



中山大學
SUN YAT-SEN UNIVERSITY

Module II. Internet Security

Chapter 4

Introduction to Internet Security

Information Security: Theory & Applications

School of Data & Computer Science, Sun Yat-sen University

Outline

- **4.1 Network Security Architectures**
 - Five Layers of Network Security Architectures
 - Information Security Models
 - OSI/ISO 7498-2
 - ISO Security Services
 - ISO Security Mechanisms
- **4.2 IPSec**
 - Introduction
 - Some Basic Concepts About IPSec
 - ESP protocol
 - Gateway and Road Warrior mode
 - Key management of IPSec

Outline

- **4.3 SSL/TLS**
 - Introduction
 - How TLS Works
 - Decryption of TLS Packet
- **4.4 VPN**
 - Introduction to IPsec VPN
 - OpenVPN



4.1 Network Security Architectures

4.1.1 Five Layers of Network Security Architectures

- **Physical Security**
 - Physical Security describes measures that are designed to deny access to unauthorized personnel (including attackers or even accidental intruders) from physically accessing a building, facility, resource, or stored information; and guidance on how to design structures to resist potentially hostile acts (抵抗潜在的敌意行为).
- **System Security**
- **Network Security**
- **Applications Security**
- **Management Security**

4.1 Network Security Architectures

4.1.1 Five Layers of Network Security Architectures

- 网络安全体系的分层结构
 - 网络安全防范体系可划分为物理安全、系统安全、网络安全、应用安全 and 安全管理5个层次，不同层次反映了不同的安全问题。
- 物理环境安全性 (物理安全层面)
 - 包括通信线路、物理设备、机房的安全等。
 - 物理层的安全主要体现在
 - ✧ 通信线路的可靠性 (线路备份、网管软件、传输介质)
 - ✧ 软硬件设备安全性 (替换设备、拆卸设备、增加设备)
 - ✧ 设备的备份容灾能力、抗干扰能力
 - ✧ 设备的运行环境 (温度、湿度、烟尘)
 - ✧ 不间断电源保障
 - ✧

4.1 Network Security Architectures

4.1.1 Five Layers of Network Security Architectures

- 操作系统安全性 (系统安全层面)
 - 来自网络使用的操作系统的安全，主要表现为：
 - ✧ 操作系统本身的缺陷带来的不安全因素
 - 身份认证
 - 访问控制
 - 系统漏洞
 -
 - ✧ 操作系统的安全配置
 - ✧ 病毒和木马对操作系统的威胁

4.1 Network Security Architectures

4.1.1 Five Layers of Network Security Architectures

- 网络安全性 (网络安全层面)
 - 网络方面的安全性包括
 - ✧ 网络身份认证
 - ✧ 网络资源访问控制
 - ✧ 数据传输的保密性与完整性
 - ✧ 远程安全接入
 - ✧ 域名系统的安全
 - ✧ 路由系统的安全
 - ✧ 入侵检测手段
 - ✧ 网络设施防病毒
 - ✧

4.1 Network Security Architectures

4.1.1 Five Layers of Network Security Architectures

- 应用安全性 (应用安全层面)
 - 应用层的安全问题主要由提供服务所采用的应用程序和数据的安全性产生，包括 Web 服务、电子邮件系统、DNS 等。此外，还包括病毒对系统的威胁。
- 管理安全性 (管理安全层面)
 - 安全管理包括安全技术和设备的管理、安全管理制度、部门与人员的组织规则等。管理的制度化极大程度地影响着整个网络的安全，严格的安全管理制度、明确的部门安全职责划分、合理的人员角色配置都可以在很大程度上降低其它层次的安全威胁。

4.1 Network Security Architectures

4.1.2 Information Security Models (信息安全模型)

- 信息安全模型和安全体系
 - 信息安全模型
 - ✧ 访问控制模型
 - ✧ 其他模型
 - 信息安全体系
 - ✧ 信息安全保障框架
 - ✧ OSI 7498-2
 - ✧ 信息技术安全性评估
 - ✧ 信息安全保障评估

4.1 Network Security Architectures

4.1.2 Information Security Models (信息安全模型)

- 信息安全模型的概念

- 信息安全模型用于精确和形式地描述信息系统的安全特征，以及用于解释系统安全的相关行为。适当的安全模型对关键安全需求分析有重要意义，有助于建立有效的安全性评估准则。

- ✧ 按机制分类：访问控制模型、信息流模型等。

- 访问控制模型：从访问控制的角度描述安全系统，主要针对系统中主体对客体的访问及其安全控制。

- 信息流模型：研究客体之间的信息传输过程的控制。目前尚处于理论阶段。

- ✧ 按服务分类：机密性模型、完整性模型、可用性模型等。

4.1 Network Security Architectures

4.1.2 Information Security Models (信息安全模型)

- 信息安全模型与安全操作系统的发展

- MIT 于1961年在 IBM7094 型机器上实现了首个分时系统 CTSS (Compatible Time-Sharing System, 相容分时系统)。1963年 MIT 启动 MAC 计划, 由 IBM 大型机连接分布在校园的160台终端, 允许30名用户同时使用。1965年 MIT 启动 MULTICS (多路信息与计算系统, MULTiplexed Information and Computing System) 计划, 项目研发基于 Compatible Time-Sharing System 和 IBM PL/I 语言, 建立在 GE645 主机上, 预计连接1000台终端, 支持300名用户同时使用。新系统的研发由 AT&T 贝尔实验室、MIT 和 GE 合作。1969年, 经历四年研发的 MULTICS 还是达不到计划中的性能, 贝尔实验室退出项目。次年 GE 将电脑业务出售, Honeywell 公司接手后将 MULTICS 改造成为商业化的操作系统产品大量销售。
- MULTICS 潮解: Many Unnecessarily Large Table In Core Simultaneously

4.1 Network Security Architectures

4.1.2 Information Security Models (信息安全模型)

- 信息安全模型与安全操作系统的发展
 - 1969年，贝尔实验室的 *Ken Thompson* 和 *Dennis Ritchie* 把原本为 MULTICS 设计的 Space Travel 游戏移植到一台空闲的 PDP-7 小型机上，后来又给程序中加入了文件管理、进程管理的功能和一组实用工具。1973年完成 C 语言实现改造。受到 MULTICS 的影响，*Brian Kernighan* 给系统取名为 UNiplexed Information and Computing System (UNICS，单路信息与计算系统)，取谐音便是 UNIX。
 - MULTICS 虽然未能达到预期目标，但为后来的安全操作系统的研究积累了大量经验。

4.1 Network Security Architectures

4.1.2 Information Security Models (信息安全模型)

- 信息安全模型与安全操作系统的发展
 - BLP 模型 (1973)。Mitre 公司的 *D. E. Bell* 和 *L. J. La Padula* 模拟军事安全策略创建，改进后于1976年用于 Multics 操作系统。BLP 是大部分安全操作系统的基础安全模型。
 - Biba 模型 (1977)。由 *K. J. Biba* 提出，增加了对信息完整性的支持。
 - BMA 模型 (1995)。由英国医学会 (BMA) 提出，由客体授权主体使用用客体信息，保证客体信息的完整性和可用性。
 - Adept-50 (1969)。基于 IBM/360 的第一个分时安全操作系统。
 - PSOS (Provably Secure Operating System, 1975)。层次结构化的基于权能 (capability-based) 的安全操作系统。
 - KSOS (Kernelized Secure Operating System, 1977)。美国国防部研究计划局主持的安全操作系统研究项目，通过形式化说明与验证的方法提供高可信度的安全性。

4.1 Network Security Architectures

4.1.2 Information Security Models (信息安全模型)

- 信息安全模型与安全操作系统的发展
 - UCLA Secure UNIX (1978)。美国国防部研究计划局主持，与 KSOS 类似的安全操作系统研究项目。
 - LINVS IV (1984)。基于 BSD UNIX 4.1 的安全操作系统。
 - Secure Xenix (1986)。由 IBM 研发的，基于 IBM PC/AT 机器。
 - OSF-1 (1990)。由 Open Software Foundation 支持。
 - UNIX SVR 4.1 EE (1991)。由 UI 支持。
 - SELinux (Security Enhanced Linux, 2001)。NSA 支持。

4.1 Network Security Architectures

4.1.2 Information Security Models (信息安全模型)

- 信息安全评估标准 (部分)

- TCSEC (Trusted Computer System Evaluation Criteria, 1985)。即橘皮书 (Orange Book)，将计算机系统的安全划分为4个等级、7个级别。
- ITSEC (IT Security Evaluation Criteria, 信息技术安全评定标准, 1991)。英、法、德、荷共同标准。
- BS 7799 (信息安全管理体制, British Standards Institute, BSI, 1995)。
 - ✧ 英国标准协会 (BSI) 制定的关于信息安全管理方面的标准。
 - ✧ ISO 27000 的前身。
- CC (Common Criteria for IT Security Evaluation, 1996)。ul>- ✧ 1996, CC 1.2 英、法、德、荷、美、加
- ✧ 1997, CC 2.0
- ✧ 1999, ISO/IEC 15408

4.1 Network Security Architectures

4.1.2 Information Security Models (信息安全模型)

- 信息安全评估标准 (部分)

- BS 7799 信息安全管理体系

- ✧ 英国标准协会 (British Standards Institute, BSI) 制定的关于信息安全管理方面的标准，它包含两个部分：第一部分是采纳为 ISO/IEC 17799:2000 标准的信息安全管理实施细则 (Code of Practice for Information Security Management)，它在10个标题框架下列举定义127项作为安全控制的惯例，供信息安全实践者选择使用；BS 7799 的第二部分是建立信息安全管理体系 (ISMS) 的一套规范 (Specification for Information Security Management Systems)，详细说明了建立、实施和维护信息安全管理体系的要求，指出实施机构应该遵循的风险评估标准。作为一套管理标准，BS7799-2 指导相关人员怎样去应用 ISO/IEC 17799，其最终目的还在于建立适合企业需要的 ISMS。

- ✧ ISO 27000 源于 BS 7799。

4.1 Network Security Architectures

4.1.2 Information Security Models (信息安全模型)

- 信息安全模型的分类

- 访问控制模型

- ✧ 自主访问控制模型 (DAC, Discretionary Access Control)

- 访问矩阵模型

- 访问控制列表 (ACL)

- 权能列表 (Capacity List)

- ✧ 强制访问控制模型 (MAC, Mandatory Access Control)

- 多级环境模型 (静态)

- Bell-Lapadula 模型 (1973)

- Biba 模型 (1977)

- Clark-Wilson 模型 (1987)

- 多边环境模型 (动态)

- Chinese Wall 模型

- BMA 模型 (1995)

4.1 Network Security Architectures

4.1.2 Information Security Models (信息安全模型)

- 信息安全模型的分类

- 访问控制模型

- ✧ 基于角色控制模型 (RBAC)

- ✧ 基于属性控制模型 (ABAC)

- 信息流模型

- ✧ 信息流安全模型主要着眼于对客体之间的信息传输过程的控制。信息流模型需要遵守的安全规则是：在系统状态转换时，信息流只能从访问级别低的状态流向访问级别高的状态。

- ✧ 信息流模型实现的关键在于对系统的描述，即对模型进行彻底的信息流分析，找出所有的信息流，并根据信息流安全规则判断其是否为异常流，据此反复修改系统的描述或模型，直到所有的信息流都不是异常流为止。

- ✧ 信息流模型的缺点：需要制定输入输出的安全性规范；对具体的实现只能提供少量的帮助和指导。

4.1 Network Security Architectures

4.1.2 Information Security Models (信息安全模型)

- **ISO 7498-2 (OSI 信息安全体系结构)**

- 国际标准化组织 (ISO) 于1989年对 OSI 开放系统互联环境的安全性进行了深入研究，在此基础上提出了 OSI 安全体系结构：ISO 7498-2：1989，该标准被我国等同采用，即《信息处理系统—开放系统互连—基本参考模型—第二部分：安全体系结构GB/T 9387.2-1995》。
- ISO 7498-2 安全体系结构由5类安全服务 (认证、访问控制、数据保密性，数据完整性和抗抵赖性) 及用来支持安全服务的8种安全机制 (加密、数字签名、访问控制，数据完整性，认证交换、业务流填充、路由控制和公证) 构成。

4.1 Network Security Architectures

4.1.2 Information Security Models (信息安全模型)

- **ISO 7498-2 (OSI 信息安全体系结构)**
 - ISO 7498-2 安全体系结构针对的是基于 OSI 参考模型的网络通信系统，它所定义的安全服务也只是解决网络通信安全性的技术措施，其他信息安全相关领域，包括系统安全、物理安全、人员安全等方面都未涉及。此外，ISO 7498-2体系关注的是静态的防护技术，它并没有考虑到信息安全动态性和生命周期性的发展特点，缺乏检测、响应和恢复这些重要的环节，因而无法满足更复杂更全面的信息保障的要求。

4.1 Network Security Architectures

4.1.2 Information Security Models (信息安全模型)

- 信息保障

- 随着网络攻击技术的发展，人们发现任何信息安全技术和手段都存在弱点，传统的“防火墙+补丁”这样的纯技术方案无法完全抵御来自各方的威胁，必须寻找一种可持续的保护机制，对信息和信息系统进行全方位的、动态的保护。因此，除了信息安全保护外，还应该重视提高安全预警能力、系统的入侵检测能力、系统的事件反应能力和系统遭到入侵引起破坏的快速恢复能力。区别于传统的加密、身份认证、访问控制、防火墙、安全路由等技术，需要强调信息系统整个生命周期的防御和恢复，同时安全问题的出现和解决方案也超越了纯技术范畴。
- 1989年卡内基·梅隆大学 CERT 开始研究如何从静态信息安全防护向动态防护转变。之后，美国防部在其信息安全及网络战防御理论探索中吸收了这一思想，并于1995年提出了“信息保障”概念。

4.1 Network Security Architectures

4.1.2 Information Security Models (信息安全模型)

- 信息保障

- “信息保障” (information assurance, IA) 概念提出以后，经过多次修改、完善，到世界范围的广泛认可。信息保障是一种保证信息和信息系统能够安全运行的防护性行为，保障的对象是信息以及处理、管理、存储、传输信息的信息系统；保障的目的是采取技术、管理等综合性手段，使信息和信息系统具备机密性、完整性、可用性、可认证性、不可否认性，以及在遭受攻击后的可恢复性。随着技术的不断发展和认识的不断深入，美军“信息保障”概念的内涵和外延也在实践中不断扩充和延伸，已经从最初的一套简单的纯技术防护措施，发展到由“人”、“技术”和“操作”三个范畴共同构成的一个综合体系，包括了政策管理、组织实施、运行使用、基础设施建设等方方面面的内容，成了指导美军构建信息安全体系的重要战略思想。

4.1 Network Security Architectures

4.1.2 Information Security Models (信息安全模型)

- 信息保障

- 信息保障体系

- ✧ 信息保障的目的是为保障对象 (信息和信息系统) 提供可用性、机密性、完整性、不可抵赖性、可授权性的安全服务。信息保障最终实现对保障对象提供持续安全性的保证, 不仅需要安全防护措施, 更重要的是基于信息保障体系, 即安全循环体系和完整的实施体系。
 - ✧ 信息保障体系包括风险分析、安全防护、安全检测、安全测试与评估、应急响应、恢复、实施体系。

4.1 Network Security Architectures

4.1.2 Information Security Models (信息安全模型)

- 信息保障

- 信息保障体系

- ✧ 风险分析 (Risk Analyze): 包括确定系统资源清单, 进行脆弱性评估, 分析系统风险级别等。风险分析是了解信息系统各方面状态的关键步骤。
 - ✧ 安全防护 (Protect): 采用相关安全技术、安全机制、安全产品, 实现安全防护方案。安全防护是保障信息安全性的主要静态措施。
 - ✧ 安全检测 (Detect): 使用实时监控、入侵检测、漏洞扫描等技术, 对系统进行安全检测, 形成资源数据库。
 - ✧ 测试与评估 (Test and Evaluate): 定期对系统的安全机制、安全产品、安全状态进行测试和评估, 及时发现其存在的安全脆弱性, 并进行公正的评估。测试评估与安全检测是保障信息安全性的关键动态措施。

4.1 Network Security Architectures

4.1.2 Information Security Models (信息安全模型)

- 信息保障

- 信息保障体系

- ✧ 应急响应 (React): 对突发事件进行快速反应, 尽可能减少突发事件对系统的影响, 保证系统安全的最小资源集合可用。
 - ✧ 恢复 (Restore): 当系统遭受毁坏时, 评估系统损失情况, 在最短时间内恢复系统数据和系统服务, 使系统迅速恢复基本的服务并重建。应急响应能力和恢复能力是信息系统生存性、抗毁性的重要衡量标准。
 - ✧ IA 实施体系: IA 的实施体系是 IA 有效实施的有力保障和基础, 它包括相关组织机构体系构筑、相关政策颁布、相关标准制订、资金支持、信息安全专家及相关人员的培养计划、人员信息安全意识的提高、IA 的实施与管理等。

4.1 Network Security Architectures

4.1.2 Information Security Models (信息安全模型)

- 信息保障

- 信息保障体系

- ✧ 由此可见，信息保障是针对信息安全的一个多层次的体系结构，通过信息保障的体系可以实现信息关键基础设施、信息、信息系统的持续安全提升，在一个风险、检测、评估、响应的循环体系和完备的实施体系中保证良好的安全性。

4.1 Network Security Architectures

4.1.2 Information Security Models (信息安全模型)

- 信息保障技术框架 IATF

- NSA 制定的《信息保障技术框架》(IATF, Information Assurance Technical Framework) 为保护美国政府和工业界的信息与信息技术设施提供技术指南。IATF 从整体、过程的角度看待信息安全问题，其代表理论为“深度防御战略 (Defense-in-Depth)”。IATF 强调人、技术、操作三个核心原则，关注四个信息安全保障领域：保护网络和基础设施、保护边界、保护计算环境、支撑基础设施。IATF 首次提出了信息保障依赖于人、技术和操作三个要素来共同实现组织职能/业务运作的思想，对技术/信息基础设施的管理也离不开这三个要素。IATF 认为，稳健的信息保障状态意味着信息保障的策略、过程、技术和机制在整个组织的信息基础设施的所有层面上都能得以实施。

4.1 Network Security Architectures

4.1.2 Information Security Models (信息安全模型)

- 信息保障技术框架 IATF

- IATF 的安全目标:

- ✧ 可用性: 合法用户的正常请求能及时、正确、安全地得到服务或回应。
 - ✧ 完整性: 信息在存储和传输时不被篡改、破坏, 或避免信息包的丢失、乱序等不破坏信息的正确性和完整性。
 - ✧ 保密性:
 - 防止对信息的非授权访问和窃听、解密。
 - ✧ 可靠性:
 - 指信息的可信度, 包括信息完整性、准确性和发送人的身份的可信度。

4.1 Network Security Architectures

4.1.2 Information Security Models (信息安全模型)

- 信息保障技术框架 IATF
 - IATF 的保护对象：
 - ✧ 网络和基础设施的防御
 - 骨干网可用性
 - 无线网安全框架
 - VPN和紧耦合连接
 - ✧ 边界防御
 - 网络访问控制
 - 远程访问
 - 多级别安全
 - ✧ 计算环境防御
 - 端用户环境
 - 应用系统安全
 - ✧ 支撑性基础设施
 - KMI/PKI
 - 监视和响应



4.1 Network Security Architectures

4.1.2 Information Security Models (信息安全模型)

- 信息保障技术框架 IATF

- IATF 信息保障体系三个要素：

- ◇ 人 (People):

- 人是信息体系的主体，是信息系统的拥有者、管理者和使用
者，是信息保障体系的核心，是第一位的要素，同时也是最脆弱的。正是基于这样的认识，安全管理在安全保障
体系中就愈显重要。信息安全保障体系，实质上就是一个
安全管理的体系，其中包括意识培训、组织管理、技术管
理和操作管理等多个方面。

- ◇ 技术 (Technology):

- 技术是实现信息保障的重要手段，信息保障体系所应具备
的各项安全服务通过技术机制实现。技术已经不单是以防
护为主的静态技术体系，而是防护、检测、响应、恢复并
重的动态的技术体系。

4.1 Network Security Architectures

4.1.2 Information Security Models (信息安全模型)

- 信息保障技术框架 IATF

- IATF 信息保障体系三个要素：

- ✧ 操作 (Operation):

- 或者叫运行，它构成了安全保障的主动防御体系，如果说技术的构成是被动的，那操作和流程就是将各方面技术紧密结合在一起的主动过程，其中包括风险评估、安全监控、安全审计、跟踪告警、入侵检测、响应恢复等内容。

4.1 Network Security Architectures

4.1.2 Information Security Models (信息安全模型)

- 信息保障技术框架 IATF

- IATF 的核心思想

- ✧ IATF 的核心思想是纵深防御战略 (Defense in Depth), 即采用一个层次化的、多样性的安全措施来保障用户信息及信息系统的安全。
 - ✧ 在纵深防御战略中, 人、技术和操作是三个主要核心因素, 要保障信息及信息系统的安全, 三者不可或缺; 从技术上讲纵深防御战略体现为在包括主机、网络、系统边界和支撑性基础设施等多个网络环节之中如何实现预警、保护、检测、反应和恢复 (WPDRR) 五个安全内容。
 - ✧ 纵深防御战略的含义是多方面的, 它试图全面覆盖一个层次化的、多样性的安全保障框架。纵深防御战略的核心目标就是在攻击者成功地破坏了某个保护机制的情况下, 其它保护机制依然能够提供附加的保护。

4.1 Network Security Architectures

4.1.2 Information Security Models (信息安全模型)

- 信息保障技术框架 IATF

- IATF 的其他信息保障原则

- ✧ 除了纵深防御这个核心思想之外，IATF 还提出了其他一些信息保障原则，这些原则对指导我们建立信息安全保障体系都具有非常重大的意义。

- ✧ 保护多个位置

- 包括保护网络和基础设施、区域边界、计算环境。这一原则提醒我们，仅仅在信息系统的重要敏感设置一些保护装置是不够的，任意一个系统漏洞都有可能导致严重的攻击和破坏后果，所以在信息系统的各个方位布置全面的防御机制，这样才能将风险减至最低。

4.1 Network Security Architectures

4.1.2 Information Security Models (信息安全模型)

- 信息保障技术框架 IATF
 - IATF 的其他信息保障原则
 - ◇ 分层防御

- 如果说上一个原则是横向防御，那么这一原则就是纵向防御，这也是纵深防御思想的一个具体体现。分层防御即在攻击者和目标之间部署多层防御机制，每一个这样的机制必须对攻击者形成一道屏障。而且每一个这样的机制还应包括保护和检测措施，以使攻击者不得不面对被检测到的风险，迫使攻击者由于高昂的攻击代价而放弃攻击行为。

4.1 Network Security Architectures

4.1.2 Information Security Models (信息安全模型)

- 信息保障技术框架 IATF

- IATF 的其他信息保障原则

- ◇ 安全强健性

- 不同的信息对于组织有不同的价值，该信息丢失或破坏所产生的后果对组织也有不同的影响。所以对信息系统内每一个信息安全组件设置的安全强健性（即强度和保障），取决于被保护信息的价值以及所遭受的威胁程度。在设计信息安全保障体系时，必须要考虑到信息价值和安全管理成本的平衡。

4.1 Network Security Architectures

4.1.2 Information Security Models (信息安全模型)

- 信息保障技术框架 IATF

- 网络与基础设施防御

- ✧ 网络和支撑它的基础设施是各种信息系统和业务系统的中枢，为用户数据流和用户信息获取提供传输机制，其安全是整个信息系统安全的基础。网络和基础设施防御包括维护信息服务，防止拒绝服务攻击 (DoS)；保护在整个广域网上进行交换的公共的、私人的或保密的信息，避免这些信息在无意中泄漏给未经授权访问者或发生更改、延时或发送失败；保护数据流分析等。

4.1 Network Security Architectures

4.1.2 Information Security Models (信息安全模型)

- 信息保障技术框架 IATF

- 区域边界防御

- ✧ 根据业务的重要性、管理等级和安全等级的不同，“一个信息系统通常可以划分多个区域，每个区域是在单一统辖权控制下的物理环境”，具有逻辑和物理安全措施。这些区域大多具有和其他区域或网络相连接的外部连接。区域边界防御关注的是如何对进出这些区域边界的数据流进行有效的控制与监视，对区域边界的基础设施实施保护。

4.1 Network Security Architectures

4.1.2 Information Security Models (信息安全模型)

- 信息保障技术框架 IATF

- 计算环境防御

- ✧ 在计算环境中的安全防护对象包括用户应用环境中的服务器、客户机以及其上安装的操作系统和应用系统，这些应用能够提供包括信息访问、存储、传输、录入等在内的服务。计算环境防御就是要利用识别与认证 (I&A)、访问控制等技术确保进出内部系统数据的保密性、完整性和不可否认性。这是信息系统安全保护的最后一道防线。

4.1 Network Security Architectures

4.1.2 Information Security Models (信息安全模型)

- 信息保障技术框架 IATF

- 支撑性基础设施

- ◇ 支撑基础设施是一套相关联的活动与能够提供安全服务的基础设施相结合的综合体。目前纵深防御策略定义了两种支撑基础设施：密钥管理基础设施 (KMI)/公钥基础设施 (PKI) 和检测与响应基础设施。KMI/PKI 涉及网络环境的各个环节，是密码服务的基础；本地 KMI/PKI 提供本地授权，广域网范围的 KMI/PKI 提供证书、目录以及密钥产生和发布功能。检测与响应基础设施中的组成部分提供用户预警、检测、识别可能的网络攻击、作出有效响应以及对攻击行为进行调查分析等功能。

4.1 Network Security Architectures

4.1.2 Information Security Models (信息安全模型)

- 信息保障技术框架 IATF

- IATF 小结

- ✧ IATF 的四个技术焦点区域是一个逐层递进的关系，从而形成一种纵深防御系统。因此，以上四个方面的应用充分贯彻了纵深防御的思想，对整个信息系统的各个区域、各个层次，甚至在每一个层次内部都部署了信息安全设备和安全机制，保证访问者对每一个系统组件进行访问时都受到保障机制的监视和检测，以实现系统全方位的充分防御，将系统遭受攻击的风险降至最低，确保档案信息的安全和可靠。
 - ✧ IATF 认为，信息安全并不是纯粹的技术问题，而是一项复杂的系统工程，表现为具体实施的一系列过程，这就是信息系统安全工程 (ISSE)。通过完整实施的 ISSE 过程，组织应该能够建立起有效的信息安全体系。

4.1 Network Security Architectures

4.1.2 Information Security Models (信息安全模型)

- 信息保障技术框架 IATF

- IATF 小结

- ✧ IATF 提出了三个主要核心要素：人、技术和操作。尽管 IATF 重点是讨论技术因素，但是它也提出了“人”这一要素的重要性。人即管理，安全管理在信息安全保障体系建设中同样起到了十分关键的作用。
 - ✧ 尽管 IATF 强调了人的核心因素，但整个体系的阐述还是侧重于技术，很少涉及安全管理的内容。所以，与其说 IATF 为我们提供了全面的信息安全体系模型，不如说为我们指出了设计、构建和实施信息安全解决方案的一个技术框架信息安全体系建设与服务过程 (ISMG002)，它为我们概括了信息安全应该关注的领域和范围、途径和方法，以及可选的技术性措施，但并没有指出信息安全最终的表现形态，这和P2DR、PDRR等模型有很大区别。

4.1 Network Security Architectures

4.1.2 Information Security Models (信息安全模型)

- PDR, P2DR 和 PDRR 安全模型

- PDR 安全模型

- ✧ PDR 模型是由美国互联网安全系统公司 (ISS, 1999?) 提出的入侵检测模型。PDR 命名取自 Protection, Detection 和 Response 的首字母。
 - ✧ 保护
 - 安全规则的制定；系统安全的配置；安全措施采用。
 - ✧ 检测
 - 异常监视；模式发现。
 - ✧ 响应
 - 在发现了攻击企图或者攻击之后，需要系统及时地进行反应。响应包括报告、记录、反应、恢复。

4.1 Network Security Architectures

4.1.2 Information Security Models (信息安全模型)

- PDR, P2DR 和 PDRR 安全模型

- PDR 安全模型

- ✧ PDR 模型建立了一个所谓的基于时间的可证明的安全模型，定义了：

- 防护时间 P_t ：黑客发起攻击时，保护系统不被攻破的时间

- 检测时间 D_t ：从黑客发起攻击到系统检测到攻击的时间

- 响应时间 R_t ：从系统发现攻击到系统作出有效响应的时间

- ✧ 当 $P_t > D_t + R_t$ 时，也即在黑客攻破系统之前安全体系发现并阻止了黑客的行为，那么系统就是安全的。

- ✧ 这是一个理想模型，系统的 P_t 、 D_t 、 R_t 难以准确定义，面对不同黑客和不同种类的攻击，这些时间都是变化的。

4.1 Network Security Architectures

4.1.2 Information Security Models (信息安全模型)

- PDR, P2DR 和 PDRR 安全模型

- P2DR 安全模型

- ✧ P2DR 模型源自 ISS 提出的自适应网络安全模型 ANSM (Adaptive Network Security Model)。P2DR 命名取自 Policy, Protection, Detection 和 Response 的首字母。
 - ✧ P2DR 认为一个良好的完整的动态安全体系，不仅需要恰当的防护 (比如操作系统访问控制，防火墙、加密等)，而且需要动态的检测机制 (比如入侵检测、漏洞扫描等)，在发现问题时还需要及时做出响应，这样的体系需要在统一的安全策略指导下进行实施，由此形成一个完备的、闭环的动态自适应安全体系。P2DR 模型建立在基于时间的安全理论基础之上。该理论的基本思想是信息安全相关的所有活动，无论是攻击行为、防护行为、检测行为还是响应行为，都要消耗时间，因而可以用时间尺度来衡量一个体系的能力和安全性。

4.1 Network Security Architectures

4.1.2 Information Security Models (信息安全模型)

- PDR, P2DR 和 PDRR 安全模型

- P2DR 安全模型

- ◇ 策略

- 策略是模型的核心，所有防护、检测和响应都是依据安全策略实施的。网络安全策略一般包括总体安全策略和具体安全策略两个部分组成。

- ◇ 防护

- 防护是根据系统可能出现的安全问题而采取的预防措施，这些措施通过传统的静态安全技术实现。采用的防护技术通常包括数据加密、身份认证、访问控制、授权、VPN、防火墙、安全扫描和数据备份等。

- ◇ 检测

- 当攻击者穿透防护系统时，检测功能发挥作用，与防护系统形成互补。检测是动态响应的依据。

4.1 Network Security Architectures

4.1.2 Information Security Models (信息安全模型)

- PDR, P2DR 和 PDRR 安全模型

- P2DR 安全模型

- ◇ 响应

- 系统一旦检测到入侵，响应系统就开始工作，进行事件处理。响应包括紧急响应和恢复处理，恢复处理又包括系统恢复和信息恢复。P2DR 模型是在整体的安全策略的控制和指导下，在综合运用防护工具 (如防火墙、操作系统身份认证、加密等) 的同时，利用检测工具 (如漏洞评估、入侵检测等) 了解和评估系统的安全状态，通过适当的反应将系统调整到 “最安全” 和 “风险最低” 的状态。

- ◇ 防护、检测和响应组成了一个完整的、动态的安全循环，在安全策略的指导下保证信息系统的安全。

4.1 Network Security Architectures

4.1.2 Information Security Models (信息安全模型)

- PDR, P2DR 和 PDRR 安全模型

- P2DR 安全模型

- ✧ P2DR 模型的安全规则:

- 公式 1: $P_t > D_t + R_t$.

- 公式 2: $E_t = D_t + R_t$, if $P_t = 0$.

- ✧ 公式1表示防护时间大于检测时间加上响应时间，也就是在入侵者危害安全目标之前就能被检测到并及时处理。

- ✧ 公式2的前提是假设防护时间为 0。Dt 与 Rt 的和就是该安全目标系统的暴露时间 Et。针对于需要保护的安全目标，Et 越小系统就越安全。

4.1 Network Security Architectures

4.1.2 Information Security Models (信息安全模型)

- PDR, P2DR 和 PDRR 安全模型

- P2DR 安全模型

- ✧ P2DR 给信息系统安全一个全新的定义：“及时的检测和响应就是安全”，“及时的检测和恢复就是安全”。这样的定义为安全问题的解决给出了明确的方向：提高系统的防护时间 P_t ，降低检测时间 D_t 和响应时间 R_t 。
 - ✧ 但是与策略相关的内在的变化因素难以界定，如人员的流动、人员的素质和策略贯彻的稳定性等。

4.1 Network Security Architectures

4.1.2 Information Security Models (信息安全模型)

- PDR, P2DR 和 PDRR 安全模型

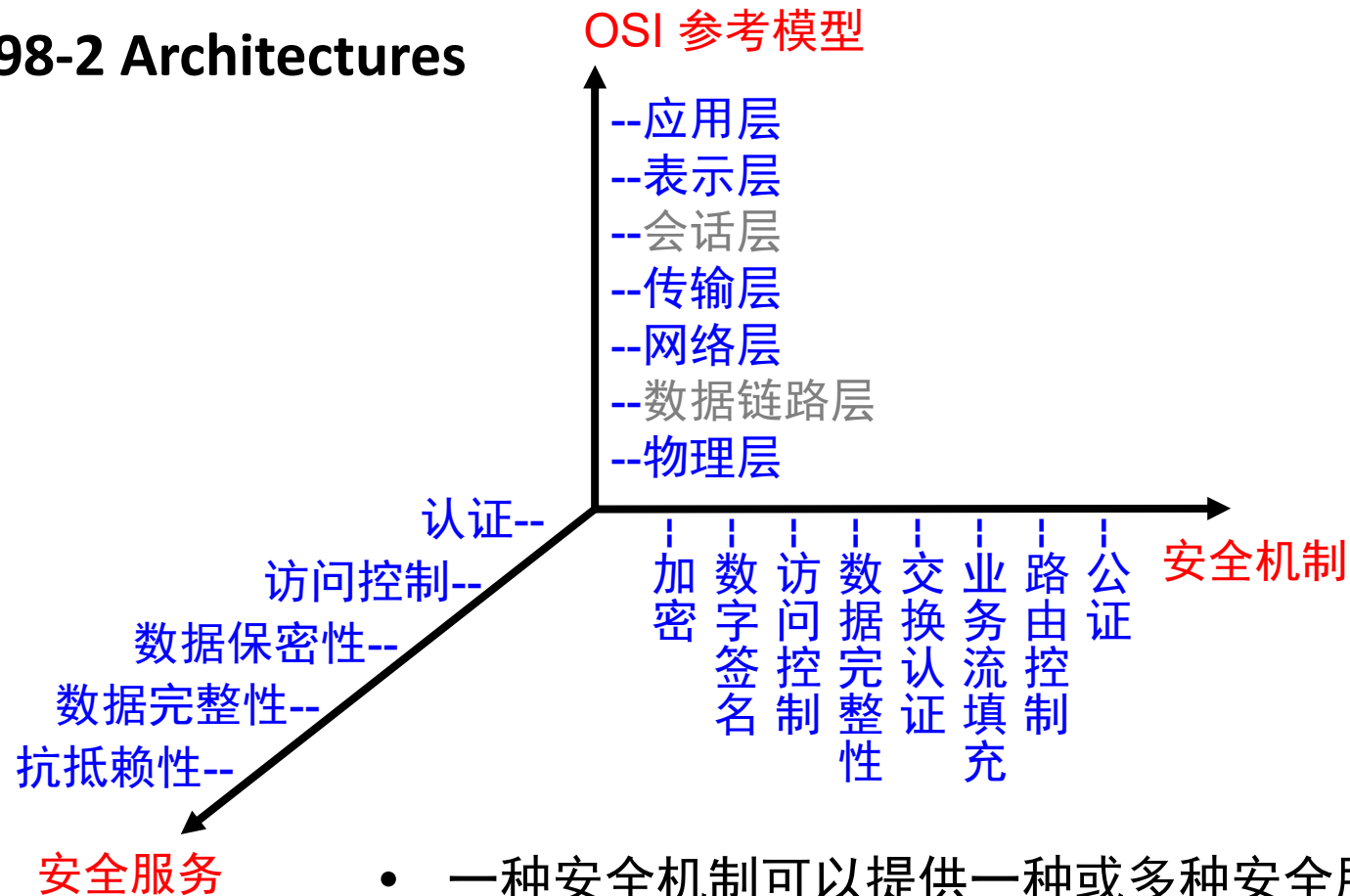
- PDRR 安全模型

- ✧ PDRR 模型，或者叫 PPDRR (或者P2DR2)，与 P2DR 非常相似，区别在于把恢复环节 (Restore) 提到了和防护，检测、响应等环节同等的高度。在 PDRR 模型中，安全策略、防护、检测、响应和恢复共同构成了完整的安全体系。

4.1 Network Security Architectures

4.1.3 OSI/ISO 7498-2

- ISO 7498-2 Architectures



- 一种安全机制可以提供一种或多种安全服务。在7层参考模型中，第2和5层不适宜配置安全服务。

4.1 Network Security Architectures

4.1.3 OSI/ISO 7498-2

- **What ISO 7498-2 Serves**

- ISO 于1989年对 OSI 的安全性进行了深入研究，提出了 OSI 安全体系结构：ISO 7498-2：1989。该标准被我国等同采用，即《信息处理系统—开放系统互连—基本参考模型—第二部分：安全体系结构 GB/T 9387.2-1995》。
- ISO 7498-2 安全体系结构由5类安全服务 (认证、访问控制、数据保密性、数据完整性和抗抵赖性) 及用来支持安全服务的8种安全机制 (加密机制、数字签名、访问控制机制、数据完整性机制、认证交换、业务流填充、路由控制和公证) 构成。ISO 7498-2 安全体系结构针对的是基于 OSI 参考模型的网络通信系统，它所定义的安全服务也只是解决网络通信安全性的技术措施，对于其他信息安全相关领域，包括系统安全、物理安全、人员安全等方面都未涉及。

4.1 Network Security Architectures

4.1.3 OSI/ISO 7498-2

- **What ISO 7498-2 Serves**

- ISO 7498-2 体系关注的是静态的防护技术，它并没有考虑到信息安全动态性和生命周期性的发展特点，缺乏检测、响应和恢复这些重要的环节，因而无法满足更复杂更全面的信息保障的要求。

4.1 Network Security Architectures

4.1.3 OSI/ISO 7498-2

- **What ISO 7498-2 Serves**

- ISO 7498-2 is intended to serve as a security-specific addition to **ISO 7498**, the **OSI reference model**.
 - ✧ It defines many security-related terms and ideas which are of importance to a variety of application areas, including many not covered by the OSI model. Of particular importance is the terminology it introduces for the description of security services and mechanisms.
 - provides standard definitions of security terminology
 - provides standard descriptions for security services and mechanisms
 - defines where in OSI reference model security services may be provided
 - introduces security management concepts

4.1 Network Security Architectures

4.1.3 OSI/ISO 7498-2

- **Security Life-Cycle**

- The underlying model, implicit to the discussion in ISO 7498-2, is that there is a generic **security life-cycle**, containing the following steps:
 - ✧ definition of a **security policy**, containing a rather abstract series of security requirements for the system,
 - ✧ a security **requirements analysis**, including a risk analysis, possibly using a tool such as **CRAMM** (CCTA Risk Analysis and Management Method), and an analysis of governmental, legal and standards requirements,
 - ✧ definition of the **security services** necessary to meet the identified security requirements,
 - ✧ system **design and implementation**, including selection of security mechanisms to provide the chosen security services
 - ✧ On-going security **management**. (持续的安全管理)

4.1 Network Security Architectures

4.1.3 OSI/ISO 7498-2

- **Threats, Services and Mechanisms**

- A security *threat* is a possible means by which a security policy may be breached (一个安全威胁是一种可能的手段，它可以破坏某种安全策略)
 - ✧ e.g. loss of integrity or confidentiality
- A security *service* is a measure which can be put in place to address a threat (一个安全服务是一种措施，它被设置用于处理某种安全威胁)
 - ✧ e.g. provision of confidentiality (提供数据保密性)
- A security *mechanism* is a means to provide a security service (安全机制是实现某种安全服务的技术手段)
 - ✧ e.g. encryption, digital signature

4.1 Network Security Architectures

4.1.3 OSI/ISO 7498-2

- **Threats, Services and Mechanisms**

- Note

- ✧ A security service is provided for a system, and a security mechanism is the means by which a security service is provided.
 - ✧ Hence ***confidentiality*** is a service, whereas ***encryption*** is a mechanism which can be used to provide confidentiality.
 - In fact encryption can be used to provide other services, and data confidentiality can also be provided by means other than encryption (e.g. by physical protection of data).

4.1 Network Security Architectures

4.1.3 OSI/ISO 7498-2

- **Security Domains and Security Policies**
 - When designing a secure system, the **scope** of the system and the **set of rules** governing the security behavior of the system are of fundamental importance; these are the **security domain** and the **security policy** respectively.
 - A security policy is defined in ISO 7498-2 as “the set of criteria for the provision of security services” (提供安全服务的一些准则的集合). A security domain can be regarded as the scope of a single security policy.
 - It is possible to have nested or overlapping security domains, and thus nested or overlapping scopes for security policies.

4.1 Network Security Architectures

4.1.3 OSI/ISO 7498-2

- **Security Domains and Security Policies**
 - ISO 7498-2 gives the following statement as an example of a possible generic security policy statement regarding **authorization**:
 - ✧ Information may not be given to, accessed by, or permitted to be inferred by, nor may any resource be used by, those not appropriately authorized.
 - ✧ An initial generic policy of this type can then be refined, in conjunction with the results of a requirements analysis, into a detailed set of rules governing the operation and management of the system.
 - ✧ This generic policy only deals with preventing unauthorized access, i.e. it does not make any statement about guaranteeing access to legitimate users. Thus it does not deal with *Availability*, and hence does not address denial of service threats.

4.1 Network Security Architectures

4.1.3 OSI/ISO 7498-2

- **Types of Security Policies**

- ISO 7498-2 distinguishes between two types of security policy.
 - ✧ *Identity-based policies* authorize system access on the basis of the identity of the client and the identity of the resource which the client wishes to make use of.
 - ✧ *Rule-based policies* rely on global rules imposed on all users, with access decisions typically made using a comparison of the sensitivity of the resources with the user attributes (e.g. the 'clearance' of the user).

4.1 Network Security Architectures

4.1.3 OSI/ISO 7498-2

- **Security Threat**

- A *threat* is a person, thing, event, or idea which poses some danger to an asset, in terms of that asset's *Confidentiality, Integrity, Availability* or *Legitimate use* (CIA+).
- An *attack* is an actual realization of a threat.
- *Safeguards* are measures to protect assets against threats, including: physical controls, mechanisms, policies and procedures.
- *Vulnerabilities* are weaknesses in a safeguard, or the absence of a safeguard.

4.1 Network Security Architectures

4.1.3 OSI/ISO 7498-2

- **Risk**
 - *Risk* is a measure of the cost of vulnerability, which takes into account the probability of a successful attack. The risk is *high* if the value of a vulnerable asset is high and the probability of a successful attack is also high. The risk is *low* if the value of a vulnerable asset is low and the probability of a successful attack is also low.
 - *Risk analysis* can provide a quantitative means of determining whether expenditure on safeguards is warranted.

4.1 Network Security Architectures

4.1.3 OSI/ISO 7498-2

- **Classification of Threats**

- *Deliberate* (蓄意的)
 - ✧ e.g. hacker penetration
- *Accidental* (偶发的)
 - ✧ e.g. a secret message being sent to the wrong address
- Deliberate threats can be further sub-divided into *passive* or *active*.
 - ✧ *Passive threats* involve monitoring but not alteration of information, e.g. wire-tapping.
 - ✧ *Active threats* involve deliberate alteration of information, e.g. changing the value of a financial transaction.
 - ✧ In general passive threats are easier to mount than active ones.

4.1 Network Security Architectures

4.1.3 OSI/ISO 7498-2

- **Fundamental Threats**

- There is no universally agreed way to identify or classify security threats. Or we can identify four *fundamental threats*, which directly relate to the four 'standard' security goals of 'CIA' together with the goal of Legitimate use (i.e. ensuring that resources are not used by unauthorized persons or in unauthorized ways).
 - ✧ *Information leakage*. Information is disclosed or revealed to unauthorized parties. (信息泄露)
 - ✧ *Integrity violation*. Data consistency is compromised. (破坏完整性)
 - ✧ *Denial of service*. Legitimate access to resources (e.g. information or processing power) is deliberately impeded. (拒绝服务)
 - ✧ *Illegitimate use*. A resource is used by an unauthorized person or in an unauthorized way. (非法使用)

4.1 Network Security Architectures

4.1.3 OSI/ISO 7498-2

- **Primary Enabling Threats**

- The following five *primary enabling threats* are significant because a realization of any of these threats can lead directly to a realization of one of the four fundamental threats. They can be sub-divided into three *penetration* and two *planting* threats

- ✧ The Three Penetration Threats (渗透威胁)

- *Masquerade*, where an entity pretends to be a different entity (假冒)
- *Bypassing controls*, where an attacker exploits system flaws or security weaknesses, in order to acquire unauthorized rights (回避控制)
- *Authorized violation*, where an entity authorized to use a system for one purpose uses it for another, unauthorized purpose (违反授权)

4.1 Network Security Architectures

4.1.3 OSI/ISO 7498-2

- **Primary Enabling Threats**

- ✧ The Two Planting Threats (植入威胁)

- *Trojan horse*, where software contains an invisible part which, when executed, compromises the security of the system (特洛伊木马)
 - *Trapdoor*, which is a feature built into a system such that the provision of specific input data allows the security policy to be violated (陷门)

4.1 Network Security Architectures

4.1.4 ISO Security Services

- **Categories of Safeguard**

- There are several categories of safeguard. What we are discussing are with communications security safeguards. Other categories include the following:

- ✧ *Computer security safeguards*

- e.g. operating system and database system security facilities.

- ✧ *Physical security*

- e.g. locks or other physical controls, equipment tamper-proofing.

- ✧ *Personnel security*

- e.g. employee screening (审查) for sensitive posts, security training and awareness.

- ✧ *Administrative security*

- e.g. controlling the importation of software, procedures for investigating security breaches, audit trail analysis.

4.1 Network Security Architectures

4.1.4 ISO Security Services

- **Categories of Safeguard**

- ✧ *Media security*

- e.g. protecting stored data, secure destruction of computer storage media, media scanning for viruses.

- ✧ *Emanations security* (电磁泄露安全)

- e.g. radio frequency emanation controls (TEMPEST protection.
 - TEMPEST, Transient Electromagnetic Pulse Emanation Surveillance Technology, 电磁脉冲瞬态特性监视技术

- ✧ *Life cycle controls*

- e.g. trusted system design, implementation, evaluation and certification, programming standards and controls, documentation controls.

4.1 Network Security Architectures

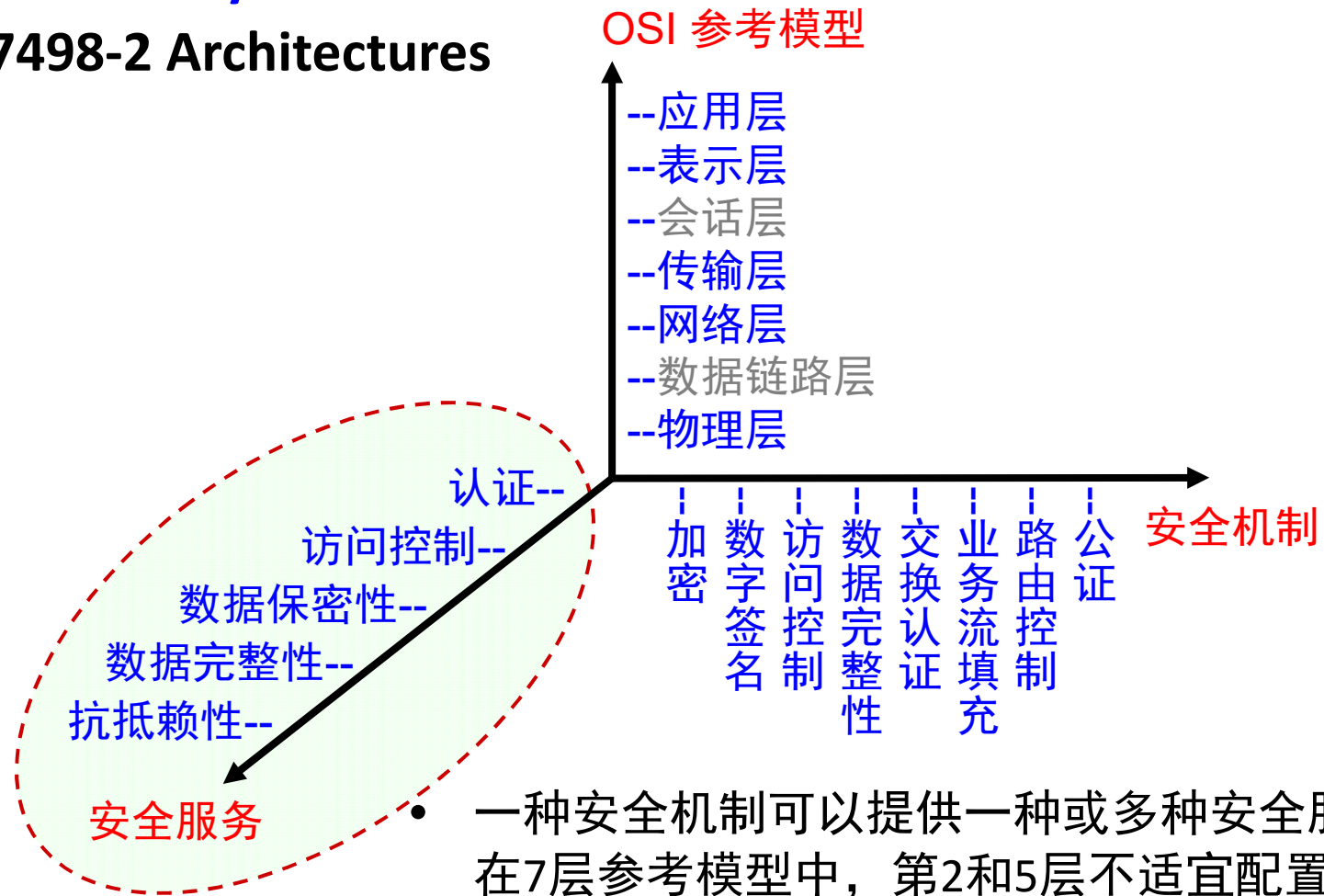
4.1.4 ISO Security Services

- **Categories of Security Service**
 - Five main categories of security service
 - ✧ *Authentication*
 - including entity authentication and origin authentication
 - ✧ *Access control*
 - ✧ *Data confidentiality*
 - ✧ *Data integrity*
 - ✧ *Non-repudiation*
 - ISO/IEC 10181
 - ✧ ISO/IEC 10181 gives specific *Security framework* standards corresponding to each of these five categories of service, a much more detailed discussion of the general ways in which these services can be provided.
 - ✧ One additional topic covered in the frameworks is *security audit*.

4.1 Network Security Architectures

4.1.4 ISO Security Services

- ISO 7498-2 Architectures



- 一种安全机制可以提供一种或多种安全服务。在7层参考模型中，第2和5层不适宜配置安全服务。

4.1 Network Security Architectures

4.1.4 ISO Security Services

- **Authentication**

- Two types of *Authentication* services

- ✧ *Entity authentication* provides corroboration (证据) to one entity that another entity is as claimed.
 - This service may be used at the establishment of (or during) a connection, to confirm the identities of one or more of the connected entities.
 - This service provides confidence, *at the time of usage only*, that an entity is not attempting a masquerade or an unauthorized replay of a previous connection.
 - ✧ *Origin authentication* provides corroboration to an entity that the source of received data is as claimed.
 - However, the service does *not*, in itself, provide protection against duplication or modification of data units.

4.1 Network Security Architectures

4.1.4 ISO Security Services

- **Access Control**

- *Access Control* service provides protection against unauthorized use of resources, including:
 - ✧ use of a communications resource,
 - ✧ reading, writing or deletion of an information resource,
 - ✧ execution of a processing resource.

4.1 Network Security Architectures

4.1.4 ISO Security Services

- **Data Confidentiality**

- Four types of *Data Confidentiality* services provide for the protection of data against unauthorized disclosure.
 - ✧ *Connection confidentiality* for the confidentiality of all user data transferred using a connection.
 - ✧ *Connectionless confidentiality* for the confidentiality of all user data transferred in a single connectionless data unit (i.e. a packet).
 - ✧ *Selective field confidentiality* for the confidentiality of selected fields within user data transferred in either a connection or a single connectionless data unit.
 - ✧ *Traffic flow confidentiality* for the confidentiality of information which might be derived from observation of traffic flows.

4.1 Network Security Architectures

4.1.4 ISO Security Services

- **Data Confidentiality**

- Note:

- ✧ *Connection communication*

- Connection-oriented communication is a network communication mode in telecommunications and computer networking, where a communication session or a semi-permanent connection is established before any useful data can be transferred, and where a stream of data is delivered in the same order as it was sent.
 - DL Layer: HDLC, PPP;
 - Network Layer: X.25;
 - Trans. Layer: TCP.

4.1 Network Security Architectures

4.1.4 ISO Security Services

- **Data Confidentiality**

- Note:

- ✧ *Connectionless communication*

- CL-mode communication is a data transmission method used in packet switching by which each data unit is individually addressed and routed based on information carried in each unit, rather than in the setup information of a prearranged, fixed data channel as in connection-oriented communication.
 - DL Layer: 802.3 CSMA/CD;
 - Network Layer: IP;
 - Trans. Layer: UDP.

4.1 Network Security Architectures

4.1.4 ISO Security Services

- **Data Integrity**

- Five types of *Data Integrity* services that counter active threats to the validity of transferred data.
 - ✧ *Connection integrity with recovery* for the integrity of all user data on a connection, and detects any modification, insertion, deletion or replay of data within an entire data unit sequence (with recovery attempted).
 - ✧ *Connection integrity without recovery* as previously but with no recovery attempted.
 - ✧ *Selective field connection integrity* for the integrity of selected fields within the user data of a data unit transferred over a connection.

4.1 Network Security Architectures

4.1.4 ISO Security Services

- **Data Integrity**

- Five types of *Data Integrity* services

- ✧ *Connectionless integrity* providing integrity assurance to the recipient of a data unit. More specifically, it enables the recipient of a connectionless data unit to determine whether that data unit has been modified. Additionally, a limited form of replay detection may be provided.
 - ✧ *Selective field connectionless integrity* for the integrity of selective fields within a single connectionless data unit.

4.1 Network Security Architectures

4.1.4 ISO Security Services

- **Non-repudiation**

- Two types of *Non-repudiation* services

- ✧ *Non-repudiation with proof of origin*. The recipient of data is provided with proof of the origin of data. This will protect against any subsequent attempt by the sender to falsely deny sending the data.
 - ✧ *Non-repudiation with proof of delivery*. The sender of data is provided with proof of delivery of data. This will protect against any subsequent attempt by the recipient to falsely deny receiving the data.

4.1 Network Security Architectures

4.1.4 ISO Security Services

- **Services vs. Layers**

- ISO 7498-2 lays down which security services may be provided in what parts of the OSI model.
 - ✧ Layers 1 and 2 are restricted to providing certain types of confidentiality services.
 - ✧ Layers 3 and 4 can provide authentication, access control, confidentiality (Layer 3 only) and integrity services.
 - ✧ No security services can be provided in Layer 5 or Layer 6, although Layer 6 may contain facilities to support the provision of services at Layer 7.
 - ✧ All security services may be provided at Layer 7.

4.1 Network Security Architectures

4.1.4 ISO Security Services

- **Services vs. Layers**

- Note:

- ✧ There are good reasons for varying the position of security functionality within the OSI layer hierarchy depending on the type of network in use. For the maximum degree of traffic flow confidentiality, data encryption needs to be placed at the lowest possible layer (to hide the protocol addresses). Low level placement also offers common security support for all the different applications running across the network. If end-to-end security is required, then the security services must be placed in Layer 3 or above. If application-specific security services are required, then the security must be placed in Layer 7.

4.1 Network Security Architectures

Service / Layer	Layer 1	Layer 2	Layer 3	Layer 4	Layer 5/6	Layer 7
Entity authentication			Y	Y		Y
Origin authentication			Y	Y		Y
Access control			Y	Y		Y
Connection confidentiality	Y	Y	Y	Y		Y
Connectionless confidentiality		Y	Y	Y		Y
Selective field confidentiality						Y
Traffic flow confidentiality	Y		Y			Y
Connection integrity with recovery				Y		Y
Connection integrity without recovery			Y	Y		Y
Selective field connection integrity						Y
Connectionless integrity			Y	Y		Y
Selective field connectionless integrity						Y
Non-repudiation of origin						Y
Non-repudiation of delivery						Y

4.1 Network Security Architectures

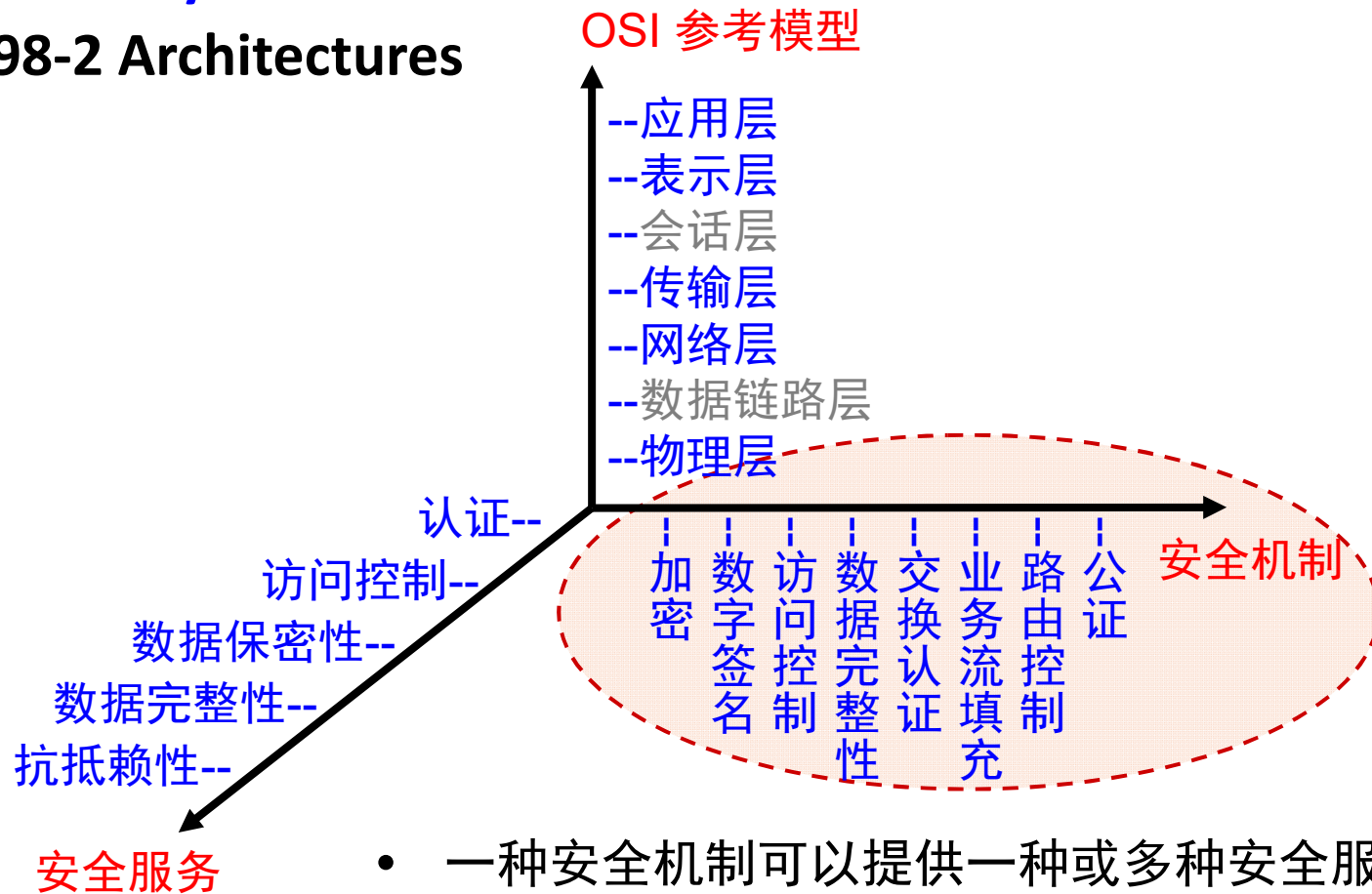
4.1.5 ISO Security Mechanisms

- **Specific & Pervasive Security Mechanism** (特定/普适的安全机制)
 - Eight types of specific security mechanisms:
 - ✧ *Encryption mechanisms*
 - ✧ *Digital signature mechanisms*
 - ✧ *Access control mechanisms*
 - ✧ *Data integrity mechanisms*
 - ✧ *Authentication exchange mechanisms*
 - ✧ *Traffic padding mechanisms*
 - ✧ *Routing control mechanisms*
 - ✧ *Notarization mechanisms* (公证)
 - ISO/IEC SC27
 - ✧ Specific standards have been developed within ISO/IEC SC27 to provide examples of most of these different classes of mechanism.

4.1 Network Security Architectures

4.1.5 ISO Security Mechanisms

- ISO 7498-2 Architectures



- 一种安全机制可以提供一种或多种安全服务。在7层参考模型中，第2和5层不适宜配置安全服务。

4.1 Network Security Architectures

4.1.5 ISO Security Mechanisms

- **Specific Security Mechanism**

- *Encryption*

- ✧ Commonly known as encryption or cipher algorithms
 - ✧ Can provide data and traffic flow confidentiality
 - ✧ Also provide the basis for some authentication and key management techniques.

- *Digital Signature*

- ✧ Including signing procedure (private),
 - ✧ And verification procedure (public).
 - ✧ Can provide non-repudiation, origin authentication and data integrity services.
 - ✧ They can be basis of some authentication exchange mechanisms.

4.1 Network Security Architectures

4.1.5 ISO Security Mechanisms

- **Specific Security Mechanism**

- *Access Control*
 - ✧ A server using client information to decide whether to grant access to resources
 - e.g. access control lists, capabilities, security labels.
- *Data Integrity*
 - ✧ Protection against modification of data.
 - Provide data integrity and origin authentication services. Also basis of some authentication exchange mechanisms.
- *Authentication Exchange*
 - ✧ Provide entity authentication service.
 - ✧ They can be thought of as a means for using information associated with a client entity and a server entity to decide whether access to the server's resource is granted to the client.

4.1 Network Security Architectures

4.1.5 ISO Security Mechanisms

- **Specific Security Mechanism**

- *Traffic Padding* (流量填充机制)
 - ✧ The addition of 'pretend' data to conceal real volumes of data traffic.
 - ✧ Provides traffic flow confidentiality.
- *Routing Control*
 - ✧ Used to prevent sensitive data using insecure channels.
 - e.g. route might be chosen to use only physically secure network components.
- *Notarization* (公证机制)
 - ✧ Integrity, origin and/or destination of data can be guaranteed by using a 3rd party trusted notary.
 - ✧ Notary typically applies a cryptographic transformation to the data.

4.1 Network Security Architectures

4.1.5 ISO Security Mechanisms

- **Pervasive Security Mechanism** (普适的安全机制)
 - Five types of *Pervasive Security* mechanism are listed in ISO 7498-2:
 - ✧ *Trusted functionality*
 - ✧ *Security labels*
 - ✧ *Event detection*
 - ✧ *Security audit trail*
 - ✧ *Security recovery*

4.1 Network Security Architectures

4.1.5 ISO Security Mechanisms

- **Pervasive Security Mechanism**

- *Trusted functionality* (可信赖性)
 - ✧ Any functionality providing or accessing security mechanisms should be trustworthy (值得信赖)
 - ✧ May involve combination of software and hardware
- *Security Labels* (安全标签)
 - ✧ Any resource (e.g. stored data, processing power, communications bandwidth) may have security label associated with it to indicate security sensitivity.
 - ✧ Similarly labels may be associated with users. Labels may need to be securely bound to transferred data.

4.1 Network Security Architectures

4.1.5 ISO Security Mechanisms

- **Pervasive Security Mechanism**

- *Event Detection*
 - ✧ Includes detection of
 - attempted security violations (and whether they succeeded)
 - legitimate security-related activity.
 - ✧ Can be used to trigger event reporting (alarms), event logging, automated recovery.
- *Security Audit Trail*
 - ✧ Log of past security-related events.
 - ✧ Permits detection and investigation of past security breaches.
- *Security Recovery*
 - ✧ Includes mechanisms to handle requests to recover from security failures.
 - ✧ May include immediate abort of operations, temporary invalidation of an entity, addition of entity to a blacklist.

4.1 Network Security Architectures

4.1.5 ISO Security Mechanisms

- **Services vs. Mechanisms**

- ISO 7498-2 indicates which mechanisms can be used to provide which services.
 - ✧ It is illustrative and NOT definitive.
- Obvious omissions include:
 - ✧ the possible use of data integrity mechanisms to help provide peer entity authentication and data origin authentication services
 - ✧ the possible use of encryption to help provide non-repudiation service (as part of notarization)

4.1 Network Security Architectures

Service / Mechanism	Encryption	Digital Signature	Access Control	Data Integrity
Entity authentication	Y	Y		●
Origin authentication	Y	Y		●
Access control			Y	
Connection confidentiality	Y			
Connectionless confidentiality	Y			
Selective field confidentiality	Y			
Traffic flow confidentiality	Y			
Connection integrity with recovery	Y			Y
Connection integrity without recovery	Y			Y
Selective field connection integrity	Y			Y
Connectionless integrity	Y	Y		Y
Selective field connectionless integrity	Y	Y		Y
Non-repudiation of origin	●	Y		Y
Non-repudiation of delivery	●	Y		Y

4.1 Network Security Architectures

Service / Mechanism	Authorization exchange	Traffic padding	Routing Control	Notarisation
Entity authentication	Y			
Origin authentication				
Access control				
Connection confidentiality			Y	
Connectionless confidentiality			Y	
Selective field confidentiality				
Traffic flow confidentiality		Y	Y	
Connection integrity with recovery				
Connection integrity without recovery				
Selective field connection integrity				
Connectionless integrity				
Selective field connectionless integrity				
Non-repudiation of origin				Y
Non-repudiation of delivery				Y



End of Chapter 4.1

