网络信息安全知识点整理

第一章 计算机与网络安全概念

1.1 计算机安全概念

1.1.1 计算机安全定义

计算机安全

对于一个自动化的信息系统，采取保护措施确保信息系统资源（包括硬件、软件、固件、信息/数据和通信）的完整性, 可用性和保密性。

计算机安全核心三目标

目标	包含	解释
保密性	数据保密性	确保隐私或秘密信息不向非授权者泄密，也不被非授权者使用
	隐私性	确保个人能够控制或确定与其自身相关的哪些信息是可以被收集的、被保存的，这些信息可以由谁来公开以及向谁公开
完整性	数据完整性	确保信息和程序只能以特定和授权的方式进行改变
	系统完整性	确保系统以一种正常的方式来执行预定的功能，免于有意或无意的非授权操纵
可用性		确保系统能工作迅速，对授权用户不能拒绝服务

附加目标

目标	包含
真实性	一个实体是真实性的、可被验证的和可被信任的特性；对传输信息来说，信息和信息的来源是正确的。也就是说，能够验证那个用户是不是他声称的那个人，以及系统的每一个输入输出是否来自可信赖的信源。
可追溯性	这一安全目标要求实体的行为要能唯一追溯到该实体。这一属性支持不可否认性、阻止、故障隔离、入侵检测和预防、时候恢复以及法律诉讼。因为无法得到真正安全的系统，我们必须能够追查到对安全泄露负有责任的一方。系统必须保留它们活动的记录，以允许事后的审计分析，进而跟踪安全事件进而解决争执。

1.1.2 实例

如果发生了安全泄露事件，我们使用三个层次说明对组织和个人的影响。

层次	定义
低	这种损失对组织的运行、组织的资产和个人的负面影响有限。有限的负面影响是指，保密性、完整性、可用性有如下的缺失可能：1. 导致执行任务的能力在一定时间和程度上降级，期间仍能完成主要的功能，但效果稍微降低。2. 导致资产的较少损失。3. 导致很小的经济损失。4. 导致对个人很小的伤害
中	这种损失对组织的运行、组织的资产和个人的负面影响严重。严重的负面影响是指，1. 导致执行任务的能力在一定时间和程度上显著降级，期间仍能完成主要的功能，但效果明显降低。2. 导致资产的显著损失。3. 导致显著的经济损失。4. 导致对个人显著的伤害，但不包括丧命或严重威胁生命安全的伤害
高	这种损失对组织的运行、组织的资产和个人的负面影响是灾难性的。灾难性的负面影响是指，1. 导致执行任务的能力在一定时间和程度上严重降级，期间不能完成主要的一项或多项功能。2. 导致大部分资产的显著损失。3. 导致大部分经济损失。4. 导致对个人的灾难性伤害，包括丧命或严重威胁生命安全

保密性

保密等级	信息
低	学生、老师、院系名单
中	学生的注册信息
高	学生的分数信息

完整性

完整性要求	信息
低	匿名在线民意调查
中	提供论坛供用户注册来讨论一定话题的Web站点
高	医院病人的过敏信息

可用性

可用性要求	信息
低	在线电话目录查询应用
中	为现有的或潜在的学生和捐助人提供信息的大学网站
高	为关键系统、应用和设备提供认证服务的系统

计算机安全的挑战

计算机安全的复杂性体现在以下方面：

序号	概述	原因	实例
1	安全对于初学者而言并没有想象的那么简单。	尽管对安全服务的大部分要求都可用含义不言自明的单词给出，但要满足这些要求的机制却非常复杂	保密性、认证、不可否认或完整性
2	设计一个特别的安全机制或算法时，一定要考虑各种各样的潜在攻击	以与设计完全不同的方式看待问题往往可以使攻击成功，此时通常利用了设计机制中未考虑到的弱点	
3	由于第2点，提供一些特殊安全服务的方法并不直观。	通常，安全机制比较复杂，只有考虑到了威胁的各个方面，精心设计的安全机制才有意义。	
4	设计好各种安全机制后，接下来是决定在哪里使用这些机制。	包括物理位置（如网络的什么地方需要某一安全机制）和逻辑位置（在协议栈的哪一层或哪几层需要安全机制）	TCP/IP 协议栈
5	安全机制所用的算法或协议通常不止一个。	这些协议或算法要求参与者拥有一些秘密信息（如加密密钥），这就带来了与秘密信息产生、分发和保护等相关问题。而且，通信协议的一些行为也可能使安全机制的构建变得复杂。	若安全机制的正确执行对发送者和接收者的消息发送时间有限制，而任何协议或网络都存在不确定且不可预测的延时，则会使这个这个时间限制变得毫无意义
	计算机和网络安全本	入侵者要努力找到漏洞，而设计者或	

6	质上是一场入侵者和设计者之间的智力战争。	管理员要努力封堵漏洞。入侵者的优势在于它仅需要找到一个弱点，而设计者必须找到并根除所有弱点来获得完全的安全	
7	多数用户和管理员都有一种倾向，即只有发生了安全事件，才会意识到安全投资的收益。		
8	安全需要经常的甚至不断的监管，而这在当今短期、负荷过重的环境中难以做到。		
9	绝大多数情况下，安全措施仍然是一种事后措施。	安全可能是在系统设计完成以后，才被考虑增加到系统中的，而不是从一开始就作为整个系统设计过程的组成部分	
10	许多用户，甚至是安全管理员，认为强的安全不利于信息系统高效工作，有碍于用户友好操作和对信息的使用		

1.2 OSI 安全架构

问题背景

需要有效评价一个机构的安全需求，以及对各种安全产品和政策进行评价和选择，负责安全的管理员要以某种系统的的方法来定义安全需求，并表征满足这些要求的措施。OSI是提供安全的一种组织方法。

OSI的关注点

OSI架构主要关注安全攻击、安全机制和安全服务。它们简短的定义如下：

关注点	定义
安全攻击	任何危机信息系统安全的行为
安全机制	用来检测、阻止攻击或从攻击状态恢复到正常状态的过程（或实现该过程的设备）
安全服务	加强数据处理系统和信息传输的安全性的一种处理过程或通信服务，目的在于利用一种或多种安全机制进行反攻击。

威胁和攻击

威胁	**破坏安全的潜在可能，在环境、能力、行为或事件允许的情况下，它们会破坏，造成伤害。也就是说，威胁是脆弱性被利用而可能带来的危险**
攻击	对系统安全的攻击，它来源于一种具有智能的威胁，即有意违反安全服务和侵犯系统安全策略（特别是方法或或技术方面的）的智能行为

1.3 安全攻击

被动攻击和主动攻击

被动攻击	**试图获取或利用系统的信息，但不影响系统资源**
主动攻击	试图改变系统资源或影响系统运行

1.3.1 被动攻击

	INTERPRET
特性	对传输进行窃听或监测，不涉及对数据的更改，很难被察觉
目标	获得传输的信息
方式	信息内容泄露攻击、流量攻击
应对	使用加密的方法来阻止攻击，重点是预防而非检测

信息内容攻击

电话、电子邮件信息、和传输的文件都有可能含有敏感的或秘密的信息，我们希望能阻止攻击者获取这些信息。

流量分析

即使我们对消息进行了恰当的加密保护，攻击者仍有可能获取这些信息的一些模式。攻击者可以确定通信主机的位置和身份，可以观察到传输消息的频率和长度。同心者可以利用这些信息来判断通信的某些性质。

1.3.2主动攻击

	说明
特性	难以被检测，由于物理通信设施、软件和网络本身潜在弱点的多样性，主体攻击难以绝对预防
目标	对数据流进行修改或伪造数据流
方式	伪装、重放、消息修改、拒绝服务
应对	检测并从攻击造成的破坏和延迟中恢复过来。如果对主动攻击有威慑效果，那么其在某种程度上也可以阻止主动攻击。

攻击方式

	说明	有效路径	实例
伪装	某实体假装成其他实体	2	截获认证消息，并且在认证消息完成合法验证后重放，无权限的实体就可通过冒充有权限的实体获得额外的权限
重放	攻击者未授权的将截获的信息再次发送	1、2、3	
消息修改	未经授权的修改和发信息的一部分，或延迟消息的传输，或改变消息的顺序。	1、2	"Allow John Smith to read confidential file accounts" -> "Allow Fred Brown to read confidential file accounts"
拒绝服务	阻止或禁止对通信设施的正常使用或管理	3	某实体可能会查禁所有发向某目的地的消息。拒绝服务的另一种形式是破坏整个网络或使整个网络失效，或者使网络过载以降低其性能

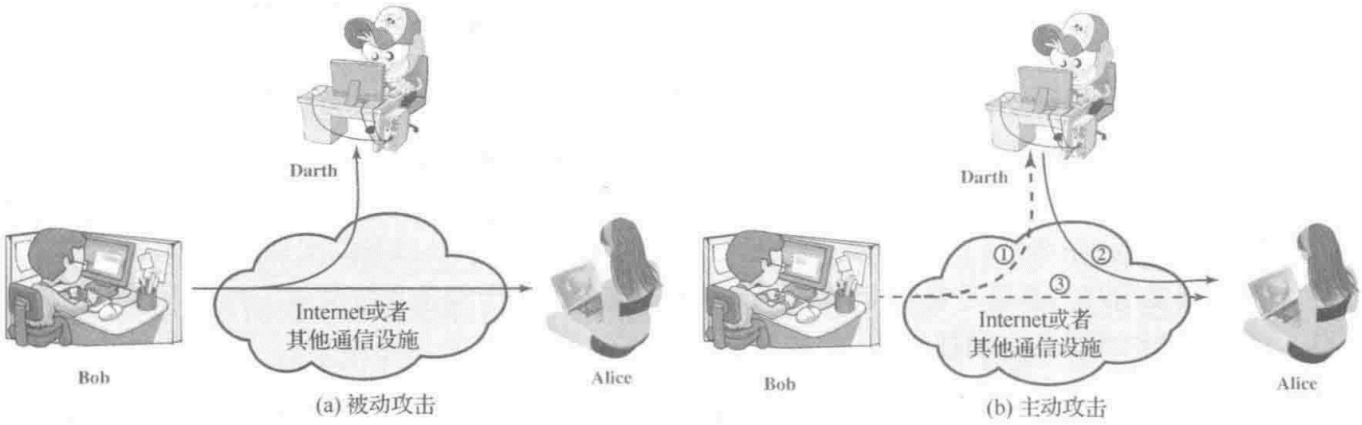

图 1.2　安全攻击

1.4 安全服务

定义

在通信开放系统中，为系统或数据传输提供足够安全的协议层服务。

安全服务是指一种由系统提供的对系统资源进行特殊保护的处理或通信服务。

这些服务被分为5类共14个服务：

表 1.2　安全服务

认　证	数据完整性
保证通信的实体是它所声称的实体 **同等实体认证** 用于逻辑连接时为连接的实体的身份提供可信性 **数据源认证** 在无连接传输时保证收到的信息来源是声称的来源	保证收到的数据的确是授权实体发出的数据（即未修改、插入、删除或重播） **具有恢复功能的连接完整性** 提供一次连接中所有用户数据的完整性。检测整个数据序列内存在的修改、插入、删除或重播，且试图恢复之 **无恢复的连接完整性** 同上，但仅提供检测，无恢复 **选择域连接完整性** 提供一次连接中传输的单个数据块内用户数据的指定部分的完整性，并判断指定部分是否有修改、插入、删除或重播 **无连接完整性** 为单个无连接数据块提供完整性保护，并检测是否有数据修改。另外，提供有限的重播检测 **选择域无连接完整性** 为单个无连接数据块内指定域提供完整性保护；判断指定域是否被修改
访问控制	**不可否认性**
阻止对资源的非授权使用（即这项服务控制谁能访问资源，在什么条件下可以访问，这些访问的资源可用于做什么）	防止整个或部分通信过程中，任一通信实体进行否认的行为 **源不可否认性** 证明消息是由特定方发出的 **宿不可否认性** 证明消息被特定方收到
数据保密性	
保护数据免于非授权泄露 **连接保密性** 保护一次连接中所有的用户数据 **无连接保密性** 保护单个数据块中的所有用户数据 **选择域保密性** 对一次连接或单个数据块中指定的数据部分提供保密性 **流量保密性** 保护那些可以通过观察流量而获得的信息	

1.4.1 认证

用以保证通信的真实性。

问题

1. 在连接的初始化阶段，认证服务保证两个实体是可信的，也就是说，每个实体都是他们所声称的实体。
2. 认证服务必须保证该连接不受第三方的干扰：这种干扰是指，第三方能够伪装成两个合法实体中的一个进行非授权传输或接收。

特殊服务

服务	说明
对等实体认证	为连接中的对等实体提供身份确认。不同系统中的两个实体执行相同的协议时，考虑他们是对等的，如位于两个通信系统中的两个TCP模块。对等实体认证用于连接的建立或数据传输阶段。这个服务期望提供这样的保证：一个实体没有试图进行伪装或对以前的连接进行非授权重放。
数据流认证	为数据的来源提供确认，对数据的复制或修改并不提供保护。这种服务支持电子邮件这样的应用，在这种应用的背景下，通信实体在通信前未预先进行交互。

1.4.2 访问控制

访问控制是限制和控制那些通过通信连接对主机与应用进行访问的一种能力。每个试图获得访问控制的实体必须被识别或认证后，才能获取相应的访问权限。

1.4.3 数据保密性

保密性是指防止传输的数据遭到被动攻击。

层级

层级	说明	实例
广义	一段时间内为两个用户间所传输的所有用户数据提供保护。	如果两个系统间建立了TCP连接，则这种广泛的保护将防止在TCP连接上传输的任何用户数据的泄露。
狭义	对单条消息或对单条消息内某个特定的范围提供保护。	

另一个方面

防止流量分析。攻击者不能观察到消息的源地址与目的地址、频率、长度或通信设施上的其他流量特征。

1.4.4 不可否认性

防止发送方或接收方否认传输或接收过某条消息。

消息发出后，接收方能证明消息是由声称的发送方发出的。同样，消息接收后，发送方能证明消息确实由声称的接收方收到。

1.4.5 可用性

定义

根据系统的性能说明，系统资源可被授权实体请求访问或使用（即当用户请求服务时，若系统能够提供符合系统设计的这些服务，则系统是可用的）。

措施

1. 自动防御措施，如认证、加密来防止。
2. 需要使用一些物理措施来阻止或恢复分布式系统中被破坏了可用性的那部分功能。

可用性服务

这种服务处理由拒绝服务攻击引起的安全问题。依赖于访问控制服务和其他安全服务。