)和封装安全负载(ESP)
- 结论
  - 探索与实验之中，尚未解决问题
  - 密钥算法与密钥分发问题

国际Internet安全技术活动(2)

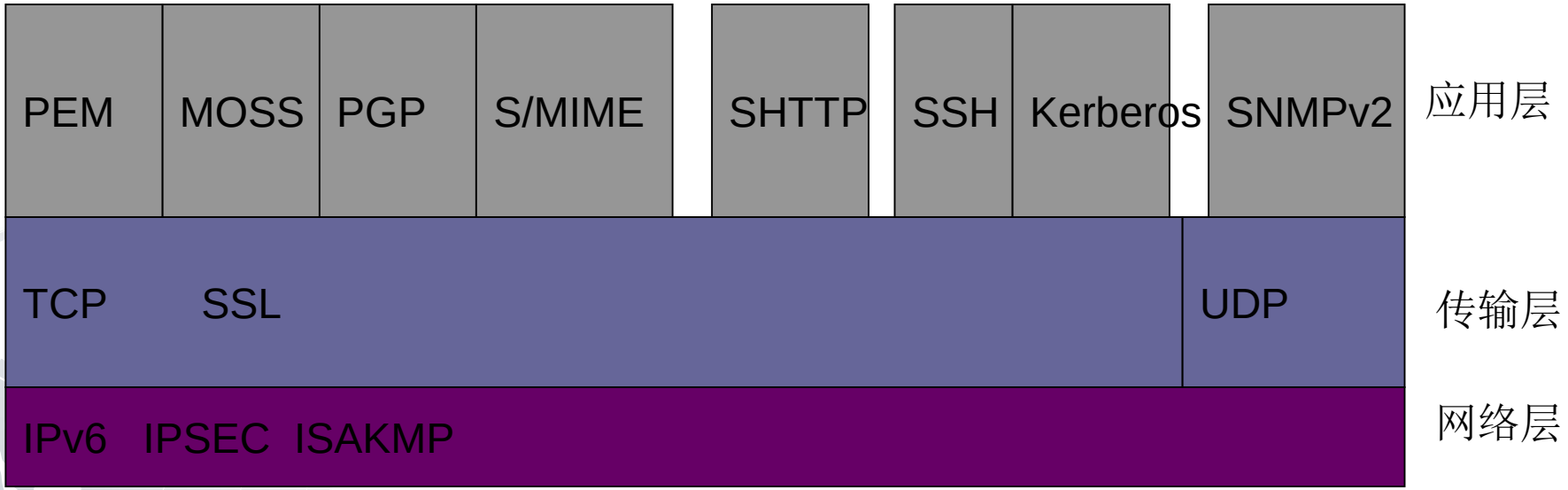
- 传输层安全协议(Sockets & TLI)
  - 安全套接层SSL(Secure Sockets Layer)
    - 1995年12月公布v3, Netscape开发
    - 1996年4月IETF/TLSG传输层安全工作组起草TLSP
    - 微软提出SSL升级版本成为PCT(private communication technology)
  - 主要问题
    - 上层应用需要改变
    - 使用X.509证书，由于X.500目录服务的领悟力极差，导致密钥分发和证书暴露许多问题。
    - 需要一个全球密钥分发机制(CA），以DNS为基础，带来法律与政治问题

国际Internet安全技术活动(3)

- 应用层安全协议
  - PEM(Private Enhanced Email)
  - MIME对象安全服务(MOSS)
  - S/MIME
  - PGP
  - S-HTTP
  - SNMPv1和SNMPv2
  - E-Commerce SET
  - 鉴别和密钥分发系统(Kerberos V5,Kryptoknight等)
  - 其它问题(PKI,安全服务的层次）

国际Internet安全技术活动(4)

- 基于TCP/IP协议的网络安全体系结构基础框架

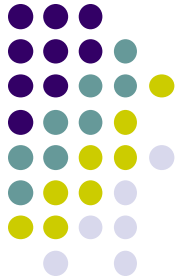


国际Internet安全技术活动(5)

- ISO7498-2映射而得的TCP/IP各层安全服务与安全协议的对应关系

层	安全协议	鉴别	访问控制	保密性	完整性	抗否认
IP层	IPSEC	Y		Y	Y	
TCP层	SSL	Y		Y	Y	
应用层	PEM	Y		Y	Y	Y
	MOSS	Y		Y	Y	Y
	S/MIM	Y		Y	Y	Y
	PGP	Y		Y	Y	Y
	SHTTP	Y		Y	Y	Y
	SNMP	Y		Y	Y	
	SSH	Y		Y	Y	
	Kerberos	Y	Y	Y	Y	Y

从信息安全到信息保障

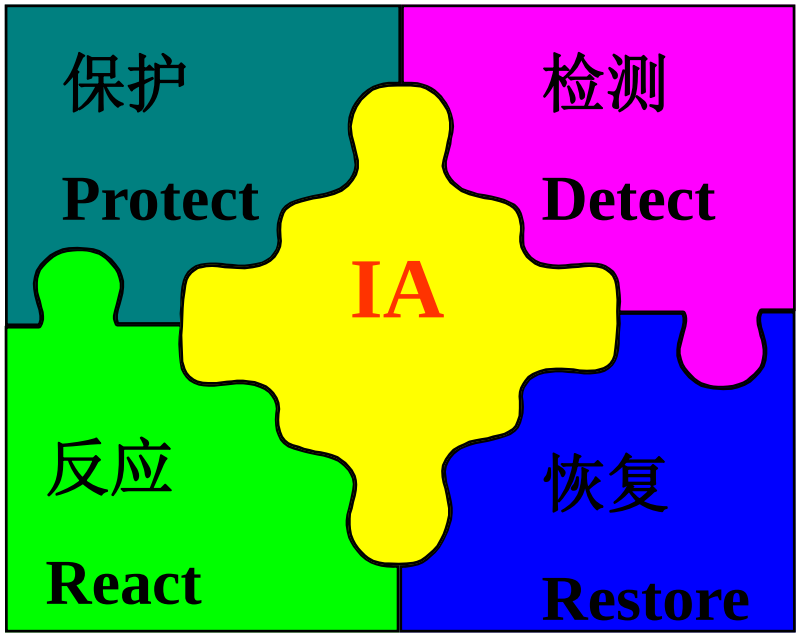


- 通信保密（COMSEC）：60年代
- 计算机安全（COMPUSEC）：60-70年代
- 信息安全（INFOSEC）：80-90年代
- 信息保障（IA）：90年代-

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）



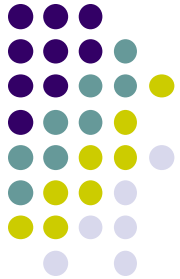
PDRR

- 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。

美国关于密码的法规

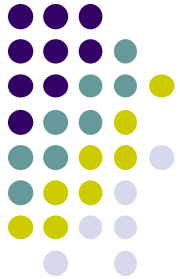


- 加密
  - 本土可以使用强密码（密钥托管、密钥恢复、TTP）
  - 视为武器而禁止出口
  - 可以出口密钥长度不超过40位的产品
  - 后来表示可以放宽到128位
- 认证
  - 出口限制相对加密宽松
  - 2000年通过了数字签名法。

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。

国内外现状及发展趋势



- 中国：
  - 制定了一系列基本管理办法
    - “中华人民共和国计算机安全保护条例”
    - “中华人民共和国商用密码管理条例”
    - “计算机信息网络国际联网管理暂行办法”
    - “计算机信息网络国际联网安全保护管理办法”
    - “计算机信息系统安全等级划分标准”等
    - 《刑法》修订中，增加了有关计算机犯罪的条款
  - 尚未形成完整的体系

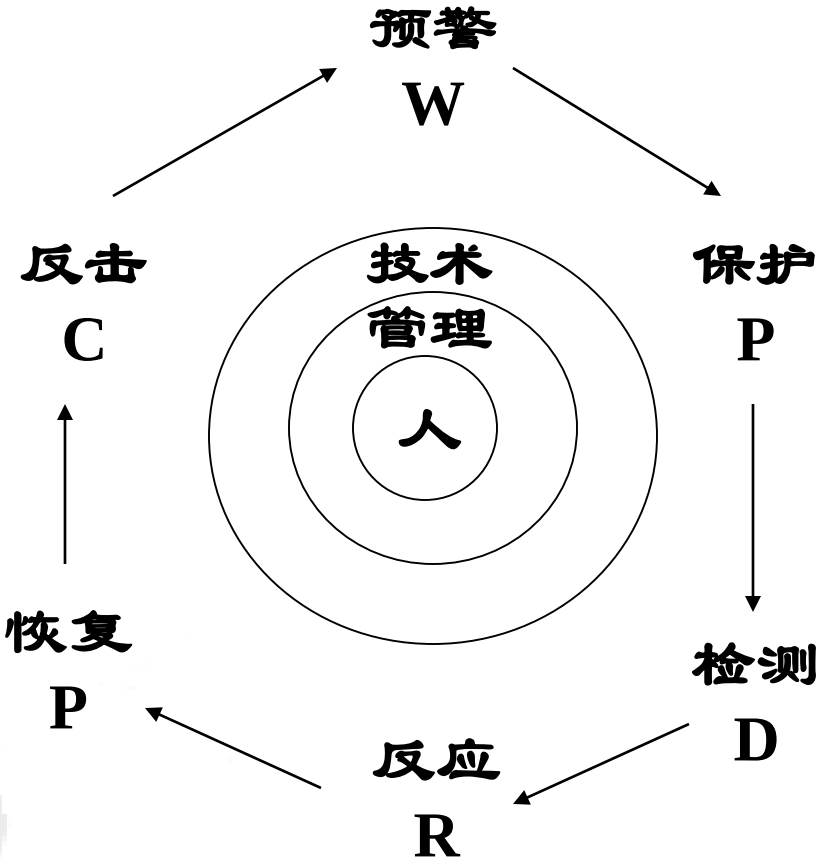
信息保障体系的组成

- 法律与政策体系
- 标准与规范体系
- 人才培养体系
- 产业支撑体系
- 技术保障体系
- 组织管理体系

信息系统安全管理准则

- 管理策略
- 组织与人员
- 资产分类与安全控制
- 配置与运行
- 网络信息安全域与通信安全
- 异常事件与审计
- 信息标记与文档
- 物理环境
- 开发与维护
- 作业连续性保障
- 符合性

信息安全管理的地位



信息安全管理的层次与内容

- 宏观管理（政府）
  - 方针
  - 政策
  - 法规
  - 标准
- 微观管理（机构）
  - 规章
  - 制度
  - 策略
  - 措施

信息安全管理的发展

- 历史发展阶段
  - 管人
  - 管密码
  - 管密钥
  - 管口令
  - 管配置
  - 管产品测评
  - 管产品采购
  - 管系统安全
  - 管等级划分

管密码

- FIPS PUB 46-1
  - Data Encryption Standard
- FIPS PUB 74
  - Guidelines for Implementing And Using the NBS Data Encryption Standard
- FIPS PUB 140 :
  - General Security Requirements for Equipment Using the Data Encryption Standard……
  - AES,CA,PKI

管密钥

- FIPS PUB 171
  - Key Management Using ANSIX9.17
- FIPS PUB 185
  - Escrowed Encryption Standard
  - ……
  - KMC
  - KMI

管口令

- FIPS PUB 48
  - Guidelines ion Evaluation of Techniques for Automated Personal Identification 4/1/77
- FIPS PUB 112
  - Standards on Password Usage 5/30/85
- CSC-STD-002-85,《DoD口令管理指南》

管产品测评

- 80年代：
  - 美国DoD TCSEC，（橘皮书。彩虹系列）
- 90年代：
  - 英、法、德、荷ITSEC（白皮书）
- 90年代末至今：
  - 六国七方：CC (Common Criteria)

管产品采购

- NCSC-TG-002
  - 《可信产品评估—厂商指南》（亮蓝
- NCSC-TG-024
  - 可信系统采购指南（紫皮书）
  - Vol.1/4：《计算机安全需求导购介绍》
  - Vol.2/4：《RFP规范和陈述语言—导购辅助》
  - Vol.3/4：《计算机安全契约数据要求列表及数据项描述指南》
  - Vol.4/4：《如何评价一个投标建议书—导购与签约者辅助》

管系统安全（一）

- 英国标准协会（BSI）于1995年制定BS7799《信息安全管理体系标准》，1999年修订改版：
  - 7799－1：《信息安全管理操作规则》
  - 7799－2：《信息安全管理系统规范》
- 7799－1已经在2000年末被采纳为国际标准，即：ISO/TEC17799《信息安全管理操作规则》

安全管理的微观粒度在加细

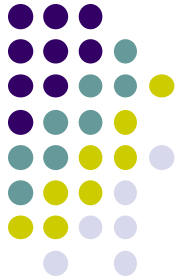
- ISO/IEC17799
  - 建立机构的安全策略
  - 机构的安全基础设施
  - 资产的分类和控制
  - 人员安全
  - 物理与环境安全
  - 通信与操作管理
  - 访问控制
  - 系统开发与维护
  - 业务连续性管理

20多个要素120多个测试点

管系统安全（二）

- ISO/IEC13335《IT安全管理方针》（GMITS）系列，可以作为替代：
  - ISO/IEC13335-1 : 1996 《IT安全的概念与模型》
  - ISO/IEC13335-2 : 1997 《IT安全管理和计划制定》
  - ISO/IEC13335-3 : 1998 《IT安全管理技术》
  - ISO/IEC13335-4 : 2000 《安全措施的选择》
  - ISO/IEC13335-5 : 《网络安全管理方针》（未公布）

管系统安全（三）



- NIST SP 800 (Special Publication 800-series)
  - SP 800-12,《计算机安全手册》（Computer Security Handbook)
  - SP 800-14,《公认【安全】原则与操作》（Generally Accepted [Security] Principles & Practices）
  - SP 800-18,《安全计划开发指南》（Guide for Developing Security Plans）
  - SP 800-23,《联邦机构安全保障和采购指南/使用可信或经评估的产品指南》（Guide to Federal Organizations on Security Assurance and Acquisition/ Use of Tested/Evaluated Products)
  - SP 800-26,《IT系统自我评估指南》(Self-Assessment Guide for IT Systems)

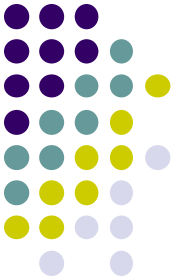
管理安全等级划分

- 计算机信息系统安全等级保护管理要求
- 第一级：用户自主保护级
  - 实施计划管理
- 第二级：系统审计保护级
  - 实施操作规程管理
- 第三级：安全标记保护级
  - 实施标准化过程管理
- 第四级：结构化保护级
  - 实施安全生态管理
- 第五级：访问验证保护级
  - 实施安全文化管理

美国制定信息系统保护计划v1.0

- 三个目标
  - 准备和防范
  - 检测和响应
  - 建立牢固的根基

十个步骤



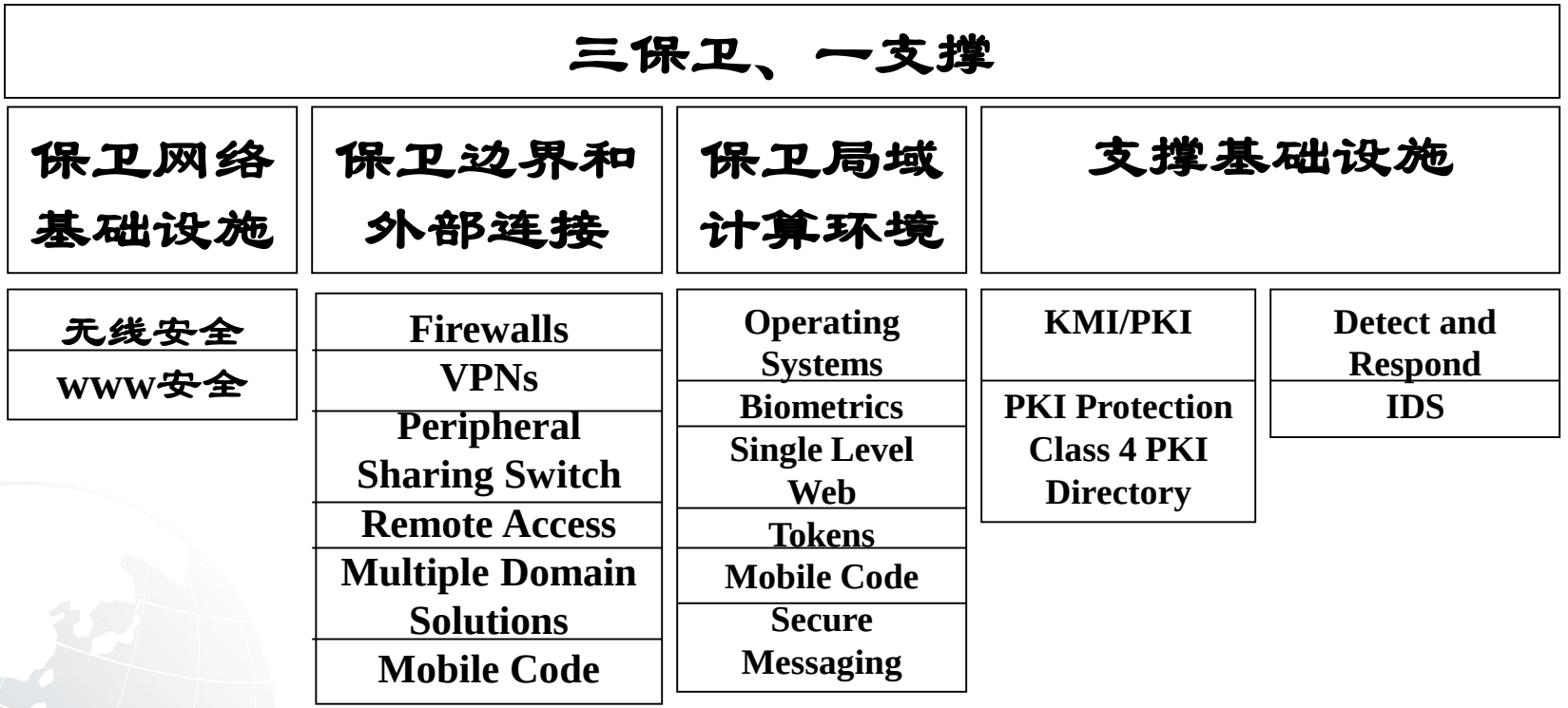
- 准备和防范
  - 步骤1：确认关键基础设施资产以及相互依赖性，发现其脆弱性
- 检测与响应
  - 步骤2：检测攻击和非法入侵
  - 步骤3：开发稳健的情报和执法功能，保持法律的一致
  - 步骤4：以实时的方式共享攻击警告和信息
  - 步骤5：建立响应、重建和回复能力

十个步骤

- 建立牢固的根基
  - 步骤6：为支持程序1—5，加强研究和开发
  - 步骤7：培训和雇用足够数量的安全专家
  - 步骤8：进行拓展，使公知晓提高计算机安全的必要性
  - 步骤9：通过立法和拨款，支持程序1—8
  - 步骤10：在计划的每一步骤和部分中，要完全保护公民的自由权、隐私权以及私有数据

IATF

- 美国国家安全局制定的信息保障技术框架（IATF）1998年开始，已发布V3.0



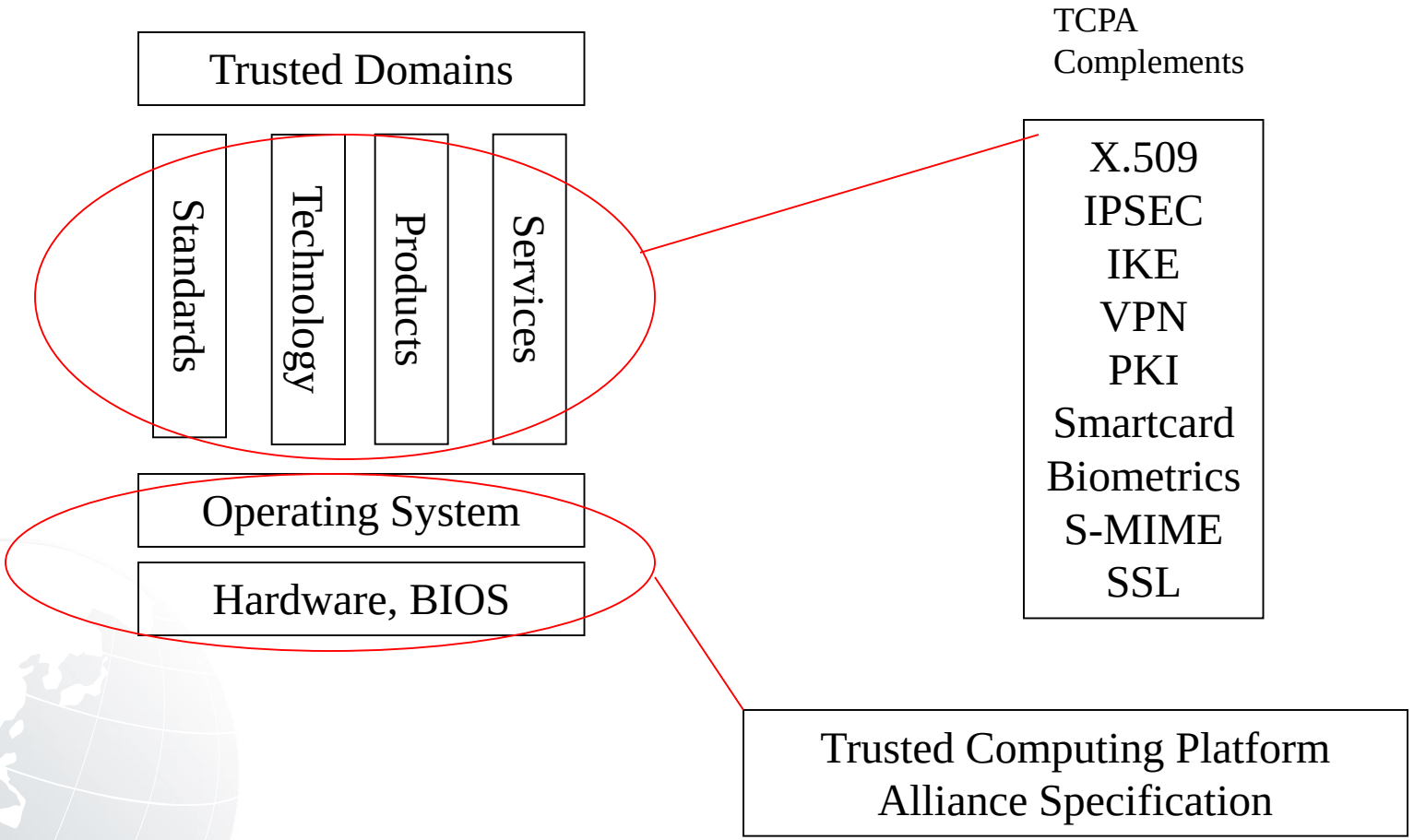
TCPA 组织

- Open membership to companies developing security technology,products and services
- Structure
  - Members
    - 135+ member companies
    - Steering Committee consisting of Compaq, HP, IBM, Intel, Microsoft
  - Ad-hoc Workgroups
    - Technical,Marketing,Legal
  - Technical Workgroups
    - BIOS,PKI,Confirmance

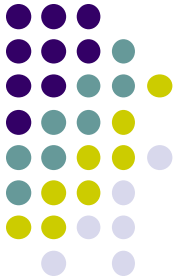
Objectives

- Develop an Industry standard specification
  - Providing a ubiquitous and standardized means to address trustworthiness of computing platforms
  - Improving the authenticity,Integrity, and privacy of Internet-based communications and commerce
- Promote the adoption of the TCPA Specification
  - Affordable and Interoperable
  - Exportable
  - Adaptable to work with existing standards and evolving solutions

TCPA Specification Scope



TCPA Specification Overview



- Baseline hardware capabilities
  - Improved traditional security features
    - Persistent storage of confidential information
    - Platform authentication
    - Random number generator
  - New security capabilities
    - Anonymous/multiple identities
    - Integrity metrics
- Exportable worldwide
  - Excludes general purpose encryption
- Owner has complete control of policy
  - Opt in – Owner decides if and when to use capability