

# 第1章 绪论

中国科学技术大学

曾凡平

billzeng@ustc.edu.cn

# 主讲教师简介

**曾凡平，计算机科学与技术学院**

个人主页：<http://staff.ustc.edu.cn/~billzeng/>

电子邮件：[billzeng@ustc.edu.cn](mailto:billzeng@ustc.edu.cn)

辅导老师：

姓名：

陶禹帆，tyf1999@mail.ustc.edu.cn

陶圣坤，nonestack@mail.ustc.edu.cn

实验室：高新校区信智楼B802

课程资源：

<https://www.bb.ustc.edu.cn/>

# 关于“信息安全导论”

学时：主讲40学时+40学时实验(10×4学时)

学分：3

时间+教室

第1至14周，周五下午(8,9,10)

15:55~16:40

16:45~17:30

17:35~18:20

3C102 (西区第三教学楼C楼102)

课程编号：011184

主要的教学对象：**19级本科生**

# 关于教材

- 教材

- 理论课：《信息安全概论》，朱节中，姚永雷，北京：科学出版社，2016年6月第一版，2019年8月第5次印刷。
- 实验课：自编电子教材

- 参考书：

- 理论课参考书：《网络信息安全》，曾凡平编著，机械工业出版社, 2016.01
  - ∞ 该教材详细讲解了网络攻防原理和技术，且透彻分析了缓冲区溢出攻击技术和Shellcode技术，有助于学员理解网络与系统攻击的技术原理。
  - ∞ 计算机学院硕士研究生《网络安全》课程教材
- 实验课参考书：电子文档，《SEED: A Suite of Instructional Laboratories for Computer SEcurity EDucation》
  - ∞ <http://www.cis.syr.edu/~wedu/seed/index.html>    <https://seedsecuritylabs.org/>
  - ∞ SEED是美国雪城大学的杜文亮教授（中国科学技术大学少年班学院的校友）精心打造的网络与信息安全方面的实验课程，受到美国自然科学基金委的连续资助，已经在国内外众多高校作为网络与信息安全方面的实验课程，具有全球的影响力。

# 课程简介

- 本课程介绍了**主要的信息安全技术及概念**，包括12个方面的内容：
  - ✓ 密码技术、身份认证、授权与访问控制技术、信息隐藏技术、操作系统和数据库安全、网络与系统攻击技术、网络与系统安全防护及应急响应技术、安全审计与责任认定技术、Internet安全、无线网络安全、恶意代码、内容安全技术。
  - ✓ 所介绍的内容涉及这些信息安全技术的基本概念、发展历史与趋势、面对的威胁与安全需求、采取的基本安全模型与策略、典型的安全体系结构和安全机制，以及基本实现方法和对策等方面。
- **本课程适合本科三年级的同学。**

# 作业和成绩

## 总评成绩：

- 期末考试（**半开卷**）50%
- 作业和考勤25% + 实验25%

## 五个实验：

10次课×4学时

## 课程作业：

- ① 在作业本上手写作业，手机拍照或扫描转换为PDF文档；
- ② 通过Blackboard（<https://www.bb.ustc.edu.cn/>）网络教学平台提交PDF文档。

# 第1章 绪论



1.1 信息安全的概念

1.2 信息安全发展历程

1.3 信息安全技术体系

1.4 信息安全模型

1.5 信息安全保障技术框架

1.6 黑客与网络信息安全（补充）

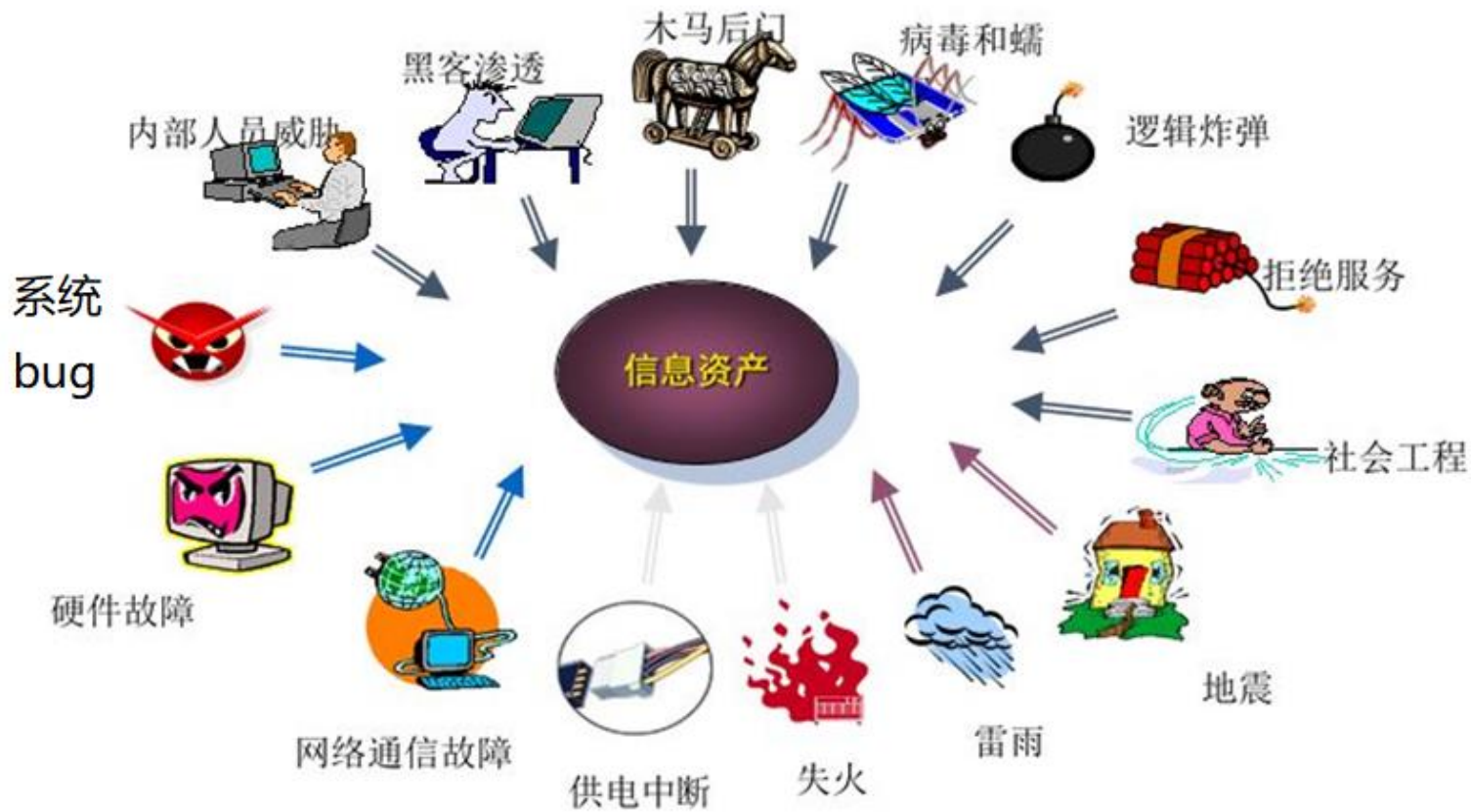
本章作业

# 第1章 绪论

- 人类已经进入信息的时代，**信息**已成为一种重要的**战略资源**，信息技术也成为了衡量国家竞争力的重要标志。
- 随着信息化技术的发展，越来越多的业务依赖于信息系统，信息安全问题日益凸显。
- 信息安全问题已经威胁到国家的政治、经济和国防等多个关键领域，必须采取措施确保我国的信息安全。
- 信息安全事关国家安全、社会稳定，已成为当今信息化建设的核心问题之一。
- 如果不重视信息安全，将会导致灾难性的后果。



# 信息安全威胁无处不在！ 严重的信息安全事件有很多！



习近平指出：没有网络安全就没有国家安全



# 1.1 信息安全的概念

- **信息**：事物运动的**状态和状态变化**的方式
  - ——钟义信，《信息科学原理》，1988
- **信息安全**：指信息系统的软件、硬件以及系统中存储和传输的数据受到保护，不因偶然的或者恶意的原因而遭到破坏、更改、泄露，信息系统连续、可靠、正常地运行，信息服务不中断。
- 信息安全的目的是保护网络与信息系统中信息的**机密性、完整性、不可抵赖性、可用性和可控性**等**信息安全属性**。
- **机密性、完整性、可用性**也称为**信息安全的三要素**。其他的信息安全属性与这3个要素密切相关、或可以从这3个要素导出。

消息层次

网络层次

# 信息安全属性

## (1)机密性(Confidentiality, secrecy)

- 能够确保敏感数据或机密数据在存储和传输过程中不被非授权的实体浏览，甚至可以保证不暴露保密通信的事实。
- 通常通过访问控制阻止非授权用户获得机密信息，通过加密变换阻止非授权用户获知信息内容。

## (2)完整性(integrity)

- 能够保障被传输、接收、存储的数据是完整和未被非法修改的，在被非法修改的情况下能够发现被非法修改的事实和位置。
- 一般通过访问控制阻止篡改行为，同时通过消息摘要算法来检验信息是否被篡改。信息的完整性包括数据和系统的完整性。

# 信息安全属性

## (3)真实性(authenticity)

- 参与通信或操作的实体（用户、进程、系统等）身份的真实以及信息来源的是否真实。确保实体就是所声称的实体。技术：标识和认证

## (4)不可否认性(non-repudiation)

- 实体的行为或事件的结果是不能被否认的。能够保证信息系统的操作者和信息的处理者不能够否认其操作行为和处理结果，防止参与操作或通信的某一方事后否认该操作和通信行为的发生。
- 技术：审计和日志，数字签名和安全协议

## (5)可靠性(dependability)

- 信息系统运行的过程和结果是可以被信赖的。通常用平均无故障时间来描述；如果系统被黑客控制，则不可靠。

# 信息安全属性

## (6)可用性(Availability, usability, 第3个信息安全要素)

- 当突发事件（故障、攻击等）发生时，用户依然能够得到或使用信息系统的数据，信息系统的服务亦能维持运行。
- 可用性是指保障信息资源随时可提供服务的能力特性，即授权用户根据需要可以随时访问所需信息。
- **可用性**是信息资源服务**功能和性能可靠性的度量**，涉及到物理、网络、系统、数据、应用和用户等多方面的因素，是对信息网络**总体可靠性**的要求。

## (7)可控性(controllability)

- 能够掌握和控制信息及信息系统的情况，对信息和信息系统的使用进行可靠的授权、审计、责任认定、传播源与传播路径的跟踪和监管等。技术：**访问控制**



# 四大安全属性？

## (8) 保鲜性(新鲜性)

- 也就是说信息必须是在其**时效之内**的，不能是过时的。新鲜性对保证**物联网的安全**尤其重要。
- **王小云**院士在2018年9月7日“**中国科大-合肥物联网安全与智慧城市高峰论坛**”的报告中提出四大安全属性：
  - ① 机密性
  - ② 可认证性：
    - 通过哈希函数实现信息的可认证？
  - ③ 不可抵赖
  - ④ 完整性

# 信息安全威胁

- 信息安全可被理解为信息系统**抵御信息安全威胁**，**保证**信息系统处理维护的**数据以及**提供的**服务**的机密性、完整性、真实性、不可否认性、可靠性、可用性、可控性等**安全属性的能力**。
- 所谓**信息安全威胁**，就是对信息资源或信息系统的**安全使用**可能造成的危害，主要包括**意外事件**和人为**恶意攻击**两大类。精心设计的人为恶意攻击的威胁最大。
- 信息安全威胁**也可以理解为**某个人、物、事件或概念对信息资源的保密性、完整性、可用性或合法使用所造成的危险。



# 信息安全威胁

## (1)信息泄露

- 保护的信息被泄露或透露给某个非授权的实体。
- 典型攻击手段是窃听和通信业务流分析。窃听是指用各种可能的合法或非法的手段窃取系统中的信息资源和敏感信息，例如对通信线路中传输的信号搭线监听；通信业务流分析则通过对系统进行长期监听，利用统计分析方法对诸如通信频度、通信的信息流向、通信总量的变化等参数进行研究，从中发现有价值的信息和规律。

## (2)非授权的篡改

- 信息的内容被非授权地进行增删、修改或破坏而受到损失。

## (3)拒绝服务

- 信息使用者对信息或其他资源的合法访问被无条件地阻止。如：分布式拒绝服务攻击。

## (4)非法使用（非授权访问）

- 某一资源被某个非授权的人或系统使用，或以非授权的方式使用（越权使用）。

## (5)假冒

- 一个非法用户或信息系统通过冒充成为另一个合法用户或合法系统，或者特权小的用户 / 系统冒充成为特权大的用户 / 系统。

# 信息安全威胁

## (6)抵赖

- 一种来自用户的攻击，涵盖范围比较广泛。比如，否认自己曾经发布过的某条消息，否认曾经处理过某些信息等。

## (7)网络与系统攻击

- 利用网络系统和协议的缺陷和漏洞，进行恶意的侵入和破坏。比如，缓冲区溢出攻击。

## (8)恶意代码

- 开发、传播意在破坏计算机系统、窃取机密或远程控制程序，主要包括计算机病毒、蠕虫、木马、僵尸网络等。比如，恶意网站的恶意网页。

# 信息安全威胁

## (9)自然灾害

- 如火灾、水灾等意外事件，损毁、破坏信息系统的硬件设备，从而使得信息和信息系统不可用。

## (10)人为失误和故意破坏

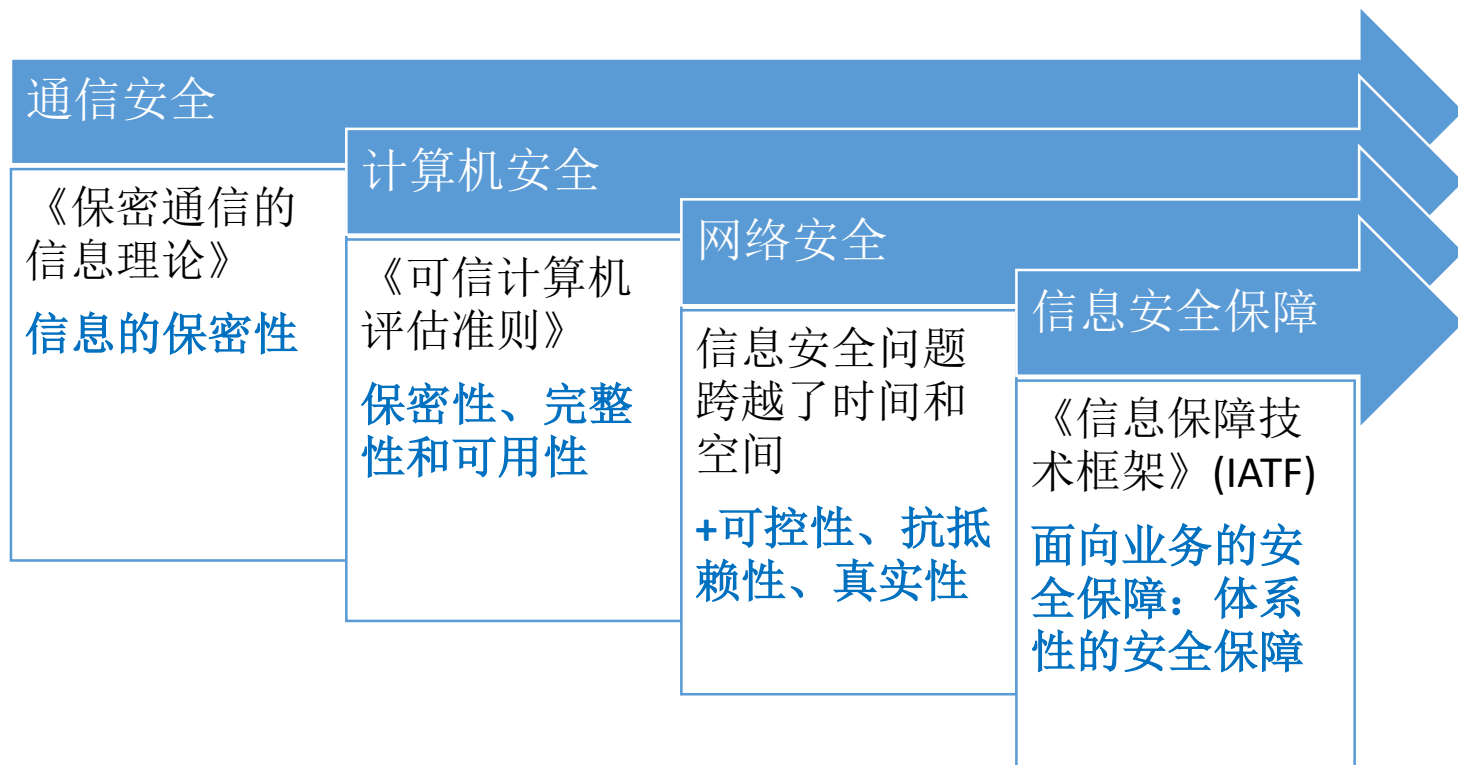
- 恶意的人故意破坏，或者授权用户的操作失误，使得信息或信息系统遭到损坏。
- 安全威胁分别破坏不同的信息安全属性。

# 信息安全是相对的，不安全才是绝对的

- 要保证网络信息安全就必须想办法在一定程度上克服以上的种种威胁，加深对网络攻击技术发展趋势的了解，尽早采取相应的防护措施。
- 需要指出的是无论采取何种防范措施都不能保证网络信息的绝对安全。**安全是相对的，不安全才是绝对的。**
- 在技术的具体使用过程中，经济因素和时间因素是判别安全性的重要指标。换句话说，**过时的“成功”和“赔本”的攻击都被认为是无效的。**

## 1.2 信息安全发展历程

- 信息安全技术随着人类社会的发展而发展，从最初的信息保密发展到现在的信息安全保障技术。
- 大体上，信息安全发展经历了4个时期。



# 第一时期：通信安全时期

- 其主要标志是1949年香农发表的《保密通信的信息理论》。
- 在这个时期通信技术还不发达，电脑只是零散地位于不同的地点，信息系统的安全仅限于保证电脑的物理安全以及通过密码技术（主要是序列密码）解决通信安全的保密问题。把电脑安置在相对安全的地点，不容许非授权用户接近，就基本可以保证数据的安全性了。
- 这个时期的安全性是指**信息的保密性**，对安全理论和技术的研究也仅限于**密码学**。这一阶段的信息安全技术可以简称为**通信安全**，关注如何**保证数据在从一地传送到另一地时的安全性**。

## 第二个时期：计算机安全时期

- 以20世纪70～80年代推出的《可信计算机评估准则》（Trusted Computer System Evaluation Criteria，俗称橘皮书，1985年再版）为标志。
- 在20世纪60年代后，信息已经分成静态信息和动态信息。人们对安全的关注已经逐渐扩展为以**保密性、完整性和可用性**为目标的**信息安全阶段**，主要保证动态信息在传输过程中不被窃取，即使窃取了也不能读出正确的信息；还要保证数据在传输过程中不被篡改，让读取信息的人能够看到正确无误的信息。
- 1977年美国国家标准局(NBS)公布的国家**数据加密标准(DES)**和1983年美国国防部公布的**可信计算机系统评估准则**标志着解决计算机信息系统保密性问题的研究和应用迈上了历史的新台阶。



## 第三个时期：网络安全时代

- 第三个时期是在20世纪90年代兴起的网络安全时代。
- 从20世纪90年代开始，由于互联网技术的飞速发展，信息无论是企业内部还是外部都得到了极大的开放，而由此产生的信息安全问题跨越了时间和空间，信息安全的焦点已经从传统的保密性、完整性和可用性三个原则衍生为**可控性、抗抵赖性、真实性**等其他的原则和目标。
- 防火墙、入侵检测、漏洞扫描、安全评估等技术迅速发展并普及。

## 第四个时期：信息安全保障时代

- 21世纪的信息安全保障时代，其主要标志是《**信息保障技术框架**》(IATF)。
- **面向业务的安全保障：体系性的安全保障**理念，不仅是关注系统的漏洞，而且是从业务的生命周期着手，对业务流程进行分析，找出流程中的关键控制点，从安全事件出现的前、中、后三个阶段进行安全保障。
- 面向业务的安全保障不是只建立防护屏障，而是建立一个“**深度防御体系**”，通过更多的技术手段把安全管理与技术防护联系起来，不再是被动地保护自己，而是主动地防御攻击。
- 也就是说，面向业务的安全防护已经从被动走向主动，安全保障理念从风险承受模式走向安全保障模式。信息安全阶段也转化为**从整体角度考虑其体系建设的信息安全保障时代**。

# 1.3 信息安全技术体系



## ①核心基础安全技术

- 密码技术
- 信息隐藏技术等

## ②安全基础设施技术

- 标识与认证技术
- 授权与访问控制技术等

## ③基础设施安全技术

- 主机系统安全技术
- 网络系统安全技术等

## ④应用安全技术

- 网络与系统攻击技术
- 网络与系统安全防护与应急响应技术
- 安全审计与责任认定技术
- 恶意代码检测与防范技术、内容安全技术等

## ⑤支撑安全技术

- 信息安全保障技术框架
- 信息安全测评与管理技术等

# 信息安全技术的关联

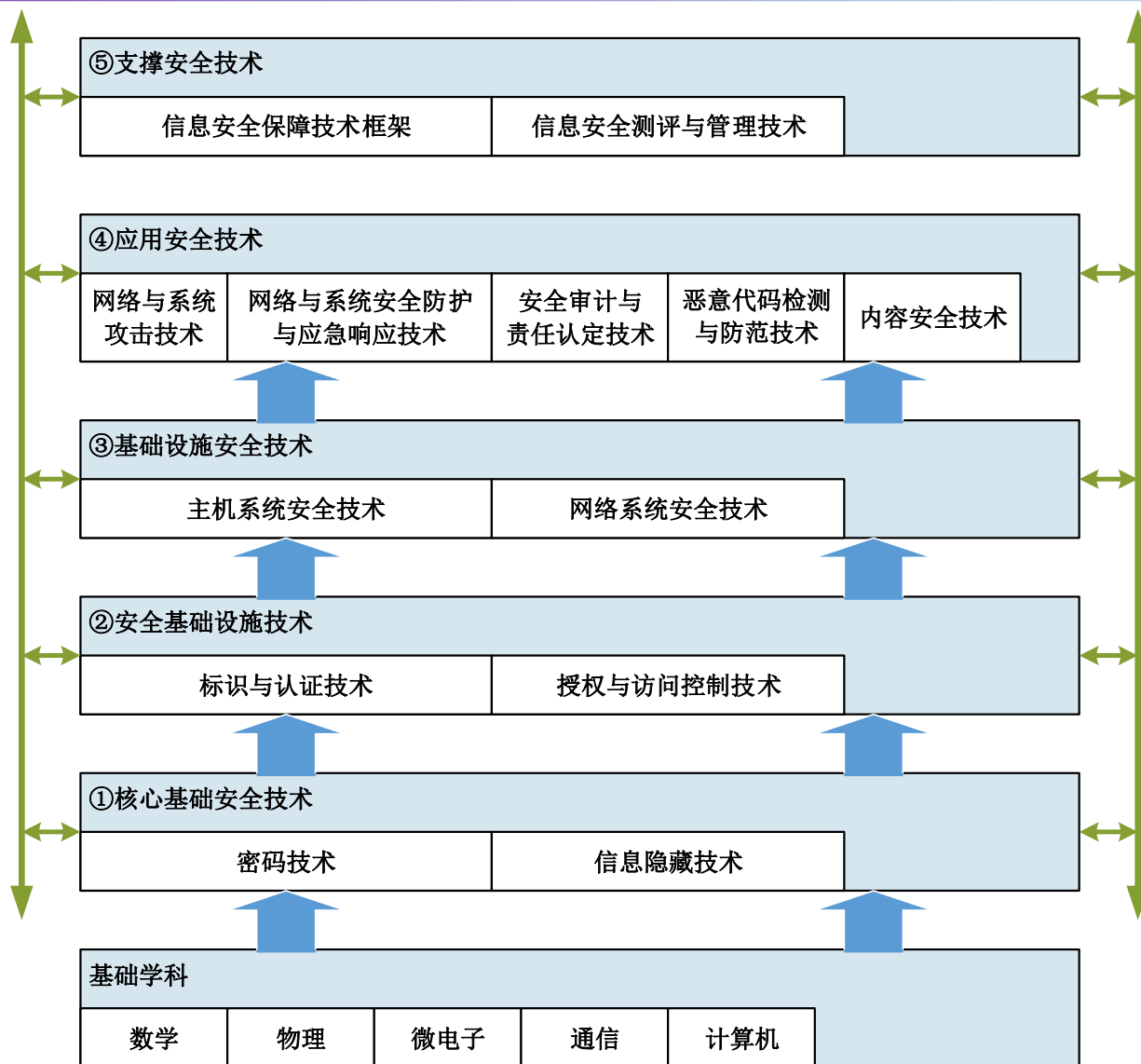


图1-1 信息安全技术体系框图

# 1)信息安全保障技术框架 ← ⑤支撑安全技术

⑤支撑安全技术		
信息安全保障技术框架	信息安全测评与管理技术	

- 信息安全保障技术框架(IATF)定义了对一个系统进行信息安全保障的过程，以及该系统中硬件和软件部件的安全要求，遵循这些要求可以对信息基础设施进行深度防御。其**基本内容是深度防御策略、信息保障框架域和信息系统安全**。
- 深度防御策略的出现使人们清晰地意识到，实施信息安全保障的难度之所以在持续不断地增大，既源于技术革新带来的挑战，又源于操作和管理方式的调整需求，同时也时刻接受处于不间断增强过程中人类智力的挑战，**必须全面考虑人、技术和操作（与管理）这三个要素**。

# 1)信息安全保障技术框架

- 相对于信息安全保障的丰富内涵而言，深度防御策略只是一个思路，由保护网络与基础设施、保护区域边界和外部连接、保护计算环境及支持性基础设施这四个框架域所共同组成的技术细节和渗透其中的众多操作与管理规则才是信息安全保障得以有效实施的基石。
- 信息系统安全工程集中体现了信息安全保障的过程化需求，使信息安全保障呈现一个多维的、多角度的操作场景，将其视为信息安全保障可以遵循的基础方法论。

## 2)密码技术← ①核心基础安全技术



- 密码技术主要包括密码算法和密码协议的设计与分析技术。
- **密码算法**包括分组密码、序列密码、公钥密码、杂凑(哈希)函数、数字签名等，它们在不同的场合分别用于提供机密性、完整性、真实性、可控性和不可否认性，**是构建安全信息系统的基本要素**。
- **密码协议**是在消息处理环节采用了密码算法的协议，它们运行在计算机系统、网络或分布式系统中，为安全需求方提供安全的交互操作。
- **密码分析技术**指在获得一些技术或资源的条件下**破解密码算法或密码协议**的技术。其中，资源条件主要指分析者可能截获了密文、掌握了明文或能够控制和欺骗合法的用户等。密码分析可被密码设计者用于提高密码算法和协议的安全性，也可被恶意的攻击者利用。

# 密码技术实例

实验环境： 32bit **ubuntu Linux** 16.04 LTS

- 杂凑(哈希)函数**md5**用于鉴别完整性

文件被修改，则其md5值变化

```
openssl md5 lshome.txt
```

```
md5sum lshome.txt
```

- 密码算法用于提供机密性

- 加密后的信息是不可（或难于）理解的

```
md5sum lsroot.txt > deskey.txt
```

```
openssl enc -e -des -in lshome.txt -out lshome.des -kfile deskey.txt
```

```
cat lshome.des
```

```
openssl enc -d -des -in lshome.des -out lshome.ttt -kfile deskey.txt
```



### 3)标识与认证技术← ②安全基础设施技术

②安全基础设施技术		
标识与认证技术	授权与访问控制技术	

- **标识(identity)是指实体的表示**，信息系统通过标识可以对应到一个实体。标识的例子在计算机系统中比比皆是，如用户名、用户组名、进程名、主机名等，没有标识就难以对系统进行安全管理。
- **认证技术就是鉴别实体身份的技术**，主要包括口令技术、公钥认证技术、在线认证服务技术、生物认证技术与公钥基础设施(public key infrastructure, PKI)技术等，还包括对数据起源的验证。随着电子商务和电子政务等分布式安全系统的出现，公钥认证及基于它的PKI技术在经济和社会生活中的作用越来越大。

## 4)授权与访问控制技术← ②安全基础设施技术

②安全基础设施技术		
标识与认证技术	授权与访问控制技术	

- 为了使得合法用户正常使用信息系统，需要**给已通过认证的用户授予相应的操作权限**，这个过程被称为授权。
- 在信息系统中，可授予的权限包括读 / 写文件、运行程序和网络访问等，**实施和管理这些权限的技术称为授权技术**。
- 访问控制技术和授权管理基础设施(privilege management infrastructure, PMI)技术是两种常用的技术。
- 从应用目的上看，网络防护中的防火墙技术也有访问控制的功能，但由于实现方法与普通的访问控制有较大不同，一般将防火墙技术归入网络防护技术。

# 安全基础设施技术实例

## ubuntu Linux系统的安全基础设施

- 标识与认证

用户标识：用户ID，存放在/etc/passwd文件

用户认证：用户的口令，存放在/etc/shadow文件

- 授权与访问控制

每个用户和组被赋予不同的访问资源的权限

通过uid,euid,gid和egid，实现自主访问控制

- 演示：

gedit /etc/passwd

id

## 5)信息隐藏技术← ①核心基础安全技术

①核心基础安全技术		
密码技术	信息隐藏技术	

- 信息隐藏是指将特定用途的信息隐藏在其他可公开的数据或载体中，使得它难以被消除或发现。
- 信息隐藏主要包括隐写 (steganography)、数字水印 (watermarking)与软硬件中的数据隐藏等，其中水印又分为鲁棒性水印和脆弱性水印。
- 比如：对数字媒体和软件的版权保护，可采用水印技术。
- 在保密通信中，加密用来掩盖保密的内容，而隐写通过掩盖保密的事实带来附加的安全。
- 与密码技术类似，信息隐藏技术也包括相应的分析技术。

# 实例：在图像中嵌入秘密信息

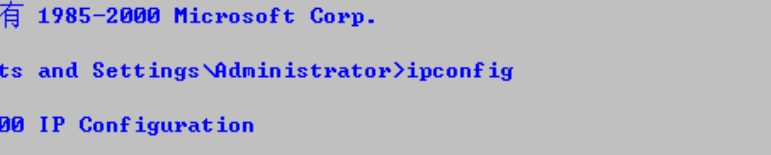


## 6)网络与系统攻击技术← ④应用安全技术

④应用安全技术				
网络与系统 攻击技术	网络与系统安全防护 与应急响应技术	安全审计与 责任认定技术	恶意代码检测 与防范技术	内容安全技术

- 网络与系统攻击技术是指攻击者利用信息系统弱点(**vulnerability**, **漏洞**)破坏或非授权地侵入网络和系统的技术。
- 主要的网络与系统攻击技术包括网络与系统调查、口令攻击、拒绝服务攻击(**denial of services**, **DoS**)、缓冲区溢出攻击等。
  - 网络与系统调查是指攻击者对网络信息和弱点的搜索与判断;
  - 口令攻击是指攻击者试图获得其他人的口令而采取的攻击;
  - 拒绝服务攻击是指攻击者通过发送大量的服务或操作请求使服务程序出现难以正常运行的情况;
  - **缓冲区溢出攻击**属于针对主机的攻击,它利用了系统堆栈结构,通过在缓冲区写入超过预定长度的数据造成所谓的溢出,破坏了堆栈的缓存数据,使程序的返回地址发生变化。

## 实例：缓冲区溢出攻击



The screenshot shows a Windows 2000 command prompt window with a blue title bar that reads "选定 命令提示符". The window contains the following text:

```
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-2000 Microsoft Corp.

C:\Documents and Settings\Administrator>ipconfig

Windows 2000 IP Configuration

Ethernet adapter 本地连接:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.86.200
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.86.1

C:\Documents and Settings\Administrator>
```

```

C:\CMM - kaht2.exe 192.168.86.199 192.168.86.201

[+] Targets: 192.168.86.199-192.168.86.201 with 50 Threads
[+] Attacking Port: 135. Remote Shell at port: 47767
[+] Scan In Progress...
- Connecting to 192.168.86.200
  Sending Exploit to a [Win2k] Server...
- Conectando con la Shell Remota...

Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-2000 Microsoft Corp.

C:\WINNT\system32>_

```

## 7)网络与系统安全防护及应急响应技术← ④应用安全技术

④应用安全技术					
网络与系统攻击技术	网络与系统安全防护与应急响应技术	安全审计与责任认定技术	恶意代码检测与防范技术	内容安全技术	

- 网络与系统安全防护技术就是**抵御网络与系统遭受攻击**的技术，它**主要包括防火墙和入侵检测技术**。防火墙设置于受保护网络或系统的入口处，起到防御攻击的作用；入侵检测系统(intrusion detection system, **IDS**)一般部署于系统内部，用于检测非授权侵入。
- 另外，当前的网络防护还包括“**蜜罐(honeypot)**”技术，它通过诱使攻击者入侵“蜜罐”系统来搜集、分析潜在的攻击者的信息。
- 当网络或系统遭到入侵并遭到破坏时，**应急响应技术**有助于管理者尽快恢复网络或系统的正常功能并采取一系列必要的应对措施。



# 防火墙实例：ubuntu linux自带的防火墙

---

- 查看防火墙的状态

`sudo ufw status`

- 关闭防火墙

`sudo ufw disable`

- 启用防火墙

`sudo ufw enable`

- 允许ssh端口

`sudo ufw allow ssh`

- 拒绝ssh端口

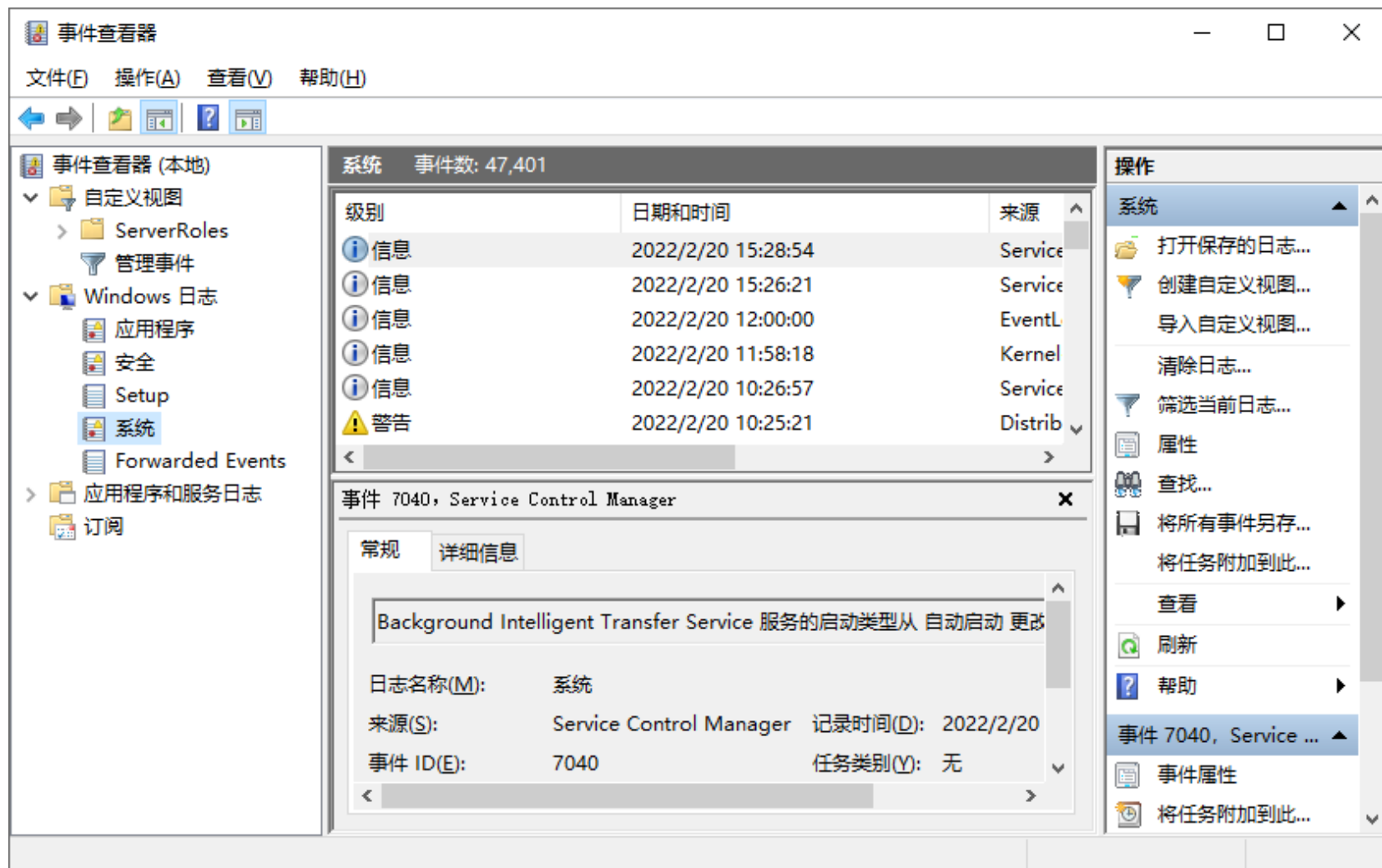
`sudo ufw deny ssh`

## 8)安全审计与责任认定技术← ④应用安全技术

④应用安全技术				
网络与系统 攻击技术	网络与系统安全防护 与应急响应技术	安全审计与 责任认定技术	恶意代码检测 与防范技术	内容安全技术

- 为抵制网络攻击、电子犯罪和数字版权侵权，安全管理部门或执法部门需要**相应事件的调查方法与取证手段**，这种技术被统称为安全审计与责任认定技术。
- 审计系统普遍存在于计算机和网络系统中，它们按照安全策略记录系统出现的各类审计事件，主要包括用户登录、特定操作、系统异常等与系统安全相关的事件。
- 安全审计记录有助于调查与追踪系统中发生的安全事件，为诉讼电子犯罪提供线索和证据，但在系统外发生的事件显然也需要新的调查与取证手段。
- 数字版权侵权的现象在全球都比较严重，数字版权技术在发现版权侵权后进行盗版调查和追踪。

# 安全审计实例：Windows系统的事件查看器

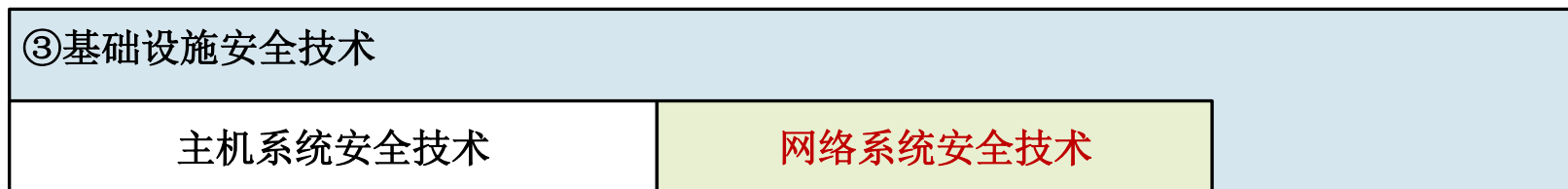


## 9)主机系统安全技术← ③基础设施安全技术



- **主机系统主要包括操作系统和数据库系统等**。操作系统需要保护所管理的软硬件、操作和资源等的安全，数据库需要保护业务操作、数据存储等的安全，这些安全技术一般被称为主机系统安全技术。
- 从技术体系上看，主机系统安全技术采纳了大量的标识与认证及授权与访问控制等技术，但也包含自身固有的技术，如获得内存安全、进程安全、账户安全、内核安全、业务数据完整性和事务提交可靠性等技术，并且设计高等级安全的操作系统需要进行形式化论证。
- 当前，**“可信计算”**技术主要指在硬件平台上引入安全芯片和相关密码处理来提高终端系统的安全性，将部分或整个计算平台变为可信的计算平台，使用户或系统能够确信发生了所希望的操作。

## 10)网络系统安全技术← ③基础设施安全技术



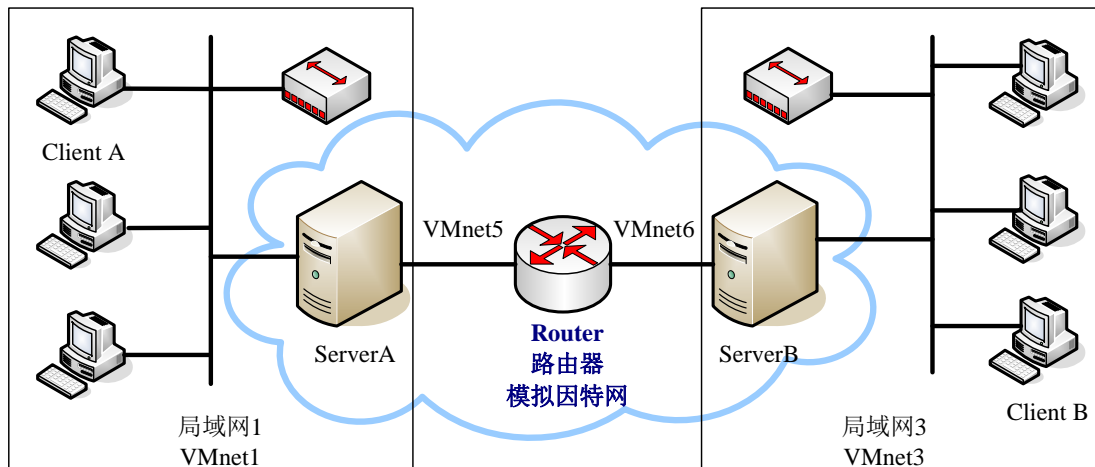
- 在基于网络的分布式系统或应用中，信息需要在网络中传输，用户需要利用网络登录并执行操作，因此需要相应的信息安全措施，本书将它们统称为网络系统安全技术。由于分布式系统跨越的地理范围一般较大，因此一般面临着公用网络中的安全通信和实体认证等问题。
- 国际标准化组织(International Organization for Standardization, ISO)于20世纪80~90年代推出了网络安全体系的参考模型与系统安全框架，其中描述了安全服务在ISO开放系统互连(open systems interconnection, OSI)参考模型中的位置及其基本组成。

## 10)网络系统安全技术

- 在OSI参考模型的影响下，逐渐出现了一些实用化的网络安全技术和系统，其中多数均已标准化，主要包括提供传输层安全的SSL/TLS (secure socket layer/transportation layer security)系统、提供网络层安全的IPSec系统及提供应用层安全的安全电子交易SET(secure electronic transaction)系统。
- 值得注意的是，国际电信联盟 (International Telecommunication Union, ITU)制定的关于PKI技术的ITU-T X.509标准极大地推进、支持了上述标准的发展和应用。

# 网络系统安全实例：IPSec VPN技术

网关至网关  
VPN:  
用IPSec实现  
2个局域网  
的安全连接。



加密的数据包

Capturing from VMnet5 [Wireshark 1.10.6 (v1.10.6 from master-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Appl Save

No.	Time	Source	Destination	Protocol	Length	Info
2	0.00302200	166.66.66.213	55.55.55.203	ESP	126	ESP (SPI=0x54fbc59)
3	1.07154200	55.55.55.203	166.66.66.213	ESP	126	ESP (SPI=0x0bb5814b)
4	1.07432200	166.66.66.213	55.55.55.203	ESP	126	ESP (SPI=0x54fbc59)
5	2.13326600	55.55.55.203	166.66.66.213	ESP	126	ESP (SPI=0x0bb5814b)
6	2.13616500	166.66.66.213	55.55.55.203	ESP	126	ESP (SPI=0x54fbc59)
7	3.19435200	55.55.55.203	166.66.66.213	ESP	126	ESP (SPI=0x0bb5814b)
8	3.20052000	166.66.66.213	55.55.55.203	ESP	126	ESP (SPI=0x54fbc59)
9	14.9406040	55.0.0.1	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
10	15.9409430	55.0.0.1	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
11	16.9416940	55.0.0.1	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
12	17.9426990	55.0.0.1	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1

VMnet5: <live capture in progress> File: C:\C Packets: 12 · Displayed: 12 (100.0%) Profile: Default

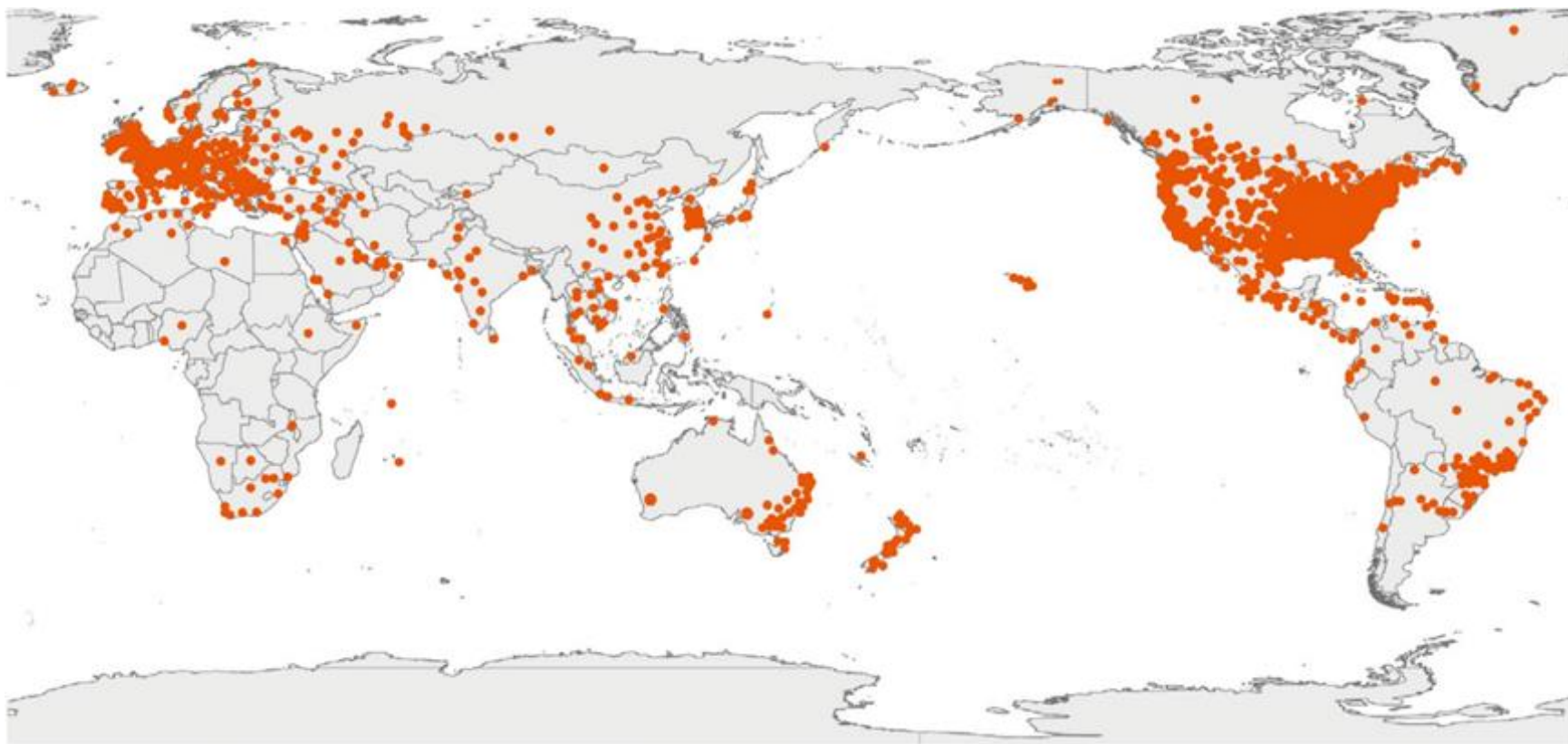
## 11)恶意代码检测与防范技术← ④应用安全技术

④应用安全技术				
网络与系统 攻击技术	网络与系统安全防护 与应急响应技术	安全审计与 责任认定技术	恶意代码检测 与防范技术	内容安全技术

- 对恶意代码的检测与防范是普通计算机用户熟知的概念，但具体技术实现起来比较复杂。在原理上，**防范技术需要利用恶意代码的不同特征来检测并阻止其运行**，但不同的恶意代码的特征可能差别很大，这往往使特征分析存在困难。如今已有了一些能够帮助发掘恶意代码的静态和动态特征的技术，也出现了一系列在检测到恶意代码后阻断其恶意行为的技术。
- 目前，一个很重要的概念就是**僵尸网络(BotNet)**，它是指采用一种或多种恶意代码传播手段，使大量主机感染所谓的**僵尸程序**，从而在控制者和被感染主机之间形成一对多的控制，控制者可以一对多并隐蔽地执行相同的恶意行为。显然，阻断僵尸程序的传播是防范僵尸网络威胁的关键。



# 恶意代码实例：Mirai僵尸网络



Mirai攻击地区分布

2019BOTNET趋势报告, [https://www.nsfocus.com.cn/html/2019/92\\_1130/133.html](https://www.nsfocus.com.cn/html/2019/92_1130/133.html)

## 12)内容安全技术← ④应用安全技术

④应用安全技术				
网络与系统攻击技术	网络与系统安全防护与应急响应技术	安全审计与责任认定技术	恶意代码检测与防范技术	内容安全技术

- 计算机和无线网络的普及方便了数字内容（包括多媒体和文本）的传播，但也使得不良信息内容和侵权内容大量散布。内容安全技术是指**监控数字内容传播**的技术，主要包括网络内容的发现和追踪、内容的过滤和多媒体的网络发现等技术，它们综合运用了面向文本和多媒体的模式识别、高速匹配和网络搜索等技术。
- 在一些文献中，内容安全技术在广义上包括所有涉及保护或监管内容制作和传播的技术，因此包括各类版权保护和内容认证技术，但狭义的内容安全技术一般仅包括与内容监管相关的技术，即本书所称的内容安全技术。

# 13)信息安全测评技术← ⑤支撑安全技术

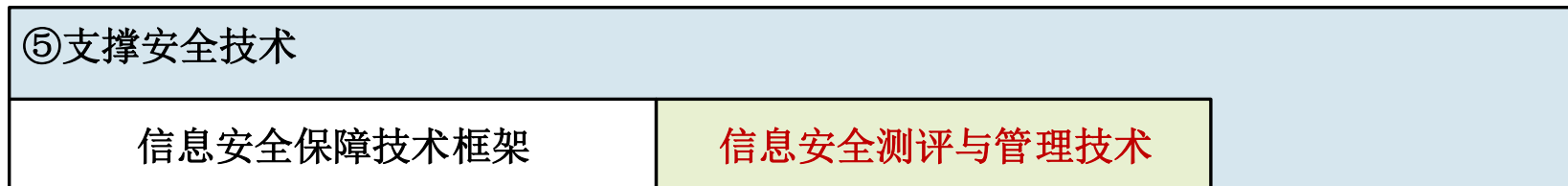
## ⑤支撑安全技术

信息安全保障技术框架

信息安全测评与管理技术

- 为了衡量信息安全技术及其所支撑的系统的安全性，需要进行信息安全测评，它是指对信息安全产品或信息系统的安全性等进行验证、测试、评价和定级，以规范它们的安全特性，而信息安全测评技术就是能够系统、客观地验证、测试和评估信息安全产品和信息系统安全性质和程度的技术。
- 前面已提到有关密码和信息隐藏的分析技术及对网络与系统的攻击技术，它们也能从各个方面评判算法或系统的安全性质，但安全测评技术在目的上一般没有攻击的含义，而在实施上一般有标准可以遵循。
- 当前，发达国家或地区及我国均建立了信息安全测评制度和机构，并颁布了一系列测评标准或准则。

# 14)信息安全管理技术← ⑤支撑安全技术



- 信息安全技术与产品的使用者需要系统、科学的安全管理技术，以帮助他们使用好安全技术与产品，有效地解决所面临的信息安全问题。
- 当前，安全管理技术已经成为信息安全技术的一部分，它**涉及安全管理制度的制定、物理安全管理、系统与网络安全管理、信息安全等级保护及信息资产的风险管理等内容**，已经成为构建信息安全系统的重要环节之一。

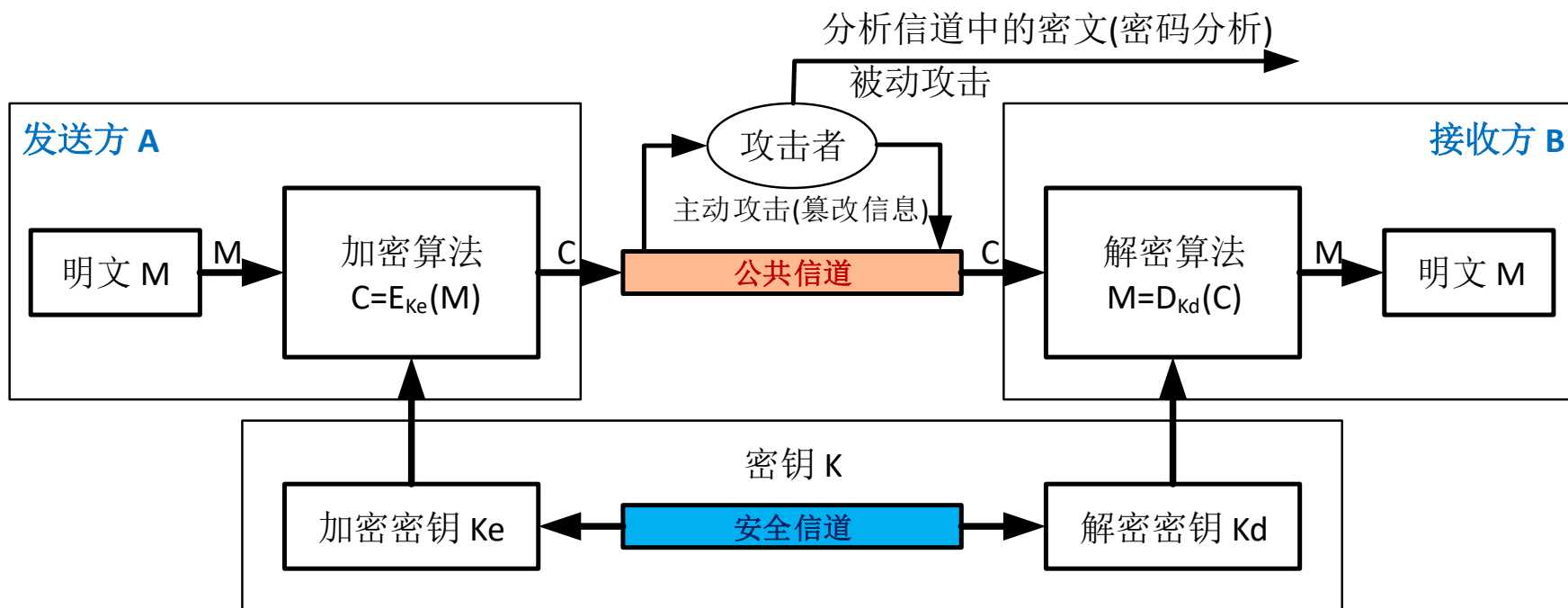
# 实例：本课题组的科研成果（物联网安全测评）



## 1.4 信息安全模型

- **信息安全模型也被称为威胁模型或敌手模型**，是信息系统在何种环境下遭受威胁并获得信息安全的一般性描述。
- 当前有很多信息安全模型，主要包括：
  - ① **Shannon提出的保密通信系统的模型**
    - 该模型描述了保密通信的收发双方通过安全信道获得密钥、通过可被窃听的线路传递密文的场景，确定了收发双方和密码分析者的基本关系和所处的技术环境；
  - ② **Simmons面向认证系统提出了无仲裁认证模型**
    - 它描述了认证方和被认证方通过安全信道获得密钥、通过可被窃听的线路传递认证消息的场景。

# 基于密码学的保密通信系统的模型



保密通信系统的模型

在密文的传输过程中可能会遭受主动和被动攻击：

- (1) 主动攻击是指攻击者篡改截获的信息，再发送到接收方。为了抵抗主动攻击，必须有一种机制识别信息的篡改，这就是**数字签名**技术。
- (2) 被动攻击是指对密文进行分析，试图恢复出明文。为了抵抗被动攻击，密码算法必须**在计算上是安全的**，同时对加密后的信息必须进行重组，以抵抗统计分析。

### ③ Dolev-Yao威胁模型

- Dolev和Yao针对一般信息安全系统提出了**Dolev-Yao威胁模型**，它定义了攻击者在网络和系统中的攻击能力，**被密码协议的设计者广泛采用**。
- 随着密码技术研究的深入，有很多学者认为密码系统的设计者应该将攻击者的能力估计得更高一些，如攻击者可能有控制加密设备或在一定程度上接近、欺骗加密操作人员的能力。这些观点被后来的实例所支持。
- Dolev和Yao还建立了攻击者模型，精确描绘了攻击者的行为。
- Dolev和Yao认为攻击者可以控制整个通信网络，并且提供一个重要的原则：**永远不能低估攻击者的知识和能力**。
- Dolev和Yao的工作具有深远影响，迄今为止的大部分有关安全协议的研究工作都参考或遵循了Dolev和Yao的基本思想。



# Dolev-Yao模型的原始论文

- D. Dolev, A. Yao, On the security of public key protocols, IEEE Transactions on Information Theory. Year: 1983 , Volume: 29 , Issue: 2, Page s: 198 - 208

## On the Security of Public Key Protocols

DANNY DOLEV AND ANDREW C. YAO, MEMBER, IEEE

***Abstract***—Recently the use of public key encryption to provide secure network communication has received considerable attention. Such public key systems are usually effective against passive eavesdroppers, who merely tap the lines and try to decipher the message. It has been pointed out, however, that an improperly designed protocol could be vulnerable to an active saboteur, one who may impersonate another user or alter the message being transmitted. Several models are formulated in which the security of protocols can be discussed precisely. Algorithms and characterizations that can be used to determine protocol security in these models are given.

## 1.5 信息安全保障技术框架

- 《信息保障技术框架》(Information Assurance Technical Framework, IATF)是美国国家安全局(National Security Agency, NSA)制定的, 描述其信息保障的指导性文件。
- 在我国国家973“信息与网络安全体系研究”课题组在2002年将IATF3.0版引进国内后, IATF开始对我国信息安全工作的发展和信息安全保障体系的建设起重要的参考和指导作用。

# 1.5.1 IATF概述

## 1. IATF形成背景

- 建立IATF主要是美国军方需求的推动。二十世纪四五十年代，计算机开始在军事中应用，六七十年代网络化开始发展，这些发展都对信息安全保障提出了要求。
- 从1995年开始，美国国防高级研究计划局和信息技术办公室(DARPA/ITO)就开始了对于长期研发投资战略的探索，以开展信息系统生存力技术研究。
- 1998年1月，美国国防部(DoD)副部长批准成立了DIAP(国防范畴内信息保障项目)，从而得以为DoD的信息保障活动和资源利用制定计划并进行协调、整合和监督。
- DIAP成为了国防部IA项目的核心部分。

## IATF形成背景

- 除了军事机构外，随着社会的发展，各种信息系统已经成为支持整个社会运行的关键基础设施，而且信息化涉及的资产也越来越多，由此产生的各种风险和漏洞也随之增多，而且现有的技术无法完全根除。
- 面对这些威胁，人们越来越深刻地认识到信息安全保障的必要性。
- 在此背景下，从1998年开始，美国国家安全局历经数年完成了《信息保障技术框架》这部对信息保障系统的建设有重要指导意义的重要文献。

## 2. IATF发展历程

- IATF的前身是《网络安全框架》(NSF)，NSF的最早版本(0.1和0.2版)对崭新的网络安全挑战提供了初始的观察和指南。1998年5月，出版了NSF1.0版，在NSF的基础上添加了安全服务、安全强健性和安全互操作性方面的内容。1998年10月又推出了NSF1.1版。
- 到了1999年8月31日，NSA出版了IATF2.0，此时正式将NSF更名为《信息保障技术框架》。IATF2.0版将安全解决方案框架划分为4个纵深防御焦点域：保护网络和基础设施、保护区域边界、保护计算环境以及支撑性基础设施。

## 2. IATF发展历程

- 1999年9月22日推出的IATF2.0.1版本的变更主要以格式和图形的变化为主，在内容上并无很大的变动。
- 2000年9月出版的 IATF3.0版通过将IATF的表现形式和内容通用化，使IATF扩展出了DoD的范围。2002年9月出版了最新的IATF3.1版本，扩展了“纵深防御”，强调了信息保障战略，并补充了语音网络安全方面的内容。
- IATF4.0目前正在编制之中。
- 随着社会对信息安全认识的日益加深，以及信息技术的不断进步，IATF必定会不断发展，内容的深度和广度也将继续得到强化。

### 3. IATF的焦点框架区域划分

- IATF将信息系统的信息保障技术层面划分成了四个技术框架焦点域：网络和基础设施、区域边界、计算环境和支撑性基础设施。
- 在每个焦点领域范围内，IATF都描述了其特有的安全需求和相应的可供选择的技術措施。
- IATF提出这四个框架域，目的就是让人们理解网络安全的不同方面，以全面分析信息系统的安全需求，考虑恰当的安全防御机制。

## 1.5.2 IATF与信息安全的关系

- IATF虽然是在军事需求的推动下由NSA组织开发，但发展至今的IATF已经可以广泛地适用于政府和各行各业的信息安全工作，它所包含的内容和思想可以给各个行业信息安全工作的发展提供深刻的指导和启示作用。

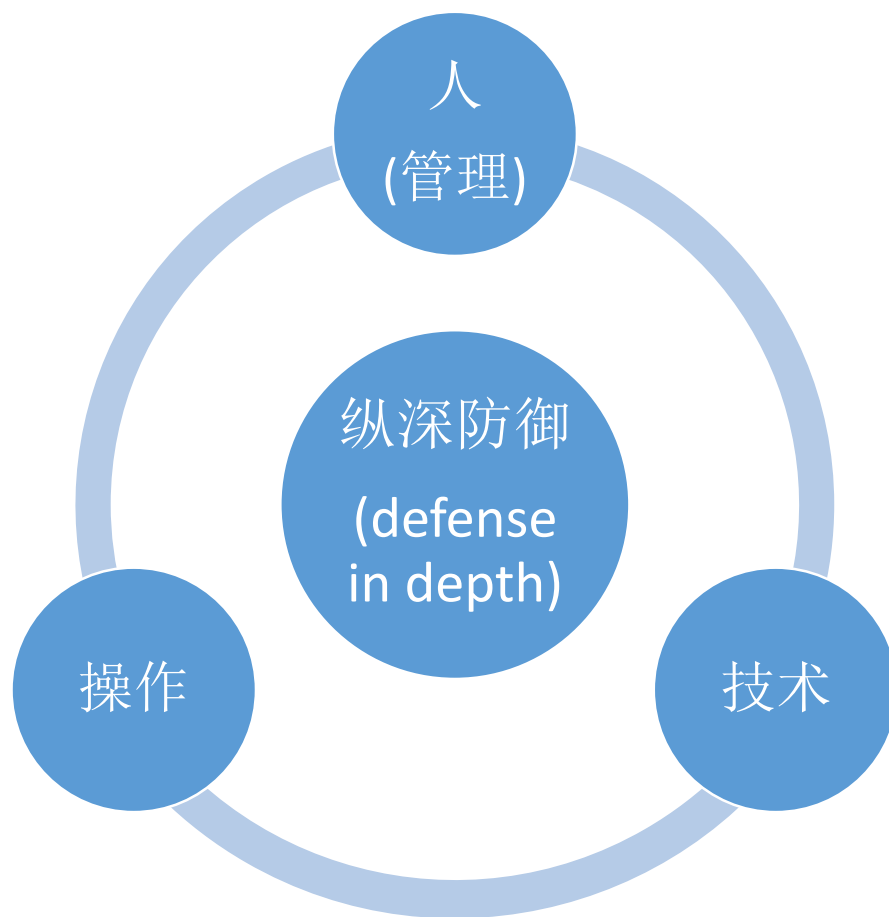
### 1. IATF的核心思想

- IATF提出的信息保障的核心思想是纵深防御战略(defense in depth)。所谓**纵深层防御战略就是采用一个多层次、纵深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要素**，要保障信息及信息系统的安全，三者缺一不可。



# 纵深防御战略(defense in depth)

IATF 提供了**全方位、多层次**的信息保障体系的指导思想，即纵深防御战略思想，通过在各个层次、各个技术框架区域中实施保障机制，才能在最大限度内降低风险，防止攻击，保护信息系统的安全。



此外，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，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，可以说技术是安全的基础，管理是安全的灵魂，所以在重视安全技术应用的同时，必须加强安全管理。

## 2. IATF的其他信息安全(IA)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安全原则，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。

### (1)保护多个位置

- 包括保护网络和基础设施、区域边界、计算环境等。这一原则提醒我们，仅仅在信息系统的重要敏感之处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，所以只有在信息系统的各个方位布置全面的防御机制，才能将风险减至最低。

## (2) 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。

## (3) 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。

# 《网络空间安全战略》

- 为了应对网络空间安全挑战，力图在网络空间安全竞争中处于领先地位，世界各主要强国都制定了“网络空间安全战略”，**将网络空间安全提升到国家战略的高度**。
- **习近平同志指出：“没有网络安全就没有国家安全”**。维护我国网络安全是协调推进全面建成小康社会、全面深化改革、全面依法治国、全面从严治党战略布局的重要举措，是实现“两个一百年”奋斗目标、实现中华民族伟大复兴中国梦的重要保障。
- **2016年12月27日**，经中央网络安全和信息化领导小组批准，国家互联网信息办公室发布《国家网络空间安全战略》。**《国家网络空间安全战略》**阐明中国关于网络空间发展和安全的重大立场，指导中国网络安全工作，维护国家在网络空间的主权、安全、发展利益。

- 《国家网络空间安全战略》指出，“**网络空间的国际竞争方兴未艾**”是我国网络空间安全面临的**重大挑战之一**。国际上争夺和控制网络空间战略资源、抢占规则制定权和战略制高点、谋求战略主动权的竞争日趋激烈。**个别国家强化网络威慑战略，加剧网络空间军备竞赛，世界和平受到新的挑战。**
- 攻击和防护是网络空间安全的两项核心关键技术，**进攻是最好的防守**。为了应对个别国家强化网络威慑战略，我国迫切需要将网络主动防御技术的研究提升为国家战略。
- 本课程介绍信息安全的基本技术，也简要介绍一些网络攻击技术，主要目的是提高同学的网络信息安全意识，提高安全防护能力。

谢谢！