

第一章 概述

- 1.1 计算机安全的概念
- 1.2 威胁、攻击和资产
- 1.3 安全功能要求
- 1.4 基本安全设计原则
- 1.5 攻击面和攻击树
- 1.6 计算机安全策略
- 1.7 标准

三个基本问题

Q1 我们需要保护什么样的资产？

Q2 这些资产是如何受到威胁的？

Q3 我们可以做些什么来应对这些威胁？

补充：安全的概念

“如果把一封信锁在保险柜中，把保险柜藏起来，然后告诉你去看这封信，这并不是安全，而是隐藏；相反，如果把一封信锁在保险柜中，然后把保险柜及其设计规范和许多同样的保险柜给你，以便你和世界上最好的开保险柜的专家能够研究锁的装置，而你还是无法打开保险柜去读这封信，这才是安全...”

-Bruce Schneier

举个例子

□ 假定我们的目标是个网站，那么网页中的数据、服务器资源、后台用户数据等等一系列资源都是我们要保护的**资产**（Q1）。

□ 从**web安全**的角度上，敌手（adversary）会从中间件到搭建平台，从CMS（Web内容管理）到操作系统详尽的对站点进行信息收集寻找漏洞加以利用进行入侵，敌手的攻击以及潜在的漏洞都是站点中资产所受的威胁（Q2）。

□ 从**管理人员**角度上，他们则会思考如何预防入侵，如何在入侵发生后使得资源损失最小化（Q3）

内容安排

- 1.1 计算机安全的概念
- 1.2 威胁、攻击和资产
- 1.3 安全功能要求
- 1.4 基本安全设计原则
- 1.5 攻击面和攻击树
- 1.6 计算机安全策略
- 1.7 标准

1.1 计算机安全的概念

- 1.1.1 计算机安全的定义
- 1.1.2 实例
- 1.1.3 计算机安全面临的挑战
- 1.1.4 一个计算机安全模型

1.1.1 定义&CIA三元组

- ❑ **NIST内部/机构间报告NISTIR 7298**（关键信息安全术语表，2013年5月）定义术语**计算机安全**（computer security）如下：
- ❑ 计算机安全：保证信息系统资产的**机密性**（confidentiality）、**完整性**（integrity）和**可用性**（availability）的措施和控制方法，其中资产包括硬件、软件、固件以及要处理、存储和通信的信息。
- ❑ **CIA三元组**，这三个指标体现的是保障计算机数据安全和**服务安全**的基本目标。

机密性缺失：非授权的信息披露

CIA三元组-机密性

❑ 机密性：保留对信息获取和披露的授权限制，包括保护个人隐私和专有信息的手段。抛去书面化表达，其想表达的就是“非授权者不得访问”。

❑ 机密性={ 数据机密性, 隐私性}, 这个定义将机密性拆分成了两个角度：

- 数据机密性：从数据出发，其表达的是确保机密数据不被非授权个人获取。
- 隐私性：从个人出发，其表达的是只有数据所有者本人才能决定自己的数据能被谁获取。

完整性缺失：非授权的信息修改或破坏

CIA三元组-完整性

□完整性：防止对信息的不正当修改获破坏，其中包括保证信息的抗抵赖性和真实性。

□完整性={数据完整性，系统完整性}，这个定义将完整性拆分成了两个角度：

- 数据完整性：确保信息和程序只能在指定的和得到授权的情况下才能够被改变。
- 系统完整性：确保系统在未受损的方式下执行预期的功能，避免对系统进行非授权操作。

CIA三元组-可用性

- ❑ 可用性：确保系统能够迅速地进行工作，并且不能拒绝授权用户的服务请求。
- ❑ 可用性缺失：对信息或信息系统的访问和使用的破坏。
 - 可用性最常见的攻击例子是拒绝服务攻击（DoS）。以SYN FLOOD为例，其原理是发送大量的SYN数据报而不回应ACK数据报，从而使得服务器处于TCP半开状态，进而耗尽其资源最终使得服务器瘫痪。

真实性和可说明性

除此之外，还引入如下两个概念来对计算机安全进行全面的描述：

- ❑ **真实性：**真实性是一种能够被验证和信任的表示真实情况或正确程度的属性，它使得传输、消息和消息源的有效性能够被充分相信。
- ❑ **可说明性：**要求实体动作能够被唯一的追踪，其作用可简述为当安全事件发生，相关责任人的行为能够被记录，方便取证追责。

补充知识：TCP/IP相关知识

- TCP报文格式
- TCP通信过程

TCP报文格式

源端口（16 位）								目的端口（16 位）							
序号（32 位）															
确认号（32 位）															
TCP 头长 （4 位）	保留位 （6 位）	U R G	A C K	P S H	R S T	S Y N	F I N	窗口大小（16 位）							
校验和（16 位）								紧急指针（16 位）							
可选项（0 或更多的 32 位字）															
数据（可选项）															

TCP控制位

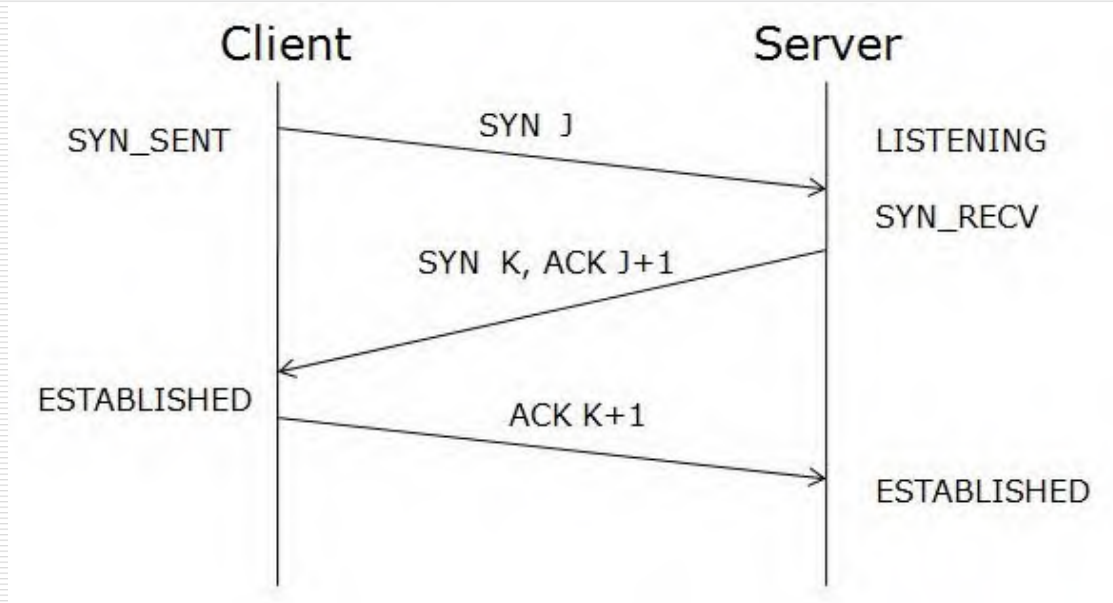
- ❑ **URG:** 为紧急数据标志。如果它为1，表示本数据包中包含紧急数据。此时紧急数据指针有效。
- ❑ **ACK:** 为确认标志位。如果为1，表示包中的确认号是有效的。否则，包中的确认号无效。
- ❑ **PSH:** 如果置位，接收端应尽快把数据传送给应用层。
- ❑ **RST:** 用来复位一个连接。**RST**标志置位的数据包称为复位包。一般情况下，如果**TCP**收到的一个分段明显不是属于该主机上的任何一个连接，则向远端发送一个复位包。
- ❑ **SYN:** 标志位用来建立连接，让连接双方同步序列号。如果**SYN=1**而**ACK=0**，则表示该数据包为连接请求，如果**SYN=1**而**ACK=1**则表示接受连接。
- ❑ **FIN:** 表示发送端已经没有数据要求传输了，希望释放连接。

TCP通信过程

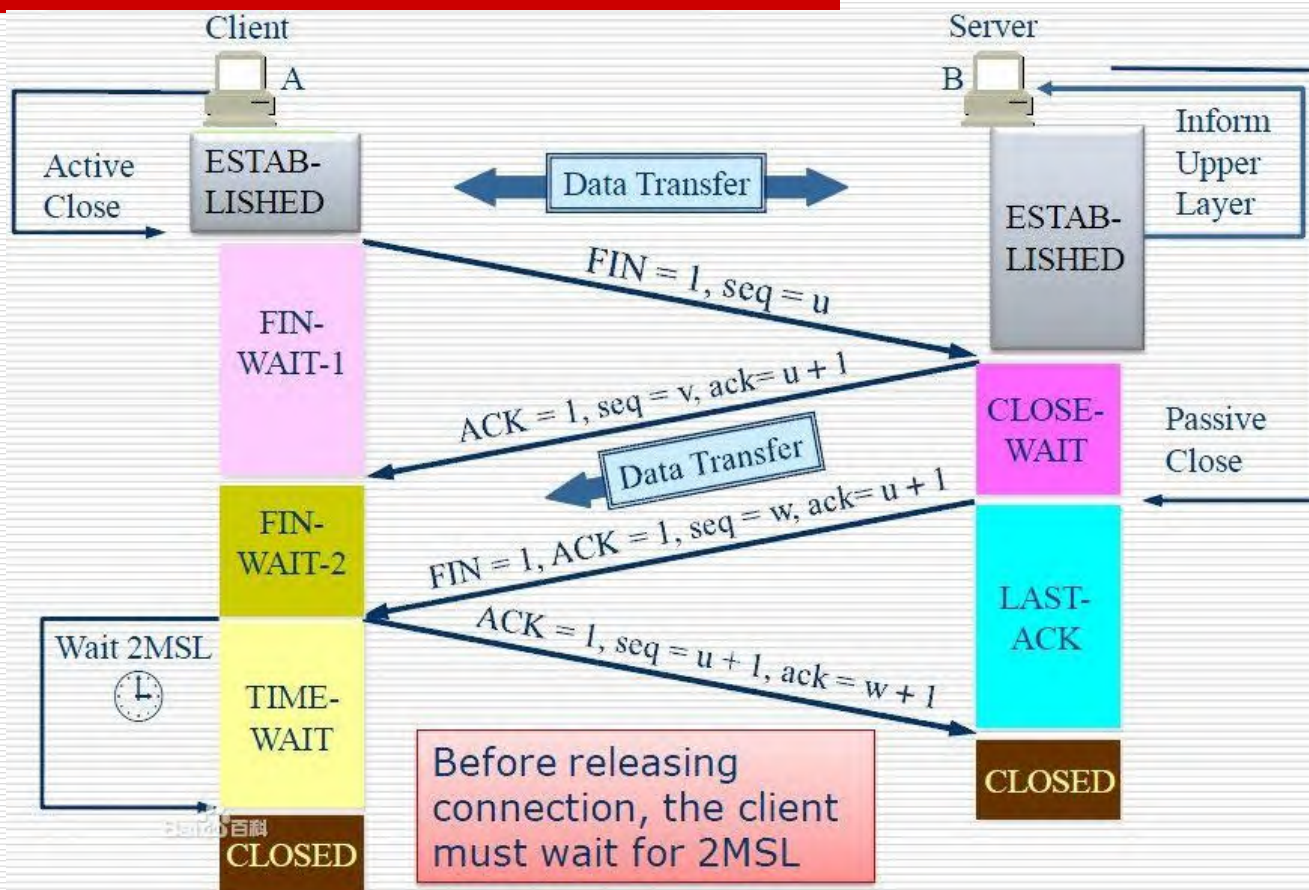
□ 正常TCP通信过程:

- 建立连接
- (数据传输)
- 断开连接

建立TCP连接(三次握手)



断开TCP连接



MSL: 最长报文寿命 (Maximum Segment Lifetime)

图片来自百度百科

案例：SYN洪水

- ❑ SYN Flood是当前最流行的拒绝服务攻击方式之一，这是一种利用TCP协议缺陷，发送大量伪造的TCP连接请求，使被攻击方资源耗尽(CPU满负荷或内存不足)的攻击方式。
- ❑ SYN Flood是利用TCP连接的三次握手过程的特性实现的。

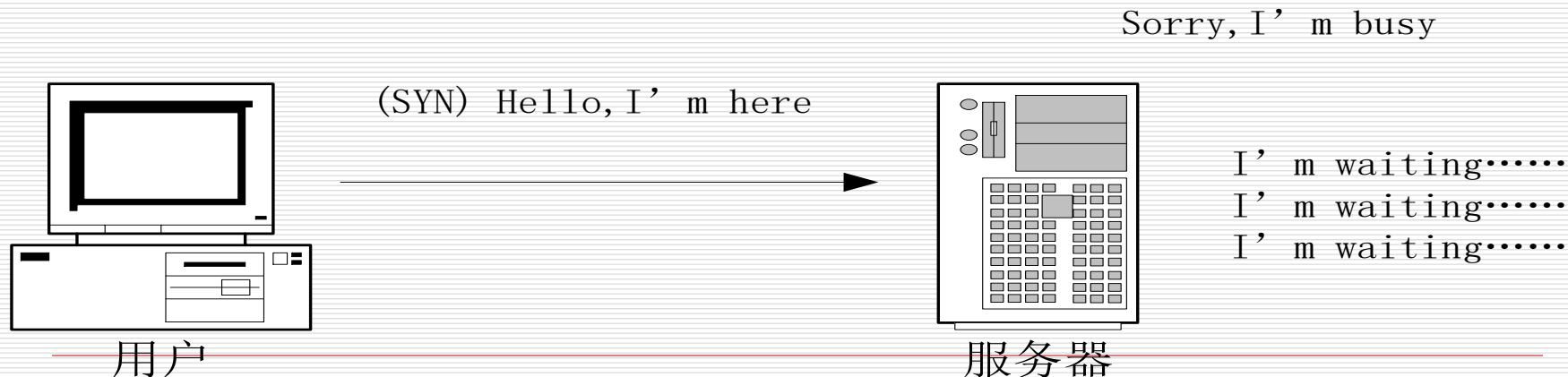
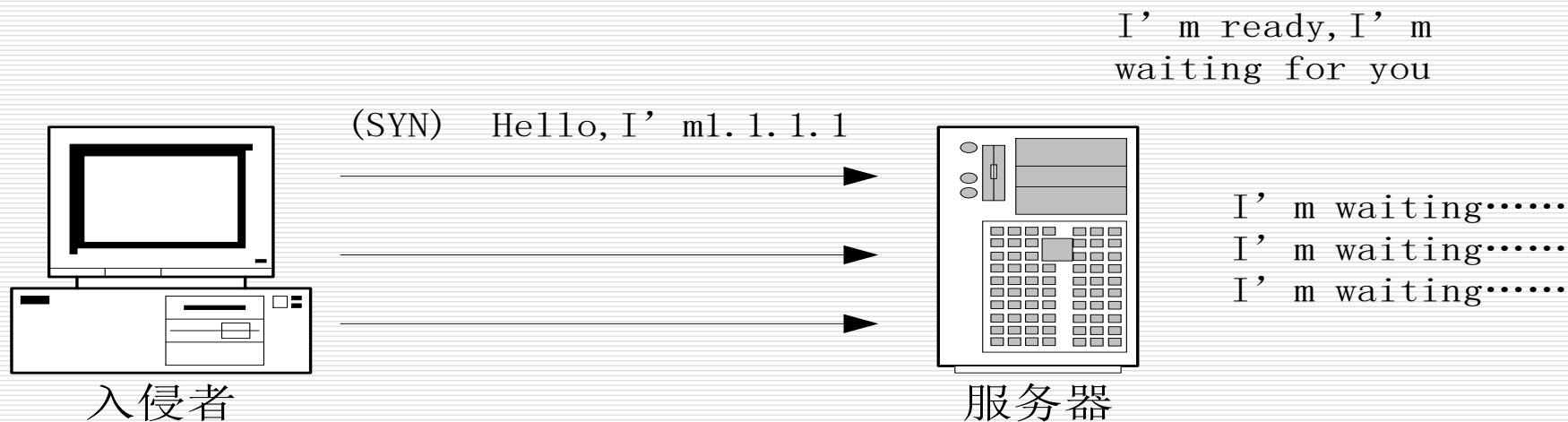
案例：SYN洪水

- 在TCP连接的三次握手过程中，假设一个客户端向服务器发送了SYN报文后突然死机或掉线，那么服务器在发出SYN/ACK应答报文后是无法收到客户端的ACK报文的，这种情况下服务器端一般会重试，并等待一段时间后丢弃这个未完成的连接。这段时间的长度我们称为SYN Timeout。一般来说这个时间是分钟的数量级。
- 一个用户出现异常导致服务器的一个线程等待1分钟并不是什么很大的问题，但如果有一个恶意的攻击者大量模拟这种情况(伪造IP地址)，服务器端将为了维护一个非常大的半连接列表而消耗非常多的资源。

案例：SYN洪水

- 即使是简单的保存并遍历半连接列表也会消耗非常多的CPU时间和内存，何况还要不断对这个列表中的IP进行SYN+ACK的重试。
- 实际上如果服务器的TCP/IP栈不够强大，最后的结果往往是堆栈溢出崩溃——即使服务器端的系统足够强大，服务器端也将忙于处理攻击者伪造的TCP连接请求而无暇理睬客户的正常请求，此时从正常客户的角度来看，服务器失去响应，这种情况就称作：服务器端受到了SYN Flood攻击(SYN洪水攻击)。

SYN“洪水”攻击示意图



1.1.2 实例

FIPS 199将安全性缺失的影响级别分成三级：低，中，高。

- 低级：对公司运作、资产以及个人影响有限
- 中等：对公司运作、资产以及个人影响严重
- 高级：对公司运作、资产以及个人产生灾难性影响

1.1.3 计算机安全面临的挑战

- ❑ 大多数主要安全服务需求都可以用含义明确的一个术语来标识。满足这些需求的机制可能非常复杂，会涉及到相当多的细致的推理论证。
- ❑ 在开发某种安全机制或算法时，我们必须始终考虑对安全特征的潜在攻击。
- ❑ 通常情况下安全机制的设计是复杂的，不能单纯通过需求来判定方法是否可用
- ❑ 对于已经设计出的各种安全机制，决定其适用场合是非常必要的。
- ❑ 安全机制通常包含不止一种算法或协议。

1.1.3 计算机安全面临的挑战

- ❑ 对于攻击者，主要优势在于他只需要找到一个安全弱点或漏洞；而管理者必须找到且消除所有的安全弱点才能得到真正的安全。
- ❑ 对于部分用户和系统管理者，有种自然倾向：在安全保障失效之前，很少能看到安全投入所带来的好处。
- ❑ 安全要求定期甚至持续地对系统进行监视，但是在目前注重时效、超负荷运转的系统环境中很难做到这一点。
- ❑ 安全性通常还是事后考虑的问题——在系统设计完成后才加入系统，而没有作为设计过程中的一个有机组成部分来看待。

1.1.4 一个计算机安全模型

资产（**asset**）是用户或者管理员希望保护的**对象**，其大致可分为**硬件、软件、数据、通信设施及网络**四类。

- **硬件**：计算机系统以及其他用于数据存储、处理和通信的设备
- **软件**：操作系统、系统实用程序、应用程序
- **数据**：文件、数据库以及口令等
- **通信设施和网络**：网络中的通信设备，如链路交换机，集线器，路由器等

1.1.4 一个计算机安全模型

脆弱性（**vulnerability**）:[NRC02]列出了有关计算机系统或网络资产脆弱性的一般分类：

- 针对完整性：系统资源可能被恶意损坏，以至于做出不当操作或给出错误应答
- 针对机密性：系统资源可能被泄露
- 针对可用性：系统资源可能不可用或者非常慢

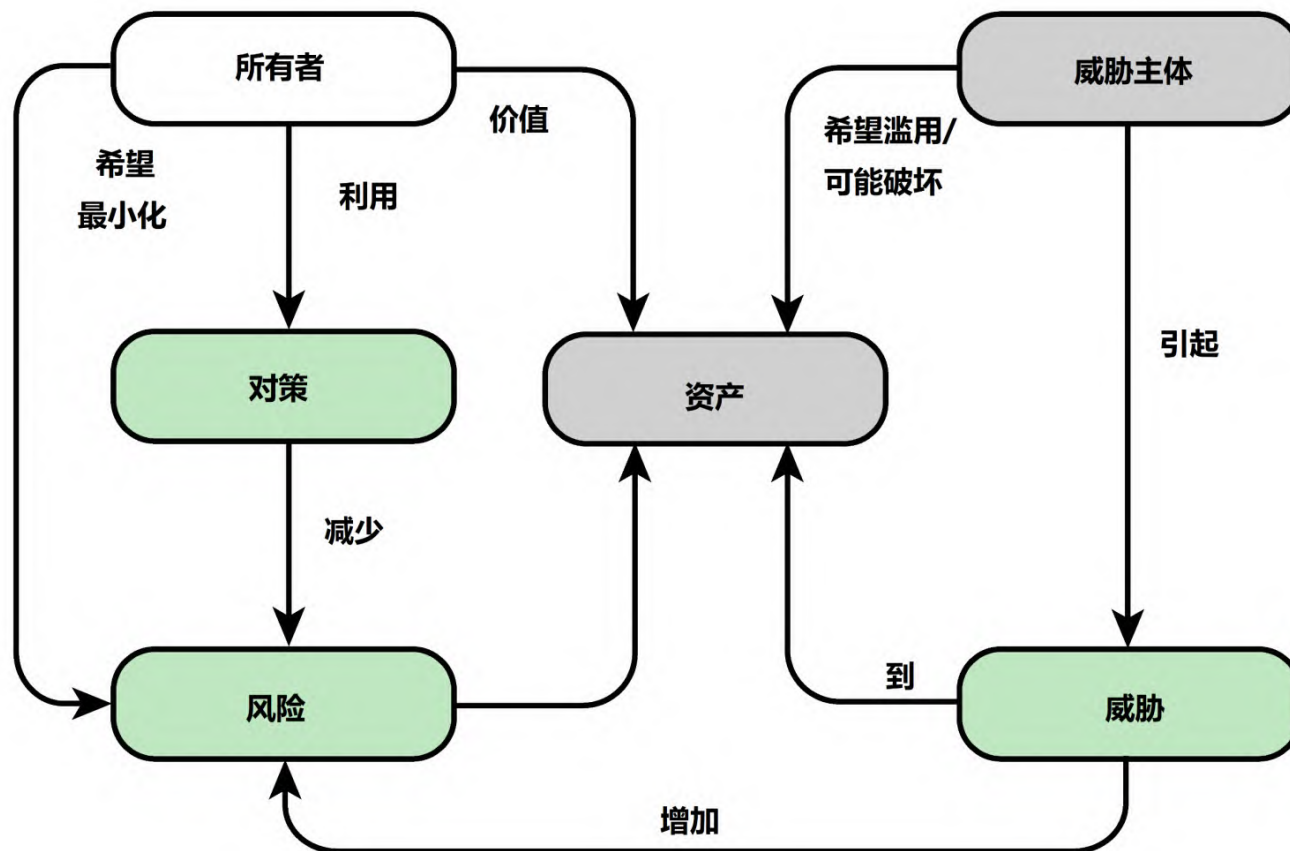
计算机安全术语

- ❑ 敌手(威胁代理) (*Adversary (threat agent)) 进行或有意进行有害活动的个人、团体、组织或政府。
- ❑ 攻击 (Attack) 任何类型的恶意活动，试图收集、破坏、拒绝、降级，或者破坏信息系统资源或信息本身。
- ❑ 对策 (Countermeasure) 一种(或多种)设备或技术。其目的是削弱不良或有害活动的操作有效性，或防止间谍活动、破坏活动、盗窃活动、未经授权访问以及使用敏感信息(或信息系统)。
- ❑ 风险 (Risk) 衡量一个实体受潜在环境或事件威胁的程度，通常是：
1) 环境或事件发生时可能产生的不利影响； 2) 发生的可能性。

计算机安全术语

- ❑ **安全策略 (Security Policy)** 提供安全服务的一套标准。它定义和约束数据处理设施的活动，以维持系统和数据的安全状况。
- ❑ **系统资源(资产) (asset)** 主要应用程序、通用支持系统、高影响程序、物理工厂、关键任务系统、人员、设备或逻辑相关的系统组。
- ❑ **威胁 (Threat)** 任何可能通过未经授权的访问、销毁、披露、修改信息以及拒绝服务而(借助信息系统)对组织运营(包括任务、职能、形象或声誉)、组织资产、个人、其他组织或国家产生不利影响的情况或事件。
- ❑ **脆弱性(vulnerability)** 可能被威胁源利用或触发的信息系统、系统安全程序、内部控制或实现中的弱点。

安全概念及其关系



补充知识：漏洞概念

- 信息安全的一个核心问题就是存在于计算机系统和网络系统中的**安全漏洞**。恶意的攻击者可以利用这些安全漏洞访问未授权资源，破坏敏感数据，进而威胁信息系统的安全。安全漏洞作为安全问题的焦点越来越受到人们的重视。

漏洞的概念

- 安全漏洞：是指信息系统在设计、实现或者运行管理过程中存在的缺陷或不足，从而使攻击者能够在未授权的情况下利用这些缺陷破坏系统的安全策略。
- 存在于信息系统的需求、设计、实现、配置、运行等环境
- 能够被恶意主体所利用，影响信息系统及其服务的正常运行
- 网络攻防的核心：
 - 攻击----漏洞利用
 - 防御----漏洞修复

Note:

*这里对于攻防的理解是比较简单和直接，当然攻防还包括除漏洞以外的技术和手段。



国家计算机网络入侵防范中心

NATIONAL COMPUTER NETWORK INTRUSION
PROTECTION CENTER

网站首页 中心简介 新闻中心 安全漏洞 联系我们

您当前的位置是：安全漏洞 | 漏洞库

搜索

首页

网站首页

中心简介

中心概况

组织结构

新闻中心

新闻动态

安全公告

安全漏洞

漏洞库

漏洞检索

漏洞周报

漏洞月报

其他

联系我们

漏洞库结果显示列表

严重级别：■ 紧急 ■ 高 ■ 中 ■ 低

第一页 ----- 最后一页

1

总共有 7 条匹配结果，共有 1 页，现为第 1 页

NIPC-2011-2075 ■ Android Picasa访问权限获取漏洞 (2011-11-17)

NIPC-2009-2829 ■ Open Handset Alliance Android SMS (2009-08-03)

NIPC-2009-2693 ■ Android手机平台权限验证多个绕过漏洞 (2009-11-17)

NIPC-2009-2098 ■ Android ' PackageManagerService类 (2009-05-26)

NIPC-2009-0688 ■ Open Handset Alliance Android M多 (2009-11-17)

NIPC-2008-0618 ■ Android软件开发工具包BMP文件处理 (2008-11-05)

NIPC-2008-0617 ■ Android Web浏览器GIF文件堆溢出漏洞 (2008-11-05)

总共有 26 条匹配结果，共有 2 页，现为第 1 页

NIPC-2010-4265 ■ Apple iOS 堆缓冲区溢出漏洞 (2010-11-26)

NIPC-2010-4264 ■ Apple iOS 不安全通信漏洞 (2010-11-26)

NIPC-2010-4263 ■ Apple iOS权限提升漏洞 (2010-11-26)

NIPC-2010-4262 ■ Apple iOS 未指明漏洞 (2010-11-26)

NIPC-2010-4261 ■ Apple iOS 未指明漏洞 (2010-11-26)

NIPC-2010-4260 ■ Apple iOS 验证不充分漏洞 (2010-11-26)

NIPC-2010-3354 ■ Apple iOS ImageIO缓冲区溢出漏洞 (2010-09-09)

NIPC-2010-3353 ■ Apple iOS WebKit对象释放后再利用漏洞 (2010-09-09)

NIPC-2010-3352 ■ Apple iOS WebKit远程代码执行漏洞 (2010-09-09)

NIPC-2010-3351 ■ Apple iOS WebKit远程代码执行漏洞 (2010-09-09)

NIPC-2010-3350 ■ Apple iOS WebKit对象释放后再利用漏洞 (2010-09-09)

NIPC-2010-3349 ■ Apple iOS ImageIO远程代码执行漏洞 (2010-09-09)

NIPC-2010-3347 ■ Apple iOS Accessibility组件未指明漏洞 (2010-09-09)

NIPC-2010-3346 ■ Apple iOS WebKit重复释放漏洞 (2010-09-09)



国家计算机网络入侵防范中心

NATIONAL COMPUTER NETWORK INTRUSION
PROTECTION CENTER

网站首页 中心简介 新闻中心 安全漏洞

您当前的位置是：安全漏洞 | 漏洞库

首页

网站首页

中心简介

中心概况

组织结构

新闻中心

新闻动态

安全公告

安全漏洞

漏洞库

漏洞检索

漏洞周报

漏洞月报

其他

联系我们

漏洞库

严重级别: ■ 紧急 ■

第一页 ----

总共有 7 条匹配结果

NIPC-2011-2075 ■ Android Pi

NIPC-2009-2829 ■ Open Hands
(2009-08-03)

NIPC-2009-2693 ■ Android手机
(17)

NIPC-2009-2098 ■ Android '
(05-26)

NIPC-2009-0688 ■ Open Hands
(17)

NIPC-2008-0618 ■ Android软件
(05)

NIPC-2008-0617 ■ Android We

Microsoft Internet Explorer 安全漏洞 (MS15-124) (MS15-125)

漏洞编号: NIPC-2015-5562

CVE编号: CVE-2015-6142

漏洞类别: 许可, 权限和访问控制错误

发布日期: 2015-12-09

更新日期: 2015-12-09

CVSS值: 9.3

严重级别: ■ 紧急

利用范围: 网络

攻击复杂度: 中

认证级别: 没有

机密性影响: 整体

完整性影响: 整体

可用性影响: 整体

漏洞描述:

Microsoft Internet Explorer 中存在安全漏洞, 受影响的产品, 11 和 Microsoft Edge, 由于对内存缓冲区的创建、修改、管理或删除有误, 允许远程攻击者, 通过精心构造的 web 站点执行任意代码或者引起拒绝服务攻击 (内存破坏).

受影响系统或软件:

Denotes Vulnerable Software Changes related to vulnerability configurations

解决方案:

厂商已修复该漏洞

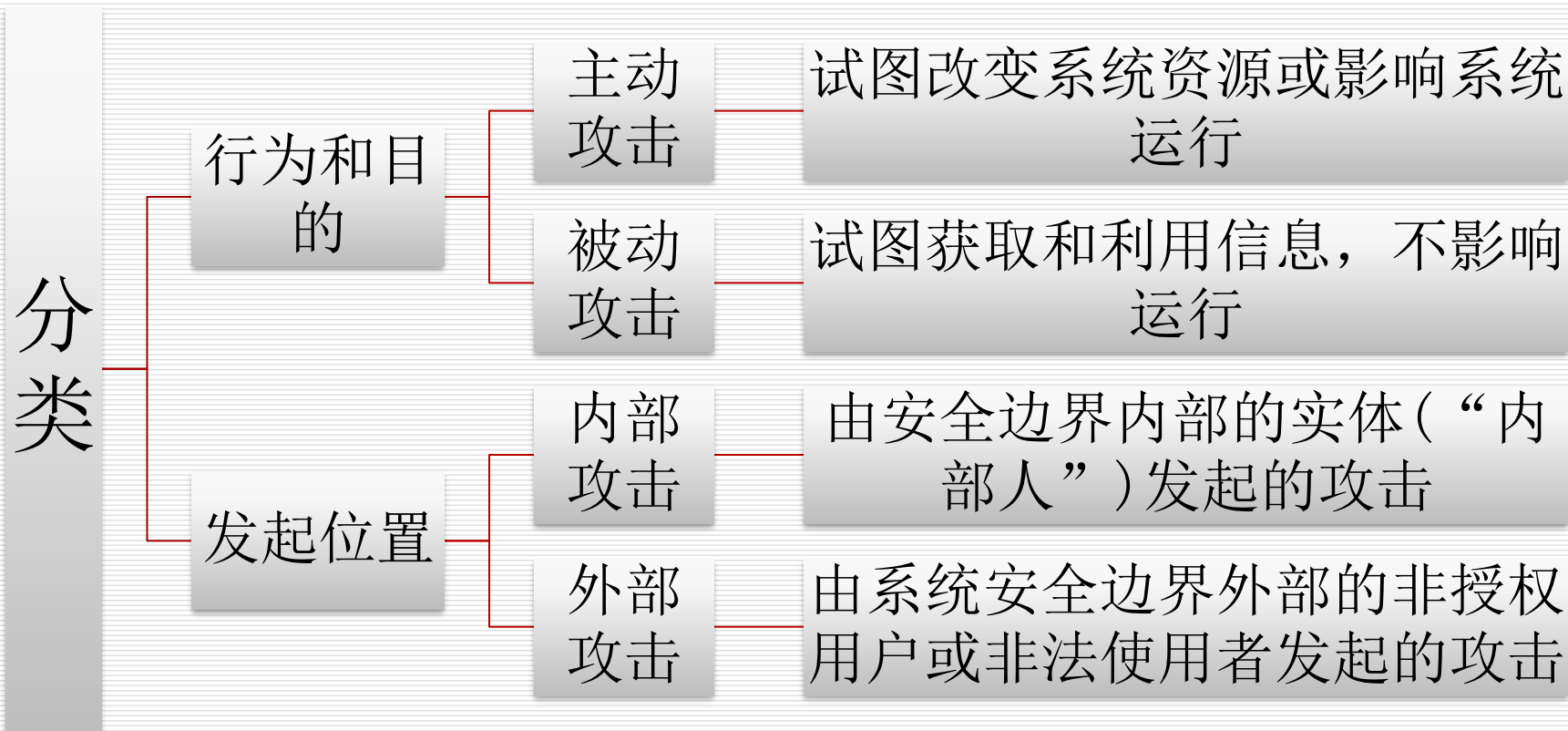
参考资料:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-0151201-wmc>

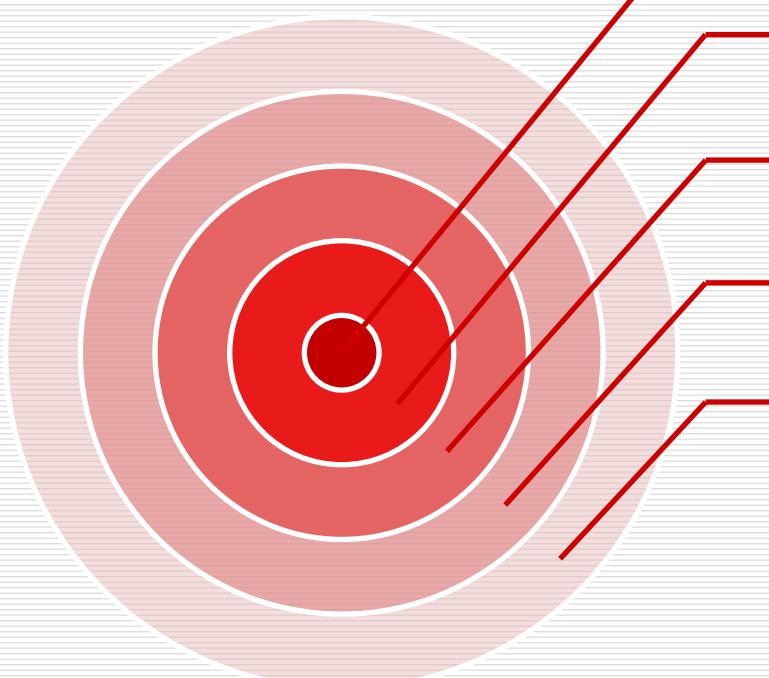
0 day漏洞

- 0 day漏洞，又称零日漏洞，指在安全补丁发布前被了解和掌握的漏洞信息。利用0 day漏洞的攻击称为0 day攻击。
 - 2006年9月27日，微软提前发布MS06-055漏洞补丁，修补了一个严重等级的IE图像处理漏洞。事实上，这个漏洞在当时属于零日漏洞，因为在微软公布补丁之前一个星期就已经出现了利用这个漏洞的网马。
- 谁在使用0 day漏洞：
 - 安全部门、渗透测试人员、黑客、甚至是蠕虫...

攻击



对策



对策：对付攻击所采取的任何手段

阻止攻击：理想情况下，对策能够成功阻止(prevent)特定类型的攻击

检测攻击：在某些情况下，当阻止不可能或失效时，目标就是检测(detect)攻击，并从攻击造成的影响中恢复

引入新脆弱性：对策本身可能会引入新的脆弱性

残余脆弱性：在执行安全对策后，残余的脆弱性可能还存在。这些脆弱性可能被威胁代理利用，表现为资产的残余风险(risk)

内容安排

- 1.1 计算机安全的概念
- 1.2 威胁、攻击和资产
- 1.3 安全功能要求
- 1.4 基本安全设计原则
- 1.5 攻击面和攻击树
- 1.6 计算机安全策略
- 1.7 标准

1.2 威胁、攻击和资产

□ 1.2.1 威胁和攻击

□ 1.2.2 威胁和资产

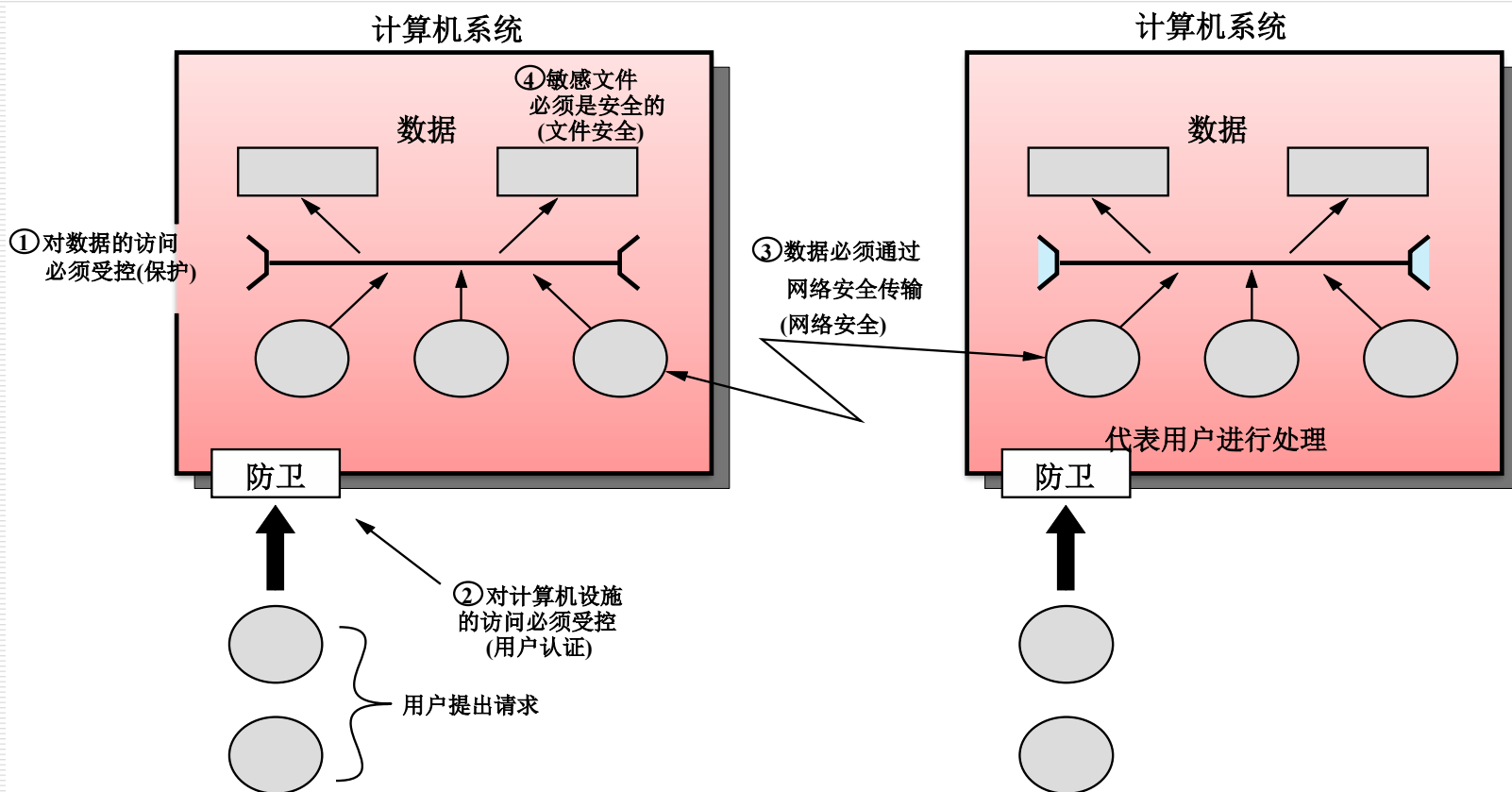
1.2.1 威胁和攻击

图表源自RFC4949，描述了四种威胁后果，并列出了导致每一种后果的攻击类型。

威胁后果	威胁动作（攻击）
非授权泄露 实体未经授权而获得对数据访问的情况或事件	暴露 ：敏感数据被直接泄露给非授权实体 截获 ：非授权实体直接访问在授权的源和目的地之间传输的敏感数据 推理 ：非授权实体通过基于特征的推理或通信产品间接访问敏感数据（但不一定是包含在通信中的数据）的威胁活动 入侵 ：非授权实体通过躲避系统安全保护措施来获得对敏感数据的访问
欺骗 导致授权实体接受虚假数据并相信其正确性的情况或事件	冒充 ：非授权实体通过伪装成授权实体来访问系统或执行恶意行为 伪造 ：以虚假数据欺骗授权实体 抵赖 ：一个实体通过虚伪地否认对行为的责任而欺骗另一个实体
破坏 中断或阻止系统服务和功能正确运行的情况或事件	失能 ：通过禁用系统组件来阻止或中断系统运行 损坏 ：通过对系统功能或数据的不利修改来对系统运行进行非期望的改变 阻碍 ：通过阻止系统运行来中断系统服务交付的威胁活动
篡夺 导致系统服务或功能被非授权实体控制的情况或事件	盗用 ：实体对系统资源采取非授权的逻辑或物理控制 误用 ：导致系统组件执行对系统安全有害的功能或服务

1.2.2 威胁与资产

计算机安全的范围，如下图：



1.2.2 威胁与资产

计算机和网络资产的威胁举例

	可用性	机密性	完整性
硬件	设备被偷盗或者禁用 因而拒绝提供服务。	未加密的USB设备 被盗	
软件	程序被删除， 拒绝用户访问	软件的非授权拷贝	正在运行的程序被 修改，使其在执行 过程中失败或执行 一些非预期的任务
数据	文件被删除， 拒绝用户访问	非授权读取数据。分 析统计数据来揭露潜 在的深层次的数据	修改已有文件或伪 造新文件
通信线路 和网络	消息被破坏或删除。 通信线路或网络不可 用	消息被读取。消息的 流量模式值观察到	消息被修改、延迟、 重新排序或复制。伪 造虚假消息

硬件和软件安全通常由计算中心的专家关注或者由个别PC用户关注

硬件、软件和数据

- **硬件：**对计算机系统硬件的主要威胁是对其**可用性**的威胁。硬件对自动化控制最不敏感。威胁包括意外或蓄意地对设备进行破坏和偷盗。个人计算机和工作站的盛行及计算机网络的广泛使用增加了该领域出现损失的可能性。偷盗USB设备导致机密性受损。需采用物理或管理方面的安全措施来处理这些威胁。
- **软件：**对于软件的主要威胁是对**软件可用性**的攻击。软件,尤其是应用软件通常很容易被删除。软件也可能被修改或被破坏而不能使用。谨慎的软件配置管理能够保持其高可用性。对软件进行修改,使其虽仍能运行,但与以前的行为大不相同,这是对软件**完整性/真实性**的威胁。计算机病毒及相关攻击就归属这一类。最后一个问题是保护软件不被盗版。尽管采取了某些对策,但总的来说软件的非授权拷贝问题还没有根本解决。

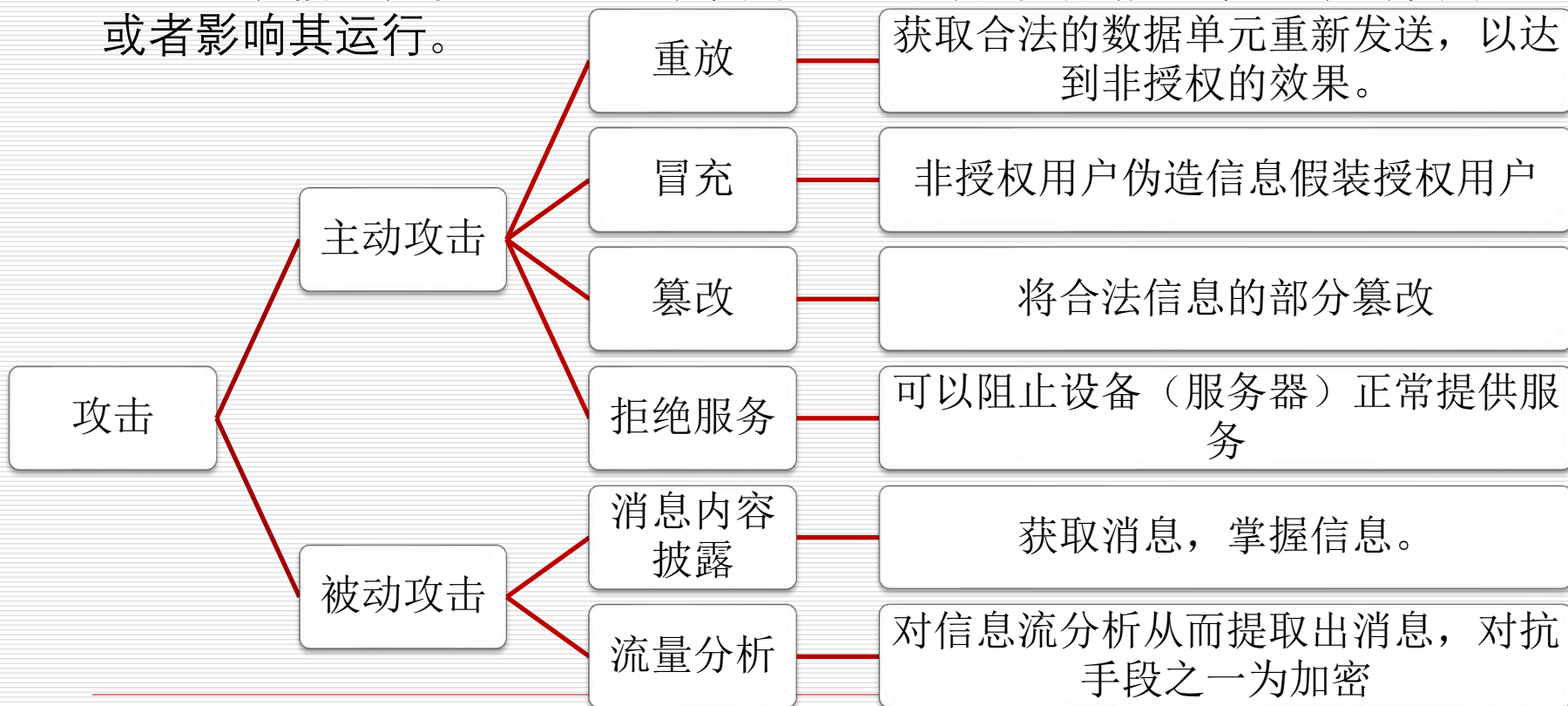
数据安全涉及由个人、团体或商业组织控制的文件或其他形式的数据库

硬件、软件和数据

- **数据：**对于可用性，关心的是**被偶然或恶意破坏的数据文件**。对于保密性的主要威胁**是非授权读取数据文件或数据库**。一种对保密不太明显的威胁是，进行数据分析并在使用提供概括和聚集信息的所谓统计数据库的过程中表现出来的。对于数据完整性，对**数据文件的修改**产生的后果可能很小也可能很严重。

网络安全攻击类型

网络安全攻击可以划分为**被动攻击**和**主动攻击**。被动攻击企图了解或利用系统信息，但不影响系统资源。主动攻击则试图改变系统的资源或者影响其运行。



1.3 安全功能要求

从功能要求角度，对减少脆弱性并处理系统资产威胁的对策进行分类和描述，下表为17个安全相关领域的功能要求，源自FIPS200

访问控制(access control):限制信息系统只能由授权用户或以授权用户名义执行的进程或设备（包括其他信息系统）访问，限制授权用户被允许执行的事务和功能的类型。

意识和培训（awareness and training): (i)确保信息系统的管理者和用户能够意识到与他们的活动相关的安全风险，以及与信息系统安全相关的法律、法规和政策; (ii)确保个人通过充分的培训能够承担与信息安全相关的任务和职责。

审计和可说明性(audit and accountability):(i)最大限度地创建、保护和保留信息系统审计记录，用于监视、分析、调查和报告不合法的、非授权的或不正当的信息系统活动;(ii)确保个别信息系统用户的活动能被唯一追踪，以便他们对自己的行为负责。

认证、信赖和安全评估（certification, accreditation and security assessment): (i)定期评估机构的信息系统的安全控制措施，确定该控制措施在其应用中是否有效;(ii)开发并实施用来纠正机构信息系统的不足、减少或消除其脆弱性的行动计划;(iii)对机构信息系统及相关的信息系统连接的运行授权; (iv)实时监视信息系统的安全控制措施确保控制措施的持续有效性。

配置管理（configuration management):(i)建立和维护贯穿于各个机构信息系统开发生命周期中的基线配置和清单（包括硬件、软件、固件和文档);(ii)建立和执行在机构信息系统中部署的信息技术产品的安全配置。

应急规划（contingency planning):建立、维护和实施针对机构信息系统的应急响应、备份操作和灾后恢复的计划，确保在紧急情况下关键信息资源的可用性和操作的持续性。

识别与认证（identification and authentication):标识信息系统用户、以用户名义进行的进程或设备，认证(或验证)这些用户、进程或设备的身份，以此作为允许访问机构信息系统的先决条件。

事故响应（incident response):建立对机构信息系统的运行事故处理能力，包括充分的准备、检测、分析、遏制、恢复和用户响应活动;(ii)跟踪、记载并将事故报告给适当的组织官员及管理机构。

维护(maintenance): (i)对机构信息系统进行定期、及时的维护;(ii)对实施信息系统维护所用到的工具、技术、机制和人员提供有效的控制。

1.3 安全功能要求

续表

介质保护(media protection):(i)保护信息系统纸质和数字的介质;(ii)限制授权用户访问信息系统介质上的信息;(iii)在销毁或放弃再次使用之前,清除或破坏信息系统介质。

物理和环境保护(physical and environmental protection):(i)限制授权个体对信息系统、设备和各自操作环境的物理访问;(ii)保护信息系统的物理厂房和支持基础设施;(iii) 提供对信系统的支持设施;(iv) 保护信息系统免受环境危害;(v)对包含信息系统的场所提供适当的环境控制措施。

规划(planning):开发、文档记录、定期更新和实施机构的安全计划,其中描述了信息系统中适当的或者规划中的安全控制措施以及个人访问信息系统的行为规则。

人员安全(personnel security): (i)确保机构 (包括第三方服务提供者)中处于责任岗位的个人是可信赖的并满足已建立的该岗位的安全准则。(ii)保证在职工离职和调动等人事活动前后,机构信息和信息系统是受保护的;(iii)对职工不能遵守机构的安全策略和程序的,制定正式的制裁方法。

风险评估 (risk assessment): 定期评估机构运行(包括任务, 职能、形象或声誉)、机构资产和个体的风险,这根据机构信息系统的运行及相关的机构信息的处理、存储或传输得出。

系统和服务获取(system and service acquisition):(i)分配足够的资源来充分保护机构信息系统;(ii)在系统开发生命周期中考虑信息安全问题;(iii)使用软件用法和安装限制;(iv)确保第三方提供充分的安全措施来保护机构外包的信息、应用或服务。

系统和通信保护(system and communication protection): (i)在信息系统的外边界和关键内边界上监视、控制和保护机构通信 (即机构信息系统的信息传输或接收);(ii)利用架构设计、软件开发技术和系统工程原理来提高机构信息系统的信息安全的有效性。

系统和信息完整性(system and information integrity): (i)及时地识别、报告和纠正信息和信息系统的缺陷;(ii)在机构信息系统的适当位置提供恶意代码防护;(iii) 监视信息系统安全报警和警告,并采取适当的行动作为响应。

1.4 基本安全设计原则

- ❑ 经济机制(economy of mechanism)原则
- ❑ 安全缺省设置(fail-safe default)原则
- ❑ 绝对中介(complete mediation) 原则
- ❑ 开放式设计(open design)原则
- ❑ 特权分离(separation of privilege)原则
- ❑ 最小特权(least privilege)原则
- ❑ 最小共用机制(least common mechanism)原则
- ❑ 心理可接受性(psychological acceptability)原则
- ❑ 隔离(isolation)原则
- ❑ 封装(encapsulation)原则
- ❑ 模块化(modularity)原则
- ❑ 分层(layering)原则
- ❑ 最小惊动(least astonishment) 原则

1.4 基本安全设计原则

经济机制 (economy of mechanism)原则

- 指嵌入在硬件和软件中的安全机制的设计要尽可能简单、短小，简单、短小的设计更易于进行彻底的测试和验证。
- 在实践中，这可能是最难遵守的原则。

安全缺省设置 (fail-safe default) 原则：

- 指访问控制应当基于许可而不是排除
- 只要没有授权的信息就不允许访问
- 不能出现本该允许的请求被拒绝与本该拒绝的请求被允许

绝对中介 (complete mediation) 原则：

- 指每一次访问都应当依据访问控制机制进行检查
- 如果访问命令被提示是将来使用它，那么如何改变优先级顺序的详细说明被传递给本地存储器

开放式设计(open design)原则：

- 指安全机制的设计应当开放而非保密
- 开放设计有助于安全机制接受广泛的审查

前八项原则最早被列入文献[SALT75], 并经历了时间的考验

1.4 基本安全设计原则

特权分离 (separation of privilege)原则

- 为对于限定资源的访问需要多特权属性的情况定义的
- 细分特权, 分配给多个主体, 减少每个特权拥有者的权利

最小特权(least privilege)原则

- 指每个进程和系统用户都应当使用完成某项任务必需的最少特权集进行操作
- 最小权限原则具有暂时性

最小共用机制 (least common mechanism)原则

- 指在设计时应当最小化不同用户共享的功能, 以提高彼此的安全性

心理可接受性 (psychological acceptability)原则

- 指安全机制不应该过度干涉用户的工作, 同时也要满足用户授权访问的要求

1.5 攻击面和攻击树

- 攻击面是由系统中可到达的和可被利用的脆弱点构成的。
- 攻击树是一个分支型的、层次化的数据结构，表示了一系列潜在技术，这些技术可利用安全漏洞进行攻击。

攻击面例子



攻击面分类

网络攻击面

- 网络攻击面指企业网、广域网或者因特网中的脆弱点，包括网络协议中的脆弱点，例如利用这些脆弱点进行拒绝服务攻击、通信线路破坏和各种不同形式的入侵攻击。

人为攻击面

- 人为攻击面指员工或者外部人员(如社会工程学、人为错误和受信任的内部人员)引起的脆弱点。

软件攻击面

- 软件攻击面是指应用程序、实用程序或操作系统代码中的漏洞，尤其是指**Web**服务器软件中的漏洞。

深度防御和攻击面

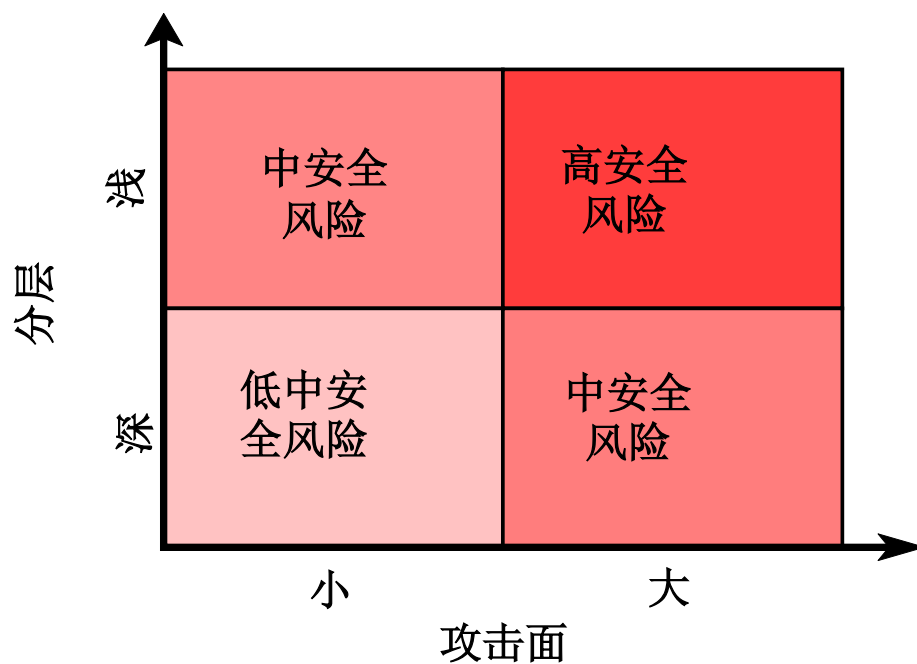


图 1.4 深度防御和攻击面

攻击树

- ❑ 根节点：攻击的主要目标，即造成安全事件。
- ❑ 子节点：具体的攻击手段或方法，可以进一步细分为更具体的子目标。
- ❑ 叶子节点：具体的攻击方式。
- ❑ 与节点 (**AND-node**)：所有子目标都必须完成以实现该节点的目标。
- ❑ 或节点 (**OR-node**)：只需要完成一个子目标即可实现该节点的目标。
- ❑ 每条分支可以赋予特定的值来表示攻击的难度、成本等属性。

案例-网银认证的攻击树



补充：黑客攻击

- 黑客（**hacker**），源于英语动词**hack**，意为“劈，砍”，引申为“干了一件非常漂亮的工作”。在早期麻省理工学院的校园俚语中，“黑客”则有“恶作剧”之意，尤指手法巧妙、技术高明的恶作剧。
- 他们通常具有硬件和软件的高级知识，并有能力通过创新的方法剖析系统。

黑客起源

□ 起源地：

- 美国

□ 精神支柱：

- 对技术的渴求
- 对自由的渴求

□ 历史背景：

- 越战与反战活动
- 马丁·路德金与自由
- 嬉皮士与非主流文化
- 电话飞客与计算机革命

□ 中国黑客发展历史

- 1998年印尼事件
- 1999年南联盟事件
- 绿色兵团南北分拆事件
- 中美五一黑客大战事件
-

黑客攻击

- ❑ 黑客基本涵义是指一个拥有熟练电脑技术的人，但大部分的媒体习惯将“黑客”指作电脑侵入者。
- ❑ 白帽黑客有能力破坏电脑安全，但不具恶意目的的黑客。白帽子一般有清楚的定义道德规范，并常常试图同企业合作去改善被发现的安全弱点。
- ❑ 灰帽黑客对于伦理和法律暧昧不清的黑客。
- ❑ 黑帽黑客骇客（“Cracker”的音译，“破解者”意思）：经常使用于区分黑帽子黑客和一般（正面的）有理性的黑客，这个词自1983年开始流行。
- ❑ 在中国，人们经常把黑客跟骇客搞混，实际区别很大。

黑客分类



白帽子创新者

- 设计新系统
- 打破常规
- 精研技术
- 勇于创新

没有最好,

只有更好

MS -Bill Gates
GNU -R.Stallman
Linux -Linus

灰帽子破解者

- 破解已有系统
- 发现问题/漏洞
- 突破极限/禁制
- 展现自我

计算机

为人民服务

漏洞发现 - Flashsky
软件破解 - 0 Day
工具提供 - Glacier

黑帽子破坏者

- 随意使用资源
- 恶意破坏
- 散播蠕虫病毒
- 商业间谍

人不为己,

天诛地灭

入侵者 -K.米特尼克
CIH -陈盈豪
攻击Yahoo -匿名

著名黑客

- Kevin Mitnick: 凯文·米特尼克，1964年美国洛杉矶出生，被称为世界上“头号电脑骇客”。
- Robert Tappan Morrisgeek: 美国历史上五大最著名的黑客之一。Morris的父亲是前美国国家安全局的一名科学家，叫做Robert Morris。Robert是Morris蠕虫病毒的创造者，也是首个通过互联网传播的蠕虫病毒。因此，他成为了首个被以1986年电脑欺骗和滥用法案起诉的人。



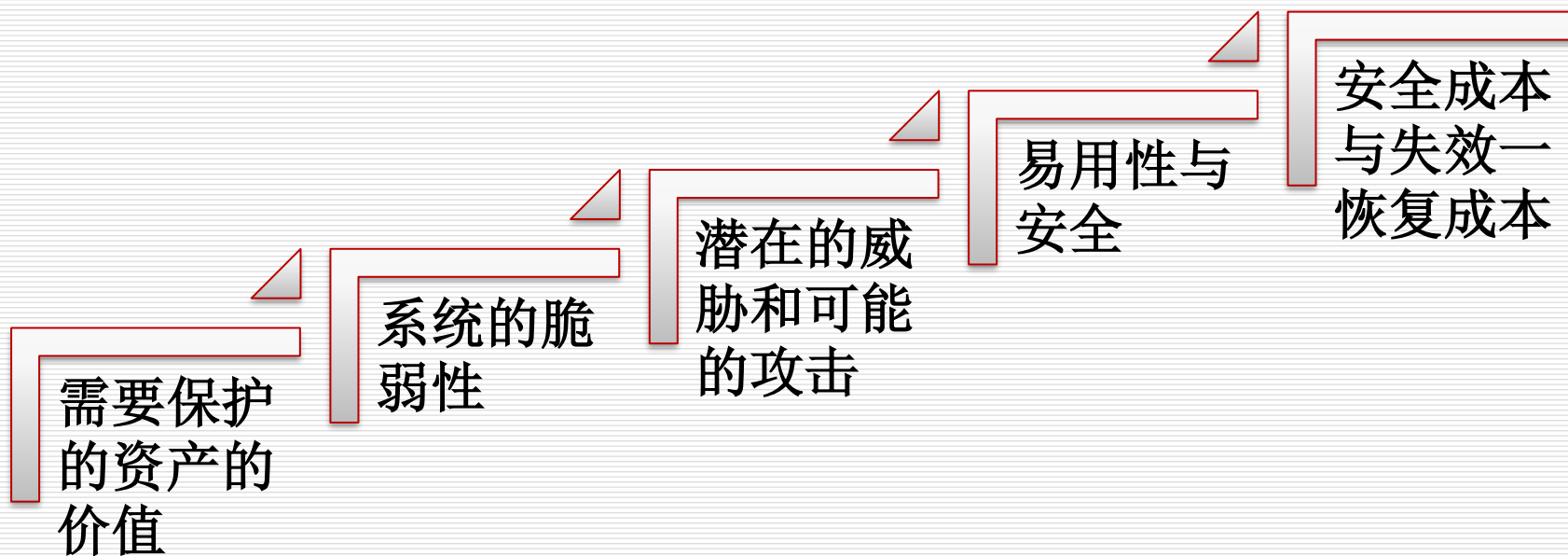
Robert Tappan Morrisgeek.

黑客攻击汽车视频演示

1.6 计算机安全策略

- ❑ 规范/策略(specification policy):安全方案应该要实现什么?
- ❑ 实施/机制(implementation/mechanism):安全策略是如何实现的?
- ❑ 正确性/保证(correctness/assurance):安全策略是否确实起作用了?

安全策略



安全实施



保证和评估

保证(assurance)是信息系统的一个属性，它为系统的运行提供了可靠的依据，从而实现了系统的安全策略。这包括系统设计和系统实现。

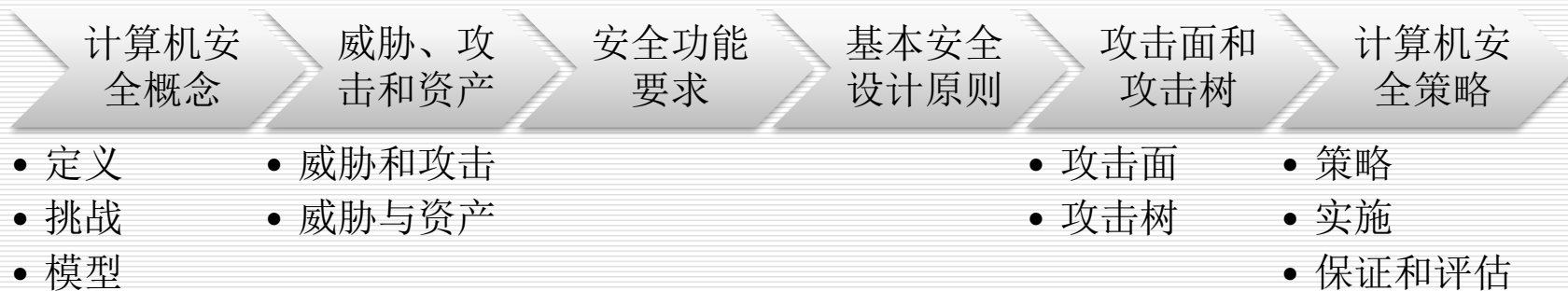
评估(evaluation)是依据某准则检查计算机产品或系统的过程。评估包括测试，可能还包括形式化分析或数学技术。该领域的中心工作是开发能够应用到任何安全系统(包括安全服务和机制)并对产品比较提供广泛支持的评估准则。

1.7 标准

本书中所描述的许多安全技术和应用已被指定为标准。一些最重要(截止到当前的版本)的组织如下:

- ❑ **美国国家标准与技术研究所(National Institute of Standard and Technology, NIST):** NIST是美国联邦政府的一个机构, 负责制定美国政府使用的度量科学、标准和技术, 也负责推动美国私营企业的创新。
- ❑ **Internet 协会(Internet Society):** ISOC 是一个专业的成员联盟, 其拥有世界性的组织成员和个人成员。在诸如 Internet的未来等前沿问题上, 它处于领导者的地位。同时, 它也是制定各种Internet 基础设施标准组织的管理机构。
- ❑ **ITU电信标准化部门(ITU-T):** Internet电子通信联盟(Internet Telecommunication Union, ITU) 是联合国系统中的一个国际性组织, 各国政府和私营企业在它的领导下一起协调全球的电子通信网络和服务。ITU 电信标准化部门是ITU的三大部门之一。ITU-T的任务是制定覆盖所有电子通信领域的标准。ITU-T 的标准被称为推荐标准(Recommendation)。
- ❑ **国际标准化组织:**国际标准化组织(ISO)是一个由全球140多个国家的国家标准组织参加的世界联盟。ISO 是一个非政府组织, 它负责推动标准化的发展, 促进国际商品和服务交换, 发展全球在智力、科学、技术和经济活动方面的合作。ISO 的工作促使国际协议变成国际标准。

总结



谢谢各位!