


# 第 9 章 网络安全

---

## 本章讨论的主要问题是：

1. 什么是网络安全？常见的网络安全问题有哪些？
  2. 为了达到保护信息的目的，可以将信息进行加密，什么是信息加密？具体加密过程是怎样？
  3. 计算机系统的安全性常常取决于系统能否正确识别用户的身份，计算机系统如何对用户的身份进行确认和鉴别？
  4. 如何将安全问题阻挡在网络之外？如何检测网络系统是否被入侵？
  5. 计算机职业道德的基本要求是什么？我国用什么方式对软件实施法律保护？
- 

# 情景问题——互联网时代还有个人隐私吗？

---

毫不夸张地说，计算机已经威胁到我们的隐私，在我们不知道也不愿意的情况下，企业和政府机构的数据库收集和共享大量关于我们的个人信息，互联网检测软件可能记下了我们在网上的活动，黑客可能窃取了我们的帐号和密码，邮件传输系统可能阅读了我们的电子邮件，购物软件正在统计我们的购物习惯.....

# 第9章 网络安全——什么是网络安全

---

## 网络安全的定义

- ▶ **网络安全**是指为保护网络不受任何损害而采取的所有措施的综合，一般包含网络的**保密性、完整性和可用性**。
- ▶ 保密性是指网络能够阻止未经授权的用户读取保密信息；
- ▶ 完整性包括**资料的完整性和软件的完整性**，资料的完整性是指在未经许可的情况下，确保资料不被删除或修改，软件的完整性是指确保软件程序不会被误操作、怀有恶意的人或病毒修改；
- ▶ 可用性是指网络在遭受攻击时确保得到授权的用户可以使用网络资源。

# 第9章 网络安全——什么是网络安全

## 网络与信息安全技术的重要性

### ➤ 是确保国家和社会稳定的重要因素

互联网技术已经应用到社会的各个领域，国家和社会稳定与网络安全息息相关。

### ➤ 提高用户安全意识

一些公司对用户不加以重视，也造成了用户个人信息外漏的现象。种种问题的出现，促使用户在使用电脑的过程中加强了对网络个人信息安全的重视。

### ➤ 经济领域中互联网技术的广泛应用

我国的互联网使用人数早在几年前就居于世界互联网使用人数的首位，而且其使用范围逐渐集中于商业性的应用。故创造一个安全的网络信息使用环境具有十分必要的意义。

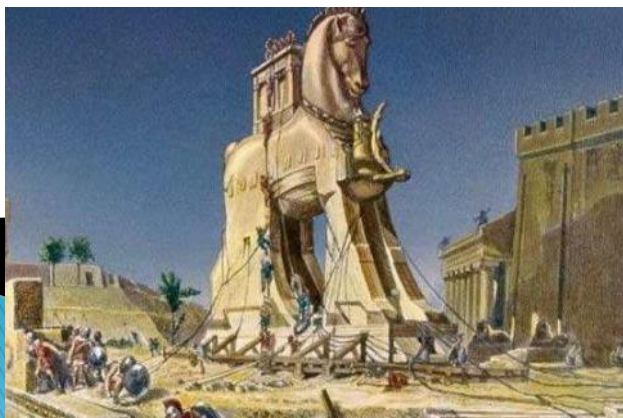
### ➤ 网络发展本身的需要

网络在给其它应用与通信提供服务的过程中，要保证信息传输的安全性和保密性，这是网络与信息技术自身应具有特性，否则网络将无法提供可靠可信的报务。

# 第9章 网络安全——什么是网络安全

## 常见的网络安全问题

1. 病毒。**计算机病毒**是一种人为蓄意制造的、以破坏为目的的程序，它寄生于其他应用程序或系统的可执行部分，通过部分修改或移动程序，将自我复制加入其中或占据宿主程序的部分而隐藏起来，在一定条件下发作，破坏计算机系统。
2. 木马。**木马**（全称为特洛伊木马）是在执行某种功能的同时进行秘密破坏的一种程序。木马可以完成非授权用户无法完成的功能，也可以破坏大量数据。



# 第9章 网络安全——什么是网络安全

---

## 常见的网络安全问题

3. 黑客。黑客是指通过网络非法进入他人系统，截获或篡改计算机数据，危害信息安全的计算机入侵者或入侵行为。

4. 系统的漏洞和后门。操作系统和网络软件不可能完全没有缺陷和漏洞，TCP/IP协议中也可能有被攻击者利用的漏洞，软件的后门通常是软件公司编程人员为了自便而设置的。

5. 内部威胁和无意破坏。事实上，大多数威胁来自企业内部人员的蓄意攻击，大部分计算机罪犯是那些能够进入计算机系统的职员。此外，一些无意失误，如丢失密码、疏忽大意和非法操作等都可能对网络造成极大的破坏。

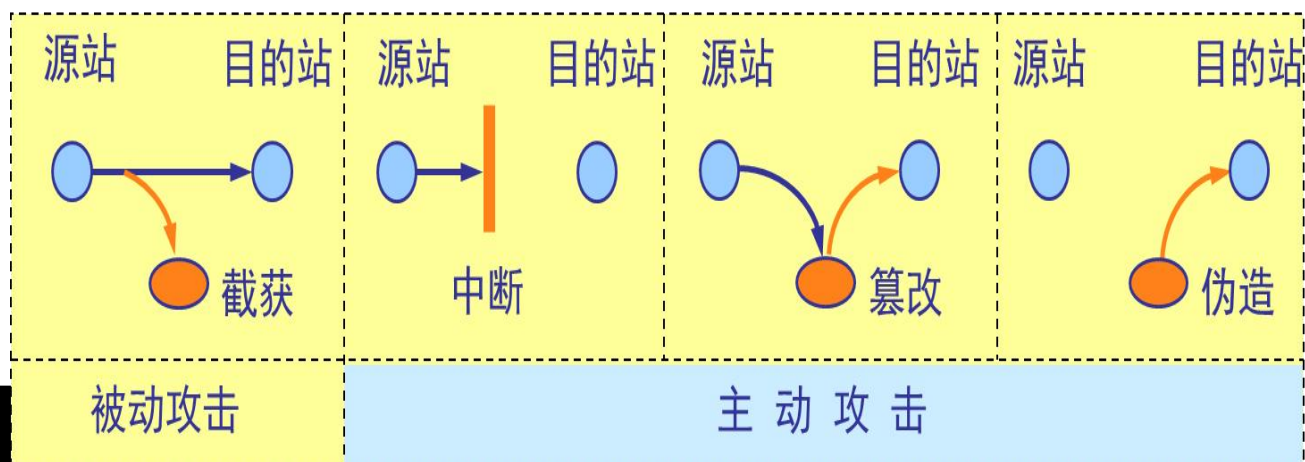


# 第9章 网络安全——什么是网络安全

## 计算机网络面临的威胁：

主动攻击：对信息的修改、删除、伪造、添加、重放、冒充和病毒入侵等；

被动攻击：对信息的侦听、截获、窃取、破译和业务流量分析、电磁信息提取等。



# 第9章 网络安全——什么是网络安全

## 信息安全的目标

- **机密性**：保证信息不被非授权访问，即使非授权用户得到信息也无法知晓信息的内容，因而不能使用。【加密】
- **完整性**：维护信息的一致性，即在信息生成、传输、存储和使用过程中不应发生人为或非人为的**非授权篡改**。【数字水印】
- **可用性**：授权用户需要时能不受其他因素的影响，方便地使用所需信息。【杀毒软件和防火墙】
- **可控性**：信息在整个生命周期内都可由合法拥有者加以安全的控制。【身份认证】
- **不可抵赖性**：用户无法在事后否认曾经对信息进行的生成、签发、接收等行为。【数字签名】



# 第9章 网络安全——信息加密

## 什么是信息加密

- ▶ **加密**：使用数学方法来重新组织数据，使得除了合法的接受者之外，其他任何人都不能恢复原先的信息。
- ▶ **明文**：加密前的信息；**密文**：加密后的信息称为。
- ▶ **加密**是将明文变成密文的过程，**解密**是将密文变成明文的过程。
- ▶ 信息为了有效地控制加密和解密过程的实现，在处理过程中要有通信双方掌握的专门信息的参与，这种专门的信息称为**密钥**。

¥@\*&DE%\$~



小明是内鬼!

# 第9章 网络安全——信息加密

---


## 密码编制-加密

- 密码编制学是对消息进行编码以隐藏明文消息的一门学问。替代和置换是古典密码中常用的变换形式。
- 替代密码
  - 构造密文字母表，然后用密文字母表中的字母或字母组来替代明文字母或字母组，各个字母或字母组的相对位置不变，但其本身改变了。
  - 包括：单表替代密码、多表替代密码和多字母替代密码。
- 置换密码
  - 将明文中的字母重新排列，字母表示不变，但其位置改变

# 第9章 网络安全——信息加密

---

## 密码分析-解密

- 密码分析学就是研究密码破译的科学。如果能够根据密文系统确定出明文或密钥，或者能够根据明文密文对系统确定出密钥，则称这个密码系统是可破译的。
  - 穷举攻击
  - 统计分析攻击
  - 数学分析攻击
- 

# 第9章 网络安全——信息加密

## 对称加密

- ▶ 在对称加密中，信息的**加密和解密使用同一密钥**。
- ▶ 优点：安全性高、加密速度快。
- ▶ 缺点：管理的密钥多；密钥的传递存在风险。
- ▶ 常用的对称加密算法有DES和IDEA。



# 第9章 网络安全——信息加密

---

## 对称加密

### 1) 替换加密:

例如，使用替换算法的Caesar 密码，采用的是 **Character+N** 的算法，假设明文为ATTACK  
BEGIN AT FIVE，采用 $N=2$  的替换算法，即A  
用其ASCII 码值加2 的字符来替代，字母Y 和Z  
分别用字母A 和B 来替代。得到密文为  
CVVCEMDGIKPCVHKXV。这种替换加密方法简  
便，实现容易但安全性较低。

## 2) 换位加密:

换位加密就是通过一定的规律改变字母的排列顺序。现假设密钥为WATCH, 明文为THE SPY IS JAMES LI (加密时需要去除明文中的空格, 故明文为THESPYISJAMESLI)。在英文26个字母中找出密钥WATCH这5个字母, 按其在字母表中的先后顺序加上编号1~5, 如下图。

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1		2					3												4			5			

图 密钥字母相对顺序

从左到右、从上到下按行填入明文。请注意, 到现在为止, 密钥起作用只是确定了明文每行是5个字母。按照密钥给出的字母顺序, 按列读出, 如右图中标出的顺序。第一次读出HIE, 第二次读出SJL, 第三次读出PAI, 第四次读出ESS, 第五次读出TYM。将所有读出的结果连起来, 得出密文为: HIESJLPAIESSTYM。

密钥	W	A	T	C	H
顺序	5	1	4	2	3
明文	T	H	E	S	P
	Y	I	S	J	A
	M	E	S	L	I



# 第9章 网络安全——信息加密

## 非对称加密

- ▶ 在非对称加密中，信息的**加密和解密使用不同密钥**，参与加密过程的密钥公开，称为**公钥**，参与解密过程的密钥为用户专用，称为**私钥**，两个密钥必须配对使用。
- ▶ 常用的非对称加密算法有RSA、背包算法等。

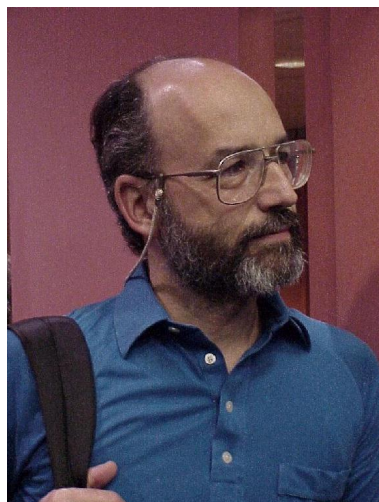


# 第9章 网络安全——信息加密

## 非对称加密



Rivest



Shamir



Adleman

理论基础：将一个由两个大质数的乘积分解回来是个难解问题

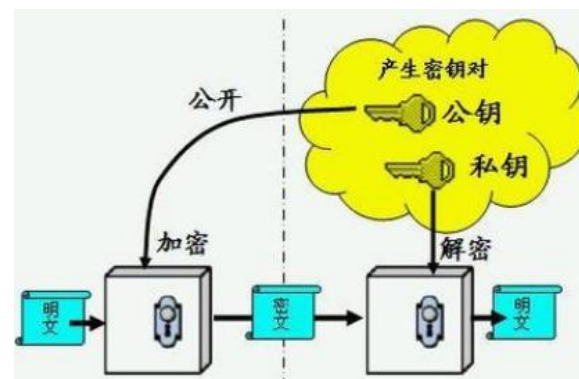
# DES加密算法

DES加密算法是一种分组密码，以64位为分组对数据加密，它的密钥长度是56位，加密解密用同一算法。DES加密算法是对密钥进行保密，而公开算法，包括加密和解密算法。

# RSA加密算法

RSA加密算法是目前最有影响力的**公钥加密算法**，并且被普遍认为是目前最优秀的公钥方案之一。**RSA**是第一个能同时用于加密和数字签名的算法，它能够抵抗到目前为止已知的所有密码攻击，已被**ISO**推荐为公钥数据加密标准。**RSA**加密算法基于一个十分简单的数论事实：将两个大素数相乘十分容易，但是想要对其乘积进行因式分解却极其困难，因此可以将乘积公开作为加密密钥。

其它还有Base64加密，MD5加密，SHA1加密等



# 第9章 网络安全——数字认证

---

## 身份认证

- ▶ **身份认证**是一种使合法用户能够证明自己身份的方法，是计算机系统安全保密防范最基本的措施。
- ▶ 主要的身份认证技术有以下三种：
  - (1) **口令验证**。口令验证是常用的一种身份认证手段，使用口令验证的最大问题就是口令泄露。
  - (2) **身份标识**。身份标识是用户携带用来进行身份认证的物理设备，例如磁卡，IC卡。
  - (3) **生物特征标识**。人类的某些生物特征具有很高的个体性和防伪造性，如指纹、视网膜、耳廓等，世界上几乎没有任何两个人是一样的，因而这种验证方法的可靠性和准

# 第9章 网络安全——数字认证

---

## 数字签名

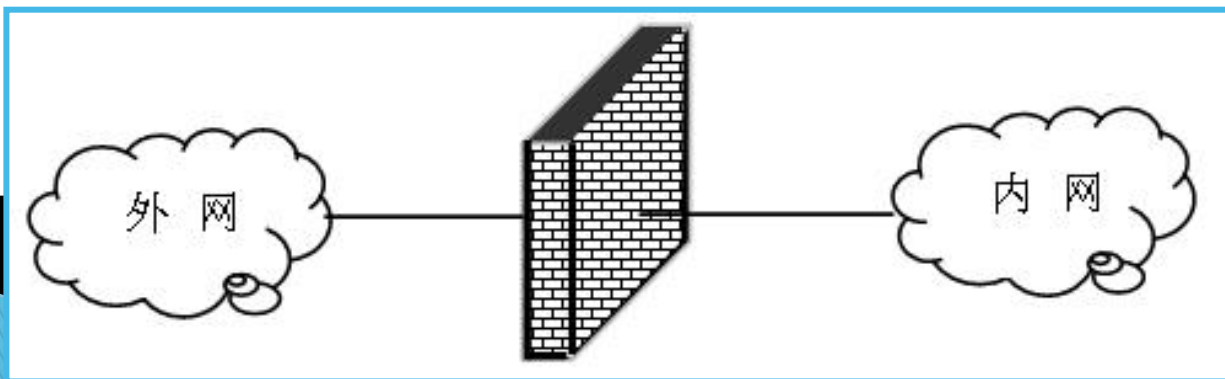
- ▶ 手写签名有两个作用：一是自己的**签名难以否认**，从而确定已签署这一事实；二是因为**签名不易伪造**，从而确定了事务是真实的这一事实。
- ▶ **数字签名**与日常生活中的手写签名效果一样，它不但能使信息接收者确认信息是否来自合法方，而且可以为仲裁者提供信息发送者对信息签名的证据。
- ▶ 数字签名主要通过加密算法和证实协议实现。



# 第9章 网络安全——网络检测与防范

## 防火墙

- ▶ **防火墙**是一种用来加强网络之间访问控制的特殊网络互联设备，它对网络之间传输的数据包和链接方式按照一定的安全策略进行检查，以此决定网络之间的通信是否被允许。
- ▶ 防火墙的功能主要有两个：阻止和允许。**阻止**就是阻止某种类型的通信量通过防火墙，**允许**的功能与阻止的功能正好相反。





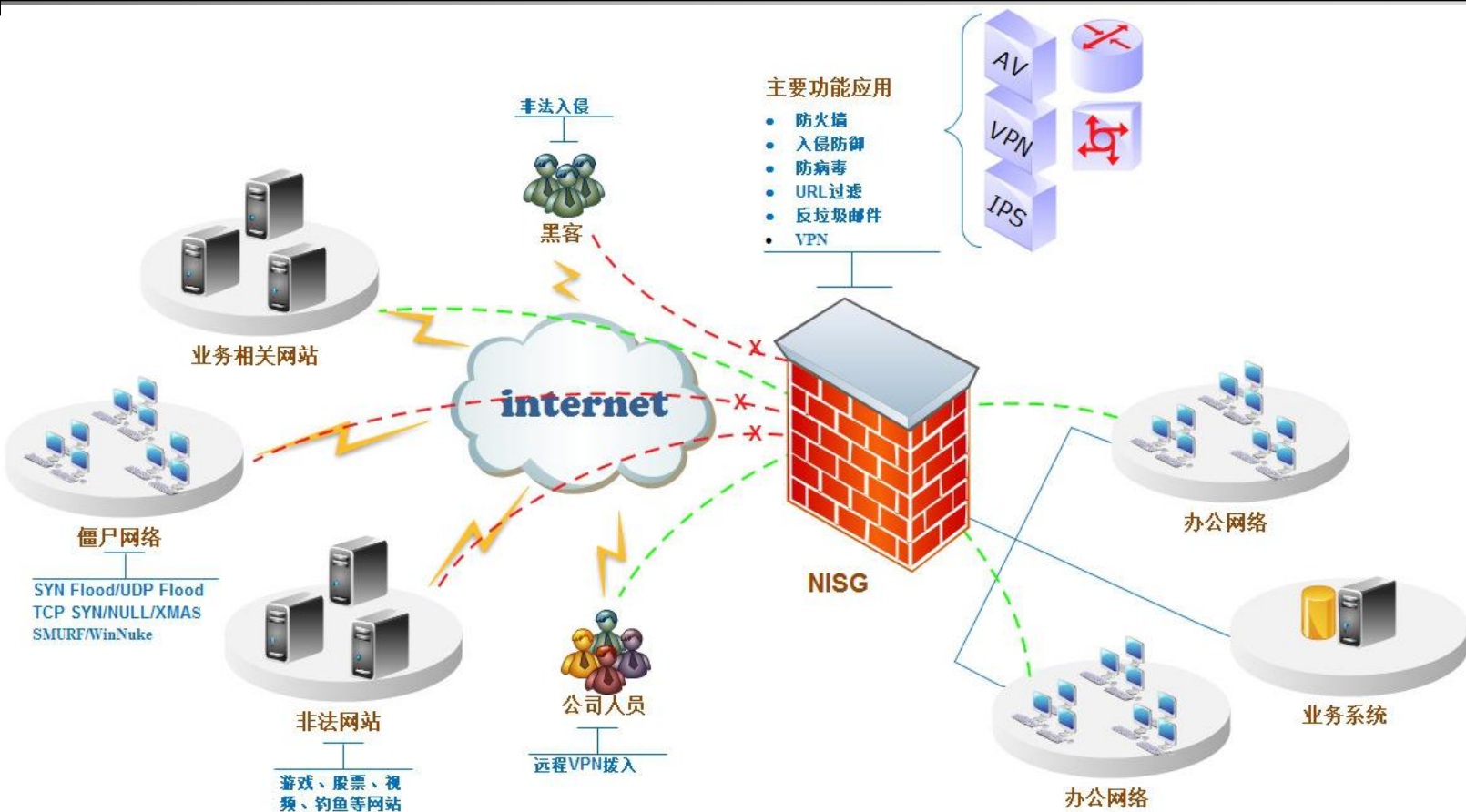
# 第9章 网络安全——网络检测与防范

---

## 防火墙的工作原理

- ▶如果外网的用户要访问内网的WWW服务器，首先由**分组过滤路由器**来判断外网用户的IP地址是不是内网所禁止使用的。
- ▶如果是禁止进入节点的IP地址，则分组过滤路由器将会丢弃该IP包；
- ▶如果不是禁止进入节点的IP地址，则这个IP包被送到应用网关，由应用网关来判断发出这个IP包的用户是不是合法用户。
- ▶如果该用户是合法用户，该IP包被送到内网的WWW服务器去处理；如果该用户不是合法用户，则该IP包将会被应用网关丢弃。

# 第9章 网络安全——网络检测与防范



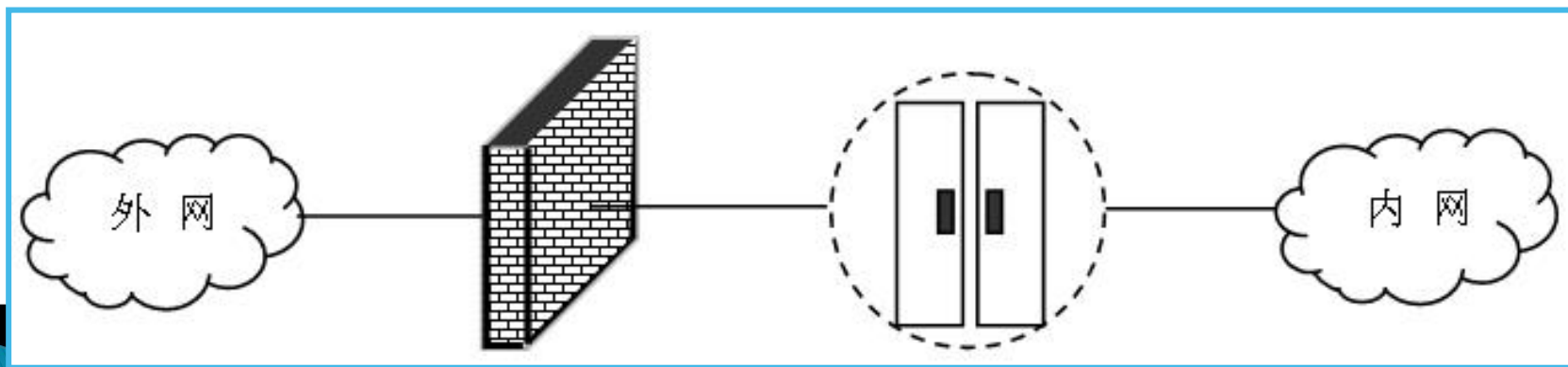
## 缺点

防火墙不能防病毒  
数据更新延迟  
防火墙滤波降低网络性能

# 第9章 网络安全——网络检测与防范

## 入侵检测

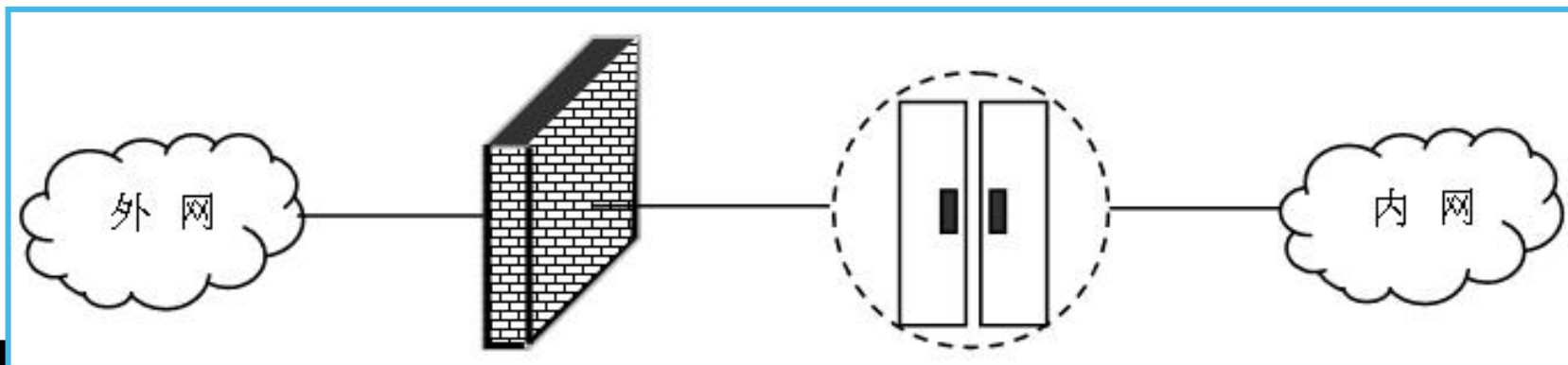
- ▶ **入侵检测**是指主动地从计算机网络系统中的若干关键点收集信息并分析这些信息，确定网络中是否有违反安全策略的行为和受到攻击的迹象，并有针对性地进行防范。
- ▶ 入侵检测被设置在防火墙的后面，它的作用是**发现那些已经穿过防火墙进入到内网或是内部的黑客**。



# 第9章 网络安全——网络检测与防范

## 入侵检测

- 入侵检测技术主要基于特征检测和异常检测。**特征检测**按照预先模式搜寻与已知特征相悖的事件，**异常检测**是将正常用户的行为特征轮廓与实际用户进行比较，并标识出正常和异常的偏离。



# 第9章 网络安全--计算机病毒与计算机犯罪

---

随着计算机应用的普及，日益严重的计算机病毒和计算机犯罪速度猛增，对计算机系统与应用的安全构成了严重的威胁。研究计算机病毒防治，防范计算机犯罪，对维护计算机的安全有着重要意义。

## 计算机病毒

是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。

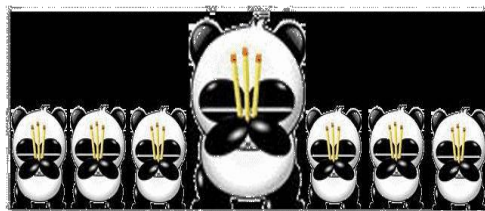


# 第9章 网络安全--计算机病毒与计算机犯罪

计算机病毒具有以下几个特征：

- 1.破坏性
- 2.隐蔽性
- 3.传染性
- 4.潜伏性
- 5.非授权可执行性

警告：你的电脑中毒了



贴图  
T2MOP.COM





# 第9章 网络安全--计算机病毒与计算机犯罪

## 计算机病毒的预防

- 不使用来历不明的程序或软件；
- 在使用移动存储设备之前应先杀毒
- 安装防火墙，防止网络上的病毒入侵
- 安装最新的杀毒软件，并定期升级，实时监控；
- 养成良好的电脑使用习惯，定期优化、整理磁盘，养成定期全面杀毒的习惯；
- 对于重要的数据信息要经常备份，以便在机器遭到破坏后能及时得到恢复。



# 第9章 网络安全--计算机病毒与计算机犯罪

## 黑客

黑客(hacker)一般是指那些未经过管理员授权或者利用系统漏洞等方式进入计算机系统的非法入侵者。他们可以查看我们的资料，窃取我们的信息，偷窥我们的隐私，破坏我们的数据，甚至获取计算机系统的最高控制权，将我们使用的计算机变成他们的傀儡，成为破坏活动的帮凶。



参与1998、1999、2000、2001中美黑客大战



中国红客联盟至今为外界所知的时事大型反击战有如下8次：反击印尼网络、反击中国台湾网络、反击日本网络3次、反击美国网络2次、对韩网站1次。

# 第9章 网络安全--计算机病毒与计算机犯罪

## 黑客攻击案例

### 1. 一台笔记本的威力

美国军方的计算机网络曾经被一种叫做“Agent.btz”的蠕虫病毒入侵过，这个病毒地址来自阿富汗境内的一台笔记本电脑上，通过优盘传播而成功黑进了北美中央司令部。“Agent.btz”盗取了大量美国政府和国防部的机密资料并把这些秘密文件传送到了一个未知的“神秘人”那里。当时的美国国防部完全对付不了这个病毒，在启动了紧急网络攻击警报后，网军使用内部网络隔离、删除恶意代码等方式全部无效。因为“Agent.btz”可以通过检索数据来自建后门把自己复制到其他的网络里隐藏起来，并且它还可以突变，不断更新自身的代码来让自己“隐形”！“Agent.btz”在自我修复完成后隐藏了起来，过了一年半又开始窃取秘密文件。这让美国军方头疼不已！最后逼得没办法了，美国军方把核心部分的计算机全部离线、断电、物理格式化重装系统并且把几乎所有内部流通的U盘全部销毁，才勉强干掉了这只病毒！

# 第9章 网络安全--计算机病毒与计算机犯罪

## 2. 伊朗核电厂的超级病毒

病毒不只是能干窃取信息的事情，它也能像电影里描述的那样直接控制电子设备！2010年6月，一种被称为“**Stuxnet**”的电脑病毒在多个国家的化学工厂、发电厂以及交管系统里被发现，但是在发现它的时候，它看起来没有任何危险，就像是没什么用的僵尸病毒一样。果然，对于许多感染了该病毒的工厂来说它确实没什么危险，那是因为它只在某个特定的地点才起作用。沉寂许久之后意料之外的事情发生了，“**Stuxnet**”病毒在伊朗的一处铀浓缩设施内的离心机上被自动激活，它的目标只有一个，就是控制伊朗的核设施。

伊朗方面对这个病毒也是束手无措，最终在该病毒控制了三分之一核设施内的计算机后，伊朗被迫暂时关闭了他们的核设施和核电厂。

# 第9章 网络安全--计算机病毒与计算机犯罪

## 3. 雅虎30亿邮箱信息泄露

雅虎是一个大家都非常熟悉的互联网企业，在2016年9月份，雅虎公司宣布2013年8月黑客盗走其至少5亿用户的账户信息，同年12月份又表示被盗账户数量约10亿个。随后又在2017年，雅虎公司正式，其所有30亿个用户账号都受到了黑客攻击。被盗信息内容包括用户名、邮箱地址、电话号码、生日以及部分用户加密或者未加密的问题和答案。雅虎和调查方曾表示，“得到国家资助的黑客”发动了这次攻击，不过却没有明确指出具体是哪个国家。

### 电脑病毒

问题1：棱镜门事件是怎么发生的？  
问题2：为什么感觉现在的电脑病毒没有那么多？



斯诺登



# 第9章 网络安全--计算机病毒与计算机犯罪

## 计算机犯罪

所谓计算机犯罪，就是在信息活动领域中，利用计算机信息系统或计算机信息知识作为手段，或者针对计算机信息系统，对国家、团体或个人造成危害，依据法律规定，应当追究刑事责任的行为。

(1) **以计算机为犯罪对象的犯罪**，如行为人针对个人电脑或网络发动攻击，这些攻击包括“非法访问存储在目标计算机或网络上的信息，或非法破坏这些信息；窃取他人的电子身份等”；

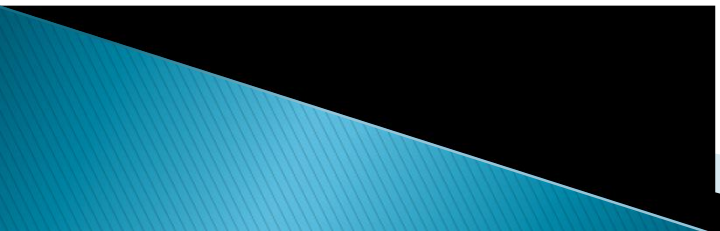
(2) **以计算机作为攻击主体的犯罪**，如当计算机是犯罪现场、财产损失的源头、原因或特定形式时，常见的有黑客、特洛伊木马、蠕虫、传播病毒和逻辑炸弹等；

(3) **以计算机作为犯罪工具的传统犯罪**，如使用计算机系统盗窃他人信用卡信息，或者通过连接互联网的计算机存储、传播淫秽物品、传播儿童色情等。

# 第9章 网络安全--计算机病毒与计算机犯罪

---

## 计算机犯罪防范对策

- (1) 完善计算机立法。
  - (2) 加强惩治计算机犯罪的应对机制。
  - (3) 加强计算机安全技术研究，提高计算机系统本身的技术防御能力。
  - (4) 加强管理与教育。
- 



# 第9章 网络安全—职业道德

---

## 计算机专业技术人员的道德责任

法律是道德的底线，每一位计算机从业人员必须牢记：严格遵守这些法律法规正是计算机从业人员职业道德的最基本要求。

世界知名的计算机道德规范组织IEEE-CS/ACM软件工程师道德规范和职业实践(SEEPP)联合工作组曾就此专门制订过一个规范，根据此项规范计算机职业从业人员职业道德的**核心原则**主要有以下两项：

**原则一：计算机从业人员应当以公众利益为最高目标。**这一原则可以解释为以下八点：

1. 对工作承担完全的责任；
2. 用公益目标节制雇主、客户和用户的利益；
- 3.. 批准软件，应在确信软件是安全的、符合规格说明的、经过合适测试的、不会降低生活品质、影响隐私权或有害环境的条件之下，一切工作以大众利益为前提；
4. 当他们有理由相信有关的软件和文档，可以对用户、公众或环境造成任何实际或潜在的危害时，向适当的人或当局揭露；
5. 通过合作全力解决由于软件、及其安装、维护、支持或文档引起的社会严重关切的各种事项；
6. 在所有有关软件、文档、方法和工具的申述中，特别是与公众相关的，力求正直，避免欺骗；
7. 认真考虑诸如体力残疾、资源分配、经济缺陷和其他可能影响使用软件益处的各种因素；
8. 应致力于将自己的专业技能用于公益事业和公共教育的发展。

**原则二：客户和雇主在保持与公众利益一致的原则下,计算机从业人员应注意满足客户和雇主的最高利益。这一原则可以解释为以下九点：**

1. 在其胜任的领域提供服务，对其经验和教育方面的不足应持诚实和坦率的态度；
2. 不明知故犯使用非法或非合理渠道获得的软件；
3. 在客户或雇主知晓和同意的情况下，只在适当准许的范围内使用客户或雇主的资产；
4. 保证他们遵循的文档按要求经过某一人授权批准；
5. 只要工作中所接触的机密文件不违背公众利益和法律，对这些文件所记载的信息须严格保密；
6. 根据其判断，如果一个项目有可能失败，或者费用过高，违反知识产权法规，或者存在问题，应立即确认、文档记录、收集证据和报告客户或雇主；
7. 当他们知道软件或文档有涉及到社会关切的明显问题时，应确认、文档记录、和报告给雇主或客户；
8. 不接受不利于为他们雇主工作的外部工作；
9. 不提倡与雇主或客户的利益冲突，除非出于符合更高道德规范的考虑，在后者情况下，应通报雇主或另一位涉及这一道德规范的适当的当事人。

# 第9章 网络安全—职业道德

## 信息产业的法律法规

以法律法规来调整和规范社会行为是现代文明社会的重要特征。随着依法治国方略的确定，我国社会主义法制建设的步伐明显加快，法律体系逐步健全。由于信息产业的特殊性，不仅要掌握法律基础知识，也要了解与信息产业相关的法律法规。

道德要高于法律，计算机专业人员在工作中首先要遵守职业道德。

# 第9章 网络安全—职业道德

## 网络信息安全的法律法规

- ▶ 我国已经建立的网络安全保障制度：

计算机信息系统安全等级保护制度、  
计算机信息系统国际联网备案制度、  
安全专用产品销售许可证制度、  
计算机案件强行报案制度、  
计算机信息系统使用单位安全负责制度、  
计算机病毒专管制度、  
商用密码管理制度、  
互联网信息服务安全管理制度、  
电信安全管理制度、  
信息安全检测、  
评估和认证安全监督管理制度、  
计算机信息媒体进出境申报制度等。

# 第9章 网络安全—职业道德

## 计算机软件著作权保护

- ▶ 根据国家颁布的著作权法，计算机软件作为作品形式之一，受到著作权法的保护。软件著作权人被赋予以下几项权利：
- ▶ **发表权**，即决定软件是否公之于众的权利；
- ▶ **开发者身份权**，即表明开发者身份的权利以及在其软件上署名的权利；
- ▶ **使用权**，即在不损害社会公共利益的前提下，以复制、展示、发行、修改、翻译、注释等方式使用其软件的权利。
- ▶ **使用许可权和获得报酬权**，即许可他人以上述方式使用其软件的权利和由此获得报酬的权利；
- ▶ **转让权**，即向他人转让上述使用权和使用许可权的权利。



# 第 9 章 网络安全——回答问题

---

学完本章，你将如何回答下列问题：

1. 什么是网络安全？常见的网络安全问题有哪些？
  2. 为了达到保护信息的目的，可以将信息进行加密，什么是信息加密？具体加密过程是怎样？
  3. 计算机系统的安全性常常取决于系统能否正确识别用户的身份，计算机系统如何对用户的身份进行确认和鉴别？
  4. 如何将安全问题阻挡在网络之外？如何检测网络系统是否被入侵？
  5. 计算机职业道德的基本要求是什么？我国用什么方式对软件实施法律保护？
- 