信息安全综述

前言

- 随着计算机技术的不断普及，信息安全的重要性日渐突显。无论是政府还是企业，乃至更多的普通Internet使用者，都面临着如何应对日益严峻的网络攻击、信息泄密、信息丢失等信息安全问题的考验。世界各国政府以及众多信息安全产品厂家在信息安全规范的制定和相关产品的研发方面投入了巨大的人力和财力。
- 本课程主要介绍信息安全管理和网络攻击防范所应采取的基本原则和措施。

信息安全的目的：保护企业信息资产

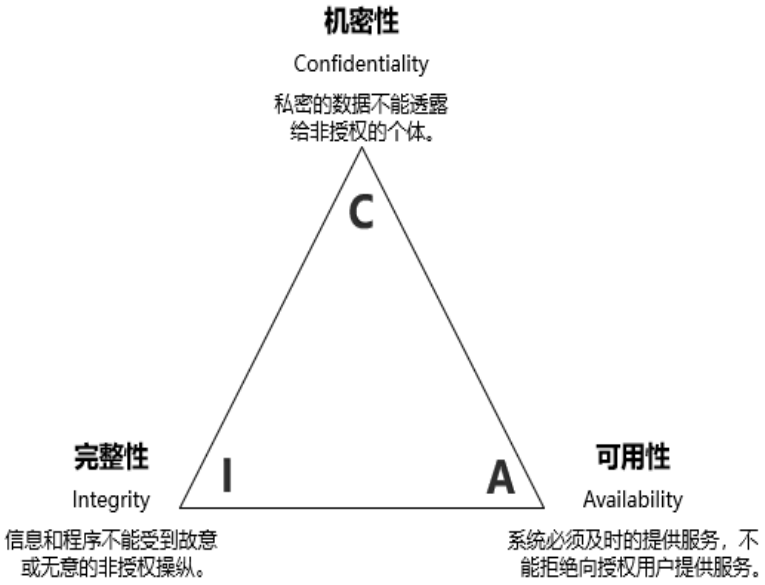
- 对于企业来说，信息资产是维持企业持续运作和管理的必要资产，例如市场报告、科研数据、计划方案、竞争情报等信息可能从多个方面对企业的运营产生影响。

- 现在，保护企业、个人信息的重要性已经毋庸置疑，对

于网络工程师来说，学习信息安全的目的主要是了解如何系统的保障企业信息资产的安全，尤其是了解我们所学习的网络技术在这中间所发挥的作用。那么，什么是信息资产呢？

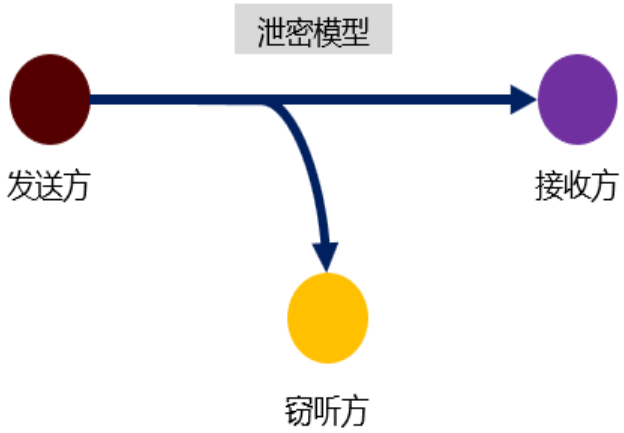
- 随着技术的发展，企业的业务流程及信息处理越来越依赖于 IT 设施，许多企业出于快速处理信息的考虑，甚至将所有的业务信息电子化。因此，IT 基础设施的正常运行及对电子信息的良好保护，成为企业业务顺利进行和发展的关键因素之一。
- 信息在企业业务中扮演着如此重要的角色，因此我们可以认为信息也是一种资产，并称之为信息资产。信息资产尽管是无形的，但由于它包含了大量的业务数据、客户信息、商业秘密等对企业的业务乃至存亡密切相关的内容，所以信息资产也面临大量的威胁和风险，包括有意或无意的销毁、黑客攻击、恶意软件所造成的数据丢失、内部人员的泄漏等。这些威胁和风险中，最有可能发生并造成严重后果的便是保密信息被泄漏。一旦发生数据泄漏事件，企业不单要承担保密数据本身价值的损失，严重的时候还会影响到企业的声誉和公众形象，并有可能面临法律上的麻烦。

为信息资产提供CIA保护



- 信息安全的核心目标是为关键资产提供机密性、完整性和可用性（CIA 三元组）保护。所有安全控制、机制和防护措施的实现都是为了提供这些原则中的一个或多个。
- CIA（Confidentiality-Integrity-Availability）三元组是信息安全的三个最基本的目标：
- 机密性（Confidentiality）：指信息在存储、传输、使用的过程中，不会被泄漏给非授权用户或实体；
- 完整性（Integrity）：指信息在存储、传输、使用的过程中，不会被非授权用户篡改或防止授权用户对信息进行不恰当的篡改；
- 可用性（Availability）：指确保授权用户或实体对信息资源的正常使用不会被异常拒绝，允许其可靠而及时地访问信息资源。

机密性与泄密模型

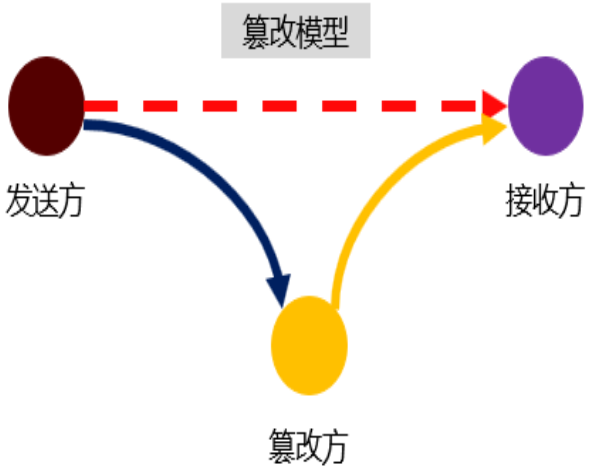


- 确保信息只能被授权访问方所接收的属性。

- 我们可以这样通俗的理解机密性：只有授权个人、实体或者过程才能访问受保护的信息。可以通过加密的方式来保障机密性。
- 对机密性而言，信息不能泄露给未授权者，这些未授权者可能包括个人、实体或者是过程。泄露的途径有很多，例如口头泄露、通过网络、打印机、复印机、USB 存储设备等。机密性是在日常的信息安全工作中强调的比较多，也是我们最容易理解的一个属性。因为机密性没有其他两个属性的含义那么宽泛，而且用户很容易将其与现实世界中的保密的概念进行类比。
- 数据加密的基本过程就是对原来为明文的文件或数据按某种算法进行处理，使其成为不可读的一段代码，通常称为"密文"，使其只能在输入相应的密钥之后才能显示出本来内容，通过这样的途径来达到保护数据不被非法窃取、阅读的目的。该过程的逆过程为解密，即将该编码信息转化为其原来数据的过程。

完整性与篡改模型

- 防止数据被未授权者意外修改、破坏或丢失。

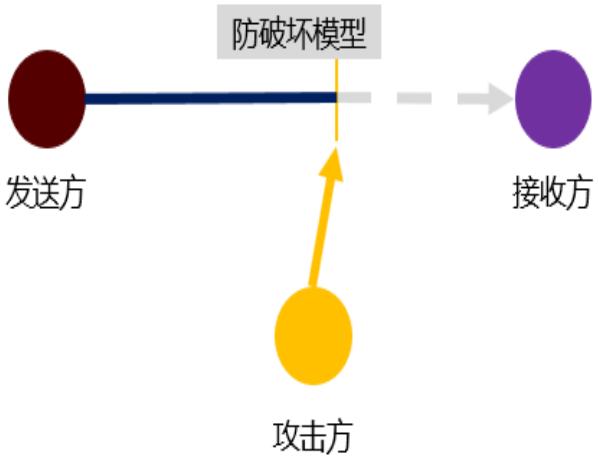


- 完整性通常被理解为“防止未经授权的更改”和“防篡改”等，在不同的环境中往往被赋予不同的含义。可以通过消息摘要来保障数据的完整性。
- 在信息安全领域，信息资产的完整性往往还意味着：
- 准确而且正确的，并非模糊的；
- 未被篡改的；
- 仅能以被认可的方法更改；
- 仅能被授权人员或过程更改；
- 有意义且能用的。
- 影响信息完整性的因素常见有：信息的来源，涉及到从哪里获得、如何获得、通过谁获得；信息到达前受保护的状况；信息在抵达本组织后受保护的情况等。
- 消息摘要（Message Digest）又称为数字摘要(Digital Digest)。它是一个唯一对应一个消息或文本的固定长度的值，它由一个单向 Hash 加密函数对消息进行作用而产生。接收者对所收到的消息进行计算所产生的摘要与原摘要进行比较，如

果消息在途中改变了，则比较的结果不一致，这样就可以判断消息是否被改变了。因此消息摘要保证了消息的完整性。

可用性与防破坏模型

- 保证信息和信息系统随时为授权者提供服务的有效特性。



- 可用性通俗的讲就是“合法用户想用时能用”。一个目标或者服务被认为是可用的，应该做到：
- 以能用的方式呈现；
- 有满足服务要求的能力；
- 有清晰的流程，如果在等待状态下，这种等待不是无限期的；
- 服务在可接受的时间段内可以完成。
- 拒绝访问和系统中断等是不可用的重要方面，而业务连续性管理是保持信息可用性的重要措施。一般而言，对信息处理设施可用性的要求会更高一些。

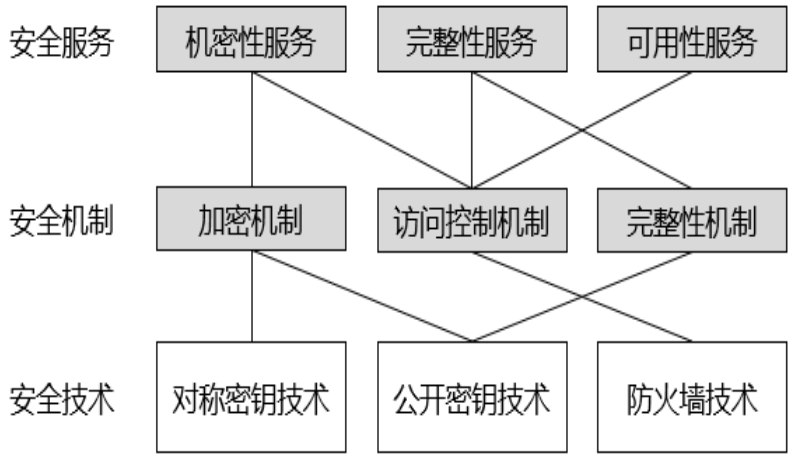
是什么威胁到了信息安全

风险	机密性	完整性	可用性
自然灾害		•	•
硬件故障	•	•	•
软件缺陷	•	•	•
未授权访问	•	•	
拒绝服务			•
数据泄露	•		•
假冒和欺诈	•	•	
线路窃听	•		
计算机病毒		•	•
特洛伊木马	•	•	
后门和陷阱	•	•	•
电磁辐射	•		
盗窃	•	•	•

- 威胁到信息安全的因素有很多，每种因素对机密性、完整性或可用性所造成的影响是不同的。例如当计算机的硬盘出现故障时，存放在硬盘上的数据丢失了，这就是数据的完整性遭到了破坏；用户现在无法在需要的时候访问到这些数据，就是数据的可用性遭到了破坏；在委托第三方修理硬盘的时候，他人可能会将硬盘上的数据拷贝给竞争对手，这就是数据的机密性遭到了破坏。
- 如表所示，威胁到信息安全的因素主要有：
- 自然灾害：指地震、火灾、水灾、风暴等这些因素将直接地到危害信息系统实体的安全。
- 硬件故障：指系统硬件的安全可靠性，包括计算机主体、存储系统、辅助设备、数据通讯设施以及信息存储介质的安全性。
- 软件缺陷：即计算机软件或程序中存在的某种破坏正常运行能力的问题、错误，或隐藏的功能缺陷。
- 未授权访问：没有经过预先同意就使用网络或计算机资

源的行为被看作是非授权访问。如有意避开系统访问控制机制、对网络设备及资源进行非正常使用、擅自扩大权限、越权访问信息等。它主要有以下几种表现形式：假冒、身份攻击、非法用户进入网络系统进行违法操作、合法用户以未授权方式进行操作等。

通过信息安全技术来保障信息安全



- 如果要保障信息的机密性、完整性、可用性，可以通过相应的安全机制来实现：
- 机密性服务可以通过加密机制和访问控制机制来实现。
- 完整性服务可以通过访问控制机制和完整性机制来实现。
- 可用性服务可以通过访问控制机制来实现。
- 安全机制则是通过安全技术来实现的：
- 加密机制可以通过对称密钥技术和公开密钥技术来实现。
- 访问控制机制可以通过防火墙技术来实现。
- 完整性机制可以通过公钥技术来实现。
- 如上所述，安全服务是指为保护信息安全所提供的安全防护措施，安全机制是支撑安全服务的手段，安全技术是安全

机制的具体表现。

- 对称密钥技术：
- 对称密钥加密又叫专用密钥加密，即发送和接收数据的双方必使用相同的密钥对明文进行加密和解密运算。对称密钥加密算法主要包括：DES、3DES 等。

只用技术保证就够了吗

- 技术措施需要配合正确的使用方法才能发挥作用。

- 如同把保险柜的钥匙落在锁眼上，精心设计的网络防御体系，因违规外连形同虚设。

通过信息安全管理来保障信息安全

- 在信息安全问题上，要综合考虑人员与管理、技术与产品、流程与体系等因素。

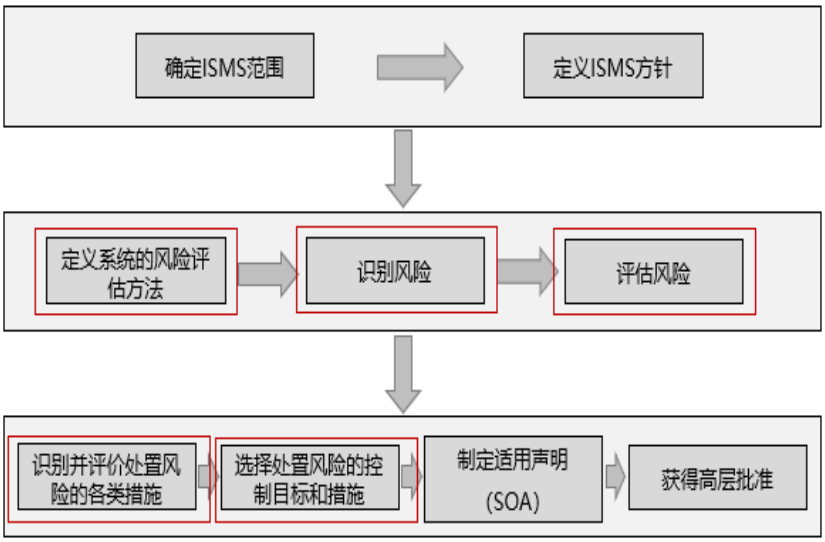
- 在信息安全问题上，要综合考虑人员与管理、技术与产品、流程与体系等因素。信息安全管理体系是人员、管理与技术三者的互动。

三种典型信息安全管理实施方法

	应用对象	应用特点
ISMS	各种类型的组织（有体系建立需求）	完全以市场化需求为主，不具备强制性。以风险管理方法为基础，如果实施体系认证，必须完全满足27001标准要求
等级保护	国家基础网络和重要信息系统	作为我国的一项基础制度加以推行，有一定强制性。主要目标是有效地提高我国信息和信息系统安全建设的整体水平，重点保障基础信息网络和重要信息系统的安全
NIST SP 800	联邦机构或非政府组织	与FIPS不同，是非强制性的。但联邦机构应采纳FIPS中要求使用的NIST SP以及OMB要求的特定NIST SP。以风险管理方法为基础，应用时有一定的灵活性

- 实施信息安全管理的三种典型方法是：信息安全管理体系（国际标准）、等级保护（中国标准）、NIST SP 800（美国标准）。在这里我们重点关注信息安全管理体系（ISMS）。
- 信息安全管理体系（Information Security Management System，简称 ISMS）起源于英国标准协会（British Standards Institution, BSI）1990 年代制定的英国国家标准 BS7799，是系统化管理思想在信息安全领域的应用。随着国际标准化组织（ISO）和国际电工学会（IEC）联合将 BSI 的相关工作转化为 ISMS 国际标准（ISO/IEC 27001:2005），ISMS 迅速得到全球各类组织的接受和认可，成为世界不同国家和地区、不同类型、不同规模的组织解决信息安全问题的有力武器。ISMS 证书也成为组织向其客户、合作伙伴等各种相关方及社会大众证明其信息安全能力和水平的标志。
- 等级保护：信息安全等级保护是对信息和信息载体按照重要性等级分级别进行保护的一种工作，在中国、美国等很多国家都存在的一种信息安全领域的工作。
- NIST SP 800：是美国 NIST（National Institute of Standards and Technology）发布的一系列关于信息安全的指南（SP 是 Special Publications 的缩写）。在 NIST 的标准系列文件中，虽然 NIST SP 并不作为正式法定标准，但在实际工作中，已经成为美国和国际安全界得到广泛认可的事实标准和权威指南。NIST SP 800 系列成为了指导美国信息安全管理建设的主要标准和参考资料。

信息安全管理体系中的风险管理



- 如图所示，信息安全管理体系的建设流程是有标准可循的，在这里面我们主要关注风险评估、风险处理、风险管理、以及管理风险的控制措施在这个流程中的地位和作用。
- 风险评估是信息安全管理的基础：
- 信息安全管理体系的建立需要确定信息安全需求；
- 信息安全需求获取的主要手段就是安全风险评估；
- 信息安全风险评估是信息安全管理体系建立的基础，没有风险评估，信息安全管理体系的建立就没有依据；
- 风险评估主要对信息安全管理体系范围内的信息资产进行鉴定和估价，然后对信息资产面对的各种威胁和脆弱性进行评估，同时对已存在的或规划的安全控制措施进行界定。
- 风险处理是信息安全管理的核心：
- 风险处理是对风险评估活动识别出的风险进行决策，采取适当的控制措施处理不能接受的风险，将风险控制在可按受的范围；
- 风险评估活动只能揭示组织面临的风险，不能改变风险

状况；

- 只有通过风险处理活动，组织的信息安全能力才会提升，信息安全需求才能被满足，才能实现其信息安全目标；
- 信息安全管理的核心就是这些风险处理措施的集合。

信息安全管理的内容

<table>
<tr><th colspan="5">信息安全管理体系控制领域（ISO/IEC 27001-2013）</th></tr>
<tr><td colspan="5">A.5 信息安全策略</td></tr>
<tr><td colspan="5">A.6 信息安全组织</td></tr>
<tr><td rowspan="5">A.7 人力资源安全</td><td colspan="4">A.8 资产管理</td></tr>
<tr><td colspan="4">A.9 访问控制</td></tr>
<tr><td colspan="4">A.10 密码</td></tr>
<tr><td>A.11 物理和环境安全</td><td>A.12 运行安全</td><td>A.13 通信安全</td><td>A.14 系统获取、开发和维护</td></tr>
<tr><td colspan="4">A.15 供应商关系</td></tr>
<tr><td colspan="5">A.16 信息安全事件管理</td></tr>
<tr><td colspan="5">A.17业务连续性管理的信息安全方面</td></tr>
<tr><td colspan="5">A.18 符合性</td></tr>
</table>

- ISO/IEC 27000 系列国际标准是从全盘考虑如何进行信息安全管理的最佳行业实践。这套标准将信息安全管理体系必要的组件划分为不同的模块。在这里我们需要掌握信息安全管理需要关注哪些控制领域。每个控制领域下的控制子域和控制目的则只需要了解即可。
- 国际标准 ISO/IEC 27001:2013《信息技术 安全技术 信息安全管理体系 要求》中列出了企业信息安全管理需要关注的 14 个领域和 113 项控制措施。这 14 个控制领域如图所示（内容前面的编号表示该项内容在该国际标准中的章节位置）。
- A.5 安全方针；
- A.6 信息安全组织；
- A.7 人力资源安全；

- A.8 资产管理；
- A.9 访问控制；
- A.10 密码学；
- A.11 物理与环境安全；
- A.12 操作安全；
- A.13 通信安全；
- A.14 信息系统获取、开发和维护；
- A.15 供应关系；
- A.16 信息安全事件管理；
- A.17 信息安全方面的业务连续性管理；
- A.18 符合性。

信息安全管理 - 控制子域 (1)

控制域	控制子域
A.5 信息安全策略	A.5.1 信息安全管理指导
A.6 信息安全组织	A.6.1 内部组织
	A.6.2 移动设备和远程工作
A.7 人力资源安全	A.7.1 任用前
	A.7.2 任用中
	A.7.3 任用的终止和变更
A.8 资产管理	A.8.1有关资产的责任
	A.8.2 信息分级
	A.8.3 介质处理
A.9 访问控制	A.9.1访问控制的业务要求
	A.9.2用户访问管理
	A.9.3 用户责任
A.10 密码	A.10.1 密码控制
A.11 物理和环境安全	A.11.1 安全区域
	A.11.2 设备
A.12 运行安全	A.12.1 运行规程和责任
	A.12.2恶意软件防范

- A.5 信息安全策略：
- A.5.1 信息安全管理指导：
- 目的：依据业务要求和相关法律法规，为信息安全提供管理指导和支持。
- A.6 信息安全组织：
- A.6.1 内部组织：

- 目的：建立一个管理框架，以启动和控制组织内信息安全的实现和运行。
- A.6.2 移动设备和远程工作：
- 目的：确保移动设备远程工作及其使用的安全。
- A.7 人力资源安全：
- A.7.1 任用前：
- 目的：确保员工和合同方理解其责任，并适合其角色。
- A.7.2 任用中：
- 目的：确保员工和合同方意识到并履行其信息安全责任。
- A.7.3 任用的终止和变更：
- 目的：在任用变更或终止过程中保护组织的利益。
- A.8 资产管理：
- A.8.1 有关资产的责任：
- 目的：识别组织资产并定义适当的保护责任。

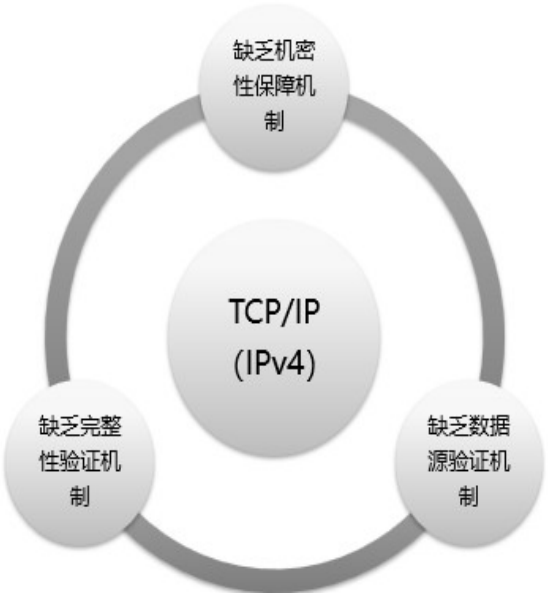
信息安全管理 - 控制子域 (2)

控制域	控制子域
A.12 运行安全	A.12.3 备份
	A.12.4 日志和监视
	A.12.5 运行软件控制
	A.12.6 技术脆弱性管理
	A.12.7 信息系统审计的考虑
A.13 通信安全	A.13.1 网络安全管理
	A.13.2 信息传输
A.14 系统获取、开发和维护	A.14.1信息系统的安全要求
	A.14.2开发和支持过程中的安全
	A.14.3 测试数据
A.15 供应商关系	A.15.1 供应商关系中的信息安全
	A.15.2 供应商服务交付管理
A.16 信息安全事件管理	A.16.1 信息安全事件的管理和改进
A.17业务连续性管理的信息安全方面	A.17.1 信息安全的连续性
	A.17.2 冗余
A.18 符合性	A.18.1 符合法律和合同要求
	A.18.2 信息安全评审

- A.12 运行安全：

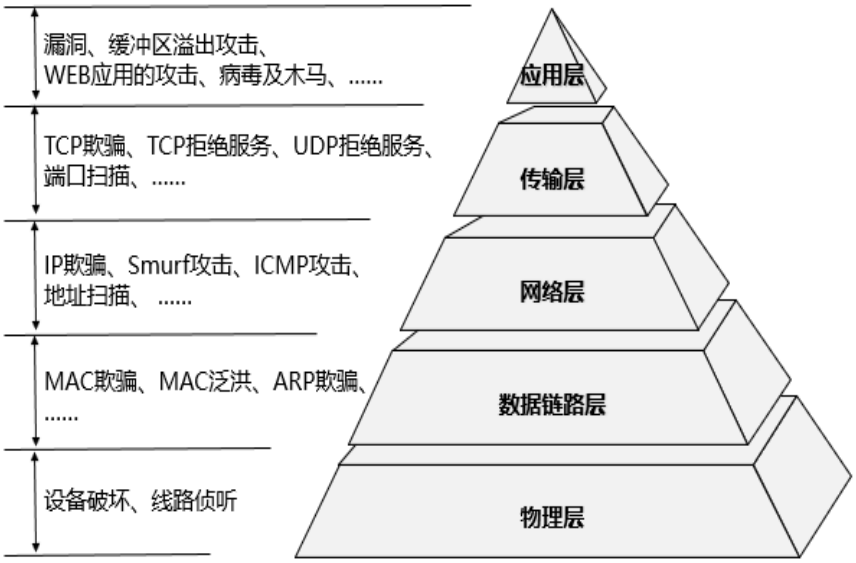
- A.12.3 备份：
- 目的：防止数据丢失。
- A.12.4 日志和监视：
- 目的：记录事态并生成证据。
- A.12.5 运行软件控制：
- 目的：确保运行系统的完整性。
- A.12.6 技术脆弱性管理：
- 目的：防止对技术脆弱性的利用。
- A.12.7 信息系统审计的考虑：
- 目的：使审计活动对运行系统的影响最小化。
- A.13 通信安全：
- A.13.1 网络安全管理：
- 目的：确保网络中的信息及其支持性的信息处理设施得到保护。
- A.13.2 信息传输：
- 目的：保持在组织内及与外部实体间传输信息的安全。
- A.14 系统获取、开发和维护：
- A.14.1 信息系统的安全要求：
- 目的：确保信息安全是信息系统整个生命周期中的一个有机组成部分。这也包括提供公共网络服务的信息系统的要求。

TCP/IP协议栈 - IPv4安全隐患



- 随着互联网的不断发展，TCP/IP 协议族成为使用最广泛的网络互联协议。但由于协议在设计之初对安全考虑的不够，导致协议存在着一些安全风险问题。Internet 首先应用于研究环境，针对少量、可信的用户群体，网络安全问题不是主要的考虑因素。因此，在 TCP/IP 协议栈中，绝大多数协议没有提供必要的安全机制，例如：
- 不提供认证服务；
- 明码传输，不提供保密性服务，不提供数据保密性服务；
- 不提供数据完整性保护；
- 不提供抗抵赖服务；
- 不保证可用性——服务质量（QoS）。

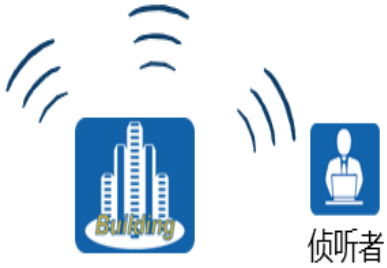
TCP/IP协议栈常见安全风险



- TCP/IP 协议栈中各层都有自己的协议。由于这些协议在开发之初并未重点考虑安全因素，缺乏必要的安全机制。因此，针对这些协议的安全威胁及攻击行为越来越频繁，TCP/IP 协议栈的安全问题也越来越凸显。接下来我们简要了解一下几种攻击类型。

物理层 - 线路侦听

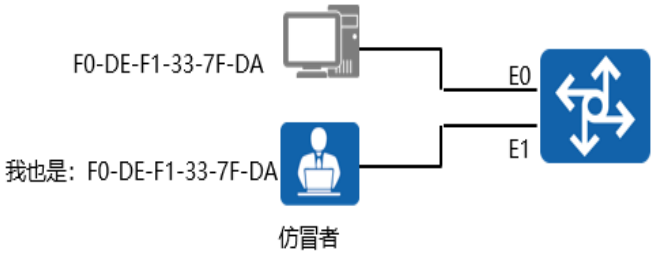
- 物理层网络设备:
  - 集线器;
  - 中继器。
- 无线网络。
- 对线路侦听的防范:
  - 对于网络中使用集线器，中继器之类的，有条件的话置换设备为交换机等。
  - 对于无线网络，使用强的认证及加密机制，这样窃听者即使能获取到传输信号，也很难把原始信息还原出来。



- 在常用网络设备中，集线器和中继器工作原理类似，从任何一个端口收上来的数据包都会转发到其它端口，这样，如果攻击者主机如果能够和这设备相连，通过相关的嗅探工具，就能够获取该网络上所有的通信数据信息。
- 对于无线网络，由于数据信息由无线信号传输，窃听者很容易获取到传输信号。
- 侦听在以太网组网中惯常使用，是基于传送进行攻击的基础。发起攻击的主机使用置于混杂模式的网卡，可以监听到同一物理网段内所有的报文。使用明文方式进行验证的协议，用户名和口令会泄露（SNMP/POP3/Telnet/……），使用明文进行传送的报文内容会泄漏；报文头中的内容也可能被利用。

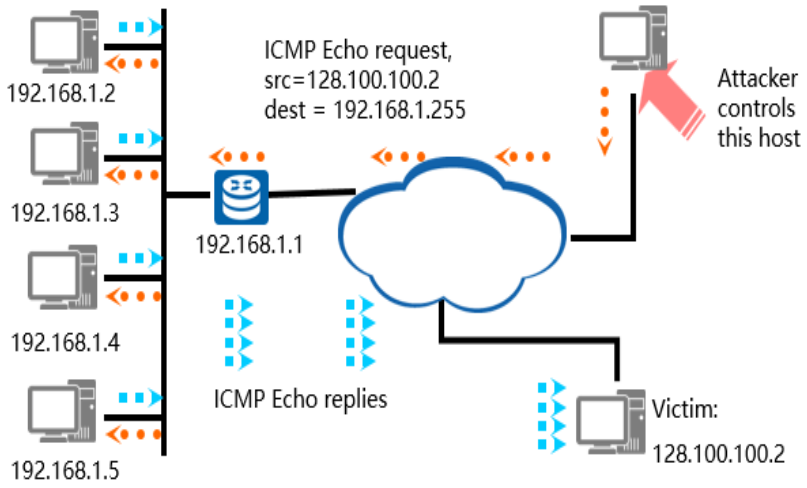
链路层 - MAC欺骗

- MAC欺骗是一种非常直观的攻击，攻击者将自己的MAC地址更改为受信任系统的地址。
- 对于MAC攻击的防范措施：
  - 在交换机上配置静态条目，将特定的MAC地址始终与特定的端口绑定。



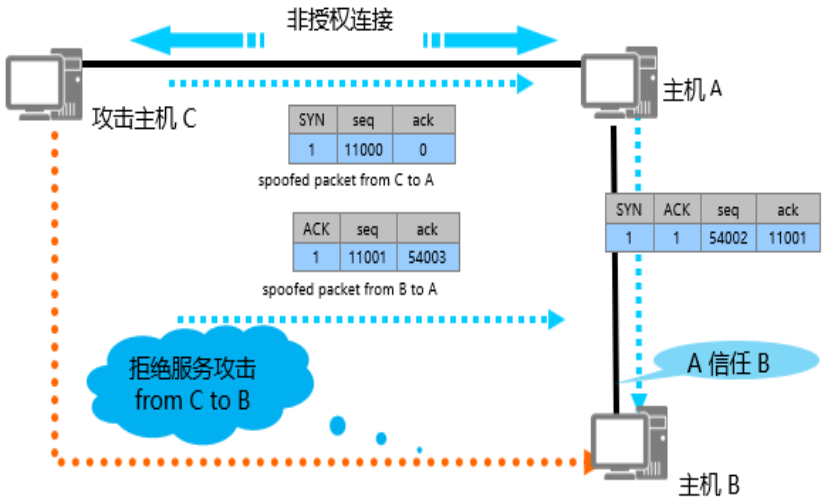
- 针对交换机的 MAC 地址学习机制，攻击者通过伪造的源 MAC 地址数据包发送给交换机，造成交换机学习到了错误的 MAC 地址与端口的映射关系，导致交换机要发送到正确目的地的数据包被发送到了攻击者的主机上，攻击者主机通过安装相关的嗅探软件，可获得相关的信息以实现进一步的攻击。
- 通过在交换机上配置静态条目，绑定到正确的出接口，就能避免 MAC 欺骗攻击风险。

网络层 - Smurf 攻击



- Smurf 攻击方法是发 ICMP 应答请求，该请求包的目标地址设置为受害网络的广播地址，这样该网络的所有主机都对此 ICMP 应答请求作出答复，导致网络阻塞。高级的 Smurf 攻击，主要用来攻击目标主机。方法是将上述 ICMP 应答请求包的源地址改为受害主机的地址，最终导致受害主机雪崩。攻击报文的发送需要一定的流量和持续时间，才能真正构成攻击。理论上讲，网络的主机越多，攻击的效果越明显。
- 针对 Smurf 攻击，在路由设备上配置检查 ICMP 应答请求包的目的地址是否为子网广播地址或子网的网络地址，如果是，则直接拒绝。

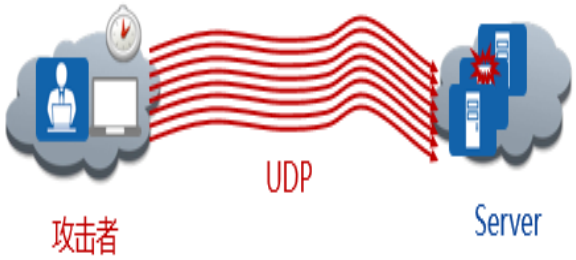
传输层 - TCP欺骗



- TCP 欺骗大多数发生在 TCP 连接建立的过程中，利用主机之间某种网络服务的信任关系建立虚假的 TCP 连接，可能模拟受害者从服务器端获取信息。具体过程与 IP 欺骗类似。
- 例如：A 信任 B，C 是攻击者，想模拟 B 和 A 之间建立连接。
- C 先破坏掉 B，例如使用 floogin, redirect, crashing 等；
- C 用 B 的地址作为源地址给 A 发送 TCP SYN 报文；
- A 回应 TCP SYN/ACK 报文，从 A 发给 B，携带序列码 S；
- C 收不到该序列码 S，但为了完成握手必须用 S+1 作为序列码进行应答，这时 C 可以通过以下两种方法得到序列码 S：
- C 监听 SYN/ACK 报文，根据得到的值进行计算；
- C 根据 A 操作系统的特性等，进行猜测。
- C 使用得到的序列码 S 回应 A，握手完成，虚假连接建立。

传输层 - UDP Flood攻击

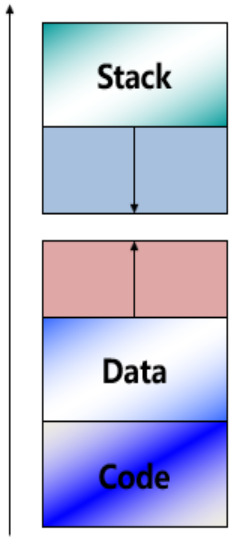
- 攻击者通过向服务器发送大量的UDP报文，占用服务器的链路带宽，导致服务器负担过重而不能正常向外提供服务。



- 由于 UDP 协议是无连接的，所以不能对其进行连接状态的检测。通过对 UDP 报文进行主动统计和学习，分析某个主机发送 UDP 报文的规律和特征，如果存在一台主机大量发送相同、相似或以某种特定规律变化的 UDP 报文时，则将其认为是攻击者。
- 通过配置对 UDP 报文速率限制，可以实现 UDP Flood 的攻击防范。

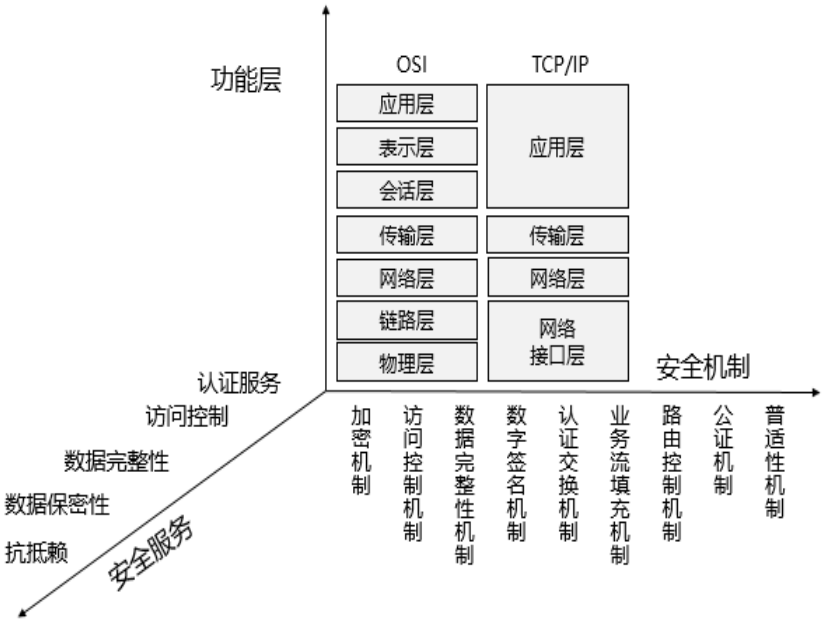
应用层 - 缓冲区溢出攻击

- 攻击软件系统的行为中，最常见的一种方法。
- 可以从本地实施，也可以从远端实施。
- 利用软件系统（操作系统，网络服务，程序库）实现中对内存操作的缺陷，以高操作权限运行攻击代码。
- 漏洞与操作系统和体系结构相关，需要攻击者有较高的知识/技巧。



- 缓冲区是内存中存放数据的地方。在程序试图将数据放到机器内存中的某一个位置的时候，因为没有足够的空间就会发生缓冲区溢出。而人为的溢出则是有一定企图的，攻击者写一个超过缓冲区长度的字符串，植入到缓冲区，然后再向一个有限空间的缓冲区中植入超长的字符串，这时可能会出现两个结果：一是过长的字符串覆盖了相邻的存储单元，引起程序运行失败，严重的可导致系统崩溃；另一个结果就是利用这种漏洞可以执行任意指令，甚至可以取得系统 root 特级权限。

OSI安全体系结构



- 为了解决网络中存在的安全性问题，OSI（开放式系统互联）安全体系结构（国际标准号：ISO 7498-2）提出，设计安全的信息系统的基础架构中应该包含 5 种安全服务（安全功能）、能够对这 5 种安全服务提供支持的 8 类安全机制和普遍安全机制，以及需要进行的 5 种 OSI 安全管理方式。某种安全服务可以通过一种或多种安全机制提供，某种安全机制可用于提供一种或多种安全服务。
- 5 种安全服务为：鉴别服务、访问控制、数据完整性、数据保密性、抗抵赖性。
- 8 类安全机制：加密、数字签名、访问控制、数据完整性、数据交换、业务流填充、路由控制、公证。
- 安全服务：是指计算机网络提供的安全防护措施。国际标准化组织（ISO）定义了以下几种基本的安全服务：认证服务、访问控制、数据机密性服务、数据完整性服务、不可否认服务。
- 认证服务：确保某个实体身份的可靠性，可分为两种类型。一种类型是认证实体本身的身份，确保其真实性，称为实

体认证。实体的身份一旦获得确认就可以和访问控 制表中的权限关联起来，决定是否有权进行访问。口令认证是实体认证中—种最常见的方式。另一种认证是证明某个信息是否来自于某个特定的实体，这种认证叫做 数据源认证。数据签名技术就是一例。

- 访问控制：访问控制的目标是防止对任何资源的非授权访问，确保只有经过授权的实体才能访问受保护的资源。
- 数据机密性服务：数据机密性服务确保只有经过授权的实体才能理解受保护的信息、在信息安全中主要区分两种机密性服务：数据机密性服务和业务流机密性服务，数据机密 性服务主要是采用加密手段使得攻击者即使窃取了加密的数据也很难推出有用的信息；业务流机密性服务则要使监听者很难从网络流量的变化上推出敏感信息。
- 数据完整性服务：防止对数据未授权的修改和破坏。完整性服务使消息的接收者能够发现消息是否被修改，是否被攻击者用假消息换掉。

安全服务和安全机制的关系

机制 / 服务	加密	数字签名	访问控制	数据完整	认证交换	防流量分析	路由控制	公证
对象认证	•	•			•			
访问控制		•	•					
数据保密	•					•	•	
数据完整	•	•		•				
防抵赖性		•		•				•

- 如表所示，对于每一种服务的提供，有些机制被认为有时是适宜的，或由一种机制单独提供，或几种机制联合提供。此表展示了这些关系的一个概貌，而且也不是一成不变的。
- 例如，对象认证服务可以通过加密、数字签名、认证交换机制来实现；访问控制服务可以通过数字签名、访问控制机制来实现等。

功能层和安全机制的关系

OSI / 机制	物理层	链路层	网络层	传输层	会话层	表示层	应用层
加密	•	•	•	•		•	•
数字签名			•	•		•	•
访问控制			•	•			•
数据完整			•	•		•	•
认证交换			•	•			•
防流量分析			•				•
路由控制			•				
公证						•	•

- 如表所示，在参考模型的各个层上能够提供某些特定的安全服务。某一具体的安全服务时是由一个特定层选择提供的，除非特别说明，这种安全服务就由运行在该层的安全机制来提供。多个层能提供特定的安全服务。这样的层不总是从它们本身提供这些安全服务，而可以使用在较低层中提供的适当的安全服务。即使在一个层内没有提供安全服务，该层的服务定义也可能需要修改以便容许安全服务的请求传递到较低层。
- 例如，网络层可以提供提供的安全服务有加密、数字签名、访问控制、数据完整、认证交换、防流量分析、路由控制。

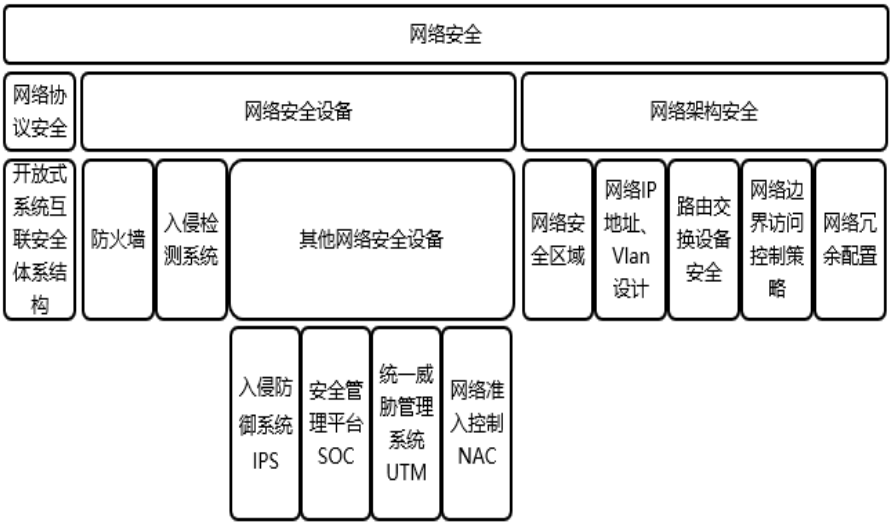
安全协议分层

协议层	针对的实体	安全协议	主要实现的安全策略
应用层	应用程序	S-HTTP	信息加密、数字签名、数据完整性验证
		SET	信息加密、身份认证、数字签名、数据完整性验证
		PGP	信息加密、数字签名、数据完整性验证
		S/MIME	信息加密、数字签名、数据完整性验证
		Kerberos	信息加密、身份认证
		SSH	信息加密、身份认证、数据完整性验证
传输层	端进程	SSL/TLS	信息加密、身份认证、数据完整性验证
		SOCKS	访问控制、穿透防火墙
网络层	主机	IPSec	信息加密、身份认证、数据完整性验证
网络接口层	端系统	PAP	身份认证
		CHAP	身份认证
		PPTP	传输隧道
		L2F	传输隧道
		L2TP	传输隧道
		WEP	信息加密、访问控制、数据完整性验证
		WPA	信息加密、身份认证、访问控制、数据完整性验证

- 前面我们知道了要保障网络安全需要做些什么，侧重于从安全原理上来描述问题；接下来我们来看一下在 TCP/IP 协议栈的各层有哪些具体的安全协议可以实现我们的网络安全理念或安全策略。当然，我们只有把能实现这些安全协议的安全设备部署在网络中，并进行相应的配置，才能最终实现这些安全策略。
- 如表所示，在网络接口层有针对端到端的安全协议，如 PAP（可实现身份认证安全策略）、PPTP（可实现传输隧道安全策略）协议等；在网络层有主机到主机的安全协议，如 IPSec（可实现信息加密、身份认证、数据完整性验证安全策略）。以此类推，每层的安全协议和可实现的安全策略如下：
- 网络接口层：
- PAP（Password Authentication Protocol，密码认证协议）。
- CHAP（Challenge Handshake Authentication Protocol，挑战握手认证协议）。

- PPTP（Point-to-Point Tunneling Protocol，点对点隧道协议）。
- L2F（Level 2 Forwarding protocol，第二层转发协议）。
- L2TP（Layer 2 Tunneling Protocol，第二层隧道协议）。
- WEP（Wired Equivalent Privacy，有线等效保密）。
- WPA（Wi-Fi Protected Access，Wi-Fi 网络保护访问）。
- 网际层：
- IPSec（IP Security，IP 层安全协议）。

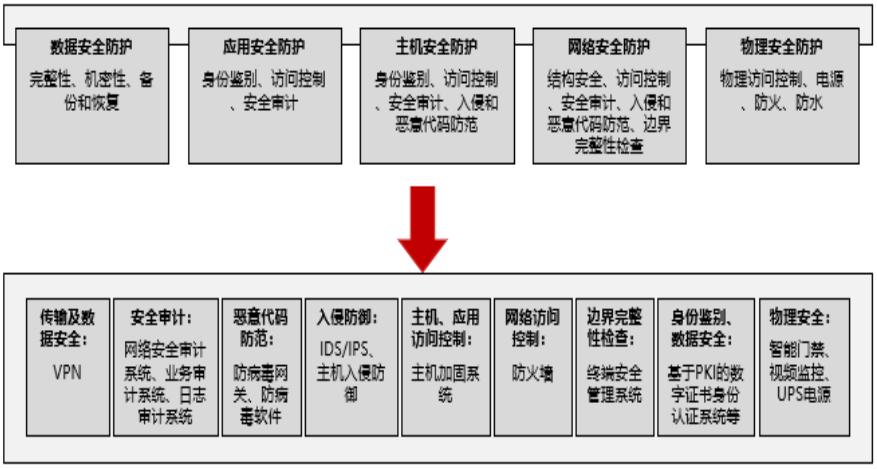
信息安全技术 - 网络安全



- 网络安全管理是信息安全管理体系的一个重要组成部分。

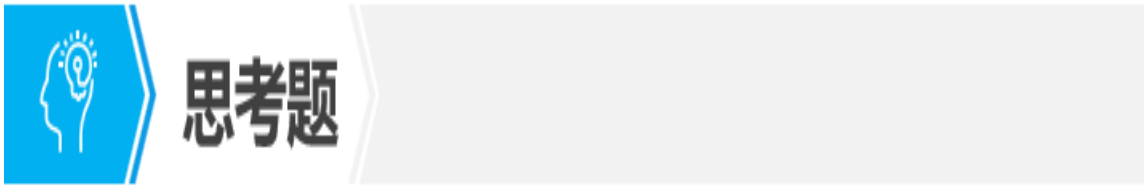
- 保障网络安全是信息安全管理中的一项重要工作。在通常的认识当中，网络安全只是意味着在网络架构中添加一台防火墙设备而已，这种认识是远远不够的。如图所示，除了防火墙，保障网络安全还需要入侵检测系统、网络边界访问控制策略、网络冗余配置等安全设备或控制措施。

安全设计需求与安全设备



- 前面我们曾经提到，只有把能实现安全协议的安全设备部署在网络中，并进行相应的配置，才能最终实现安全策略。那么如何进行部署呢？
- 进行信息系统的安全性设计应首先明确系统的安全需求，对信息系统的架构、承载的业务等进行综合分析，确定系统的安全风险和防护需求，平衡安全、成本和效率之间的关系，确定安全保护措施。随着信息系统和业务的发展，安全保证系统也应不断完善。
- 物理安全：包括物理位置的选择、物理访问控制和防盗、防火、防水、防雷、温湿度控制、电力供应、防静电和电磁防护。例如重要区域配置电子门禁系统，机房设置防盗报警系统和设置火灾自动消防系统。
- 网络安全：包括结构安全、安全审计、访问控制、边界完整性检查、恶意代码防范、入侵防范和网络设备防护等。
- 主机安全：包括身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范和资源控制等。

- 应用安全：包括身份鉴别、访问控制、安全审计、通信完整性、通信保密性、抗抵赖、软件容错和资源控制等。
- 数据安全：包括数据完整性和保密性、数据的备份和恢复。



1. 信息安全最关心的三个属性是什么?

A. 机密性 (Confidentiality)

B. 完整性 (Integrity)

C. 可用性 (Availability)

D. 身份验证 (Authentication)

- 1、答案：ABC。